ISA/IEC 62443-4-1 Audit and Certification Process Overview

LIVE WEBINAR
2021-04-28

TÜVRheinland®
Precisely Right.

Agenda

- General overview of the multi-standard IEC 62443
- General overview of audit and certification process
- Introduction ISASecure® ISA/IEC 62443-4-1 SDLA program
- Overview of ISASecure® ISA/IEC 62443 SDLA requirements
- Q&A Session

Your Speakers

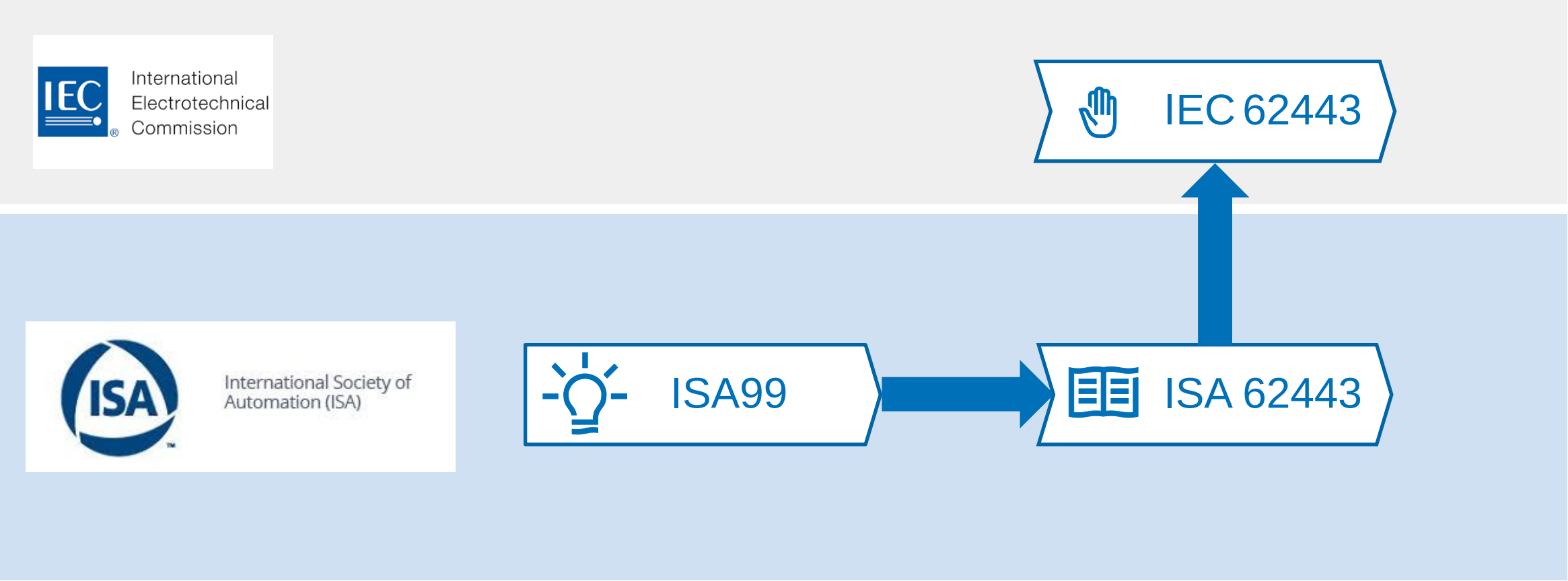
Sergei Biberdorf
TÜV Rheinland Industrial Service

Zakarya Drias
Schneider Electric

General overview of the multi-standard IEC 62443

Part 1/3

ISA/IEC 62443 International Standard



TÜVRheinland®
Precisely Right.

