ExMC/1400/R
July 2018

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC) SYSTEM FOR CERTIFICATION TO STANDARDS RELATING TO EQUIPMENT FOR USE IN EXPLOSIVE ATMOSPHERES (IECEx SYSTEM)

Ex Management Committee, ExMC

TITLE: IECEx Cybersecurity Workshop, June 2018, Weimar – Report as copy of workshop presentation

INTRODUCTION

The following slide set is a copy of that used during the IECEx Cybersecurity Workshop conducted by the IECEx Secretariat during the 2018 IECEx Operational Meetings in Weimar, Germany.

This document is issued for the information of members - questions and suggestions on the content are welcomed by the IECEx Secretariat and should be directed to *mark.amos@iecex.com* .

Address:	**Contact Details:**
IECEx Secretariat Level 33, Australia Square 264 George Street Sydney NSW 2000 Australia	Tel: +61 2 4628 4690 Fax: +61 2 4627 5285 e-mail: info@iecex.com http://www.iecex.com

CONFORMITY ASSESSMENT ACTIVITIES REGARDING CYBER SECURITY

Mark Amos
IECEx Secretariat
June 2018

OBJECTIVES of this Workshop

- PART 1 = to inform
- PART 2 = to develop and list Actions needed for IECEx Conformity Assessment outcomes with respect to cybersecurity

PART 1

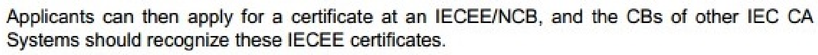
INFORMATION

RECENT DEVELOPMENTS .....

September 2017

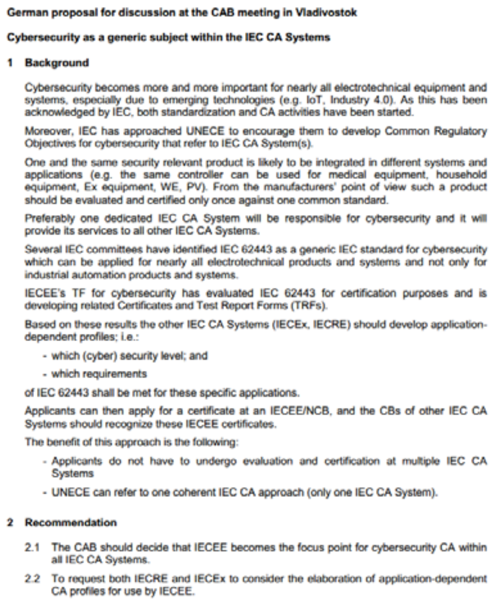
- IECEE CMC-PSC WG3 has finalized the format and content of Stakeholder Workshops on IEC 62443 and use of these for certification under the IECEE System – a number of the relevant slides from the workshop will be included (as detailed background information) in a Green Paper version of this presentation after this ExMC Meeting

- Members of IECEE CMC-PSC WG3 were advised Tuesday of last week that the German IEC National Committee will submitting a proposal to the October 2017 meeting of the IEC CAB that, regarding cybersecurity certification, includes a recommendation that ....



Applicants can then apply for a certificate at an IECEE/NCB, and the CBs of other IEC CA Systems should recognize these IECEE certificates.

RECENT DEVELOPMENTS .....



German proposal for discussion at the CAB meeting in Vladivostok

Cybersecurity as a generic subject within the IEC CA Systems

1 Background

Cybersecurity becomes more and more important for nearly all electrotechnical equipment and systems, especially due to emerging technologies (e.g. IoT, Industry 4.0). As this has been acknowledged by IEC, both standardization and CA activities have been started.

Moreover, IEC has approached UNECE to encourage them to develop Common Regulatory Objectives for cybersecurity that refer to IEC CA System(s).

One and the same security relevant product is likely to be integrated in different systems and applications (e.g. the same controller can be used for medical equipment, household equipment, Ex equipment, WE, PV). From the manufacturers' point of view such a product should be evaluated and certified only once against one common standard.

Preferably one dedicated IEC CA System will be responsible for cybersecurity and it will provide its services to all other IEC CA Systems.

Several IEC committees have identified IEC 62443 as a generic IEC standard for cybersecurity which can be applied for nearly all electrotechnical products and systems and not only for industrial automation products and systems.

IECEE's TF for cybersecurity has evaluated IEC 62443 for certification purposes and is developing related Certificates and Test Report Forms (TRFs).

Based on these results the other IEC CA Systems (IECEx, IECRE) should develop application-dependent profiles; i.e.:

- which (cyber) security level; and
- which requirements

of IEC 62443 shall be met for these specific applications.

Applicants can then apply for a certificate at an IECEE/NCB, and the CBs of other IEC CA Systems should recognize these IECEE certificates.

The benefit of this approach is the following:

- Applicants do not have to undergo evaluation and certification at multiple IEC CA Systems
- UNECE can refer to one coherent IEC CA approach (only one IEC CA System).

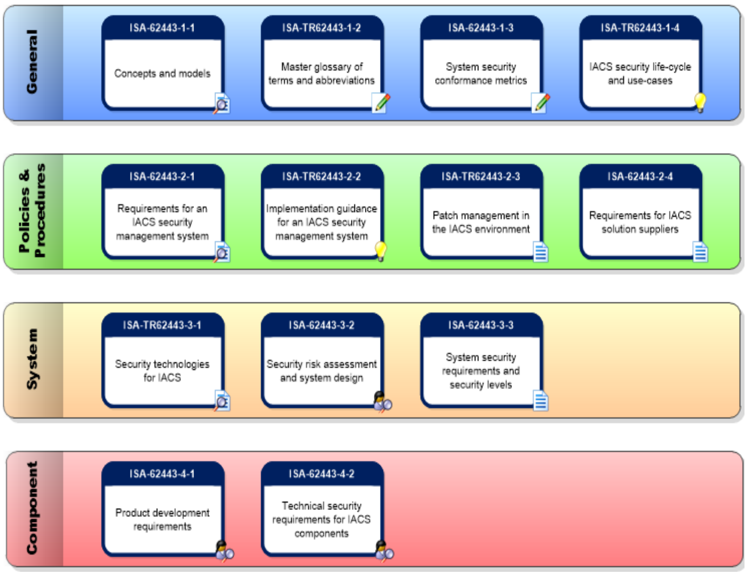
2 Recommendation

2.1 The CAB should decide that IECEE becomes the focus point for cybersecurity CA within all IEC CA Systems.

2.2 To request both IECRE and IECEx to consider the elaboration of application-dependent CA profiles for use by IECEE.

CAB Decision 42/12 — *CAB WG 17 – Cyber Security* The CAB thanked the WG 17 Convenor, Mr Pierre Selva, for his verbal report and thanked the German NC for their proposal given in document CAB/1679/DC, with comments in CAB/1679A/CC. CAB recognized that efficiency could be gained by concentrating all IEC operational CA cybersecurity activities. To serve the needs of the market and regulators, IECEE shall serve as the focus point for technical evaluation forming part of the conformity assessment services for all IEC CA Systems. The other IEC CA Systems shall define any additional sector-specific requirements as far as appropriate.

ISA / IEC 62443 PARTS OVERVIEW



General

ISA-62443-1-1 Concepts and models

ISA-TR62443-1-2 Master glossary of terms and abbreviations

ISA-62443-1-3 System security conformance metrics

ISA-TR62443-1-4 IACS security life-cycle and use-cases

Policies & Procedures

ISA-62443-2-1 Requirements for an IACS security management system

ISA-TR62443-2-2 Implementation guidance for an IACS security management system

ISA-TR62443-2-3 Patch management in the IACS environment

ISA-62443-2-4 Requirements for IACS solution suppliers

System

ISA-TR62443-3-1 Security technologies for IACS

ISA-62443-3-2 Security risk assessment and system design

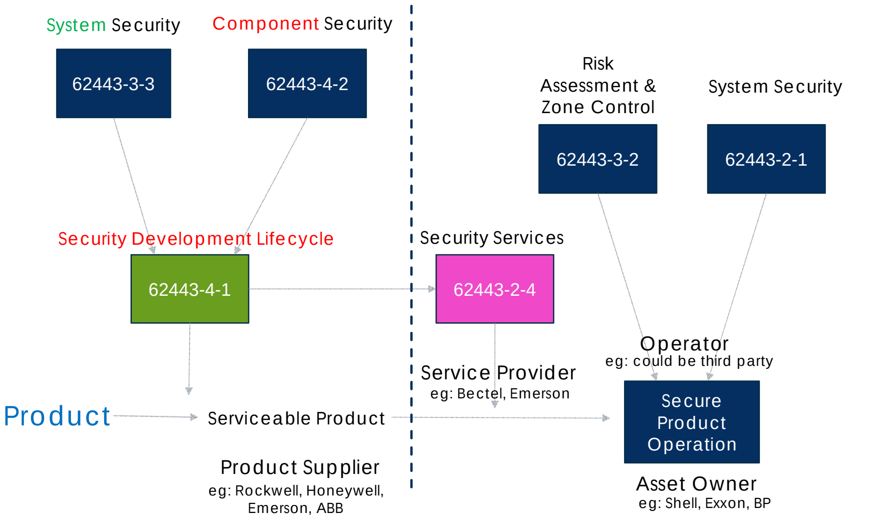
ISA-62443-3-3 System security requirements and security levels

Component

ISA-62443-4-1 Product development requirements

ISA-62443-4-2 Technical security requirements for IACS components

IEC Cyber Security Standards “Application Map”



System Security

62443-3-3

Component Security

62443-4-2

Security Development Lifecycle

62443-4-1

Product

Serviceable Product

Product Supplier

eg: Rockwell, Honeywell, Emerson, ABB

Security Services

62443-2-4

Service Provider

eg: Bectel, Emerson

Risk Assessment & Zone Control

62443-3-2

System Security

62443-2-1

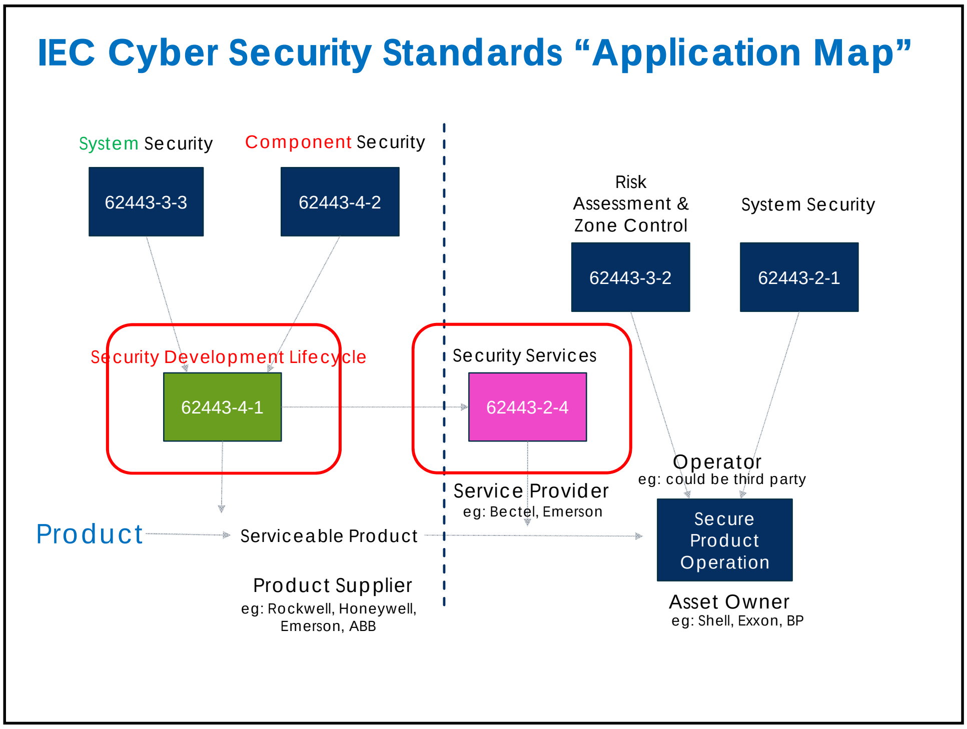
Operator

eg: could be third party

Secure Product Operation

Asset Owner

eg: Shell, Exxon, BP



IEC Cyber Security Standards “Application Map”

