OCORA

Open CCS On-board Reference Architecture

Acceptance of Global Standards

Focus on Safety in CCS

Document ID: OCORA-BWS09-020

Version: 1.00

Release: Delta

Date: 30.06.2021

Revision history

Version	Change Description	Initial	Date of change
0.00	▪		DD-MM-YYYY
0.1	▪ Creation + added SIL allocation	HAK	2021-04-26
0.2	▪ Part on functional safety agreed on 27/04/2021	HAK	2021-04-27
0.21	▪ Internal SNCF review – SIN allocation/safety faction, intrinsic safety + introduction of constitutive component	HAK	2021-05-07
0.22	▪ Internal SNCF review – main issues to be addressed, competency, and cultural differences done	HAK	2021-05-12
0.23	▪ Internal SNCF review – first global review	HAK	2021-05-18
0.24	▪ Internal SNCF review – introduction of Non-Railway component	HAK	2021-05-21
0.25	▪ Resolution of Comment – introduction – with OCORA	HAK	2021-05-25
0.26	▪ Modification after resolution and agreement from NS	HAK	2021-05-28
0.27	▪ Integration of comments from DB CH, SBB CG, SNCF OC		2021-06-04
0.28	▪ Final Draft from BWS09	HAK	2021-06-08
1.00	Official version for OCORA Delta Release	RM	2021-06-30
	▪		
	▪		

Table of contents

List of figures

List of tables

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references.

The following references are used in this document:

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-010 – Problem Statements

[7] EN 50126-1:2017 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process

[8] EN 50126-2:2017 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Systems Approach to Safety

[9] EN 50128:2011 – Railway Applications – Communication, signalling and processing systems – Software for railway control and protection systems

[10] EN 50129:2018 – Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

[11] IEC EN 61508:2010 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Parts 1 to 7

[12] CENELEC TR 50506-1 Application Guide for EN 50129 – Part 1: Cross-acceptance, approved by CENELEC on 2007-01-16.

NOTE 1: IEC 61508-x and IEC 61511-x are parallelly voted and published as IEC and EN version. For reasons of simplification this document refers always to IEC EN versions.

Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). We always reference to the latest available official version of the SUBSET, unless indicated differently.

Management Summary

The workstream on Acceptance of Global Standard aims to explore the strategy to be considered for improving competition and increasing economy of scale through the mean of re-using off-the-shelves components (COTS) designed for other sectors of activities and which have been produced using alternative largely applied and well-recognized standards from another sector of activities (Global Standards as defined here). Different approaches are possible with respect to the fact that an EU railway legislation is already referencing or not a standard.

The core activities of cross-acceptance, if anticipated and agreed at sectoral level, can reduce the time-to-certification and consequently the time-to-market and thus delays in the authorization process.

The application of European RAMS standards CENELEC EN 50126-x, CENELEC EN 50128 and CENELEC EN 50129 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.

The safety demonstration made with EN 5012x, at system level benefits from a global consensus from railway RAMS experts. However, outside railway domain, many individual Non-Railway Components are rather certified according to the IEC EN 61508-x whose scope is general to all kinds of industry.

The railway specific RAMS-related standards CENELEC EN 50126, EN 50129, EN 50155 and EN 50128 / EN 50657 have many common parts with the set of IEC EN 61508 standards for functional safety software and E/E/PE, while the IEC EN 61508-x addressed a larger market.

We have identified nine major areas of differences between IEC EN 61508-x and CENELEC EN 5012x that have to be carefully addressed for cross-acceptance purposes:

1. Single failure for SIL3 and SIL4:

   No single random failure should lead to an unsafe state which could lead to a catastrophic accident. It has to be assessed qualitatively and may also need to be done quantitatively.

2. Intrinsic safety:

   CENELEC EN 50129 needs to be applied when intrinsic safety is required, as no requirements are specified in IEC EN 61508-x.

