Can not See the Wood for the Trees -
Too Many Security Standards for Automation Industry

Frank Ackermann at DeepSec 2018

Profile Frank Ackermann

- Head of Automation Security at Yokogawa Deutschland GmbH
- Working since over 17 years in IT-/OT- and Information-Security
- ‚Security is not my job – it‘s my passion‘
- Certified

CISSP® Certified Information Systems Security Professional

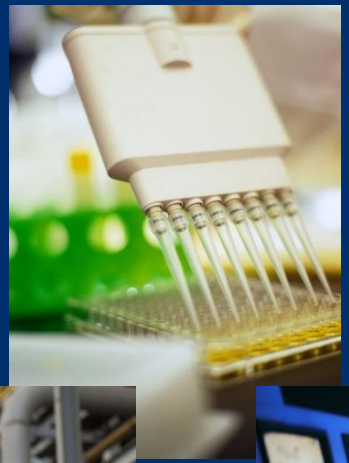
PECB ISO/IEC 27001 Lead Auditor

Products and Solutions

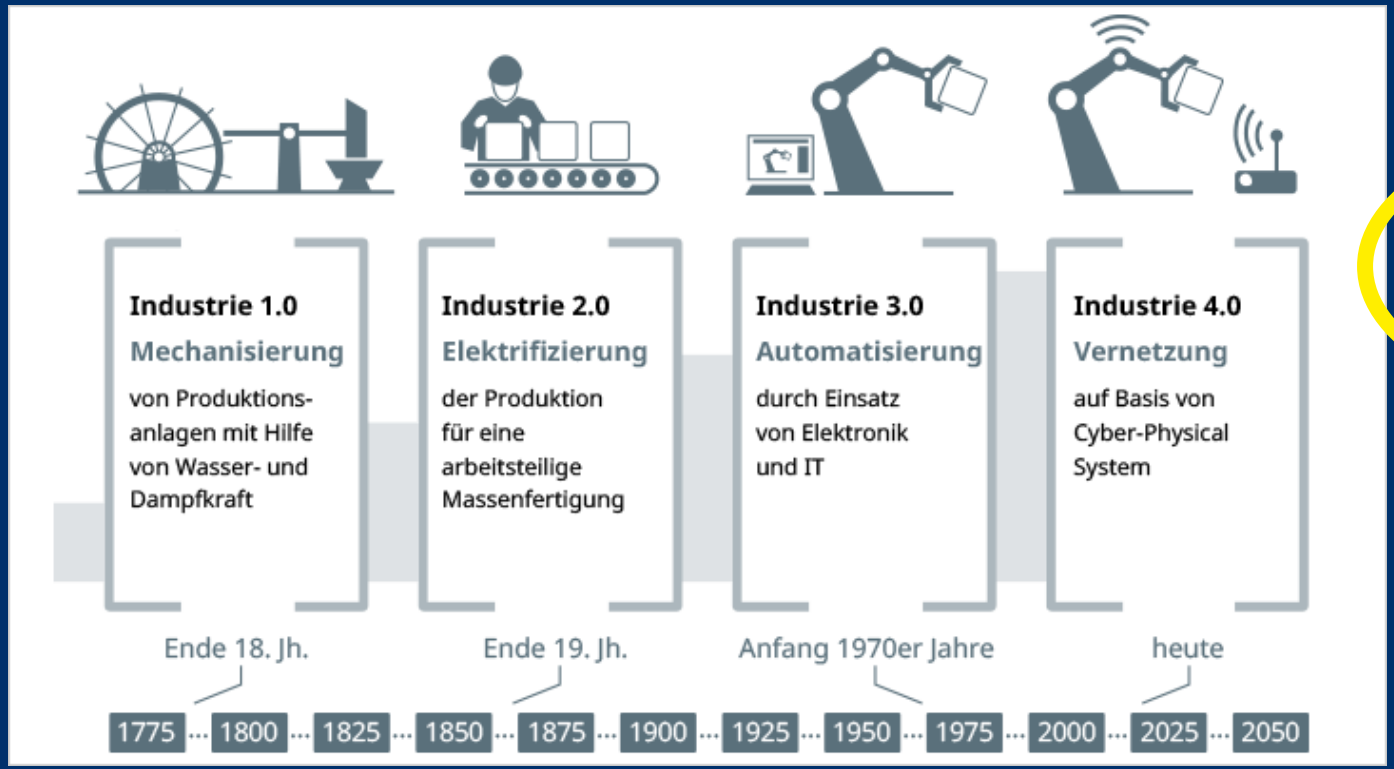
- Processoptimization and Industrial Automation
- Control Systems for industrial environments
- Energie Efficiency Management
- …

Vendor, Solution Provider and Integrator

Where to find us?