System Security

62443-3-3

Component Security

62443-4-2

Security Development Lifecycle

62443-4-1

Security Services

62443-2-4

Risk Assessment & Zone Control

62443-3-2

System Security

62443-2-1

Product

Serviceable Product

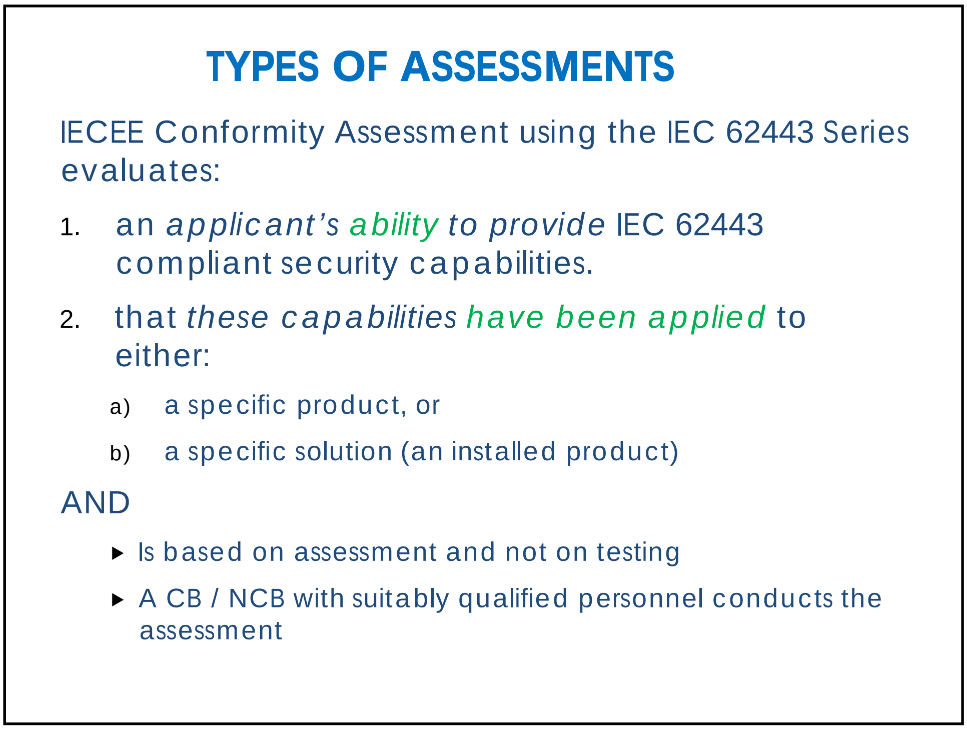
Product Supplier
eg: Rockwell, Honeywell, Emerson, ABB

Service Provider
eg: Bectel, Emerson

Operator
eg: could be third party

Secure Product Operation

Asset Owner
eg: Shell, Exxon, BP



TYPES OF ASSESSMENTS

IECEE Conformity Assessment using the IEC 62443 Series evaluates:

1. an *applicant’s ability to provide* IEC 62443 compliant security capabilities.
2. that *these capabilities have been applied* to either:
   a) a specific product, or
   b) a specific solution (an installed product)

AND

- Is based on assessment and not on testing
- A CB / NCB with suitably qualified personnel conducts the assessment

“MAIN STANDARDS”

IEC 62443-2-4 Security program requirements

Security requirements for capabilities that service providers can offer to customers for installation/integration (also called deployment) and maintenance of a control system – like a checklist of procedures an airplane mechanic will follow when installing new equipment or performing maintenance

“MAIN STANDARDS”

IEC 62443-4-1 Product security development life-cycle requirements

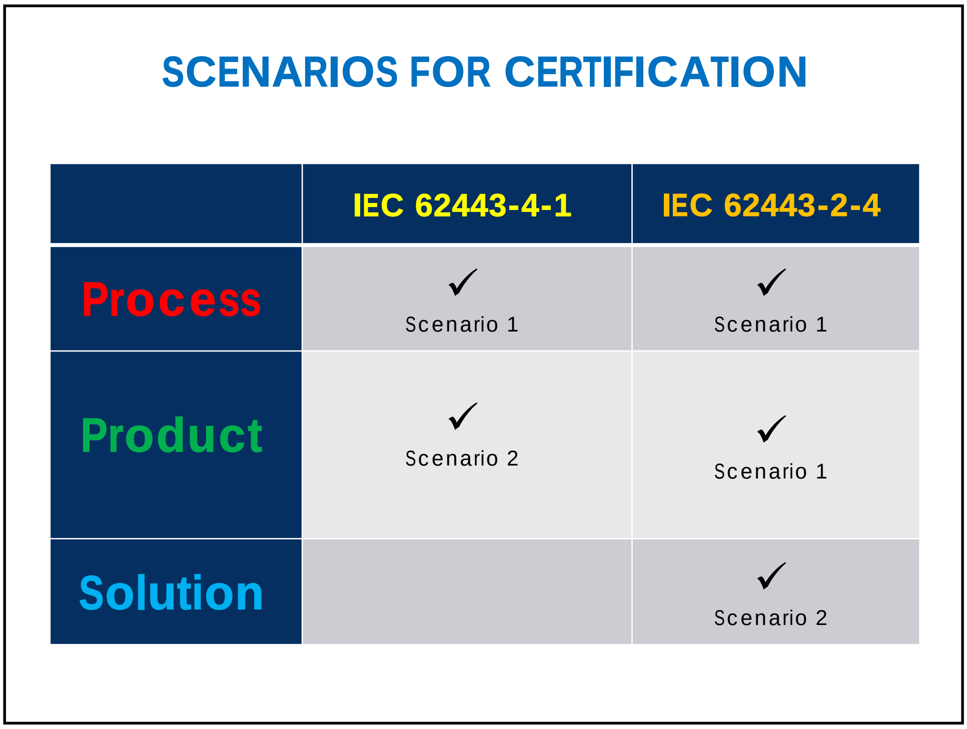
Security requirements for processes used during product development and support by a product supplier. One of the required development processes is to define security requirements for the product

Supporting standards for the definition of product security requirements

- IEC 62443-3-3 System security requirements and security levels

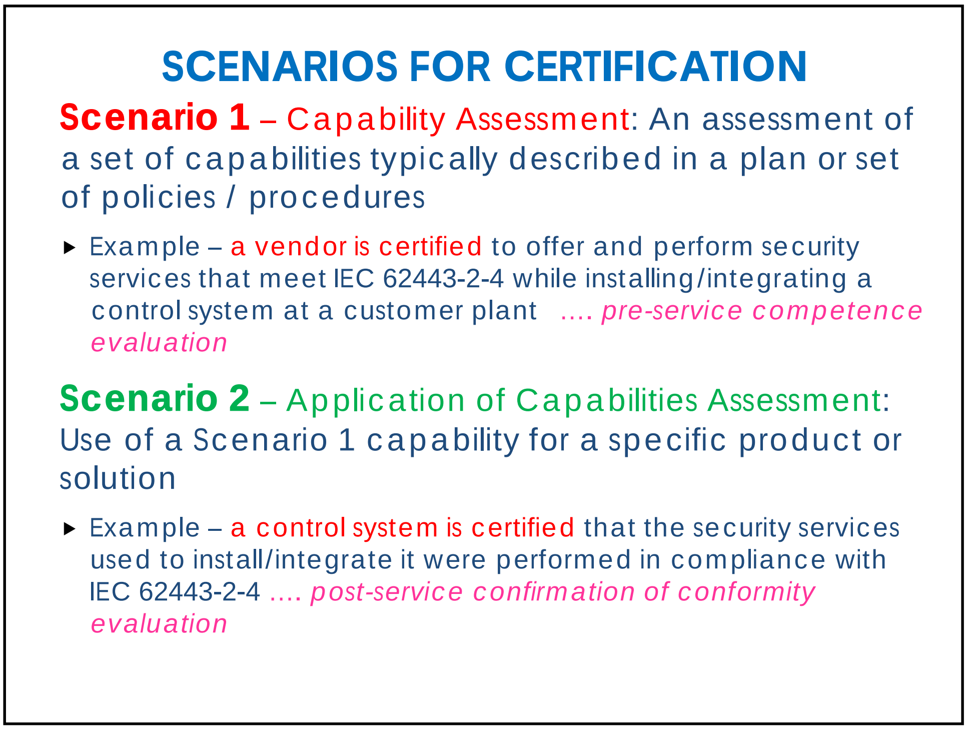
  Requirements for security capabilities of control systems taken as a whole
- IEC 62443-4-2 Technical security requirements for IACS components

  Requirements for security capabilities of components used in control systems



SCENARIOS FOR CERTIFICATION

	IEC 62443-4-1	IEC 62443-2-4
Process	✓ Scenario 1	✓ Scenario 1
Product	✓ Scenario 2	✓ Scenario 1
Solution		✓ Scenario 2



SCENARIOS FOR CERTIFICATION

Scenario 1 – Capability Assessment: An assessment of a set of capabilities typically described in a plan or set of policies / procedures

- Example – a vendor is certified to offer and perform security services that meet IEC 62443-2-4 while installing/integrating a control system at a customer plant .... *pre-service competence evaluation*

Scenario 2 – Application of Capabilities Assessment: Use of a Scenario 1 capability for a specific product or solution

- Example – a control system is certified that the security services used to install/integrate it were performed in compliance with IEC 62443-2-4 .... *post-service confirmation of conformity evaluation*

ASSESSMENT FOR IEC 62443-2-4

IEC 62443-2-4

Edition 1.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

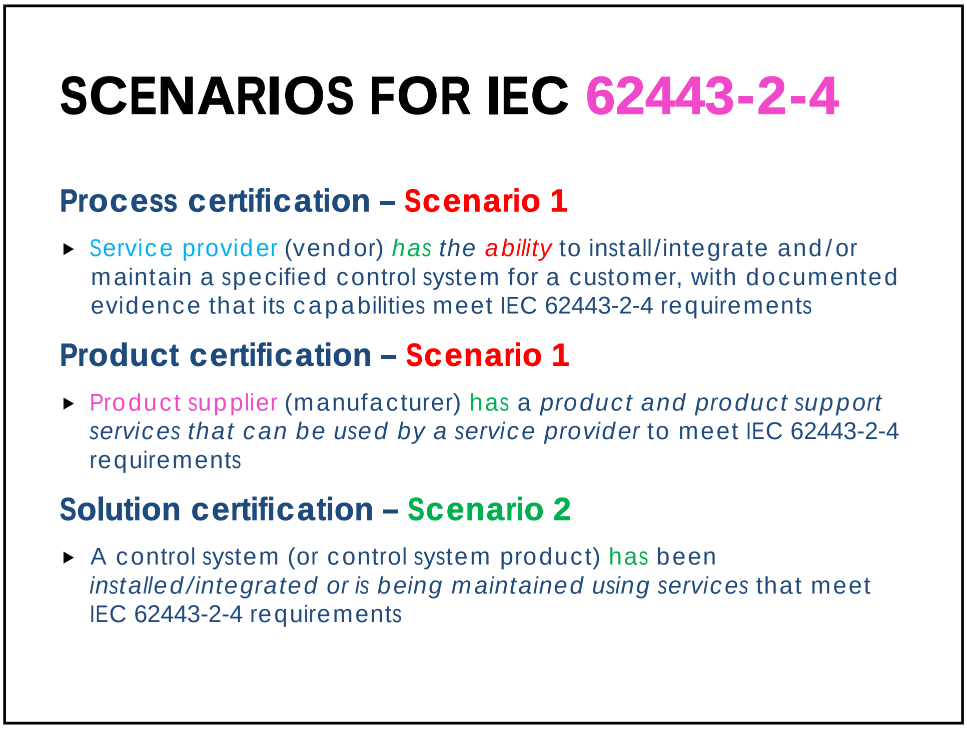
Sécurité des automatismes industriels et des systèmes de commande –
Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

IEC62443-2-4 CERTIFICATION

is NOT granted on the basis of specific components, software, hardware etc. BUT the capability that is being certified may be a function of specific components, software, hardware etc.

