OCORA

Open CCS On-board Reference Architecture

Acceptance of Global Standards
Beta Release

Document ID: OCORA-30-008-Beta

Version: 9.00

Date: 26.06.2020

Status: final

Revision history

Version	Change Description	Name (Initials)	Date of change
1.00			2020-05-16
2.00	§5 and Annexes		2020-05-19
3.00	Comments from SBB and SNCF		2020-06-03
4.00			2020-06-04
5.00	Comments from NS et SBB + meeting comments	JW+CG+OC+AA+HAK	2020-06-16
6.00	Improvement of the §1.1 Introduction, §2 General overview and §6 Conclusion+ clarification of definition of global standard + §3 definitions of Referenced standards	HAK+AA+LS	2020-06-18
7.00	Modification of the §5.3.1 to clarify the relation between SIL levels of EN5012x and IEC61508	HAK +AA + OC +NA	2020-06-18
8.00	Modification of the §5.3.1	JW+CG+OC+AA+HAK+MM	2020-06-24
9.00	Final Version for Beta Release	RM	2020-06-26

Table of contents

Table of figures

References

The following references are used in this document:

[1] OCORA-10-001-Beta – Release Notes

[2] CLC/TR 50506-2: 2009 Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129 - Part 2: Safety assurance

1 Introduction

1.1 Document context and purpose

This document is published as part of the OCORA Beta release, together with the documents listed in the release notes [1]. It is the first release of this document and it is still in a preliminary state.

This document aims to explore means to boost innovation and to improve the technical and operational performance in the CCS railway industry, by the means of standardization.

1.2 Why should I read this document?

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA technical concepts for on-board CCS. The reader will gain insights regarding the topics listed in chapter 1.1, will be able to provide feedback to the authors and can, therefore, engage in shaping OCORA.

2 General overview

The primary objective of standardisation is the definition of voluntary technical specifications with which current or future products, production processes or services may comply.

Standardisation plays an increasingly important role in international trade and the opening-up of markets.

Standardisation helps to boost the competitiveness of enterprises by facilitating in particular the free movement of goods and services, network interoperability, means of communication, technological development and innovation.

EU railway standards shall not be a hindrance to the railway sector take-off, they should help to boost the EU railway market technically and economically.

Yet, there are few particular areas in current rail standardisation framework that require improvement.

1. There have been too many standards elaborated for the rail sector that are sector-specific. This is an impediment to economies of scale and innovation take-off, which could be avoided if well-proven standards from other sectors such as aeronautics and space were used when applicable.
2. The financial impact a standard may have and even the business rationales for a standard are often underestimated. The business-added value of a standard must be assessed before elaborating a new standard.

This document focuses on the standardisation improvements that could be undertaken in the frame of Control Command and Signalling in the European Union in order to:

- Facilitate for the railway industry the use of off-the-shelf components compliant with well-proven and largely-applied standards
- Reduce the time necessary to introduce new technologies in the railway industry
- Allow for safety-related electronic systems the use of well-proven and largely-applied standards

As a first example, this document in its beta version tries to highlight the possible bridges in safety standards. This represents a first attempt toward our goals.

3 Definitions

A ‘standard’ means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, except when referenced in a Technical Specification for Interoperability, or any other regulatory text (e.g. national rule, law, …).

A ‘European standard’ means a standard adopted by a European standardisation organisation (CEN, CENELEC or ETSI).

A ‘harmonised standard’ means a European standard published on the basis of a request made by the Commission supporting the application of Union harmonisation legislation Its application can be mandatory (referenced standard) or voluntary (standard listed in the Official Journal of the EU in the New Legislative Framework).

A ‘Referenced standard’ means a standard or a part of a standard referenced in a Technical Specification for Interoperability (TSI). Furthermore, article 4.8 of Directive (EU) 2016/797 sets out that normative documents, such as specifications or technical documents can also be referenced in a Technical Specification for Interoperability (TSI). When referenced, their nature changes from voluntary to mandatory. .

An ‘International standard’ means a standard adopted by an international standardisation body (ISO, IEC or ITU).

‘Presumption of conformity’ The presumption of conformity is a concept that is widely used in the context of the European “New Approach” for better regulation. The presumption of conformity means that a manufacturer who has complied with a harmonised standard listed in the OJEU can legally assume he has met the requirements of the directive (or TSI) covered by that standard, as described in its Annex Z.

ANNEX Z of standards and the Official Journal of the European Union

The listing of a European standard in the OJEU requires a positive assessment of the Harmonized Standard Consultant and a corresponding positive statement of the EC desk officer. Furthermore, it is required that the listed standard contains an Annex Z detailing to which requirements of the directive (or TSI) it provides presumption of conformity.