Connectivity and Information Exchange in Industry 4.0



> Industry 4.0 and Digitalization reduces costs!

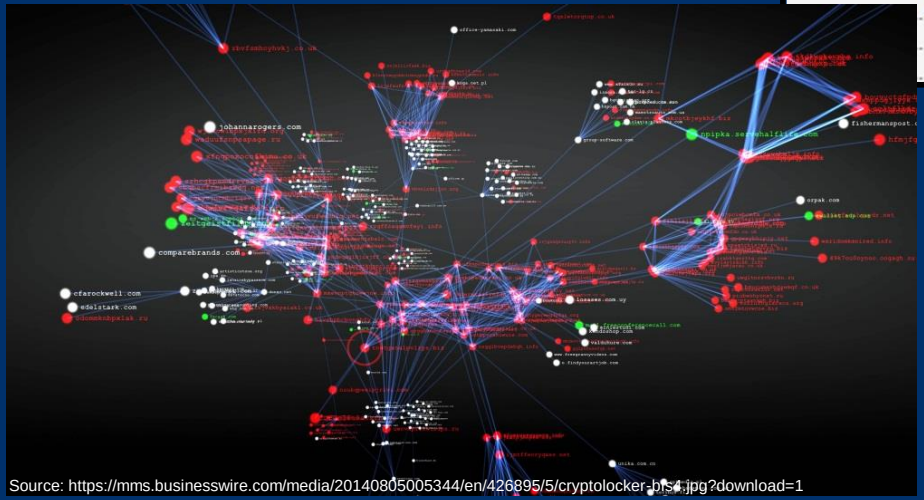
> OT-environment information increases in value!

> Separated networks grow together!

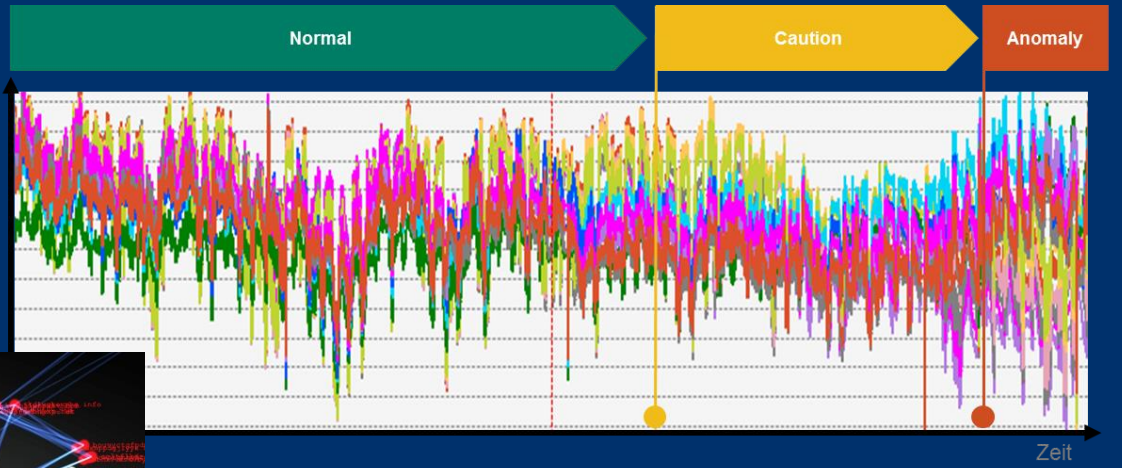
> Industrial plants becoming attractive targets!

OT-environment information increases in value!