For example, a vendor’s capability may be limited to Brand X hardware using Brand Y firewalls and Brand Z PLCs

OR perhaps even further limited to models or versions



SCENARIOS FOR IEC 62443-2-4

Process certification – Scenario 1

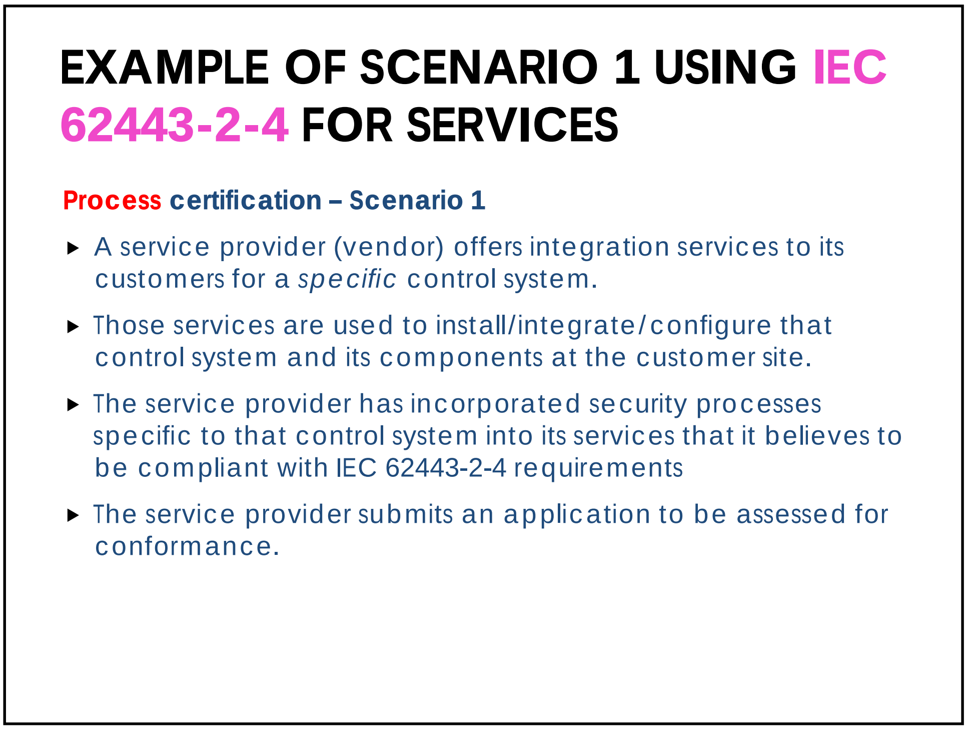
- Service provider (vendor) *has the ability* to install/integrate and/or maintain a specified control system for a customer, with documented evidence that its capabilities meet IEC 62443-2-4 requirements

Product certification – Scenario 1

- Product supplier (manufacturer) has a *product and product support services that can be used by a service provider* to meet IEC 62443-2-4 requirements

Solution certification – Scenario 2

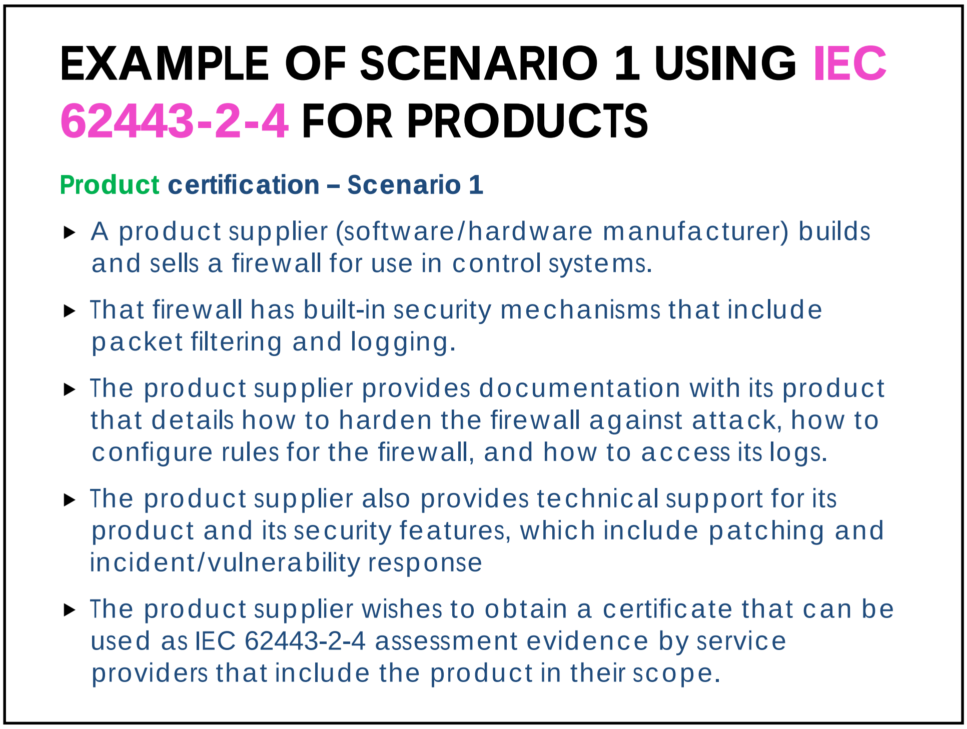
- A control system (or control system product) has been *installed/integrated or is being maintained using services* that meet IEC 62443-2-4 requirements



EXAMPLE OF SCENARIO 1 USING IEC 62443-2-4 FOR SERVICES

Process certification – Scenario 1

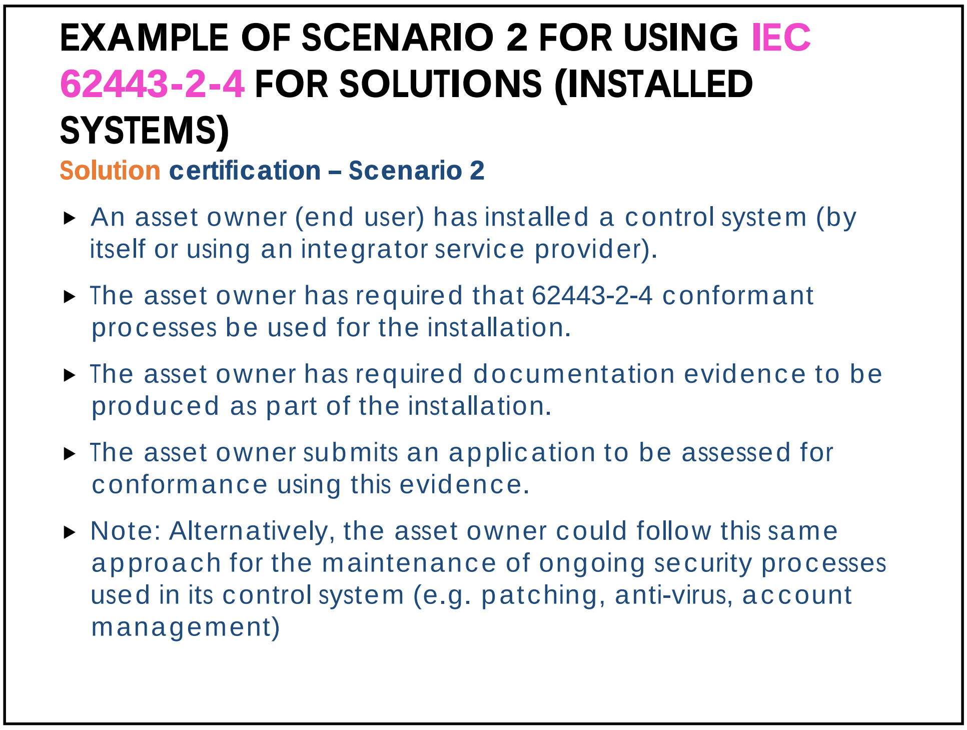
- A service provider (vendor) offers integration services to its customers for a *specific* control system.
- Those services are used to install/integrate/configure that control system and its components at the customer site.
- The service provider has incorporated security processes specific to that control system into its services that it believes to be compliant with IEC 62443-2-4 requirements
- The service provider submits an application to be assessed for conformance.



EXAMPLE OF SCENARIO 1 USING IEC 62443-2-4 FOR PRODUCTS

Product certification – Scenario 1

- A product supplier (software/hardware manufacturer) builds and sells a firewall for use in control systems.
- That firewall has built-in security mechanisms that include packet filtering and logging.
- The product supplier provides documentation with its product that details how to harden the firewall against attack, how to configure rules for the firewall, and how to access its logs.
- The product supplier also provides technical support for its product and its security features, which include patching and incident/vulnerability response
- The product supplier wishes to obtain a certificate that can be used as IEC 62443-2-4 assessment evidence by service providers that include the product in their scope.



EXAMPLE OF SCENARIO 2 FOR USING IEC 62443-2-4 FOR SOLUTIONS (INSTALLED SYSTEMS)

Solution certification – Scenario 2

- An asset owner (end user) has installed a control system (by itself or using an integrator service provider).
- The asset owner has required that 62443-2-4 conformant processes be used for the installation.
- The asset owner has required documentation evidence to be produced as part of the installation.
- The asset owner submits an application to be assessed for conformance using this evidence.
- Note: Alternatively, the asset owner could follow this same approach for the maintenance of ongoing security processes used in its control system (e.g. patching, anti-virus, account management)

ASSESSMENT FOR IEC 62443-4-1

IEC

IEC 62443-4-1

Edition 1.0

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems –

Part 4-1: Product security development life-cycle requirements

SCENARIOS FOR IEC 62443-4-1

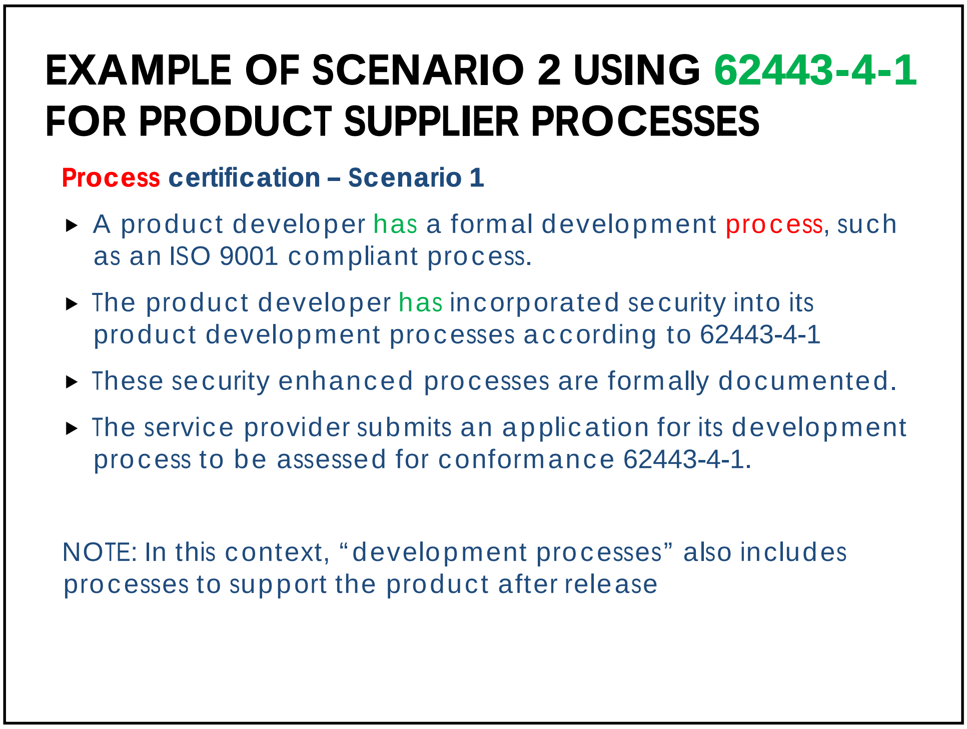
Process certification – Scenario 1

- Product supplier (manufacturer) *has a development process* for securely developing and supporting one or more products as required by IEC 62443-4-1