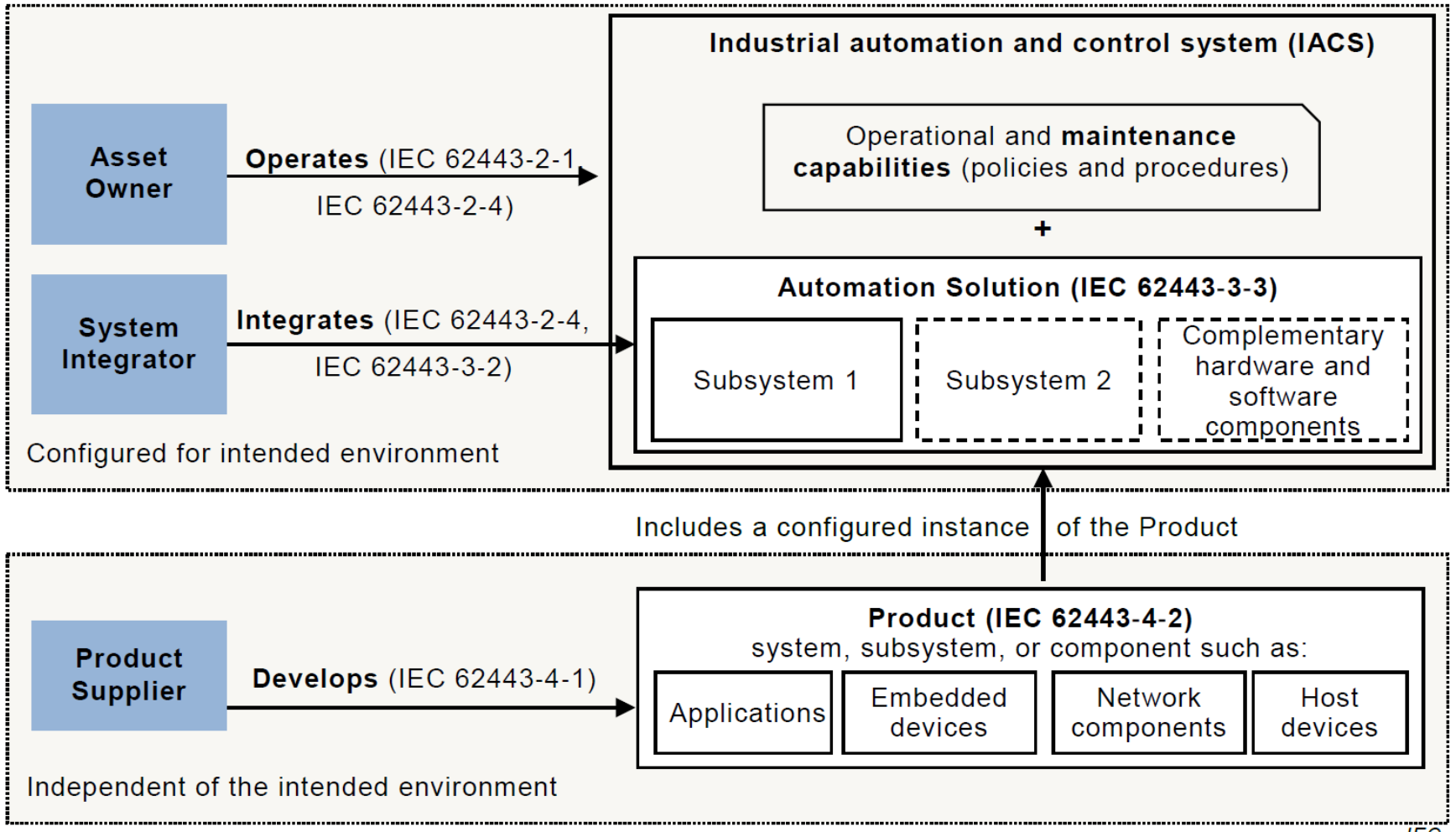
General overview of the multi-standard IEC 62443

Part 2/3

General Definitions Metrics	**Operator** Requirements on processes of the plant owner	**System Integrator** Requirements to achieve a secure system	**Product Supplier** **Requirements** to secure system components
IEC 62443-1-1 Terminology, concepts and models	**IEC 62443-2-1** Requirements for an IACS security management system	**IEC 62443-3-1** Security technologies for IACS	**IEC 62443-4-1** **Product development requirements**
IEC 62443-1-2 Master glossary of terms and abbreviations	**IEC 62443-2-2** Implementation guidance for an IACS security management system	**IEC 62443-3-2** Security risk assessment and system design	**IEC 62443-4-2** **Technical security requirements for IACS products**
IEC 62443-1-3 System security compliance metrics	**IEC 62443-2-3** Patch management in the IACS environment	**IEC 62443-3-3** System security requirements and security levels	
IEC 62443-1-4 IACS security lifecycle und use-case	**IEC 62443-2-4** Requirements for IACS solution suppliers		

General overview of the multi-standard IEC 62443

Part 3/3



*Source of the picture: IEC 62443-4-1:2018

TÜVRheinland®
Precisely Right.

