KNORR-BREMSE

How should my Product Security Management Program look like?

CoC Product Cybersecurity (R/DPC) – November/2023

“Security Management Program”

IT

- Information security strategy aligned with business strategy
- Cost-effective Information Security Management System
- Acceptable level of information security risks

OT

- Definition of security capabilities to operate the IACS securely
- Priority shifts from confidentiality to availability
- Minimization of production/operation downtime

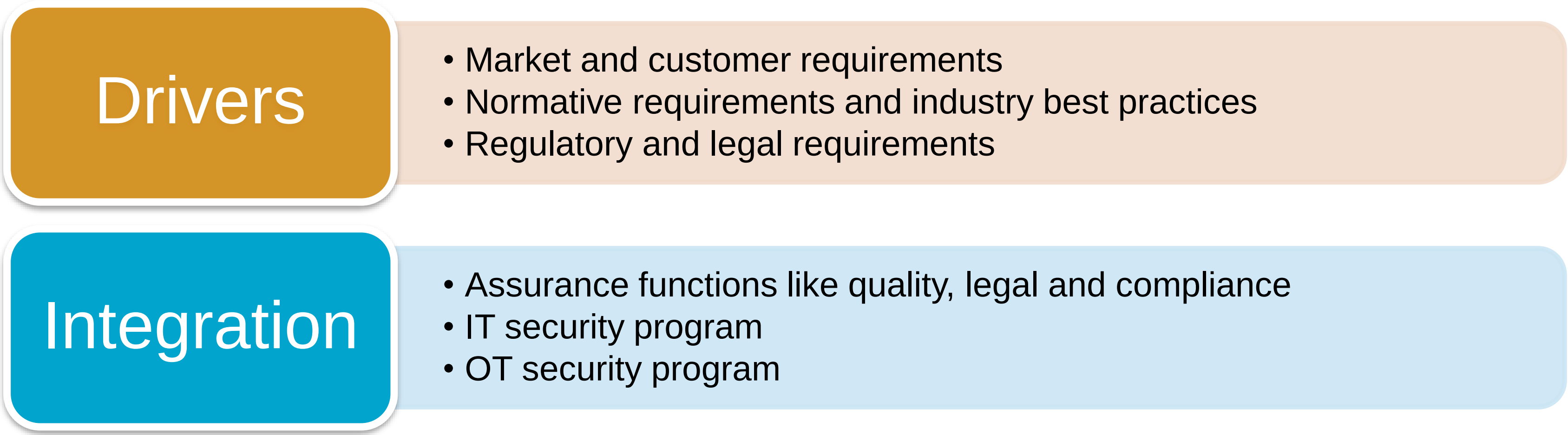
Product

- Subsystems for rolling stock and signalling fixed installations
- No operational responsibilities
- Isn’t a Secure development process enough?

Drivers and integration of the product security management program

- Developing secure products that our customers can integrate in their railway solutions.
- Contributing to the secure operation and maintenance of the railway system.

