



IEC 62443 Cybersecurity Certification Explained: Requirements, Process, and Benefits



Agenda:

1. IEC 62443 Standards
2. IEC 62443 Certification

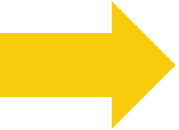
Certification Types

Assessment Steps

3. Next steps toward starting certification



Agenda:

A yellow arrow pointing to the right, highlighting the first item in the agenda.

1. IEC 62443 Standards

2. IEC 62443 Certification

Certification Types

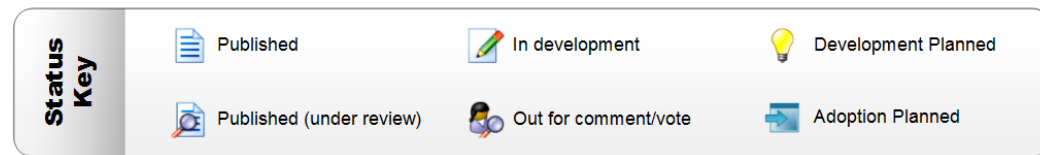
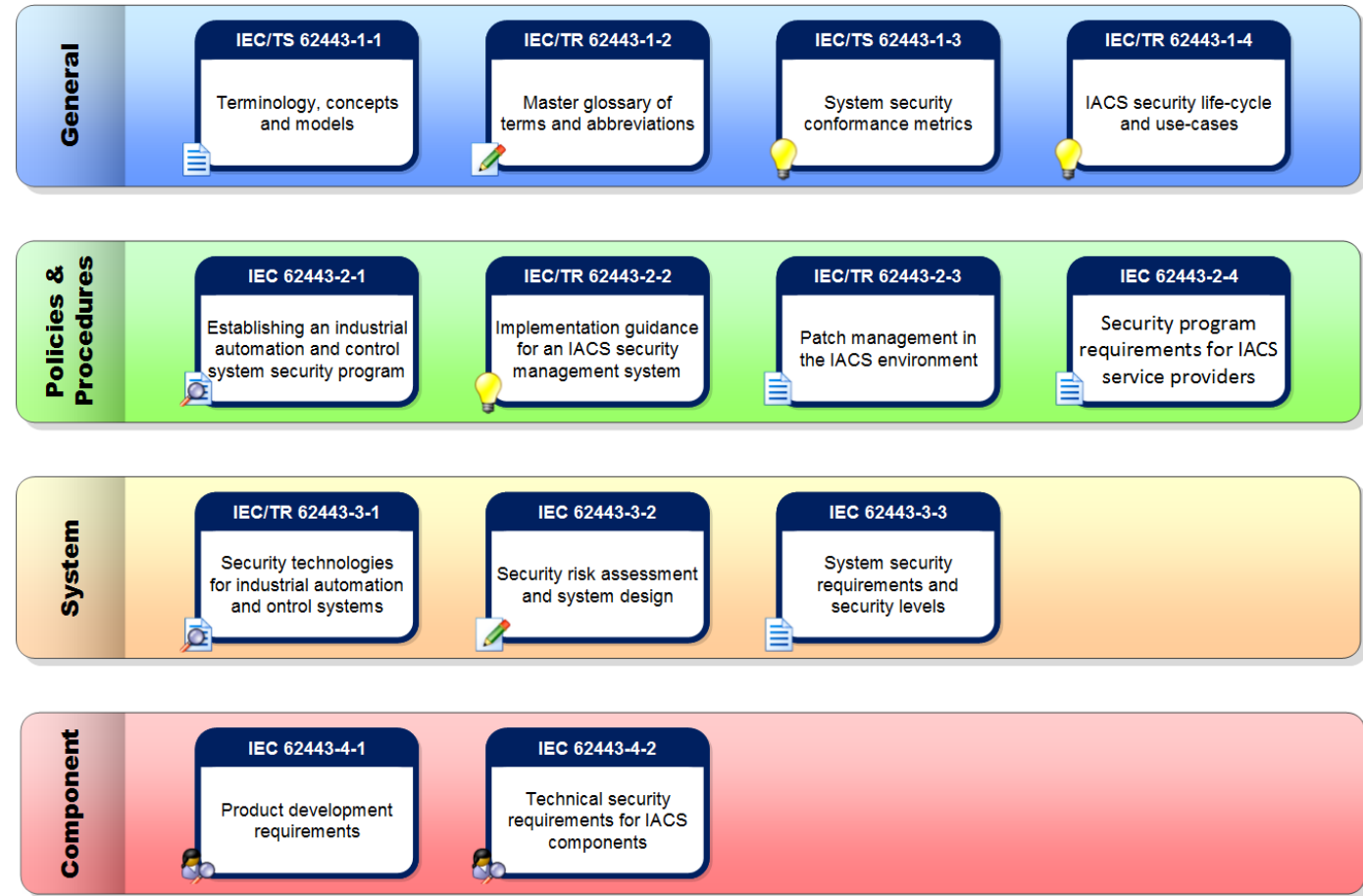
Assessment Steps

