21 April 2026

EIM statement on non-adoption of CRA Guideline for rail

The **Cyber Resilience Act** (CRA) is a horizontal EU regulation—adopted in October 2024—that defines obligations for a supplier in making available **products with digital elements** (PDEs) in the Single Market.[1] Each PDE placed on the market from **11 December 2027** must comply with the **essential cybersecurity requirements** of the CRA,[2] and the manufacturer must provide vulnerability support for the PDE throughout its expected lifetime.

EIM welcomes the CRA and the fundamental shift in the paradigm of digital security that it brings with it in the EU—the current level of cybersecurity of PDEs is low and needs to be increased to reduce cyber risks in the sector. The CRA covers the entire life cycle of the product—from planning, design, development or production, testing, maintenance, up to its decommissioning.

Despite being horizontal legislation that applies across many sectors, the CRA contains specific provisions recognising that certain PDEs must comply with sector-specific legislation (such as technical specifications for interoperability (TSIs)) and, as a result, may need to depart from some of the CRA's essential requirements. To that end, it establishes clear mechanisms that accommodate such situations.

Furthermore, as stated in preamble, the CRA aims to complement the legal framework established by **NIS2 Directive** by ensuring that hardware and software products used by infrastructure managers meet certain essential cybersecurity requirements.[3]

The value of a guide for rail

Rail, like many other non-consumer sectors, is characterised by B2B arrangements, long asset life, a concentrated supplier base and safety critical systems.

A guide to the CRA would be useful in that it:

- helps present and explain terms within the CRA,
- guides the reader to specific relevant articles in the CRA and,
- provides sector specific examples of the application of the CRA to the industry (including examples that reflect the need for a case-by-case assessment). The examples should assist the reader in its understanding of the CRA and its nuances.

Following discussions with CER, UITP and UNIFE in the context of EIM's participation in the **Cybersecurity Rail Sector Group** (CRSG) and its collaboration on the "**Expert guidance on the implementation of the Cyber Resilience Act mainline and urban railways**" ('Guide'), EIM believes that the Guide risks confusing the reader by deviating from the CRA and does not meet the stated goal of "offering clear explanations and sector-wide guidance for the implementation of Regulation (EU) 2024/2847". Therefore, EIM will not co-adopt the Guide.

Why EIM cannot co-adopt the Guide

As obligations stemming from the CRA as legislation cannot be altered by a document like the Guide, EIM believes that a guide on the CRA should not introduce concepts that do not follow from a reading of the CRA, nor qualify, limit or alter any of the provisions of the CRA. The guide should be easier for its audience to digest

[1] Article 1 and Article 71(2) of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA): ELI: http://data.europa.eu/eli/reg/2024/2847/oj.
[2] Annex 1 to the CRA.
[3] Recital 3 of the CRA.

than the original text of the CRA and it should not try to add additional layers to implementing the law. Unfortunately, EIM believes that the Guide fails in this respect for the following reasons, among others:

1) The Guide misrepresents certain concepts in the CRA and provides a definition or application method, which could lead to an incorrect application of the obligations in the CRA.

For example, "spare parts" are wholly exempt from the scope of the CRA. Meaning individual components can always be replaced by a spare part without requiring a risk-assessment or proving conformity with essential requirements. The CRA provides a narrow definition of spare parts which are components "that are manufactured according to the same specifications as the components that they are intended to replace"[4] to eliminate the possibility of cyber risks being introduced to a PDE without proper mitigating measures.

The Guide, however, adds that *"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*".[5] It does not discuss the need for risk analysis for this kind of "spare part", which would be necessary to determine that it "*does not bring additional threats or exposure to the legacy product they are integrated in*". EIM notes that spare parts feature prominently in vulnerability databases, hence the need to be cautious with how they are treated regarding cybersecurity.

For all the above reasons, EIM cannot accept the risk of including this new concept of spare parts proposed in the Guide.

2) The Guide introduces additional concepts and analytical layers derived from railway terminology, thereby blurring the distinction between what is legally required for the correct application of the CRA and what constitutes a further interpretation proposed by the CRSG.

The Guide frequently applies the CRA by reference to an engineering abstraction and additional concepts that are not grounded in, and are largely irrelevant to, the legal framework and criteria established by the CRA. Furthermore, the way in which these terms are introduced may confuse readers. The Guide refers to its own definition of a concept (whether from the CRA or not) rather than directly to the CRA.

