



Cybersecurity and IEC 62443

# Part III – Component Certification

## White Paper

# Contents

- 1. List of Acronyms and Abbreviations ..... 3
- 2. Introduction ..... 5
- 3. Security Levels ..... 6
- 4. Example ..... 7
- 5. Components ..... 8
- 6. Component Requirements ..... 11
- 7. Foundational Requirements ..... 12
- 8. Number of Component Requirements ..... 13
- 9. Common Component Security Constraints ..... 14
- 10. Certification (Conformity Assessment) ..... 15
- 11. Scoring Rubric ..... 16
- 12. Security Vectors ..... 19
- 13. Certificate Format and Interpretation ..... 20
- 14. Not Applicable Requirements vs Out of Scope Requirements ..... 21
- 15. Summary ..... 22
- 16. Endnotes ..... 23

# 1. List of Acronyms and Abbreviations

|       |                                                                                                            |
|-------|------------------------------------------------------------------------------------------------------------|
| AB    | Accreditation Body                                                                                         |
| ANSI  | American National Standards Institute                                                                      |
| BR    | Base Requirement                                                                                           |
| CB    | Certification Body                                                                                         |
| CC    | Compensating Countermeasure                                                                                |
| CCSC  | Common Component Security Constraint                                                                       |
| CPU   | Central Processing Unit                                                                                    |
| CR    | Component Requirement                                                                                      |
| DCS   | Distributed Control System                                                                                 |
| DSR   | Device-Specific Requirement                                                                                |
| EDR   | Embedded Device Requirement                                                                                |
| ESD   | Emergency Shutdown Device                                                                                  |
| FR    | Foundational Requirement                                                                                   |
| HDR   | Host Device Requirement                                                                                    |
| HMI   | Human Machine Interface                                                                                    |
| IACS  | Industrial Automation and Control System                                                                   |
| IEC   | <a href="#">International Electrotechnical Commission</a>                                                  |
| IECEE | <a href="#">IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components</a> |
| ISA   | <a href="#">International Society of Automation</a>                                                        |
| NDR   | Network Device Requirement                                                                                 |
| OS    | Operating System                                                                                           |
| PC    | Personal Computer                                                                                          |
| PCA   | Product Capability Assessment                                                                              |
| PLC   | Programmable Logic Controller                                                                              |
| RE    | Requirement Enhancement                                                                                    |
| SAR   | Software Application Requirement                                                                           |
| SDL   | Secure Development Lifecycle                                                                               |

|      |                              |
|------|------------------------------|
| SIF  | Safety Instrumented Function |
| SIS  | Safety Instrumented System   |
| SL-A | Achieved Security Level      |
| SL-C | Capability Security Level    |
| SL-T | Target Security Level        |

## 2. Introduction

Introduction This is the third 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 Paper 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 Certification Overview*                                 | 3-3           |
| *        | Part XI – System I Certification*                                       | 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 the first installment, we provided a broad overview of the entire 62443 family.<sup>2</sup> In the second installment, we examined 62443-4-1 and the secure development process – a process to which Bently Nevada is certified and which guides all secure products we develop. In this third installment, we turn our attention to the general<sup>3</sup> topic of component (product) certification. We will explain in more detail what a component is, what a component requirement is, how component requirements are used as part of certification to a particular security level, and how asset owners and others can read and interpret a manufacturer's Product Capability Assessment<sup>1</sup> (PCA) certificate issued against the criteria of 62443-4-2.

### 3. Security Levels

In part I, we introduced the concept of security levels (SLs). By way of refresher and for ease-of-reference, the table that was used to summarize the four security levels<sup>4</sup> set forth in 62443 is repeated here.

**Table 2: 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) |

SLs are fundamental to a discussion of component certifications because an asset owner will divide their automation solution (see Figure 1) into zones and each zone will have an associated **target security level** (SL-T). All of the components within that zone will then need to exhibit a security level that meets or exceeds the zone’s SL-T.

One of the ways<sup>5</sup> an asset owner meets an SL-T is by requiring component certifications. A component certification results in a **capability security level** (SL-C) designation which indicates the security level that the component is *capable* of meeting – provided it is installed, configured, and maintained correctly. The SL that it *actually* meets is known as the **achieved security level** (SL-A). The goal is always for the zone’s SL-A to meet or exceed the zone’s SL-T, and to maintain all of the components in a zone at such a level.