Product certification – Scenario 2

- Product supplier (manufacturer) has developed a product and supporting services (e.g. patching) using processes that were performed in accordance with IEC 62443-4-1 requirements

  NOTE: IEC 62443-4-1 requirements require that security requirements for the product are identified (e.g. from IEC 62443-3-3 or IEC 62443-4-2) and properly implemented in the product (with verification)

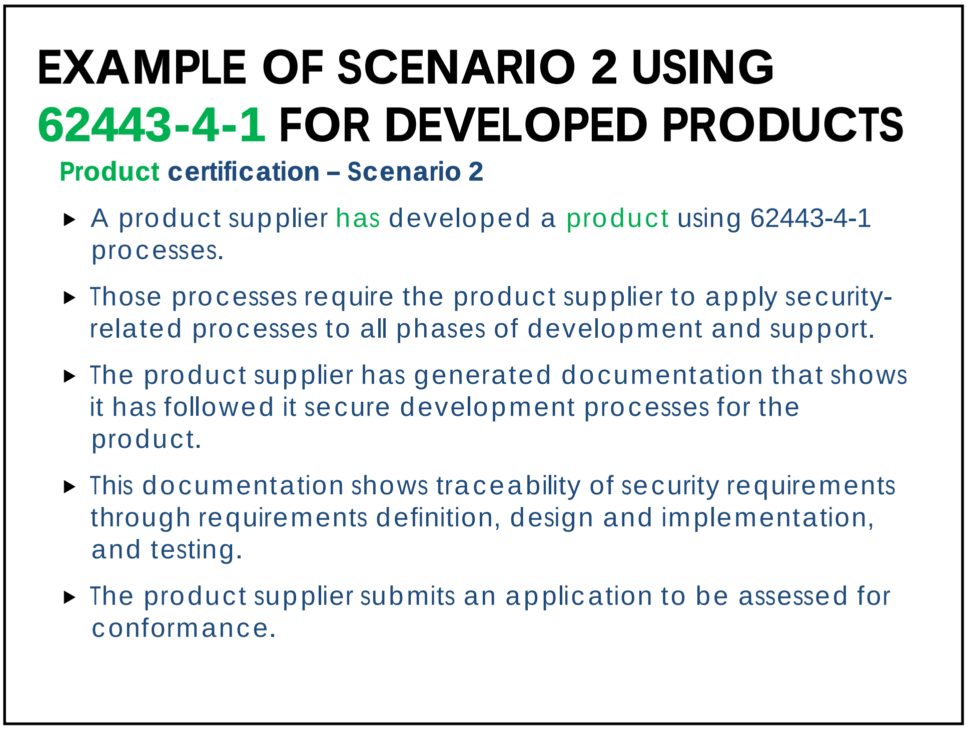


EXAMPLE OF SCENARIO 2 USING 62443-4-1 FOR PRODUCT SUPPLIER PROCESSES

Process certification – Scenario 1

- A product developer has a formal development process, such as an ISO 9001 compliant process.
- The product developer has incorporated security into its product development processes according to 62443-4-1
- These security enhanced processes are formally documented.
- The service provider submits an application for its development process to be assessed for conformance 62443-4-1.

NOTE: In this context, “development processes” also includes processes to support the product after release

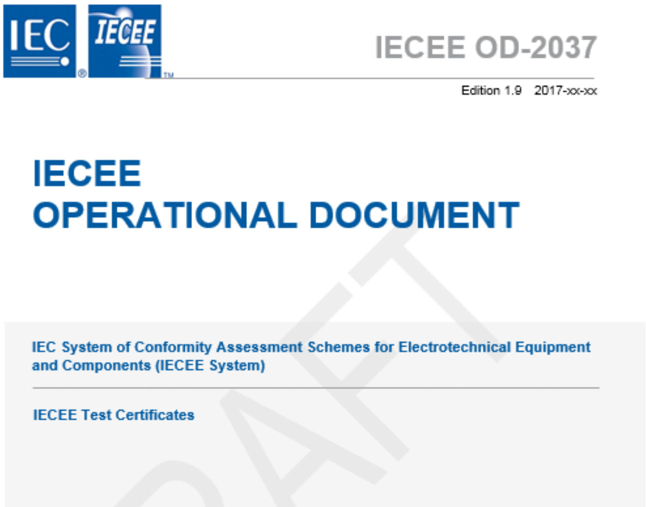


EXAMPLE OF SCENARIO 2 USING 62443-4-1 FOR DEVELOPED PRODUCTS

Product certification – Scenario 2

- A product supplier has developed a product using 62443-4-1 processes.
- Those processes require the product supplier to apply security-related processes to all phases of development and support.
- The product supplier has generated documentation that shows it has followed it secure development processes for the product.
- This documentation shows traceability of security requirements through requirements definition, design and implementation, and testing.
- The product supplier submits an application to be assessed for conformance.

CYBER-SECURITY “CERTIFICATES”



IECEE OD-2037

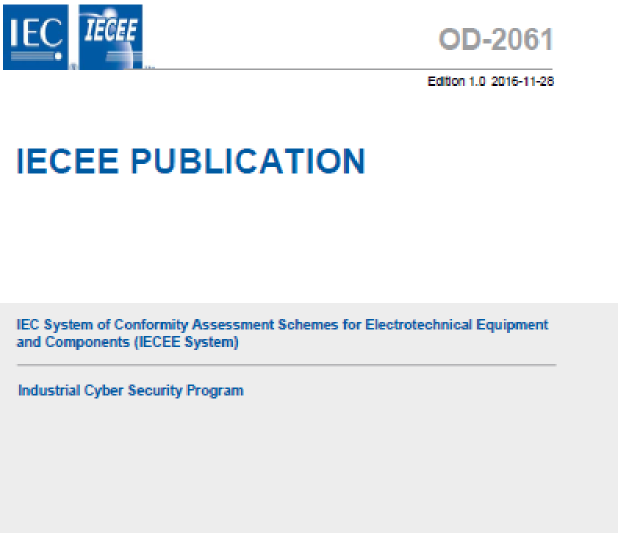
Edition 1.9 2017-xx-xx

IECEE
OPERATIONAL DOCUMENT

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System)

IECEE Test Certificates

IECEE SYSTEM OPERATIONAL DOCUMENT



OD-2061

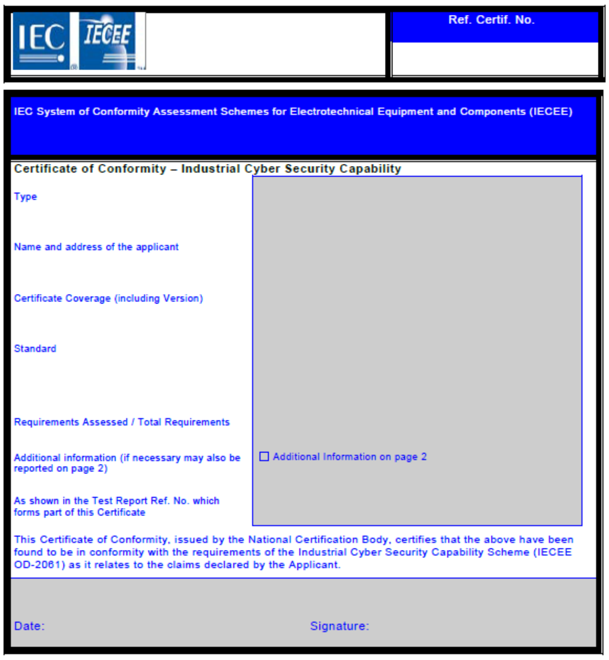
Edition 1.0 2016-11-28

IECEE PUBLICATION

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System)

Industrial Cyber Security Program

IECEE CERTIFICATE FORMAT & CONTENT ….



Ref. Certif. No.

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)

Standard

Requirements Assessed / Total Requirements

Additional information (if necessary may also be reported on page 2)

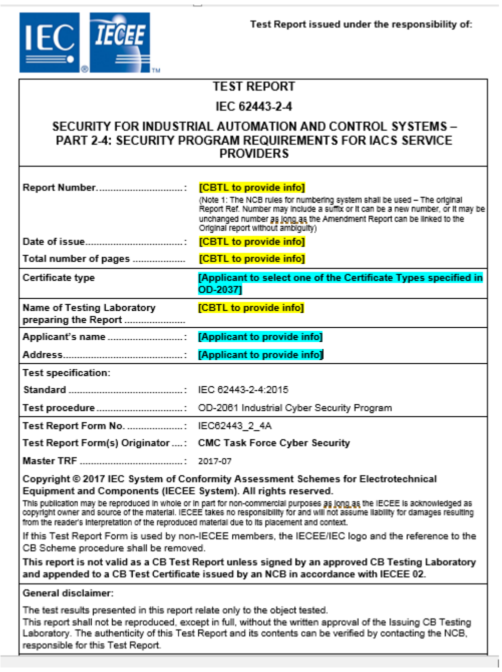
□ Additional Information on page 2

As shown in the Test Report Ref. No. which forms part of this Certificate

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.

Date:

Signature:



Test Report issued under the responsibility of:

TEST REPORT

IEC 62443-2-4

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS – PART 2-4: SECURITY PROGRAM REQUIREMENTS FOR IACS SERVICE PROVIDERS

Report Number.................................:	**[CBTL to provide info]** (Note 1: The NCB rules for numbering system shall be used – The original Report Ref. Number may include a suffix or it can be a new number, or it may be unchanged number as long as the Amendment Report can be linked to the Original report without ambiguity)
Date of issue......................................:	**[CBTL to provide info]**
Total number of pages	**[CBTL to provide info]**
Certificate type	**[Applicant to select one of the Certificate Types specified in OD-2037]**
Name of Testing Laboratory preparing the Report	**[CBTL to provide info]**
Applicant's name ....:	**[Applicant to provide info]**
Address..:	**[Applicant to provide info]**
Test specification:	
Standard ....:	IEC 62443-2-4:2015
Test procedure ....:	OD-2061 Industrial Cyber Security Program
Test Report Form No. ....:	IEC62443_2_4A
Test Report Form(s) Originator ....:	**CMC Task Force Cyber Security**
Master TRF ....:	2017-07

Copyright © 2017 IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System). All rights reserved.

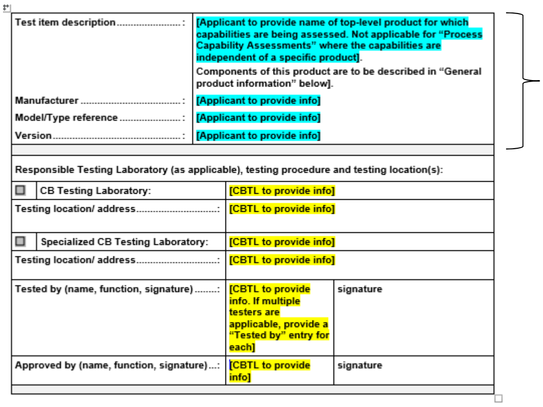
This publication may be reproduced in whole or in part for non-commercial purposes as long as the IECEE is acknowledged as copyright owner and source of the material. IECEE takes no responsibility for and will not assume liability for damages resulting from the reader's interpretation of the reproduced material due to its placement and context.

If this Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the CB Scheme procedure shall be removed.

