Cybersecurity Regulation and Implementation

WAGO Solution Provider Meeting 2026

Stéphane Rey

How much **damage** was done in 2024 Caused **by cyber attacks** worldwide?

9 Trillion USD

Damage was caused worldwide by cyber attacks in 2024

Source: https://www.cysuranceinstitute.com/insights/report-cybercrime-to-cost-the-world-95-trillion-usd-annually-in-2024-according-to-cybersecurity-ventures?/.

Security Regulation in Europe

Cybersecurity Act

EU Cybersecurity Strategy

Operator

NIS2 (Network Information Security)

Manufacturer

RED (Radio Equipment Directive)

Manufacturer

CRA (Cyber Resilience Act)

Manufacturer

MVO (Machinery Regulation)

Operator

Country-specific implementation

Network and Information Security 2 (NIS2) [directive]

In force Jan. 2023, time for adoption by countries Oct. 2024, in Germany since Nov. 2025
for Switzerland the implementation of NIS2 is still open !

Target

- Strengthening cyber resilience of the operation of key and essential entities in the EU

Scope (simplified):

- Information Security of Systems (incl. Production and Development Environments)
- Essential entities (critical infrastructure) and important entities (new)
- Depending on sector >= 250 employees or >= 50 million. Sales
  - or >= 50 employees or >= 10 million. Sales

Effects

- Maintaining the "state of the art" (mandatory security requirements)
- Regular evaluation by market supervision for essential entities
- Demand for monitoring and attack detection
- High fines for infringements
  - Up to €10 million. EUR or up to 2% of global annual sales

Implementation in Germany

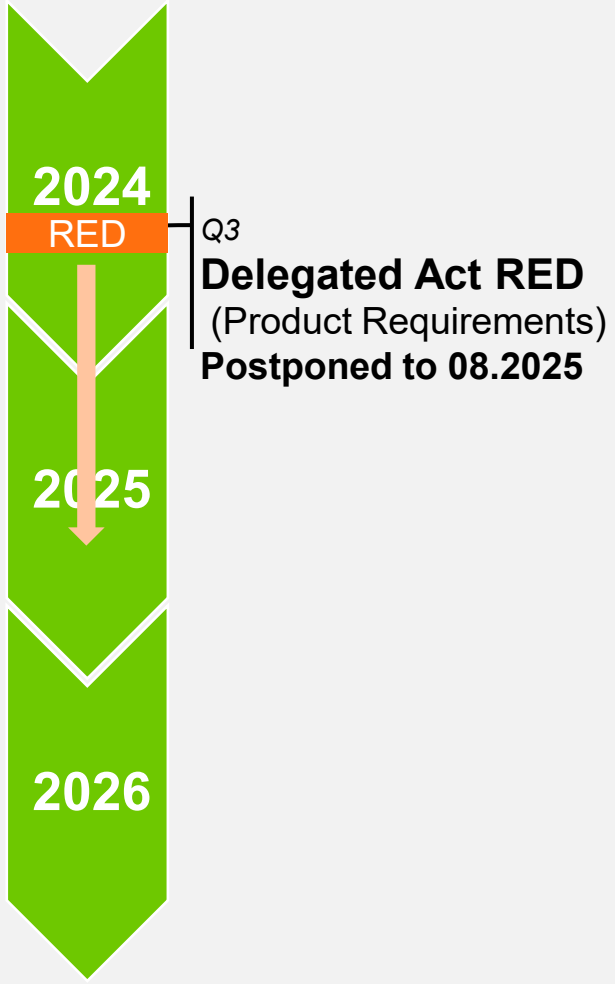
- NIS directive
  <> IT Security Act 1.0 / 2.0
- NIS2 directive
  <> NIS2 Implementation Act

Delegated Act on RED 3(3) d)e)f) [directive]

Status: In force

Status 16.02.2025

Conversion timeline



Target

- Delegated Regulation 2022/30 on radio equipment directive 2014/53/EU activated:

3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

*d) Radio equipment does not **harm the network or its functioning nor misuse network resources**, thereby causing an unacceptable degradation of service;*

*e) Radio equipment incorporates safeguards to ensure that **the personal data and privacy of the user** and of the subscriber are protected;*

*f) Radio equipment supports certain features ensuring protection from **fraud**;*

- **CE marking is linked to Product Security!**

Scope

"...any radio equipment that can **communicate itself over the internet**, whether it communicates **directly** or **via any other equipment** ('internet-connected radio equipment')."