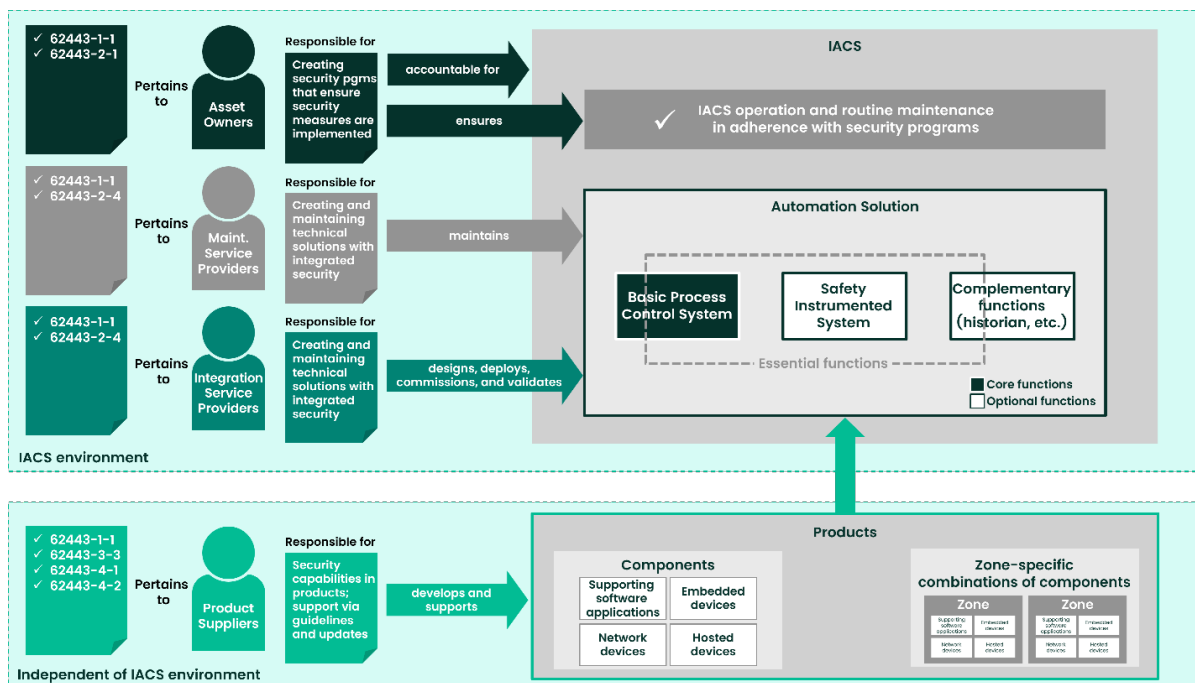
Because the SL-A of a component is dependent on factors outside the component manufacturer’s control – such as proper configuration, installation, and maintenance – a component is certified to an SL-C, not an SL-A. Whether or not it then actually *achieves* the level it is *capable* of meeting is up to the system integrators and service providers responsible for the Industrial Control and Automation System (IACS).

## 4. Example

Consider a process controller that is in an SL-T3 zone and assume that the process controller is certified for SL-C3. Assume now that the component manufacturer is advised of a new threat – such as a worm – by the provider of their real-time operating system and concludes that it could result in a vulnerability that derates the controller to SL-C1. Even though they release a patch, the asset owner may fail to install it – or perhaps their service provider installs it improperly such that only some modules are updated rather than all modules. In this case, the SL-A of the controller would become SL-A1 rather than SL-A3 – for reasons outside the manufacturer’s control.

# 5. Components

The concept of an IACS as described in 62443 was introduced in part I of this white paper series and was shown as Figure 2. For convenience, it is repeated here as Figure 1.



**Figure 1:** An IACS consists of components and zone-specific combinations of components.<sup>6</sup> Component manufacturers can certify their products to part 4-2 of the standard and certify their secure development lifecycle (SDL) processes to part 4-1 of the standard.

For our purposes in this white paper, the most important aspect of Figure 1 is that components are the software and hardware building blocks of an IACS. Part 4-2 defines them as follows:

## Component

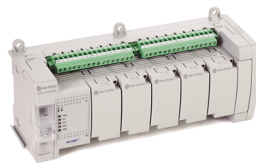
*Entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device.*

Components are further categorized according to the type of component. This is done because the requirements for cybersecurity differ according to the type of component. Indeed, as should be intuitively obvious, the security attributes incumbent upon a software application will be different than those upon an industrial monitor or controller that connects to a network, and still different than those upon an industrial firewall or panel-mount PC.

