CER
The Voice of European Railways

UITP
EUROPE

unife
THE EUROPEAN RAIL INDUSTRY

EXPERT GUIDANCE ON THE IMPLEMENTATION OF THE CYBER RESILIENCE ACT IN MAINLINE AND URBAN RAILWAYS

V 1.0.0 APRIL 2026

LEGAL DISCLAIMER:

THIS PRACTICAL GUIDANCE IS PROVIDED BY RAIL SECTOR ORGANISATIONS, FOR USAGE BY THE RAIL SECTOR. IT IS NOT LEGALLY BINDING IN ANY WAY AND DOES NOT REPRESENT THE VIEWS OR AN OFFICIAL POSITION OF EU INSTITUTIONS AND IS WITHOUT PREJUDICE TO THEIR POSITION ON THESE MATTERS. ALL APPLICABLE LEGISLATION AND LEGAL OBLIGATIONS NATURALLY REMAIN UNAFFECTED BY THIS GUIDANCE.

THE INFORMATION IN THIS DOCUMENT IS FOR REFERENCE ONLY AND MAY NOT BE UP-TO-DATE OR ACCURATE. THE SUPPORTING ORGANISATIONS DO NOT GUARANTEE ITS COMPLETENESS OR RELIABILITY. THIS DOCUMENT SHOULD NOT BE USED AS PROOF OR RELIED UPON FOR LEGAL PURPOSES. THE INFORMATION MAY BECOME OBSOLETE OVER TIME. PLEASE CONSULT A PROFESSIONAL IF NEEDED. THE SUPPORTING ORGANISATIONS AND THEIR MEMBERS ARE NOT RESPONSIBLE FOR ANY ACTIONS TAKEN BASED ON THIS DOCUMENT. STAKEHOLDERS IN THE RAIL SECTOR ARE NOT BOUND BY THE CONTENT OF THIS DOCUMENT, WHICH DOES NOT CONSTITUTE A COMMITMENT AND HAS NO BINDING EFFECT.

TLP: CLEAR

TABLE OF CONTENTS

INDEX OF DIAGRAMS AND TABLES IN THE MAIN TEXT:

INTRODUCTION

THE ORGANISATIONS BEHIND THIS GUIDANCE

The writing of this guidance has brought together representatives from much of the European rail sector to support a coherent and clear implementation of the Cyber Resilience Act in the sector. The following organisations representing both rail operators and suppliers support this guidance and have provided experts to write it:

CER
The Voice of European Railways

Founded in Brussels in 1988, the Community of European Railway and Infrastructure Companies (CER) brings together railway undertakings, their national associations as well as infrastructure managers and vehicle leasing companies, representing their interests towards EU policy makers and transport stakeholders. With close to 70 members, CER represents the large majority of the rail infrastructure network, rail freight business and rail passenger operations in EU, EFTA and EU accession countries.

https://www.cer.be

UITP EUROPE

UITP is the International Association of Public Transport, established in 1885 in Brussels. It is the worldwide network to bring together public transport stakeholders and sustainable transport modes. In Europe, UITP's main activity consists of working closely with European Union Institutions, bringing together more than 450 urban, suburban and regional public transport operators and authorities from all member states.

www.uitp.org

unife
THE EUROPEAN RAIL INDUSTRY

Based in Brussels since 1992, UNIFE is the association representing Europe's rail supply industry at the European Union (EU) and international levels. UNIFE's members include more than 120 companies from 18 European countries – from SMEs to large industrial players – active in the design, engineering and manufacture of rolling-stock as well as rail signalling and infrastructure equipment. UNIFE also brings together the national rail industry associations of 11 European countries.

www.unife.org

CONTEXT AND PURPOSE OF THIS GUIDANCE

This document aims at providing clear explanations and sector-wide guidance for the implementation of Regulation (EU) 2024/2847 – the Cyber Resilience Act (CRA) – and its obligations, with a view of helping the rail sector implement the regulation quickly and effectively. It is meant to complement the existing regulation and support its understanding and the effectiveness of its implementation.

The rail industry, a highly regulated sector governed by industry-specific legislation and standards, has long been integrating cybersecurity measures in its systems, all the while adapting progress to its situation and challenges, as shown in Diagram I.

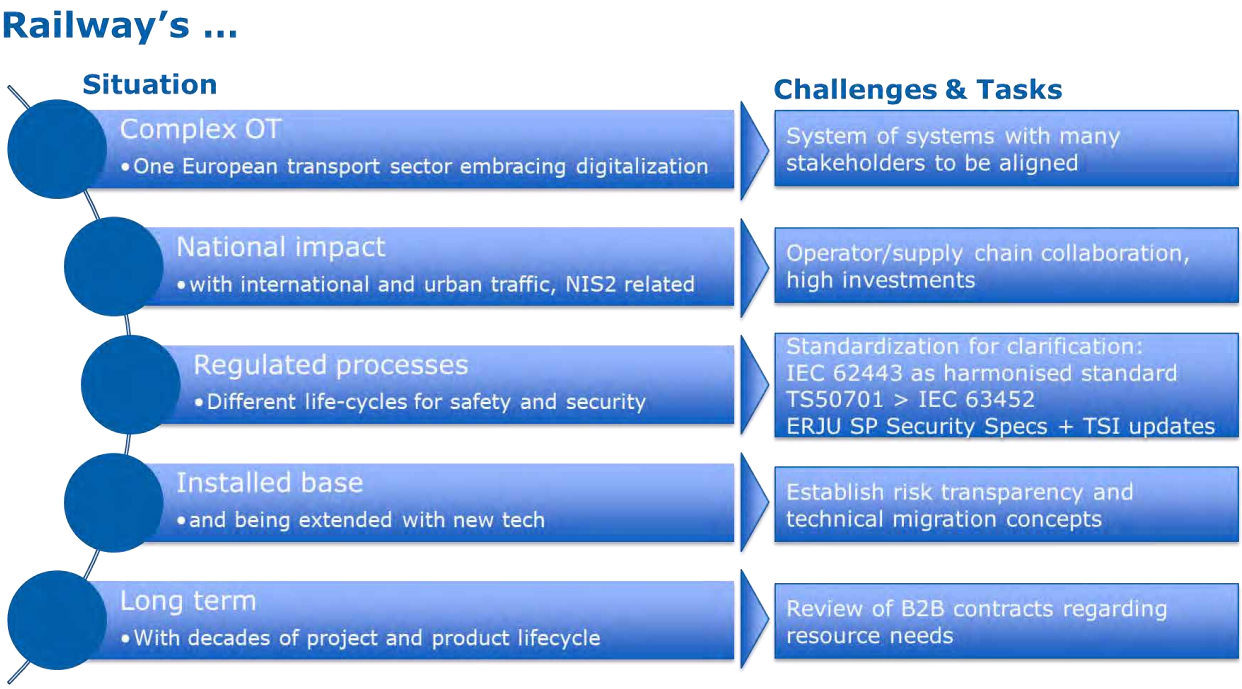


Diagram I – Cybersecurity adaptation challenges in rail

Rail is defined by the long life-cycle of its products – some of them up to 25 or even 50 years – with development and delivery cycles averaging around 10 years. For this reason, progress in cybersecurity must be compatible with the need to maintain ongoing operation and development of the railway system and its projects. The Interoperability Directive manages their life-cycle challenges through migration phases, by exempting rail projects at an advanced stage of development from compliance with newly published TSIs.

The CRA gives further support to the sector to overcome its challenges. The organisations and companies behind this document fully support the objectives of the CRA and are committed to implementing it as quickly as possible. As shown throughout this text, the CRA text itself provides the tools for a smooth and proper implementation, and its cybersecurity risk assessment-based approach can help prevent disruptions in the rail supply chain and the broader sector.

However, due to its horizontal, cross-sectorial nature, the CRA text does not provide ready-made sector-specific or operational guidance for applying it, and makes use of terminology and concepts not present in rail-specific legislation, although partially overlapping with it. For the rail sector – characterised by complex systems, subsystems, and components within a supply chain involving numerous stakeholders – any lack of precision could lead to misunderstandings or divergent interpretations between stakeholders or even across projects leading to potential traffic, functional or operational disruptions.

To avoid this, this present technical guidance document provides operational guidelines – developed by both rail operators and suppliers together – to the sector and stakeholders through criteria and principles which apply the risk assessment-based approach used in the railway domain.

This document is divided into two main sections: its first part explains the CRA, the concepts present in the text and the obligations it creates. The second part outlines a series of suggested practices to effectively apply the regulation in the rail sector, with particular attention to easing the transition between pre-CRA procedures and the establishment of fully CRA-compliant supply chains.

Where possible, usual practices of the rail sector have been extended to cybersecurity. Notably, it is often the case in rail that suppliers export constraints (e.g.: SRACs) to their users, which are dealt with through mutual agreements and formal risk acceptance. These concepts have been adapted for cybersecurity (e.g.: SecRACs), mirroring practices in the safety domain. Using this pragmatic approach, the authors ultimately aim to define in detail how CRA compliance for railway components and systems should be demonstrated, and how to best apply its provisions to meet CRA requirements effectively. Through this approach, the CRA and guidance together will allow for an effective and consistent increase in cybersecurity for the sector – optimised through defined priorities and managed costs – avoiding uncertainty and paralysis in implementation efforts.

Furthermore, the guidance supports manufacturers in avoiding sensible fines that would arise from noncompliance with the CRA due to misunderstanding or ignorance of its provisions. These fines may be up to 15 million Euro or 2,5 % of the annual world-wide turnover – whichever is higher (CRA art. 64). In addition, a binding request of withdrawal of all distributed Product with digital elements (PDE) which are affected may be requested by the market authority (CRA art. 13.21)

The document is intended to be incremental; as such, the topics presented here are only the first and the most fundamental which have been tackled; new topics and suggestions may be added over time.

The guidance does not alter any law, nor does it alter the legal accountability concerning CRA obligations for manufacturers, importers or distributors.

PART I
THE CRA IN A NUTSHELL

This section is focused on the CRA text, explaining its concepts and wording, as well as clarifying the key provisions, requirements and obligations of the legal text

1.1 ESSENTIAL DEFINITIONS

The CRA applies to products with digital elements (PDEs) made available on the market[1] from the application date of the regulation of 11/12/2027[2]. To understand the scope of the regulation and the terms used in this guidance document, the following definitions are provided:

Making available on the market is the supply of a PDE for distribution, consumption or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge (CRA art. 3.22). This definition is elaborated in the Blue Guide[3], which states that a product is made available on the market, when it fulfils the following two criteria:

1. It is offered or agreed upon (e.g. through catalogue, presence in store, under contract…) **AND**
2. It has been manufactured (it is built)

Note: the delivery date from manufacturer to user (integrator, asset owner) is not necessarily relevant for this definition (Blue Guide Section 2.2, paragraph 6)

The making available of a product supposes an offer or an agreement (written or verbal) between two or more legal or natural persons for the transfer of ownership, possession or any other right concerning the product in question after the stage of manufacture has taken place. The transfer does not necessarily require the physical handover of the product. Making available can, therefore, occur multiple times in a product's life-cycle: see Diagram II.

When determining when a product was made available on the market, the specific date that applies is the moment when both of the above criteria are fulfilled, i.e. whichever is later between the date of the offer and the manufacturing date.

Placing on the market: according to the Blue Guide[4] a product is "placed on the market" when it is "made available on the market" **for the first time** on the European Union market.

Based on this definition, the following applies:

- An integrator is a manufacturer or entity that incorporates third-party hardware or software components into their own product.
- An asset owner is an individual or organisation owning one or more PDE for the purpose of operation, referred to in the CRA as 'user' or 'business user'.

[1] The term "market" has a special meaning within the CRA and EU legislation and should be read in conjunction with other legislation and European Commission publications, such as the Blue Guide (see note 2).
[2] Reporting obligations for actively exploited vulnerabilities apply to all PDEs, not only to those made available on the market after 11/12/2027
[3] 'Blue Guide' on the implementation of EU product rules (2022/C 247/01) Section 2.2
[4] 'Blue Guide' on the implementation of EU product rules (2022/C 247/01) Section 2.3

Note: placing on the market is considered not to take place where a product is only kept in the stocks of the manufacturer without being subject to further commercial transaction. (Blue Guide Section 2.3)

Following these definitions, it transpires that the CRA applies to **each individual PDE, distinguished by serial number or other unique identifiers**, and not to an entire line of identical products, as illustrated by diagram II. This also means that the CRA will apply to every PDE placed on the market after 11/12/2027 even if it is part of a series and identical to PDEs placed on the market before 11/12/2027 to which the CRA did not apply.

Example:

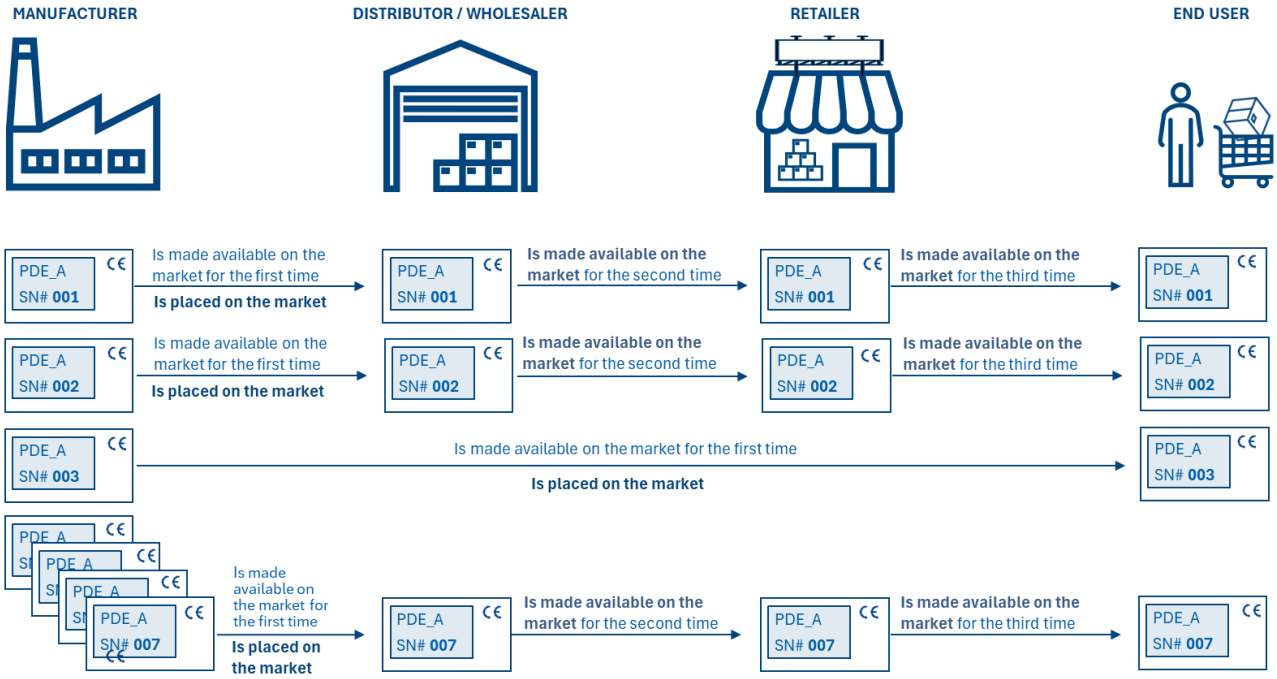
- A rail project begins with a contract;
- The manufacturer then develops and manufactures a PDE within the context of the project. This is point of time of placing on the market;
- The PDE is then delivered;

As a general rule: every product placed on the market after 11/12/2027 has to be CRA compliant, and the CRA applies to each individual product.

Note: according to the Blue Guide and CRA, renting is an act of distribution and therefore an act of "making available on the market". The concept of renting is not elaborated on further within this guidance.

In this document, the term **manufacturer** is generally used to represent both suppliers and integrators.

The following diagram is intended to help visualise and clarify the distinction between the concepts of “making available” and “placing on the market”.



*PDE_A: Imaginary name of a product with digital elements; **SN: Serial Number

Diagram II - "Placing" and "Making available" on the market

Product with digital elements: According to CRA art.3.1, 'product with digital elements' (PDE) means a software and/or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately. The CRA makes extensive use of the concept of PDE, and the application of this definition to rail sector products is discussed in section 2.1.

Core functionality: A product's core functionality refers to the main features and technical capabilities of a PDE, considering its architecture and key components. It represents what the product must do for it to qualify as a certain product type. The core functionality is determined considering the PDE's intended or reasonably foreseeable context and conditions of use, as well as its technical documentation. A PDE can have more than one core functionality, but for the purposes of determining its class and assessment (see section 1.3), only one must be selected, the most representative of the PDE's overall function.

Intended purpose: The intended purpose of a PDE (CRA art. 3.23) is the use for which it is intended by the manufacturer, including the specific context and conditions of use specified in the information supplied by the manufacturer in the instructions for use and in the technical documentation. Other indications of the intended purpose may be included in promotional or sales materials and statements by the manufacturer.

SBoM: A Software Bill of Material is a formal, machine-readable inventory documenting components, libraries and dependencies within a software product. The CRA (Annex I Part II) mandates the creation of SBOMs. This document further elaborates on SBOMs in section 2.8.

Spare parts: Spare parts are products "*that are made available on the market to replace identical components in PDEs and that are manufactured according to the same specifications as the components that they are intended to replace*" (CRA art. 2.6). Spare parts that correspond to this definition, both for legacy pre-CRA products and for CRA-compliant ones (CRA rec. 29), are excluded from the scope of the CRA, and therefore from compliance with it. This document further elaborates on spare parts in section 2.3.

Substantial modification: According to CRA art. 3.30, 'substantial modification' means a change to the product with digital elements following its placing on the market, which either:

- affects the compliance of the product with digital elements with the CRA essential cybersecurity requirements (Annex I Part I), **OR**
- reflects a change to the intended purpose for which the product with digital elements has been assessed.

Note: a modification that purposefully and directly decreases the level of cybersecurity risk without adding new functionalities or changing the intended purpose, is not considered substantial (CRA rec. 39). for more detail on substantial modifications, see section 2.2.

Project: The CRA does not make use of the concept of project, but as it is an essential concept within the rail domain, it is used within this guidance to provide concrete examples and help the practical application of the regulation. The definition of project is found in section 2.7. It should be noted that the CRA applies to individual PDEs. Accordingly, this definition of project does not affect the scope or applicability of the obligations arising under the regulation.

1.2 SCOPE OF APPLICATION

1.2.1 TIMELINE

The Cyber Resilience Act entered into force on 10 December 2024 and will become entirely applicable on 11 December 2027. Here follow the key dates of the implementation process relevant for manufacturers obligations:

- **11 September 2026 – CRA art. 14, Reporting obligations begin.** Manufacturers must report actively exploited vulnerabilities and major security incidents for all PDEs, regardless of the date of their placing on the market.