- Obligations focus only on product security features
- EN 18031 was published in February as the first harmonized standard

The EU Cyber Resilience Act (CRA) [Regulation]

Status: In force

Target

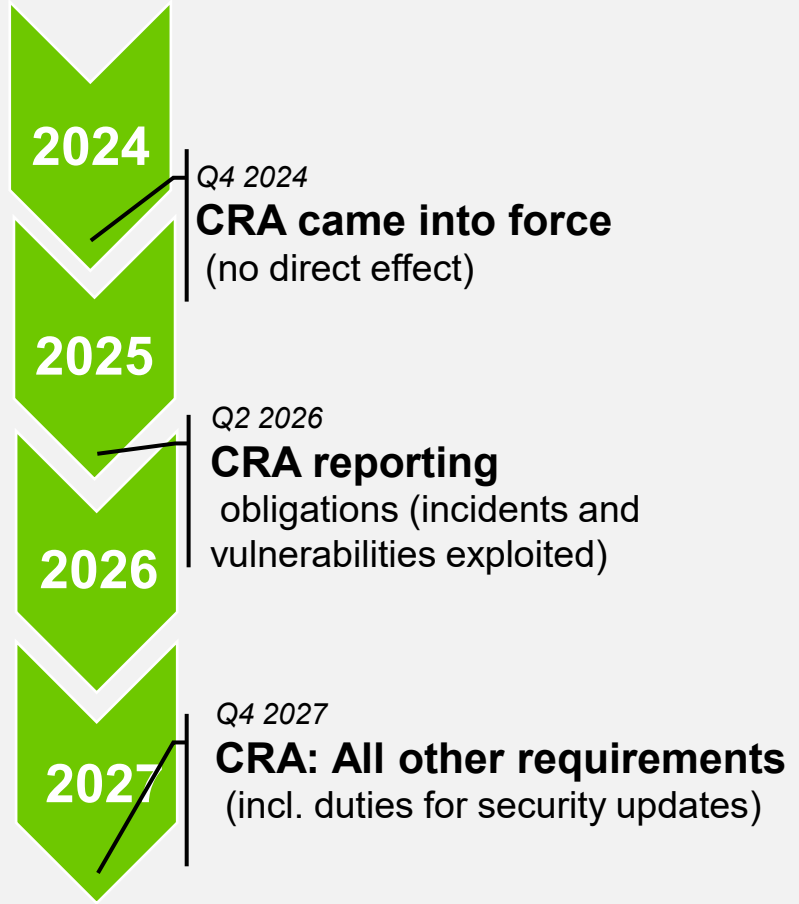
- Horizontal regulation of product security in the EU
- Obligations for products and processes
- **CE marking is linked to Product Security!**

Scope

- ‘The proposed Regulation will apply to all products with digital elements whose intended and reasonably foreseeable use includes a direct or indirect **logical** or **physical** data connection to a device or network’
- Applies to existing portfolio and new developments
- Consider complete product life cycle
- Date of conformity is “placing on the market“
- High fines up to 2.5 % of global annual sales

Status 05.05.2025

Conversion timeline



Machine Ordinance (MVO) [directive]