3. Next steps toward starting certification

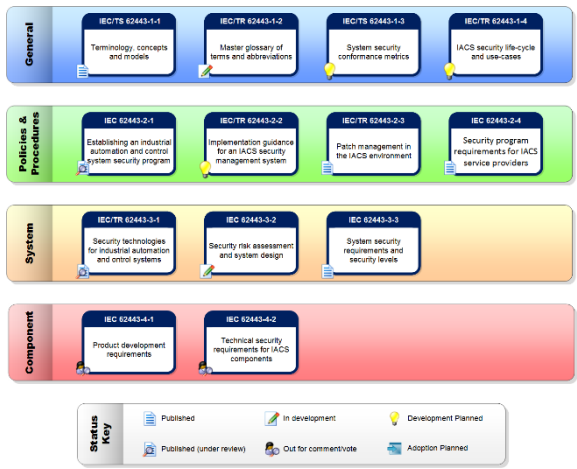


ISA/IEC 62443 Standards

- Focused on Operational Technology (OT) rather than Information Technology (IT).
- Applicable to many industries – process control, building automation, robotic automation, transportation, etc.



ISA/IEC 62443 KEY Certification Standards



IEC Standard	Overview	OEM	Systems Integrator
IEC 62443-2-4	System integrator - Policies and process		
IEC 62443-4-1	Vendor - Secure development lifecycle		
IEC 62443-4-2	Vendor – Component specification		
IEC 62443-3-3	Vendor/Integrator – System specification		

ISA/IEC 62443 Security Levels

Security Level	Skills	Motivation	Means	Resources
SL1 - Staff	No Attack Skills	Mistakes	Non-intentional	Individual
SL2 – Low Level Hacker	Generic	Low	Simple	Low (Isolated Individuals)
SL3 – Hacker, Terrorist	ICS Specific	Moderate	Sophisticated (attack)	Moderate (Hacker Groups)
SL4 Nation State	ICS Specific	High	Sophisticated (campaign)	Extended (Multi-disciplinary Teams)

Agenda:

1. IEC 62443 Standards
2. IEC 62443 Certification

Certification Types
Assessment Steps

3. Next steps toward starting certification



What is IEC 62443 Certification?

- Third party technical expert attestation of compliance against IEC 62443 requirements from three categories:
 - Detailed Analysis of engineering processes to determine Systematic Capability and Cybersecurity Strength
 - Detailed Analysis of product design and validation testing to show cybersecurity protection mechanisms in the product.
 - Network Testing to show safe, correct operation and Cybersecurity Susceptibility



Benefits of IEC 62443 Cybersecurity Certification

Structured, auditable, repeatable approach to evaluating the security of an IACS product and the development practices of the manufacturer/integrator against an established benchmark.

