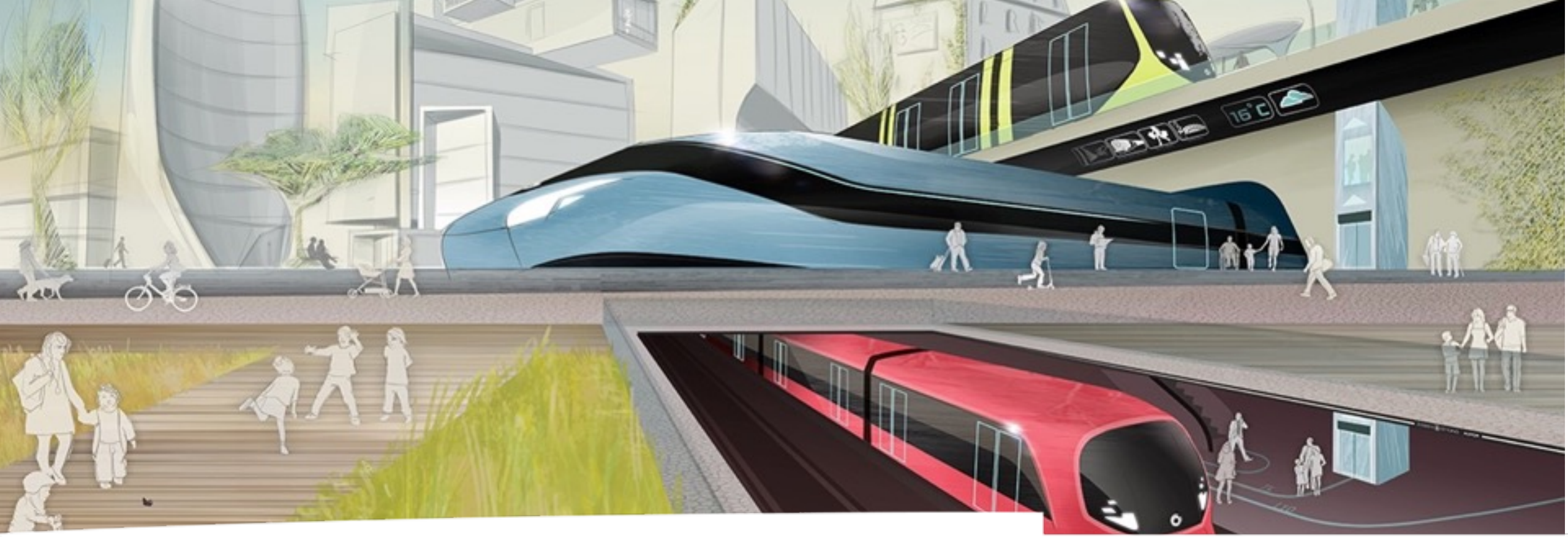


On the way of a common cyber security approach dedicated to Railways

27 November 2017

Shift2Rail

X2RAIL 1

ALSTOM
Designing fluidity

Francois Hausman

francois.hausman@alstomgroup.com

Alstom Mainline cyberdefense manager

Shift2Rail cybersecurity WP leader

CEB, CENELEC, UNIFE

Francois Hausman, having an experience of 18 years in railway signalling, is currently Mainline cyberdefense manager for Alstom in charge of the definition of the cyber security solutions for the mainline portfolios.

Since 2015, he is leading the Shift2Rail work package dedicated to the definition of common approaches and solutions for railway cybersecurity.

