Applying the CRA in rail: A sector-wide approach

KEY GUIDANCE FROM THE CYBERSECURITY RAIL SECTOR GROUP

Amelia Alder

Quentin Rivette

The Cybersecurity Rail Sector Group

- A joint group of the **Railway Operating Community**, the **Rail Supply Industry** and **Urban Rail**
- Teaming up as a **unified sector** to improve cybersecurity for rail in Europe
- An initiative planned **to go beyond** (more than 20 other topics identified)

Expert guidance on the implementation of the CRA in railways

- A common understanding of requirements and implementation approach
- System-level approach and progressivity
- A living document

Still under discussion and pending approval by the sector

Key aspects of the guidance

Contextualisation and precisions on key concepts:

- **Spare Parts** are excluded from CRA application
- **Substantial Modifications** trigger the need to comply with the CRA
- **Tailor-Made vs COTS:** Tailor-Made products are allowed non-secure configurations and chargeable patches

Combination with existing parts and in-progress projects:

- How to apply the CRA with **system-level** approach
- **Progressivity** for components within a system: **priority to the new/redesigned & Cyber-Critical Assets** (CCA – IEC 63452)
- System Extension (adding a new section to a line, adding a new coach to a train, …) managed at the **interface**

Responsibility and mutual agreement:

- **Accountability** for demonstration of CRA compliance and CE marking belongs to the Manufacturer
- Earliest **transparency** (status, criteria, risk acceptability, SecRACs, …) achieved via **mutual agreement with the customer (asset owner)**

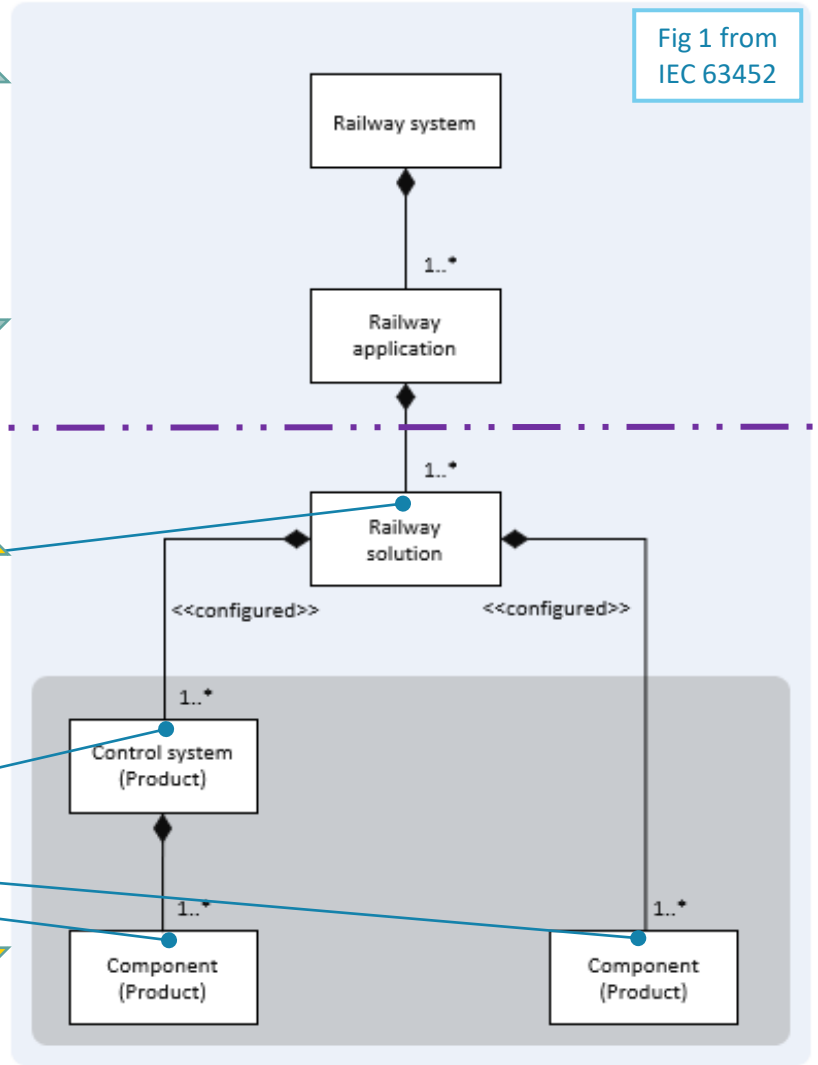
What is a product? Application of the CRA to rail products