General overview of audit and certification process

TÜV Rheinland Services for the Certification of Management Processes

CSM – Cyber Security Management

- ISA/IEC 62443
- ISASecure® SDLA

DAkkS

ISASecure®

FSM – Functional Safety Management

- IEC 61508
- IEC 61511

DAkkS

AFSM – Automotive Functional Safety Management

- ISO 26262

DAkkS

NSM - Nuclear Safety Management

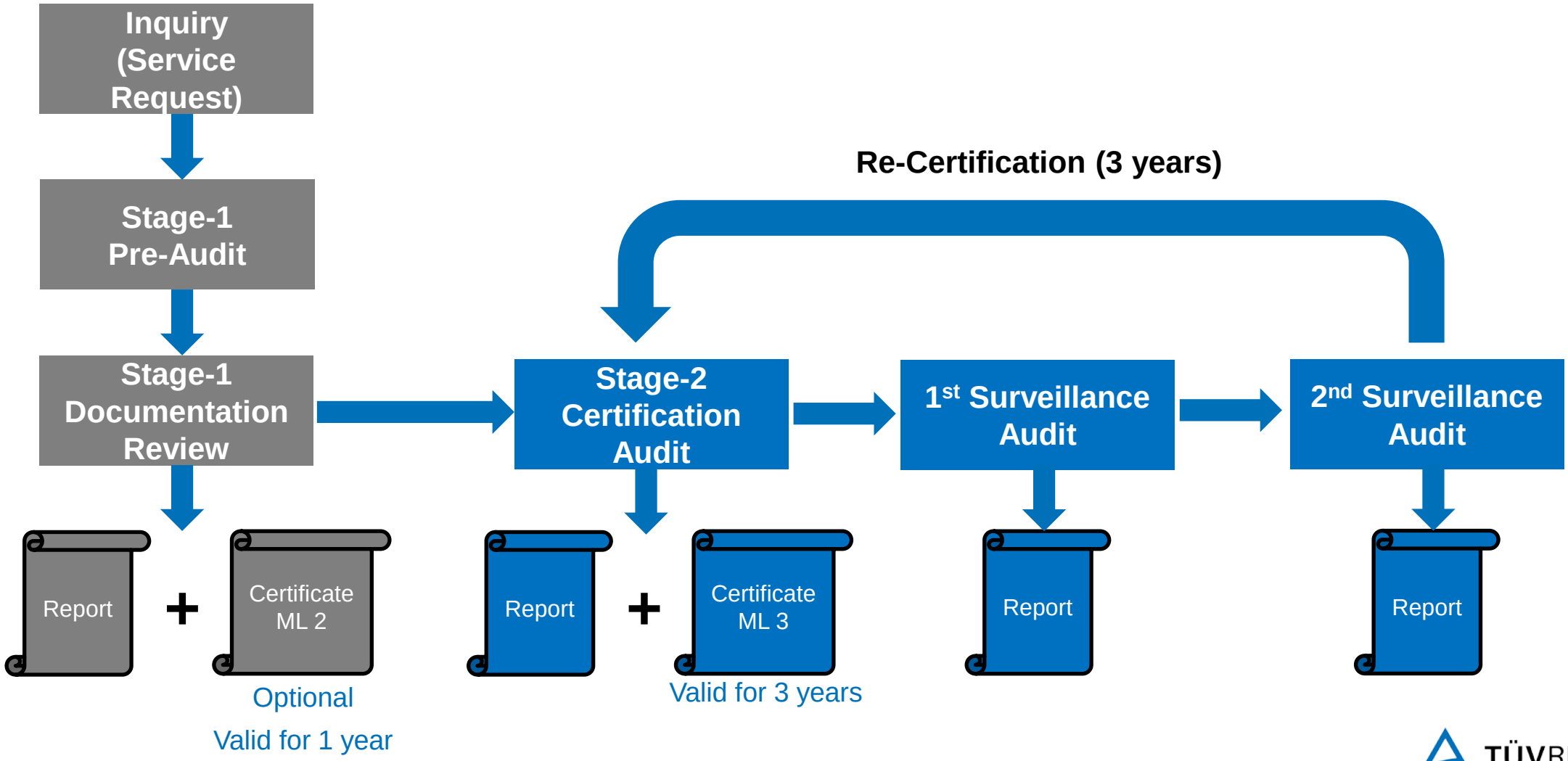
- IEC 61513

DAkkS

TÜV Rheinland organization and procedures of certification program are based on ISO/IEC 17021

General overview of audit and certification process

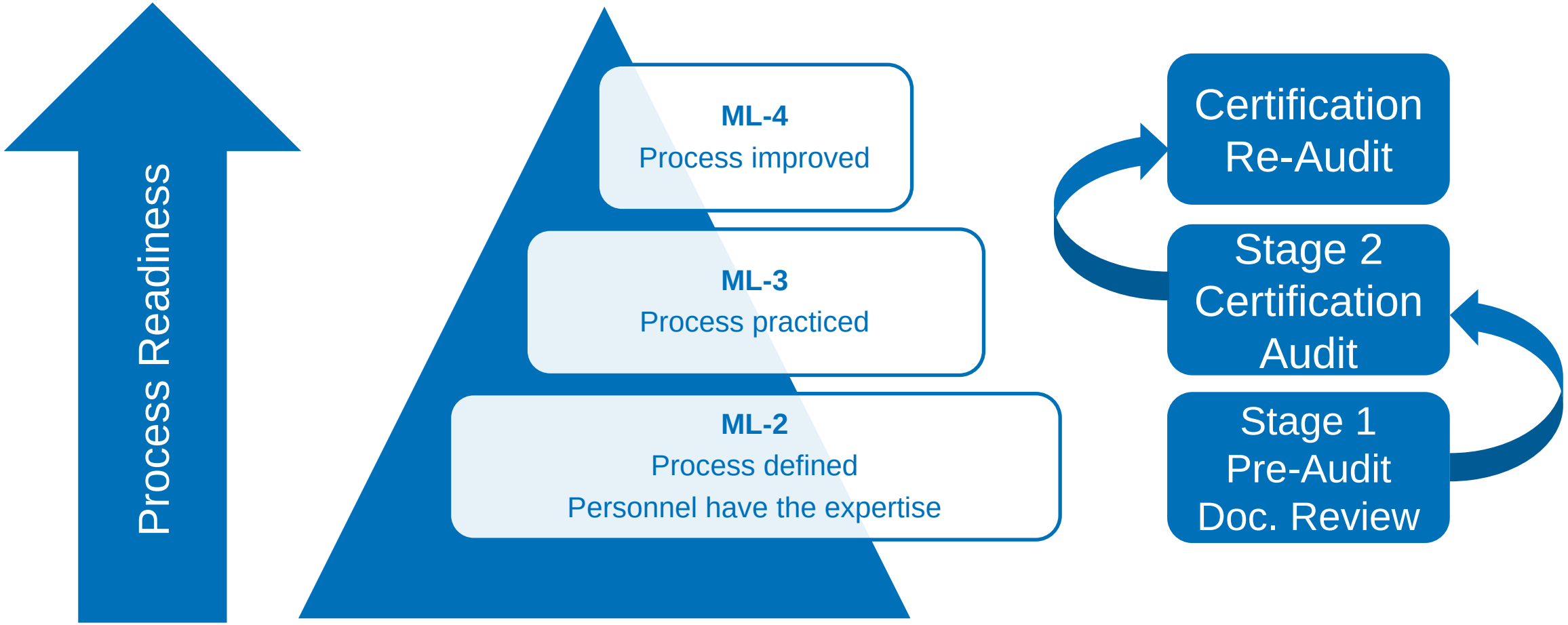
Audit and Certification Procedure (based on ISO/IEC 17021)