… in the industrial plant …

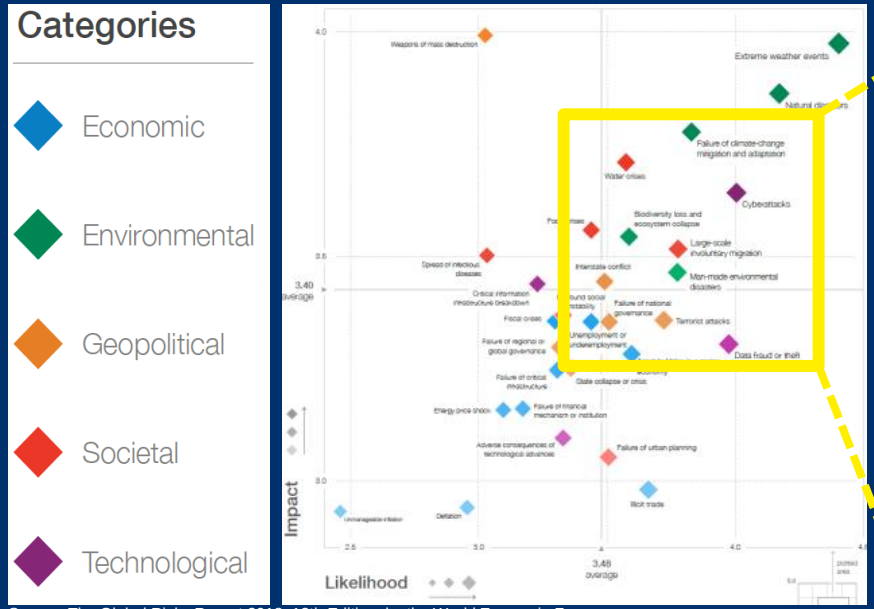


Source: https://mms.businesswire.com/media/20140805005344/en/426895/5/cryptolocker-bts4.jpg?download=1



… as well as in the security environment.

Global Risks Landscape 2018



Source: The Global Risks Report 2018, 13th Edition, by the World Economic Forum

Structured Approach to Increase Security

- To increase the implemented security within the OT-environment, several industry standards, recommendations and rulesets were defined
- Not all of the standards and recommendations complement each other – therefore it‘s worth to have a closer look …

… and there are Many Standards!

- VDI/VDE 2180 (Functional Security for the Processindustry, German)
- VDI/VDE 2182 (Informationsecurity for OT, German)
- DIN/IEC 61508 (Standard for the development of safety-functions)
- DIN/IEC 61511 (Standard for operating safety-functions)
- BSI Standards 200-1 bis 200-3 (BSI IT-Grundschutz neu)
- Namur-Recommendations
- NIST-Framework
- US Food and Drug Administration (https://www.fda.gov)
  (US, Chemie / Pharma; recognized in Europe as a reference)
- NERC CIP (https://www.nerc.com/pa/Stand/Pages/Default.aspx) (US, Standard for Power)
- ISO/IEC 2700* (Standard to specify an ISMS)
- DIN/IEC 62443 (Security standard for OT)
- KRITIS/BSI-KritisV + IT-Sicherheitsgesetz (Critical infrastructure law and regulation, Germany)
- And many many more …

ISO / IEC 2700*

ISO/IEC 2700*

- Standard to specify an Information Security Management Systems (ISMS)
- Broad in scope (…privacy, confidentiality and ‚cyber' security issues, incident management)
- Provides guidelines to develop, implement and maintain an ISMS and Risk-Management
- Focus on Information Security (Confidentiality, Integrity and Availability)

ISO/IEC 2700*

- Suitable for organizations / enterprises of any size and type
- Family Standards
  - ISO/IEC 27000 - ITSM IT Service Management
  - ISO/IEC 27001 - Specification of ISMS
  - ISO/IEC 27002 - Best practice, specifications and controls
  - ISO/IEC 27005 - Risk Management
  - ISO/IEC 27019 - Best Practice (Energy Sector)

ISO/IEC 2700*

+ Standards for organizations of any discipline
+ IEC 2700* is a finalized standard and an ISMS organization can be certified

- No procedure to implement and maintain an ISMS
- Not directly applicable for OT (Operational Technology) environment and systems

IEC 62443

IEC 62443

- As of now THE standard regarding security in the Industrial Environment / Operational Technology
- Industrial Automation Control Systems (IACS) and its protection in the foreground
- In the past named *ISA99*, since 2010 renamed in ANSI/ISA-62443

IEC 62443

- IEC 62443 adds to IEC 61508 (safety standard for control systems)
- Addresses four different aspects of security in the IACS environment and it‘s management system
  - General (e.g. terminology, definitions)
  - Policies & Procedures (e.g. requirements and implementation)
  - System (e.g. security technologies, risk assessment)
  - Components (e.g. product development requirements)