CRA product in operation under the NIS2 directive, including organisation (supply chain, incident management…)

NIS2

CRA

- **Systems** (interlocking, rolling stock, …)
- **Sub-Systems** (RBC, TCMS, platform screen doors, …)
- **Set of components** (CCTV, door system control, …)
- **Component** (switch, router, PLC, IHM, sensors, camera, recorder…)



OPERATOR

RAILWAY CYBERSECURITY IEC 63452

SYSTEM INTEGRATOR

RAILWAY CYBERSECURITY IEC 63452 · Europe's Rail

PRODUCT SUPPLIER

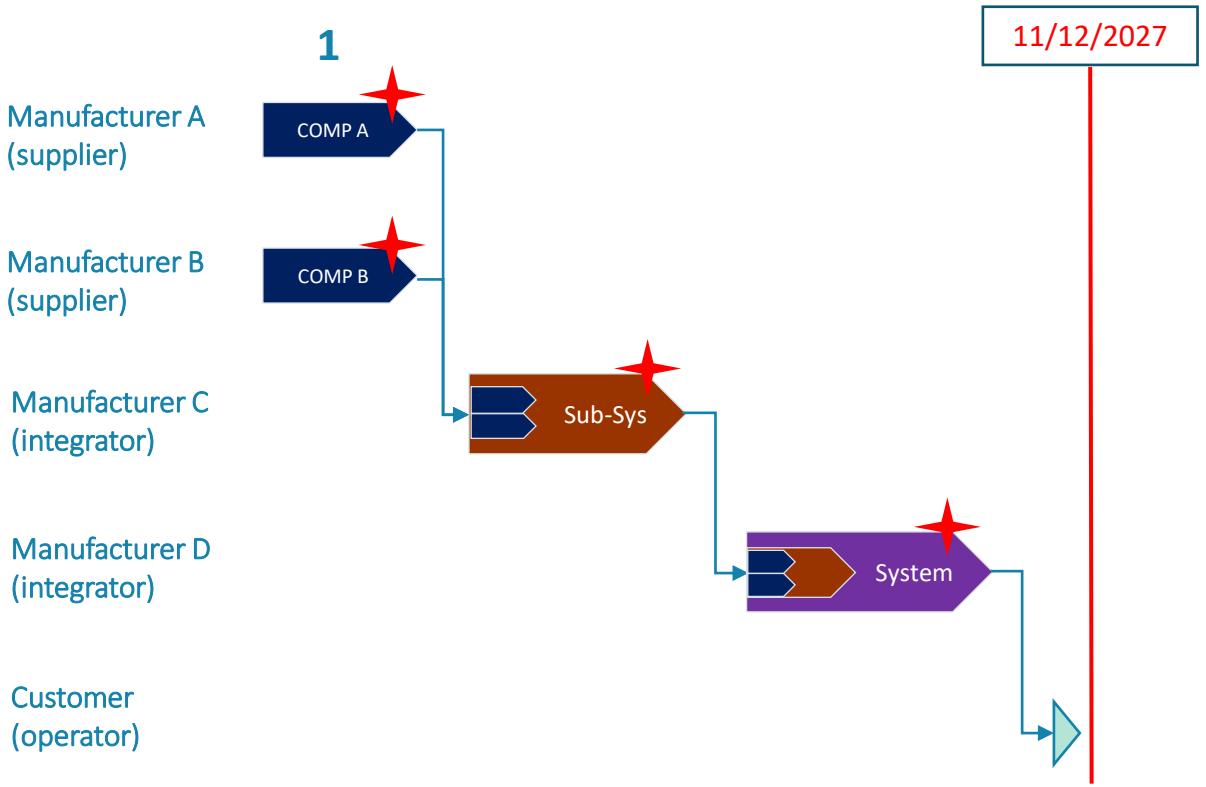
Europe's Rail · IEC 62443 INTERNATIONAL STANDARD

RAILWAY CYBERSECURITY IEC 63452

Europe's Rail

IEC 62443 INTERNATIONAL STANDARD

Ongoing Projects: Progressivity and Prioritisation



Example 1:
Components, Subsystems and the System are all made available on the market before 11/12/2027:
CRA compliance <u>not required</u>

CRA compliance not required, pre-existing component, subsystem or system.

