



Cybersecurity and IEC 62443

Part II–Process Certification

White Paper

Contents

- 1. List of Acronyms and Abbreviations 3
- 2. Introduction 4
- 3. Security Practices 5
- 4. Maturity Levels 6
- 5. Process Capability Assessment 7
- 6. Interpreting a 4-1 Process Conformity Assessment (PCA) Certificate under the IEC EE Scheme 8
- 7. An Additional Word on Maturity Levels 10
- 8. Bently Nevada’s 4-1 PCA Certificate 11
- 9. Summary 12
- 10. Endnotes 13

1. List of Acronyms and Abbreviations

CR	Component Requirement
DM	Security-Related Issue ¹
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ML	Maturity Level
PCA	Process ² Capability Assessment
SD	Security Design
SDL	Secure Development Lifecycle
SG	Security Guidelines
SI	Secure Implementation
SM	Security Management
SR	System Requirement
SUM	Security Update Management
SVV	Security Verification and Validation

2. Introduction

This is the second 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 1 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 the first installment, we provided a broad overview of the entire 62443 family³. In this second installment, we examine 62443-4-1 and the secure development process – a process to which Bently Nevada is certified and which guides all secure products we develop. We will explain in more detail what this process entails and how a company’s maturity level is assessed. This will allow asset owners and others to read and interpret a manufacturer’s Process Capability Assessment² (PCA) certificate issued against the criteria of 62443-4-1 using the IEC EE certification scheme⁴.

3. Security Practices

62443-4-1 lays out eight (8) security practices that should be present within a company's secure development lifecycle (SDL). Table 2 summarizes the eight practices along with the number of requirements characterizing each practice.

Table 2: SDL Practices and Number of Requirements per IEC 62443-4-1

Topic	4-1 section	Requirements
Practice 1: Security Management (SM)	§5	13 (SM1-SM13)
Practice 2: Specification of Security Requirements (SR)	§6	5 (SR1-SR5)
Practice 3: Secure by Design (SD)	§7	4 (SD1-SD4)
Practice 4: Secure Implementation (SI)	§8	2 (SI1-SI2)
Practice 5: Security Verification and Validation (SVV)	§9	5 (SVV1-SVV5)
Practice 6: Management of Security-Related Issues (DM) ¹	§10	6 (DM1-DM6)
Practice 7: Security Update Management (SUM)	§11	5 (SUM1-SUM5)
Practice 8: Security Guidelines (SG)	§12	7 (SG1-SG7)
TOTAL		47

For example, there are 7 top-level requirements for Security Guidelines, SG1 through SG7. While there are a total of 47 top-level requirements, this actually consists of hundreds of sub-requirements⁵.

4. Maturity Levels

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 3.

Table 3: SDL Process Maturity Levels (MLs) used in IEC 62443-4-1

Maturity Level	Description
1 (Initial)	No written, controlled documentation exists to characterize processes; processes are instead ad-hoc and as a result, may lead to non-repeatable, inconsistent results with regard to security.
2 (Managed)	Written, controlled documentation exists to characterize processes and is available for an auditor to assess.
3 (Practiced)	Written, controlled documentation exists to characterize processes and the supplier is able to demonstrate via documentation and other evidence that the processes are actually being followed.
4 (Improving)	The supplier is not only following written processes, and can demonstrate this with evidence, but is actively measuring the effectiveness of those processes and continuously improving those processes

5. Process Capability Assessment

When a supplier has their SDL process assessed for conformity with the requirements of IEC 62443-4-1, they are essentially being assessed for their maturity level in each of the 8 practices (47 sub-practices) shown in Table 2. However, a supplier may selectively remove one or more of these 47 requirements (sub-practices) from the scope of their conformity audit. This means that a supplier's certificate issued under the IECCE certification scheme⁴ must be carefully inspected to understand whether they were assessed for all 47 possible requirements, or a lesser number. Those with a lesser number of assessed requirements obviously have a weaker certification than those assessed for all 47.

It is important at this juncture to distinguish removing a requirement from assessment scope versus that of a requirement that is *not applicable*. These terms are not used interchangeably. Although rare in the scheme of 4-1, there may be instances in which a requirement is simply not applicable to the manufacturer's SDL processes. For example, SM-8 deals with controls for private keys. If a manufacturer uses a security technology different than private keys, SM-8 would be non-applicable. From a cybersecurity standpoint, a requirement that is "not applicable" is generally deemed to be just as robust as a requirement that is applicable and to which the process conforms – because neither situation presents a security vulnerability. Thus, extending our example of Security Management (SM) a bit further, if a supplier achieved ML2 for SM-1 through SM-7 along with SM-9 through SM-13, but SM-8 was deemed "not applicable", one could argue that their processes are just as robust at preventing vulnerabilities as a supplier for whom SM-1 through SM-13 were all applicable and could demonstrate ML2. For this reason, "not applicable" is generally viewed just as favorably from a security standpoint as "assessed and found to conform".

