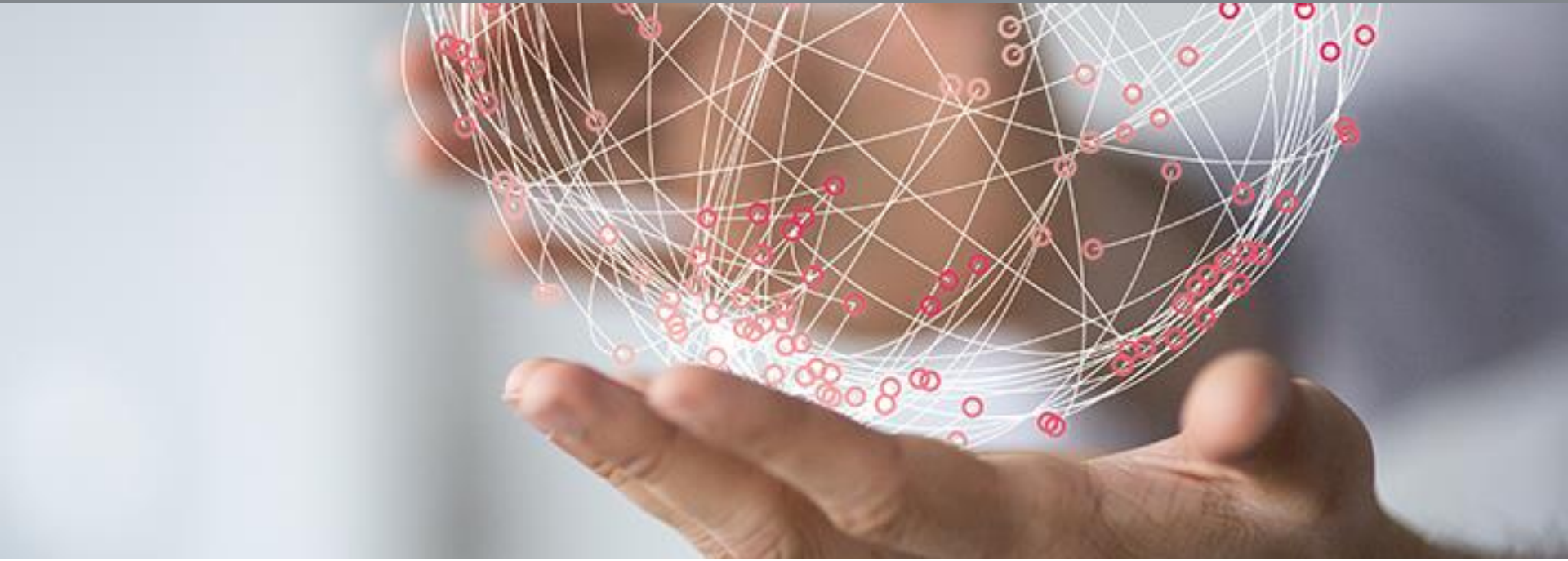


IEC 62443 certification – Management Summary

Gerald Krebs / g.krebs@tuvit.de / +49 160 8885427/ http://https://www.tuvit.de/de/startseite/

How to ensure Security for „Industrial Automation & Control System“?

TÜV NORD GROUP

TÜV NORD GROUP

TÜV NORD AG

Business Unit Industrial Services	Business Unit Mobility	Business Unit Natural Resources	Business Unit Training	Business Unit Aerospace	Business Unit IT	Group Services
TÜV NORD Systems	**TÜV NORD Mobilität**	**DMT**	TÜV NORD Bildung	ATN	TÜV Informationstechnik TÜV NORD Secure Communications	TÜV NORD Service
further companies	further companies	further companies	further companies	further companies	further companies	further companies