To reflect these differences, and to allow requirements to be more easily segregated according to the type of component, 62443-4-2 categorizes components into the four categories shown in Figure 2.



**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 2:** Components are delineated into one of four categories in 62443-4-2 as shown here. Although some components may reflect the attributes of multiple device types, most fall completely into a single category. Bently Nevada monitoring systems such as Bently Nevada™ Orbit 60, for example, are considered “embedded devices”.

62443-4-2 provides definitions for each of these four types of components along with examples and typical attributes.

### 1. **Embedded Device<sup>7</sup>**

*Special purpose device designed to directly monitor or control an industrial process.*

**TYPICAL ATTRIBUTES:** limited storage, limited number of exposed services, programmed through an external interface, embedded operating systems (OSs) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface

**GENERIC EXAMPLES:** PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, distributed control system (DCS) controllers

**BENTLY NEVADA EXAMPLES:** Orbit 60 monitoring system, Bently Nevada™ Orbit DCM, Bently Nevada™ 2300 monitoring system, 3701/55 ADAPT Overspeed/ESD.

### 2. **Host Device<sup>7</sup>**

*General-purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers.*

**TYPICAL ATTRIBUTES:** filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.)

**GENERIC EXAMPLE:** Panel-mount PC

**BENTLY NEVADA EXAMPLE:** External Display CPU Module (60X/CMP01)

### 3. **Network Device**<sup>7</sup>

*Device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process.*

**TYPICAL ATTRIBUTES:** *embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface*

**GENERIC EXAMPLES:** *Industrial firewall, industrial network switch, industrial wireless router*

**BENTLY NEVADA EXAMPLE:** *Ranger Pro Wireless Gateway (70M320)*

### 4. **Software Application**<sup>7</sup>

*One or more software programs and their dependencies\* that are used to interface with the process or the control system itself.*

*\* Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third-party or open-source software.*

**TYPICAL ATTRIBUTES:** *usually execute on host devices or embedded devices*

**GENERIC EXAMPLES:** *configuration software, historian*

**BENTLY NEVADA EXAMPLES:** *Orbit Studio configuration software, System I condition monitoring software, Orbit Display software*

Bently Nevada sensors are not generally considered components in the context of 62443 because they use analog signal formats for interconnection to machinery protection monitors and/or condition monitors. As such, the sensors are not a cybersecurity vulnerability. An exception would be wireless sensors as used in the Bently Nevada™ Ranger Pro system because they use wireless digital communications and are thus digitally networked to other components (gateways, condition monitoring software).

## 6. Component Requirements

Component certification under IEC 62443-4-2 consists of the ability to conform to enumerated **component requirements** (CRs). A CR is simply a particular security feature or function that the component must possess. Each CR consists of a **base requirement** (BR) and may be accompanied by one or more associated **requirement enhancements** (RE) that are related to the base requirement and necessary to achieve increasingly higher SL-Cs. Table B.1 of 62443-4-2:2019 summarizes each and every base requirement and requirement enhancement against the corresponding SL-C. A small excerpt of this table is reproduced as Figure 3.

Most CRs apply uniformly across all component types. However, there are instances where a CR is device-specific. In other words, the requirement will be different depending on whether the component is an embedded device, a host device, a network device, or a software application. These are referred to as **device-specific requirements** (DSRs).

Referring to Figure 3, notice that there is not a component requirement CR 1.6. Instead, the table jumps immediately from CR 1.5 and its RE to something labeled NDR 1.6 and its associated RE. Then, the table continues to CR 1.7 and its two REs, CR 1.8, etc.

NDR stands for Network Device Requirement, and this is because the requirement for CR 1.6 is actually a DSR. Further, CR 1.6 (wireless access management) does not pertain to embedded devices, software applications, or host devices – it only pertains to network devices. Hence, there is no EDR 1.6 (Embedded Device Requirement), HDR 1.6 (Host Device Requirement), or SAR 1.6 (Software Application Requirement) in Table B.1; there is only an NDR 1.6. The format of Table B.1 is such that DSRs are placed in sequence with their surrounding CRs.

