Security-By-Design Quale potrebbe essere lo standard di riferimento in ambito ferroviario?

Prof. Massimo Ficco

Università degli Studi della Campania Luigi Vanvitelli

massimo.ficco@unicampania.it

Security-by-Design

- Approach to System Engineering which takes into account security requirements and measures to protect ICT assets during the whole engineering process

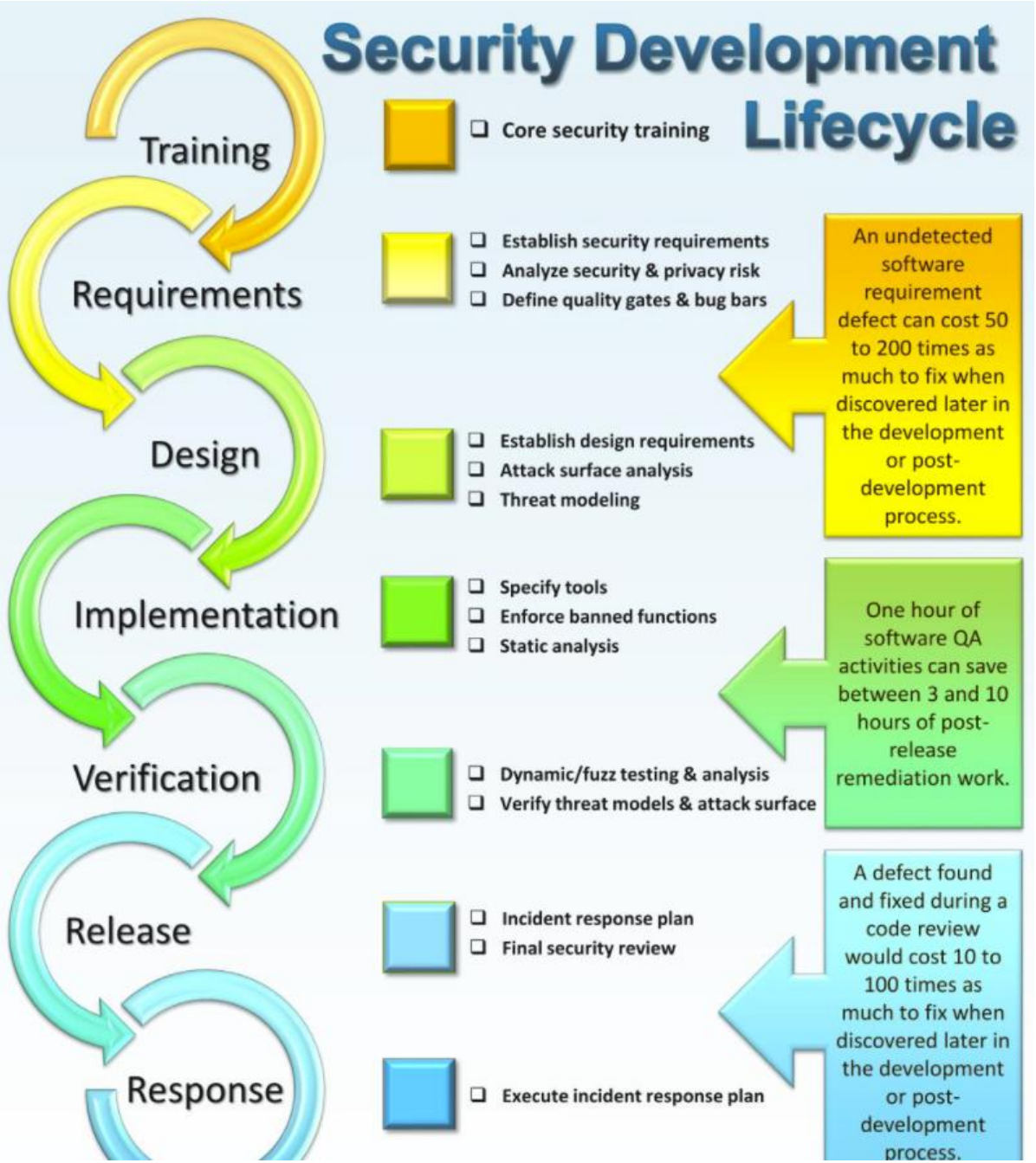
- Minimize the number of security vulnerabilities in design, implementation and deployment
  - Identify and remove vulnerability in the development lifecycle as early as possible

Secure Development Lifecycle (SDL)

SDL – Used along with traditional/current system development techniques in order to introduce security at every stage of system development