- **11 December 2027 – All CRA requirements apply to products made available on the EU market from this date onward.**

Furthermore, the CRA sets the following dates as a timeline for the European Commission to follow:

- 11 December 2025 – publication of Commission Implementing Regulation (EU) 2025/2392, containing a more detailed description of Important and Critical products (Annexes III-IV);

- 11 June 2026 – the provisions in Chapter IV, related to the notification of Conformity Assessment Bodies, become applicable;

- 11 December 2026 – the process of notification of relevant Conformity Assessment Bodies by Member States should be in an advanced stage;

- 11 June 2028 – Expiration date for all EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for relevant products that are subject to Union harmonisation legislation (unless otherwise specified by said other legislation);

1.2.2 SCOPE AND EXEMPTIONS

The regulation applies to all products with digital elements (PDEs) placed on the market after 11 December 2027[5].

Some PDEs are excluded from the scope of the CRA in the context of railways:

- Spare parts replacing identical components and produced with the same specifications of the PDEs/components they are meant to replace (see dedicated section 2.3).
- PDEs placed on the market before the end of the transition period on 11/12/2027 according to the exception provided by CRA art. 69.2 as long as they are not substantially modified (see section 2.2 on substantial modification).

The CRA applies whenever PDEs are **made available** on the EU market. Diagram III shows three cases, which illustrate the concept of making available on the market before, around, and after the application date of the CRA on 11/12/2027.

- Case 1 concerns a PDE that was manufactured and bought by a distributor **before** 11/12/2027. The PDE is then sold, without substantial modifications, **after** 11/12/2027 to an end user. Therefore, this PDE is exempted from the application of the CRA in accordance with art. 69.3

- Case 2 concerns a PDE, PDE_A (produced **before** 11/12/2027), which is sold to an integrator (**before** 11/12/2027) and integrated into another PDE (PDE_B) constituting a new product. In this case, **PDE_A is not required to comply with the CRA**. However, **the final product PDE_B** is placed on the market after 11/12/2027 and, therefore, **must comply with the CRA** when it is placed on the market, including through a cybersecurity risk assessment and proof that the essential cybersecurity requirements have been met.

- Case 3 concerns a PDE that is placed on the market **after** 11/12/2027. It must in all cases comply with the CRA, as the transition period does not apply to it.

[5] Reporting obligations for actively exploited vulnerabilities apply to all PDEs, not only to those made available on the market after 11/12/2027

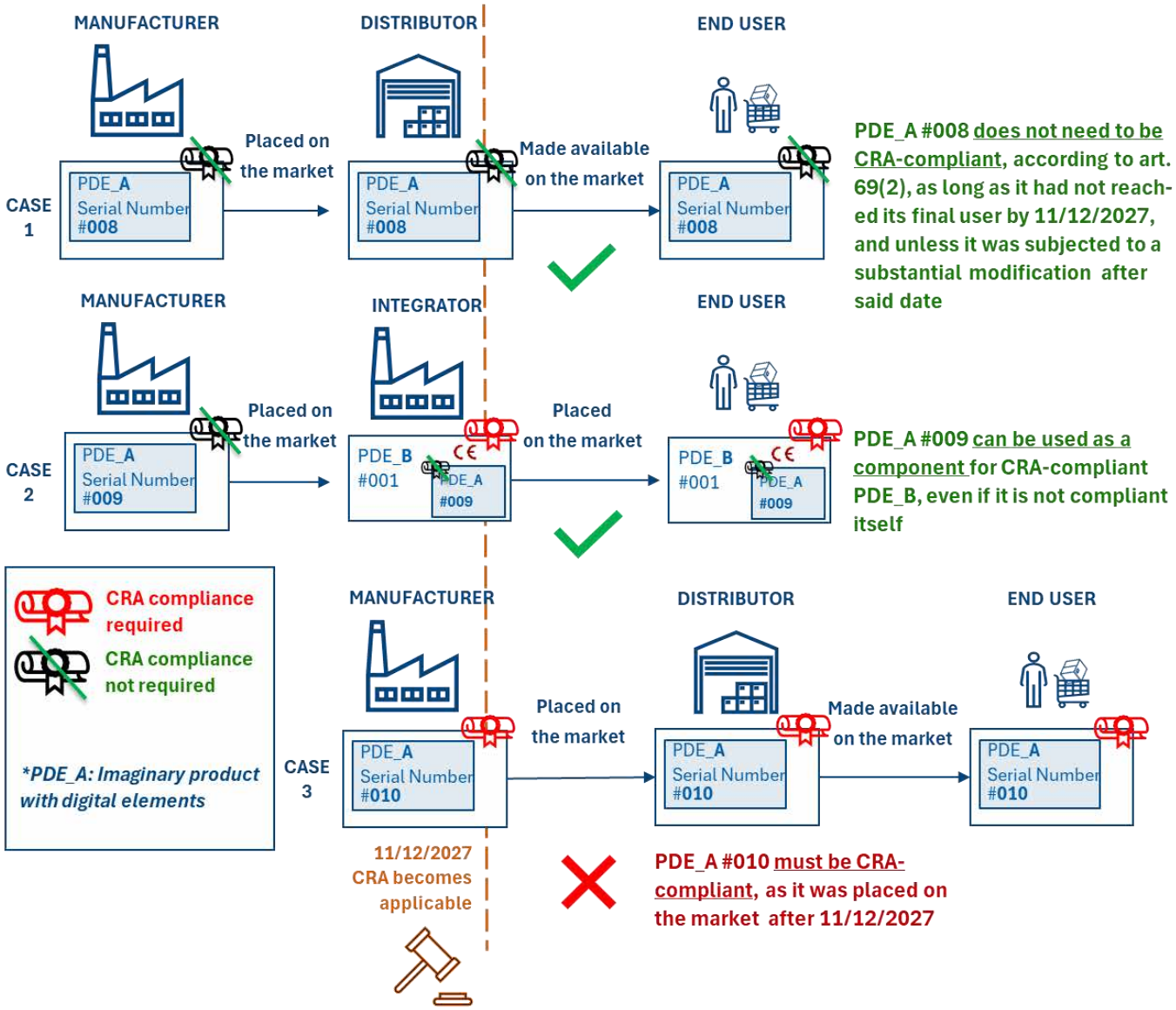


Diagram III - PDE compliance at the end of the transition period

1.3 PRODUCT CLASSES

PDEs which fall within the scope of the CRA are divided into four classes, according to their core functionality. Depending on whether a product is considered an important PDE (listed in Annex III) or critical PDE (listed in Annex IV) different methods for their conformity assessment are available as set out in art. 32 and Annex VIII of the CRA:

- **Default**. This category will comprise the vast majority of PDEs, as it includes any product that does not fall into any of the categories below, i.e. is not listed as an Important or Critical product in Annexes III and IV. To assess the conformity of PDEs in this category, an internal control and declaration of conformity by the manufacturer are sufficient, as described in Annex VIII Part I. This procedure is also called self-assessment or Module A procedure. All other assessment procedures set out in the CRA are also allowed, but not mandatory, for these PDEs;

> **Note: the European Commission may amend the list of products in Annex III or IV.**

- **Important, Class I.** For PDEs in this category, manufacturers have three conformity assessment options:
  - Self-assessment through compliance with existing harmonised standards, common specifications or European cybersecurity certification schemes of at least assurance level 'substantial';
  - External assessment of the PDE's design and development by a notified body (Module B procedure) followed by internal production control to ensure compliance with the PDE type validated by the notified body (Module C).
  - External assessment of the entire quality system by a notified body (Module H procedure);

> **Note: within the CRA the term "notified body" indicates an organisation with cybersecurity expertise notified for the purposes of the CRA. these are not to be confused with the notified bodies defined in the TSIs.**

- **Important, Class II.** PDEs in this category have the same conformity assessment options as Class I, with one additional restriction: self-assessment through compliance with harmonised standards or common specifications is **not considered sufficient**, while compliance with European cybersecurity certification schemes (if available) is still allowed.

- **Critical.** For PDEs in this category, manufacturers *must* demonstrate conformity through an external assessment, either of the product (Modules B+C) or of the quality assurance system (Module H). If required by a Delegated Act (art. 8.1) manufacturers of concerned

critical products *must* demonstrate conformity against a European cybersecurity certificate of at least assurance level 'substantial'.

Note: within the CRA, the term "critical" is unrelated to the concept of criticality used in the rail sector, i.e. in the sense of availability for operation or in a safety-related sense. Instead, it is only used to refer to the category of PDEs with the most stringent cybersecurity requirements.

The following table summarises the assessment methods and shows relevant product examples for each category:

Default	Important Class I	Important Class II	Critical
■ **Self-assessment**, (a.k.a Module A procedure) ■ **Third party assessment**, if requirements for self-assessment are not fulfilled or if preferred by the manufacturer	■ **Self-assessment**, only if a harmonised standard or European cybersecurity Certification Scheme can be applied ■ **Third party assessment** (Module B+C or Module H)	■ **Self-assessment**, only if a European cybersecurity Certification Scheme can be applied ■ **Third party assessment** (Module B+C or Module H)	■ **Third party assessment** (Module B+C or Module H) ■ **Other methods can be mandated** by a relevant Delegated Act in the future.
Any PDE not listed in other categories. Examples may be: RBC, EVC, Interlocking, Object Controller, Passenger information system, Door controller, Brake system, Ticket vending machine, Ticketing system, Passenger counting system, Video surveillance system, DMI, TCMS, Train information Management System, HVAC, Rolling-Stock, CBTC, ETCS	Full list in Annex III of the CRA. Examples: ► IAM, PKI ► Anti-virus ► SIEM ► Network products (routers, switches, VPNs, network management systems) ► Operating Systems ► Microprocessors and controllers with security-related functionality ► ASIC+FPGA with security-related functionality ► GSM, 4G, 5G, FRMCS, routers/modems	Only the following PDEs are included: ► Firewalls, IDS, IPS ► Hypervisors, Container runtime systems ► Tamper-resistant micro-controllers/ processors	Only the following PDEs are included: ► Hardware Devices with Security boxes (e.g. HSM, TPM) ► Smart meter gateways (not including smart meters from locomotives, self-propelled units or multiple units) ► Smartcards or similar devices, including secure elements

Table I – Product classes

The class of a PDE is determined by its core functionality (defined in section 1.1). Although the classification of a PDE must ultimately be assessed on a case-by-case basis, the purpose of this document is to provide general guidance to support that assessment. The examples included are intended solely as illustrative guidance and do not constitute definitive or exhaustive classifications. It is important to highlight that according to CRA art. 7.1 **the class of a product is not inherited in any direction**, i.e. if a critical or important PDE is integrated into a larger product, the latter is not considered critical or important as a consequence, nor does a critical/important PDE change its class if it is made of default class components. Diagrams IV and V in section 2.1.1 shows the variety of components from different risk categories present in railway elements without inheritance to any direction.

1.4 PRODUCT REQUIREMENTS AND OBLIGATIONS

1.4.1 ESSENTIAL CYBERSECURITY REQUIREMENTS

The CRA imposes minimum horizontal cybersecurity requirements to all PDEs within its scope made available on the market after 11/12/2027. The full requirements are set out in Annex I Part I of the regulation.

1.4.2 MANUFACTURER OBLIGATIONS OVERVIEW

Manufacturers of PDEs are assigned several obligations related to the manufacturing of the product and post-sale support (art. 13.1 to 25) as well as several reporting obligations (art. 14.1 to 10). The key obligations are summarised below:

1. Check the relevance according to CRA;
2. Perform cybersecurity risk assessments on the PDE;
3. Perform due diligence on third-party components, if they are integrated, i.e. check the CE marking and ensure they do not compromise the cybersecurity of the PDE they are being integrated into;
4. Ensure the PDE is designed, developed and produced according to the appropriate level of cybersecurity according to the risk assessment with selected security measures to mitigate the identified risks;
5. Ensure that the life-cycle processes for vulnerability handling, continuous (periodic and event based) risk analysis update and documentation are in place for the defined support period (taking into account the expected lifetime of the PDE and with a minimum period of five years, unless the PDE is expected to have a shorter lifetime);
6. Assess compliance for the PDE according to its class (default, important class I, important class II, critical);
7. Execute life-cycle processes according to point 5.

According to CRA art. 13.8, manufacturers are required to determine the support period for each PDE so that it reflects, among others, the length of time during which it is expected to be in use. For more details on the support period, see section 2.4.

Due diligence for third party components, referred to in point 3, refers to the risk assessment, treatment and conformity evaluation activities to be performed by the manufacturer before integrating third-party components into a larger PDE. It is a

necessary step to ensure that the components that are integrated do not compromise the cybersecurity of the PDE, and that an appropriate level of cybersecurity is maintained based on the risks throughout the support period of the larger PDE.

Practical steps to perform due diligence on a third-party component may include:

- Performing a security compliance assessment of the component, e.g. by verifying if it receives regular updates or if it is affected by known vulnerabilities;
- Evaluating whether the component is fit for purpose;
- Reviewing the component's SBOM, when available, for dependencies and exposure points;
- Ensuring that the component meets the CRA requirements (e.g., CE marking, secure-by-design principles, vulnerability disclosure and patching mechanisms in place) by verifying that the component is supplied with the appropriate conformity documentation;

Note: more guidance on due diligence will be made available directly by the European Commission through guidelines and FAQ documents.

1.4.3 REPORTING OBLIGATIONS

The following reporting obligations will apply to ALL products, regardless of the date of their placing on the market, from September 11, 2026 (and continue after 11 December 2027):

- The manufacturer shall report **any actively exploited vulnerability** (by attackers) contained in the product with digital elements and any serious security incident immediately, and in any case within 24 hours **after becoming aware of it**.

- The manufacturer shall also inform impacted users of an actively exploited vulnerability or a severe incident having an impact on the security of the PDE[6]. If appropriate, all users should be informed.

- Notifications shall be made available simultaneously to the CSIRT designated as coordinator in accordance with CRA art. 14.7, and to ENISA.

[6] Defined in art. 14.5 as an incident having an impact on the security of the PDE that negatively affects or is capable of negatively affecting the ability of the PDE to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or has led or is capable of leading to the introduction or execution of malicious code in a PDE or in the network and information systems of a user of the PDE.

- Notifications shall be submitted via the single notification platform (CRA art. 16) as an electronic notification.

- The following timeline applies according to CRA art. 14.2 and 14.4:
  - An early warning notification of the exploit without undue delay and in any event within 24 hours after becoming aware of it.
  - Details of the exploit within 72 hours;
  - A final report at the latest 14 days after corrective measures are made available, in the case of an actively exploited vulnerability, or within one month in case of a severe incident;

The requirements to report actively exploited vulnerabilities and severe incidents apply to ALL products that the manufacturer has made available on the market. This means that it also covers all products already on the market before 11/12/2027.

In addition to mandatory reporting obligations, the CRA provides for manufacturers and other persons to voluntarily report known vulnerabilities to the CSIRT or ENISA.

Note I: The manufacturer must put in place a procedure to fulfil the reporting obligations of CRA art. 14. This means that the manufacturer must inform the impacted users about actively exploited vulnerabilities in a timely, and where appropriate, automatic, manner.

Note II: For PDEs made available on the market before 11/12/2027, under the CRA the manufacturer is not legally required to actively search for actively exploited vulnerabilities.

1.4.4 VULNERABILITY HANDLING OBLIGATIONS

The following requirements only apply to PDEs that must be CRA-compliant, i.e. PDEs placed on the market after 11 December 2027 and apply to any vulnerability, not only to actively exploited vulnerabilities:

- Identify and document vulnerabilities based on Software Bill of Materials (SBoM) and regular and effective testing.

- Address vulnerabilities in accordance with associated risk and without delay. Security updates to address identified vulnerabilities must be made available free

of charge, unless otherwise agreed for a tailor-made product (see section 2.5), according to CRA Annex I Part II, point 8;

- The information about actively exploited vulnerabilities, major incidents and availability of security updates must be made available to users without undue delay according to coordinated disclosure and B2B agreement for tailor-made PDEs;

- The information must be made available in an appropriate manner;

The full requirements are set out in CRA art. 13.6, 13.7, 13.8, and in Annex I Part II.

1.4.5 IMPORTER AND DISTRIBUTOR OBLIGATIONS

Importers and distributors:

- Are assigned several obligations (CRA art. 19 and 20) towards the PDEs that they make available on the market.
- Are considered as a manufacturer (CRA art. 21) and shall be subject to CRA art. 13 and 14, where the importer or distributor:
  - **places a PDE on the market** under its name or trademark **OR**
  - **carries out a substantial modification** of a PDE and makes that product available on the market.

Note: Manufacturers become importers if they import PDEs and they become distributors if they buy and sell PDEs without modification.

PART II
APPLICATION TO THE RAIL SECTOR AND IMPLEMENTATION

This section builds on the provisions of the CRA to provide actionable recommendations to support an effective implementation of the CRA in the rail sector.

INTRODUCTION

As described in the introduction, the legal text is 'horizontal' and does not provide sector-specific or operational guidance needed to address provisions that apply to specific cases such as 'where applicable,' 'where technically feasible,' or 'unless otherwise agreed'**.** More sector-specific information is needed to clarify how the concepts, requirements and obligations set out by the CRA can be applied to rail.

To address these needs, this second part of the guidance builds on the provisions of the CRA and provides actionable recommendations intended to support their effective implementation, in line with the goals of the regulation.

The following sections provide guidance on the keys topics to be well understood to practically apply CRA in the railway context:

- What should be considered a PDE in the rail sector (section 2.1)
- How to assess whether a modification is substantial (section 2.2)
- How to handle spare parts (section 2.3)
- How to determine the support period (section 2.4)
- What defines a tailor-made product (section 2.5)
- How to deal with system extensions (section 2.6)
- How to allocate responsibilities among suppliers, railway undertakings, and infrastructure managers in a railway project context (section 2.7)
- How to address the SBoM topic (section 2.8)

To allow for efficiency and transparency along the supply chain, this guidance encourages exchange between stakeholders and in particular mutual agreement between manufacturer and asset owner for pre-existing projects. Such agreements do not constitute a transfer of accountability regarding CRA obligations. Instead, they are statements allowing for a clear and as timely as possible alignment on CRA implementation, notably on key topics (status for substantial modification, tailor-made and spare parts), on the efficiency of the measures taken and on their compatibility with the operation and maintenance phases after delivery.

This guidance offers an approach to conformity based on the risks at system level for railway operation. This means that the purpose and the conditions of use are defined according to the PDE's integration and function in the system for which it is intended to be used.

This approach allows for prioritised adaptation of the products most crucial for cybersecurity, according to the risks to be managed at system level. Depending on the progress of pre-existing projects, CRA compliance is achieved via progressive, viable and efficient application of the CRA requirements to each part of the railway system, both at (sub)system

and component levels. The annexes of this guidance provide specific use-cases and combinations of projects, (sub)systems and components to improve the reader's understanding.

For the development of new PDEs, it is highlighted that design will need to support regular security updates – if necessary – minimizing impact on safety or interoperability approvals of the system.

Note: Security updates must respect the system context, be planned and accepted by the asset owners.

2.1 WHAT IS A PRODUCT IN RAIL?

As the CRA applies to PDEs, it is essential to understand what falls under the term PDE, as this will define whether a manufacturer needs to apply the CRA in relation to its product or not. In the B2B context, especially in sectors such as rail that rely on complex supply chains, a clear-cut application of the terms *product* and *product with digital elements* is not immediately understood. In sector-specific legislation and standards the rail sector distinguishes between "products", "subsystems" and "systems" under the TSI definitions, as well as between "components", "control systems", "railway solutions" and "railway applications" within the IEC standards. In the CRA there is no clear-cut way to relate PDE and components to these definitions. Therefore, when applying the CRA, suppliers, manufacturers, integrators, and distributors should primarily refer to the definition of PDE set out in the CRA itself, while being supported by the clarifications and guidance provided in this document to facilitate a consistent and informed application within the sector.