3. SIL allocation including “safe failure fraction”:

   In IEC EN 61508, SIL allocation can be made according to two different tables: ‘on-demand use’ or ‘continuous-use’.

   In CENELEC only continuous-use table exists. To allow SIL allocation, a conversion from on-demand use into continuous-use is necessary.

   Safe failure fraction is a concept that does not exist in CENELEC EN 5012[6/8/9] standards and which may be used to allocate less requiring SIL than necessary. Its use is therefore unlikely to be accepted in the railway domain.

4. The personnel competency:

   The competency verification is not explicitly required by the IEC 61508 arrangements. The competency of different involved persons needs therefore a verification.[1]

5. Structuration and contents of the documentation:

   It is recommended to adopt or confirm the division of the documentation into generic product, generic application and specific application. If this is not the case, we may lose the reusability of the generic product for multiple applications.

6. Cultural approach and associated impact: Terminologies and definitions

   Differences in terms and scopes need to be considered and translated into additional requirements for the cross-acceptance.

7. Functional Safety:

[1] Competency is a wider subject than our concern regarding differences between standards, as it relates to the educational system

Two contradicting definitions of functional safety leads to different understanding which can impede the cross-acceptance.

8. Independent assessment by an external party:

   The “Independent” Safety Assessor in CENELEC EN 5012x and in IEC EN 61508 are defined based on different criteria for SIL3 and SIL4 development.

9. Organisation and independence of roles:

   The independence in the project organization in CENELEC EN 5012x and in IEC EN 61508-x are defined based on different criteria depending on the different roles.

A Cross-Acceptance guideline is therefore required and is the next important step to be conducted with respect to safety. This Cross-Acceptance guideline concerns the supplementary requirements/conditions to fulfil in order to achieve the Cross-Acceptance of a Non-Railway Component which was originally developed and approved with an alternative Global Standard, meaning that this alternative standard is comparable in terms of requirements with the referenced Standard.

1 Introduction

1.1 Document context and purpose

This document BWS09-020 takes the case of CENELEC EN 5012x and IEC EN 61508-x as a starting point in order to analyse and expose the additional demonstrations to be carried out in order to accept the reusability of a Non-Railway Component certified under IEC EN 61508 in the context of system integration under EN 5012x. It is the 1st release of this document and it is still in a preliminary state.

This document aims to:

- Explain the rationales for a focus on CENELEC EN 5012x and IEC EN 61508-x
- List the key activities to accept a Non-Railway Component for system integration under CENELEC EN 5012x

The important next step after this document will be the creation of a guideline regarding the cross-acceptance between IEC EN 61508 and CENELEC EN 5012x.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing on-board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Why should I read this document and how to provide feedback?

This document is published as part of the OCORA Delta release, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

1.3 Definitions and used terminology

Do refer also to BWS09-010 for the full list of definitions and used terminology.

For the sake of understandability, find below the definition of the most important expressions used all over this document.

Non-Railway Component: A part of or a single building block that originates from a non-railway domain.

In this document, a non-railway component can be integrated into the (CCS) on-board or (CCS) trackside system.

Cross-Acceptance [of a product, system or process]: is 'an aspect of the technical and legal process principally aimed at establishing the fastest route to the deployment of Product, System or Process in a target (new) context or environment. The Product, System or Process considered for cross-acceptance is generally assumed to satisfy the qualifications for reliability, tolerable safety and environmental performance in their native (original) context or environment' (c.f. [12]).

In this document, 'Cross-Acceptance' is understood as the fact that equivalence between two requirements of two different standards is recognized once for all and has not to be re-demonstrated each time. Cross-acceptance also includes cases where a re-demonstration is required, but only on particular issues.

'**Global Standard**',a well-proven and largely-applied standard adopted by an international body or a European standardization organization in a different domain than the railway sector.

'RAMS' stands for "Reliability, Availability, Maintainability and Safety, as defined in standards like CENELEC EN 50126-1 [7] (part 2 [8] specific to Safety) and IEC EN 61508-1 [11].