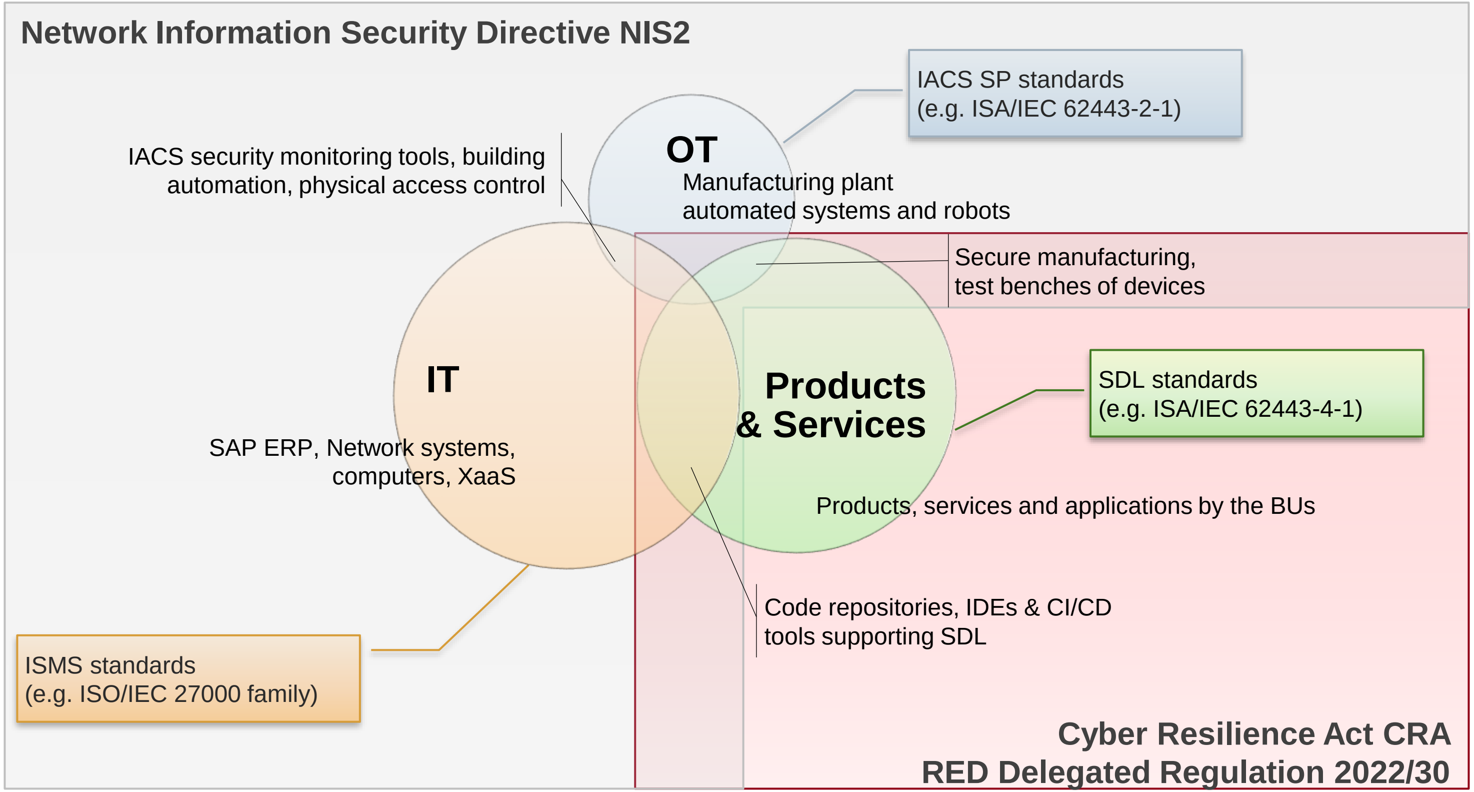
The product security management program implements the strategy to achieve these objectives



- Market and customer requirements
- Normative requirements and industry best practices
- Regulatory and legal requirements

- Assurance functions like quality, legal and compliance
- IT security program
- OT security program

Product Security Scope, Standards, Regulations – EU


Network Information Security Directive NIS2
IACS SP standards
(e.g. ISA/IEC 62443-2-1)
OT
Manufacturing plant
automated systems and robots
IACS security monitoring tools, building
automation, physical access control
Secure manufacturing,
test benches of devices
IT
SAP ERP, Network systems,
computers, XaaS
Products
& Services
SDL standards
(e.g. ISA/IEC 62443-4-1)
Products, services and applications by the BUs
Code repositories, IDEs & CI/CD
tools supporting SDL
ISMS standards
(e.g. ISO/IEC 27000 family)
Cyber Resilience Act CRA
RED Delegated Regulation 2022/30

Delegated Regulation 2022/30 supplementing the Radio Equipment Directive (RED)

Applies to any radio equipment that communicates over the internet directly or indirectly;

(exclusions: medical, aviation, automotive and road toll)