Bold type: Lead Company of the Business Unit

UNSERE THEMEN, WAS UNS ANTREIBT

IT-Sicherheit und -Qualität – unabhängig geprüft

https://www.tuvit.de/de/themen/

Security4Safety

Industrie 4.0: Vernetzung braucht Sicherheit

Cyber Security

Prüfung von IT-Systemen/Netzwerken und Applikationen

Automotive Security

Das sichere „Connected Car“

Mobile Security

Mobile Sicherheit durch „Trusted Mobile“ Siegel

Datenschutz

Aus der „Pflicht“ eine „Kür“ machen

KRITIS

Umsetzung der Vorgaben aus IT-Sicherheitsgesetz

Sicherheitsevaluierungen

Schutz von sensitiven Daten für Hard- und Software

eIDAS

Elektronische Signaturen und Siegel

Data Center Security

400+ Zertifikate für sichere Rechenzentren

TÜV NORD GROUP

TÜVIT COMITTMENT IN IECEE

About IECEE | Members | News | Testing & Certification | Committees | Peer Assessment | Documents | Events & Meetings | Search... Search | Log in

Committees > CTL > CTL ETF 16

Committee of Testing Laboratories (CTL)

Home | Expert Task Forces & Working Groups | Meetings | Decisions | Testing Equipment | Proficiency Testing | Documents

Working Groups & Task Forces > CTL ETF 16

Title / Description

CTL ETF 16

CTL Expert Task Force 16 "Cyber Security"