2 Framework for safety requirements

The railway specific RAMS-related standards CENELEC EN 50126, EN 50129, EN 50155 and EN 50128/EN 50657 have many common parts with the set of IEC EN 61508-x standards for functional safety software and E/E/PE. The target of the requirements is very similar for both set of standards.

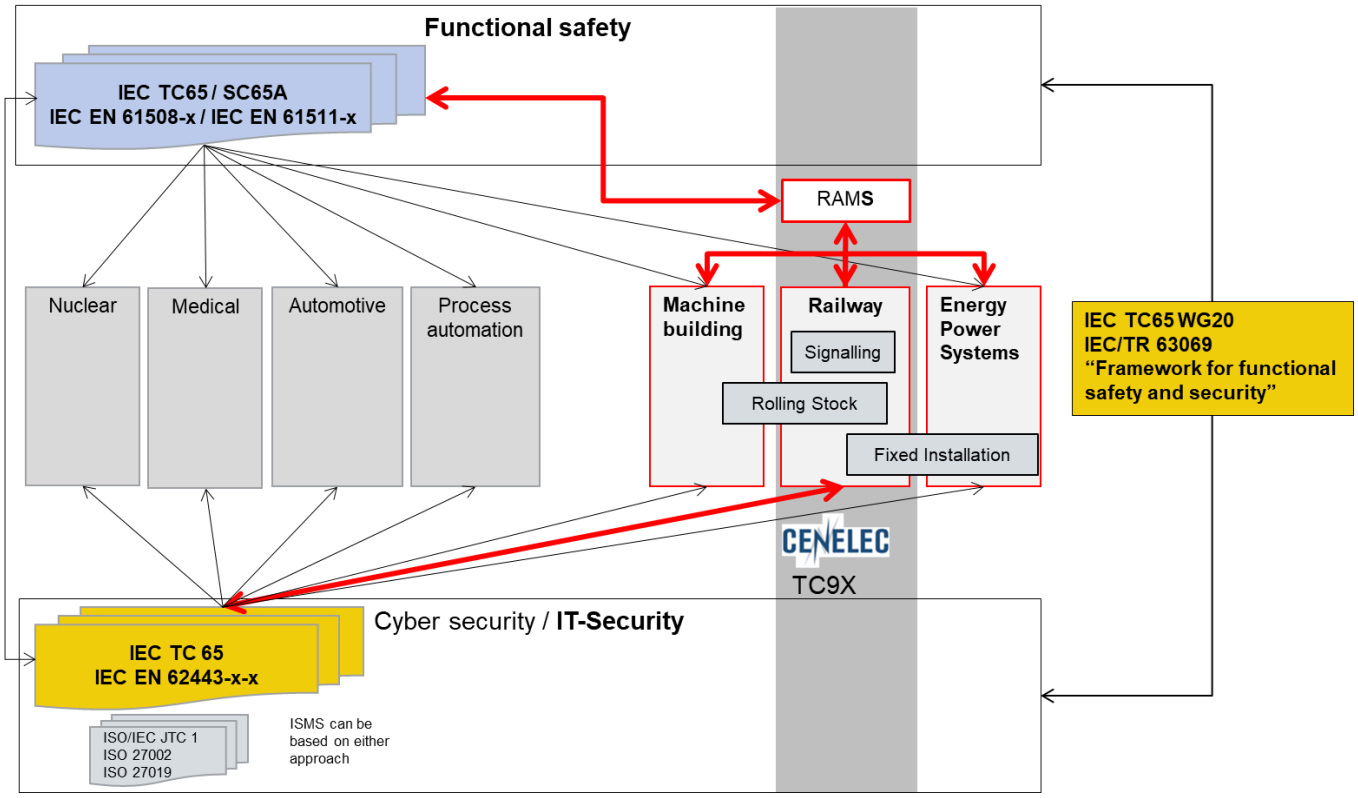

Figure 1 Horizontal standard framework for functional safety and IT-Security (ISMS stands for Information Security and Management system