Status: in force

Target

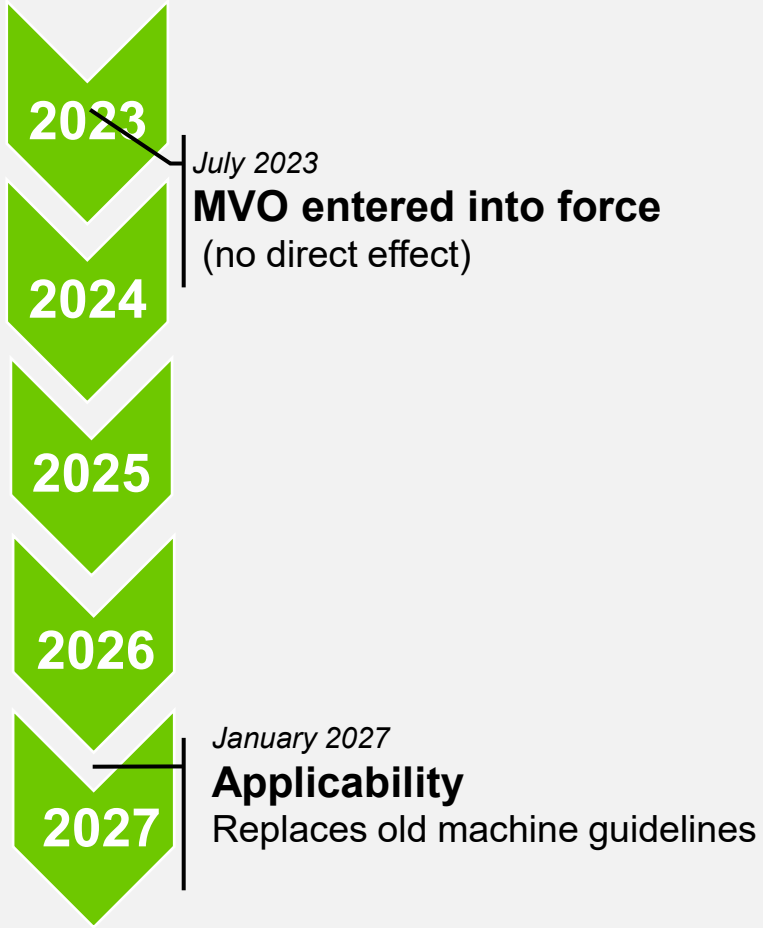
- Horizontal regulation of machine safety in the EU
- **CE marking is linked to Product Security!**

Scope

- ‘The machine or the associated product must be **designed** and **constructed** in such a way that **connection from another device** to the machine or the associated product by any function of the connected device itself or by a remote access device **communicating** with the machine or the associated product does not lead to a dangerous situation.’
- Affects all safety products at WAGO
- Existing portfolio and new developments
- Date of conformity is "placing on the market"