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

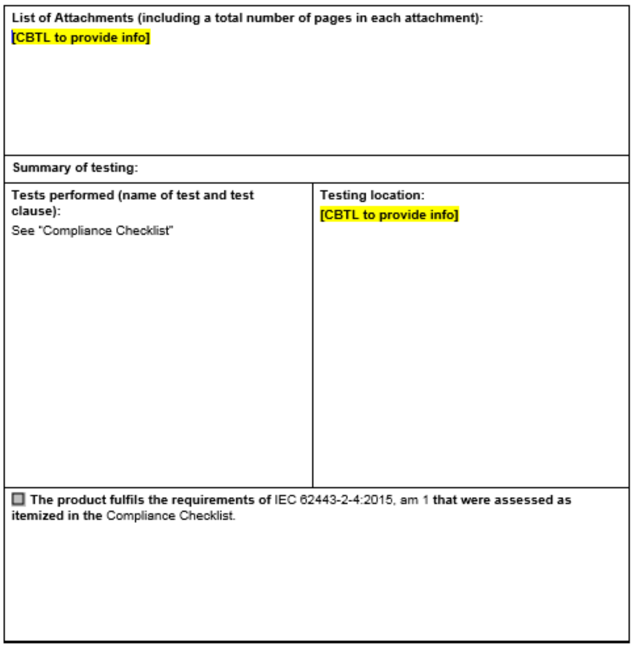
General disclaimer:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing CB Testing Laboratory. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.



Test item description.........................:	**[Applicant to provide name of top-level product for which capabilities are being assessed. Not applicable for "Process Capability Assessments" where the capabilities are independent of a specific product].** **Components of this product are to be described in "General product information" below].**	
Manufacturer ....:	**[Applicant to provide info]**	
Model/Type reference ....:	**[Applicant to provide info]**	
Version...:	**[Applicant to provide info]**	
Responsible Testing Laboratory (as applicable), testing procedure and testing location(s):		
☐ **CB Testing Laboratory:**	**[CBTL to provide info]**	
Testing location/ address...............................:	**[CBTL to provide info]**	
☐ **Specialized CB Testing Laboratory:**	**[CBTL to provide info]**	
Testing location/ address...............................:	**[CBTL to provide info]**	
Tested by (name, function, signature) ....:	**[CBTL to provide info. If multiple testers are applicable, provide a "Tested by" entry for each]**	**signature**
Approved by (name, function, signature) ....:	**[CBTL to provide info]**	**signature**

- Typically capabilities to be assessed are associated with a specific product, such as a control system that an integrator installs, or a component that a maintenance contractor maintains.
- In layman's terms, if the applicant were an auto mechanic, the applicant would be certified to work on a specific model/make (e.g. Mercedes E-Class)

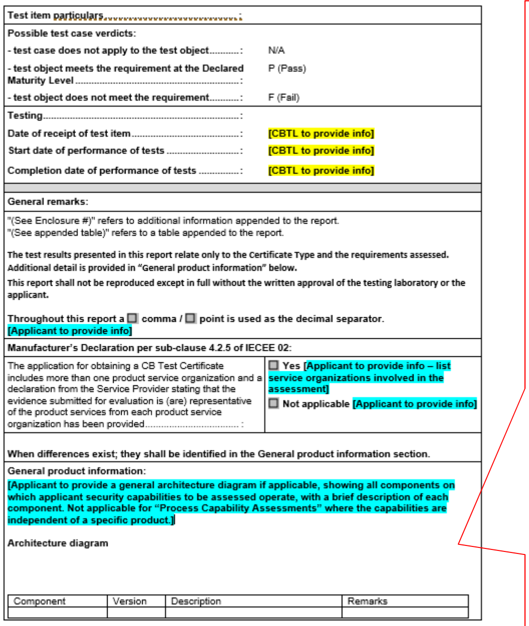


List of Attachments (including a total number of pages in each attachment):
[CBTL to provide info]

Summary of testing:

Tests performed (name of test and test clause): See "Compliance Checklist"	Testing location: [CBTL to provide info]

□ The product fulfils the requirements of IEC 62443-2-4:2015, am 1 that were assessed as itemized in the Compliance Checklist.



Test item particulars..:	
Possible test case verdicts:	
- test case does not apply to the test object...........:	N/A
- test object meets the requirement at the Declared Maturity Level ....:	P (Pass)
- test object does not meet the requirement...........:	F (Fail)
Testing...:	
Date of receipt of test item...:	[CBTL to provide info]
Start date of performance of tests ....:	[CBTL to provide info]
Completion date of performance of tests ....:	[CBTL to provide info]

General remarks:

"(See Enclosure #)" refers to additional information appended to the report.
"(See appended table)" refers to a table appended to the report.

The test results presented in this report relate only to the Certificate Type and the requirements assessed. Additional detail is provided in "General product information" below.

This report shall not be reproduced except in full without the written approval of the testing laboratory or the applicant.

Throughout this report a □ comma / □ point is used as the decimal separator.
[Applicant to provide info]

Manufacturer's Declaration per sub-clause 4.2.5 of IECEE 02:

The application for obtaining a CB Test Certificate includes more than one product service organization and a declaration from the Service Provider stating that the evidence submitted for evaluation is (are) representative of the product services from each product service organization has been provided.................................. :	□ Yes [Applicant to provide info – list service organizations involved in the assessment] □ Not applicable [Applicant to provide info]

When differences exist; they shall be identified in the General product information section.

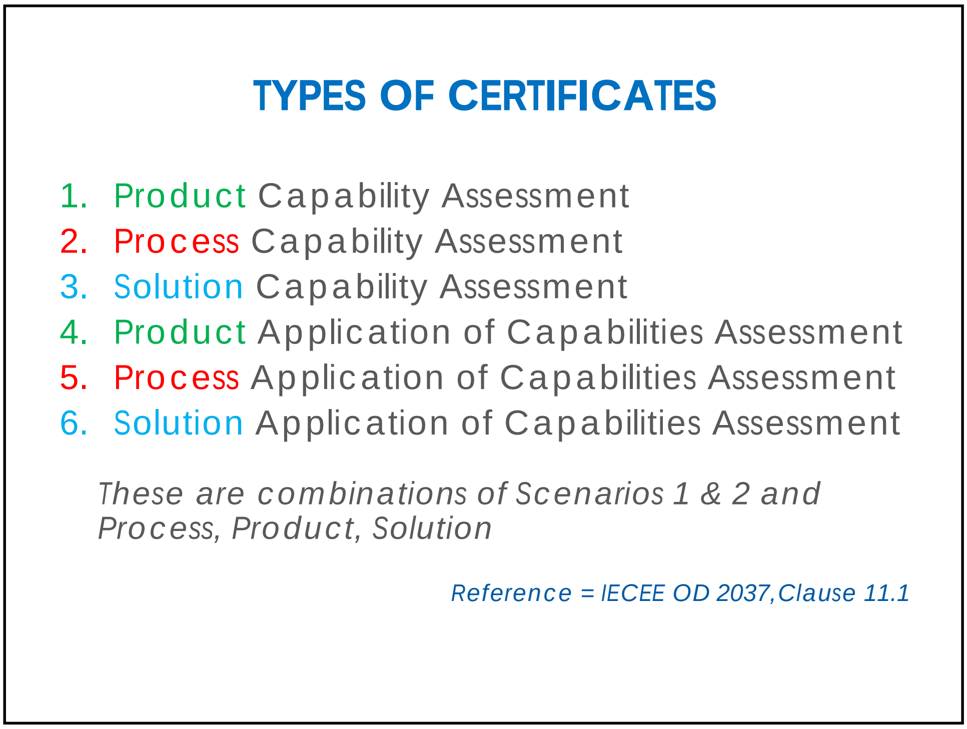
General product information:

[Applicant to provide a general architecture diagram if applicable, showing all components on which applicant security capabilities to be assessed operate, with a brief description of each component. Not applicable for "Process Capability Assessments" where the capabilities are independent of a specific product.]

Architecture diagram

Component	Version	Description	Remarks

- Diagram of the *product* identified in the "Test Item Description" above.
- Diagram to be accompanied by a brief description of each component or component type (e.g. Windows 10 workstation)
- Used by the assessor to determine what is "in scope" of the assessment, and what is not
- Often used by customers of the application to see what was "in scope"

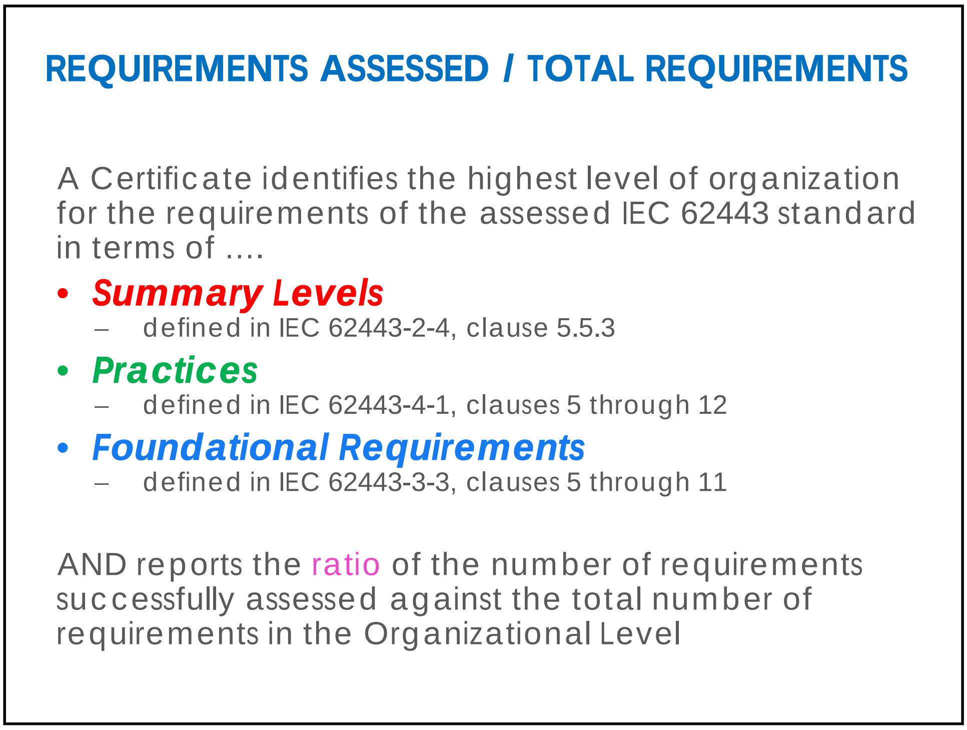


TYPES OF CERTIFICATES

1. Product Capability Assessment
2. Process Capability Assessment
3. Solution Capability Assessment
4. Product Application of Capabilities Assessment
5. Process Application of Capabilities Assessment
6. Solution Application of Capabilities Assessment

These are combinations of Scenarios 1 & 2 and Process, Product, Solution

Reference = IECEE OD 2037, Clause 11.1

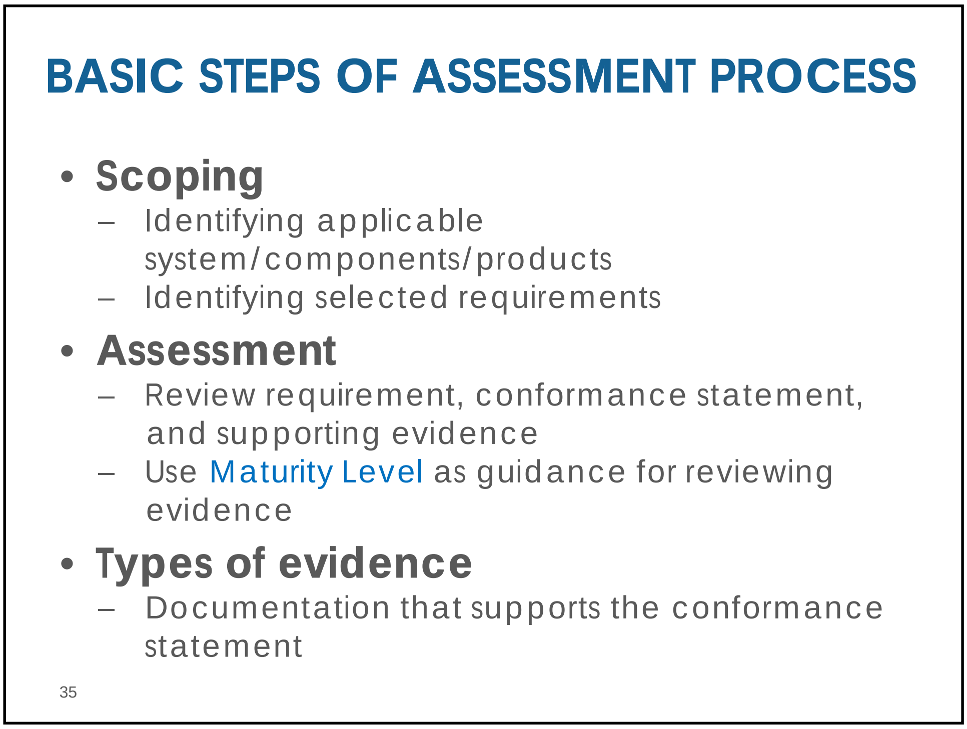


REQUIREMENTS ASSESSED / TOTAL REQUIREMENTS

A Certificate identifies the highest level of organization for the requirements of the assessed IEC 62443 standard in terms of ….