Cyber threats on railway

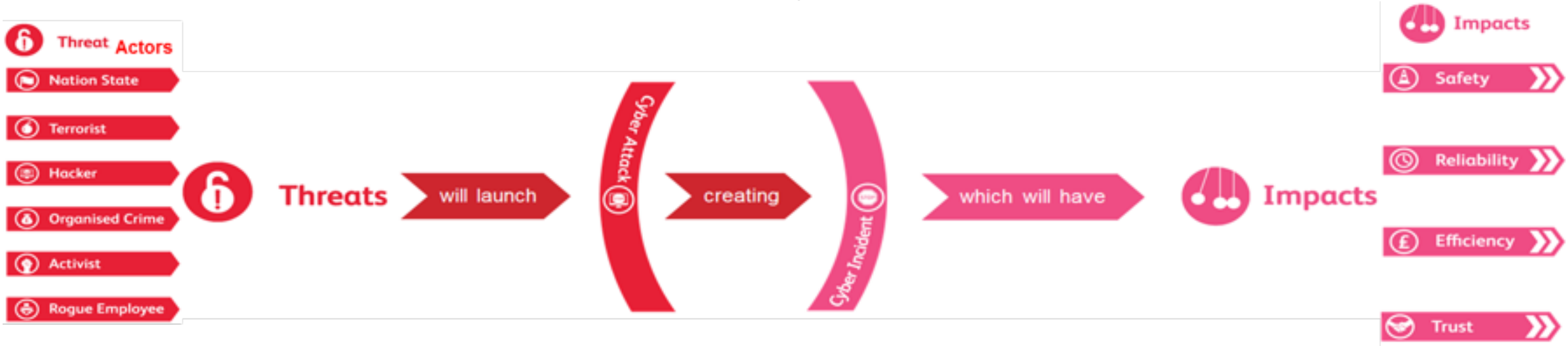
Evolution of cyber threats on railway

- Until recently, Industrial Automated Control Systems (IACS) were considered isolated from external influence ⇒ immune to security threats and attacks
- This is no longer a reality:
  - Digitalisation of most of the systems (electro-mechanical to digital IP-enabled technology)
  - Connections between operational and business railway areas
  - Railway systems more and more interconnected: ERTMS, ETCS, GSM(R), ATO, Electrification, Intelligent Transport System
  - Significant increase of the cyber attacks on ICS (more than 600% between 2012 and 2014 (source:IBM))
  - IACS cyber attacks with severe financial and safety impacts are continuously reported

Cyber threats on railway

Railway specificities

- Railway specificities:
  - ✓Distributed aspect: electronic components scattered along track or train
  - ✓Heterogeneous aspect of railway network
  - ✓Very long life cycle (>25 years)
  - ✓High level of certification for safety related systems
  - ✓Diversity of supply chain and of technology
  - ✓Small to medium volume production for railway components