# 7. Foundational Requirements

Notice from Figure 3 that CRs are grouped according to the particular **foundational requirement** (FR) they support. There are seven FRs set forth in part 1-1 of the standard and they comprise a set of basic characteristics within the overall framework of IACS security. CRs are numbered according to the FR they support. For example, CR 1.1 through 1.9 shown in Figure 3 all support foundational requirement #1 (Identification and authentication control) and thus use the numbering format CR 1.X. Those that support FR #2 are labeled CR 2.X, etc.

– 88 – IEC 62443-4-2:2019 © IEC 2019

**Table B.1 – Mapping of CRs and REs to FR SL levels 1-4**

| CRs and REs                                                                              | SL 1 | SL 2 | SL 3 | SL 4 |
|------------------------------------------------------------------------------------------|------|------|------|------|
| <b>FR 1 – Identification and authentication control (IAC)</b>                            |      |      |      |      |
| CR 1.1 – Human user identification and authentication                                    | ✓    | ✓    | ✓    | ✓    |
| RE (1) Unique identification and authentication:                                         |      | ✓    | ✓    | ✓    |
| RE (2) Multifactor authentication for all interfaces                                     |      |      | ✓    | ✓    |
| CR 1.2 – Software process and device identification and authentication                   |      | ✓    | ✓    | ✓    |
| RE (1) Unique identification and authentication                                          |      |      | ✓    | ✓    |
| CR 1.3 – Account management                                                              | ✓    | ✓    | ✓    | ✓    |
| CR 1.4 – Identifier management                                                           | ✓    | ✓    | ✓    | ✓    |
| CR 1.5 – Authenticator management                                                        | ✓    | ✓    | ✓    | ✓    |
| RE (1) Hardware security for authenticators                                              |      |      | ✓    | ✓    |
| NDR 1.6 – Wireless access management                                                     | ✓    | ✓    | ✓    | ✓    |
| RE (1) Unique identification and authentication                                          |      | ✓    | ✓    | ✓    |
| CR 1.7 – Strength of password-based authentication                                       | ✓    | ✓    | ✓    | ✓    |
| RE (1) Password generation and lifetime restrictions for human users                     |      |      | ✓    | ✓    |
| RE (2) Password lifetime restrictions for all users (human, software process, or device) |      |      |      |      |
| CR 1.8 – Public key infrastructure certificates                                          |      |      |      |      |
| CR 1.9 – Strength of public key-based authentication                                     |      |      |      |      |
| RE (1) Hardware security for public key-based authentication                             |      |      |      |      |

**Figure 3:** An excerpt of Table B.1 from IEC 62443-4-2:2019 showing how component requirements (CRs) and requirement enhancements (REs) correspond to a particular security level (SL).<sup>8</sup> Notice that some CRs have no corresponding REs while others have one or more.

## 8. Number of Component Requirements

Table 3 shows the total number of CRs and REs for a given security level and component type. As would be expected, the total number of requirements (base and enhancements) increases with each successive SL.

The group labeled “CCSCs” will be discussed in the next section of this white paper. For now, suffice to say that the number of requirements incumbent upon a component is a function of two variables:

- The security level (1, 2, 3, or 4)
- The type of component (embedded, host, network, or software)