Initial baseline

CRA compliance "on the basis of the (system) risk assessment" May be used "as is" or with additional mitigating measures (inside or around in the sub-system architecture) => conditions of use (e.g. SecRACs)

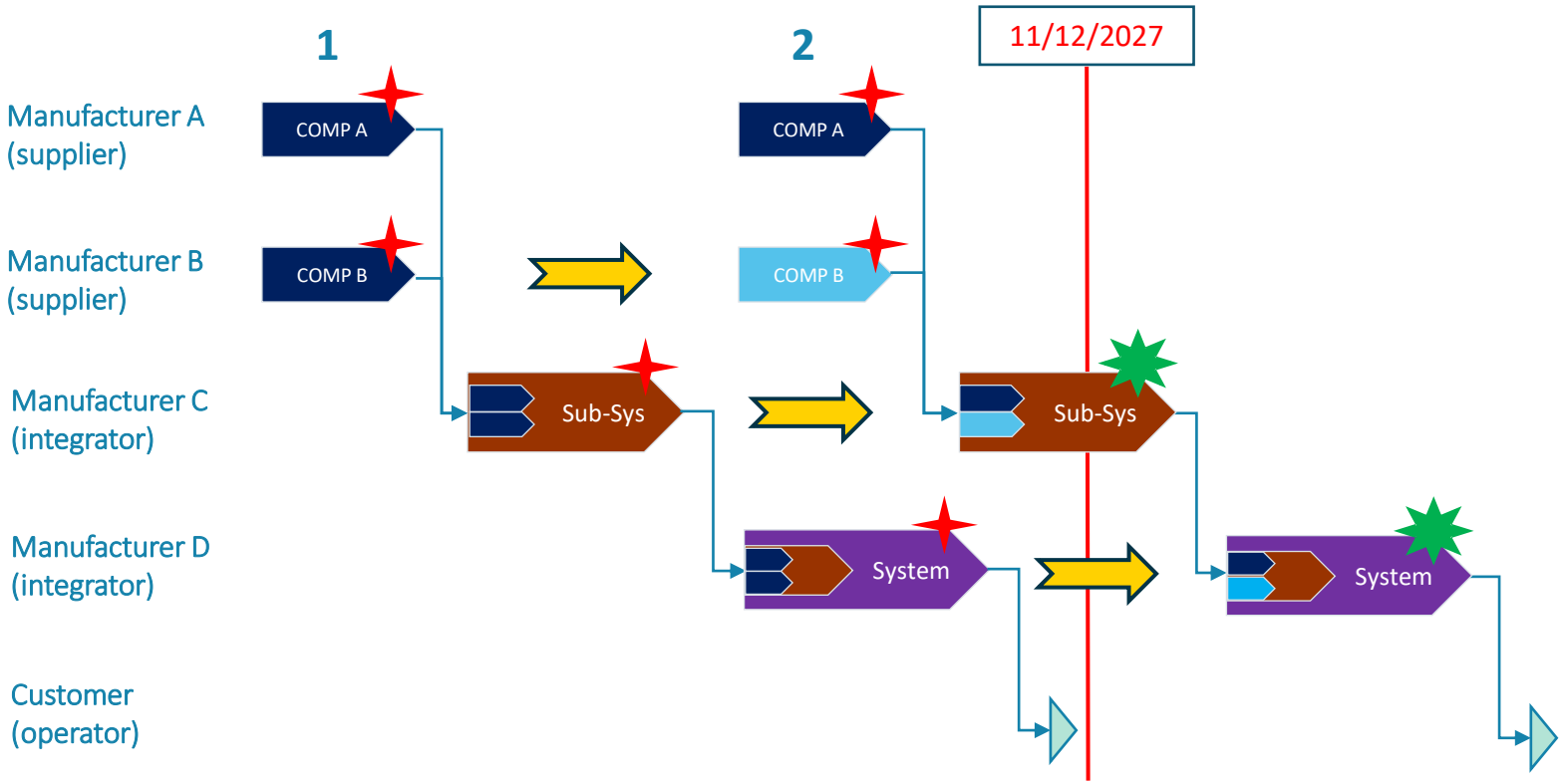
Increase of cybersecurity

New baseline

CRA compliance "by design" Designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity

ALWAYS with acceptable risks at system level

Ongoing Projects: Progressivity and Prioritisation



Example 2: still no need for COMP A and COMP B to be CRA compliant, as they are made available on the market before 11/12/2027.
However, Sub-System and System are delivered after 11/12/2027: **CRA compliance is required for both**

To achieve this, in the example COMP B is adapted to a new baseline that increases cybersecurity. This allows the overall (Sub-)System to achieve compliance at system level (acceptable risk at system level):
Prioritisation for increasing cyber for COMP B

Conversely, COMP A may continue to be used "as is", with additional mitigating measures within it (e.g.: configuration) or around it in the sub-system (better architecture – e.g.: better segregation) to achieve (sub-)system-level CRA compliance
Conditions of use for COMP A must be precised (e.g. SecRACs)

CRA compliance not required, pre-existing component, subsystem or system.