IEC 62443

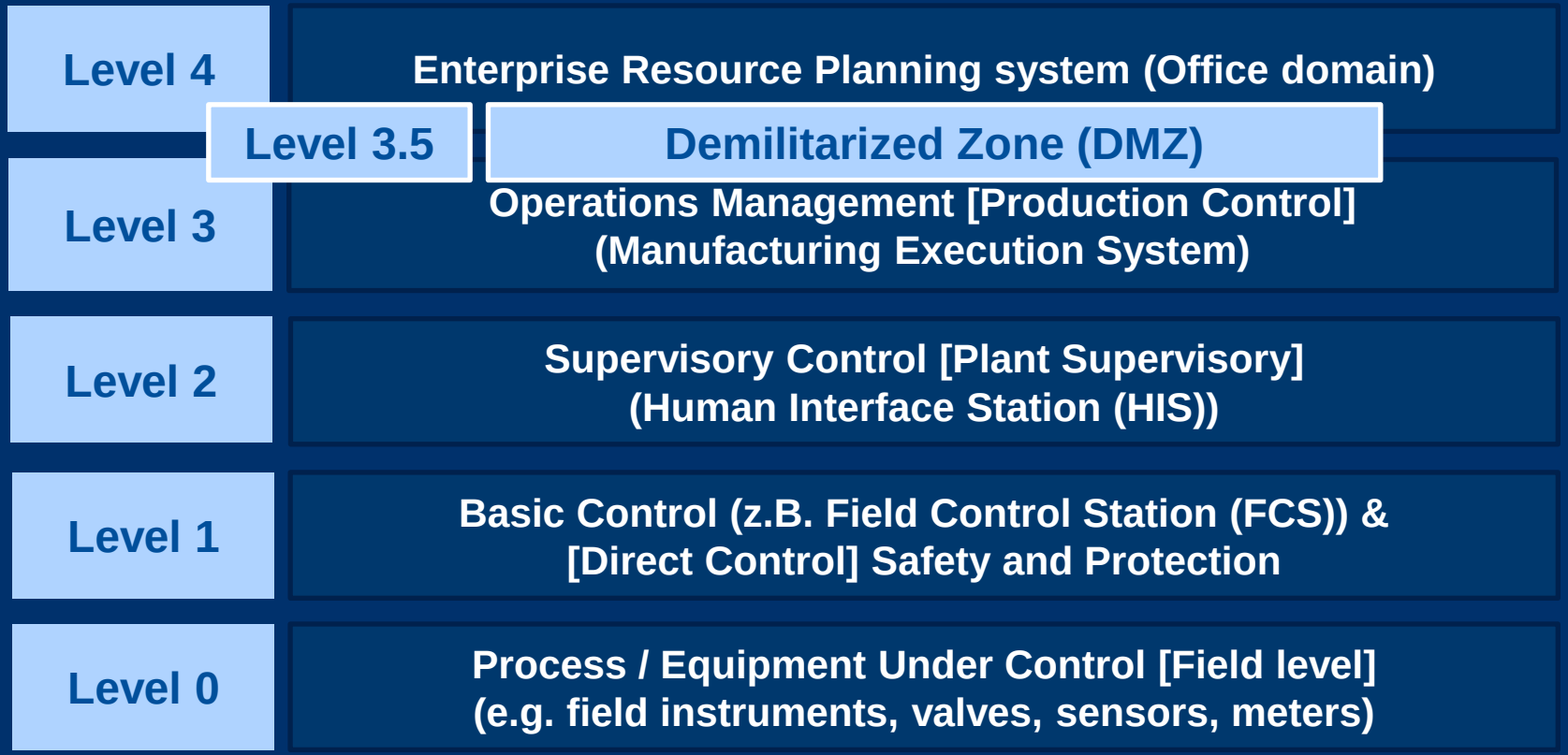
Published parts of the IEC 62443

IEC 62443: Industrial communication networks – Network and system security

General		Policies & Procedures		System		Component/Product	
1-1	Terminology, concepts and models	2-1	Requirements for an IACS security management system	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	Implementation guidance for an IACS security management system	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 environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-case	2-4	Security program requirements for IACS service providers				

published

IEC 62443


Level 4
Enterprise Resource Planning system (Office domain)
Level 3.5
Demilitarized Zone (DMZ)
Level 3
Operations Management [Production Control]
(Manufacturing Execution System)
Level 2
Supervisory Control [Plant Supervisory]
(Human Interface Station (HIS))
Level 1
Basic Control (z.B. Field Control Station (FCS)) &
[Direct Control] Safety and Protection
Level 0
Process / Equipment Under Control [Field level]
(e.g. field instruments, valves, sensors, meters)