It is important to recognise that the rail industry comprises a broad spectrum of stakeholders – including suppliers, manufacturers, integrators, and distributors – each playing a distinct role in the design, development, assembly, and commercialisation of products. In categorising Products with Digital Elements (PDEs) within the rail sector, this guidance has primarily relied on the criterion established by existing EU legislation, documentation such as the Blue Guide[7] and prevailing EU law practice: an item is considered a product if it is placed or made available on the market (see section 1.1) as a unit, distinguished by other units via a serial number or other unique identifier.

The resulting application of the term PDE to the sector includes any good containing software or hardware (with a direct or indirect data connection) which once manufactured, assembled or integrated, is placed or made available on the market as an individual product.

Table II showcases a general indicative mapping of the categories existing within the TSIs and the upcoming IEC 63452 standard, comparing them with the equivalent terminology adopted within this document and showing whether each category is expected to be considered a PDE under the CRA in most situations. "Functional Systems" such as interlocking, substations, individual rolling-stock and block trains like high-speed trains can be PDEs, due to their availability on the market as individual products. Conversely, "Elements" such as tunnels, large stations and trains which consist of individually assembled PDEs are generally not a considered a single PDE, as they are not made available on the market together as one product. These Elements are therefore usually outside the scope of the CRA, although they may be constituted of CRA-compliant products.

The test for whether an item qualifies as a PDE considers the commercial arrangements in which it is supplied (i.e. how it is made available on the market). Determination of

[7] 'Blue Guide' on the implementation of EU product rules (2022/C 247/01) Section 2.2

whether an item is a PDE should always be assessed on an individual basis in line with the definition under the CRA.

Every PDE that is foreseen for commercial use in the EU has to comply with the CRA. As a result, the following examples also drive the obligation for the PDE to comply with the CRA:

- Renting rolling-stock to be used in the EU from an organisation outside of EU;
- Buying an interlocking outside the EU, installing it and operating it in the EU.

If rolling-stock is intended to be operated (even if partially) in the EU, CRA compliance must be assured (including by non-EU manufacturers, non-EU economic operators…).

CRA	TSI (mainlines)	IEC 63452	NIS 2	In this guidance	Explanation	Examples
"Product with digital elements" (CRA applies if placed on the market by itself)	Product *Sometimes* Interoperability constituents	Component (product)	N/A	**COMPONENT**	Individual single component ("in the hand") containing hardware or software *Could be SPARE-PART*	- Actuator, Sensor, field element controller - PLC/CPU, I/O Module - 19" Rack with backplane, 19" Card - Router, Switch - Camera, Radio - Single recorder, Local HMI, Balise
"Product with digital elements" (CRA applies if placed on the market by itself)	Product *Sometimes* Interoperability constituents	Control system (product)	N/A	**Set of COMPONENTS**	Group of components, subassembly or complete assembly of equipment to run partially, scoped tailormade functions *Could be SPARE-PART*	- Energy 19" Rack and Card in Enclosure - On-board PLC/CPU + I/O Module + Power supply (e.g. Door control unit, HVAC, Brake control unit, Juridical event recorder, Main Control/Processor Unit, ...) - Trackside PLC/CPU + I/O Module + Power supply (e.g. local management of light, of water, high voltage security unit, ...) - CCTV (recorder + cameras) - Elevator - Fire detection (local supervision + smoke sensors + smoke fans + sprinklers) - Redundant recorders, Group of HMIs, Balises
"Product with digital elements" (CRA applies if placed on the market by itself)	Part of subsystem *or* Subsystem Infrastructure, energy, trackside control-command Incl. signalling, on-board control-command incl. signalling, rolling-stock, N.V.	Railway Solution (before handover)	N/A	**FUNCTIONAL SUBSYSTEM** *NB: Functional subsystem is not to be considered as 1-to-1 with subsystem as defined in TSI.*	Functional group of Components / Set of Components. From other functional subsystems independent or logical separated working subsystem.	- RBC, ETCS-ON-BOARD (EVC+BTM+DMI+...) - Interlocking central unit - Set of Components or Components in 110kV or 15KV VLANs - TCMS, OMTS, CCS (Rolling-stock including On-board units) - Platform screen doors - Light integrated system (central supervision + set of light units) - HVAC integrated system (central supervision + set of HVAC units) - Fire detection integrated system (central supervision + set of fire detection units)
"Product with digital elements" (CRA applies if placed on the market by itself)	Part of subsystem *or* Subsystem Infrastructure, energy, trackside control-command Incl. signalling, on-board control-command incl. signalling, rolling-stock, N.V.	Railway Solution (before handover)	N/A	**SYSTEM**	Group of functional Subsystems. Single and independent parts of the System Railway. In smaller "Systems", a "functional subsystem" may be equivalent to a "system".	- Interlocking (central unit + track side equipment), Substation, Powerplant, - SCADA System (incl. DMZ, Management Systems...) - Rolling-stock (incl. block train, self-propelled units) - CBTC
N/A (unless placed on the market as a unit)	Elements Network, Vehicle	Railway Application(s) (solution in operation – after handover)	A (or more) „network and information system"	**ELEMENTS**	"Elements" under TSI umbrella	- Trains* (composed of rolling-stock as one or more locomotive, one or more coaches ...) - Big Station (incl. Light, HVAC, Elevator, Fire detection...) - A railway track from A to B composed of multiple systems, tunnel
N/A	Union rail system	Railway System, including main line and urban	All „network and information system"	**RAILWAY SYSTEM**	All subsystems that compose the railway system of an enterprise	ALL in operation and ALL of an enterprise

Table II – Taxonomy Map

**Trains are composed of multiple rolling-stock and are in operation. Rolling-stock may be a single wagon, a locomotive, a block train (e.g. TGV, ICE)*

The following graphics of rolling-stock and infrastructure shows a potential chain of integration of PDEs (components, subsystems, systems). Products belonging to different classes according to the CRA may be integrated on all levels. Nevertheless, there is **no inheritance** of the classes. Each product is evaluated individually.

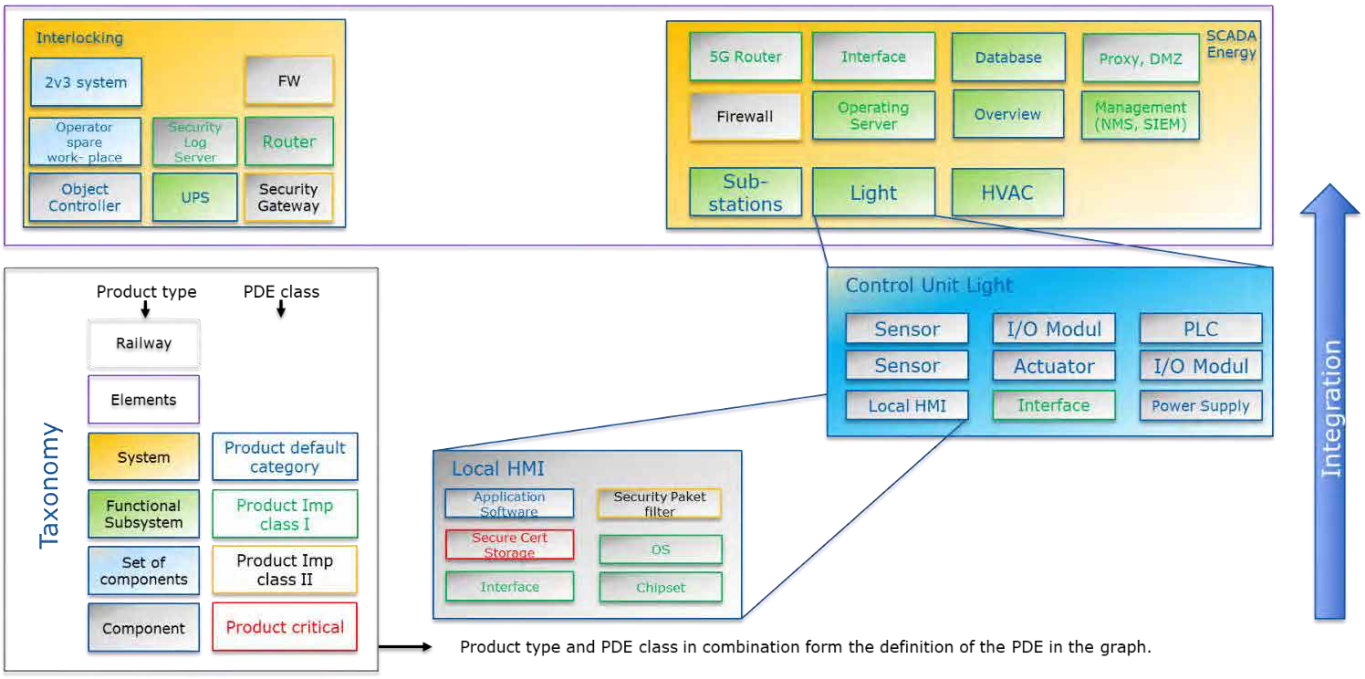


Diagram IV – PDE classes integration (Fixed installation & Trackside)

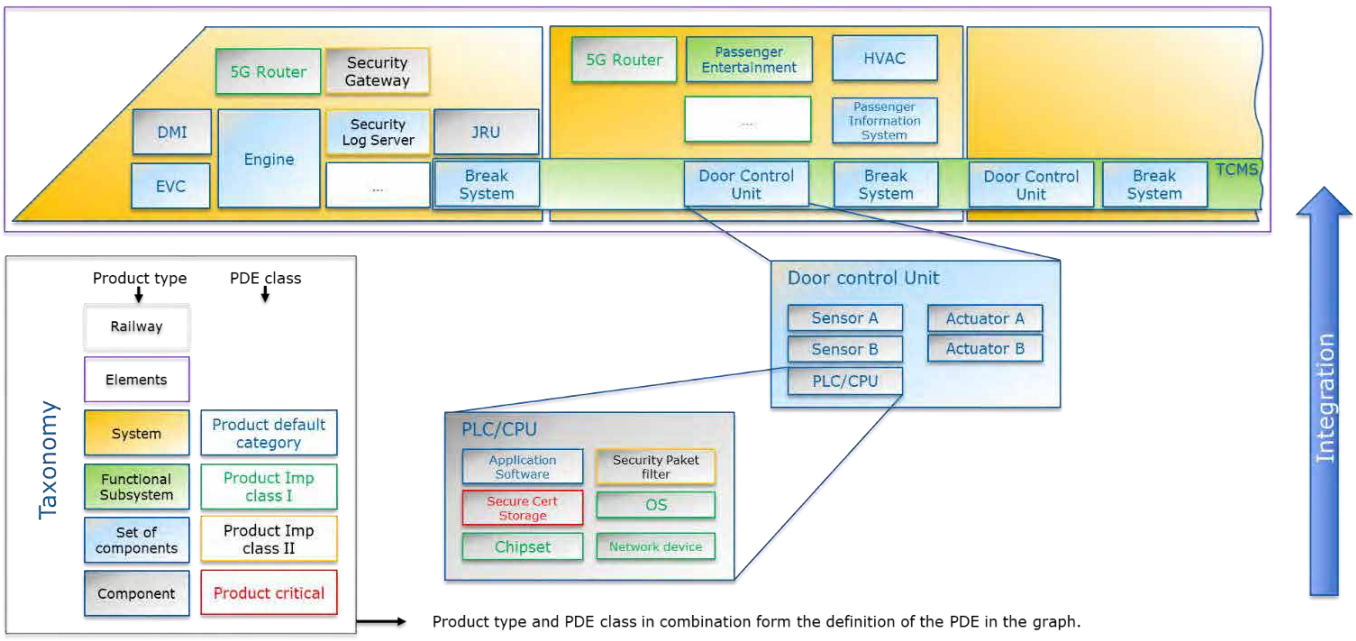


Diagram V - PDE classes integration (Rolling-stock)

Notably, for illustrative purposes diagrams IV and V assume that each component, subsystem and system shown is a separate PDE. However, as stated earlier, a hardware or software product is only considered a PDE if it is placed or made available on the market as an individual product. Therefore, a component that is already integrated into a PDE when

placed on the market is not concerned by CRA provisions (see also section 1.2.2, Case 2). For instance, as shown in Diagram V a chipset placed on the market on its own by a manufacturer is a PDE of risk category "Important class I". Conversely, the same chipset produced and integrated in-house into a PLC/CPU without being placed on the market is not considered a PDE. In this case, if the manufacturer supplies the integrated PLC/CPU to a client, the PLC/CPU will be the PDE, belonging to the Default risk category. The examples in Table III here below showcase how the same item can be considered a PDE or not in different contexts.

Router	■ A router which is supplied in the context of a contract to provide a router would be considered to be a PDE. ■ A router supplied as an integrated part of a rolling-stock, in the context of a contract to supply a rolling-stock would be considered as one part of the rolling-stock PDE. ■ That same router, in the context of a contract between the router supplier and the rolling-stock manufacturer for supply of a router would be considered to be a PDE by the router supplier.
Rail cars	■ A rail coach supplied in the context of a contract to deliver a rail cars would be considered to be a PDE. ■ The supply of multiple rail coaches, in the context of a contract to deliver rail cars, would be considered to be multiple separate PDEs.
Block Train	■ The supply of an integrated rolling-stock set (block train) in the context of a contract for the delivery of a block train would be considered to be a PDE. ■ The delivery of individual rail cars, each being part of the block train, in the context of a contract for the delivery of a block train, an individual rail car would not be considered as delivery under the contract and therefore not a PDE.
Interlocking	■ The supply of an interlocking in the context of a contract for the delivery of one or more interlockings would be considered to be a PDE. ■ The supply of an interlocking in the context of a contract to deliver a signalling system would be considered to be a part of that signalling system. ■ The signalling system, being delivered by the lead contractor and being uniquely identifiable would be considered to be the PDE in the context of the contract to deliver a signalling system.

Table III – Examples of product integration and CRA application

2.1.1 APPLICATION AND PRODUCT-IN-PRODUCT INTEGRATION

From the interaction between the application of the CRA to rail sector PDEs and the transition period end-date of 11 December 2027, different use-case situations emerge. Here are the key scenarios (see Diagrams III and VI):

- Case 1 – PDEs (e.g. components, subsystems and systems alike) which were made available on the market before 11/12/2027 and whose production ceased before that same date. These PDEs are not required to comply with CRA provisions. For the transitional provision exempting these PDEs, see section 1.2.2.

- Case 2 – PDEs placed on the market after 11/12/2027. All these PDEs shall be CRA-compliant including sufficient mitigating measures when integrating Case 1 components.

- Case 3 – PDEs whose first unit was placed on the market before 11/12/2027 and whose production continues after the same date. As mentioned in section 1.1, the regulation applies to each individual product by serial number or other unique identifiers, not to an entire line of identical products. Therefore, PDEs which are placed on the market after 11/12/2027 are required to be compliant, even if they are identical to previous products of the same line.

For instance, **a PDE acquired by an integrator before 11/12/2027, kept in storage until after 11/12/2027 and *then* integrated as a component into another PDE does not, per default, hinder the ability of the latter to be CRA-compliant**. Since it is possible that the non-compliant integrated component (made available on the market before 11/12/2027) does not fulfil all the essential cybersecurity requirements, the residual risk shall be analysed and managed at the level of the PDE integrating it. The integrator – acting as manufacturer – has the obligation to ensure CRA compliance of the overall PDE.

Note: the CRA does not acknowledge the concept of a product type as a whole. The relationship between the CRA and the type approval process of vehicles - notably for new and updated type approval after 11/12/2027 - is explored in a separate annex to this guidance: *"on the impact of the CRA on the rail interoperability Directive (EU) 2016/797 and practical arrangements for the railway vehicle authorisation Regulation (EU) 2018/545"*

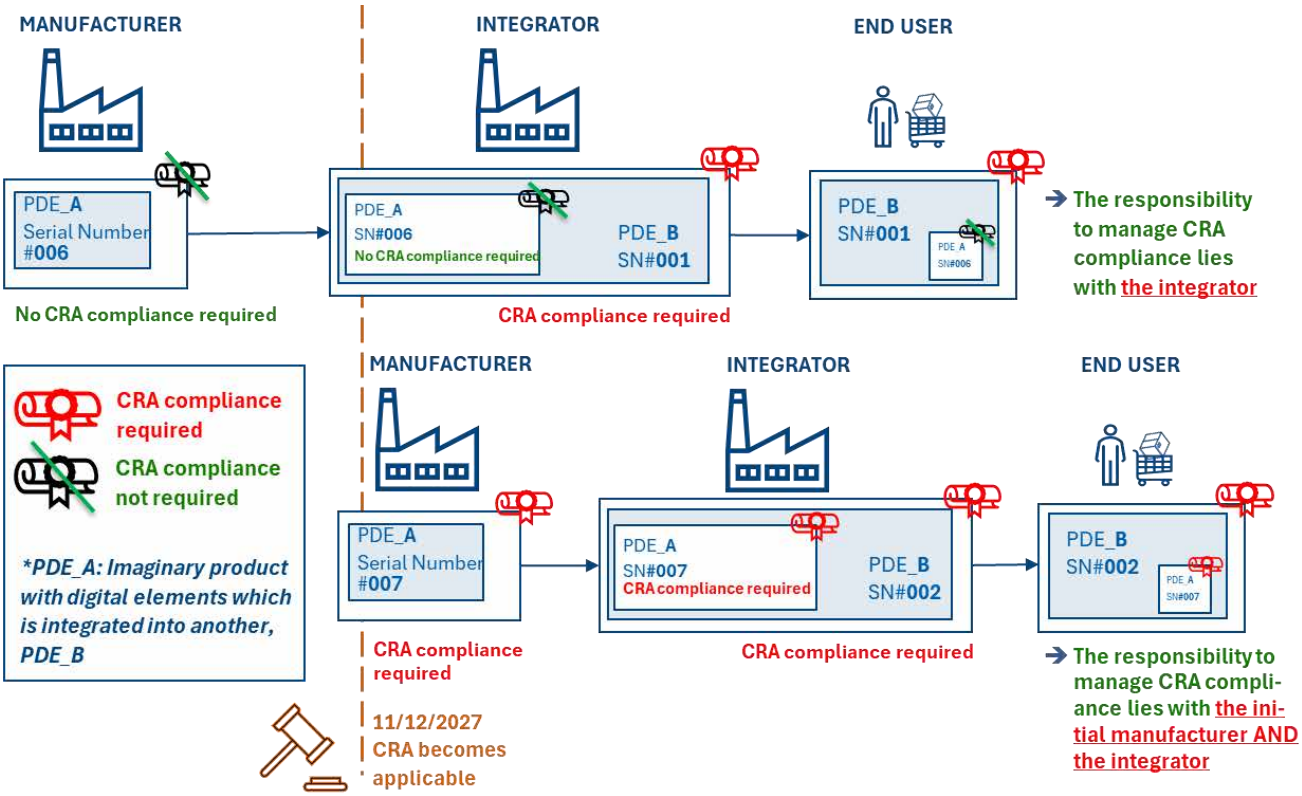


Diagram VI – Integrated component compliance and management

Based on the cybersecurity risk assessment, referred to in Art. 13(3), where the manufacturer determines that the residual risks at the component level – and their impact at the system level – are appropriately addressed, the manufacturer may use the CRA's flexibilities for acceptable compliance under the conditions applicable during system-level integration. This approach is explained in CRA recital 55, which states that where certain essential cybersecurity requirements are not applicable to a PDE, the manufacturer needs to identify and properly justify this in the technical documentation. Furthermore, where residual risks have been identified at the system level, compliance must be managed through mitigating countermeasures and risk management. The manufacturer shall describe this integration aspect in the user documentation (CRA Annex II): intended purpose, security environment (CRA Annex II, point 4), necessary measures (CRA Annex II, point 8a), information for integration (CRA Annex II, point 8f).