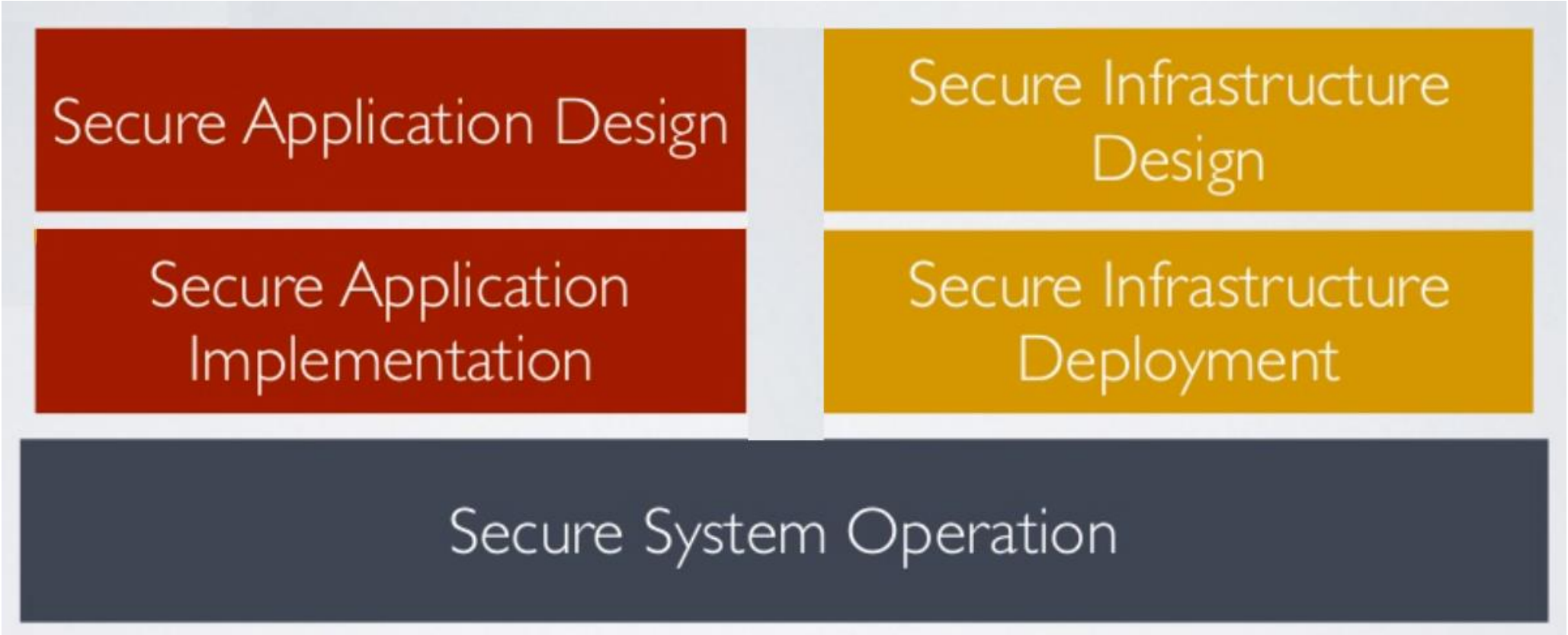
Three essential components:

- *Engineer Education*
- *Repeatable process*
- *Metrics and Accountability*

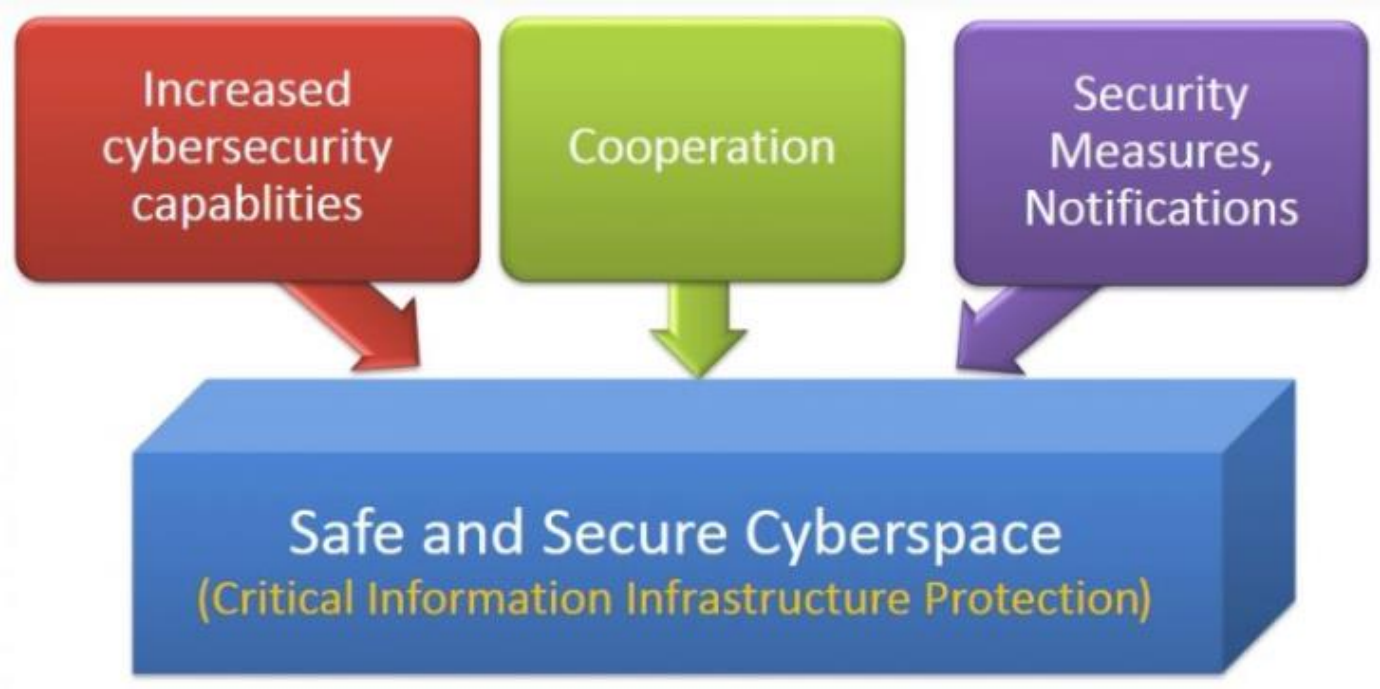


Development process

- Consider security
  - At the start of the process
  - Troughout development
  - Through deplyment
  - At all system review milestones



NIS Directive



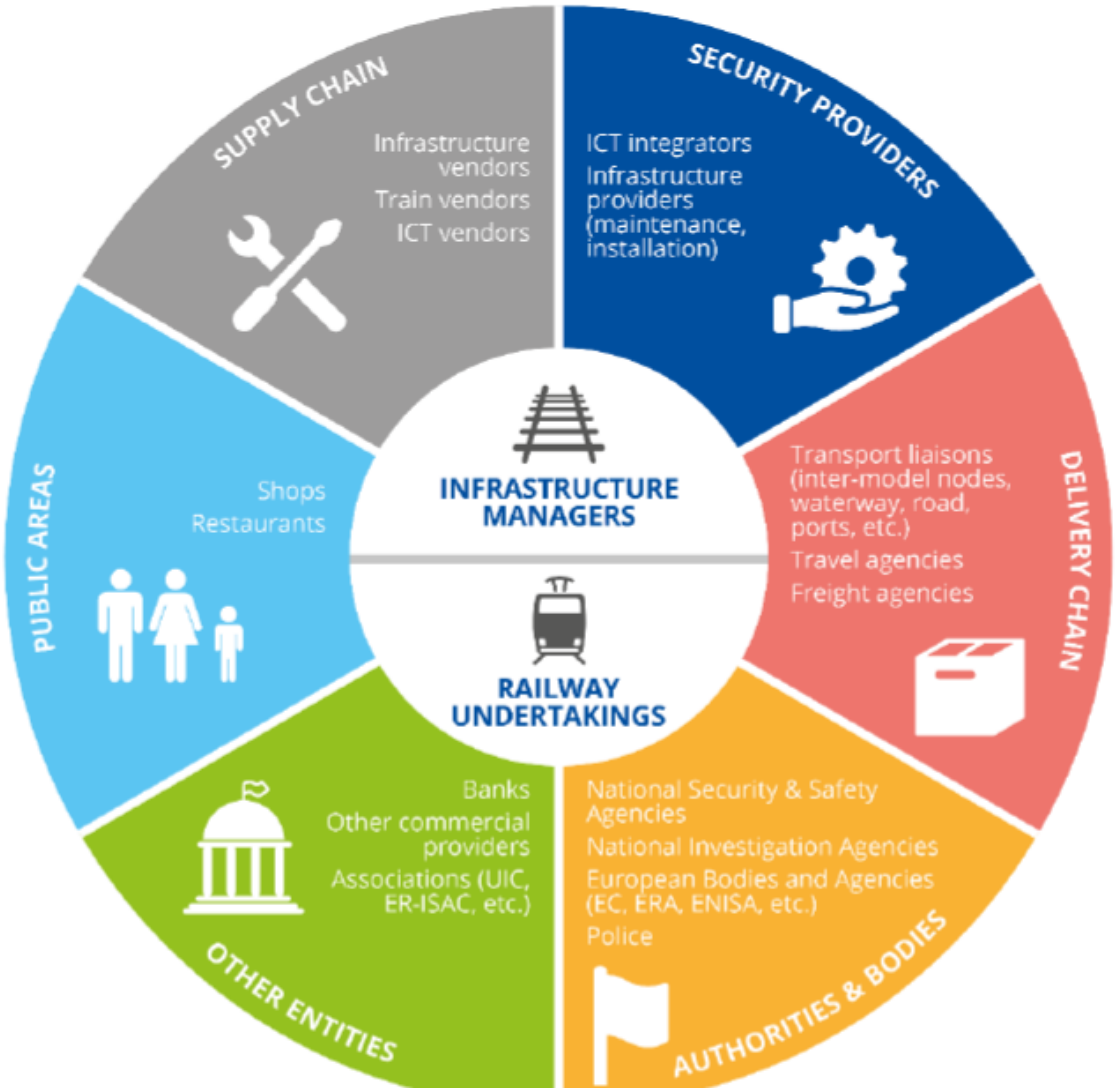
- As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive [1], which includes three parts:
  - **1. National capabilities:** EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.
  - **2. Cross-border collaboration:** Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.
  - **3. National supervision of critical sectors:** EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, …), ex-post supervision for critical digital service providers (online marketplaces, cloud,..)