Objective of S2R cyber security WP

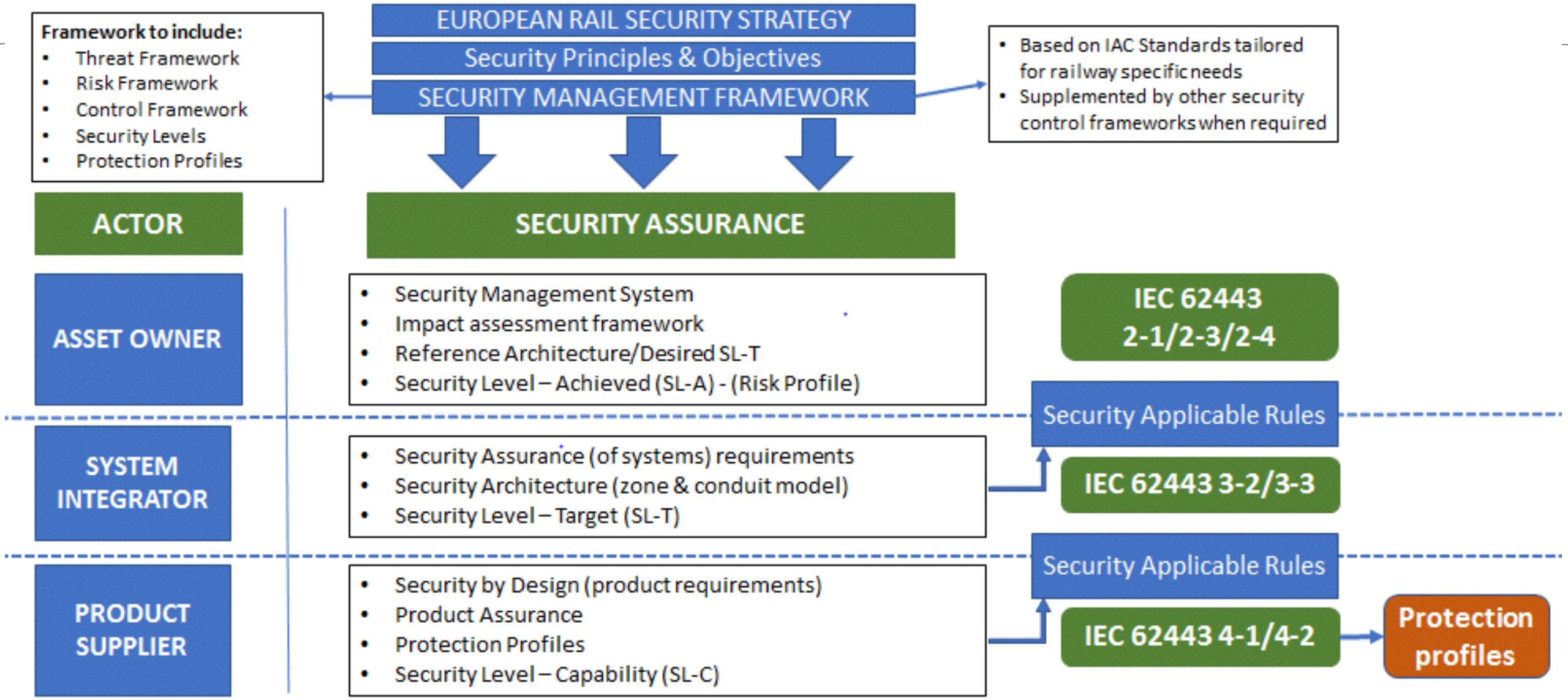
- Brought together key European railway stakeholders from suppliers, integrators, infrastructure managers and operating companies to define how different aspects of cyber security should be applied in an harmonised way to the railway sector.
- This includes definition of common approaches for :
  - ✓Security assessment process
  - ✓Security assurance and “secure by design” processes
  - ✓“Defense in depth” implementation
  - ✓“Defense in breadth” process to secure system at each stage of its life cycle
  - ✓Secure integration at system level through definition of component protection profiles

Cyber security standard for railway

Applicable Standards and Rationale for Selection

- Standard cybersecurity framework for railway
  - Multiple standards assessed
  - IEC 62443 selected
- Rationale:
  - Set of standards dedicated to Industrial Automation Control Systems (IACSs)
  - Define and encompass expectations, responsibilities and duties for all stakeholders
  - Address product and system life cycles
  - Cover security risk assessment processes
  - Define security levels based on functional security requirements
  - Used by other critical infrastructures
  - Approach compliant with definition of protection profiles