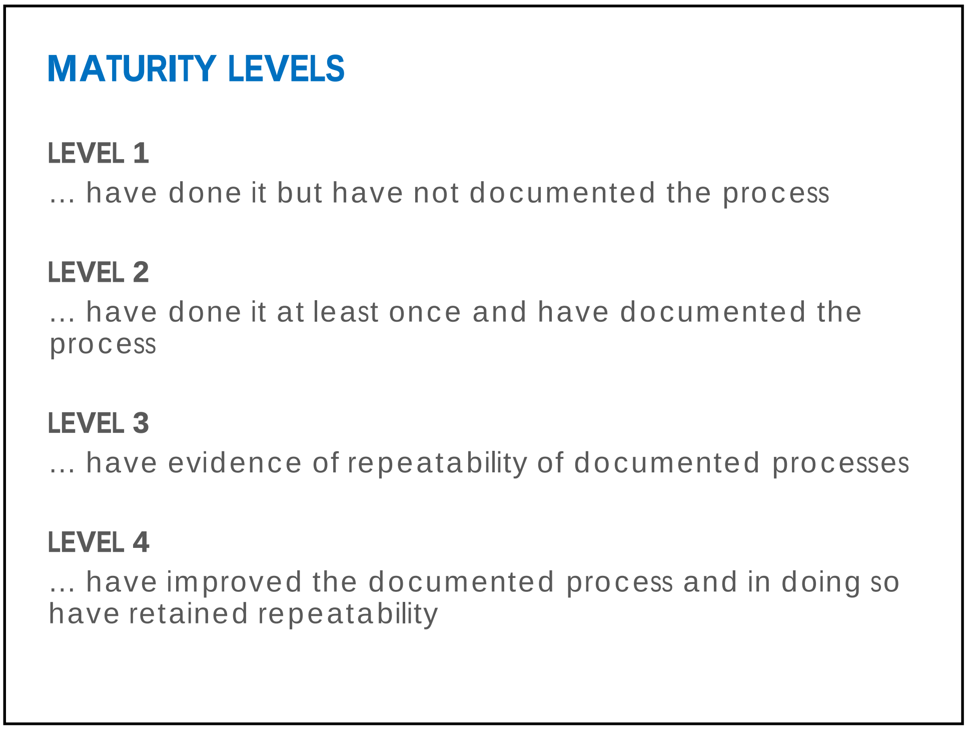
- ***Summary Levels***
  - defined in IEC 62443-2-4, clause 5.5.3
- ***Practices***
  - defined in IEC 62443-4-1, clauses 5 through 12
- ***Foundational Requirements***
  - defined in IEC 62443-3-3, clauses 5 through 11

AND reports the ratio of the number of requirements successfully assessed against the total number of requirements in the Organizational Level



BASIC STEPS OF ASSESSMENT PROCESS

- **Scoping**
  - Identifying applicable system/components/products
  - Identifying selected requirements
- **Assessment**
  - Review requirement, conformance statement, and supporting evidence
  - Use Maturity Level as guidance for reviewing evidence
- **Types of evidence**
  - Documentation that supports the conformance statement



MATURITY LEVELS

LEVEL 1

… have done it but have not documented the process

LEVEL 2

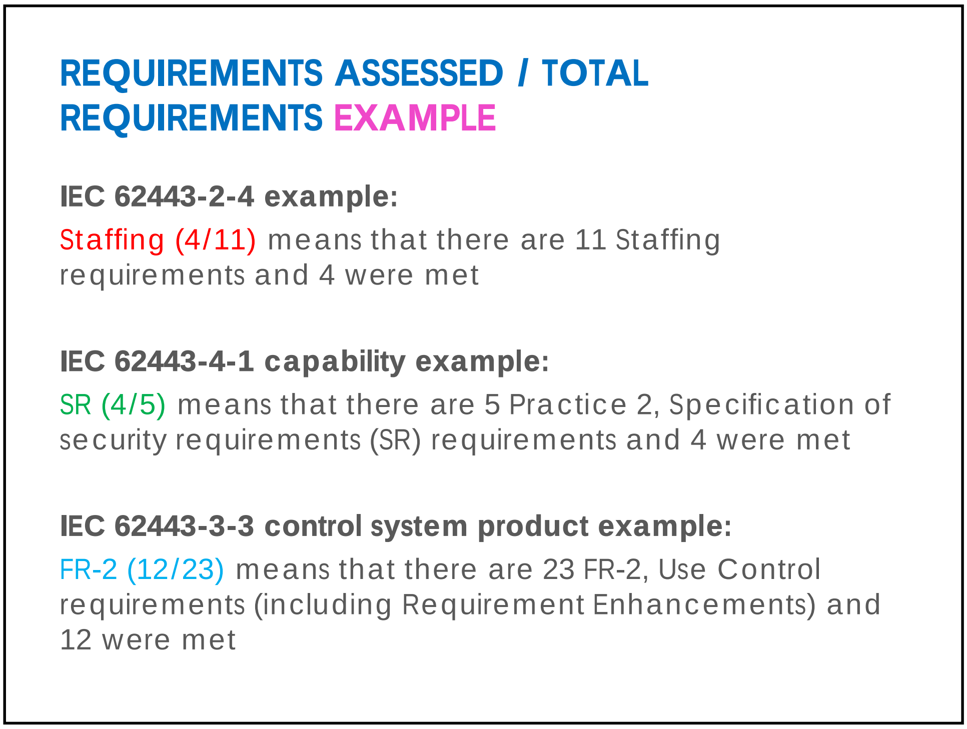
… have done it at least once and have documented the process

LEVEL 3

… have evidence of repeatability of documented processes

LEVEL 4

… have improved the documented process and in doing so have retained repeatability



REQUIREMENTS ASSESSED / TOTAL REQUIREMENTS EXAMPLE

IEC 62443-2-4 example:

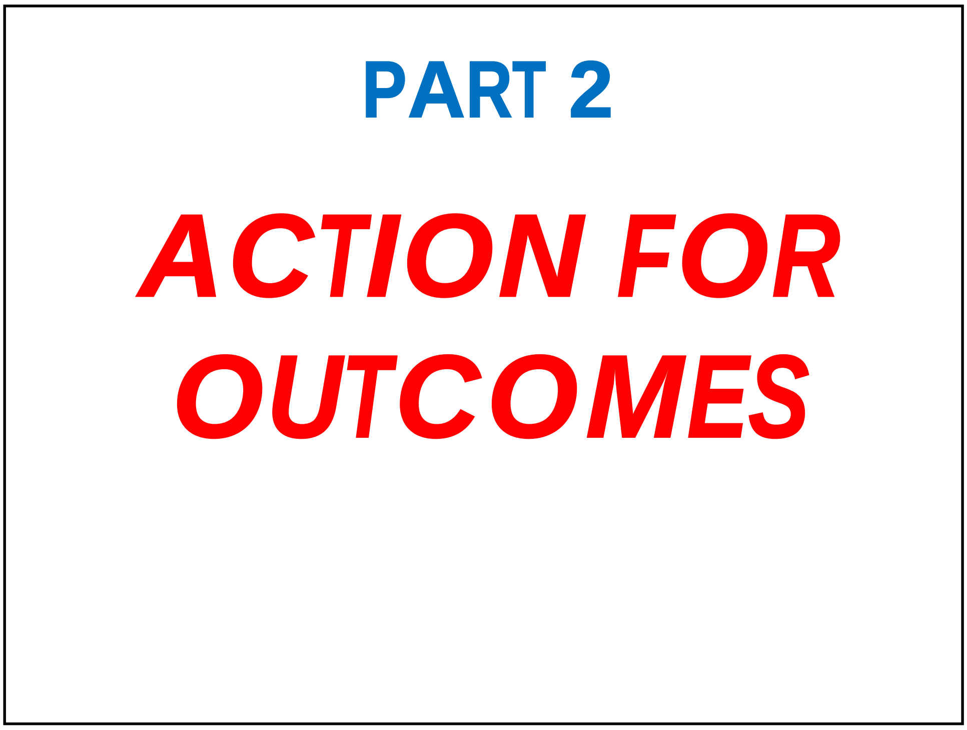
Staffing (4/11) means that there are 11 Staffing requirements and 4 were met

IEC 62443-4-1 capability example:

SR (4/5) means that there are 5 Practice 2, Specification of security requirements (SR) requirements and 4 were met

IEC 62443-3-3 control system product example:

FR-2 (12/23) means that there are 23 FR-2, Use Control requirements (including Requirement Enhancements) and 12 were met



PART 2

ACTION FOR OUTCOMES

CAB Decision 42/12

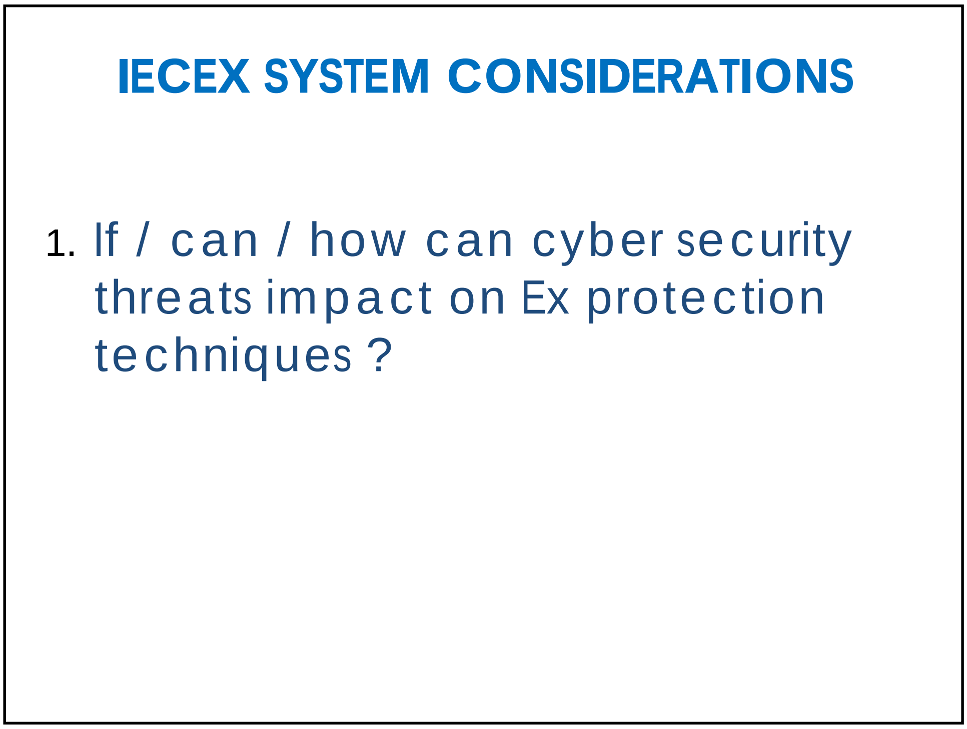
…………

………….