Directive 2016/1148 (NIS Directive) is the first legislative document focusing on cybersecurity, extending the scope also to the railway sector

[1] the EU Network and Information Security directive: https://www.enisa.europa.eu/topics/nis-directive

Security measures in the Railway Transport Sector

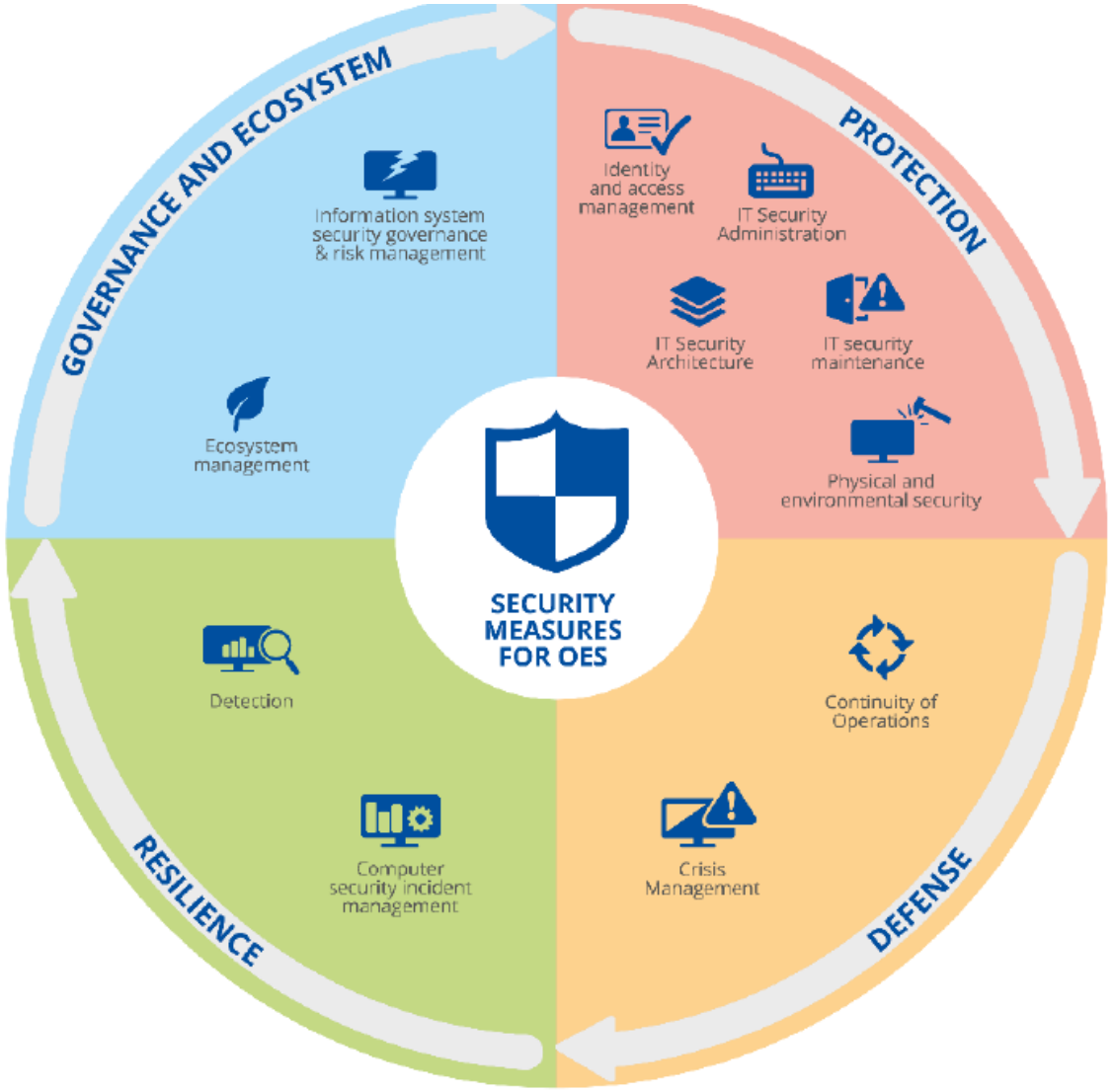
- The study regards the level of implementation of cybersecurity measures in the railway sector, within the context of the enforcement of the NIS Directive in each European Member State [2]
- The stakeholders involved in the scope of this study are European infrastructure managers (IM) and railway undertakings (RU).



[2] ENISA Report, NOV. 2020, RAILWAY CYBERSECURITY, Security measures in the Railway Transport Sector