Status 05.05.2025

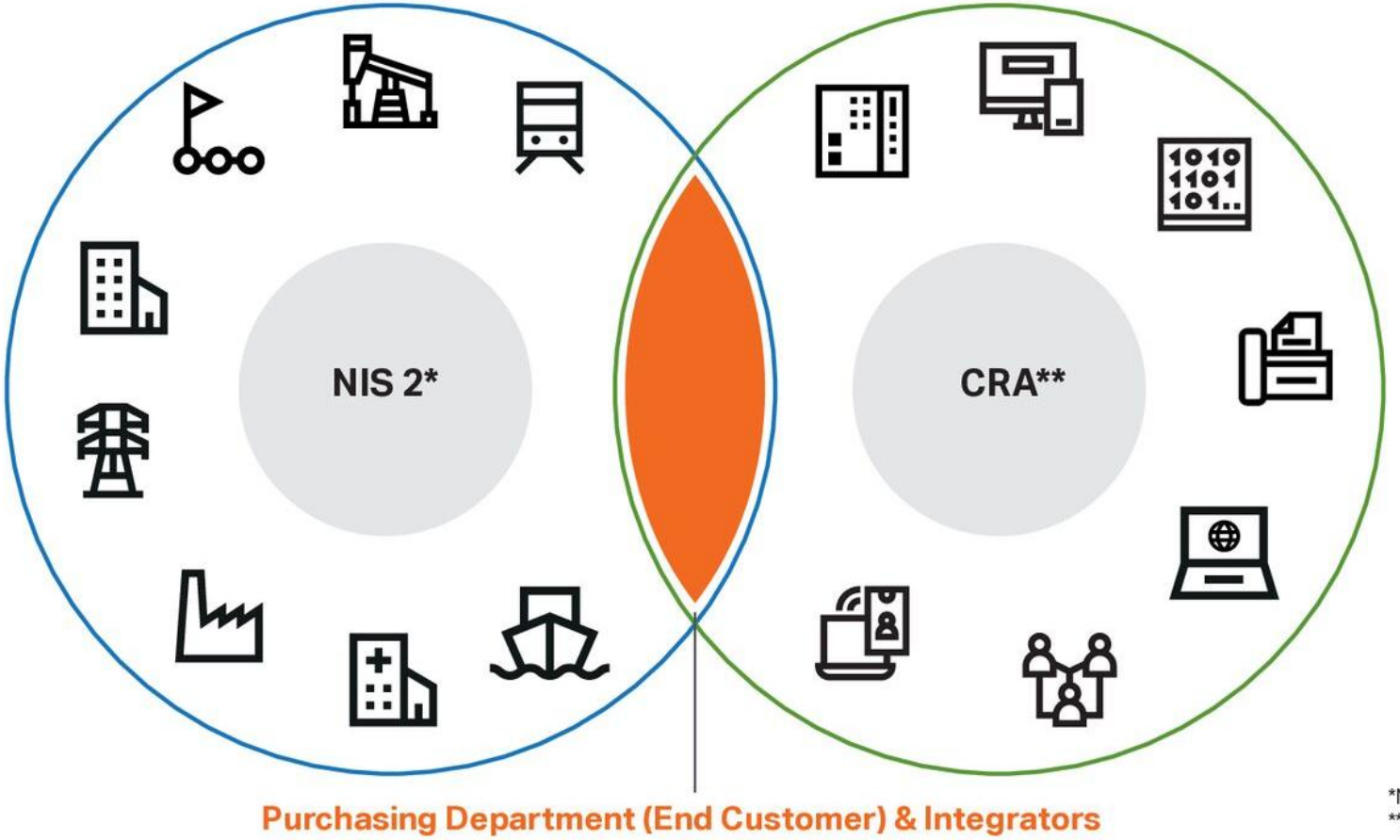
Conversion timeline



Network and Information Security 2 (NIS2) Directive & Cyberresilience Act (CRA)

User
CIO. CISO

focus:
cyberresilience of essential & important entities;
reporting of cyber incidents;
cyber risk mitigating measures



Manufacturer

focus:
cyberresilience of products with digital elements & vulnerabillty handling of manufacturers of those products

*NIS2: Network and Information Security Directive
**CRA: Cyber Resilience Act

How does WAGO approach security regulation?

What follows from regulation?

- Security is an essential component for all industries and market participants
- Manufacturers must develop secure products as part of a safe supply chain
- Customers must operate their infrastructure and systems securely

How does WAGO deal with this?

- Many points in regulation are still vague and short implementation period along the supply chain increases the pressure
- Harmonized standards and other supporting documents should help
  - In December, FAQs about the CRA were published
  - Initial drafts for certain product classes are available (e.g., operating systems)
  - Draft prEN 40000-1-2 / -1-3 describe security activities in development life cycle
- For automation products secure development lifecycle is certified acc. to IEC 62243
  - We assume that this fulfills the emerging security regulations

The CRA is there, how do we deal with it?

New Products

- IEC 62443-4-1/-2 as the basis for conformity assessment
  (mapping with CRA necessary)
- Compliance with IEC 62443-4-1/-2 enables conformity to CRA
- Certified secure development process in place since 2023

Existing products

- Existing products were not developed according to the current state of the art
- Existing products must be evaluated accordingly and, if necessary, strengthened on the basis of the intended use, a threat model and a risk analysis

The CRA affects more than just products;
corporate processes are also affected!