4 Problem description for the CCS TSI

4.1 General review on referenced standards

There are several alternatives for the referenced standards in the CCS TSI that provide the same level of quality and safety, are globally accepted, are regularly applied in safety critical branches of industry including the transportation industry and are tolerant to the application of state of art technologies. Therefore, there is ample technical and economic justification to ease the use of components compliant with globally accepted industry standards that ensure at least an equivalent RAMS level.

Since alternative standards that are widely used in substantially bigger markets (e.g. petrochemical industry, aviation and automotive) are also rigorous with the fit for use testing, they could provide a viable alternative to specific railway standards. Components especially designed for safety applications are generally certified against standards providing access to bigger markets and not against railway standards. This is for instance the case in markets for (safe) microprocessors and complete programmable logic controller where the railway sector is just a niche in a huge global market for industry and automotive.

It would be possible to address the problem in two ways:

- Open the option to apply well-proven and largely-applied standards as an alternative to railway-specific mandatory standards: it will speed up the introduction of new technology in the railway industry.
- Facilitate the recertification against railway standards of off-the-shelf components already compliant with well-proven and largely-applied standards: it will enable the swift introduction and use in the railway domain of off the shelve products to the benefit of the European railway community.

Due to time constraint we will focus on the second option which will provide inputs to use for the first option.

4.2 New challenge: Introduction of innovation in ERTMS

Automation, digitalization and virtualization of functions require to anticipate the certification and safety demonstration of individual component and of the whole CCS system composed of those individual components.

When applied to future innovations that are envisaged for the on-board CCS system, the main concerns are:

- For certification: How to certify non-railway components for the railway Control Command and Signalling domain.
    - e.g. a Computing Platform or a fail-safe GNSS-based localisation, which are already used in safety applications outside the railway sector
- For lifecycle management: It shall be possible to add, in the global CCS architecture, off-the-shelf hardware component compliant with either railway standards or other standards

Facilitating the use of non-railway specific component helps to ensure consistency, thus enhancing the ability to manage system over the life cycle, improving user satisfaction, protecting IT investments, maximizing return on investment and reducing life cycle costs. The installed base for CCS products will be enlarged because non-institutional suppliers can enter the market which enables the swift exchange of suppliers, necessary in case of e.g. bankruptcy or change of business policy. Supply chain integration will be facilitated.

5 Proposals for further study on cross-acceptance between IEC61508 and EN5012X

5.1 Status of safety standards in current TSI CCS

The application of EN standards EN50126-129 is mandatory according to the current TSI CCS and the alternative use of similar well-proven and largely-applied standards or open standards is not allowed without a specific recertification as shown in the table below.

As argued above, this imposes a prolonged and expensive certification procedure to be followed by railways and industry for the integration of off-the-shelf products that are already fully compliant with and certified using (safety) standards leading to at least an equivalent level of safety.

Table A 3

List of mandatory standards

The application of the version of the standards listed in the table below, and their subsequent amendments when published as harmonised standard in the certification process is an appropriate means to fully comply to the risk management process as set out in Annex I of the Commission Implementing Regulation (EU) No 402/2013, without prejudice for the provisions of chapter 4 and chapter 6 of this TSI.

No	Reference	Document name and comments	Version	Note
A1	EN 50126-1	Railway applications —The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process	2017	
			1999	1,2
A2	EN 50128	Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems	2011	
A3	EN 50129	Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling	2003	1
A4	EN 50159	Railway applications — Communication, signalling and processing systems	2010	1
A5	EN 50126-2	Railway Applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety	2017	3

Note 1: this standard is harmonised, see 'Commission Communication in the framework of the implementation of the Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community (recast)' (OJ C 435, 15.12.2017), where also published editorial corrigenda are indicated.

Note 2: this version of the standard may be used during the transitional period defined in the updated version of the standard.

Note 3: To be used in combination with EN 50126-1 (2017).

Figure 1: List of mandatory standards (from CCS TSI)

5.2 Comparison

The core activities of equivalence demonstration (total or partial), if anticipated and agreed at sectoral level, can reduce the time-to-certification and consequently the time-to-market and delays in the authorization process.

To enhance the adaptation of innovative solutions from other sectors in the Railway market, a comparison is made at various aspects between the railway safety standards (EN5012x) and the generic industrial safety standard suite (IEC61508).

The EN5012x and IEC61508 standards are grossly comparable, except for the determination of an acceptable architecture and the way independence between electronic circuits shall be proven. Therefore, cross-acceptance of electronic components certified against IEC61508 could be possible if those two aspects are solved.