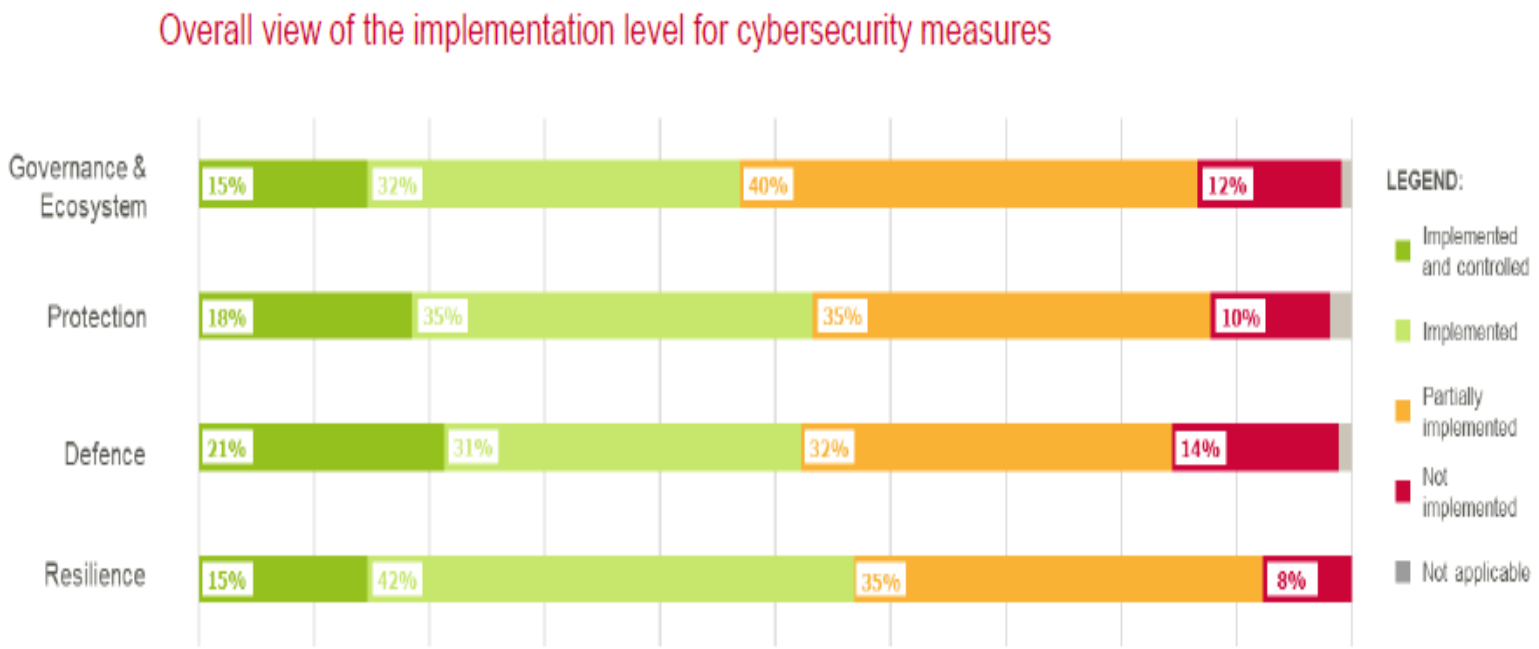
CYBERSECURITY CHALLENGES

- Low digital and cybersecurity awareness in the railway sector;
- Difficulty in reconciling safety and cybersecurity worlds;
- Geographic spread of railway infrastructure and the existence of legacy systems;
- Digital transformation of railway core business;
- Dependence on the supply chain for cybersecurity;
- The need to balance security, competiveness and operational efficiency;
- Complexity of regulations for cybersecurity;
- Finally, the security measures promoted by the NIS Directive are not at present specific to each sector.