IEC 62443

- \+ Security standard for the automation / process industry (IACS)
- \+ Provides guidelines for maintenance (e.g. patching)
- \+ Consistent use with other standards possible

- \- Only parts if the standard are final and published, therefore foundations for full certification missing
- \- Risk assessment academic

BSI 200 (-1, -2, -3)

BSI 200

- Defined by the German Federal Office for Information Security (BSI)
- Standard for the requirements for an Information Security Management System (ISMS)
- Focus on privat sector; including smaler companies
- Compatible with ISO/IEC 2700*

BSI 200

- The standard splits up in three areas
  - BSI 200-1 ISMS-Management
  - BSI 200-2 Definition of baseline security including methods (including maintaining an ISMS)
  - BSI 200-3 Riskmanagement
- Englisch version is available too

BSI 200

+ Provides a simple and practical explanation of setting up an ISMS
+ Defines baseline security elements and supports also smaler companies
+ Considers ICS and OT in the framework

- Generic wordings and parts focus IT (office IT) only
- Not suitable for 27001-certification

Namur NE 153

Namur NE 153

- User Association of Automation Technology in Process Industries (NAMUR)
- NE 153 provides guidance to implement cyber security measures and gives recommendation for the Design, Implementation and Operation of Industrial Automation Systems
- The design concepts of IEC 62443 and VDI 2182 serve as a basis for NE 153

Namur NE 153

- The recommendations focus on the following aspects
  - Secure by Default
  - Secure by Design
  - Secure by Implementation
  - Secure in Deployment

Namur NE 153

+ Simple recommendations for vendors and operators
+ Available in German and Englisch

- Not a standard itself (only a recommendation)
- Very generic
- Does not covers the operation and maintenance of an Industrial Automation and Control Systems

NIST
Cyber Security Framework

NIST Cyber Security Framework

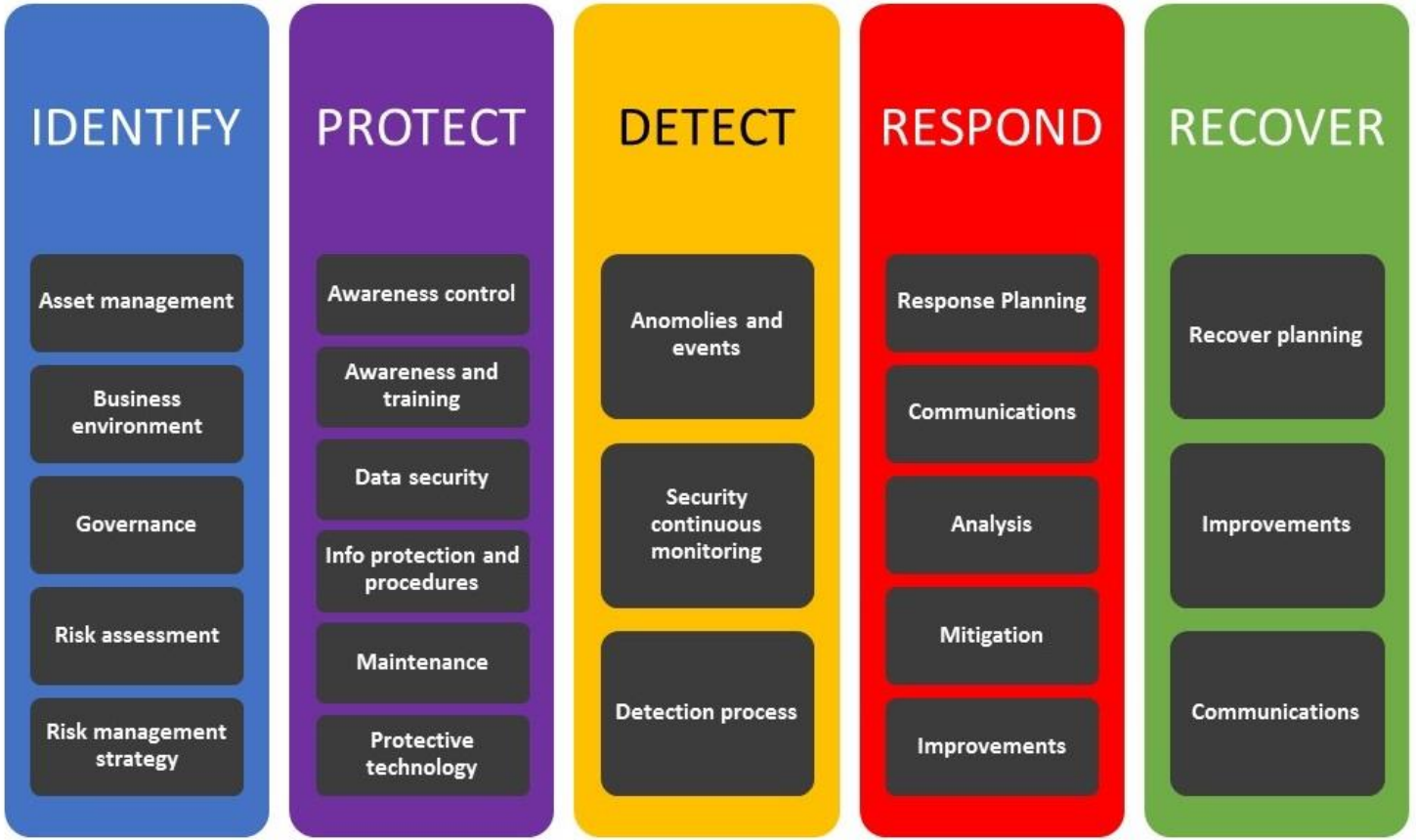
- Policy framework and guideline focussing the management of risks
- Maintained and published by NIST (National Institute of Standards and Technology)
- Designed for individual businesses and organizations to assess the risks
- Applicable for all private sectors