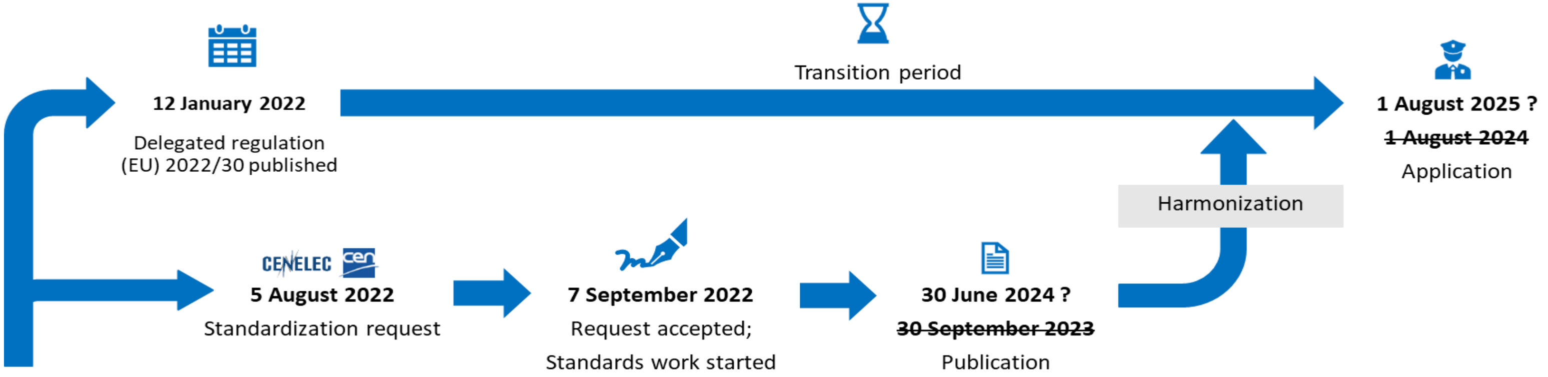
Activates requirements 3.3.d, e and f of the directive

d) addresses the protection of the network,

e) applies if the equipment is capable of processing personal data or traffic data or location data

f) applies if the equipment enables transferring money, monetary value or virtual currency.

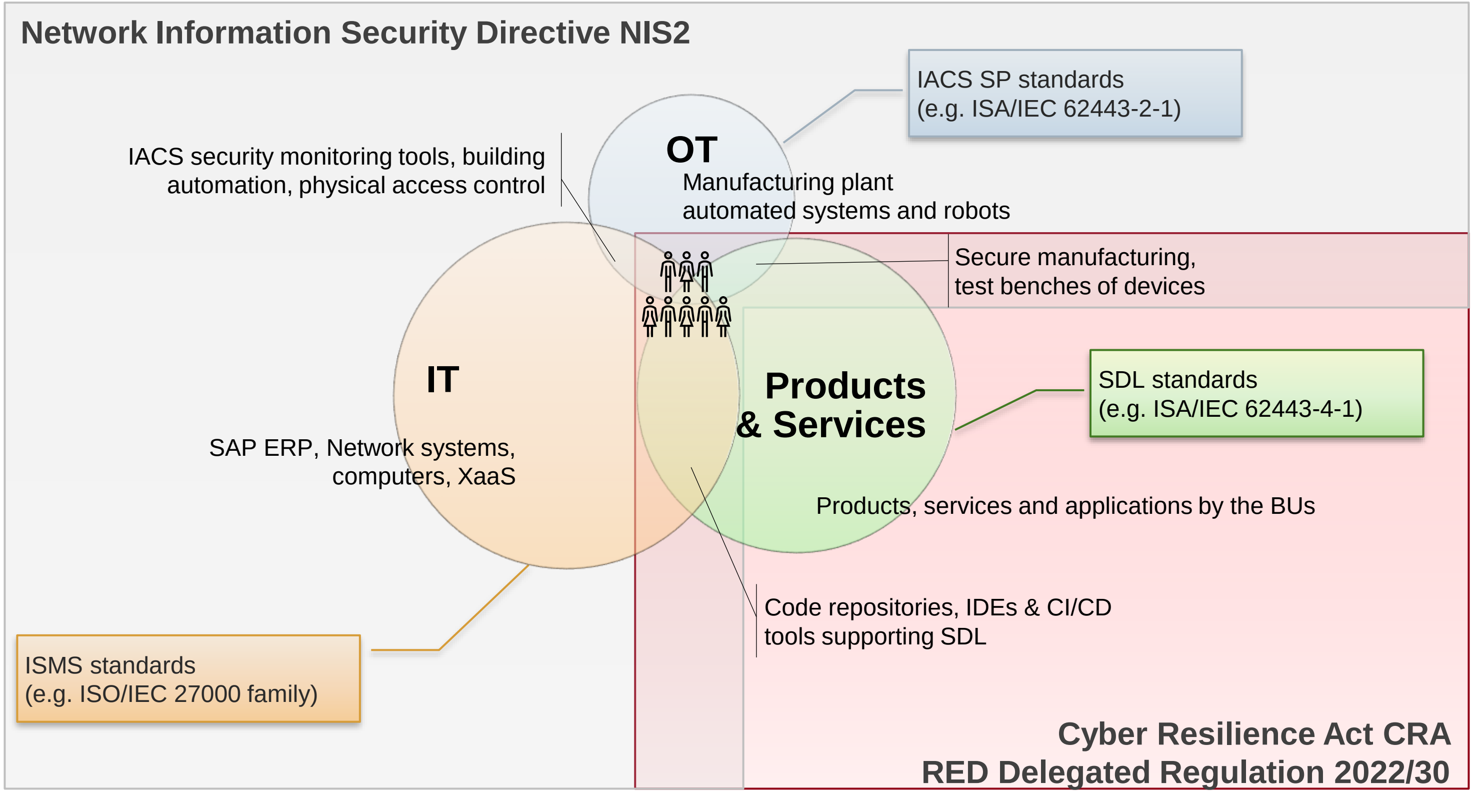
Specifies technical requirements for the products, no process requirements