End-user

- Easy to specify security needs – security level
- Build security requirement into RFP
- Reduced time in FAT/SAT
- Know security level out of the box
- Better cybersecurity strength
- Provides confidence from independent expert technical assessment

Supplier

- Evaluated once
- Recognition for effort
- Build in security
- Product differentiator
- Reduce support costs
- Enhance credibility
- Break the pen/patch cycle

Who does IACS cybersecurity certification?

Most of the market requires an accredited Certification Body. To maximize the OEM market impact, a Certification Body needs to have:

- **Deep technical understanding of the standards and why each requirement is there.**
- **Cybersecurity Certification Experience**
- **Cybersecurity Accreditation**

What is this Accreditation?

- ◆ An **Accreditation Body (AB)** will audit and accredit a **Certification Body (CB)**.
- ◆ Certification Bodies must operate any product certification program under ISO/IEC 17065 requirements and have an accredited test lab per ISO/IEC 17025

CERTIFICATE OF ACCREDITATION
ANSI-ASQ National Accreditation Board/AClass
500 Montgomery Street, Suite 625, Alexandria, VA 22314, 877-344-3044

This is to certify that
exida.com, LLC
64 N. Main Street
Sellersville, PA 18960

has been assessed by ACLASS
and meets the requirements of international stan
ISO/IEC 17025:2005
while demonstrating technical competence in the fi
TESTING

Refer to the accompanying Scope(s) of Accreditation for infor
types of tests to which this accreditation appli

AT-1531
Certificate Number
Karl Buehner
AClass Approval

Certificate Valid: 03/24/2011-03/24/2013
Version No. 001 Issued: 03/24/2011

This laboratory is accredited in accordance with the recognized International Standard 1
accreditation demonstrates technical competence for a defined scope and the operati
management system (refer to joint ISO/IEC 17025:2005/ILAC-MRA Communication dated Ja

CERTIFICATE of ACCREDITATION
PRODUCT CERTIFICATION

The American National Standards Institute hereby affirms that
exida.com L.L.C.
80 North Main Street, Sellersville, PA 18960, United States

ACCREDITATION ID# 1104
meets the ANSI accreditation program requirements and those set forth in
ISO/IEC 17065:2012 Conformity assessment – Requirements for Bodies certifying products, processes and service

LIST OF CERTIFICATION SCHEME(S)
ISA SSA (System Security Assurance)
ISA SDLA (Security Development Lifecycle Assurance)
ISA Secure EDSA

IEC 61508- Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
IEC 61511 Functional safety - Safety instrumented systems for the process industry sector
IEC 62061 Industrial networks - Wireless communication network and communication profiles
ISO 28262 Road Vehicles Functional Safety Package
ISO 13849 Safety of Machinery Package
EN 50128/EN 50129 Railway applications. Communication, signaling and processing systems
ESCP - IEC 62443-4-1, 62443-4-2 & 62443-2-4 (INDUSTRIAL NETWORK AND SYSTEM SECURITY)
ESTS exida Security Test Scheme (IEC 62443-4-1, Section 9)

for programs within the following
SCOPE OF ACCREDITATION
(please see page 2)
Sam Finkbecker
ANSI VICE PRESIDENT, ACCREDITATION SERVICES

ANSI ACCREDITED

2019-12-01
VALID THROUGH



ISA Secure International Recognition

exida is fully accredited per ANSI, the United States IEC liaison, as a Certification Body for Cybersecurity and Functional Safety

ANSI is a member of the International Accreditation Forum (IAF). Most countries of the world are signatories of the IAF Multilateral Recognition Arrangement (MLA) which assures global certificate acceptance.



CERTIFICATE of ACCREDITATION

PRODUCT CERTIFICATION

The American National Standards Institute hereby affirms that

exida.com L.L.C.