NIST Cyber Security Framework

- Current version V1.1, 16th April 2018
- Focusses on the process steps
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

  to identify and manage (cybersecurity) risks.

NIST Cyber Security Framework



Source: http://www.petermorin.com/2017/12/nist-releases-new-cyber-security-framework-draft/

NIST Cyber Security Framework

- Structure and references, example:

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5

NIST Cyber Security Framework

- Requirements and recommendations to improve security in OT-environment can directly be deduced
- Standards such as the 2700* are not fully covered
- Therefore the NIST framework is no substitution for a certification (and its preparation)

NIST Cyber Security Framework

+ Provides a systematic methodology for managing risks and incidents including its improvement
+ Helps to guide key decision and action items
+ Contains informative references to other standards

- No standard itself
- No procedure to measure risks

Critical Infrastructure Protection (CIP)

Critical Infrastructure Protection (CIP)

- CIP originates out of the US-Directive PDD-63 "Critical Infrastructure Protection“ from 1998
- Equivalent in Europe = European Programme for Critical Infrastructure Protection (EPCIP)
- Concept to prepare and react on incidents in critical infrastructures
- Compareable to the legal regulations KRITIS (Deutschland) and NIS Directive

Critical Infrastructure Protection (CIP)

- CIP conciders the following areas:
  - Banking and finance
  - Power/Energy
    (here NERC CIP - North American Electric Reliability Corporation)
  - Information and communications
  - Federal and municipal services
  - Emergency services
  - Fire departments
  - Law enforcement agencies
  - Public works; Transportation

Critical Infrastructure Protection (CIP)

+ The individual regulations, e.g. NERC-CIP, are mandatory and shall be implemented

- Focusses more on compliance and controls
- The implementation mostly ends up in an Internal Control System
- OT-environment is not always in focus

European NIS Directive (Directive on security of network and information systems)

European NIS Directive

- The European NIS Directive requests member states to pro-actively take precautions to avoid incidents regarding defined industry sectors
- Valid since August 2016 and has to be enforced as local law since May 2018 (e.g. KRITIS für Germany)