5.3 Architecture – coherence in the safety demonstration

The safety demonstration made with EN5012x, at system level benefits from a global consensus from railway RAMS experts.

However, many individual components are rather certified according to the IEC 61508 whose scope is general to all kinds of industry.

5.3.1 No single failures?

The main objection from railway experts against the IEC61508 standard, compared to EN5012X, is the acceptance of systems with “hardware fault tolerance” (HFT).

- For railway experts it is unacceptable that, a single fault lead directly to an unsafe state which could lead to a catastrophic accident (for random failures). Systematic failures are dealt through the SIL.
- Theoretically systems could be accepted according to IEC61508 for SIL3/4 even if a single fault might lead to an unsafe state, provided that, the risk is sufficiently low.

Therefore, for each component which certification against IEC61508 is to be cross accepted into an EN50126-129 product, it shall additionally be proven that no single fault can lead to an unsafe state which could lead to a catastrophic accident (for random failures).

The main point to be clarified to deal with this “single fault” issue is the notion of “credible” failure:

- It has to be done qualitatively, identifying the possible failure for a component and whether any of these failures can lead to an unsafe state which could lead to a catastrophic accident[1]
- It may also be done quantitatively by calculating the probability (or rate) of an unsafe state to occur. In that case, the impact of exported constraint has to be carefully assessed by the end-user (impact on the operation, maintenance … i.e. periodic reset of an equipment). In case the probability of reaching an unsafe state due to the failure is orders of magnitude below the quantitative safety requirement, then it can be classified as “incredible”.

[1] see paragraph 4.1.1 [2]

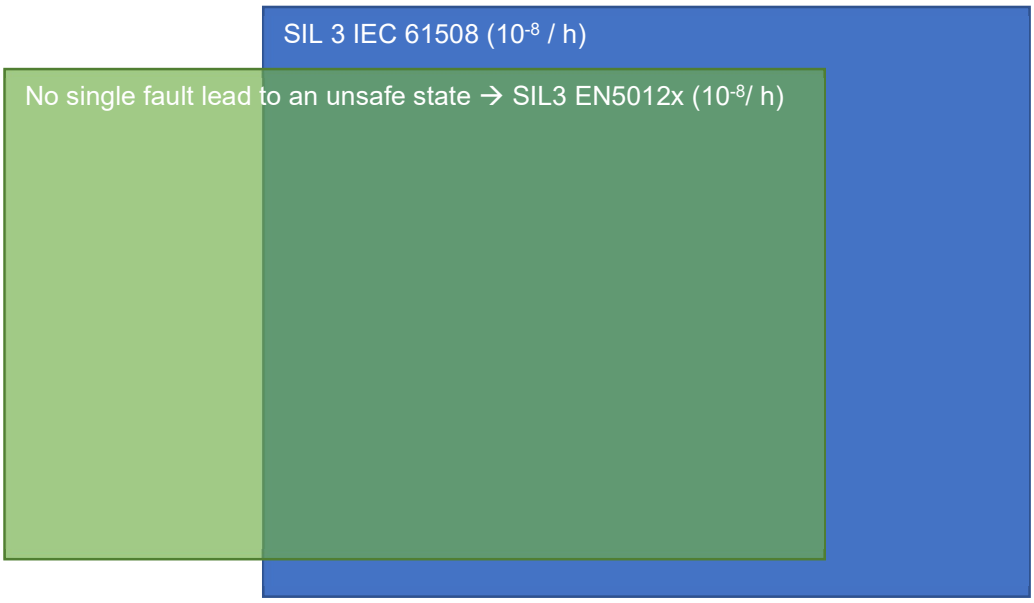

Figure 2: Nesting of SIL Level

In CCS systems, EN5012x ensures that for the component under study, **no failure** can lead to a catastrophic accident (all failure modes are fail-safe, or lead to non-catastrophic consequences).

➔ This is the « no single failure » requirement

When using IEC 61508, the “no single failure” may also be met by using redundancy of components.

Arithmetical view:

SIL 3 IEC 61508 (10^{-8} / h) & No single fault → SIL3 EN5012x

Further relations are to be investigated during the project

OCORA collaboration is proposing to further study this item with European organizations (CER, EIM, CENELEC, JPCR, NBRAIL, ERA…) to identify the appropriate demonstration necessary to ensure cross acceptance between IEC 61508 and EN 5012X.