TÜVRheinland®
Precisely Right.

General overview of audit and certification process

Maturity Level (according to IEC 62443)



TÜVRheinland®
Precisely Right.

General overview of audit and certification process

Scope of Certificate


Certificate

Cyber Security Management

CS Management (TÜV Rheinland)
ISA 62443-4-1:2018 (Edition 1.0) - Product Supplier
CSM 109, Maturity Level 3: Defined - Practiced

Certificate No. 968/CSM 106.01/20

Certified Company & Location: Schneider Electric, Product Security Office, 5 Rue Henri Sainte-Claire Deville, 92500 Rueil-Malmaison, France

Scope of Certification: Centralized Group Certification for Product Supplier, assisted to IEC 62443-4-1:2018 (Edition 1.0) Security for Industrial Automation and Control Systems Part 4-1: Secure Product Development Lifecycle Requirements

Details and limitations regarding the Technical Scope and Local Scope of Certification of committed company locations are listed in the attached Certificate Appendix 968/CSM 106.01/20, which forms integral part of this certificate.

The certified company organization and its committed company locations as listed in attached Certificate Appendix have successfully demonstrated during an audit process that a Secure Product Development Lifecycle has been implemented and applied.

This Certification does not imply approval or certification for specific security related developments of products.

Validity: This certificate is valid until 2023-09-10

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2020-09-06

Dr.-Ing. Thorsten Gantevoort

TÜV Rheinland Industrie Service GmbH
Automation und Funktionale Sicherheit
Am Grauen Stein
51105 Cologne - Germany

www.fs-products.com
www.tuv.com

TÜVRheinland®

Local Scope:

Named Development Organization(s)

Technical Scope:

Standard considered as basis for audit

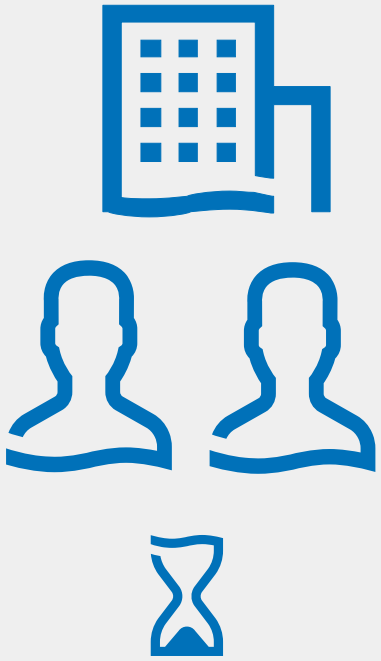
TÜVRheinland®
Precisely Right.

General overview of audit and certification process

Certification Procedure Stage 1: Pre-Audit

- Auditee’s security process is mostly pre-defined
- Evaluation of auditee’s processes to identify possible deviations or gaps
- Auditing responsible roles and their expertise
- Evaluation of the Auditee's location and site-specific conditions

Result → Open Item List with identified gaps



Auditee Location

2 Auditors

2-3 Days

General overview of audit and certification process

Certification Procedure Stage 1: Documentation Review

- Evaluation of documented version of the organization's process
- Review of all relevant process documentation:
  - organization chart
  - procedures
  - work instructions
  - templates, forms
  - further process documentation

Result → (optional) ML-2 Certficate

Offline
TÜV Location

1 Auditor

As soon as all open items are closed

General overview of audit and certification process

Certification Procedure Stage 2: Initial Certification Audit

- Review of representative artifacts to verify that each requirement has been followed for products under the scope of the process

  Pre-conditions:

  - Stage 1 audit has been completed, open items have been clarified,
  - **at least one project has been completed**

Result → ML-3 Certficate

Auditee Location

2 Auditors

2 Days

General overview of audit and certification process

Certification Procedure: Surveillance Audit (annual)

- Evaluation of process application in everyday operations of auditee
- Based on project execution
- Based on spot checks of selected topics

Auditee Location

1 Auditor

1 Days

TÜVRheinland®
Precisely Right.