The same is not true, however, for "out of scope". In the 62443 certification scheme, a supplier is allowed to unilaterally remove requirements from scope. For example, if a supplier decided that their product would be released in phases, and that anything pertaining to security event log files in 62443-4-2 would not be addressed until a phase 3 release, they might remove all the component requirements (CRs) dealing with security event log files from their 4-2 certification scope until such time as they released these capabilities in phase 3. In like manner, if a supplier felt that there were parts of their SDL process that were either absent, or too immature, they could elect to remove them from the scope of assessment. In this manner, 62443 certifications can be somewhat "a la carte" in nature and for customers and other interested parties to understand what did and did not fall within the scope of the conformity audit, they must examine the certificate and – in some cases – the full test report.

6. Interpreting a 4-1 Process Conformity Assessment (PCA) Certificate under the IECCE Scheme

To aid customers and others in interpreting a certificate issued against the requirements of 4-1, a scoring system consisting of three numbers (A, B, C) is used. This score is provided adjacent to each of the eight practices so the reader can ascertain how the supplier scored. Refer to Figure 1 for an example.

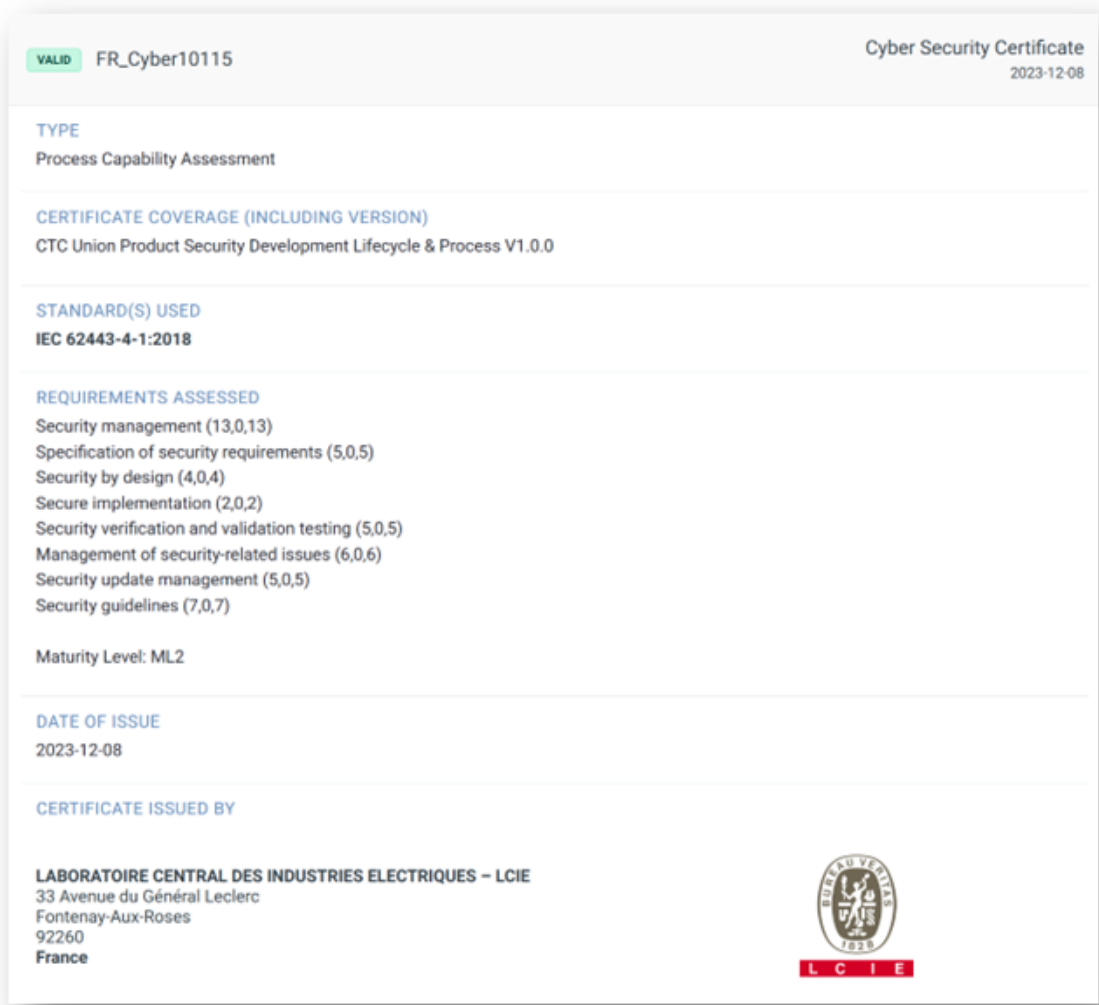


Figure 1: A typical cybersecurity certificate for an SDL process conforming to 62443-4-1 under the IECCE scheme⁴. Notice that each of the 8 practices are scored in the form of (A,B,C). For this supplier, every one of the 47 requirements was assessed with no items being “not applicable” as evidence by B=0 for all practices. Because A=C for all practices, this conveys that no requirements were removed from scope. Finally, the certificate itself clarifies that this supplier was assessed at Maturity Level ML2.