5.3.2 SIL3 and SIL4 cross acceptance

Another difference concerning the architecture is the difference in qualitative requirements concerning SIL3 and SIL4 systems made in the IEC61508. In the EN5012x the qualitative requirements concerning SIL3 and SIL4 systems are equal, where the IEC61508 has different requirements. Therefore it shall be determined at which level components certified as SIL3 according to IEC61508 can be cross accepted for use in systems to be certified against EN5012x.

The additional qualitative requirements concerning SIL4 in IEC61508 are not relevant in EN5012x as those concern additional redundancy, and conditions for using redundancy to achieve a higher SIL which are not applicable in EN5012x. However, for EN5012x it shall be proven that no single fault can lead to an unsafe state.

Therefore, if a system is certified as SIL3 according to IEC 61508 and provided that no single fault can lead to an unsafe state, then it may be considered as cross accepted as SIL3 according to EN5012X.

Furthermore, if this system meets the quantitative safety requirements of EN5012x SIL4, then it should be considered as cross accepted as SIL4 according to EN5012X.

5.3.3 Independence

IEC61508 provides more concrete starting points for showing independence of electronic circuits compared to the EN50126-129 (especially EN50129).

The EN50129 provides examples (not requirements) to enhance independence which are primarily focussed on insulation between independent components. Insulation is an effective measure to achieve independence in case of digital (e.g. relay) circuits, however much less effective for electronic circuits.

Designs which are certified against the IEC61508-2, comply with the independence requirements as stated in that standard. It is difficult to prove that this implies that the design also complies with independence requirements as stated in EN50129, as those requirements are not as concrete as formulated in IEC61508-2. For this purpose, a comparison between the requirements concerning independence of electronic circuits stated in EN50129 and IEC61508-2 shall be made.

Especially concerning on-chip redundancy the EN5012x doesn't give a starting point for proving independence while IEC61508 provides a detailed list of requirements concerning design aspects of IC's with IEC61508-2 annex E.

6 Conclusions

This document is a first attempt towards boosting the EU railway market technically and economically. It presents the examples of possible cross-acceptance between standards or at least the highlighting of similarities and differences between a widely-used standard (IEC 61508) and railway specific standards (EN 5012X).

Innovation take-off in railway industry could be enhanced by multiple ways:

- By opening the opportunity to find "bridges" between well-recognized standards to enlarge the markets.
- By simplifying the recertification of equipment already certified with well-proven standards from other sectors such as aeronautics and space when applicable.
- By better highlighting and isolating in EU railway standards the railway-specific parts from the non-railway specific parts, so that they can be easily applied for certification.

Recognizing:

- the limited size of the overall EU railway market in terms of number of units,
- the fierce competition between railway, automotive and aviation sectors,

it is of paramount importance that the European railway sector carefully address its standardisation strategy to foster innovation and boost its market share. In order to do so our objectives are defined as:

- Facilitate for the railway industry the use of off-the-shelf components compliant with well-proven and largely-applied standards
- Reduce the time necessary to introduce new technologies in the railway industry
- Allow for safety-related electronic systems the use of well-proven and largely-applied standards
- And ensure still reaching the safety level required by CSM

OCORA collaboration is therefore proposing to further study this item with European organizations (CER, EIM, CENELEC, JPCR, NBRAIL, ERA…).

7 Annexes

7.1 The high-level objectives of the acceptance of global standards

- Title: Facilitate the use in the railway industry of off the shelf components compliant with well-proven and largely-applied standards
  Description: ensure the easy introduction in Railway Control Command and Signalling Systems of up to date technologies already validated in other safety related industries.
- Title: Reduce the time necessary to introduce new technologies in the railway industry Description : allowing an express process for the certification of new technologies already used in other industries ,
- Title: Allow for safety-related electronic systems the use of well-proven and largely-applied standards
  Description : For selected uses allow equipment compliant with the EN IEC 61508 in railway safety systems, or at least reduce the further demonstration necessary

These high-level objectives are also in the set of requirements section 6.1

7.2 Definition of independence

7.2.1 IEC 61508

In IEC 61508-2: 7.4.3.4 sufficient independence, in the design between elements and in the application of elements, shall be justified by common cause failure analysis to show that the likelihood of interference between elements and between the elements and the environment is sufficiently low in comparison with the safety integrity level of the safety function under consideration.

In IEC61508-6 annex D a guideline for the common cause failure analysis is given

In IEC61508-2 annex E specific requirements are formulated concerning independence in the case of on-chip redundancy.

7.2.2 EN 50129 & 50126

In the 50129: A description on how the standard defines the independence is in the annex B § 3.2.1

In the EN 50126-2: A description on how the standard defines the independence is in chapter 10.2