General overview of audit and certification process

Certification Procedure: Re-Certification Audit (three years cycle)

- Confirm the effectiveness of the complete management processes of the auditee
- Review of process applicability and improvement measures
- Evaluation of auditee's potential to achieve ML-4 certificate

Result → ML-3/4 Certficate

Auditee Location

1-2 Auditors

1-2 Days

General overview of audit and certification process

Certificate


Certificate

Cyber Security Management

CS Management (TÜV Rheinland)
IEC 62443-4-1:2018 (Edition 1.0) - Product Supplier
CSM 106, Maturity Level 3: Defined - Practiced

Certificate No. 968/CSM 106.01/20

Certified Company & Location [redacted]
Product Security Officer
6 Rue Pierre Sainte-Claire Deville
92500 Rueil-Malmaison
France

Scope of Certification Centralized Group Certification
for Product Supplier, related to IEC 62443-4-1:2018 (Edition 1.0)
Security for Industrial Automation and Control Systems
Part 4-1: Secure Product Development Lifecycle Requirements

Details and limitations regarding the Technical Scope and Local Scope of Certification of committed company locations are listed in the attached Certificate Appendix 968/CSM 106.01/20, which forms integral part of this certificate.

The certified company organization and its committed company locations as listed in attached Certificate Appendix have successfully demonstrated during an audit process that a Secure Product Development Lifecycle has been implemented and applied.

This Certification does not imply approval or certification for specific security-related developments of products.

Validity This certificate is valid until 2022-09-16

TÜV Rheinland Industrie Service GmbH
Bereich Automotive
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2020-03-06

Dr.-Ing. Thorsten Gantevoort

TÜV Rheinland
Industrie Service GmbH
Automotive and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

www.fs-products.com
www.tuv.com

TÜVRheinland®

- Local Scope
  - Development Organization
  - Named Development Process
- Technical Scope
  - ISA/IEC 62443-4-1 (or ISA/IEC 62443-2-4)
- Expiration Date
  - ML-2: 1 year
  - ML-3: 3 years
- Puplished
  - www.certipedia.com/fs-products

Introduction ISASecure® ISA/IEC 62443-4-1 SDLA program

ISASecure® Certification Program

IEC 62443 - CSA Certification

- ***Component Security Assurance***
- Certification of
  - software applications
  - embedded devices
  - host devices
  - network devices
- Equivalent to IEC 62443-4-2

IEC 62443 -SSA Certification

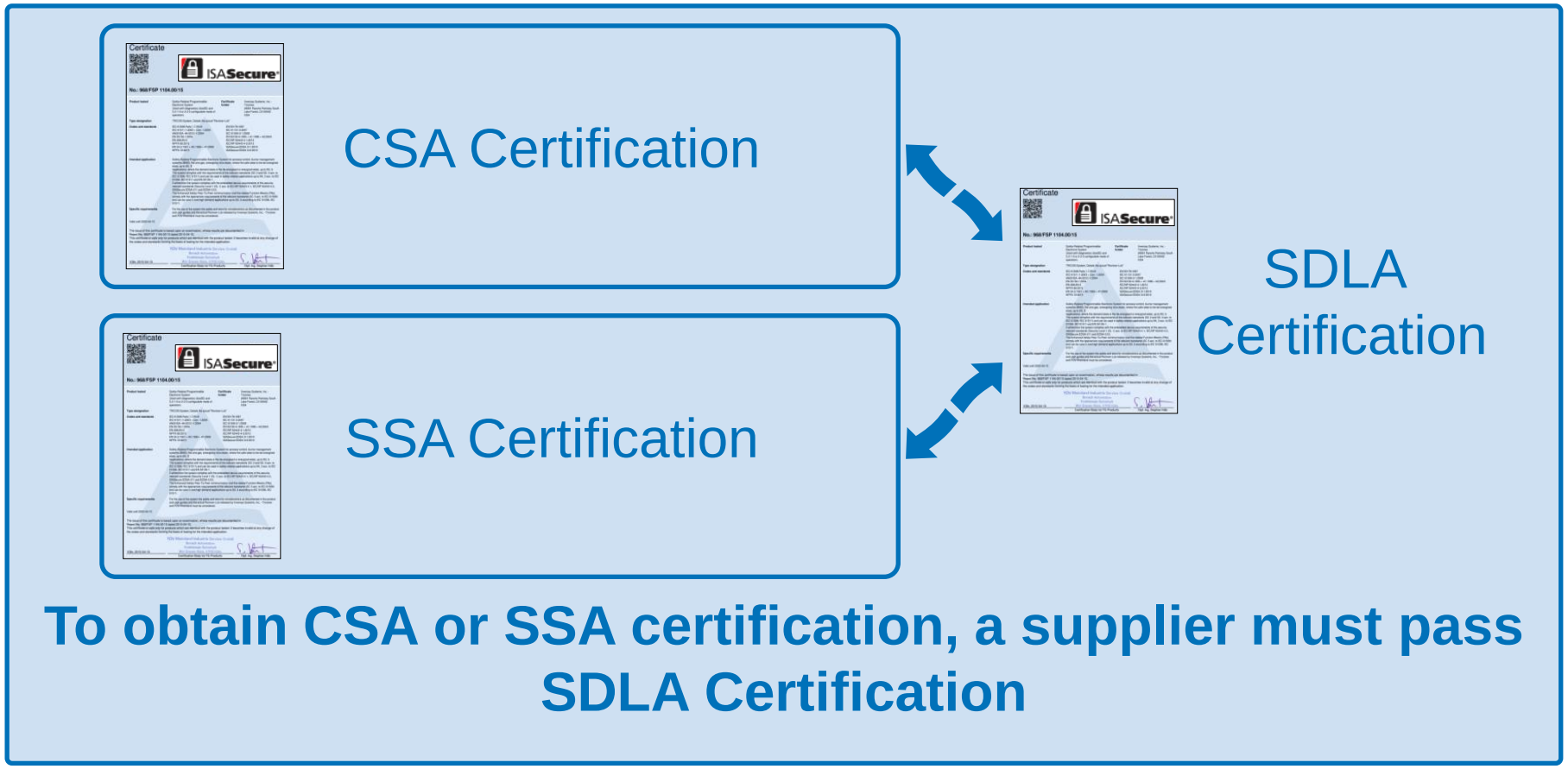
- **System Security Assurance**
- Certification of automation control systems
- Equivalent to IEC 62443-3-3