Convenor

Mrs Michael Michelle
TÜV NORD CERT GmbH

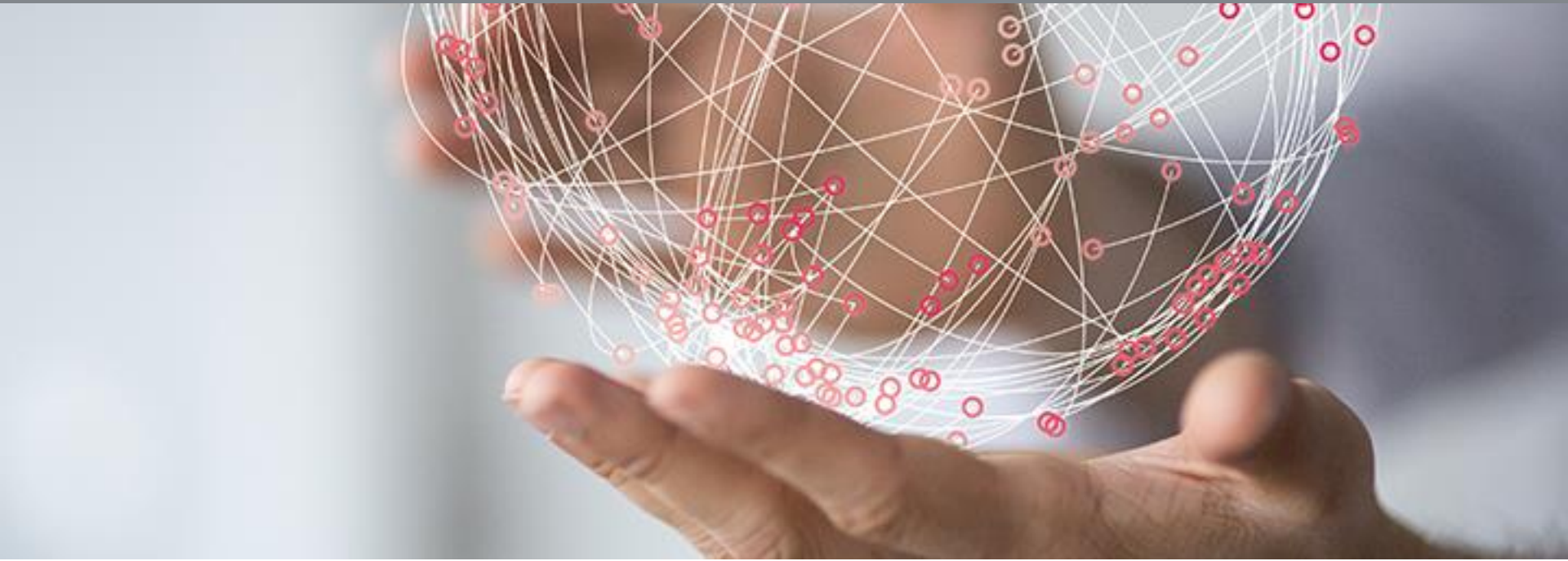
Technical Advisors

Last Name, First Name	Company

Members

Last Name, First Name	Company
Mr Bang Jiho	KTC - Korea Testing Certification
Mr Cambronero Suárez Giovanni	ANCE - Asociación de Normalización y Certificación, A.C.
Mr Chien Koh Wei	TÜV SÜD PSB Pte. Ltd.
Mr Cohen Ilan	I.T.L. (PRODUCT TESTING) Ltd.
Mr Fritsch Sebastian	secuvera GmbH
Mr Hamel Jérôme	Laboratoire Central des Industries Electriques (LCIE)
Mr Petri Bernhard	Siemens
Mr Posner Daniel	TUV Rheinland of North America, Inc.
Mr Wardaschka André	DEKRA Testing and Certification GmbH

TÜVIT
TÜV NORD GROUP



Introduction in IEC 62443

TÜV NORD GROUP

MOTIVATION

- **Digitalization** of Industrial Automation & Control System (IACS) and rapid growing technology for **Industrie 4.0.** increase the complexity

Networking takes place between

- Within the Operational Technology (OT) environment
- Between IT and OT environments
- Between business partners (suppliers and customers etc)

! Previously isolated areas are networked. This increases the attack possibilities

MOTIVATION
NEW CHALLENGES IT & OT

IT

Extensive impact in case of breakdown

Business & reputation damage because of e.g. information theft

Outdated or individual systems

- small changes cause big problems
- no compatibility with standard IT security packages