**Table 3: Requirements as a function of security level and component type**

|                                                     | SL 1 |     | SL 2 |     | SL 3 |     | SL 4 |     |
|-----------------------------------------------------|------|-----|------|-----|------|-----|------|-----|
|                                                     | BRs  | REs | BRs  | REs | BRs  | REs | BRs  | REs |
| <b>CCSCs</b>                                        |      |     |      |     |      |     |      |     |
| Common Component Security Constraints               | 4    | 0   | 4    | 0   | 4    | 0   | 4    | 0   |
| <b>FOUNDATIONAL REQUIREMENTS</b>                    |      |     |      |     |      |     |      |     |
| 1 – Identification and Authentication Control (IAC) | 10   | 0   | 14   | 1   | 14   | 7   | 14   | 8   |
| 2 – Use Control (UC)                                | 11   | 0   | 12   | 3   | 13   | 5   | 13   | 8   |
| 3 – System Integrity (SI)                           | 12   | 0   | 14   | 2   | 14   | 3   | 14   | 5   |
| 4 – Data Confidentiality (DC)                       | 2    | 0   | 3    | 0   | 3    | 2   | 3    | 2   |
| 5 – Restricted Data Flow (RDF)                      | 4    | 0   | 4    | 0   | 4    | 0   | 4    | 0   |
| 6 – Timely Response to Events (TRE)                 | 1    | 0   | 2    | 0   | 2    | 1   | 2    | 1   |
| 7 – Resource Availability (RA)                      | 7    | 0   | 8    | 2   | 8    | 3   | 8    | 3   |
| <b>DEVICE-SPECIFIC REQUIREMENTS</b>                 |      |     |      |     |      |     |      |     |
| Embedded Device Requirements (EDRs)                 | 4    | 0   | 8    | 3   | 8    | 5   | 8    | 5   |
| Host Device Requirements (HDRs)                     | 4    | 0   | 8    | 4   | 8    | 6   | 8    | 6   |
| Network Device Requirements (NDRs)                  | 8    | 0   | 12   | 8   | 12   | 10  | 12   | 10  |
| Software Application Requirements                   | 2    | 0   | 2    | 1   | 2    | 1   | 2    | 1   |
| <b>TOTAL</b>                                        |      |     |      |     |      |     |      |     |
| FOR EMBEDDED DEVICES                                | 55   |     | 80   |     | 96   |     | 102  |     |
| FOR HOST DEVICES                                    | 55   |     | 81   |     | 97   |     | 103  |     |
| FOR NETWORK DEVICES                                 | 59   |     | 86   |     | 105  |     | 111  |     |
| FOR SOFTWARE APPLICATIONS                           | 53   |     | 72   |     | 86   |     | 92   |     |

## 9. Common Component Security Constraints

The individual CRs and REs enumerated within 62443-4-2 are intended to be implemented and understood within four basic constraints. These are known as common component security constraints (CCSCs) and are listed below.

### CCSC 1 – Support of Essential Functions

This constraint is that security measures are not to adversely affect essential functions.<sup>9</sup> Essential functions were discussed in part I of this series of white papers. 62443 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.*



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. In some industries, additional functions such as history may be considered essential.

### CCSC 2 – Compensating Countermeasures

The spirit and intent of 62443-4-2 is that the component itself will provide the necessary security measures. However, there may be some circumstances in which a manufacturer needs to rely on external apparatus or measures to meet the particular component requirement or requirement enhancement. These are known as **compensating countermeasures** (CCs) and when employed, they must be clearly spelled out by the manufacturer and explained in the documentation for the component that the CC is necessary for conformity – and not merely recommended.

### CCSC 3 – Least Privilege

Least privilege is the concept of giving an individual only the minimum security privileges necessary for them to perform their job duties – or giving other connected IACS devices only the minimum security privileges necessary for them to carry out their assigned functions. For example, some users might have no privileges to view data in an event list, others might be able to view but not edit such data, and still others might be able to both view and edit data. Under the principle of Least Privilege, the component will be capable of distinguishing between these different types of users and will not give edit privileges to those who do not need them.

### CCSC 4 – Secure Development Process

62443-4-2 assumes that the component was developed and is being sustained by way of a Secure Development Lifecycle (SDL) process as laid out in 62443-4-1. In order for a manufacturer to certify a component or system to part 4-2, they must first demonstrate that their SDL processes are certified to part 4-1 of the standard. It is thus not possible to achieve 4-2 certification without first obtaining 4-1 certification.

## 10. Certification (Conformity Assessment)

When a component manufacturer decides to certify their component, they undergo a **product capability assessment** (PCA) by a **certification body** (CB). A CB is itself authorized to certify components by an **accreditation body** (AB). There are thus more than a dozen CBs globally that are able to perform conformity assessments against 62443-4-2, but all are accredited by an AB such as ANSI, IECEE, or others. This white paper and the scoring rubric described herein assumes the IECEE conformity assessment scheme. Other schemes are available such as ISASecure but are not discussed herein.

One of the primary differences in component certification under the IECEE conformity scheme to 62443-4-2 is that the scope of certification is more granular than just the security level being sought. In other words, a component manufacturer can selectively remove certain component requirements from the conformity assessment and obtain a certification based on only some of the CRs rather than all of them. This is typically done because the manufacturer has not yet introduced functionality specifically designed to meet a particular CR or group of CRs.