In simpler terms, the following approach to implementation is suggested:

1. No non-compliant PDE will be placed on the market after 11 December 2027.

2. Every PDE expected to be placed on the market after 11 /12/2027 will follow the necessary "security by design" principles to comply with CRA. Components, subsystems and systems (when placed on the EU market as individual products) are PDEs according to the CRA and consequently require CRA compliance for CE marking. They must be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks

to demonstrate CRA compliance. To this end, the manufacturer should perform the following steps:

a. For the manufacturing of components:
    i. Perform Risk Assessment at component level;
    ii. Fulfil all the applicable CRA essential cybersecurity requirements according to the risk;
    iii. Provide mitigating measures, if required and applicable (e.g. if some essential cybersecurity requirements are not applicable or if the component must interface with an existing insecure environment, section 2.6);
    iv. Provide information for the customer (integrator or asset owner) with application conditions if required, including Security Related Application Conditions (SecRACs);
    v. In B2B activities, agree on risk management – sufficient measures and residual risk – and vulnerability handling with the customer.

b. For the manufacturing of functional subsystems and systems:
    i. Produce a list of components the subsystem or system consists of and, with information about the classification (Critical, Important class I, Important class II or Default);
    ii. Perform risk assessment and provide traceability back to the components' security related application conditions. In addition, if agreed in a B2B context, Cyber Critical Assets (CCA) – a concept defined in the upcoming IEC 63452 – should be identified.
    iii. Fulfil all the applicable CRA essential cybersecurity requirements according to the risk assessment;
    iv. Provide mitigating measures, if required and applicable;
    v. Provide documentation for the asset owner with application conditions (if required);
    vi. In B2B activities, agree on risk management – sufficient measures and residual risk – and vulnerability handling with the asset owner.

3. Projects (defined in section 2.7) whose development began before the CRA entered into force on 11/12/2024 and will conclude after 11/12/2027 will need to adapt to CRA requirements to ensure that their output is CRA-compliant. Such projects may need to integrate PDEs that are exempt from CRA compliance (see section 1.2.2) or that comply with the CRA through imposing requirements on the integration and the operating environment to fulfil the CRA essential cybersecurity requirements set out in Annex I Part I. For such PDEs made available on the market after 11/12/2027 the following conditions shall be taken into account:
    a. Each PDE must include a clear justification (on the basis of risk assessment) for the essential cybersecurity requirements of the CRA which are declared not applicable to that PDE in its technical documentation;

b. The risk assessment shall take into consideration its operational environment (reasonably foreseeable use and intended purpose);
c. The residual risk must be evaluated, including by defining mitigating measures. In addition, the security-related application conditions (SecRACs) shall be documented;
d. Both the justification and the evaluation of the residual risk (including application conditions for mitigating the risk) must be provided to the customer for information. It is recommended to have an early discussion and acceptance through an mutual agreement with the customer (see section 2.7.2) based on the previous steps *a* to *c* to avoid disagreement at a later project stage;
e. If no agreement is reached, the parties have to analyse and discuss the next steps to take on the basis of the individual project contract.
f. The manufacturer provides a CE marking with a compliance sheet expressing the application conditions and residual risk.

2.2 SUBSTANTIAL MODIFICATION

As per its definition (see section 1.1), a modification of a PDE is considered substantial when:

- It modifies the intended purpose (section 2.2.2) for which the PDE has been assessed, **OR**
- If the modification negatively impacts the PDE's compliance with the CRA essential cybersecurity requirements (section 1.4) for instance by increasing the attack surface.

The definition of substantial modification applies to products substantially modified after 11/12/2027, independent of when they were placed on the market.

A modification designed solely to decrease the level of cybersecurity risk of a PDE does not constitute a substantial modification under the CRA, provided it does not introduce new functionality or alter the product's intended purpose (CRA rec. 39). For instance, security updates addressing known vulnerabilities are not considered substantial modifications. This includes modifying functions or the performance of a product for the sole purpose of decreasing the level of cybersecurity risk.

A modification of the architecture (e.g., by adding new network links, components, or interfaces) likely qualifies as a substantial modification based on the above criteria. This also applies if the architectural change does not change the intended purpose, if compliance with the CRA essential requirements is affected.

The CRA defines substantial modifications in art. 3.30 as well as in recitals 38, 39, 40, 41, 42.

Note: further guidance for Substantial Modification is planned to be developed and provided by the European Commission. This section may be reviewed accordingly to align with EC Guidance when available.

2.2.1 APPLICATION

To ensure continued compliance, the possible impact of the modification should be confirmed with the asset owner based on the following procedure:

1. Every change to an existing PDE is to be analysed by the manufacturer (entity who performs the change) to verify if it affects the intended purpose of the PDE, if it affects negatively the level of cybersecurity risk or compliance with the essential cybersecurity requirements set out in Part I of Annex I of the CRA. If at least one of these conditions is fulfilled, the modification is substantial according to the CRA.

2. If the analysis results in the conclusion that no substantial modification is present, the result has to be documented. The result shall be communicated at an early stage to the asset owner.

3. If the analysis results in the conclusion that a substantial modification is present, the manufacturer (entity who performs the change) has to verify the conformity, and must ensure that the modified PDE meets the CRA essential requirements. In case of substantial modification of important or critical PDEs (see section 2.2), a new third-party assessment may be required. A substantial modification to a component can have an impact on the higher level (set of components or subsystem) leading to substantial modification at higher level (and need to reassessment for CRA compliance). However, a substantial modification to a component or a fixed set of components does not automatically require the entire set or the subsystem it is integrated into to comply with the CRA, unless it also qualifies as a substantial modification of the set, subsystem or system. The asset owner shall be informed about the result of the analysis.

It is recommended that manufacturer aligns with the asset owner at an early stage on the status of a modification as "substantial" and on its defined impact. This alignment does not reflect a transfer of accountability to the asset owner.

Note: The modification of a PDE might have impact on its integration in broad subsystems or systems. This must be managed in the individual B2B relationship.

2.2.2 INTENDED PURPOSE

According to CRA art. 3.23, the "intended purpose" of a PDE is the use for which a PDE is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

The key elements which constitute the intended purpose of the PDE are its **main functions** as well as its **context and conditions of use**. Considering a functional subsystem composed of functions:

- The modification of an existing main function (including configuration update) does likely not constitute a change to the intended purpose.
- Adding a new main function to the subsystem likely constitutes a change to the intended purpose.

Note: main functions are related to the list of functionalities provided by the PDE. Whereas core functionality as defined per the CRA allows to define the category of PDEs according to section 1.3 of the guidance.

The following table illustrates several practical examples of modifications and their consequences on the PDE's intended purpose:

Example of Modification	Intended purpose status
A TCMS (that manages control and command in a rolling-stock) is modified (software/application only) without new main function added and without new components added (e.g.: A software change inside a door management subsystem to change the door's behaviour)	**No change of the intended purpose** (control and command that includes door control function)
A SCADA is modified (software/application only) without new main function added and without new components added (e.g.: to add a new datapoint and/or symbol without changing the process)	**No change of the intended purpose**
An interlocking software update to integrate another point or signal of the already existing type due to change of track layout requirements without new main function added and without new interface types.	**No change of the intended purpose**
A TCMS on which a new main function is added with potential new associated risk (e.g.: adding a new part managed by TCMS such as wired lighting replaced by software-controlled lighting management)	**Change of the intended purpose**
A SCADA on which a new main function is added (e.g.: adding a new zone(s) for database server or API to other railway systems)	**Change of the intended purpose**
An interlocking receives a new central diagnostic system with remote access interface, which wasn't available before.	**Change of the intended purpose**
A TCMS already including a telemetry functionality, is modified (software/application only) to improve the data generated by telemetry functionality (e.g.: Adding a new diagnostic report from an existing component), without new link, ne w component, or new exposure.	**No change of the intended purpose** (control and command that includes a telemetry diagnostic functionality)
A SCADA already including a telemetry functionality, is modified (event alerting and monitoring) to improve the data generated by the telemetry functionality (e.g.: Adding a new message from an existing component), without new link, new component, or new exposure.	**No change of the intended purpose** (SCADA that includes a telemetry diagnostic functionality)
An interlocking software update to mitigate vulnerabilities.	**No change of the intended purpose**
A subsystem is modified (for obsolescence treatment) without new main function being added, without change in intended use and environment (e.g.: no new architecture, no new exposure).	**No change of the intended purpose**

Table IV – Examples of modifications

2.2.3 OBSOLESCENCE TREATMENT

To maintain systems over a long period of time, as is the case in the rail sector, spare parts are required. However, over time some parts may be no longer produced or slightly modified to address obsolescence. Following a strict interpretation of CRA art 2.6 (see section 2.3), only exactly identical parts are considered spare part under the CRA. As a result, **replacement parts that perform the same function but are not identical to the original cannot considered spare parts under the CRA**, even if cybersecurity is not affected by the change. **Such parts can be called "functional replacements" to distinguish them from the identical spare parts defined in the CRA.**

This section clarifies how to deal with obsolescence management in relation to functional replacements.

Where the replacement component is not identical according to CRA art. 2.6, it has to be analysed if the replacement component constitutes a substantial modification of the product it is integrated in. According to CRA rec. 42 **a PDE being subject to "refurbishment", "maintenance" and "repair" does not necessarily lead to a substantial modification**, for instance if its intended purpose and functionalities are not changed and the level of risk remains unaffected (Blue Guide section 2.1). This concept can also be applied if the repair is not performed at the installed PDE but brought in via a functional replacement.

Replacing defective parts or worn items by parts that perform better (e.g. because the old part is no longer produced) also does not in itself trigger a substantial modification of the repaired product. The manufacturer is not required to recreate historical design or test documentation, as this would not contribute to enhancing the cybersecurity of the product.

As a result, in the context of a repair, if the supplier of the replacement has assessed that modification is not substantial and documented the result of the analysis, **a functional replacement can generally be integrated into an existing system without triggering a substantial modification.**

Here below some examples are provided to support the application. A indicates PDE-A, the PDE concerned by obsolescence treatment, and B indicates PDE-B, the PDE where the PDE-A is integrated in.

- Change of a chip (or a set of chips) (A) on an existing electronic card (B)
- Change of an electronic card (A) in a calculator (B)
- Change of a module (A) in a PLC (B)
- Change of a camera (A) in a CCTV architecture (B)

Obsolescence treatment requires changing PDE-A with a new one (PDE-Av2) because the original (PDE-Av1) is no longer produced. If the performance change or the way the repaired

product operates doesn't affect the intended purpose and the cybersecurity (no new cybersecurity risk or exposure) of the overall product (PDE-B), the change from PDE-Av1 to PDE-Av2 does not trigger a substantial modification of the repaired product PDE-B.

As a result, the CRA conformity of PDE-B is limited to the obsolescence treatment (PDE-A v1 to PDE-A v2) itself:

- The need for CRA conformity is limited to the PDE-A (sub-component treated for obsolescence)
- Thanks to the demonstrated non-substantiality of the modification to PDE-B, PDE-B does not need to become CRA compliant, and it is not required to recreate historical design or test documentation for PDE-B.

In conclusion, a replacement made in the context of obsolescence treatment that constitutes a non-substantial modification in specification due to "refurbishment", "maintenance" and "repair" constitutes a functional replacement and does not require the PDE in which the new replacement part is integrated into to become CRA compliant.

2.2.4 MODIFICATION BY OTHER ACTORS

If an actor, other than the original manufacturer of the PDE, performs a substantial modification, that actor become responsible for evaluating the significance of the change and handling the CRA compliance as a manufacturer, if they make the PDE available on the market. If the asset owner performs the substantial modification, it is recommended that the asset owner coordinates with the original manufacturer to obtain additional support on a contractual basis.

If the actor is an importer or distributor and makes that modified product available on the market, it shall be considered to be the manufacturer and will be subject to the CRA manufacturer obligations (section 1.4.2).

If the actor is an end-user such as a railway operator, it does not become a manufacturer, as long as it is only using the modified PDE and not making it available on the market. The moment said end-user sells it to another legal entity (including under the same holding umbrella), it becomes a manufacturer for the part of the PDE they substantially modified or the PDE as a whole depending on the impact of the introduced change (CRA art. 22) for the remaining duration of the original manufacturer's support period.

In cases where the end-user performs a substantial modification on a PDE that is intended for its own use and does not wish to agree on a support contract with the original manufacturer which takes into account this modification, it becomes impossible for the original manufacturer to be responsible for the entirety of the modified PDE**.** In this case, it is recommended that the end user assume partly or entirely the manufacturer obligations, even if the PDE is not made available in the market again. The following chart details the

proposed handling of responsibilities in different cases of PDE modification by the asset owner:

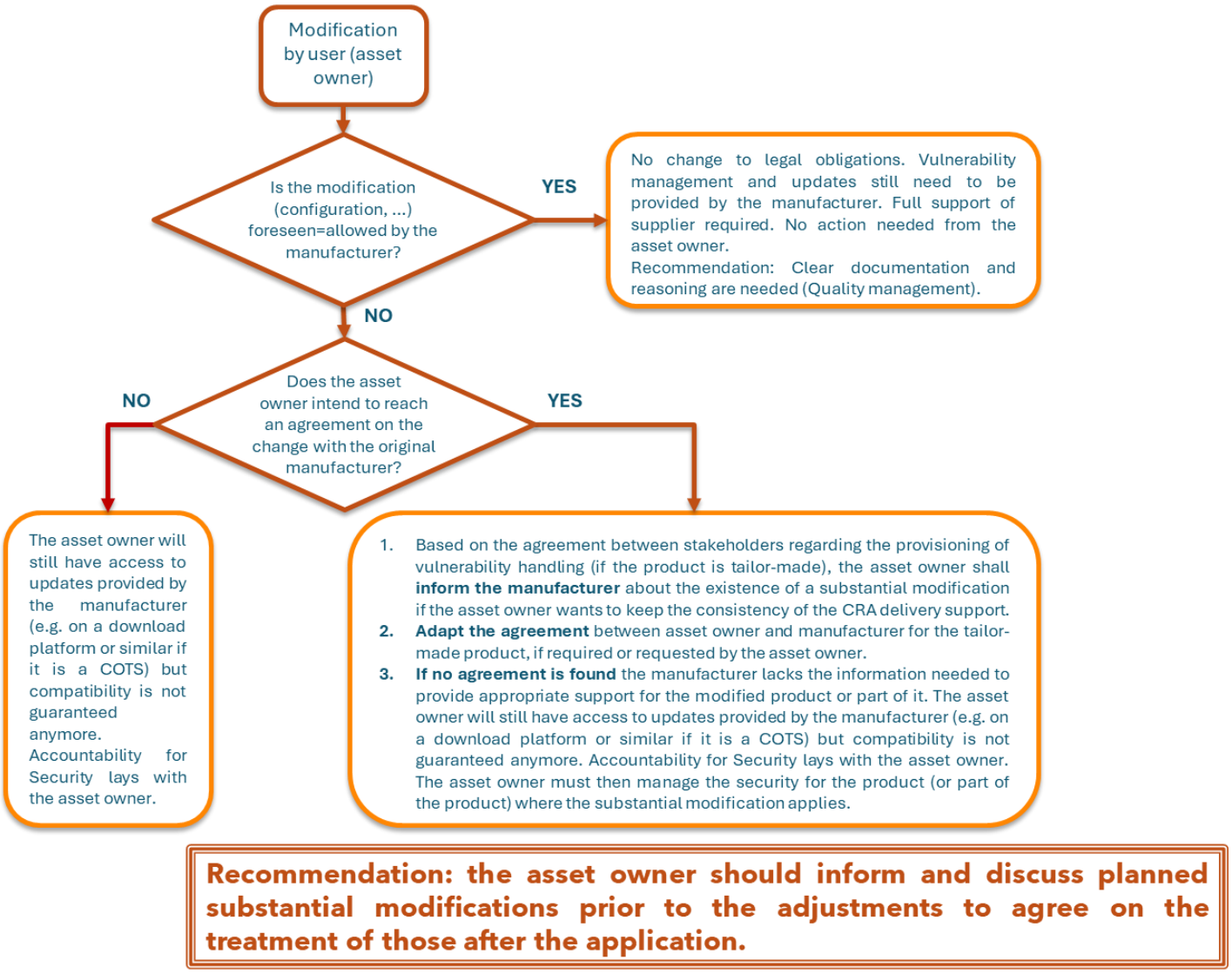


Diagram VII – Modification by asset owner

If the support period is ongoing, it is recommended that the asset owner informs and discusses planned substantial modifications with the manufacturer prior to their implementation, in order to agree on the support to the modified product.

2.3 SPARE PARTS

As seen in section 1.1, art. 2.6 of the CRA defines spare parts as products "*that are made available on the market to replace identical components in PDEs and that are manufactured according to the same specifications as the components that they are intended to replace*".

Such spare parts are excluded from the scope of the CRA and from the need for CRA compliance, and can be manufactured, made available on the market and integrated with no limitation within the context of repairing existing products.

2.3.1 APPLICATION

The CRA definition of spare parts hinges on the terms "identical" and "same specifications", which are not elaborated further within the regulation. As such, it has been the subject of much discussion. According to a recent draft guidance by the European Commission (*Draft Communication from the Commission - Commission guidance on the application of the CRA)*, the definition should be interpreted very strictly, limiting the category to **identical or "original" spare parts, using the exact same hardware and software as the part they replace.**

This strict interpretation excludes **parts that have the same functionalities as the original part, but which make use of new hardware and/or software due to obsolescence (i. e. *functionally* identical spare parts or "functional replacements").** Instead of being excluded from CRA compliance like identical spare parts, these functionally identical spare parts may constitute a product in its own right and therefore fall within the scope of the CRA. For further guidance on how to integrate replacement parts for obsolescence treatment, see section 2.2.3.

As a recommendation, production and delivery of CRA-compliant spare parts (hardware and software) that can be used both as new components and as spare parts before and after the end of the transition period (11/12/2027) would prevent costly changes later in operational systems and reduce number of spare parts for railways and suppliers to maintain in inventory. Such spare parts would ease the transition of existing systems to CRA compliance (see section 2.6 on System Extension). By limiting the CRA compliant spare part's functionality, the integration into systems/products in use is possible with an information to the customer, but without affecting their approval.

Newly designed or updated products (with CRA compliance), whose functionality have been **limited through configuration** to only perform the functions of the part they replace, in a way that does not modify the intended purpose of the part and does not bring additional threats or exposure to the legacy product they are integrated in, could be considered as spare part because used with identical specifications in the original purpose.