Timeline by CEN/CLC/JTC 13/WG 8 "Special Working Group RED Standardization Request"

RED Delegated Regulation 2022/30

Product Security Scope, Standards, Regulations – EU



Network Information Security Directive NIS2

IACS SP standards
(e.g. ISA/IEC 62443-2-1)

IACS security monitoring tools, building
automation, physical access control

OT

Manufacturing plant
automated systems and robots

Secure manufacturing,
test benches of devices

IT

Products
& Services

SDL standards
(e.g. ISA/IEC 62443-4-1)

SAP ERP, Network systems,
computers, XaaS

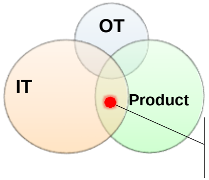
Products, services and applications by the BUs

Code repositories, IDEs & CI/CD
tools supporting SDL

ISMS standards
(e.g. ISO/IEC 27000 family)

Cyber Resilience Act CRA
RED Delegated Regulation 2022/30

Security of the product during development

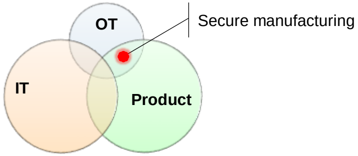


Code repositories, IDEs & CI/CD tools supporting SDL

- ISA/IEC 62443-4-1 SM-7 requires security controls protecting the product and patches during development
- Recommends application of ISO/IEC 27001/27002 controls to protect from unauthorized access, corruption or disclosure of source code, configuration files, authenticators, design information, test results …