# 11. Scoring Rubric

Referring to the certificate in Figure 4, notice that for each of the 7 foundational requirements (Identification and Authentication Control, Use Control, System Integrity, etc.) there is a 3-number score of the format (RA,NAR,TR).<sup>10</sup> These numbers designate the following information:

RA = number of **requirements assessed** (and passed)

NAR = number of **not applicable requirements**

TR = number of **total requirements** possible

**The RA score** is self-explanatory.

**The NAR score** requires more elaboration as it is important at this juncture to distinguish between “not applicable” and “not in scope”. Not applicable means exactly what it says: that the component requirement is simply not applicable. As such, it cannot be assessed or tested. For example, CR2.4 deals with mobile code. If a component does not use mobile code, this requirement is not applicable. From a cybersecurity standpoint, a requirement that is not applicable is secure because it does not represent a vulnerability that can be exploited. In contrast, the concept of “not in scope” means that it was excluded from the assessment scope. The user thus does not know whether the component is secure or not with respect to this requirement; at the request of the manufacturer, it was removed from the scope and thus not assessed. This is generally done, as noted above, if the manufacturer has not introduced that particular functionality yet – as is often the case when products are released in phases with gradually increasing capabilities. However, it can also be done because the manufacturer has the particular functionality present but it cannot fully satisfy the requirements at the desired security capability level. The number of “not in scope” requirements is not directly conveyed by this 3-number score and must instead be inferred, as discussed next.

**The TR score** represents simply the total number of requirements and requirement enhancements that are possible.<sup>11</sup> The TR number is always the same for a given category. For example, every 4-2 PCA certificate will exhibit TR=21 for FR2 and TR=5 for FR4. In like manner, every 4-2 PCA certificate will exhibit TR=3 for Software Application Requirements, TR=13 for Embedded Device Requirements, etc. Thus, when comparing 4-2 certificates, the TR score will always be the same in each category because it is a function of the number of requirements within 62443-4-2 itself and not something that fluctuates from one manufacturer’s component to the next. Table 4 summarizes this information.

**Table 4: Total Requirements (TR) appearing on 62443-4-2 PCA certificates**

| Category                                       | TR |
|------------------------------------------------|----|
| Common Component Security Constraints          | 4  |
| FR1: Identification and Authentication Control | 22 |
| FR2: Use Control                               | 21 |
| FR3: System Integrity                          | 19 |
| FR4: Data Confidentiality                      | 5  |
| FR5: Restricted Data Flow                      | 4  |
| FR6: Timely Response to Events                 | 3  |

| Category                                 | TR |
|------------------------------------------|----|
| FR7: Resource Availability               | 11 |
| Device-Specific Requirements             |    |
| Software Application Requirements (SARs) | 3  |
| Embedded Device Requirements             | 13 |
| Host Device Requirements                 | 14 |
| Network Device Requirements              | 22 |

Ideally, a certificate will reflect  $RA+NAR=TR$  when SL-C4 is being sought. This signifies that each and every requirement and enhancement was either assessed or deemed to be “not applicable” and thus every possible requirement was dispositioned without removing any from scope.

When  $RA+NAR < TR$ , this means that some requirements were removed from the assessment scope. This occurs either because a level lower than SL-C4 is being pursued, or because entire CR categories have been omitted. It then becomes necessary to look at the full test report to determine whether a requirement was omitted because it exceeded the SL-C level sought, or because the manufacturer could not meet the requirement at the SL-C level sought. It is thus generally necessary to look at the full test report in order to ascertain whether deficiencies in a score reflect simply the requirements of a higher security level, or because a manufacturer removed otherwise applicable requirements from scope. Consult Table 3 for the specific totals corresponding to each FR and each SL-C level. If even greater visibility to the specific granularity of requirements and requirement enhancements for each individual CR and DSR is required, consult a copy of 62443-4-2:2019 itself.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <b>VALID</b> FR_Cyber10112                                                                                                                                                                                                                                                                                                                                                                                                                     | Cyber Security Certificate<br>2023-11-02 |
| <b>TYPE</b><br>Product Capability Assessment                                                                                                                                                                                                                                                                                                                                                                                                   |                                          |
| <b>CERTIFICATE COVERAGE (INCLUDING VERSION)</b><br>SUN2000<br>SUN2000-***KTL-H*<br><br>Version SUN2000HA V500R023                                                                                                                                                                                                                                                                                                                              |                                          |
| <b>STANDARD(S) USED</b><br><b>IEC 62443-4-2:2019</b>                                                                                                                                                                                                                                                                                                                                                                                           |                                          |
| <b>REQUIREMENTS ASSESSED</b><br>Identification and authentication control (11, 4, 22)<br>Use control (10, 4, 21)<br>System integrity (15, 1, 19)<br>Data confidentiality (3, 0, 5)<br>Restricted data flow (0, 4, 4)<br>Timely response to events (1, 1, 3)<br>Resource availability (7, 2, 11)<br>Software application (0, 0, 3)<br>Embedded device (9, 2, 13)<br>Host device (0, 0, 14)<br>Network device (0, 0, 22)<br><br>Security level 2 |                                          |
| <b>DATE OF ISSUE</b><br>2023-11-02                                                                                                                                                                                                                                                                                                                                                                                                             |                                          |
| <b>CERTIFICATE ISSUED BY</b><br><br><b>LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES – LCIE</b><br>33 Avenue du Général Leclerc<br>Fontenay-Aux-Roses<br>92260<br>France                                                                                                                                                                                                                                                                      |                                          |
|                                                                                                                                                                                                                                                                                                                                                           |                                          |