80 North Main Street, Sellersville, PA 18960, United States

ACCREDITATION ID# 1104

meets the ANSI accreditation program requirements and those set forth in ISO/IEC 17065:2012 Conformity assessment – Requirements for Bodies certifying products, processes and service

LIST OF CERTIFICATION SCHEME(S)

- ISA SSA (System Security Assurance)
- ISA SDLA (Security Development Lifecycle Assurance)
- ISA Secure EDSA
- IEC 61508- Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- IEC 61511 Functional safety - Safety instrumented systems for the process industry sector
- IEC 62061 Industrial networks - Wireless communication network and communication profiles
- ISO 26262 Road Vehicles Functional Safety Package
- ISO 13849 Safety of Machinery Package
- EN 50128/EN 50129 Railway applications. Communication, signaling and processing systems
- ESCP - IEC 62443-4-1, 62443-4-2 & 62443-2-4 (INDUSTRIAL NETWORK AND SYSTEM SECURITY)
- ESTS exida Security Test Scheme (IEC 62443-4-1, Section 9)

for programs within the following

SCOPE OF ACCREDITATION

(please see page 2)

ANSI VICE PRESIDENT, ACCREDITATION SERVICES

2019-12-01
VALID THROUGH



Accreditation Confirmation

- ◆ A Certification Body will show the Accreditation Body (AB) logo on the certificate for all work done under the accredited procedures.

ABB 1709205 HPC800
IEC62443 Cert Report V1R3
(or later)

Validity:
This Certificate is restricted to the specified version of the referenced Device (including the model number, hardware / firmware / software version) set forth in the certification report. Furthermore, the unit shall be operated in a network and operational environment meeting the assumptions in the certification report.




ANSI Accredited Program
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Model Number: HPC800 Controller
System Software Version: HC800 rev B_1 & CP8

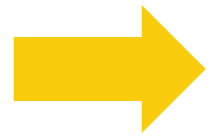


David A. Johnson
Evaluating Assessor

Michael M. Nelson
Certifying Assessor

Agenda:

1. IEC 62443 Standards
2. IEC 62443 Certification



Certification Types
Assessment Steps

3. Next steps toward starting certification



Cybersecurity Certification Categories

IEC 62443 cybersecurity certification programs in three categories:

- **Process Certification**

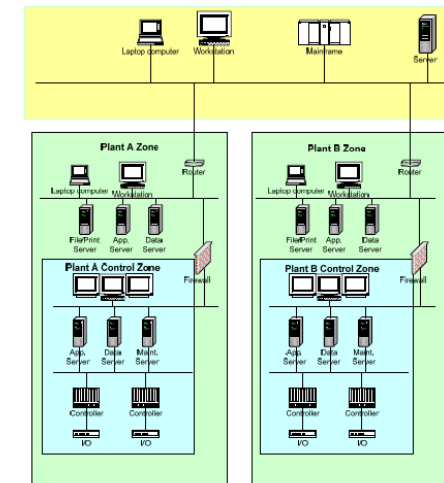
Assessment of the engineering and test process used to design and integrate devices and networks

- **Device Certification**

Assessment focused on a device, e.g. a PLC, Safety PLC, a Gateway, a Firewall, or DCS controller

- **System Certification**

Assessment of a system including multiple devices and networks



IEC 62443 Cybersecurity Certification Types

1. Security Development Lifecycle Assurance (SDLA)

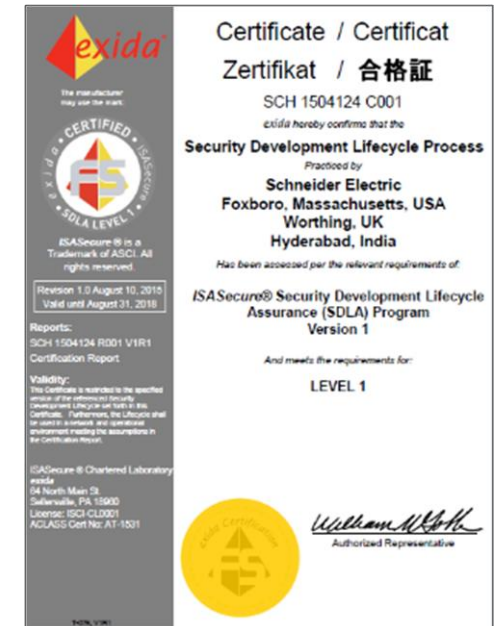
1. IEC-62443-4-1 Process

2. Embedded Device Security Assurance (EDSA)

1. IEC 62443-4-2 Security Capability
2. IEC 62443-4-1 Process
3. Network Testing

3. System Security Assurance (SSA)

1. IEC-62443-3-3
2. IEC 62443-4-1
3. Network Testing



Agenda:

1. IEC 62443 Standards
2. IEC 62443 Certification

Certification Types

Assessment Steps

3. Next steps toward starting certification



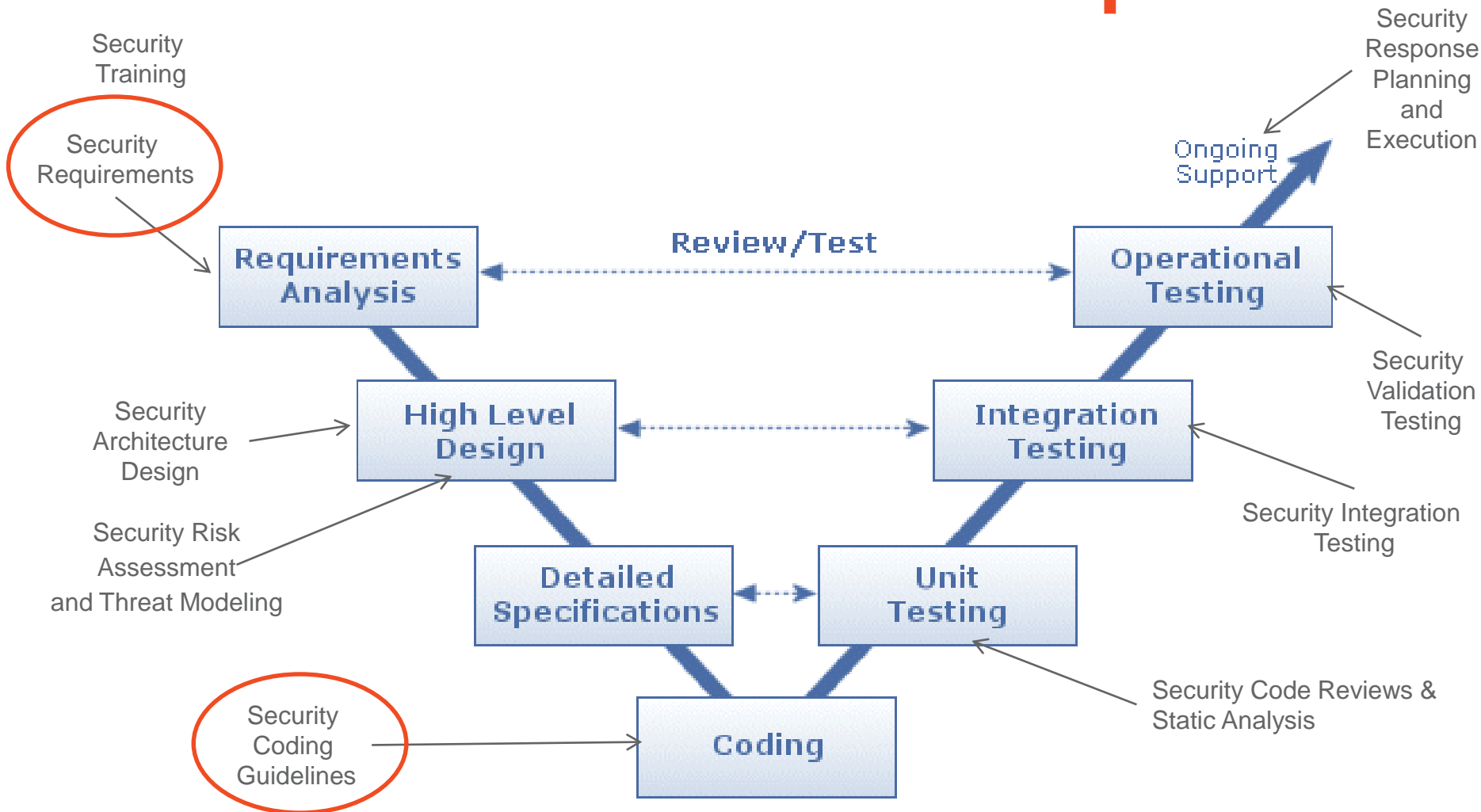
Cybersecurity Certification Process

Any Cybersecurity Certification Scheme uses one or more of the following three process steps:

1. Audit the development process used to create the product
2. Perform cybersecurity network stress testing to find network vulnerabilities – focus on most effective tests
3. Analyze and test cybersecurity features of the product to determine if they are sufficient.

Security Level equates a minimum set of security features/capability as well as assurances for secure development process and security testing

1. Audit the Development Process



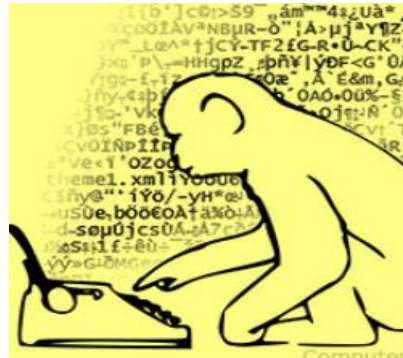
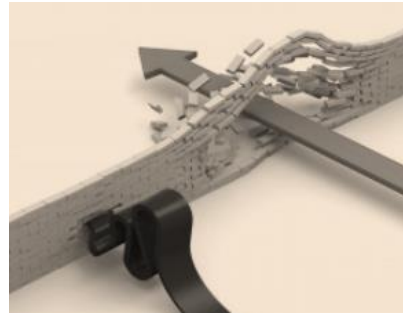
Certificate / Certificat
Zertifikat / 合格証
SCH 1504124 C002
exida hereby confirms that the
Security Development Lifecycle Process
Practiced by
Schneider Electric
Foxboro, Massachusetts, USA
Worthing, UK
Hyderabad, India
Has been assessed per the relevant requirements of:
IEC 62443-4-1 Security for Industrial Automation and Control Systems
Version DC
And meets the requirements for:
LEVEL 1



Cybersecurity
Process
Certification

2. Perform Network Stress Testing

- Fuzz Testing
- Penetration Testing
- Malformed Packet Testing