IEC 62443 - SDLA Certification

- **Security Development Lifecycle Assurance**
- Certification of development lifecycle processes of suppliers for control system and products
- Equivalent to IEC 62443-4-1

Introduction ISASecure® ISA/IEC 62443-4-1 SDLA program

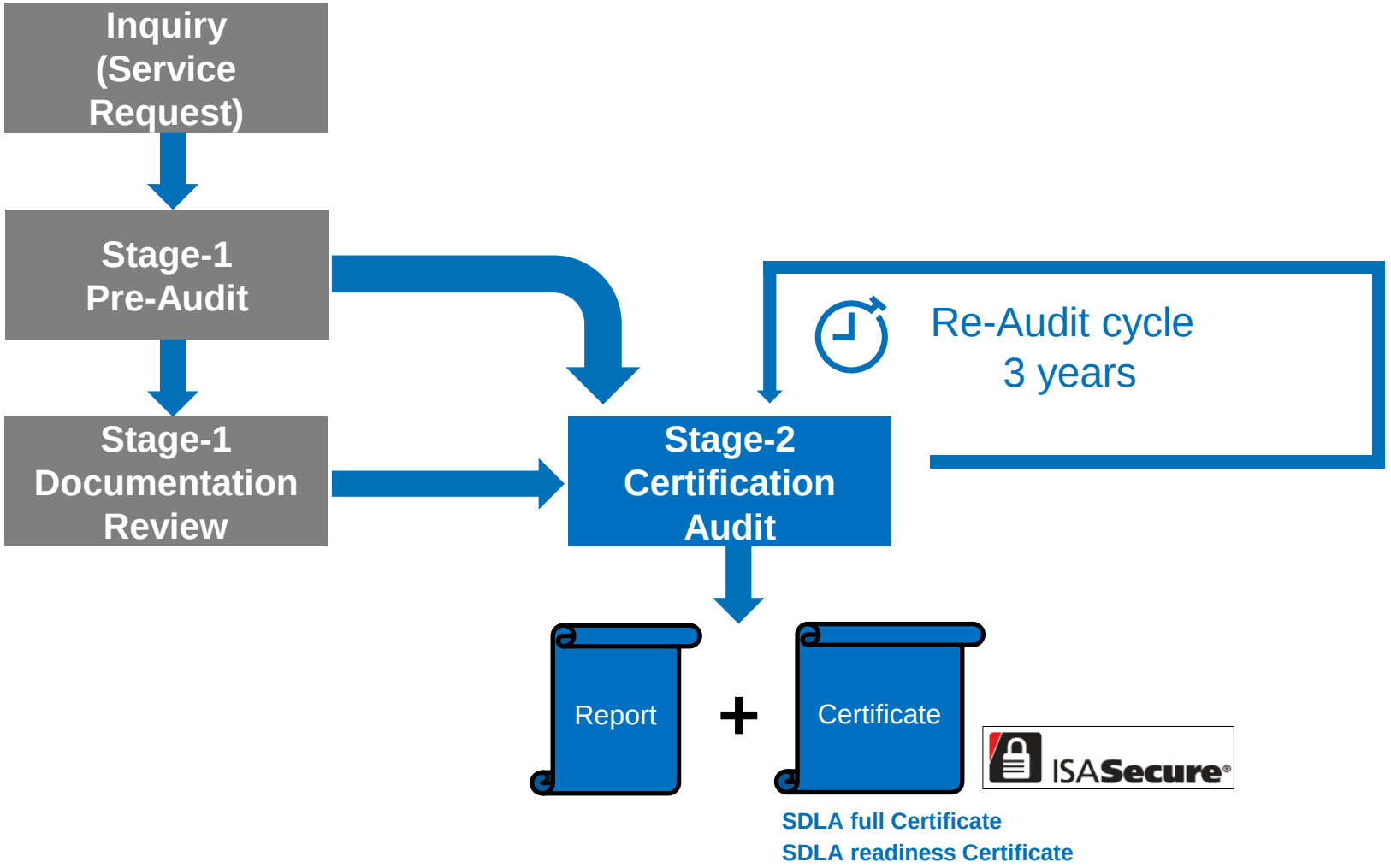
ISASecure® Certification Program



TÜVRheinland®
Precisely Right.