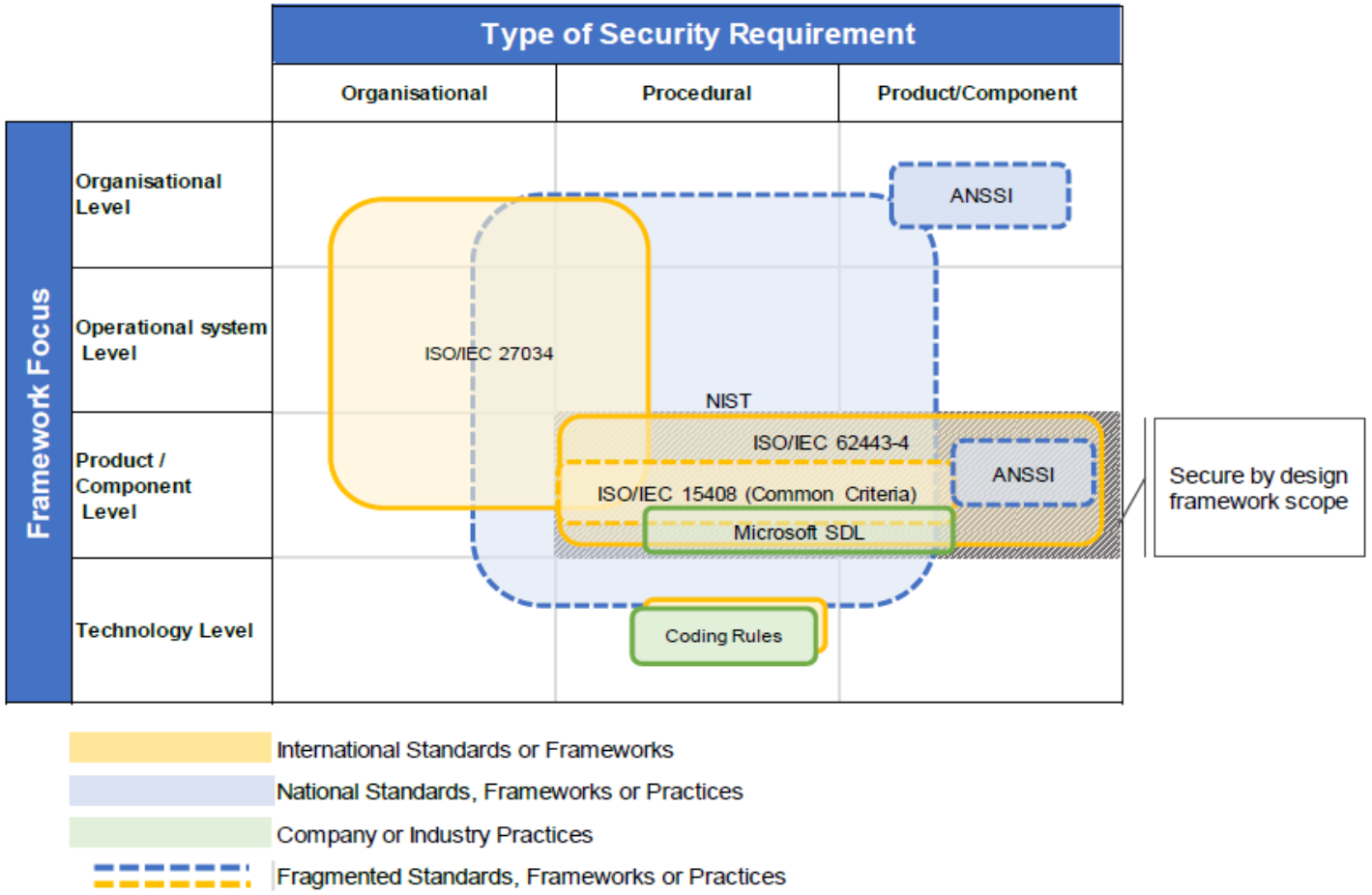
MINIMUM SECURITY MEASURES

- The security measures examined in the survey were defined by the NIS Directive Cooperation Group.
- They have been classified in 4 domains, and 29 security measures as depicted in the figure below.

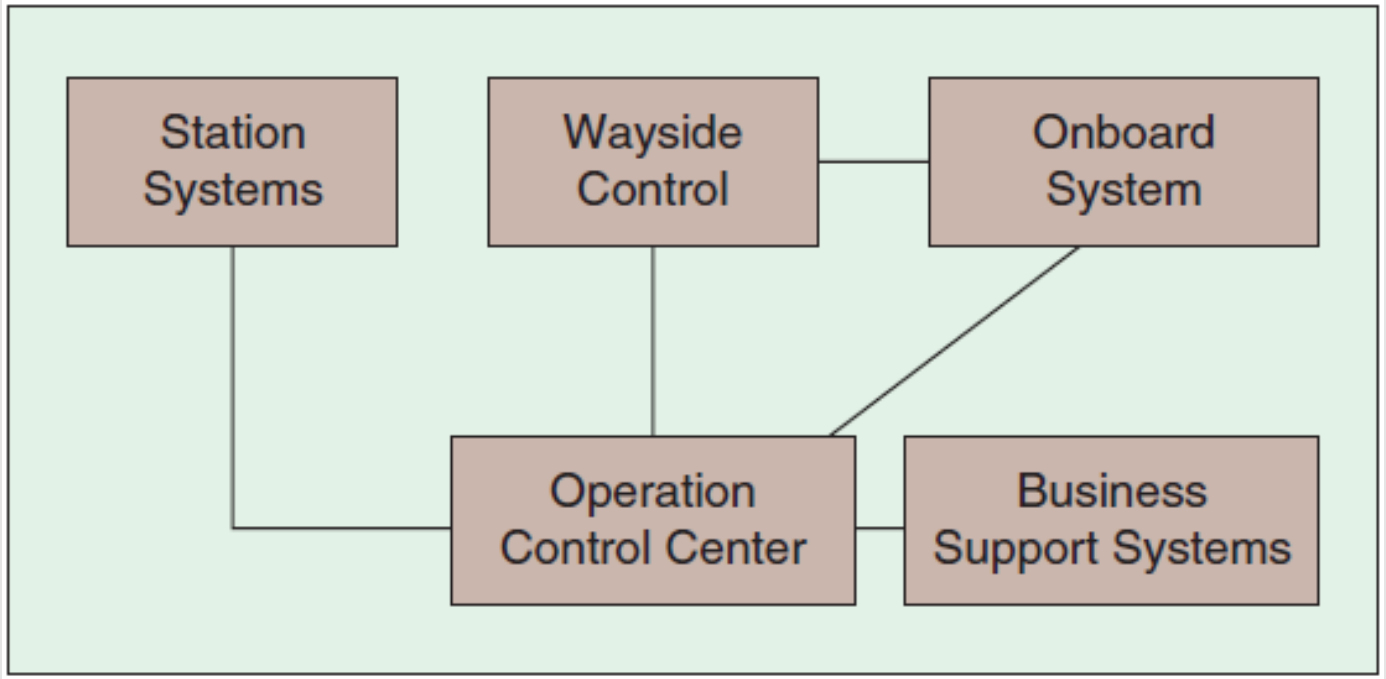


Overview on security standards and frameworks

- Frameworks operate on different levels and may provide guidance for different aspects within an organisation.
- A standard or framework provides guidance in the form of requirements for an organization or user.