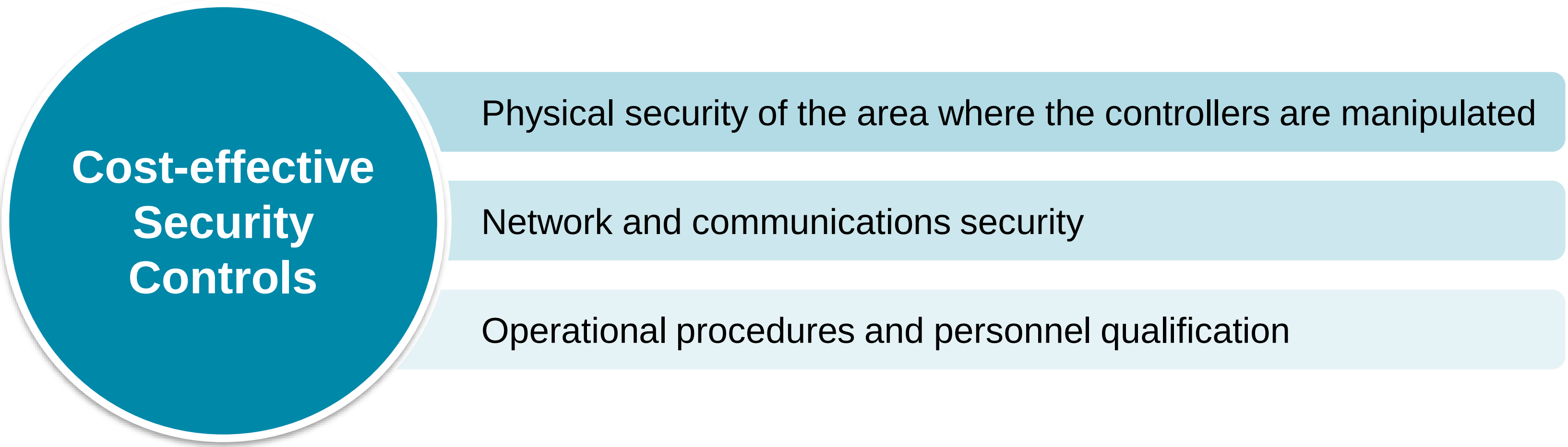
Product security IT Security	• Definition of appropriate security measures
IT Security	• Implementation of the technical controls
Business Unit	• Classification of assets based on their business value (sensitivity and criticality)

Secure Manufacturing



Provisioning of certificates or injection of secrets in the electronic controllers

- Security controls to avoid compromise of sensitive items and issuing to counterfeited parts
- Additional steps and controls in the manufacturing process → more time and higher cost per unit



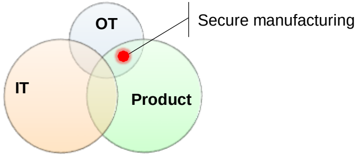
Cost-effective Security Controls

Physical security of the area where the controllers are manipulated

Network and communications security

Operational procedures and personnel qualification

Secure Manufacturing



What if your EMS supplier is going to provision the devices?

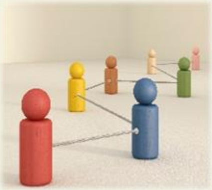
Supply chain management

- Transversal to the three domains, addressed in ISO/IEC 27000 family and ISA/IEC 62443 series
- Cybersecurity risk management measure required in NIS2
- Product security defines requirements for the suppliers, but other functions like legal, data protection, purchasing and information security also have responsibilities in this process

Takeaways

Product security cannot be a silo

- Overlaps with IT and OT domains
- Cross-references among cybersecurity standards
- Impact of regulatory framework



Establish and maintain relationships with other groups and functions in the organization:

- Human resources, development, legal, quality assurance, compliance, data privacy, insurance …

The better these relationships are,
the better the product security management program will look like!

Thank you very much for your attention!

Knorr-Bremse RVS
CoC Product Cybersecurity – R/DPC
Lola Fernández

Mobile: +41 79 243 89 42
Email: Lola.FernandezGonzalez@knorr-bremse.com
www.knorr-bremse.com

BACK UP

Abbreviations

CI/CD	Continuous Integration and Continuous Delivery (or Deployment)
CRA	Cyber Resilience Act
DMZ	Demilitarized Zone
EMS	Electronics Manufacturing Service
ERP	Enterprise Resource Planning
hEN	Harmonized European Norm (standard)
IACS	Industrial Automation and Control System
IACS SP	Industrial Automation and Control System Security Program
IDE	Integrated Development Environment
ISMS	Information Security Management System
IT	Information Technology
OT	Operational Technology
RED	Radio Equipment Directive
SDL	Secure Development Lifecycle
SM	Security Management (practice in ISA/IEC 62443-4-1)
SP	Security Program
XaaS	Anything as a Service