The rubric used for this scoring system is as follows:

A = number of requirements assessed and passed

B = number of requirements deemed “not applicable”

C = total possible number of requirements

Referring back to Table 2, it can be seen that $C=5$ for Practice 2 since there are five total requirements (SR1 – SR5); for Practice 8, $C=7$ since there are 7 total requirements (SG1-SG7).

Ideally, a certificate will reflect $A+B=C$. This means no requirements were removed from the assessment scope. When $A+B < C$, this implies some requirements were removed from the assessment scope. For example, if a supplier scored (9,0,13) for Practice 1 (Security Management), this would mean that 9 requirements were assessed and conformed, 0 requirements were deemed not applicable, and 13 total requirements (SM1-SM13) exist. Thus, 4 requirements were removed from the assessment scope and this supplier’s score for Practice 1 would not be as strong as one with a rating of (13,0,13). In like manner, if a supplier had a score of (12,1,13) this conveys that 12 requirements were assessed and found to conform, one (1) requirement was “not applicable”, and 13 total requirements exist. As argued previously, this supplier’s process could be deemed just as robust as the one for whom a score of (13,0,13) had been achieved.

As was mentioned earlier, a supplier can elect to remove requirements from the scope of the assessment. Unfortunately, there is no number in the scoring rubric that explicitly conveys whether requirements were removed from scope. This can only be ascertained by examining whether $A+B=C$ as noted earlier. When $A+B < C$, this means that some requirements were removed from scope by the supplier, and the number removed from scope is $C-(A+B)$. Thus, a score of (5,1,7) for Practice 8 (Security Guidelines SG1-SG7) tells us that five (5) requirements were assessed and found conforming, one was deemed “not applicable”, and one (1) must have been removed from scope by the supplier since there are seven (7) total possible requirements. If we wanted to know which specific requirement was “not applicable” and which one was removed from scope, we would have to examine the full test report – or ask the supplier.

As might be obvious, due to maturity levels, two identical scores for a practice or even an entire certificate does not necessarily mean that the two suppliers have identically robust processes. Obviously, a supplier that obtains a 4-1 PCA certificate to ML1 would not be deemed the same as one operating their processes at an ML4 level of maturity. The one operating at ML1 would not even need to show that written documentation existed while the one operating at ML4 would have to show that for each and every process requirement, not only would written, controlled processes need to exist, and that not only do they have documentation proving that they are following each and every process, but that they are continually measuring and improving each and every process. ML4 is thus a substantial achievement.

All of this should suggest that there is a significant jump in moving from one ML to the next. Level 1 suppliers do not even have the burden of showing written processes exist. Level 2 suppliers have written processes, but they do not need to demonstrate that each and every one of those processes is being followed by way of documentation. Level 3 suppliers must show their processes are being followed – not just a scattered few processes – but *all* processes. And, Level 4 suppliers must take things to the next level by measuring every process and demonstrating that they are using these measurements to go back and continually refine/improve those processes.

Customers must ultimately decide whether a certificate for ML2 that covers all 47 requirements (such as the one in Figure 1) is, for example, preferable to a certificate that might be ML3 but covers only 35 of the 47 requirements. In this manner, deciding the so-called “strength” of a certificate becomes subjective – even though the scoring rubric itself is completely objective.

7. An Additional Word on Maturity Levels

When a supplier is operating at a particular Maturity Level, this means that all of their processes (not just a select few) are operating at that level. A supplier with 6 practices operating at ML1, 40 operating at ML2, and 2 operating at ML3 might elect to omit 6 of the practices from its conformity assessment so that it could achieve ML2. If it left those processes in, the entire certificate would be pulled down to the “lowest common denominator” of ML1. In like fashion, just because a few of its processes are operating at ML3, this does not automatically elevate their entire SDL process to ML3 performance. Most suppliers offering cybersecure products in conformity with 62443 requirements will represent a mix of Maturity Levels but will ideally be operating at a level of at least ML2 and aiming to improve over time. Ultimately, a supplier’s SDL process maturity is one factor in selecting a supplier but not the only factor. Indeed, a flawless SDL process does not automatically translate to components or systems that are themselves conforming to IEC 62443-4-2 or 3-3, respectively.