Introduction ISASecure® ISA/IEC 62443-4-1 SDLA program

Audit and Certification Procedure (according to ISASecure® SDLA program)



SDLA full Certificate
SDLA readiness Certificate

TÜVRheinland®
Precisely Right.

Introduction ISASecure® ISA/IEC 62443-4-1 SDLA program

ISASecure® SDLA Certificate


Certificate

ISASecure®

Certificate No. 968/CSM 106.01/20

Certified Company & Location

Scope of Certification

Centralized Group Certification
for Product Supplier, related to IEC 62443-4-1:2018 (Edition 1.0)
Security for Industrial Automation and Control Systems
Part 4-1: Secure Product Development Lifecycle Requirements

Details and limitations regarding the Technical Scope and Local Scope of Certification of committed company locations are listed in the attached Certificate Appendix 968/CSM 106.01/20, which forms integral part of this certificate.

The certified company organization and its committed company locations as listed in attached Certificate Appendix have successfully demonstrated during an audit process that a Secure Product Development Lifecycle has been implemented and applied.

This Certification does not imply approval or certification for specific security related developments of products.

Validity This certificate is valid until 2022-09-16

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2020-09-08

Dr.-Ing. Thorsten Gandevoort

TÜV Rheinland Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

www.fs-products.com
www.tuv.com

TÜVRheinland®

- Local Scope
  - Development Organization
  - Named Development Process
- Technical Scope
  - ISASecure® SDLA Program (incl. Version)
  - ANSI/ISA-62443-4-1
  - IEC 62443-4-1
- Expiration Date
  - SDLA readiness: 1 year
  - SDLA full: 3 years
- Published
  - www.ISASecure.org
  - www.certipedia.com/fs-products

TÜVRheinland®
Precisely Right.

Overview of ISASecure® ISA/IEC 62443 SDLA requirements

Part 1/2

ISASecure® SDLA Requirements (SDLA-300)

- Named development organization or organizations

- Named, documented security development lifecycle (SDL) process under version control

- Responsible roles are defined and expertise available

- Process artifacts as evidence that the organization is following SDL
  - Readiness evaluation
  - Full evaluation

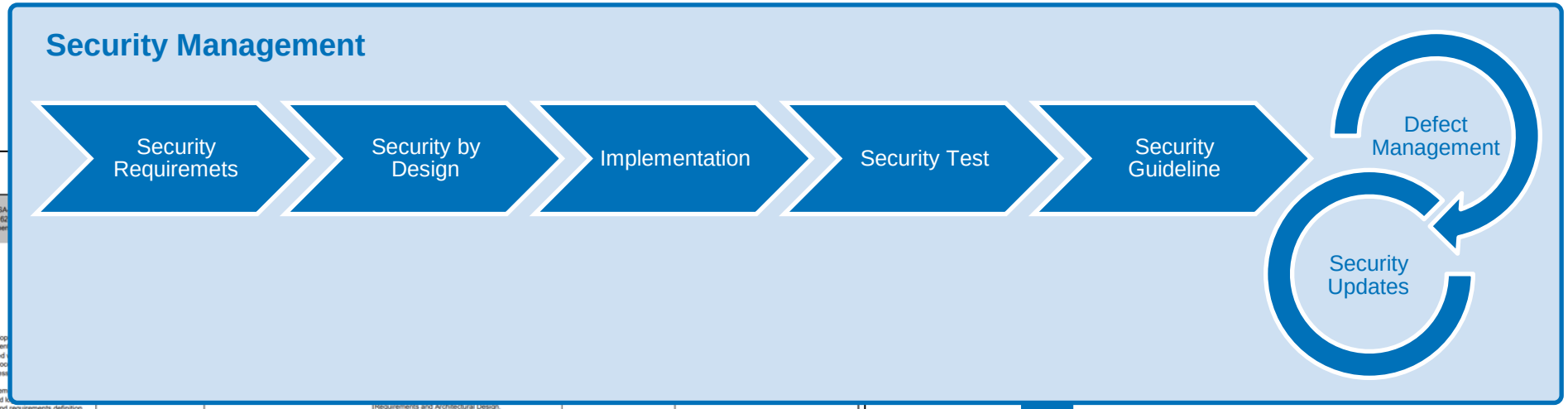
TÜVRheinland®
Precisely Right.