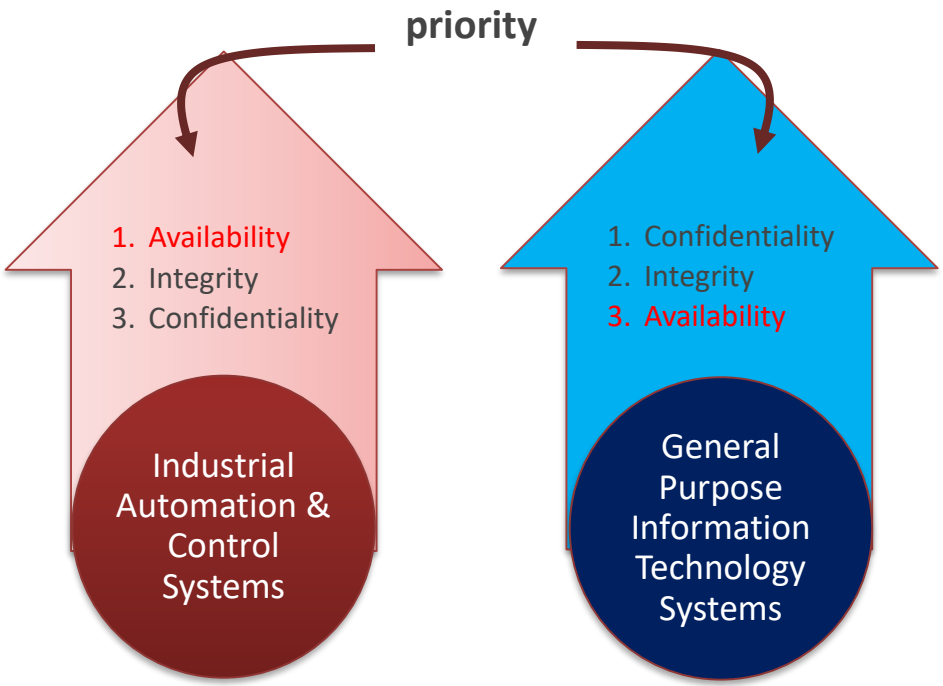
OT

Growing danger for cyber attacks with the possibility of breakdowns

Loss of confidentiality and integrity

IT employees have little experience with industrial systems

INDUSTUSTRIAL SECURITY VS. GENERAL IT SECURITY PRIORITY



MOTIVATION
DIFFERENCE BETWEEN OFFICE IT & PRODUCTION IT SYSTEMS

Security Topic	Office IT Systems	Production IT systems
Antivirus	Widely used and easily updated	complicated and often impossible to implement
Life Cycle	3-5 Years	5-20 Years
Awareness	Good	Not good
Patch Management	Often	Rare, approval from Plant manufacturers
Change Management	Regular and scheduled	Rare
Evaluation of log files	Established practice	Unusual practice
Time Dependency	Delays Accepted	Critical
Availability	Not always available, failures accepted	24*7
Security tests	Widespread	Rare and problematic
Testing environment	Available	Rarely available

MOTIVATION
STANDARD FINDINGS

- NO patch management
- NO malware protection
- NO awareness on site
- NO backup

The International standard IEC 62443 addresses all these issues for the security of IACS and makes the IACS environment conform.

MOTIVATION
BENEFITS OF IEC 62443 CERTIFICATION FOR INDUSTRIAL SECURITY

- Standardized Industrial Security on international level
- products, solutions and processes according best practice security
- Certification possibility
- Key argument for buyers and answer to ensure secure Industry 4.0 introduction
- Ensuring availability, confidentiality and integrity on highest level
- Investment protection

SOME DEFINITIONS IN IEC62443

Security Level (SL) definition for e.g. IEC62443-4-2 & -3-3:

- SL-1: any Internet user
- SL-2: interested individuals and companies with generic security knowledge
- SL-3: Experts and companies that have clear objectives and effective, but cost-oriented attack scenarios
- develop and deploy
- SL-4: governmental organisations which focus on achieving the specifically selected target at almost any price

Maturity Level (ML) definition for e.g. IEC62443-2-4 & -4-1:

- Maturity Level 1 – Ad-hoc process
- Maturity Level 2 – Documented process, but not necessarily repeatable
- Maturity Level 3 – Documented process that is repeatable and consistently followed
- Maturity Level 4 – Documented process that is repeatable, consistently followed, measured, and steadily improved

Applicability:
software application one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)
embedded device special purpose device running embedded software designed to directly monitor, control or actuate an industrial process
host device general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers
network device device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

IEC 62443 DESIGN

Certification:
- Product
- Solution

Certification:
- Process
- Product (mandatory for 4-2)

IEC 62443 Series

General		Management System		Industrial IT Security (IACS)		Embedded Security Component	
1-1	Terminology, concepts & models	2-1	Establishing an IACS security program	3-1	Security technologies for IACS	4-1	Product development requirements
1-2	Master glossary of terms and abbreviations	2-2	Operating an IACS security program	3-2	Security risk assessment and system design	4-2	Technical security requirements for IACS components
1-3	System security compliance metrics	2-3	Patch Management in the IACS enviroment	3-3	System security requirements and security levels		
		2-4	Requirements for IACS solution suppliers				
		For Operators		For Integrators		For manufacturers	

Certification:
- process
- product
- solution

Certification:
- product

IEC62443-2-4 “REQUIREMENTS FOR IACS SOLUTION SUPPLIERS“ IN MORE DETAIL (EXAMPLE)

- **Solution Staffing:** Capabilities relate to staffing of automation solutions by service providers. All certification applications must include this conformance block.
- **Solution Hardening:** Capabilities relate to reducing automation solution attack surface, including risk assessments, detection of threats and vulnerabilities, and management of USB ports.
- **Network Security:** Capabilities relate to supporting the segmentation and administration of networks.
- **User Security:** Capabilities relate to supporting the administration of operating system security and user accounts.
- **Application Security:** Capabilities relate to specific control and monitoring features of the automation solution
- **Security Information and Event Management (SIEM):** Capabilities relate to supporting the management of security-related information and events, generally for the purpose of security incident handling and forensics.
- **Patch Management:** Capabilities relate to supporting the validation and installation of security patches.
- **Backup&Restore:** Capability relate to support backup&restore functionalities of the automation solution and its products

IEC62443-4-1 ”PRODUCT DEVELOPMENT REQUIREMENTS“ IN MORE DETAIL (EXAMPLE)

Requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware.