To serve the needs of the market and regulators, IECEE shall serve as the focus point for technical evaluation forming part of the conformity assessment services for all IEC CA Systems. The other IEC CA Systems shall define any additional sector-specific requirements as far as appropriate.

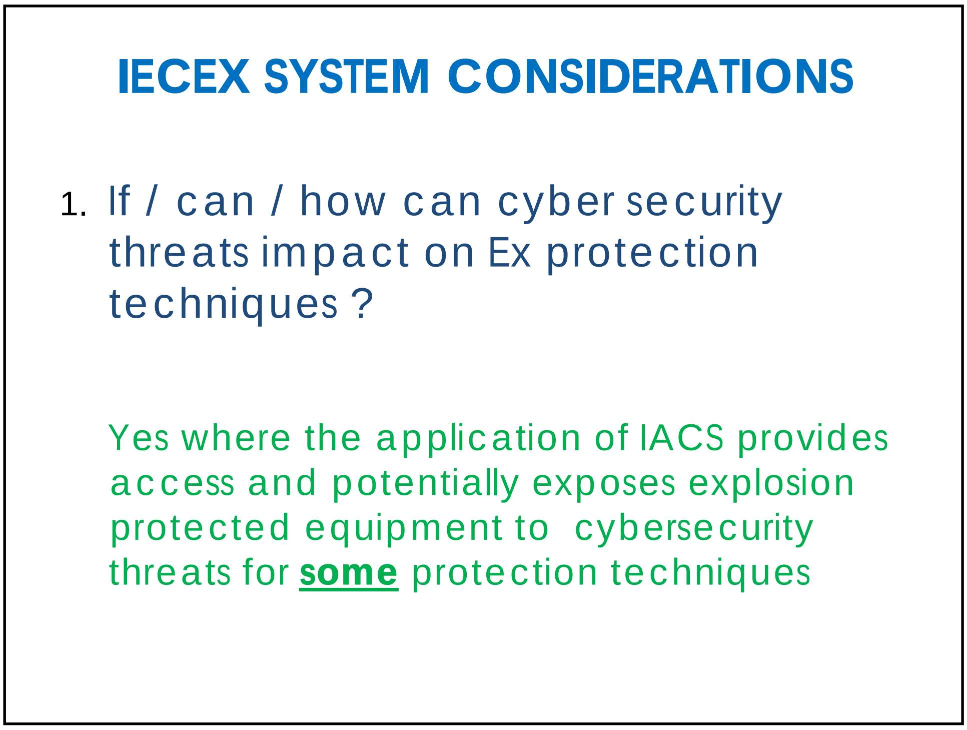
"TASKS" ….

1. first define which Ex products may be impacted by cyber security threats and then determine which parts of IEC 62443 may apply to IECEx
2. create a written statement that sets up a common understanding of Cyber Security for Ex-protected equipment and will be the basis for further discussion within this group and with CAB/WG 17 and IECEE PSC WG 3 both dealing with cyber security.



IECEX SYSTEM CONSIDERATIONS

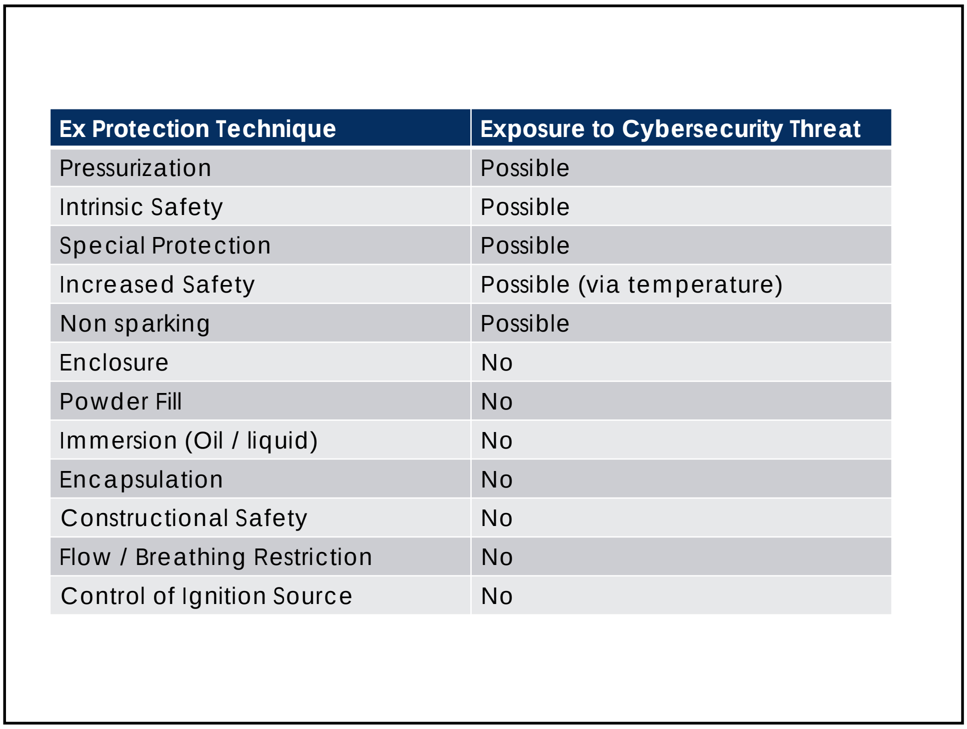
1. If / can / how can cyber security threats impact on Ex protection techniques ?



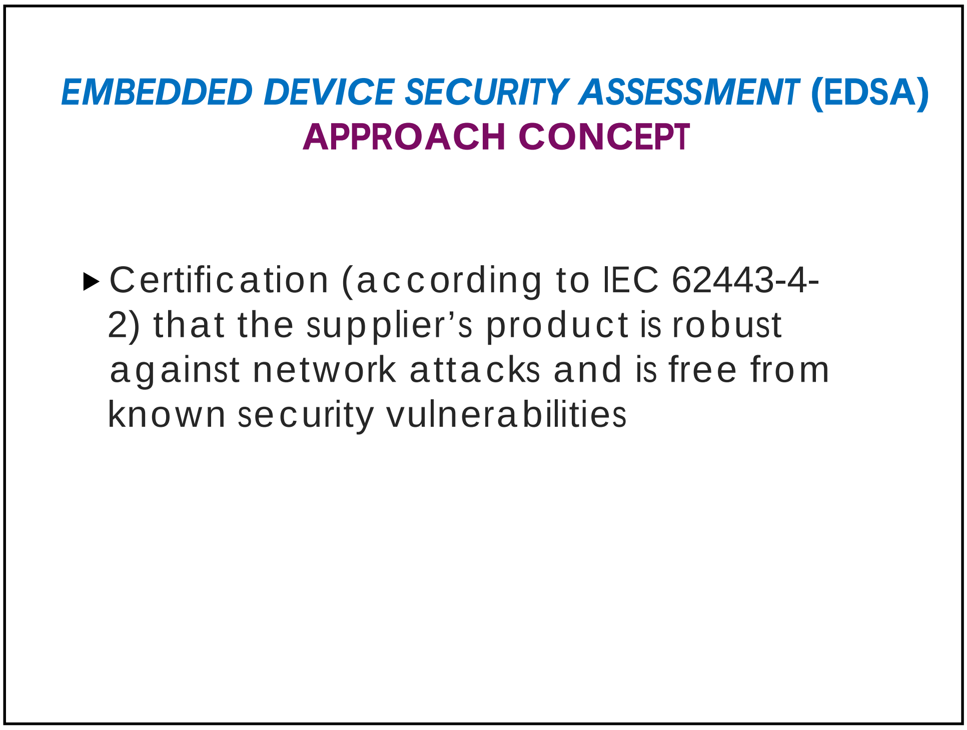
IECEX SYSTEM CONSIDERATIONS

1. If / can / how can cyber security threats impact on Ex protection techniques ?

Yes where the application of IACS provides access and potentially exposes explosion protected equipment to cybersecurity threats for **some** protection techniques



Ex Protection Technique	Exposure to Cybersecurity Threat
Pressurization	Possible
Intrinsic Safety	Possible
Special Protection	Possible
Increased Safety	Possible (via temperature)
Non sparking	Possible
Enclosure	No
Powder Fill	No
Immersion (Oil / liquid)	No
Encapsulation	No
Constructional Safety	No
Flow / Breathing Restriction	No
Control of Ignition Source	No



EMBEDDED DEVICE SECURITY ASSESSMENT (EDSA) APPROACH CONCEPT

- Certification (according to IEC 62443-4-2) that the supplier’s product is robust against network attacks and is free from known security vulnerabilities

WHAT IS AN EMBEDDED DEVICE ?

Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process:

Examples are:

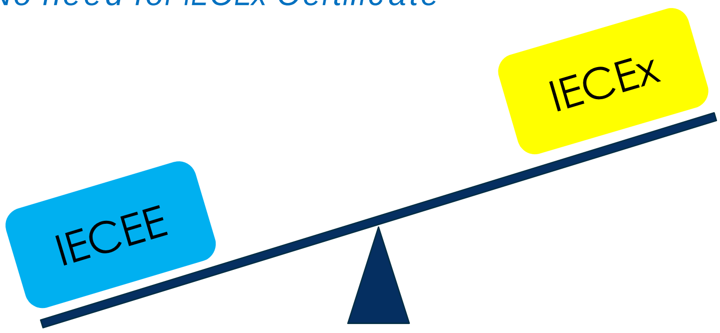
- Programmable Logic Controller (PLC)
- Distributed Control System (DCS) controller
- Safety Logic Solver (Emergency Shut down Logic Unit)
- Programmable Automation Controller (PAC)
- Intelligent Electronic Device (IED)
- Digital Protective Relay
- Smart Motor Starter/Controller
- SCADA Controller
- Remote Terminal Unit (RTU)
- Networked Vibration monitoring controller
- Net worked Gas detectors

CERTIFICATION CHOICE BALANCE

SITUATION

Ex equipment as an embedded device in a IACS controlled system ....

1. *IECEE Certificate to IEC 62443-4-2 or IEC 62443-3-3*
2. *No need for IECEx Certificate*

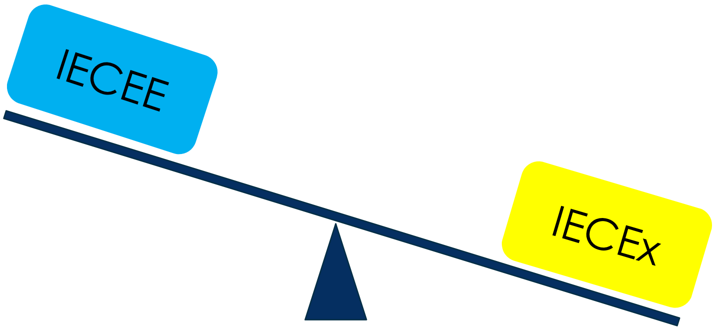


CERTIFICATION CHOICE BALANCE

SITUATION

Explosion protected system with exposure to a cybersecurity threat via use of IACS ....

1. *IECEE Certificate to IEC 62443-4-2 or IEC 62443-3-3 used as a basis for an IECEx Certificate*



IECEx System Requirements

IECEx 02,

8.1.1 Issue

An IECEx Certificate of Conformity is issued by an ExCB, on the basis of an ExTR and QAR. It certifies that the type of Ex equipment identified on the certificate conforms in all relevant respects with the standard(s) specified on the certificate. The manufacturer named on the certificate manufactures the product under a quality system and associated quality plan(s) complying with the requirements of ISO/IEC 80079-34, as a means of providing adequate confidence that the Ex equipment will be produced in conformity with the design of the certified equipment.