Initial baseline

CRA compliance "on the basis of the (system) risk assessment" May be used "as is" or with additional mitigating measures (inside or around in the sub-system architecture) => conditions of use (e.g. SecRACs)

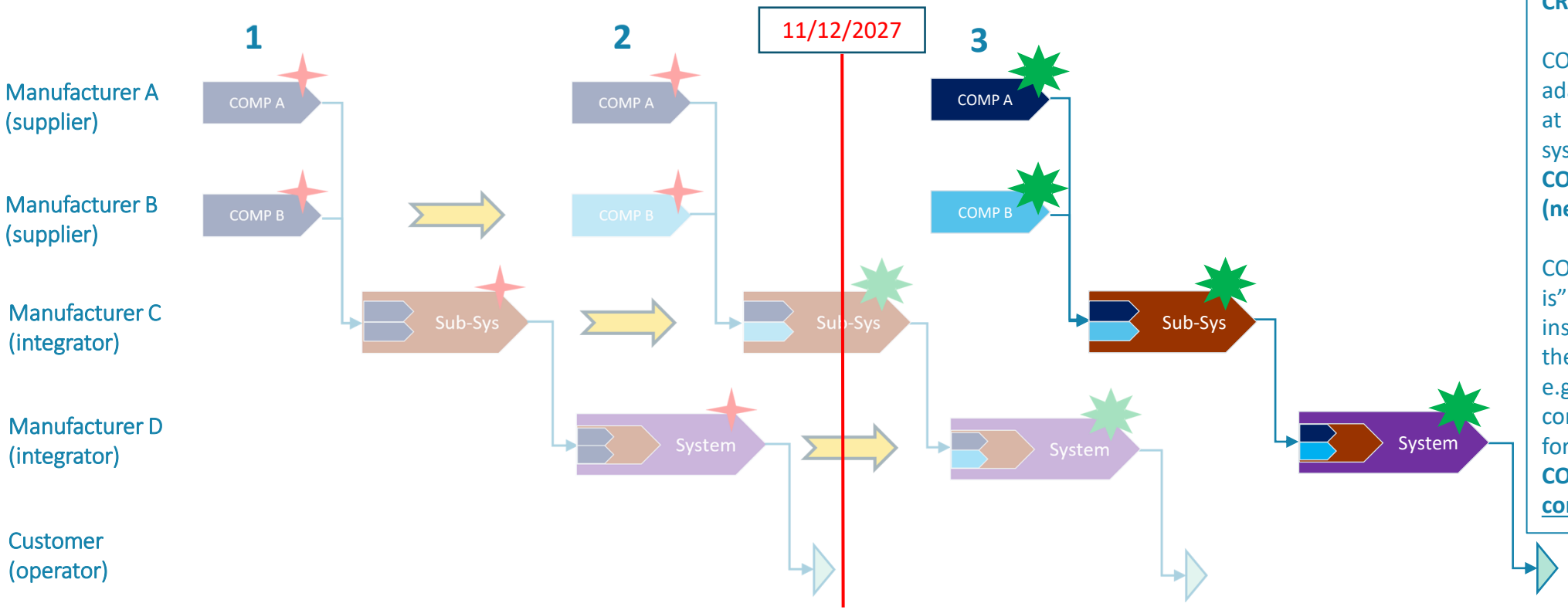
Increase of cybersecurity

New baseline

CRA compliance "by design" Designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity

ALWAYS with acceptable risks at system level

Ongoing Projects: Progressivity and Prioritisation



Example 3: COMP A, COMP B, Sub-System and System are all made available after 11/12/2027:
CRA compliance is required <u>for all</u>

COMP B (new baseline) was already adapted to allow achieving compliance at system level (acceptable risks at system level)
COMP B is CRA compliant <u>by design</u> (new baseline)

COMP A may continue to be used "as is" with additional mitigating measures inside (e.g.: configuration) or around in the sub-system (better architecture – e.g.: better segregation) => these conditions of use needs to be precised for COMP A (e.g. SecRACs)
COMP A is CRA compliant <u>through conditions of use</u> (Annex 2)

CRA compliance not required, pre-existing component, subsystem or system.