- Storm Testing
- ...



IP Fragmented Storm (L1/L2)
IP Fragmented Storm (L1/L2)
IP Bad Checksum Storm (L2)
IP Grammar - Header Fields (L2)
IP Grammar - Fragmentation (L2)
IP Grammar - Options Fields (L2)
ICMP Storm (L1/L2)
ICMP Storm (L1/L2)
ICMP Grammar (L2)
ICMP Type/Code Cross Product (L1/L2)
TCP SYN Storm (L1/L2)
TCP SYN Storm from Broadcast (L2)
TCP SYN Storm from Broadcast (L2)
TCP/IP LAND Storm (L1/L2)
TCP/IP LAND Storm (L1/L2)
TCP URG Storm (L2)
TCP FIN Storm (L2)
TCP RST Storm (L2)
TCP Closed Receive Window Storm (L2)
TCP Segment Reassembly Storm (L2)
TCP Grammar - Header Fuzzer (L2)
TCP Grammar - Contextually Invalid Packets (L2)
TCP Priority Traffic Interleaving (L2)
TCP Timestamp Manipulation (L2)
TCP/IP Grammar (L2)
TCP Selective Acknowledgement (L2)
TCP Receive Window (L2)
TCP Data Grammar (L2)
TCP Maximum Concurrent Connections (L2)
TCP Initial Sequence Number Randomness Check (L2)
UDP Unicast Storm (L1/L2)
UDP Unicast Storm (L1/L2)
UDP Multicast Storm (L1/L2)
UDP Multicast Storm (L1/L2)
UDP Broadcast Storm (L1/L2)
UDP Broadcast Storm (L1/L2)
UDP Broadcast Storm (L1/L2)
UDP Broadcast Storm (L1/L2)
UDP Grammar (L2)
UDP Data Grammar (L2)
Ethernet Unicast Storm (L1/L2)
Ethernet Multicast Storm (L1/L2)
Ethernet Broadcast Storm (L1/L2)
ARP Request Storm (L1/L2)
ARP Host Reply Storm (L1/L2)
ARP Cache Saturation Storm (L1/L2)
IP Unicast Storm (L1/L2)