8. Bently Nevada's 4-1 PCA Certificate

Now that the details of interpreting a PCA certificate to IEC 62443-4-1 have been addressed, Figure 2 showing Bently Nevada's certificate can be better understood.

Bentley Nevada's SDL process was assessed across 46 of the 47 possible requirements at a Maturity Level of ML2 and found to conform. The only requirement omitted from the assessment scope was SM-2 and while Bentley Nevada conformed to the so-called "spirit" of the law, it did not conform fully to the "letter" of the law and was operating at only ML1. SM-2 was removed from the assessment scope for that reason.



	<table border="1"> <tr> <td data-bbox="573 480 992 554"></td> <td data-bbox="992 480 1190 554"> Ref. Certif. No. US/10272/ITS </td> </tr> </table>		Ref. Certif. No. US/10272/ITS
	Ref. Certif. No. US/10272/ITS		
IEC SYSTEM OF CONFORMITY ASSESSMENT SCHEMES FOR ELECTROTECHNICAL EQUIPMENT AND COMPONENTS (IECEE)			
Certificate of Conformity – Industrial Cyber Security Capability			
Type Name and address of the applicant Certificate Coverage (including Version) Standards Requirements Assessed <i>The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)</i> Additional information (if necessary may also be reported on page 2) As shown in the Test Report Ref. No. which forms part of this Certificate	Process Capability Assessment Bentley Nevada 1631 Bentley Pkwy. Minden, NV, 89423 United States of America Bentley Nevada Secure Development Lifecycle (SDL) Process, Version: 1 IEC 62443-4-1:2018 Security Management (12/0/13); Security Requirements (5/0/5); Secure by Design (4/0/4); Secure Implementation (2/0/2); Security Verification and Validation Testing (5/0/5); Management of Security-Related Issues (8/0/6); Security Update Qualification (5/0/5); Security Guidelines (7/0/7) <input type="checkbox"/> Additional information on page 2 2081-059-D002		
<p>This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.</p>			
Intertek Testing Services NA, Inc. 545 E. Algonquin Road, Arlington Heights IL 60005 United States of America Issue date: 2024-02-22	 Signature: Matt Snyder <i>Matthew Snyder</i>		

Figure 2: Bently Nevada's Process Capability Assessment (PCA) certificate to IEC 62443-4-1:2018.

9. Summary

Because the supply of cybersecure products must consider not only the development, but also the full lifecycle during which the product operates and is eventually removed from service in a secure fashion, processes must exist that cover this full lifecycle and ensure the following:

- The product's security requirements are properly specified (SR1-SR5)
- The design reflects the security requirements (SD1-SD4)
- The design is properly implemented (SI1-SI2)
- The implementation is properly verified and validated (SVV1-SVV5)
- Security-related issues arising after commissioning are properly addressed (DM1-DM6)
- Security updates (i.e., patches) for released products are properly deployed and managed (SUM1-SUM5)
- Security Guidelines in the form of clear documentation for installing, commissioning, hardening, operating, maintaining, and de-commissioning exist (SG1-SG7)
- A management system for the entire SDL is in place to ensure properly trained and competent personnel are used and that the entire SDL operates effectively, repeatably, and consistently (SM1-SM13)

Because cybersecure products are of such substantial importance to our customers – given the industries in which they operate and the grave consequences of cyberattacks therein – conformity to the requirements of IEC 62443 are very important as well. This helps assure our customers that our products are developed in accordance with internationally recognized standards embodying best practices in both the processes used to develop those products, and the functionality those products embody.

In part II of this series of white papers, we have examined the basic elements of a certificate issued as part of a Process Capability Assessment to the requirements enumerated in IEC 62443-4-1. Finally, we have provided Bently Nevada's PCA certificate for IEC 62443-4-1:2018 showing that we operate at a Maturity Level of ML2 and our assessment covered 46 of the 47 possible SDL practices.

10. Endnotes

1. DM nomenclature to describe the management of security-related issues can be thought of stemming from “Defect Management” although not all defects are security-related. Admittedly, however, SRI might have been a better choice.
2. PCA is also used to denote Product Capability Assessment (not just Process 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
3. If you have not yet read part I, you are encouraged to do so as it will make part II easier to understand by providing proper context and background.
4. There are currently three different certification schemes that can be used for 62443 conformity assessment. Bently Nevada is certified using the IECCE scheme. Please refer to Part I in this series of white papers for more details on the three different schemes.
5. Most requirements consist of numerous sub-requirements, meaning there are hundreds of requirements for full process conformity. SG3, for example, consists of 11 sub-requirements – all of which must be fulfilled for a supplier’s process to conform with SG3.



Bently Nevada 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)