Overview of ISASecure® ISA/IEC 62443 SDLA requirements

Part 2/2

ISASecure® Security Development Lifecycle Assessment (SDLA-312)

Security Development Lifecycle (IEC 62443-4-1)



SDLA-312

ASCI Automation Standards Compliance Institute

System	Component	ANSI/ISA-62443-4-1 IEC 62443-4-1 Requirement Number	ANSI/ISA-62443-4-1 IEC 62443-4-1 Requirement Name	ANSI/ISA IEC 62 Requiremen					
x	x	SM-1	Development Process	A general product develop process shall be documen consistent and integrated product development proc 9001 [13] certified process limited to: a) configuration managem controls and audit record b) product description and requirements definition with requirements traceability, c) software or hardware design and implementation practices, such as modular design; d) repeatable testing verification and validation process; e) review and approval of all development process records; and f) life-cycle support.					
x	x				SDLA-SM-1C	Verify that the component or system being evaluated has a documented software and hardware (if applicable) design.	Verify that the documented development process includes software and hardware (if applicable) design practices. Verify that these practices include items that promote modular design.	SDLA-DSD-1	
x	x				SDLA-SM-1D	Verify that the verification and validation tests specified by the development process were carried out on the component or system being evaluated.	Verify that the documented process includes verification and validation tests. The validation tests should provide coverage on all of the product requirements. The verification tests should include some level of module testing and integration testing.	None	
x	x				SDLA-SM-1E	Verify that the reviews and approvals of artifacts described in the development process were done for the latest major release.	Verify that the documented process includes steps to review and approve development process artifacts such as requirements specifications, design specifications, and test plans.	None	
x	x				SDLA-SM-1F	None.	None	None	Note that lifecycle support is really covered by all of the other requirements in IEC 62443-4-1 since they cover the different phases of the lifecycle. Therefore, there are no additional requirements for this item.
x	x	SM-2	Identification of Responsibilities	A process shall be employed that identifies the organizational roles and personnel responsible for each of the processes required by this standard.	SDLA-SM-2	Verify that all security related activities and that those responsible for carrying out the activities are listed in the project documentation.	Verify the documented standard development lifecycle requires that all security related activities and those responsible for carrying out the activities are documented.	SDLA-SMP-1.1	
x	x	SM-3	Identification of applicability	A process shall be employed for identifying products (or parts of products) to which this standard applies.	SDLA-SM-3	Verify that the system or product under evaluation is one where it has been determined and documented that the security development lifecycle applies to the entire product (not just a part).	Verify that a documented process for identifying which products (or parts or products) the security development lifecycle exists. Do some sample auditing to confirm that the process is being used on the products identified by this process. At least 3 products should be reviewed in the sample auditing, unless there are not that many products identified by this process. In that case all products identified by this process should be reviewed.	None	
x	x	SM-4	Security expertise	A process shall be employed for identifying and providing security training and assessment programs to ensure that personnel assigned to the organizational roles and duties specified in 5.3, SM-2 – Identification of responsibilities, have demonstrated security expertise appropriate for those processes.	SDLA-SM-4	Verify that there is evidence of the competence of all people assigned processes defined in SDLA-SM-2 for the component or system being evaluated. This evidence can take the form of experience and qualifications, performance reviews, tests, or other assessments. Verify that everyone involved in software development has received the appropriate training and that this training and associated testing / demonstration of baseline competency has been documented.	Verify that company has a documented procedure to assess that personnel assigned to processes defined in SDLA-SM-2 have demonstrated security expertise appropriate for those processes. Verify that the documented development process states that for each defined role a list of required security training must be created and tracking who attends that training must be done. Verify that the required security training has been identified and that at least some developers have been trained.	SDLA-SMP-1.4, SDLA-SMP-1.5	Engineers must understand what it takes to build and deliver secure features; not how to develop security features. These skills are currently not taught in most colleges and universities and on average most software engineers know very little about software security.

TÜVRheinland®
Precisely Right.

SDLA Certification

Choose your Certification Schema

In PA, we have chosen ISCI Certification Schema. The Schema is aligned with the IEC62443-4-1 maturity levels

Implement Certification requirement

- Make sure your SDL covers all the requirements

Select your certification version (2.0/2.1)

- Sec Management
- Security Requirements
- Secure by design
- Secure Implement
- Security V&V testing
- Security defect Mgt
- Security Update Mgt
- Security Guidelines

12 weeks with 1 person full time

Select a Project to drive your certification

The certification requires artifacts from projects following the Dev process and applying SDL. The project could be an old project as soon as you are able to show artifacts for the requirements.

2 weeks in the case of PA

Contact your Certifier

TUV and Exida are the certifiers for ISASecure. Select a certifier who knows your development process.
Get a Quote from the certifier and schedule preparation sessions (Remote).

Organize Site Assessment

Before organizing your site assessment.
Prepare all the artifacts and anticipate questions.
If first time certification, the assessment might take a week to go through the process and validate the Artifacts

4 weeks in the case of PA including the site assessment

We hope this presentation was informative and helpful
Happy to take Questions!

Thank you for joining our webinar

Sergei Biberdorf:
E-mail: sergei.biberdorf@de.tuv.com

Zakarya DRIAS
E-mail: zakarya.drias@se.com

Life Is On Schneider Electric

TÜVRheinland®
Precisely Right.