Challenges of Adopting Security Standard in Safety-Critical Transportation Systems



The general modules of railway infrastructure.

1. The standards are not designed with consideration for the entire transportation infrastructure, so they often contradict each other or leave gaps;
2. Standards do not seem to be flexible, i.e., it is very difficult to implement the same solution in different modules.
3. Professionals who develop railway safety modules are often not aware of the security issues/standards, so if any security technique is implemented, it is more than likely done after the development of the system or module.
   - Any hardware or software that performs critical functions needs to be safety certified, and if security modules are included, it is very difficult to achieve the certification, since the modules are not designed with respect to safety standards.
   - Even if the safety certification is achieved with a security system included, there is another issue: new cyberthreats appear daily, so security modules need to be updated to ensure protection. But if any change is applied to a safety-certified system, it must then be recertified.

Cybersecurity—The Forgotten Issue in Railways: Security Can Be Woven into Safety Designs February 2018, IEEE Vehicular Technology Magazine PP(99):1-1

Shift2Rail Joint Undertaking

- The **Shift2Rail Joint Undertaking** was launched under the Horizon 2020 programme to seek focused research and innovation (R&I) and market-driven solutions and promote competitiveness in the European railway industry.
- The initiative included cybersecurity issues in the railway sector, for example, under the CYRAIL (CYbersecurity in the RAILway sector) project [3], or under the X2Rail-1 [4] project and X2Rail-3 [5] projects which included cybersecurity work packages.

[3] CYbersecurity in the RAILway sector, https://cyrail.eu/
[4] X2Rail-1, Start-up activities for Advanced Signalling and Automation Systems, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1
[5] X2Rail-3, Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

CYRAIL - CYbersecurity in the RAILway sector

- An analysis of threats targeting Railway infrastructures will be developed as well as innovative, attack detection and alerting technique;
- Adapted mitigation plans and countermeasures will be defined, taking into account their potential impact on operations;
- Protection Profiles for railway control and signalling applications will be delivered to ensure security by design of new rail infrastructures.

Selection of the ‘Secure-by-design’ standard”

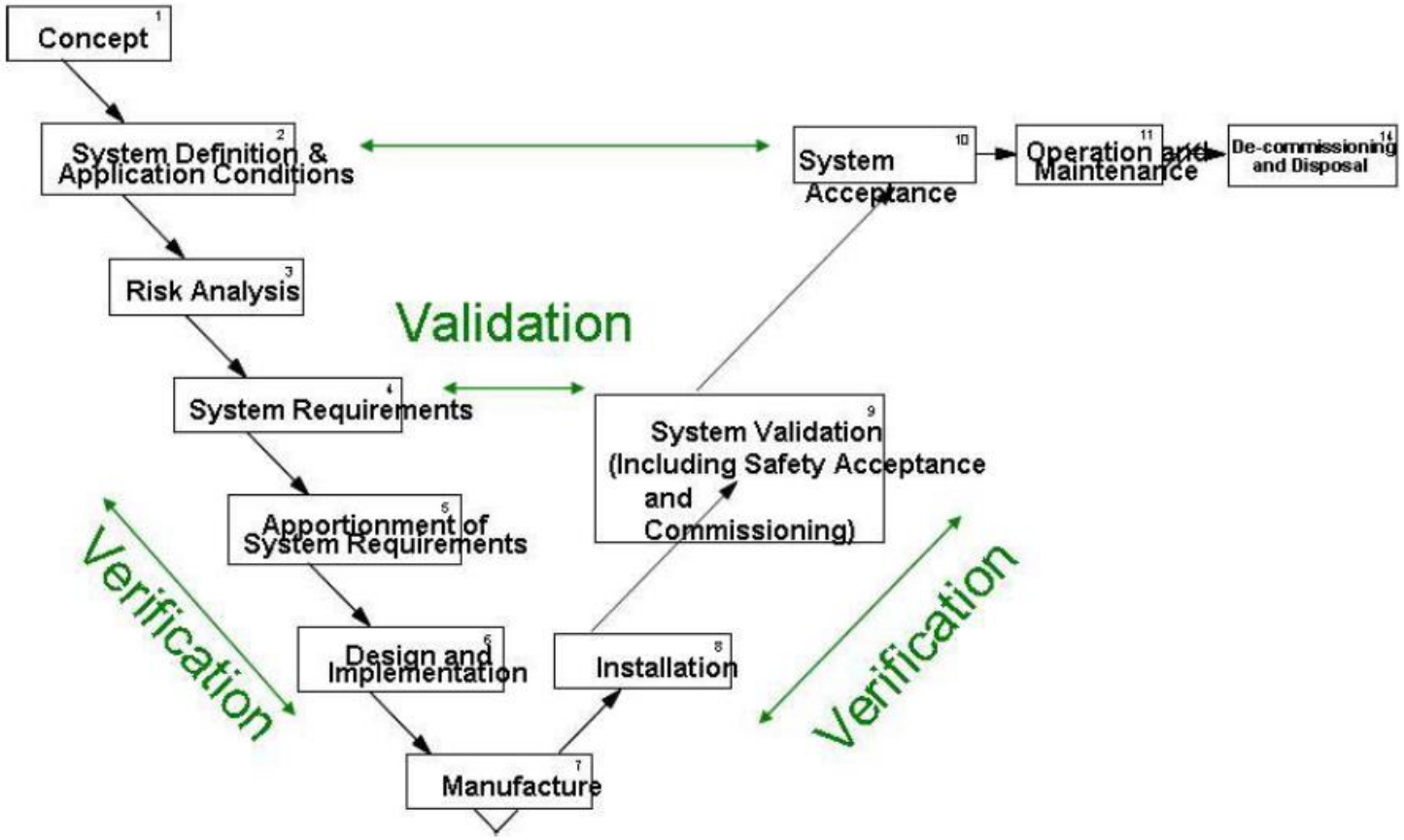
X2Rail-1: Start-up activities for Advanced Signalling and Automation Systems (GA No 730640)