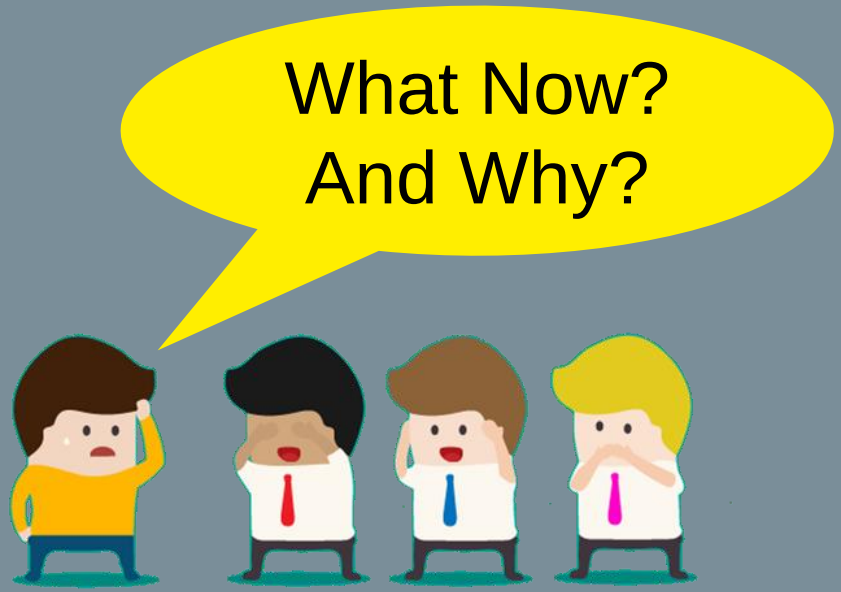
European NIS Directive

- Focusses on relevant services of public life (energy, traffic, finance, health, drinking water, digital infrastructures)
- Risik- and Incidentmanagement of the core businesses
- Reporting of significant incidents is obligated

European NIS Directive

+ Binding regulation for defined industries
  -> may lead to compliance-penalties

- Very generic
- Requiremets on critical infrastructures and OT-environments not specified in detail


What Now?
And Why?

Why are Standards Important?

- Common definition
- Compareablility
- Homogeneous implementation in the system- and industrial landscape
- Basis for explicit requirements, e.g. in customers technical- and functional requirement documentation (example)

Security-Requirement in a Specification (example)

- 7.3 Requirements on Automation Security

  The controlsystem has to consider latest Automation Security- and IT-Security standards.

  The implementation of IT-components in the controlsystem-network have to be performed following the latest security standards, the policy of <the customer> and legal requirements.

Which Standard to pick to Protect the Values?

Source: https://www.tagesspiegel.de/images/circled-wagons/9590398/6-format43.jpg

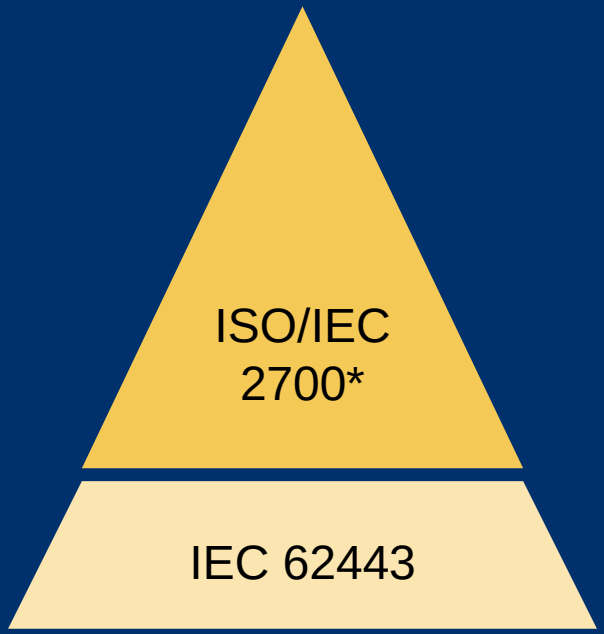
Recommendations

- Identifying core-business and essential production processes and
- Evaluating the risks (Business-Impact- resp. Risk-Analysis)
- Knowing and balance legal requirements
- Considering and (if required) revising internal standards and policies

Recommendations

- Implement Industry Standards, as basis for your security concept, only with management backup
- Defining, adjusting and implementing a reference architecture
- Defining minimum security requirements
- Addressing these requirements in early stages e.g. in a project

Possible Variants (example)



Thank you!

Co-innovating tomorrow™

Frank Ackermann
Head of Automation Security

+49 2102 4983 645
+49 172 6872030
Frank.Ackermann@de.yokogawa.com

Yokogawa Deutschland GmbH
Broichhofstr. 7-11, D-40880 Ratingen