**Figure 4:** A typical PCA certificate for a component conforming to 62443-4-2. This particular component is an embedded device as can deduced by noting that none of the device-specific requirements for network devices, software applications, or host devices were assessed and thus RA=0. The only device type where RA≠0 is an embedded device where a score of (9,2,13) was achieved.

## 12. Security Vectors

The certification approach within 4-2 is consistent with the concept inherent to 62443 of a **security vector** where a given foundational requirement category is composed of numerous requirements and requirement enhancements. In other words, conformity is not measured by a single number or attribute – it is measured by multiple attributes. For example, referring to Table 4, Foundational Requirement FR 3 (System Integrity) consists of 22 total requirements if one were to achieve the highest possible security level. There are thus 22 “increments” to characterize the degree of security along the System Integrity (FR 3) “vector”. Indeed, if we think of each FR as its own vector, we have 7 vectors along which OT cybersecurity can be assessed for a component under 62443-4-2. The length of each vector is a measure of security ranging from none to partial to full. Also, to reflect the nuances of differences in vector length among different device types, device-specific requirements are used. As would be expected, the vector lengths vary in each category according to whether SL-C1, SL-C2, SL-C3, or SL-C4 is achieved. The longer the vector in each category, the better the potential security “posture” and the higher the security capability level.

# 13. Certificate Format and Interpretation

The information conveyed up to this point allows us to examine an actual 4-2 PCA certificate (Figure 4) and make sense of its score. However, in addition to the scoring, there are three other noteworthy items that merit additional comment:

1. **Security Capability versus Security Achieved**

Notice in Figure 4 that the certificate states it is a Product Capability Assessment (PCA) and thus a measure of the product's security *capability* as opposed to its security *achieved*. As was discussed previously, the achieved security level can differ from the capability security level because achieved security is installation-dependent and can change over time as new threats are introduced and new vulnerabilities thus arise.

2. **Product Version**

Notice in Figure 4 that the section titled "Certificate Coverage" includes reference to the version number. This is important because as a product goes through successive releases, each new release should be assessed. Thus, just because version 3.1 of a product resulted in a particular certificate, it does not mean that version 4.2 would result in an identical certificate.

Manufacturers will thus periodically refresh their certificates to reflect the most recent builds of their products and will maintain their certificates for previous builds to allow asset owners and service providers to ascertain security levels for the particular release they are using.

3. **Edition**

Notice in Figure 4 that the certificate explicitly calls out the specific edition of 62443-4-2 used as the basis of the certification. In this case, the 2019 edition. As newer editions are released, they would be reflected here. Since part 4-2 is only in its first edition, the product has been certified to the most recent edition<sup>12</sup>.

## 14. Not Applicable Requirements vs Out of Scope Requirements

It is important to note that requirements deemed “not applicable” require the consensus of the manufacturer and the CB. An example might be a software application that does not use mobile code (CR 2.4). In this case, the manufacturer would state that their software does not use mobile code and the CB would verify that this was indeed the case. CR 2.4 would then be treated as “not applicable” for purposes of the conformity audit. Any requirements deemed “not applicable” are essentially equivalent to a requirement that has been satisfied in terms of cybersecurity. In other words, if a particular attribute is not present in a component, it cannot be exploited and it is thus secure from vulnerabilities related to the attribute.