Initial baseline

CRA compliance "on the basis of the (system) risk assessment" May be used "as is" or with additional mitigating measures (inside or around in the sub-system architecture) => conditions of use (e.g. SecRACs)

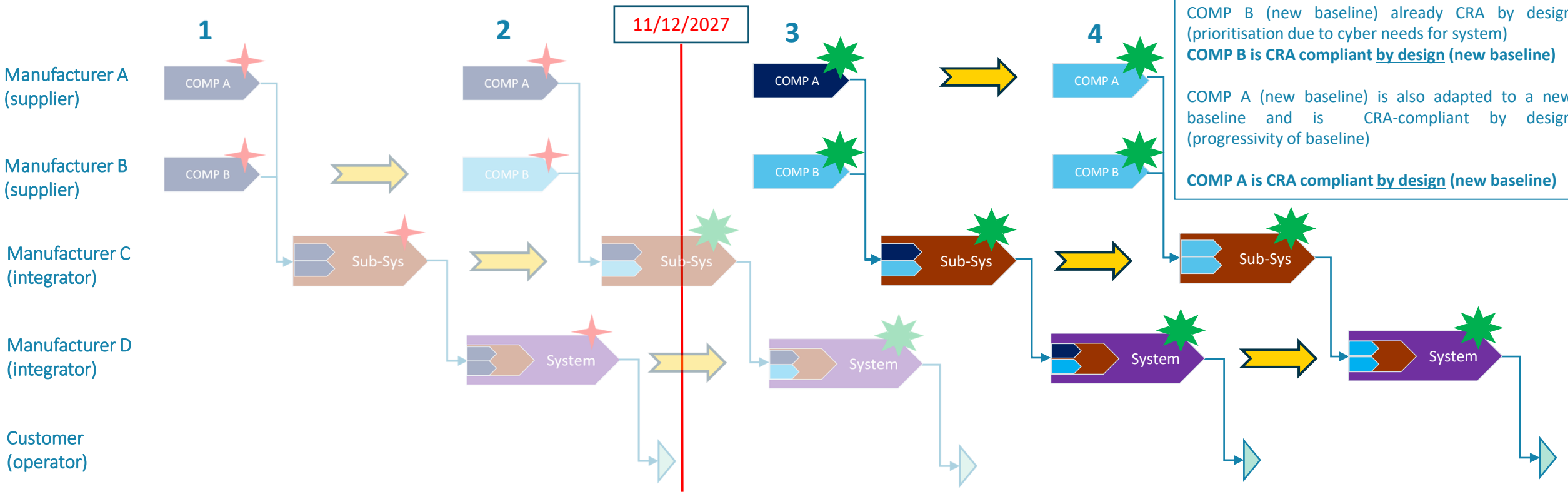
Increase of cybersecurity

New baseline

CRA compliance "by design" Designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity

ALWAYS with acceptable risks at system level

Ongoing Projects: Progressivity and Prioritisation



Example 4: COMP A, COMP B, Sub-System and System are all made available after 11/12/2027:
CRA compliance is required for all

COMP B (new baseline) already CRA by design (prioritisation due to cyber needs for system)
COMP B is CRA compliant by design (new baseline)

COMP A (new baseline) is also adapted to a new baseline and is CRA-compliant by design (progressivity of baseline)

COMP A is CRA compliant by design (new baseline)

CRA compliance not required, pre-existing component, subsystem or system.

Initial baseline

CRA compliance "on the basis of the (system) risk assessment" May be used "as is" or with additional mitigating measures (inside or around in the sub-system architecture) => conditions of use (e.g. SecRACs)

Increase of cybersecurity

New baseline

CRA compliance "by design" Designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity

ALWAYS with acceptable risks at system level

Key take aways and example of practical application

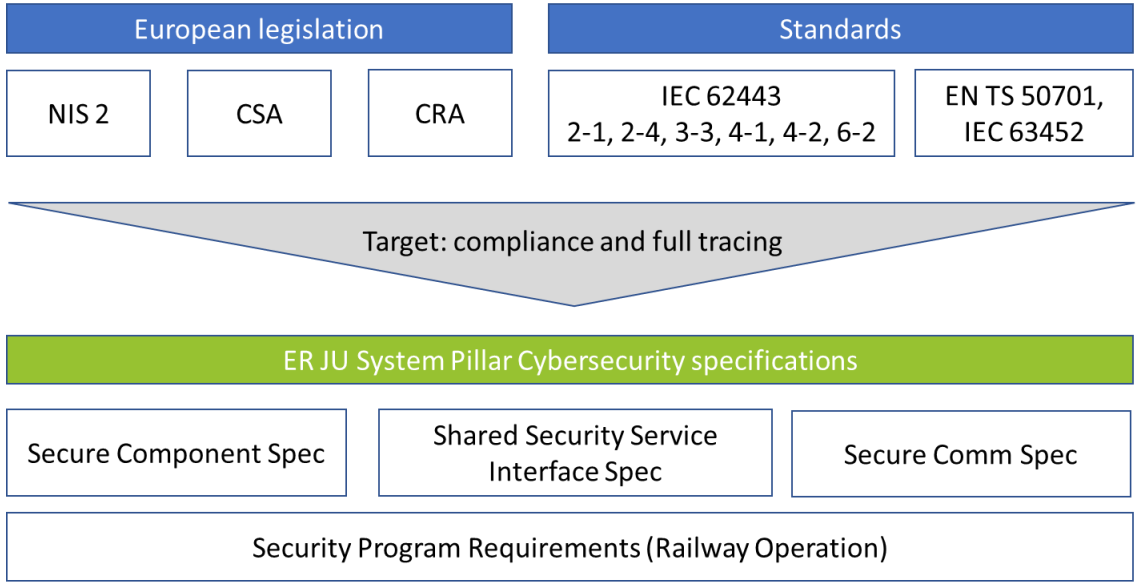
Key take aways:

- **Expert Guidance supports understanding and implementation of CRA**
- **Security-by-design is the key principle for every product development**
- **Communication between Manufacturers and Railways is essential for transition**

System Pillar Cybersecurity Specifications:

- **Support compliance with standards and regulations**
- **Support interoperability**
- **Reduce development effort**
- **Reduce time to market**

CCS for now and maybe more in the future …



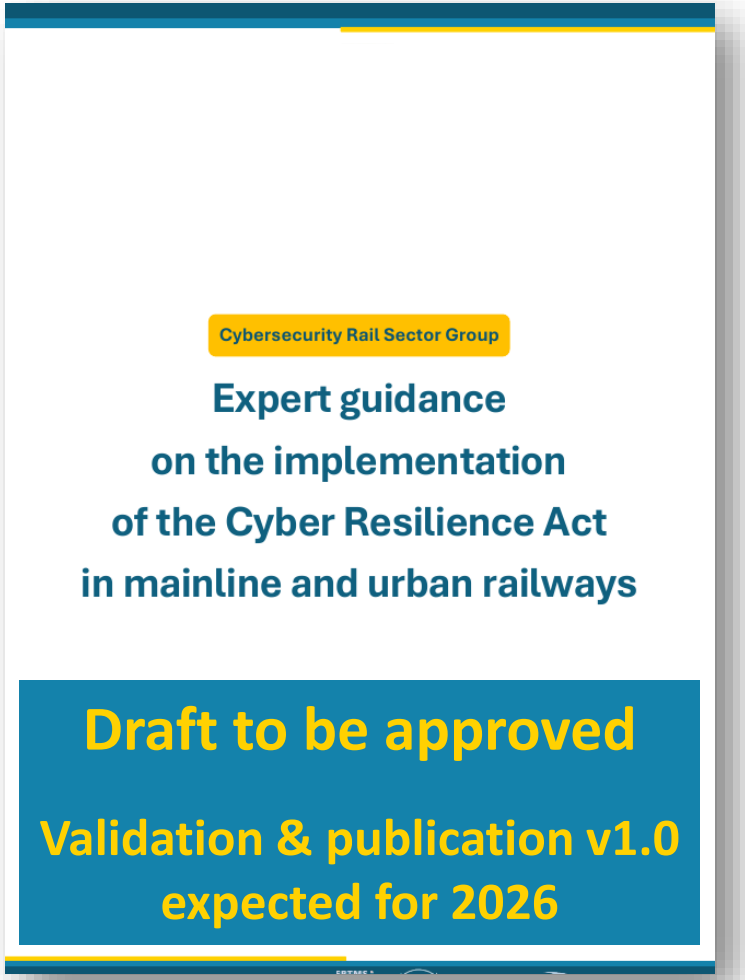
The Path Forward

Scope of Application

Substantial Modification

Tailor Made

Support Period



Spare Parts

System Extensions

Use Cases

SBOMs