IEC62443

GOLD STANDARD

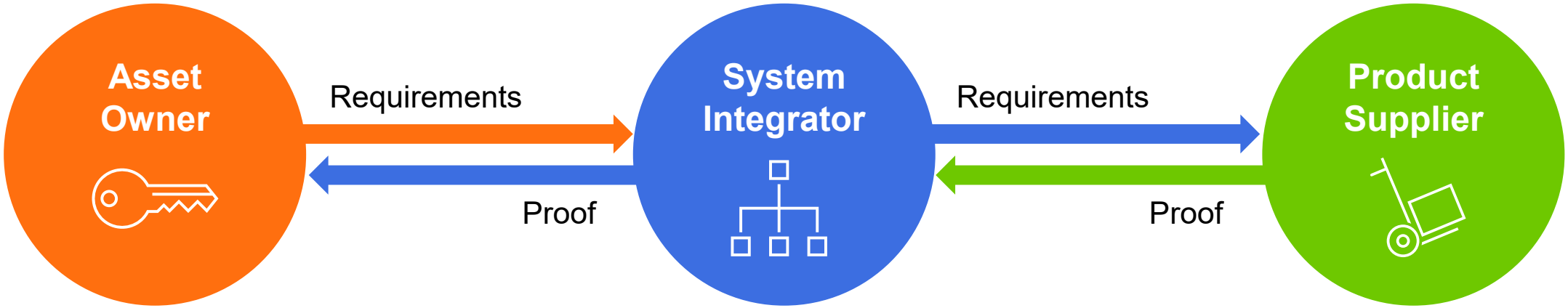
IEC 62443 - Gold Standard for OT

IEC-62443-Normenreihe

ISA/IEC-62443
Industrielle Kommunikationsnetze: – Netzwerk- und Systemsicherheit

Allgemeines	Richtlinien und Verfahren	System	Komponente/Produkt	Sicherheitsprofile (in Planung)	Kriterien zur Bewertung
1-1 Terminologie, Konzepte und Modelle	**2-1** Anforderungen an das Sicherheitsprogramm für IACS-Anlagenbesitzer	**3-1** Sicherheitstechnologien für IACS	**4-1** Anforderungen an einen sicheren Produktentwicklungslebenszyklus		**6-1** Sicherheitsbewertungsmethodik für IEC 62443 Teil 2-4
1-2 Master-Glossar der Begriffe und Abkürzungen	**2-2** IACS-Sicherheitsklassifizierungen	**3-2** Bewertung des Sicherheitsrisikos und Systementwurf	**4-2** Technische Sicherheitsanforderungen an die IACS-Komponenten		**6-2** Sicherheitsbewertungsmethodik für IEC 62443 Teil 4-2
1-3 Anlagensicherheit –Konformitätsmetriken	**2-3** Patch-Management in der IACS-Umgebung	**3-3** Anlagensicherheit – Anforderungen und Sicherheitsstufen			
1-4 IACS-Sicherheitslebenszyklus und Anwendungsfälle	**2-4** Anforderungen an Sicherheitsprogramme für IACS-Dienstleister				
1-5 Schema für Cybersecurityprofile gemäß IEC 62443	**2-5** Umsetzungsleitfaden für IACS-Anlagenbesitzer				

Roles and Responsibilities in IEC 62443



- Responsible for operation of an IACS
- Also called "operator"