- For the description of obligations regarding PDEs, the Guide tries to add a technical layer of abstraction to the provisions of the CRA. The obligations of manufacturers in relation to PDEs are defined in the Guide in relation to "component" and "functional subsystem and system" and explained differently depending on whether a PDE is a component or functional subsystem.[6] The term component has a different meaning in the CRA and throughout the guidance it is not clear which meaning of component is intended.
- The obligation of the manufacturer to conduct a cybersecurity risk assessment is sometimes explained in the guide as occurring at the "system" level rather than the most appropriate level.[7] Annex A of the Guide, which provides the "use case approaches" that are referred to throughout the document, makes no reference whatsoever to "PDE" and instead relies entirely on "component", "(sub)system" and "project" making it utmost unclear how this helps the reader in faithfully applying the CRA. Whether an assessment on "system" level is justified, depends on what is delivered: when a "component" or "subsystem" is delivered as a PDE, a "system" level risk assessment is not the appropriate level of assessment.

To determine whether a product is a PDE and whether the CRA applies to it, it is necessary to adhere to the definition and scope contained in the CRA and its position within the supply chain. Interpretations based on the concepts mentioned above and not covered in the CRA create confusion.

3) The Guide could be interpreted as presuming that manufacturers will not be able to provide CRA compliant PDEs after December 2027.

[4] Article 2(6) of the CRA.
[5] Section 2.3.1 of the Guide.
[6] Section 2.1.1 of the Guide.
[7] The Commission's draft guidance on the CRA specifies that the cybersecurity when conducting the risk assessment in Art. 13(2) of the CRA "the risks to the product as a whole, elements outside of the product, such as environmental elements, external infrastructure, other systems or networks, must be considered."

Several instances of the Guide already provide for the eventuality in which a manufacturer does not deliver a PDE which fulfils all the essential requirements in Annex I to the CRA, simply because the contract was signed before December 2024.[8]

It is clear to EIM that outdated design specifications for PDEs do not justify non-compliance with the essential requirements of the CRA.[9] PDEs that do not meet the essential cybersecurity requirements in the CRA will not obtain the CE marking and, consequently, cannot be made available on the Market after 11 December 2027.

4) The Guide could be interpreted as shifting the burden of complying with the CRA from the manufacturer to the user.

Paragraph 2.7 of the Guide appears to describe how to allocate responsibilities between suppliers, railway undertakings and infrastructure managers in a railway project context. According to the CRA, the obligation to comply with the CRA rests (in principle) on the manufacturer of the PDE, not on the user.[10]

For example, the Guide provides that manufacturers may supply PDEs (after December 2027) that do not fulfil all essential cybersecurity requirements for "projects" that are signed before December 2024. In order to do so, the Guide suggests that the manufacturer and user mutually agree on the "residual risk" and the mitigating measures (i.e., "imposing requirements on the integration and the operating environment").[11]

EIM reiterates that responsibility for placing a compliant product on the market after December 2027 rests with the manufacturer. Compliance with the CRA may necessitate changes to the PDE's design, functionality, or intended purpose.[12] Information and instructions may support secure use and inform users of residual risks, but cannot compensate for shortcomings in product design and increased costs does not justify leaving relevant risks unaddressed.

Therefore, the CRA does not allow the manufacturer and the customer to mutually agree that certain products supplied need not comply with all essential cybersecurity requirements. The non-application of certain essential cybersecurity requirements can only be justified, say, by their incompatibility with mandatory interoperability requirements and must be justified in the technical documentation of that product.[13]

Conclusion

While EIM fully supports the usefulness of guidance on the CRA, and appreciates the work done so far, **EIM fundamentally disagrees on key topics presented in the guidance provided by the authors of the Guide.**

EIM does not believe that the Guide makes it clear that any PDE placed on the Single Market after 11 December 2027 needs to be CRA compliant subject only to the legitimate exemptions provided in the CRA itself. In this regard, EIM cannot endorse a Guide that establishes exemptions and limitations on manufacturers' obligations that are not in the text of the CRA. If there are indeed concerns of not being able to achieve CRA compliance for PDEs (at any point on the supply chain) then this issue should be explicitly stated and addressed in an appropriate forum and such issues officially addressed by the European Commission.[14]

A limitation of the cybersecurity obligations of manufacturers, distributors, and importers to comply with the essential requirements set out in Annex I of CRA, would increase the responsibility of infrastructure managers who, under Article 21 of the Directive NIS 2, must ensure, among others, the supply chain security and the security in network and information systems acquisition, development and maintenance.

Even though EIM has chosen not to endorse the Guide that has been developed in the context of the CRSG, **EIM remains committed to working on other projects with the CRSG** including further work in the context of the CRA**.**

[8] Section 2.7 of the Guide.
[9] § 146 of the Commission's draft guidance on the CRA.
[10] See also § 145 of the Commission's draft guidance on the CRA.
[11] Section 2.7.2 of the Guide.
[12] § 147 of the Commission's draft guidance on the CRA.
[13] Article 13(4) of the CRA.
[14] For example, by using its delegated empowerments in Article 2(5) and Article 61.