Cyber security standard for railway: IEC 62443

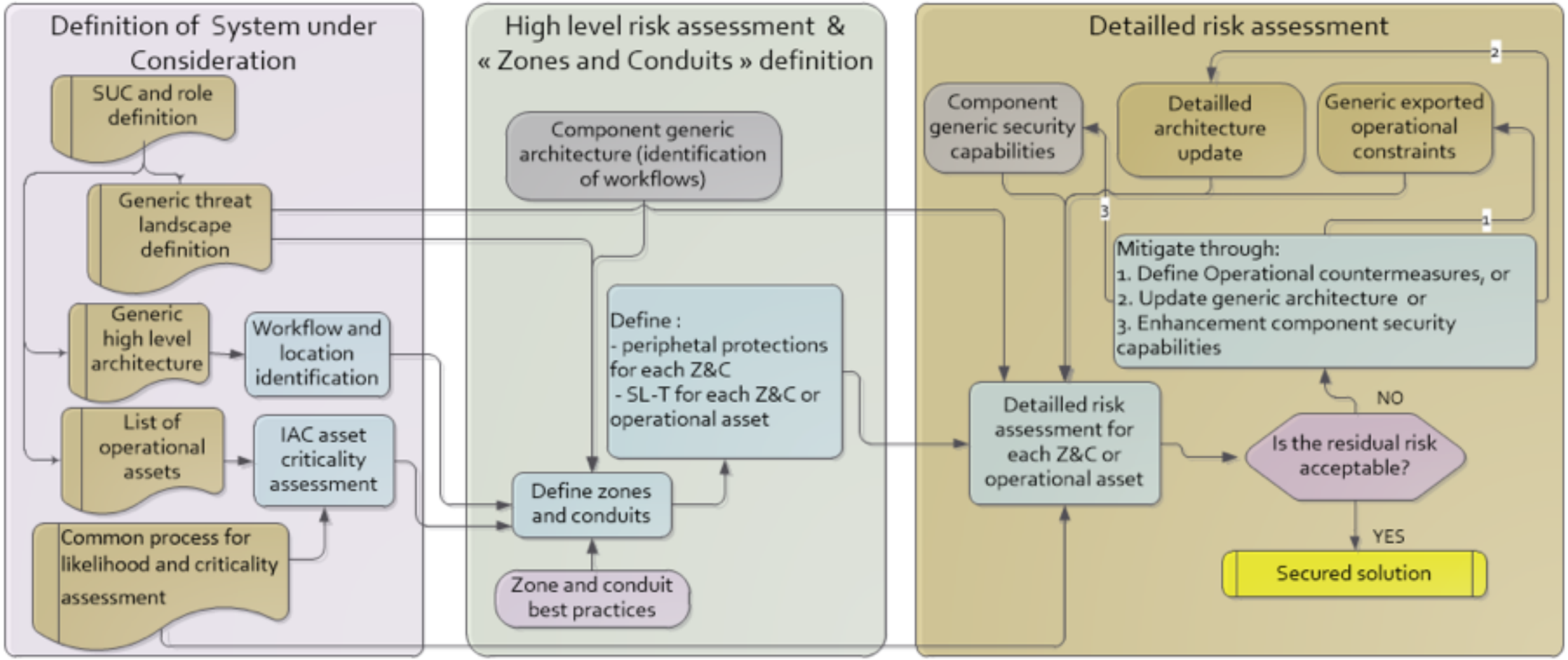


Security risk assessment

Methodology

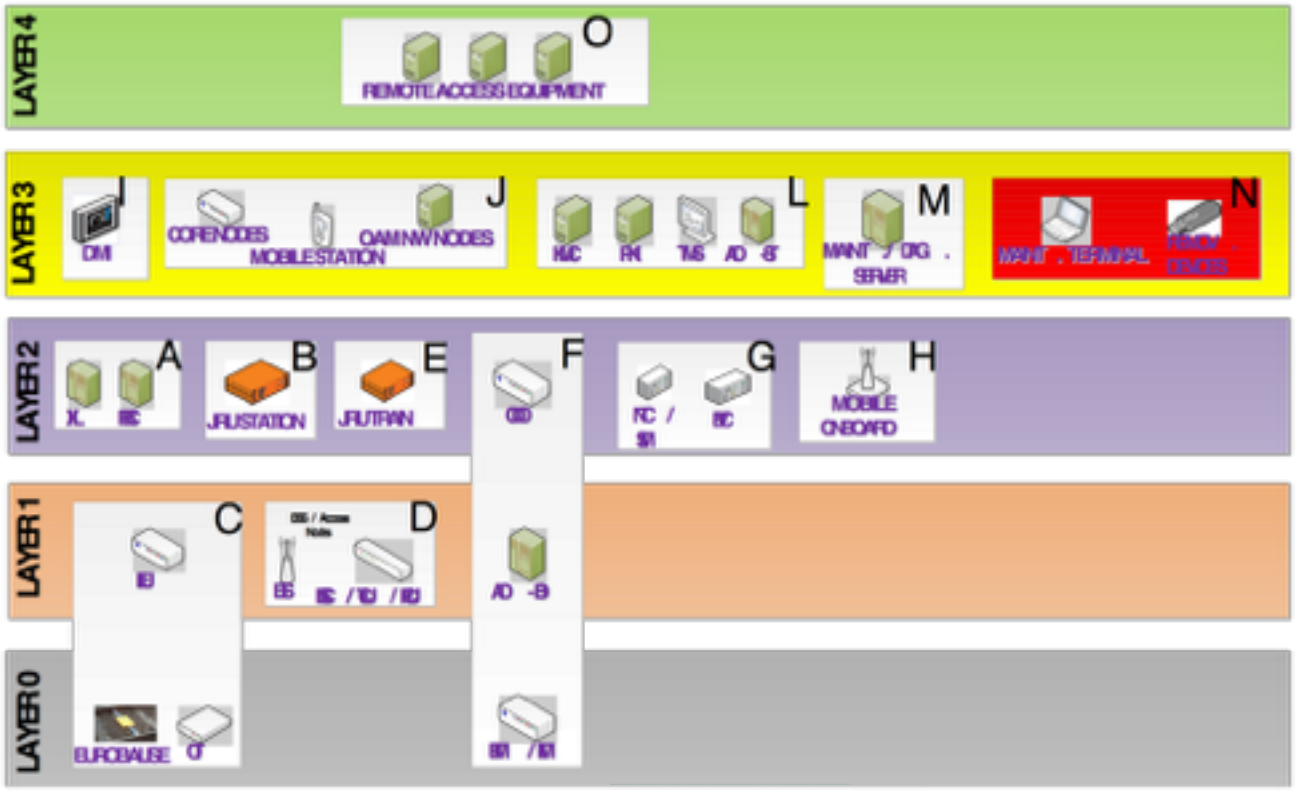
- Risk assessments allow asset owners to understand:
  - ✓the criticality of specific assets
  - ✓the appropriate protection measures that need to be applied
- 3 steps IEC 62443 3-2 risk assessment:
  - ✓Define System under Consideration (SuC)
  - ✓High level risk assessment
  - ✓Detailed risk assessment
- High-level risk assessment :
  - ✓Identify worst case unmitigated risk
  - ✓Define reference architecture and “Zones and Conduits”
  - ✓Allocate Security Level Target to each zone and conduit
- Detailed risk assessment:
  - ✓Analyse impact of each threat for each zone, conduit and/or asset for each IAC property
  - ✓Identify potential mitigations if residual risk not tolerable