Example:
In an existing system a PLC in version 2 (not CRA-compliant) needs to be replaced due to malfunction. The PLC is only available in a newer version 3 (CRA-compliant). To use the newer version 3, some of its functionalities, including cyber security features, need to be disabled for compatibility reasons, to allow its use in the existing system. Disabling these features may go against the conditions of use guaranteeing the CRA compliance of version 3. In this case the PLC version 3 is used in a non-CRA compliant configuration, but due to its use as a spare part only, it is acceptable under the accountability of the user. In addition, the integration of the PLC version 3 needs to be analysed to ensure that it does not increase the cybersecurity risk of the legacy product it is integrated in.

2.4 SUPPORT PERIOD

Manufacturers are required to determine the support period for each PDE so that it reflects the length of time during which it is expected to be in use (art. 13.8). However, **manufacturers should not simply declare support periods that correspond to the expected use time**. They must include the information that was taken into account to determine the support period of the PDE in the technical documentation as set out in CRA Annex VII. Therefore, they should take the following elements into account:

- Reasonable user expectations;
- The nature of the product, including its intended purpose;
- Other Union law determining the lifetime of PDEs.
- Other relevant factors that manufacturers may consider include:
- The support period of similar products placed on the market by other manufacturers;
- The availability of the operating environment;
- The support period of third-party integrated components providing core functions;
- Relevant guidance provided by the CRA ADCO.

All the listed factors should be considered in a manner that ensures proportionality in the determination of the support period. The minimum allowed support period is either five years or the expected use time of the PDE, whichever is shorter.

Support periods should be determined accordingly and cover a reasonable proportion of the expected use time.

Note I: it is strongly recommended that B2B contracts clearly identify the support period

Note II: further guidance will be provided by the Commission on the topic of support periods (CRA art. 26).

2.5 TAILOR-MADE PRODUCTS

The CRA has specific provisions related to tailor-made products (Annex I part I, art. 2b & Annex I part II art. 8). Under these provisions, tailor-made products are allowed two exemptions from the regulation's general requirements:

- In dealing with a tailor-made product, the manufacturer and business user can decide, through mutual agreement, that the necessary security updates will be delivered for a fee, instead of being free of charge;

- At the request of the business user, a manufacturer is allowed to deliver tailor-made products without an active “secure by default” configuration and the “reset to default” option. However, the product must still have the capability to be configured securely.

Tailor-made PDEs are still within the scope of the CRA and must apply all other requirements. The status of tailor-made does not grant an exclusion from CRA requirements. Without an agreement between manufacturer and business user the rules of the CRA are fully applicable even to tailor made products.

Manufacturers and asset owners within the rail sector make widespread use of customisations on their products. To help the sector take advantage of these provisions without overextending the definition, the following recommendations are meant to help determine what should be considered a tailor-made product or not. The general rule is as follows:

A product with digital elements is considered tailor-made when the technical solution is engineered or adapted based on specific and unique customer requirements, so that additional design/development work is required. This applies in particular to all categories of special vehicles.

In addition, the following criteria should be applied to determine if a product is tailor-made:

A product is not tailor-made **only** because of:

- Changes in parameters (e.g. selecting functionality by configuration inherent in the product design);
- Changes in configuration which are in a defined range or don’t need customised processes on the manufacturer side;
- Development of the PDE following standards like TSI, ERJU System Pillar or EULYNX;
- Combination of available PDEs in a project-specific way, as long as the product’s standard capabilities are used and no design/development work is required (e.g. a PLC with I/O Modules, or a Substation with different amount of the same shortcut breaking units).

A product with digital elements should not be considered tailor-made only because of changes in mechanical design or hardware without having impact on the software or

configuration and thus on the obligations to provide vulnerability management and security updates, e.g.:

- replacing a 24” display by a 28” display with the same resolution;
- adding a redundant instead of a single power supply (e.g., for a server).

In general, PDE categories listed as Important class I, Important class II or Critical in Annexes III-IV of the CRA are not to be considered tailor-made, as they include COTS network products (modems, switches, routers...), security products (Firewalls, IDS, IPS, EDR/XDR, AV, IAM, PKI, SIEM, HSM, ...), Operating Systems, Hypervisors, Secure microcontrollers, smartcards and PLCs. Exceptions are possible.

Similarly, any PDE present in a catalogue (e.g. product offer + price) of a supplier or system integrator should be considered as a COTS, and consequently not as tailor-made.

2.5.1 PROVIDING UPDATES TO TAILOR-MADE PRODUCTS

As the CRA allows for the delivery of security updates to tailor-made products with digital elements for a fee, instead of being free of charge, the following actions are recommended:

- The "tailor-made" status needs to be justified by the manufacturer and accepted by the asset owner. This acceptance is a prerequisite before contractual agreement.
- The manufacturer is obliged to manage vulnerabilities occurring in its products throughout the contractually agreed upon support period. The costs for remediating these vulnerabilities should be mutually agreed upon including terms like update frequency and support period in the service contract.
- The manufacturer should agree on a standard update frequency for security updates for business calculation purposes (e.g. 6 months, 12 months...) in the service contract.
- The manufacturer should agree to the planned support period for security updates proportional to the foreseen life-cycle (e.g. 5 years, 10 years, 20 years...). Also, as a prerequisite before contractual agreement, the manufacturer shall provide information about the support period of non-tailor-made (COTS) products.
- After the agreed support period, the manufacturer should offer the asset owner a service agreement for continued maintenance of the products at reasonable and customary market conditions.

The support period may also be fulfilled by planned hardware or software replacements. This may, for instance, apply for a complex system like a rolling-stock with regular replacement of components (e.g. critical category COTS products) with a compatible support period. It may be possible that, after replacement, the asset owner manages the replaced products independently from the manufacturer of the complex system.

2.6 COMPATIBLE SYSTEM EXTENSION

Once the CRA becomes fully applicable, upgrades and extensions of existing systems – whether of infrastructure or rolling-stock – made after 11/12/2027 will fall within the scope of the regulation.

This creates a conflict between meeting the cybersecurity requirements of the CRA and ensuring compatibility between upgraded or added components and the older systems they integrate with. Compatibility is essential for the continued operation of these systems and, in some cases, is mandated by rail-specific interoperability related legislation.

According to CRA recital 55, essential cybersecurity requirements must be applied based on actual risk and in alignment with interoperability obligations set by other regulations, such as the Technical Specifications for Interoperability (TSI). Therefore, a manufacturer may justify in the technical documentation of that PDE that certain cybersecurity requirements do not apply to that PDE by virtue of necessitating compliance with interoperability related legislation.

For the purposes of this guidance, a PDE respecting these conditions is labelled a **compatible system extension**, and defined as follows: **a new component, set of components, subsystem or system added to an existing system or railway system that needs to interact with existing systems or railway systems and, therefore, is meant to be interoperable with existing systems or railways systems on external interfaces. Additionally, the new component, set of components, subsystem or system added to an existing system or railway system does not necessarily qualify as a substantial modification of the existing system.**

2.6.1 APPLICATION

If a regulation (e.g. a TSI) or the presence of legacy systems requires the PDE to use interfaces that are not fully compliant with the relevant requirements of the CRA. It is recommended for the manufacturer to align with the asset owner at an early stage on the outcome of the analysis and the measures to be taken, and to then take the following actions:

1. Provide a justification in the technical documentation. Acceptable justifications are:
    a. Obligations of interoperability coming from TSIs or other EU legislation;
    b. The need to follow outdated standards in order to ensure compatibility with existing system interfaces, where the Product with Digital Elements (PDE) would not be able to perform its intended function without doing so. In the cybersecurity risk assessment, evaluate how the PDE in question interacts with the existing system and with the railway system as a whole

2. Address any risks resulting from parts that are not compliant with some of the essential cybersecurity requirements, for instance by:
    a. Adding compensating countermeasures;
    b. Limiting the intended purpose of the PDE;
    c. Defining additional requirements to the operating environment;

3. Inform the asset owner of chosen measures (a-c) and the resulting residual risks.

In every case, this approach is only valid for the interoperability interface. This has no impact on the design of the rest of the PDE.

Here follows a list of examples of compatible system extensions:

- New coach in a block train that needs to interact with the rest of the existing block train;
- New coach that needs to be compatible to an existing fleet;
- New Eurobalise on an ETCS line that needs to interact with on-board units of the existing fleet;
- Onboard unit of a new rolling-stock on existing ETCS line that needs to interact with existing Eurobalises and RBC along the track;
- New station of a metro line that needs to interact with the existing signalling system and fleet;
- New infrastructure to a national train control system that needs to interact with existing fleet;

- New rolling-stock with latest onboard unit baseline that needs to interact with existing national train control system;
- Connection of industrial complex to an existing railway line that needs to interact with the existing signalling system and fleet;
- New siding to an existing railway line that needs to interact with the existing signalling system and fleet.

It is essential to highlight that all new compatible system extensions made available on the market after 11/12/2027 must be entirely CRA-compliant PDEs. They will however have the capability to interoperate with older existing equipment through legacy interfaces and protocols.

Note: a system extension implies one or more interfaces between a new part delivered under the CRA framework, and an existing part already in place outside the CRA framework. The CRA conformity of the new part delivered has to take into account this interface and the mandatory interoperability or the technical compatibility associated. The impact of the new part added on the existing part needs also to be taken into account. A risk analysis regarding the interface(s) should be performed by the integration stakeholder to identify the potential impact of the new part on the existing one. Depending on the results, the system extension does not necessarily qualify as a CRA substantial modification of the existing system, nevertheless, independently of the CRA, implementation of security measures or controls could be needed on the interface(s), on the new part or on the existing part to well manage the cybersecurity risks at system level.

2.7 PROJECT-BASED APPROACH AND ONGOING PROJECTS

The railway sector is a critical infrastructure – as identified under the NIS2 Directive – governed by extensive regulatory frameworks to ensure safety, interoperability, and operational continuity. As a result of these frameworks and the long life-cycle of its products, the sector is characterised by complex, long project cycles, with major infrastructure or rolling-stock projects often spanning 7 to 20 years from planning to completion.

Railways operate as systems of systems – interconnected across borders and integrating legacy technology with emerging digital components – under the oversight of national and European regulators. The introduction of the CRA and its cybersecurity obligations pose a challenge to the sector industry. However, it is essential that all stakeholders including manufacturers adapt to new challenges and new risks brought by growing digitalisation. All stakeholders from the sector must adapt their working methods to tackle these risks and conciliate safety and cybersecurity in their risk management practices.

The unique operational and regulatory structure of the railway sector functions has been adopted with a **project-based approach** in mind. Railway systems are typically developed and deployed as large-scale, long-term projects involving complex integration of infrastructure and rolling-stock – often across national borders. Within these projects, components are carefully selected, certified, and installed as interoperability constituents under the TSIs, with well-established approval and assurance processes designed to guarantee system-wide safety and compatibility.

While the CRA does not make use of the concept of "project", dealing only with individual PDEs, its cybersecurity requirements have significant impact to projects. In order to achieve the CRA's and NIS2's objectives of more secure products and infrastructure in a consistent and practical way, it is essential to analyse and manage the legislation's impact on ongoing projects. This guidance therefore defines how the CRA's objectives – particularly around digital security – are aligned with the railway industry's project-driven, safety-critical framework.

For the purposes of this guidance, a project is a B2B-scoped assignment between an asset owner and a manufacturer – either system integrator or product supplier – involving design, tests, certification and acceptance, carefully planned to achieve a delivery of a specified number of 'products' for operation, including migration/integration and acceptance. The products designed, developed and delivered within a project are in many cases PDEs.

A project, based on a requirements specification, is covered by a contractual agreement that defines the starting point (beginning of project) and the end (migration/integration and end of delivery, including warranty and potentially options).

Examples of projects are the acquisition or renovation of a fleet of rolling-stock, of a set of RBCs for an ERTMS line, of an energy power station, as well as an extension for a metro line or for a fleet of rolling-stock.

For the purpose of this guidance, **pre-existing projects** are projects whose development began before the application date of the CRA (11/12/2027) and whose output will partially or entirely fall under the scope of the CRA, due to it being delivered at least in part after 11/12/2027. These projects were designed and approved with sets of technical specifications which at the time could not yet take the CRA essential requirements into account. Guidance on adapting pre-existing projects to the CRA is presented in the next sections.

2.7.1 APPLICATION

The CRA applies equally to all PDEs placed on the market or made available on the market with substantial modifications after 11/12/2027 even if the contract for sale of that PDE was concluded before 11/12/2027 or even before 11/12/2024. However, to ease the adaptation challenges of pre-existing projects while remaining in line with CRA, the following approach is particularly recommended for pre-existing projects (see also Project 1 and 2 in Annex B of this guidance).

- Every PDE placed on the market after 11/12/2027 must be CRA compliant.

- It is possible that PDEs components selected for pre-existing projects may not fulfil all the risk-based essential requirements, following the exemption (CRA art. 69.2, see section 1.2.2) or interoperability requirements (CRA rec. 55). In such cases where a component only fulfils a subset of risk based essential requirements, the following procedure shall apply:
    1. The manufacturer provides a risk analysis for the component, subsystem or system for the pre-existing project;
    2. Each PDE includes a clear justification for each requirement not met in the cybersecurity risk assessment at the system level, as well as an analysis of the residual risk, to inform the customer;
    3. Mitigating measures are proposed to reduce the initial residual risk;
    4. The residual risk may be managed at system level;
    5. The residual risk may be communicated in advance to the asset owner, and an agreement is recommended(see section 2.7.2).

Note I: in general, and independently of the CRA, residual risks and SecRACs shall be validated and accepted by the asset owner under the contractual agreement for the project – if such a requirement had been included in the agreement. Of course, these

residual risks shall be aligned and consistent with the residual risks analysed for the CRA compliance provided by the manufacturer.

Note II: The major difference between Project 1 (signed before 2024) and Project 2 (signed after 2024) is the following:

- for Project 1, the (sub)system (subsystem 1.2) may stay "as is" from a technical standpoint if CRA compliance can be proven;
- for Project 2, all subsystems (subsystem 2) shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance.

See tables in Annex B for more details

2.7.2 MANUFACTURER – ASSET OWNER RISK ACCEPTANCE VIA MUTUAL AGREEMENT

The CRA allows for some flexibility in how manufacturers fulfil the essential cybersecurity requirements for their PDEs, as explained in section 2.1.1 – e.g. integrating PDEs that are exempt from CRA compliance or that comply with the CRA through imposing requirements on the integration and the operating environment. However, in such cases transparency and communication between manufacturer and asset owner are essential.

To facilitate both the PDE's risk assessment – i.e. the essential requirements it implements – and the residual risk acceptance by the customer, the following procedure is suggested:

1. To ready the product for CE marking, the manufacturer has the obligation to document the cybersecurity risk assessment and how the CRA essential requirements are implemented in the technical documentation. In addition, the manufacturer has to provide information and instructions to the user for actions to be performed by the user (application conditions).

2. Supplier and customer should engage in an exchange of information regarding:
    a. Security related application conditions (SecRACs according to TS 50701/IEC 63452) for the security capabilities that cannot be provided by the product;
    b. The operational environment of the product;
    c. Compensating countermeasures provided by the manufacturer.

3. Supplier and customer should mutually agree on the mentioned points in order to avoid discussions later in the project. The agreement should be formalised and be enacted as soon as possible. The cybersecurity case can be or may be in the future, a valid basis for this formal acceptance (current TS 50701, IEC 62443 and the future IEC 63452). However,

if no agreement is reached the manufacturer provides the relevant information to the customer.

> Note: the cybersecurity case can be created in an earlier project phase and be updated in the project's life-cycle.

4. **The agreement shall not be interpreted as a transfer of accountability from the supplier to the customer nor as a relief to the manufacturer to comply with the CRA requirements**. Each party retains responsibility for their respective obligations under the contractual and regulatory framework.

5. The agreement cannot be extended to other customers or future separate transactions. As such, it does not allow the supplier to make the product generally available on the market to other customers without justifications for the CRA variance used and a consequent mutual agreement with said customers.

2.8 SOFTWARE BILL OF MATERIALS (SBOM)

A Software Bill of Materials (SBoM) is a formal, machine-readable inventory documenting all components, libraries and dependencies within a software product. The inventory contains the details and supply chain relationships of various components used in building software. SBoMs are widely used in the sector to offer increased transparency and speed up the identification of vulnerabilities.

The CRA (Annex I Part II) mandates the use of SBoMs covering at the very least the top-level dependencies of the PDE as a means to identify and document vulnerabilities and components.

To ensure compliance with the CRA, the following practice should be followed with regards to SBoMs:

- Manufacturers have the obligation of maintaining a SBoM of each PDE to perform vulnerability management and meet patching or mitigations obligations;
- Manufacturers have the obligation to share SBoM with a Market Surveillance Authority, if requested;
- Manufacturers are recommended to provide top-level dependencies SBoM in a commonly used and machine-readable format to its users. “Top-level” means that the SBoM shall contain at the minimum the description of all components, which the primary component directly depends on, in addition to the description of the primary component.

The sharing of detailed SBoM with users is subject to B2B contracts, under which the protection and sensitivity of information must be defined. Detailed SBoM may not be available to users due to Intellectual Property or Patent laws.

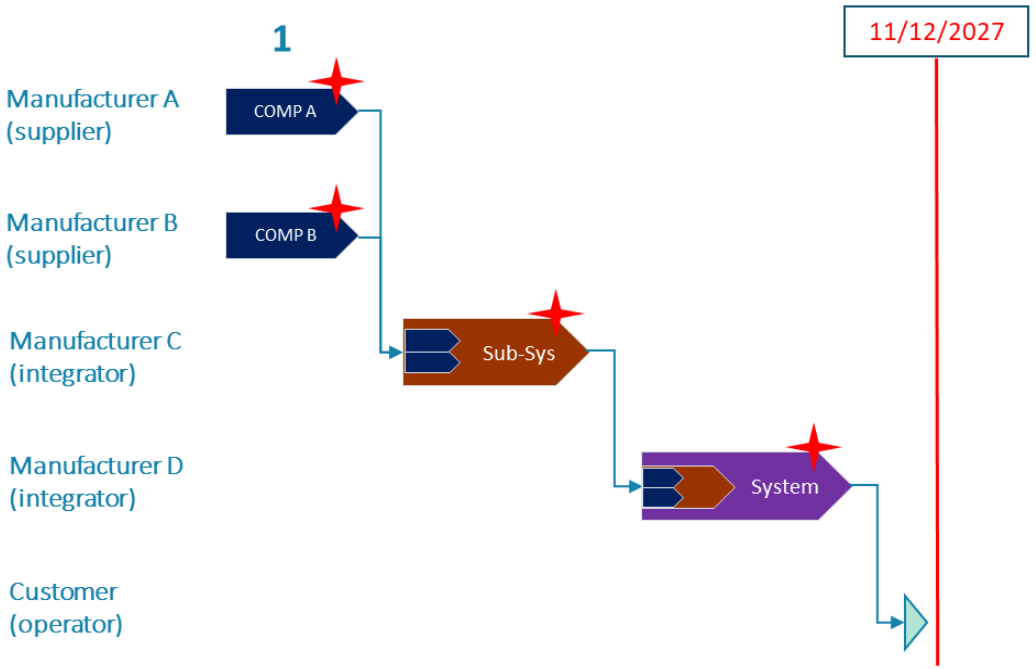
Note: details on how, when and under which conditions to deliver an SBoM to the asset owners will be integrated in a future iteration of these guidelines. The CRA does not mandate practices on the topic, but SBoMs may be the object of an implementing act by the European Commission, and the topic is highly relevant for security monitoring and vulnerability management for the asset owners. For further details and an example, the technical guideline TR-03183 may be used.