3. Analyze and Test Cybersecurity Features

Foundational Requirement	SL-1	SL-2	SL-3	SL-4
FR 1 – Identification and Authentication Control	10	16	22	24
FR-2 Use Control	8	12	21	24
FR-3 System Integrity	5	10	16	19
FR-4 Data Confidentiality	2	4	5	6
FR-5 Restricted Data Flow	4	6	10	11
FR-6 Timely Response To Events	1	2	3	3
FR-7 Resource Availability	7	10	13	13

Example: A product meets all SL-1 requirements, and perhaps some SL-2 or SL-3. That certification will show SL-1.

Cybersecurity levels are defined with stronger requirements needed as the level goes from 1 to 4.



Certificate / Certificat
Zertifikat / 合格証

ABB 1709205 C001

exida hereby confirms that the

HPC800 Controller

Manufactured by

**ABB
Wickliffe, Ohio
USA**

Has been assessed per the relevant requirements of:

IEC 62443 Part 4-1

IEC 62443 Part 4-2

**exida Security Device Certification (eSDC)
Program**

And meets the requirements for:

CAPABILITY SECURITY LEVEL 1

Model Number: HPC800 Controller

System Software Version: HC800 rev B_1 & CP800 rev A_7



ANSI Accredited Program
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004



David A. Zahar
Evaluating Assessor

Michael M. Dehoff
Certifying Assessor

Agenda:

1. IEC 62443 Standards
2. IEC 62443 Certification

Certification Types

Assessment Steps

- 
- A large yellow arrow pointing to the right, highlighting the third item in the agenda.
3. Next steps toward starting certification



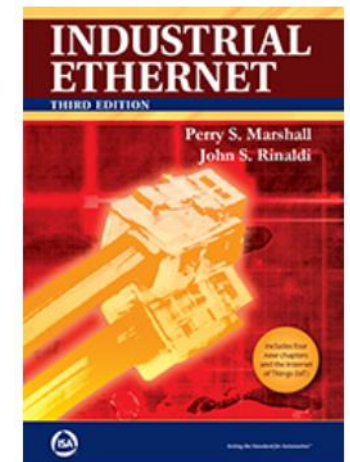
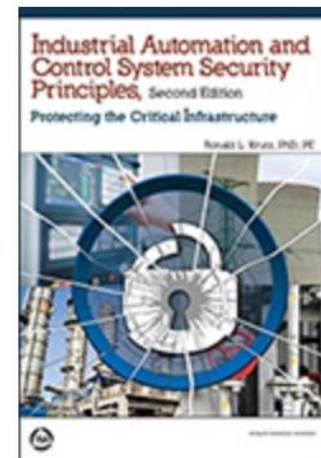
Next Steps:

- Training
- Choose a CB
- Contact CB – e.g. www.exida.com
- Schedule “Gap Analysis”/Informal Audit
- Proceed with certification



References:

- www.isa.org
- www.isasecure.org
- www.exida.com
- Webinars
- Books



Conclusions:

- ISA/IEC 62443 is a set of standards documents applicable to automation systems in many industries.
- Cybersecurity Certifications require an organization with strong technical credentials, experience, and accreditation.
- Cybersecurity Certifications provide strong benefits for both end users and OEMs.

Questions??