- security requirements definition,
- secure design,
- secure implementation (including coding guidelines),
- verification and validation,
- change management,
- patch management ,
- product end-of-life.

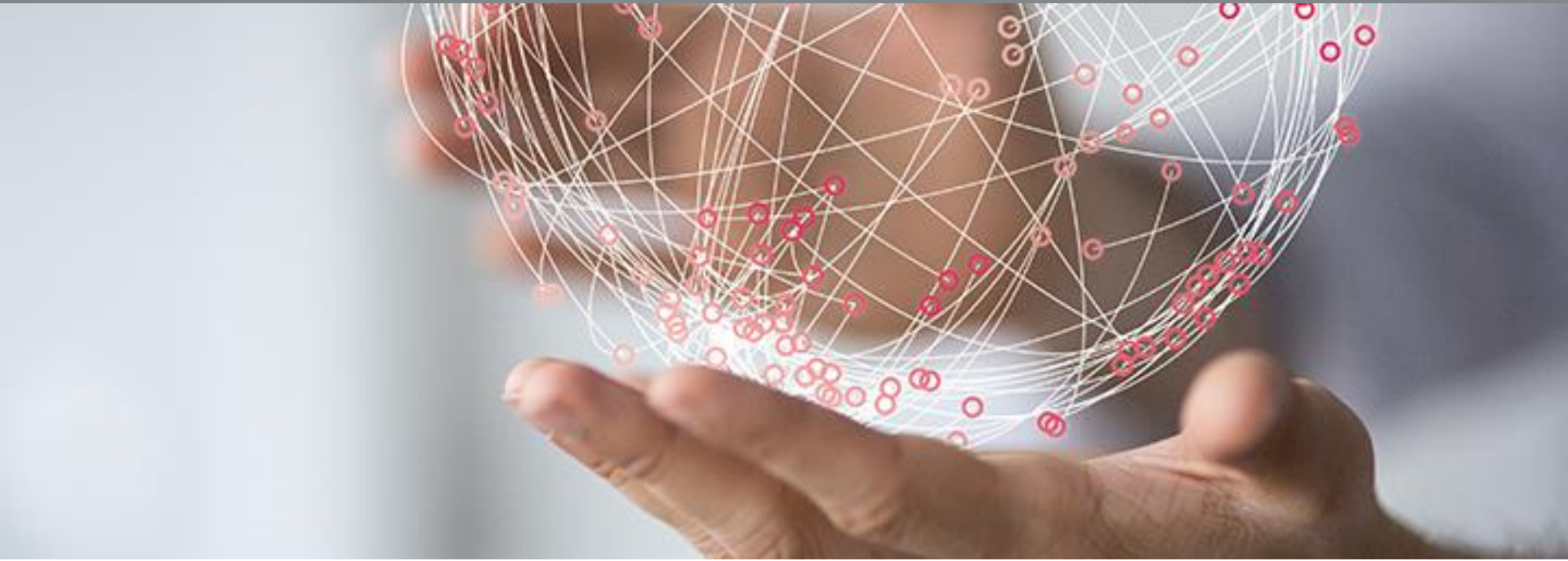
IEC62443-4-2 “TECHNICAL SECURITY REQUIREMENTS FOR IACS COMPONENTS“ IN MORE DETAIL

FR1 – Identification and Authentication Control

Sub-Chapters	Requirements	Results	Remarks	SL-1	SL-2	SL-3	SL-4
5.3	**CR 1.1 – Identifizierung und Authentifikation von menschlichen Nutzern**	-					
5.3.3.1	(1) Eindeutige Identifizierung und Authentifikation Die Komponente muss die Fähigkeit haben, alle menschlichen Nutzer eindeutig zu identifizieren und zu authentifizieren.				✔	✔	✔
5.3.3.2	(2) Multifaktor-Authentifikation über alle Schnittstellen Die Komponente muss die Fähigkeit haben, eine Multifaktor-Authentifikation für den Zugriff aller menschlichen Nutzer auf die Komponente zu verwenden.	-					✔