- This memo describes the process for the choice of the “secure-by-design” standard framework by evaluating some of the most common standards, guidelines and best practices in cyber-security from several international and national organisms, putting special emphasis onto industry-oriented publications.

- The choice of the standard framework resulting from this analysis will be used as basis for railway dedicated secure-by-design standard that may be amended to take into account railway specific aspects (e.g., safety, life-cycle, etc.) during the development of railway components.

Evaluation Criteria

The product life-cycle considered for this evaluation and the definition of evaluation criteria.



V-Model from railway international standard EN50126. © CENELEC

Evaluation criteria coverage overview on candidate standards

The criteria aim to set out key requirements on different technical and organizational aspects and for different stakeholder, that act as a guidance throughout the selection of a secure-by-design standard.

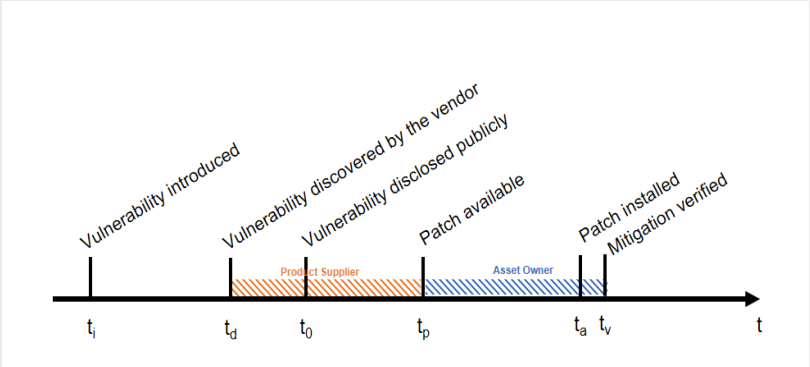
Criteria	ISA/IEC 62443-4	ISO 15408 (CC)	ISO/IEC 27034	NIST	ANSSI	Microsoft SDL	Coding Rules
Design and Development	OK	OK	OK	OK	High-level	Partial	NOK
Verification and validation	OK	OK	OK	OK	Partial	Partial	Partial
Security level	OK	High-level	NOK	OK	OK	Partial	NOK
Maturity level	OK	OK	NOK	High-level	NOK	Partial	NOK
Defence in depth	OK	OK	OK	OK	OK	Partial	NOK
Security defect management	OK	OK	OK	OK	OK	Partial	NOK
Patch management	OK	OK	OK	OK	OK	Partial	NOK
Security assessment	OK	OK	OK	OK	OK	Partial	NOK
Guideline/documentation	OK	OK	OK	OK	OK	OK	OK
System integration and use	OK	OK	OK	OK	NOK	Partial	NOK
Technological watch	OK	Partial	OK	OK	OK	OK	OK
Protection profile	OK	OK	NOK	High Level	OK	NOK	Partial
Product lifecycle	OK	OK	Partial	OK	NOK	Partial	NOK

Use cases

The overall aim of X2Rail-1 WP8 Cyber Security is to identify and specify a Cyber Security Framework applicable for railways. The framework shall cover the different stakeholders and needs from the railway industry.

In order to cover a wide spectrum of the ISA/IEC 62443, two different approaches are proposed:

- A top-down approach that aims at analysing how new cybersecurity requirements from the asset owner could impact the component secure development;
- A bottom-up approach that aims at identifying how the component security requirements are linked to the cybersecurity needs from the asset owner and the system integrator.



Conclusions

- There are general and specific standards for achieving the desired safety level of an electronic module that will be used in railways. But in cybersecurity, there are only recommendations to follow and general norms, which means that each manufacturer has its own criteria for following or not following the standards.
- It is very difficult to reach an optimum level of security because the norms recommend different things, and if a manufacturer achieves an acceptable security level in one module, it is very complicated to apply the same solution to other modules.

- ***The ideal solution for safety and security issues is to create a standard that includes both areas and have all manufacturers follow it.***