IECEx System Requirements

IECEx 02,

8.2 IECEx Test Report (ExTR)

8.2.1 Preparation

An ExTR is prepared and issued by an ExTL but must be endorsed by an ExCB, associated with the ExTL, recording the product design assessment, examination and assessment and testing work carried out in order to verify the conformity of Ex equipment with the requirements of the stated standards.

IECEx System Certification OPTIONS

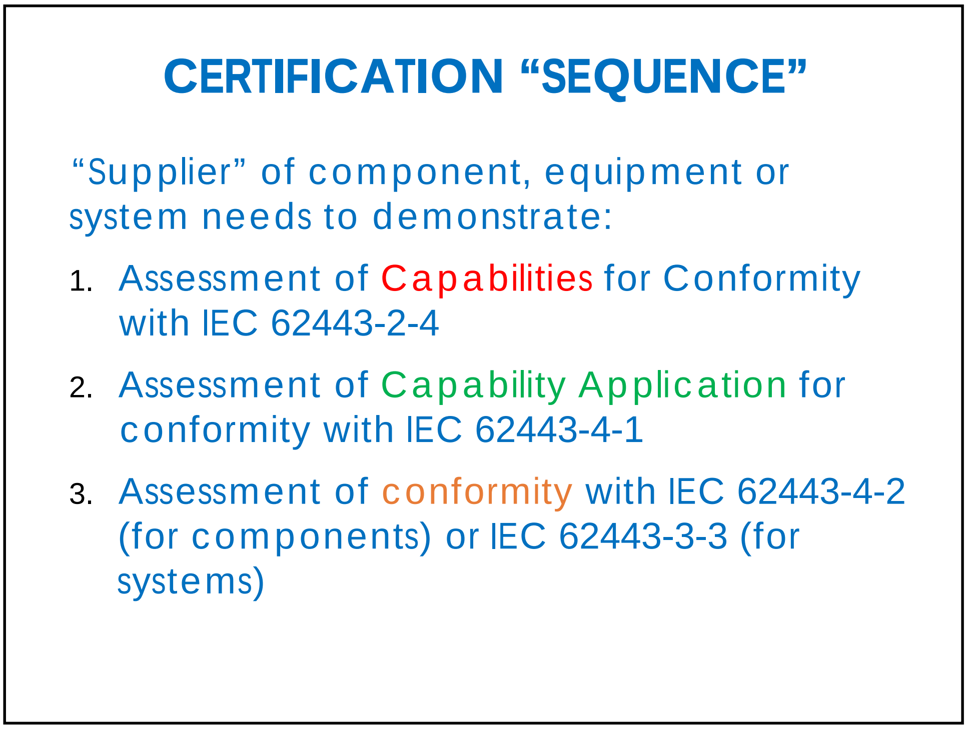
OPTION #1

"Normal IECEx Certificate of Conformity" based on an ExTR for tested sample (compliance with relevant Standards) **and** a QAR (continued capability) based on ongoing surveillance

OPTION #2

"Unit Verification" type IECEx Certificate of Conformity" for specified units of production based on an ExTR for tested sample (compliance with relevant Standards) – *no QAR (continued capability) required BUT no up-issue permitted.*

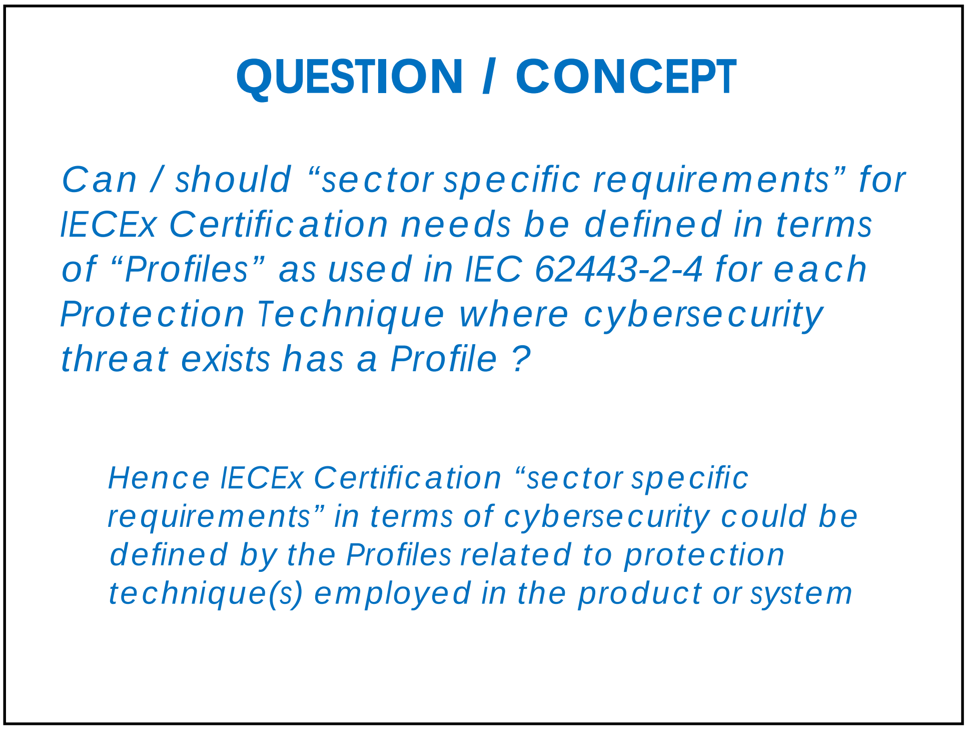
NOTE: DS 2015/001A for assemblies is based on Unit Verification Certificates



CERTIFICATION “SEQUENCE”

“Supplier” of component, equipment or system needs to demonstrate:

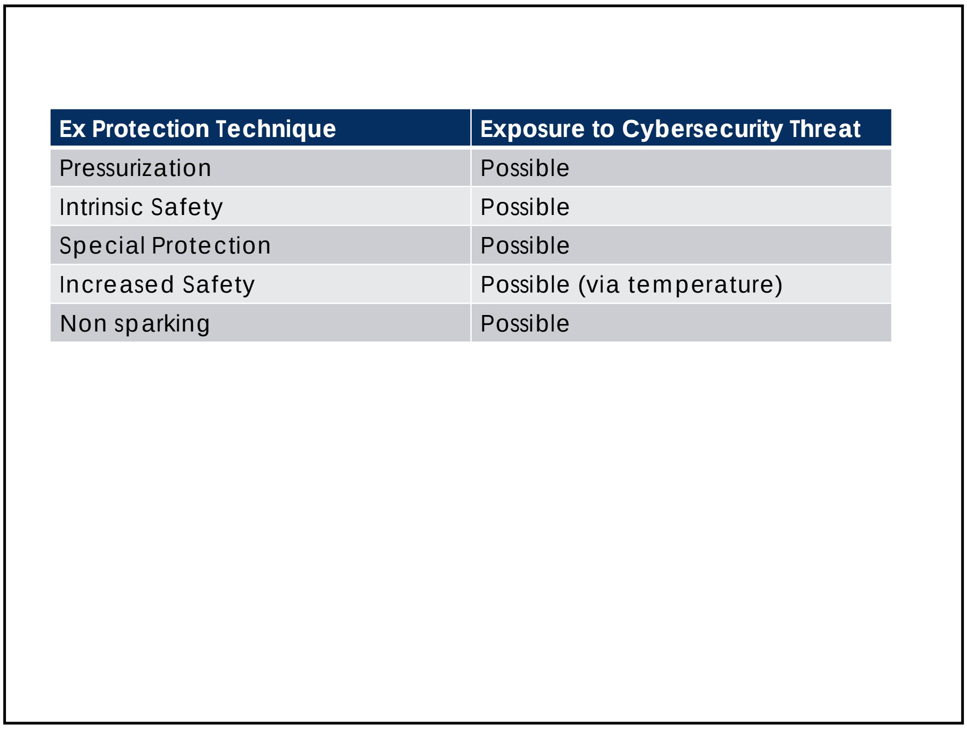
1. Assessment of Capabilities for Conformity with IEC 62443-2-4
2. Assessment of Capability Application for conformity with IEC 62443-4-1
3. Assessment of conformity with IEC 62443-4-2 (for components) or IEC 62443-3-3 (for systems)



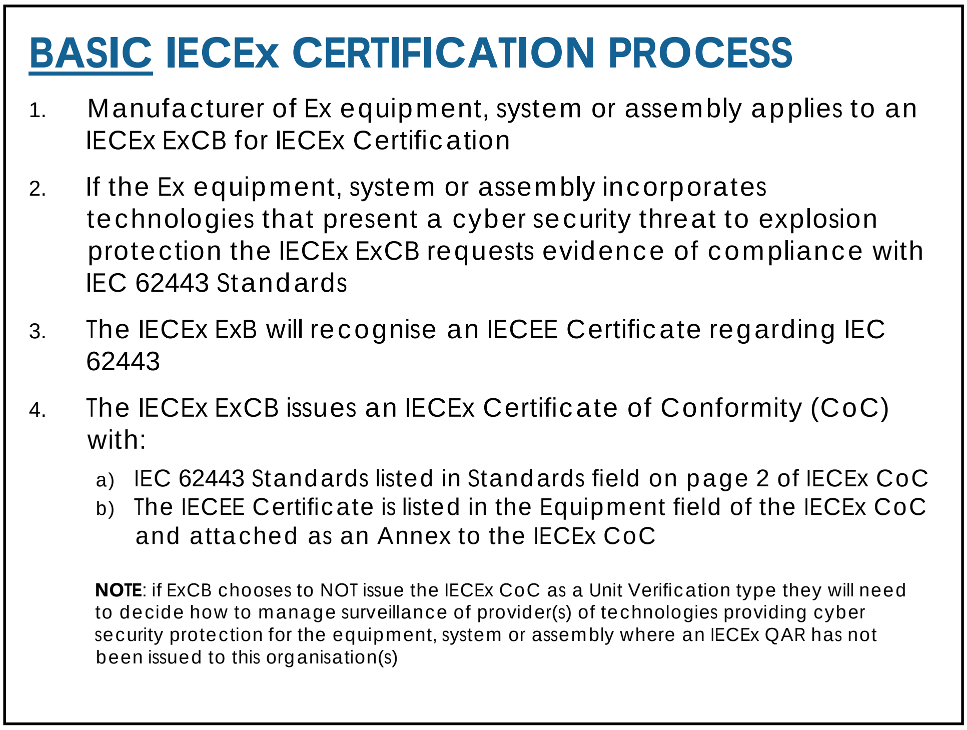
QUESTION / CONCEPT

Can / should “sector specific requirements” for IECEx Certification needs be defined in terms of “Profiles” as used in IEC 62443-2-4 for each Protection Technique where cybersecurity threat exists has a Profile ?

Hence IECEx Certification “sector specific requirements” in terms of cybersecurity could be defined by the Profiles related to protection technique(s) employed in the product or system



Ex Protection Technique	Exposure to Cybersecurity Threat
Pressurization	Possible
Intrinsic Safety	Possible
Special Protection	Possible
Increased Safety	Possible (via temperature)
Non sparking	Possible



BASIC IECEx CERTIFICATION PROCESS

1. Manufacturer of Ex equipment, system or assembly applies to an IECEx ExCB for IECEx Certification
2. If the Ex equipment, system or assembly incorporates technologies that present a cyber security threat to explosion protection the IECEx ExCB requests evidence of compliance with IEC 62443 Standards
3. The IECEx ExB will recognise an IECEE Certificate regarding IEC 62443
4. The IECEx ExCB issues an IECEx Certificate of Conformity (CoC) with:
   a) IEC 62443 Standards listed in Standards field on page 2 of IECEx CoC
   b) The IECEE Certificate is listed in the Equipment field of the IECEx CoC and attached as an Annex to the IECEx CoC

NOTE: if ExCB chooses to NOT issue the IECEx CoC as a Unit Verification type they will need to decide how to manage surveillance of provider(s) of technologies providing cyber security protection for the equipment, system or assembly where an IECEx QAR has not been issued to this organisation(s)