FR2 – Use Control
FR3 – System Integrity
FR4 – Data Confidentiality
FR5 – Restricted Data Flow
FR6 – Timely Response to Events
FR7 – Resource Availability

TÜVIT®
TÜV NORD GROUP

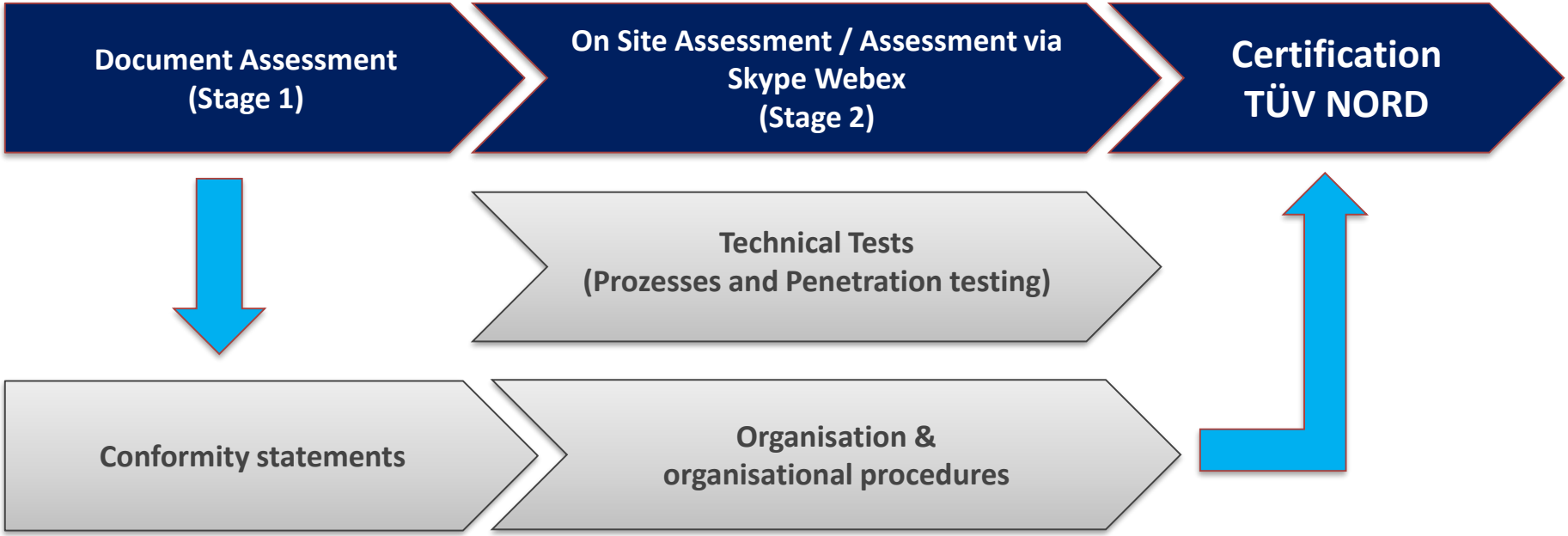


IEC 62443 certification assessment process

Industrial Automation Control Systems

TÜV NORD GROUP

IEC 62443
CERTIFICATION ASSESSMENT PROCESS



CERTIFICATION PROCESS TÜV NORD CERT

		Duration
Review of application	• scope definition • approval of applicable standards • approval of certification ability • allocating resources and assessment and certification team	1 week
Evaluation (Lab)	• specific requirements for policies and procedures • specific requirements for systems • specific requirements for components	acc. to part of IEC 62443 and/or SL
Review (Cert Body)	• conducted assessment and checklists • conformity documentation • recommendation of certification	2 weeks
Certification (Cert Body)	• initiating certification • registering • issuing certificate	2 weeks