ANNEXES

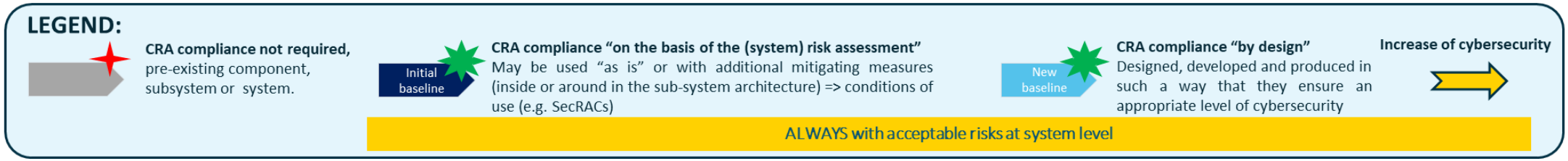
A. ONGOING PROJECTS: PROGRESSIVITY AND PRIORITISATION

The schemes below illustrate how to apply in four steps the project-based approach, generically described in Annex B and C, to the concrete use-case of an on-going project.

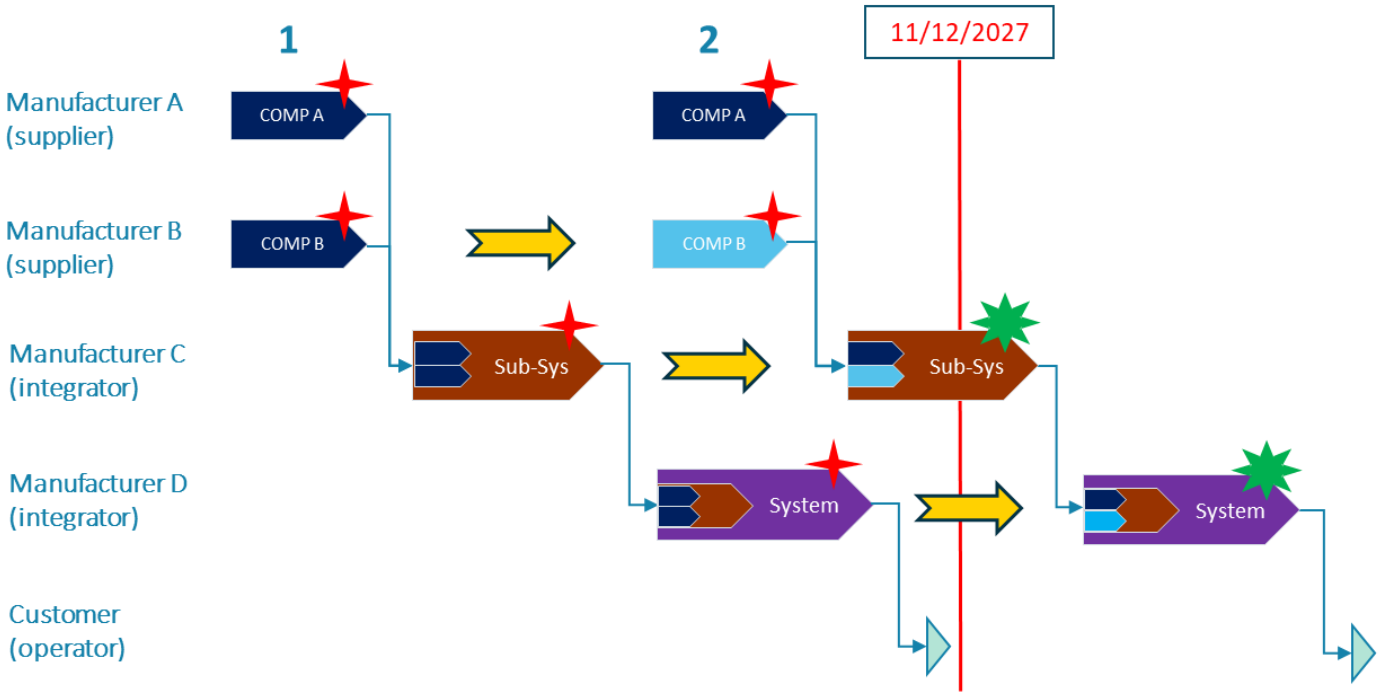
Ongoing Projects: Progressivity and Prioritisation



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



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)

LEGEND:

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

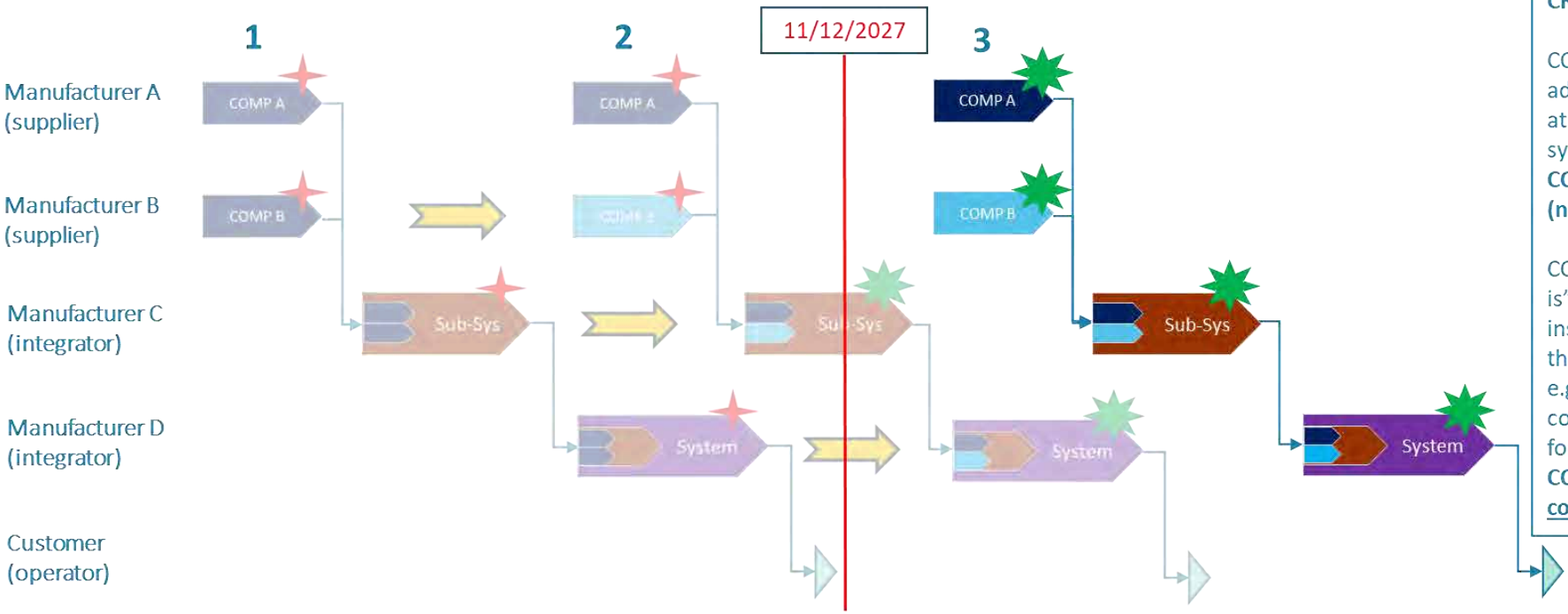
Initial baseline — **CRA compliance "on the basis of the (system) risk assessment"** May be used "as is" or with additional mitigating measures (inside or around in the sub-system architecture) => conditions of use (e.g. SecRACs)

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

Increase 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 for all

COMP B (new baseline) was already adapted to allow achieving compliance at system level (acceptable risks at system level)
COMP B is CRA compliant by design (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 through conditions of use (Annex 2)

LEGEND:

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

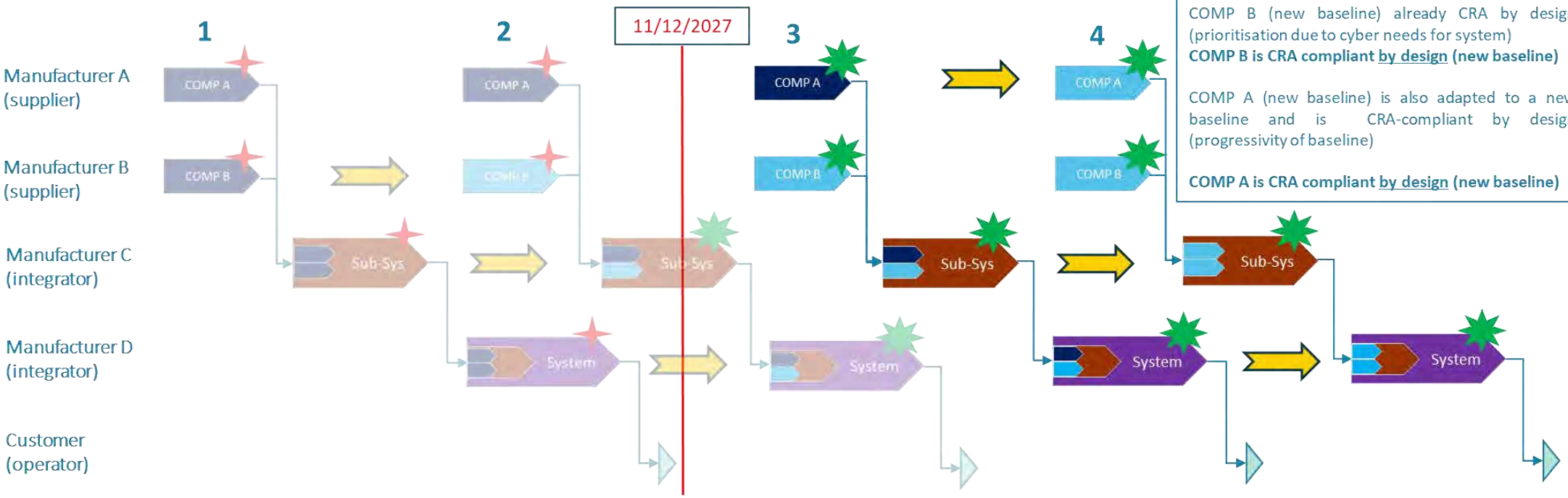
Initial baseline — **CRA compliance "on the basis of the (system) risk assessment"** May be used "as is" or with additional mitigating measures (inside or around in the sub-system architecture) => conditions of use (e.g. SecRACs)

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

Increase 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)

LEGEND:

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)

New baseline

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

Increase of cybersecurity

ALWAYS with acceptable risks at system level

B. USE-CASE APPROACH

This section presents three tables with use case approaches for and "naming" of **COMPONENT**, **(SUB)SYSTEM** and **PROJECT** to facilitate exchanges during projects discussions. Based on PROJECT approach, some cases (SUB)SYSTEM and COMPONENT could be applied.

USE-CASE APPROACH (PROJECT)

Use-case	Nature of the Project	Application for the Railway Sector
PROJECT 1	Project for delivery with (sub)systems contract signed **before** 11/12/2024 **and** starting delivery **before** the CRA application date of 11/12/2027 (e.g. rolling-stock series) *In case of purchase options / decision to buy the same (sub)system decided after 11/12/2027 ; PROJECT 1 could continue to be applied, based on the initial delivery*	*COMPONENT 1.2 and (SUB)SYSTEM 1.2 could apply.* The manufacturer (provides, based on a risk analysis, the information required by the CRA which may include instructions for usage. It is recommended that the supplier and customer agree on the instructions for usage.
PROJECT 2	Project for delivery with subsystems contract signed **after** 11/12/2024 **and** starting delivery also **after** the CRA application date of 11/12/2027 (e.g. rolling-stock series)	*(SUB)SYSTEM 2 applies*
PROJECT 3	PROJECT 1 Or PROJECT 2 and product (again) placed on the market **due to substantial modification** after 11/12/2027	*PROJECT 1 applies* *Or* *PROJECT 2 applies* *(SUB)SYSTEM 3 applies with compliance needed for the part with substantial modification*

USE-CASE APPROACH (SUBSYSTEM & SYSTEM)

Use-case	Nature of the product	Application for the Railway Sector
(SUB)SYSTEM 1.1	(Sub)systems made available on the market **before** the CRA application date of 11/12/2027 (and stopped being made available on the market by 11/12/2027)	No impact at (sub)system level **=> The (sub)system does not require CRA compliance**
(SUB)SYSTEM 1.2	(Sub)Systems (of a type): ► **already** made available on the market during the transition period (**before** "CRA application date" = 11/12/2027) ► **and further units placed** on the market after 11/12/2027. ► **and required for case [Project 1]**	**For the specific project (case PROJECT 1), the (sub)system may stay "as is" from a technical standpoint if CRA compliance can be proven by the following procedure.** For the case "PROJECT 1", in general the CRA applies, so the (sub)system should be analysed concerning the cybersecurity risk. Some to all essential requirements of Annex 1 may not be implementable. The risk shall be analysed, the components shall be properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen by the system integrator or the asset owner. The residual risk is to be managed **at system level**. Justifications (where applicable) to achieve the CRA compliance with CE-marking could be allowed if the residual **risks at system level** are acceptable. These justifications (and the context of usage / acceptability of these flexibilities regarding risks) needs to be identified in the technical documentation. **=> The (sub)system** (placed on the market after 11/12/2027) **requires CRA compliance with CE-marking. If the subsystem will be integrated, the integrator manufacturer shall exercise due diligence.**
(SUB)SYSTEM 2	(Sub)Systems placed on the market **after** the CRA application date of 11/12/2027 consisting of components of type COMPONENT 3 and/or COMPONENT 2 and/or COMPONENT 1	**The (sub)system shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance:** ▪ List of components classified as Critical / Imp Class 1 / Imp Class 2 / Default ▪ Risk Assessment that (if B2B agreed) identify Cyber Critical Asset (CCA) and make the link with Class of components ▪ Provide mitigating measures, if required and applicable ▪ Provide technical documentation with application conditions (if required) ▪ COMPONENT 1 can stay "as-is'; analysis of COMPONENT 1 impact in Risk Assessment of the (sub)system level **=> The (sub)system requires CRA compliance with CE-marking. If the subsystem will be integrated, the integrator manufacturer shall exercise due diligence.**
(SUB)SYSTEM 3 **Usage of IEC63452 & TS50701 may support CRA compliance**	(Sub)Systems already made available on the market and (again) placed on the market **due to substantial modification** after 11/12/2027	**The part of (sub)system with substantial modification shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance:** ▪ Impact at (sub)system level, limited to the part of (sub)system that was substantially changed ▪ Perform Risk Assessment at least for the scope "change and the boundaries of the change" ▪ List of components classified as Critical / Imp Class 1 / Imp Class 2 / Default ▪ Risk Assessment that (if B2B agreed) identify Cyber Critical Asset (CCA) and make the link with Class of components ▪ Provide mitigating measures, if required and applicable ▪ Provide technical documentation with application conditions (if required) ▪ Agree on risk management (sufficient measures and residual risk) and vulnerability handling with asset owner (B2B) **=> The adapted version of the (sub)system requires CRA compliance on the basis of the cybersecurity risk assessment at the "boundaries of the change". The rest of the (sub)system without change can stays as-is, if the change has no impact on the rest of the (sub)system and if the modification is not performed by the manufacturer, importer or distributor. If the modification of the (sub)system also qualifies as a substantial modification of the system, the measures listed above would have to be performed for the whole system.**

USE-CASE APPROACH (COMPONENTS)

Use-case	Nature of the product	Application for the Railway Sector
COMPONENT 1.1	Components made available on the market **before the** CRA application date of 11/12/2027 (and stopped being placed on the market by 11/12/2027)	No impact at component level **=> The component does not require CRA compliance**
COMPONENT 1.2	Components of a type ► **already** made available on the market during the transition period (**before** the CRA application date of 11/12/2027) ► **and further units placed** on the market after 11/12/2027. ► **and required for case [Project 1 x (Sub)System 1.2] or [Project 2 x (Sub)System 2]**	**For the specific project (case PROJECT 1/2), the component may stay "as is" from a technical standpoint if CRA compliance can be proven by the following procedure.** For the case "PROJECT 1&2", in general the CRA applies, so the components should be analysed concerning the cybersecurity risk. ▪ Some to all essential requirements of Annex 1 may not be implementable. The risk shall be analysed, the component shall be properly installed, maintained, used for its intended purpose or under conditions which can reasonably be foreseen by the system integrator or the asset owner. ▪ The residual risk is managed at component level. anticipating consequences at system level. ▪ Justifications for usage of flexibilities (where applicable) to achieve the CRA compliance with CE-marking could be allowed if the residual risks at component level (**and their consequences at system level**) are acceptable. These justifications, along with the context of usage / acceptability of these flexibilities regarding risks needs to be identified in the technical documentation. **=> The component** (placed on the market after 11/12/2027) **requires CRA compliance with CE-marking. If the component will be integrated, the integrator manufacturer shall exercise due diligence.**
COMPONENT 2	Components placed on the market **after** the CRA application date of 11/12/2027. Independently of any usage into any subsystem	**The Component shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance:** ▪ Perform Risk Assessment at component level ▪ Fulfil all the applicable CRA essential cybersecurity requirements according to the risk; ▪ Provide mitigating measures, if required and applicable ▪ Provide technical documentation with application conditions (if required) **=> The component requires CRA compliance with CE-marking. If the component will be integrated, the integrator manufacturer shall exercise due diligence.**
COMPONENT 3	Components already made available on the market and (again) placed on the market **due to substantial modification** after 11/12/2027.	**The Component shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance:** ▪ Perform Risk Assessment at component level ▪ Fulfil all the applicable CRA essential cybersecurity requirements according to the risk; ▪ Provide mitigating measures, if required and applicable ▪ Provide technical documentation with application conditions (if required) **=> The adapted version of the component (also if it is deployed in installed base) requires CRA compliance with CE-marking.**

Usage of 62443-4-x may support CRA compliance demonstration.

Note: SET OF COMPONENTS are treated like COMPONENTS.

C. ILLUSTRATED USE-CASES (EXAMPLES)

Key for the Use-Case graphs:

- **Comp** → **Component**; The numbering reflects the Annex B use-cases: Component 1.1, 1.2, 2, 3
- **Sub-Sys** → **Subsystem**; The numbering reflects the Annex B use-cases: (Sub)System 1.1, 1.2, 2, 3
- **S/S** → **System or Group of Subsystems**; The numbering reflects the Annex B use-cases: (Sub)System 1.1, 1.2, 2, 3

- The first delivery of every Comp, Sub-Sys and S/S is “A”, the second is “B”, and so on. “n” stands for and undefined higher count.
- Each project ends with the setting in operation of the delivered “product” or system.