- IACS Planning and Design
- Installation and Commissioning
- Changes to IACS

- Provides secure Products Ready
- No reference to specific IACS

IACS = Industrial Automation and Control System

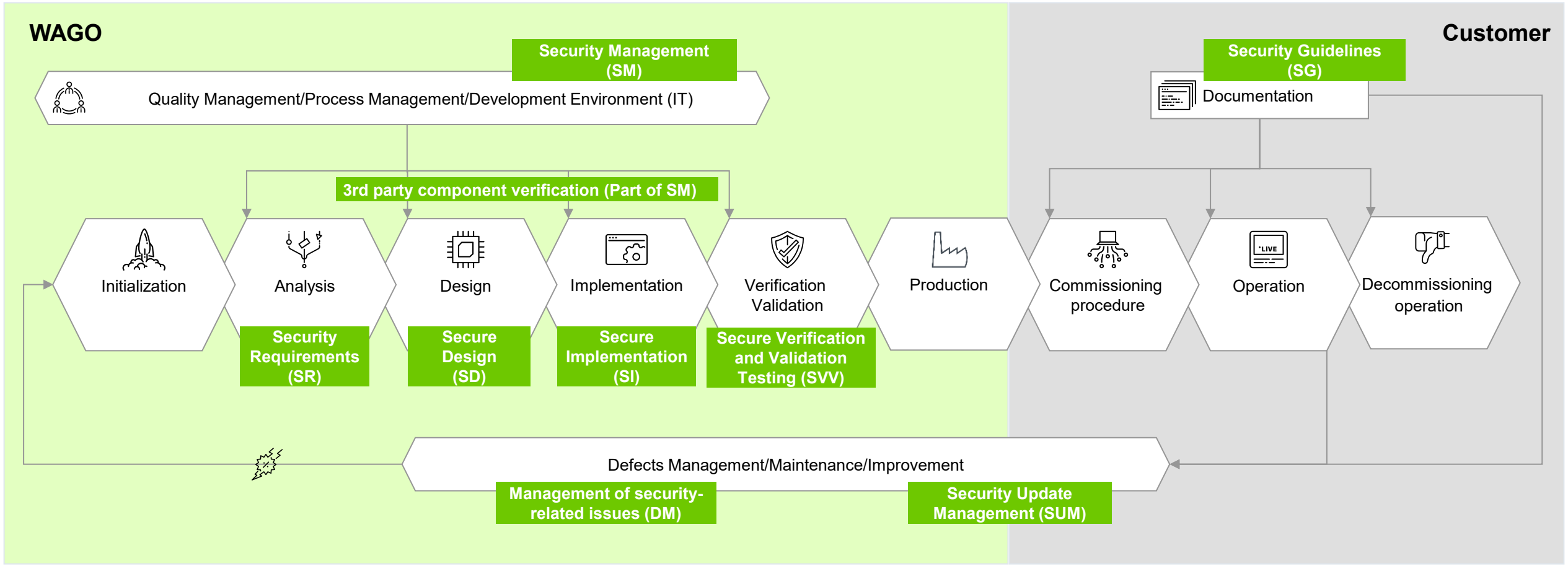
The standard contains requirements for the product life cycle and product for manufacturers

IEC 62443
Industrial communication networks - Network and system security

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	IACS Security Protection Ratings	3-2	Security Risk Assessment and System Design	4-2	Technical security requires-ments for IACS components
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	System security require-ments and security levels		
1-4	IACS security lifecycle and use cases	2-4	Security program require-ments for IACS service providers				
1-5	Scheme for IEC 62443 cyber security profiles	2-5	Implementation guidance for IACS asset owners				

IACS = Industrial Automation and Control System

The IEC 62443-4-1 integrates security into the product lifecycle



Vulnerability Management as an Essential Part of Security

Regulation & IEC 62443 require consistent vulnerability management

- Defined process and responsibilities
- Monitoring of product components for vulnerabilities
- Publish vulnerability information and remediation
- Reporting obligation to market surveillance

➔ WAGO meets this with its Product Security Incident Response Team (PSIRT)

Vulnerability Management as an Essential Part of Security

Regulation & IEC 62443 require consistent vulnerability management

- Defined process and responsibilities
- Monitoring of product components for vulnerabilities
- Publish vulnerability information and remediation
- Reporting obligation to market surveillance

➔ WAGO meets this with its Product Security Incident Response Team (PSIRT)

WAGO SPIRT

Mail	psirt@wago.com
PGP fingerprint	CF3C644680087D124E3AE111D820A2B3E087ED2C
Security.txt	www.wago.com/.well-known/security.txt
Advisories	certvde.com/en/advisories/vendor/wago
RSS Feed	certvde.com/en/advisories/vendor/wago/feeds/rss/

Dimensions of Cybersecurity

Consulting

- Consulting Service with tailor-made hardware and software

Policies

- IEC62443
- NERC CIP
- NIS2
- CRA

Products

- Software and Hardware e.g.:
  - Wago Cybersecurity Network Sight
  - Wago Cybersecurity Collector
  - Wago Cybersecurity Management
  - Wago Cybersecurity Analysis

PSIRT

- Product Security Incidences Response Team
- Vulnerability Management

Industries

- Smart Factory
- Smart Energy
- Smart Building

Time for questions!


WAGO