The same is not true, however, when a manufacturer removes a requirement from the scope of the conformity assessment. The device may or may not be secure with respect to the particular requirement – it simply was not assessed and this will normally trigger more in-depth discussions between the asset owner (or system integrator) and the component manufacturer to ascertain the level of partial conformity that might exist. Bear in mind that when a requirement is not assessed, it is either one of two things: the requirement is not incumbent on the particular security level being pursued OR the requirement IS incumbent for the security level, but the manufacturer has excluded it from the test scope because they do not believe their component will conform.

## 15. Summary

In part III of this series of white papers, we have examined the basic elements of a certificate issued as part of a Product Capability Assessment to the requirements enumerated in IEC 62443-4-2. We have shown that this approach to certification is different from many other types of certifications where the criteria is more discrete and consists of an all-or-nothing “pass / fail” approach; for example, hazardous area approvals. We showed that the reason for such a granular certification scheme is rooted in an understanding of so-called “security vectors” as discussed in part 3-3 of the 62443 family of standards. This vector-based approach treats security as a sliding scale in multiple dimensions, where each dimension is one of the seven Foundational Requirements (FRs) set forth in part 1-1 of the standard.

Using the information presented here in part II, users of not just Bently Nevada products but other products will be better able to read and interpret a 4-2 PCA certificate. Part IV of this series of white papers provides an in-depth review of the PCA certificate issued for v22.1 of the Orbit 60 platform. Other parts of this series of white papers will likewise provide in-depth reviews of the PCA certificates for other Bently Nevada products as they are obtained. Refer to Table 1 for the full list of installments envisioned for this series of white papers.

## 16. Endnotes

1. PCA is also used to denote Process Capability Assessment (not just Product Capability Assessment). When used in conjunction with 62443-4-1, it is a process capability assessment. When used in conjunction with 62443-4-2, it is a product capability assessment
2. If you have not yet read parts I and II, you are encouraged to do so as they make part III easier to understand by providing proper context and background.
3. Parts IV and V examine the Orbit 60 platform in detail with respect to cybersecurity certification. Parts VII and beyond will examine other Bently Nevada products.
4. 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.
5. Meeting the SL-T of a zone involves more than just using components certified to a particular SL-C. It also involves verifying their security functionality once installed and in establishing conduits within and between zones that reflect the necessary security levels.
6. 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](http://www.iec.ch).
7. The definitions, typical attributes, and many of the generic examples for the four component types are taken directly from clause 3 of IEC 62443-4-2: 2019 and are used by permission. Copyright © 2019 IEC Geneva, Switzerland. [www.iec.ch](http://www.iec.ch).
8. Table excerpt reproduced by permission. Copyright © 2019 IEC Geneva, Switzerland. [www.iec.ch](http://www.iec.ch).
9. Unless supported by a risk assessment. There may be instances in which sacrificing essential functionality to maintain security is preferable, given the nature and severity of a particular cybersecurity breach.
10. Certificate formats were revised in 2023 to include Requirements Assessed (RA), Total Requirements (TR), and Not Applicable Requirements (NAR). Prior to this, only RA and TR were shown. If a requirement is “not applicable” it does not present a security vulnerability and is thus practically equivalent to a requirement that was assessed and met. The so-called “security vector length” can thus be thought of as the requirements assessed plus the not applicable requirements. Ideally, this sum will be equal to the total requirements. If they are not equal, this signifies that some requirements were removed from the assessment scope or are only used for SL-C levels above that in the certificate.
11. The totals in Table 3 reflect the TR number shown on 4-2 certificates. Reconciliation of the totals on a 4-2 PCA certificate to the 4-2 standard itself is accomplished as follows:
  - Sum the number of CRs and REs (assume SL-C4) in clauses 5 through 11 of the standard.
  - When encountering any paragraph that states “there are no component-level requirements” count this as 1 (not zero).
  - When encountering any paragraph that states the requirements are device-specific, count this as 1 (not zero).
  - For the total number of **device-specific requirements** (including requirement

enhancements), simply sum the number of DSRs and corresponding REs (assume SL-C4).

12. As of this writing, the only part of the standard currently in Edition 2 is part 2-4; 62443-2-4:2015 was Edition 1 and has been superseded by Edition 2 (62443-2-4:2023).

Copyright 2025 Baker Hughes Company. All rights reserved.

Bently Nevada, a Baker Hughes Company  
1631 Bently Parkway South, Minden, Nevada USA 89423  
<https://bntechsupport.com>