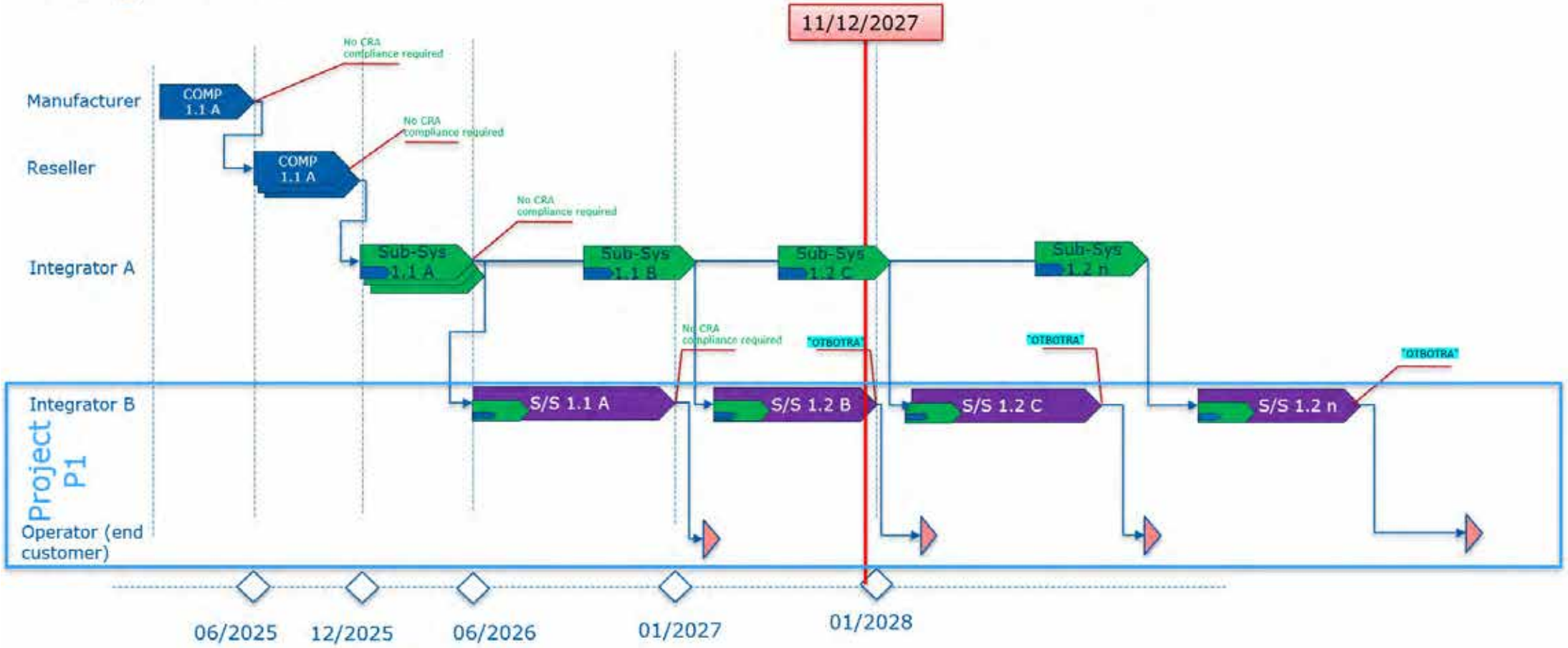
- Indicates a component, set of components or subsystem
- Tip of the triangle on the right indicates the date of placing on the market
- Length of the form does not represent any time period or effort

- Indicates that the subsystem is operated after setting into operation
- The time period is undefined

“**OTBOTRA**” = *On the basis of the cybersecurity risk assessment* at system level (with or without additional mitigating measures) as per CRA Annex I Part I, Point 2	When this legend is used, based on the risk assessment and with acceptable residual risk at system level, the component or the (sub)system could stay technically "as is" until the next substantial modification (next evolution / baseline). When the outcome of the risk assessment requires it, the supplier shall propose cybersecurity measures that can reduce the residual risk (where required) towards an acceptable level of cybersecurity in the sense of the CRA and, if contractually required, agreed with the asset owner. , These measures should ideally have minimal impact to the design. Obligations of project time plan and approval (e.g. TSI) shall be taken into consideration. Costs are to be negotiated. Typically achievable measures of this kind are for instance Security Monitoring or the use of already available protection functions (VLAN, encryption, hardening).
“CRABD” = *CRA compliance By Design* for component or (sub)system (designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance)	When this legend is used, the component or (sub)system shall be designed / adapted, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks to demonstrate CRA compliance; and fulfil all the applicable requirements according to the risk assessment of the PDE.

Project "P1"

Project for delivery with (sub)systems contract signed **before** 11.12.2024 **and** starting delivery **before** "CRA application date" = 11.12.2027 (e.g. rolling-stock series)

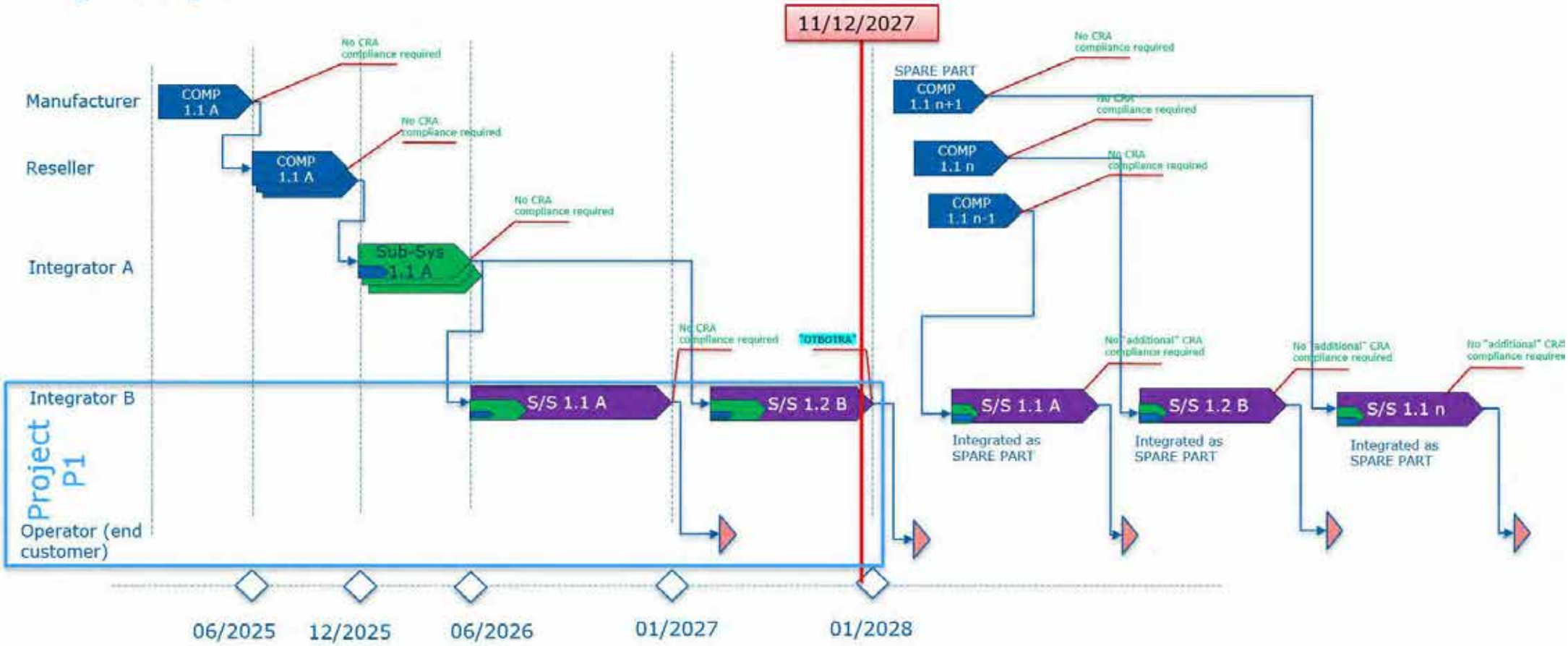


Compliance for **S/S 1.2 B/C/n that stay "as-is" onwards** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...) in the **existing project.**

Note: To improve readability, the integration of Comp 1.1 n and Sub-Sys 1.1 n into S/S B, C, .. is not shown but assumed. It is further assumed that these Comp and Sub-Sys are first placed on the market before 11.12.27.

Operation for 20, 30, 40 years after handover

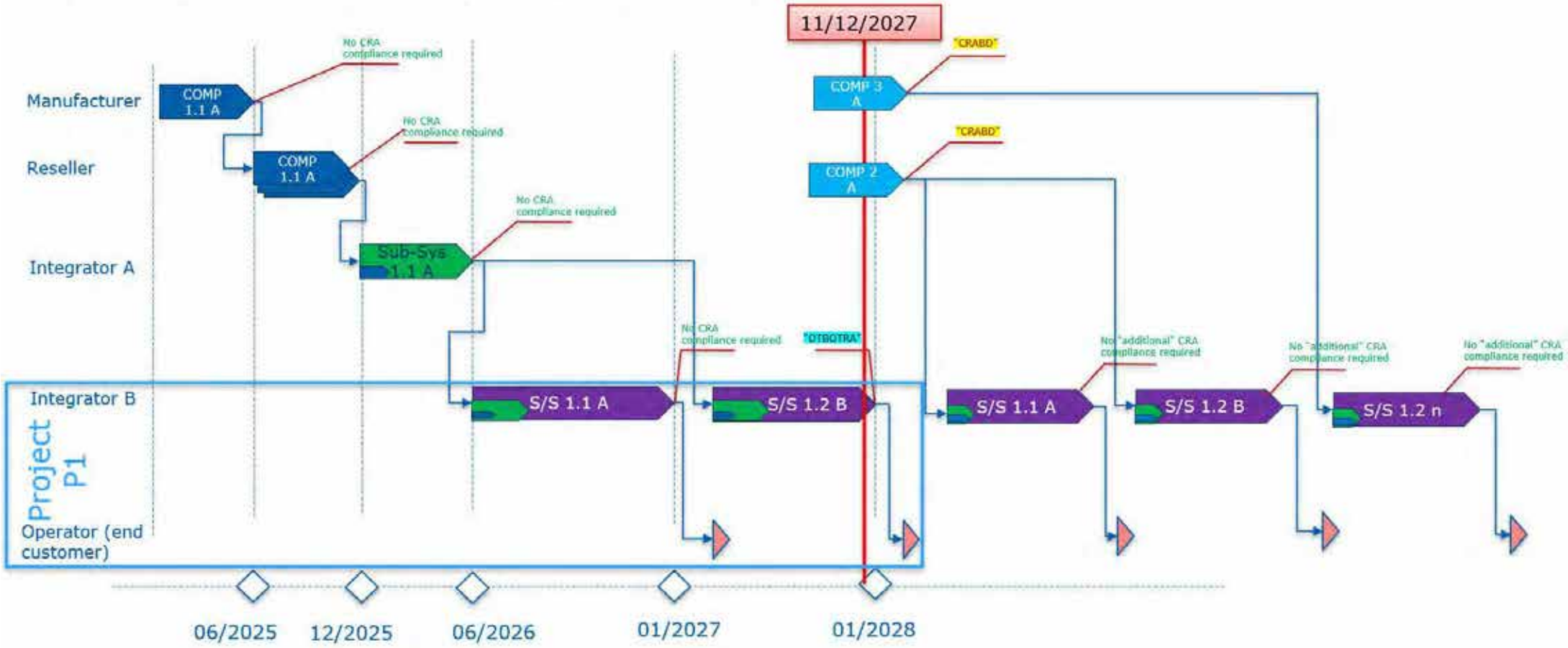
Spare parts



Compliance for **S/S 1.2 B that stay "as-is" onwards** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...)
Compliance not needed for spare-parts
SPARE PARTs can be integrated **without affecting** the compliance of the S/S 1.1 or 1.2.

Note: To improve readability, the integration of Comp 1.1 n and Sub-Sys 1.1 n into S/S B, C, .. is not shown but assumed. It is further assumed that these Comp and Sub-Sys are first placed on the market before 11.12.27.

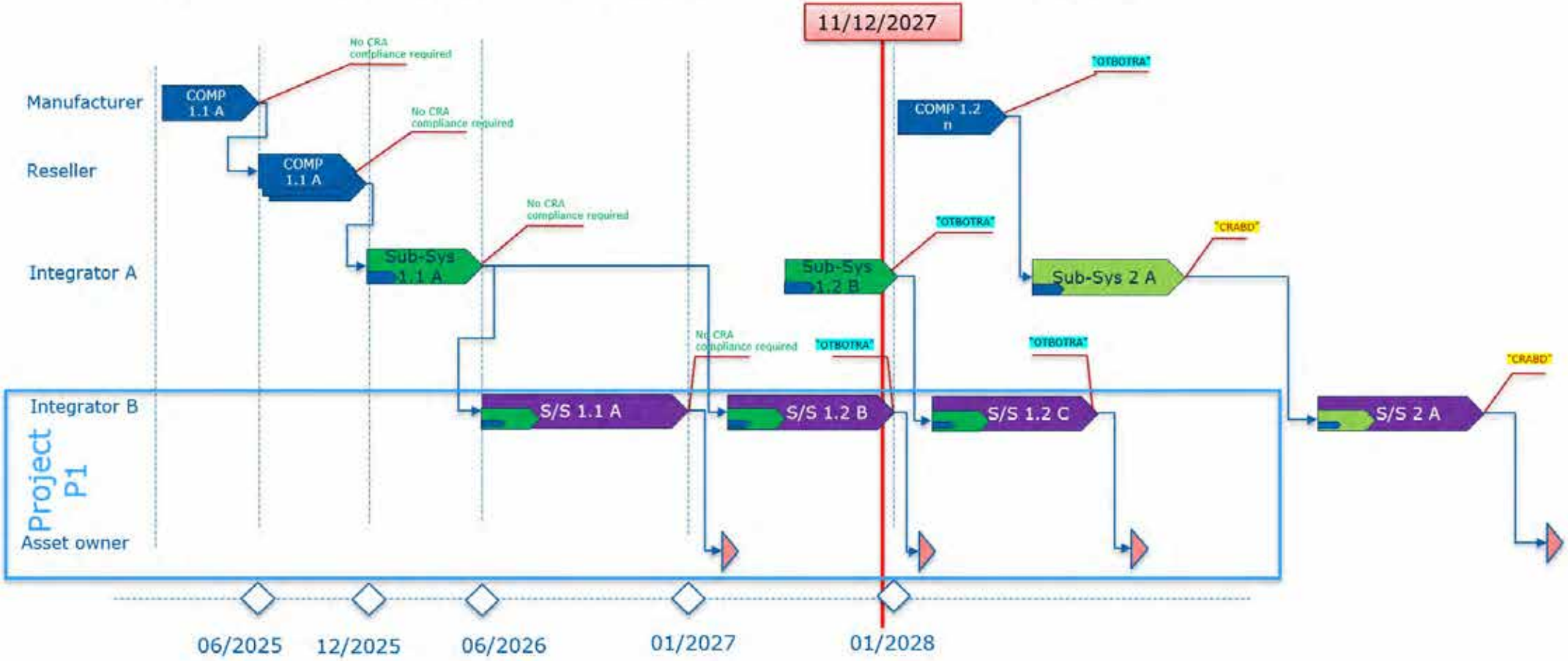
Component NEW (under SUBSYSTEM 3 case)



Compliance for **S/S 1.2 B that stay "as-is" onwards** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...)
NEWly developed **components (COMP 2A /3A)** needs to **comply with CRA by design**.
The **integration of NEW**ly developed PDE does **not affect** the **compliance** requirements of the rest of S/S 1.1 or 1.2., as long as the function within the S/S is the same (SUBSYSTEM 3 case)

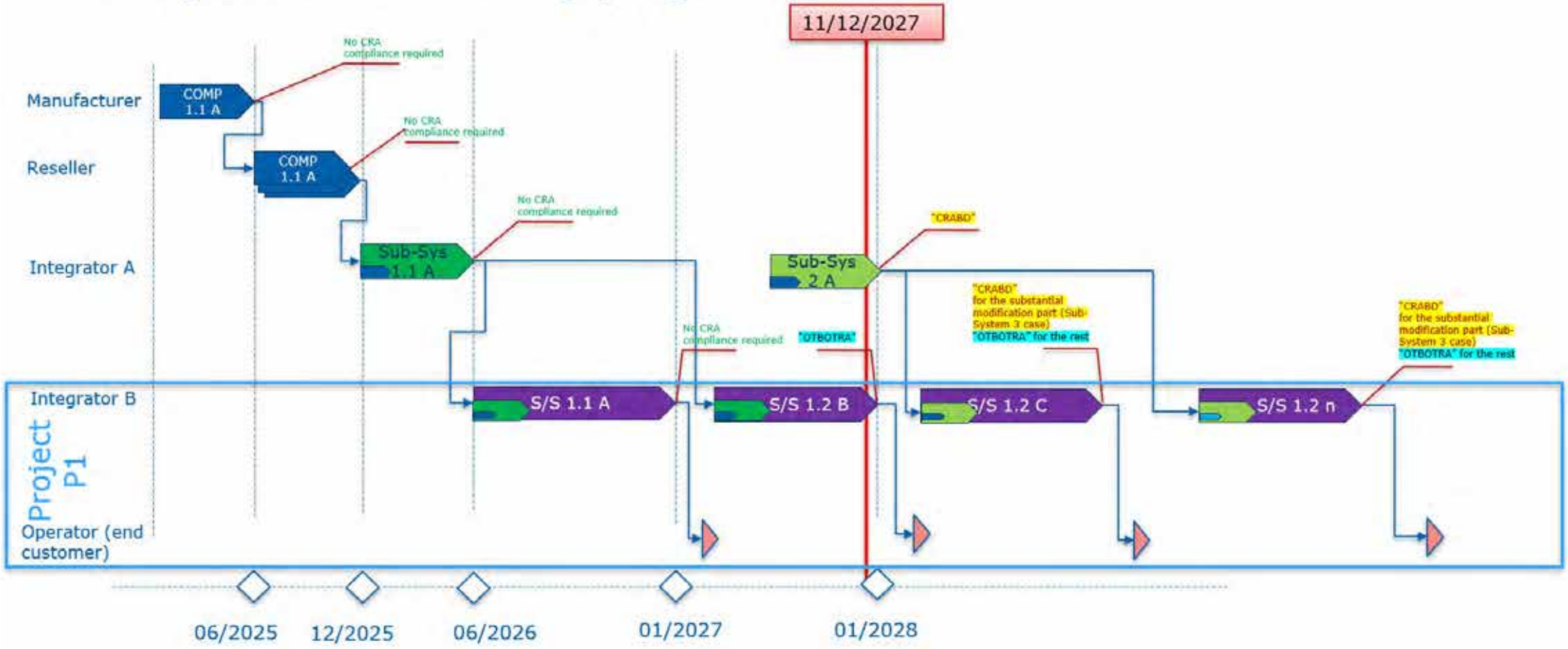
Note: To improve readability, the integration of Comp 1.1 n and Sub-Sys 1.1 n into S/S B, C, .. is not shown but assumed. It is further assumed that these Comp and Sub-Sys are first placed on the market before 11.12.27.