Security risk assessment



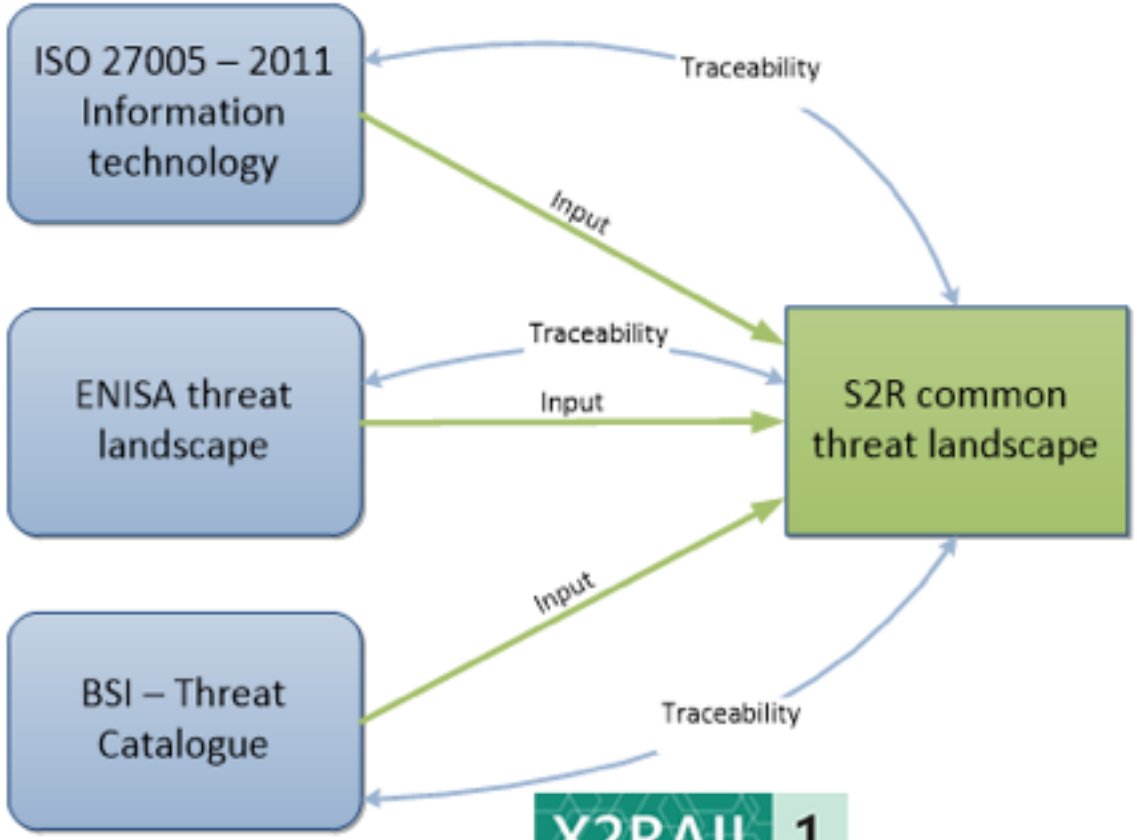
Reference architecture

- Criticality of reference architecture
  - Threat impact assessment needs a clear image of asset interconnections, location and dataflows.
  - Allows clear threat impact assessment and countermeasure allocation for each component
  - Architecture could be logical and /or geographical



Common threat landscape

- A common threat taxonomy allows a standardised classification of threats that will be used as a baseline reference
- S2R threat landscape reference:



Security by design

Why it is important for Railway

- “security by design” encompasses a framework of good design principles, patterns, processes, functional requirements, … that enables to design, build and maintain components with security implicitly considered in each stage of the development, resulting in a product that is – secure by its design.
- “security by design” contributes to improving a system’s security footprint and helps to increase the robustness against most of today’s and future security pitfalls.
- Importance of such approach for railway specific components with:
  - A life cycle > 25 years
  - A high level of certification
  - Very binding update process

⇒ “Security by design” is a key building block for establishing and assuring security capabilities in the future Railway Security Architecture

Security by design

Objectives

- Objectives of « security by design » process :
  - ✓Define a common and shared framework of requirements and processes for development, validation, deployment and maintenance of railway component security functions
  - ✓Ensure **defence-in-depth** principles are followed
  - ✓Ensure a **systematic approach to assess and manage security defects** during lifecycle
  - ✓Ensure **clear** requirements and **responsibilities among stakeholders**
  - ✓Ensure a **systematic** approach to assess the **quality assurance level**
  - ✓Allow **definition of several security levels** depending on the level of protection required by the system

Protection profile: objectives and content

- Protection profile objectives:
  - ✓Based on generic architecture, have a common threat impact assessment at component level
  - ✓Define a generic security framework for each component of a zone consistent with the zone security level target
  - ✓Ensure that the system Security Level Target is fulfilled after integration of the components compliant with the agreed protection profiles
- The definition of the protection profile requires to:
  - ✓Define the context of use/operation
  - ✓Identify the sub-system borders/interfaces
  - ✓Identify the subset of applicable threats
  - ✓Specify the high level security objectives and requirements
  - ✓Specify the required security level for each security objective

Conclusion

- Shift2Rail cyber security work stream aims at defining a **consistent cyber security approach** shared by **all railway stakeholders** taking into account the **railway requirements and specificities** to deliver a safe and secure system during the complete system life cycle.
- Benefits from this common approach:
  - Common understanding of risks, threats and security mitigations
  - Definition of clear interfaces between all stakeholders
  - Reduction of time and cost to market through the definition of generic reference protection profile for each component
  - Ensure the system security level target during its complete life cycle

Shift2Rail

X2RAIL 1

ALSTOM
Designing fluidity