Sub-Sys NEW with existing COMP + NEW Project



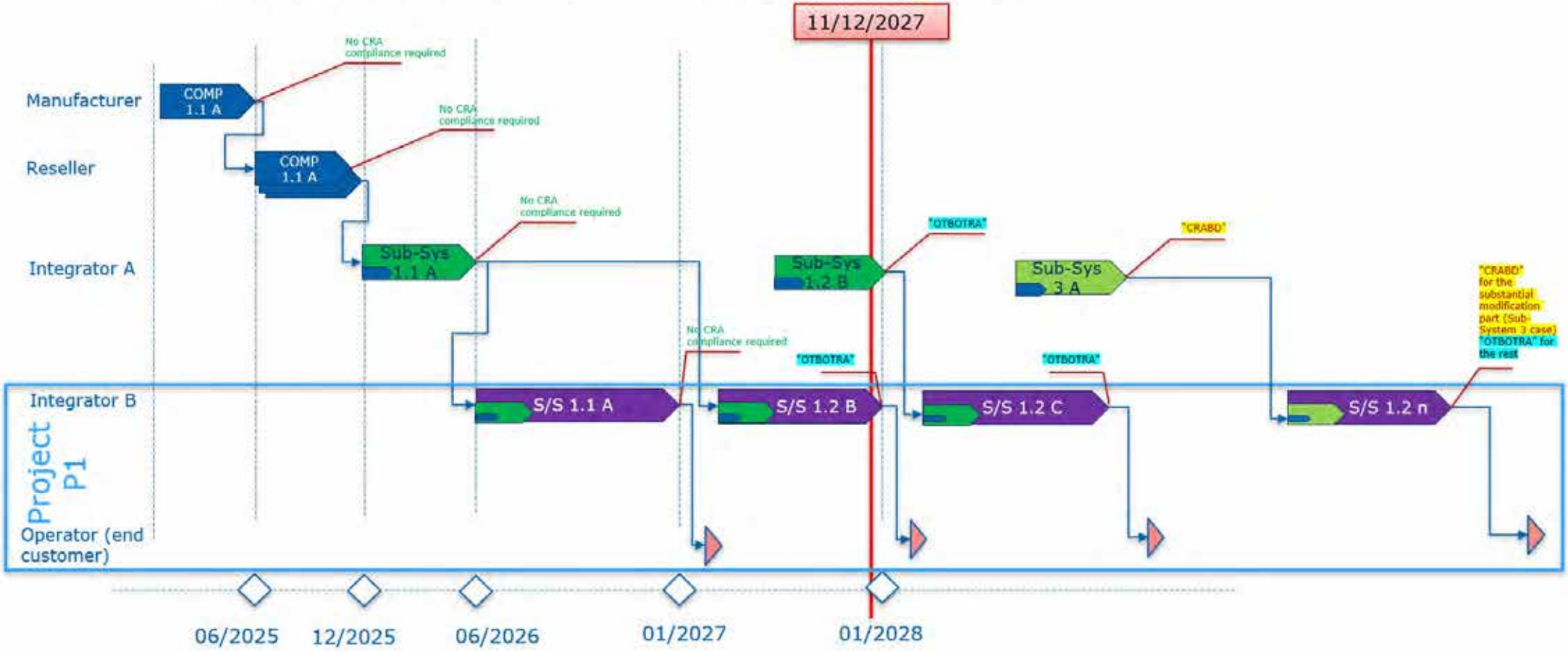
Compliance for **S/S 1.2 B/C that stay "as-is"** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...)
The **integration of "old" Sub-Sys 1.1A 1.2B** into an **existing project** delivery, does **not affect** the **compliance** requirements of the S/S, as long it is used for the defined project
NEWly developed **Sub-Sys 2A** needs to **comply with CRA by design** (even if it integrates "old" Comp 1.2).
The **integration of Sub-Sys 2 A** (which integrates "old" Comp 1.2) into a **new project**, **requires** the **compliance by design** of the Sub-Sys 2 A and the S/S 2A.

Sub-Sys NEW + Existing project



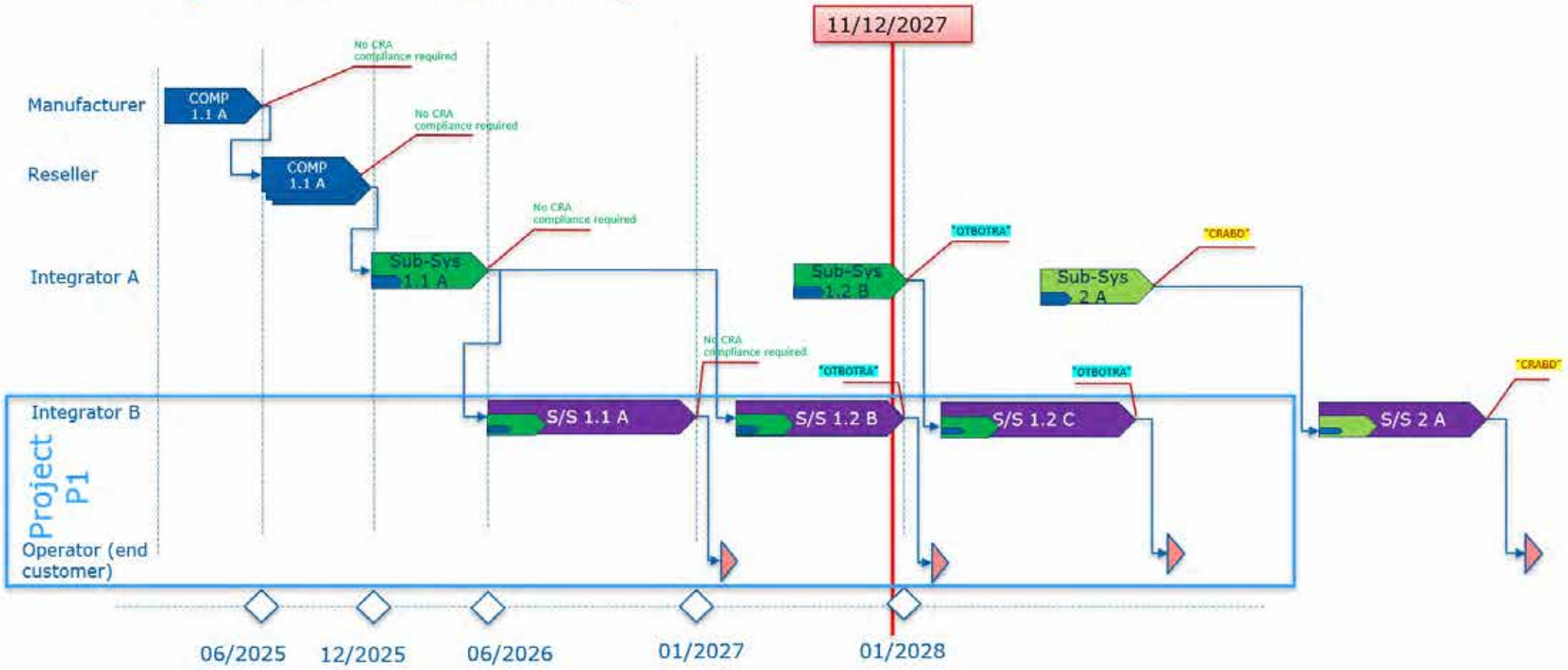
Compliance for **S/S 1.2 B/C/n that stay "as-is" onwards** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...)
NEWly developed **Sub-Sys 2A** needs to **comply with CRA by design**.
The **integration of NEW**ly developed **Sub-Sys 2A** into a project delivery, does **not affect** the **compliance** requirements of the rest of S/S in the project, as long as the function within the S/S is the same.

Substantial Modification + Existing Project



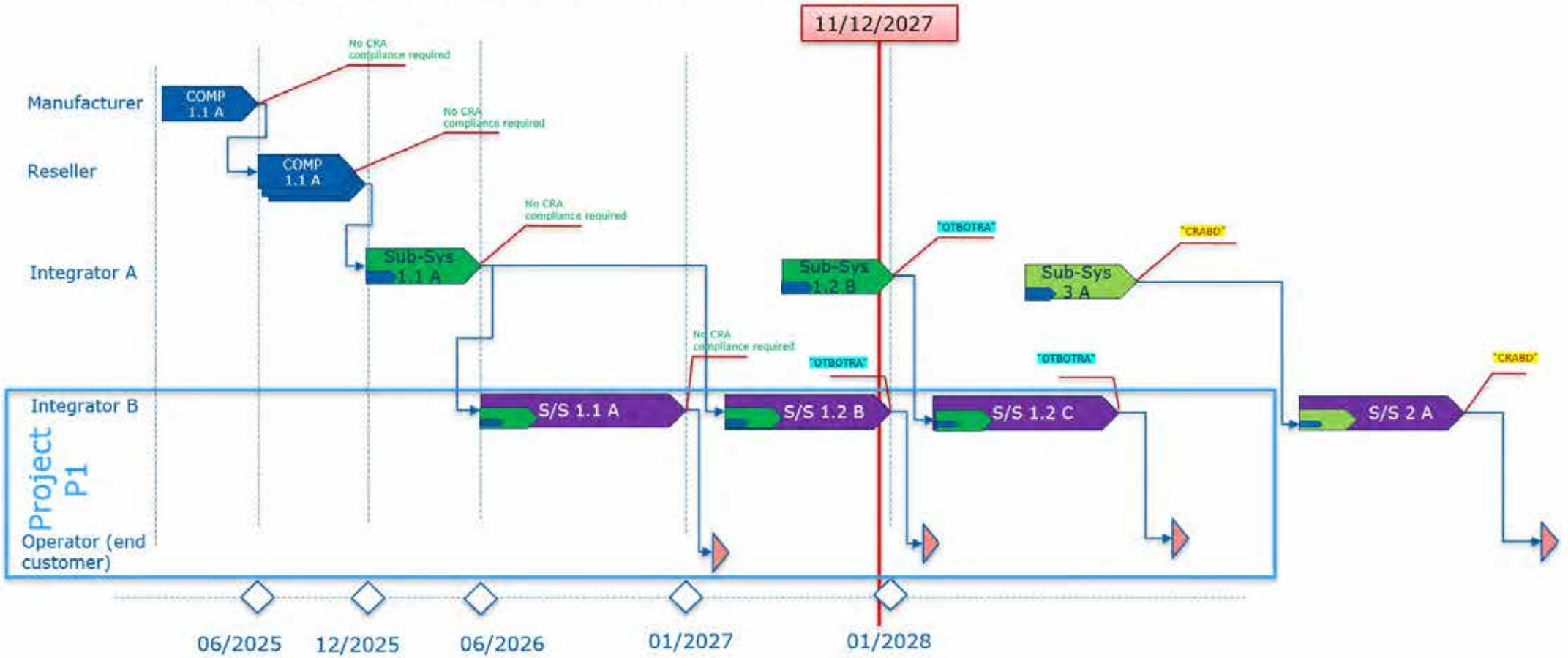
Compliance for **S/S 1.2 B/C/n that stay "as-is"** by providing the **mutual agreement** with the underlaying requirements (risk assessment, …)
The **integration of "old" Sub-Sys 1.1A 1.2B** into an **existing project** delivery, does **not affect** the **compliance** requirements of the S/S, as long it is used for the defined project.
NEWly developed **Sub-Sys 3A** (Sub-Sys 1.x with substantial modification) needs to **comply with CRA by design.**
The **integration of new Sub-Sys 3A** into an **existing project** delivery, does **not affect** the **compliance** requirements of the rest of the S/S, as long it is used for the defined project.

Sub-Sys NEW + NEW Project



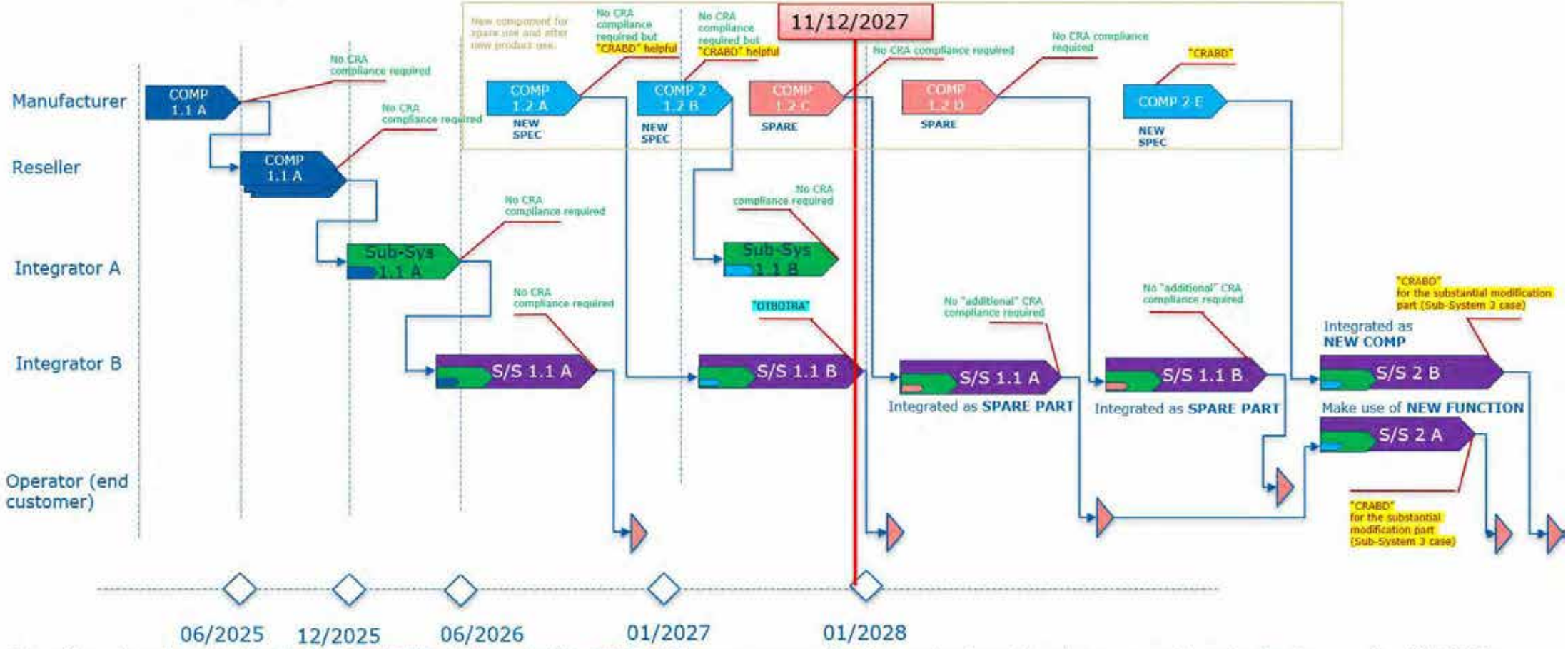
Compliance for **S/S 1.2 B/C that stay "as-is"** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...)
The **integration of "old" Sub-Sys 1.1A 1.2B** into an **existing project** delivery, does **not affect** the **compliance** requirements of the S/S, as long it is used for the defined project.
NEWly developed **Sub-Sys 2A**, needs to **comply with CRA by design**.
The **integration of new Sub-Sys 2A** into a **new project**, **requires** the **compliance by design** of the Sub-Sys 2A and the S/S 2A.

Substantial Modification + NEW Project



Compliance for **S/S 1.2 B/C that stay "as-is"** by providing the **mutual agreement** with the underlaying requirements (risk assessment, ...)
The **integration of "old" Sub-Sys 1.1A 1.2B** into an **existing project** delivery, does **not affect** the **compliance** requirements of the S/S, as long it is used for the defined project.
NEWly developed **Sub-Sys 3A** (Sub-Sys 1.x with substantial modification) needs to **comply with CRA by design**.
The **integration of new Sub-Sys 3A** into a **new project**, **requires** the **compliance by design** of the Sub-Sys 3A and the S/S 2A.

NEW component as spare part that becomes NEW component



Compliance is not required for COMP 1.2 A/B/C/D ; but required for COMP 2E (because new specifications and not considered as spare part); so to allow to **comply with CRA by design** for COMP 2E, it's highly recommended to **anticipate to comply with CRA by design** for COMP 1.2 A/B/C/D even if CRA compliance is not yet required for them.
NEWly developed **components**, according to different specifications or functionalities that the component shall be replaced with, need to **comply with CRA by design**.
The **integration of NEW**ly developed spare parts, does **not affect** the **compliance** requirements of the Sub-Sys, as long as the function within the Sub-Sys is the same (1.1A/1.1B)
The **integration of NEW**ly developed component / new function inside, **affect** the **compliance** requirements of the Sub-Sys (2A/2B) at least for the substantial modification part.

Note: To improve readability, the integration of Comp 1.1 n and Sub-Sys 1.1 n into SYS B, C, .. is not shown but assumed. It is further assumed that these Comp and Sub-Sys are first placed on the market before 11.12.27.

D. TABLE OF ACRONYMS AND REFERENCE DOCUMENTS

ADCO	Administrative Cooperation Group	**IAM**	Identity Access Management
ASIC	Application-Specific Integrated Circuits	**IDS**	Intrusion Detection System
AV	Anti-Virus	**IEC**	International Electrotechnical Commission
B2B	Business to Business	**IPS**	Intrusion Prevention System
CBTC	Communication-Based Train Control	**ISO**	International Organisation for Standardisation
CCA	Cyber Critical Assets	**JRU**	Juridical Recording Unit
CCTV	Closed Circuit Television	**NIS2**	Network and Information Systems Directive (2022)
COTS	Commercial Off-The-Shelf	**OMTS**	Onboard Multimedia & Telematics
CPU	Central Processing Unit	**PKI**	Public Key Infrastructure
CRA	Cyber Resilience Act (2024)	**PDE**	Product with Digital Elements
CSIRT	Computer Security Incident Response Team	**PLC**	Programmable Logic Controller
DMI	Driver Machine Interface	**RBC**	Radio Block Centre
EDR	Endpoint Detection & Response	**SBoM**	Software Bill of Materials
ENISA	European Union Agency for Cybersecurity	**SCADA**	Supervisory Control and Data Acquisition
ERJU	Europe's Rail Joint Undertaking	**SecRACs**	Security Related Application Conditions
ETCS	European Train Control System	**SRACs**	Safety Related Application Conditions
EVC	European Vital Computer	**SIEM**	Security Information & Event Management
FPGA	Field-Programmable Gate Arrays	**TCMS**	Train Control and Monitoring System
FRMCS	Future Railway Mobile Communication System	**TPM**	Trusted Platform Module
GSM	Global System for Mobile Communication	**TSI**	Technical Specification for Interoperability
HMI	Human Machine Interface	**VLAN**	Virtual Local Area Network
HSM	Hardware Security Module	**VPN**	Virtual Private Network
HVAC	Heating, ventilation, & air conditioning	**XDR**	Extended Detection & Response

'Blue Guide' on the implementation of EU product rules	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_247_R_0001
Cyber Resilience Act (2024/2847)	https://eur-lex.europa.eu/eli/reg/2024/2847/2024-11-20
IEC PT 63452 standard	https://www.iec.ch/dyn/www/f?p=103:14:405172316768605::::FSP_ORG_ID:28802
NIS2 Directive (2022/2555)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227
Technical Guideline TR-03183	https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html