IEC TC65 including sub-committee SC65A is responsible for IEC EN 61508-x and IEC EN 61511-x. At the moment, the maintenance of IEC EN 61508-x:2015, Edition 2 is ongoing. IEC TC65 is responsible for standards on functional safety and IT-Security. The relationship between safety-related software and IT-Security is identified and TC65 tasks this issue to TC65 WG20. A Technical Report is in preparation.

When developing a railway specific set for RAMS the differentiation of Equipment under Control (EuC) and Control Unit (CU) used in IEC EN 61508 series is not part of railway RAMS standards:

- The IEC EN 61508 set deals with functional safety requirements.
- The scope of CENELEC EN 50129:2018 and CENELEC EN 50128:2011 is limited to safety-related functions.

The maintenance of CENELEC EN 50126:1999, TS 50126-1 and TS 50126-2 for Safety has been finalized in 2017. The rolling stock version of CENELEC EN 50128:2011 is published as CENELEC EN 50657 in 2017. The maintenance of hardware standard for RAM EN 50155 for rolling stock is finalized in 2017.

The maintenance of the signalling specific safety standard CENELEC EN 50129 for safety-related applications has been finalized in 2018.

The approach of IEC TC65 to describe all requirements in a horizontal set of standards, which have no sector specific relation, is very useful. On **Figure 1** are represented with red arrows the relationships between Technical committee that are not sector specific.

As this document is concentrated on CCS and safety, only the following standards will be studied in this document: CENELEC EN 50126-x, EN 50129, EN 50128 and IEC EN 61508-x[2].

3 Control Command and Signalling Safety standards

3.1 Status of safety standards in the current EU legislation (CCS TSI and CSM-RA)

The application of European RAMS standards CENELEC EN 50126, EN 50128 and EN 50129 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 (**Figure 2**).

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.

[2] Other standards may be added in further version of this document; For instance, EN 13849 standard deals with performance levels (PL) and EN 62061 gives advice to transform Performance Levels into SIL

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 2 List of mandatory standards (from CCS TSI)

The application of the specifications described in Table A3 of CCS TSI is the only one recognised as an appropriate means to fully comply with the risk management process set out in Annex I of the Implementing Regulation (EU) N° 402/2013 for the design, implementation, production, installation and validation (including safety acceptance) of interoperability constituents and subsystems.

Nevertheless, the chapter §3.2.1 of the CCS TSI leaves a possibility to use different means for presumption of conformity with the regulation (EU) 402/2013, as long as a demonstration of equivalence with CENELEC EN 5012X and EN 50159 standards is provided:

> *"[..]*
>
> *When different specifications from the ones referred to in Annex A, Table 3 are applied, at least equivalence shall be demonstrated with the specifications in Annex A, Table 3.*
>
> *[..]"*

The sufficient elements of demonstration of equivalence need therefore to be provided and agreed with the different Assessors (ISA according to CENELEC EN 50126, NoBo, DeBo, AsBo) of the Non-Railway Components of the CCS Subsystem under the EU railway regulation.

A sectoral agreement on those generic elements of demonstration to be provided can simplify the cross-acceptance process and the conformity with the regulation CSM-RA on a common safety method for risk evaluation and assessment.

3.2 Roles and responsibilities of the different Assessors

Figure 3 represents the scope and role of each assessor under the overarching responsibility of the applicant in charge of the risk assessment and risk management at the system level. The ISA (Independent Safety Assessor) has a role apart as it is only defined in the frame of CENELEC EN 5012x. The DeBo is here represented in its role of evaluation against safety requirements.

With a modular architecture, a proper design with a clear separation between specific application, generic application and generic product as prescribed in CENELEC EN 50126 would simplify the integration task.

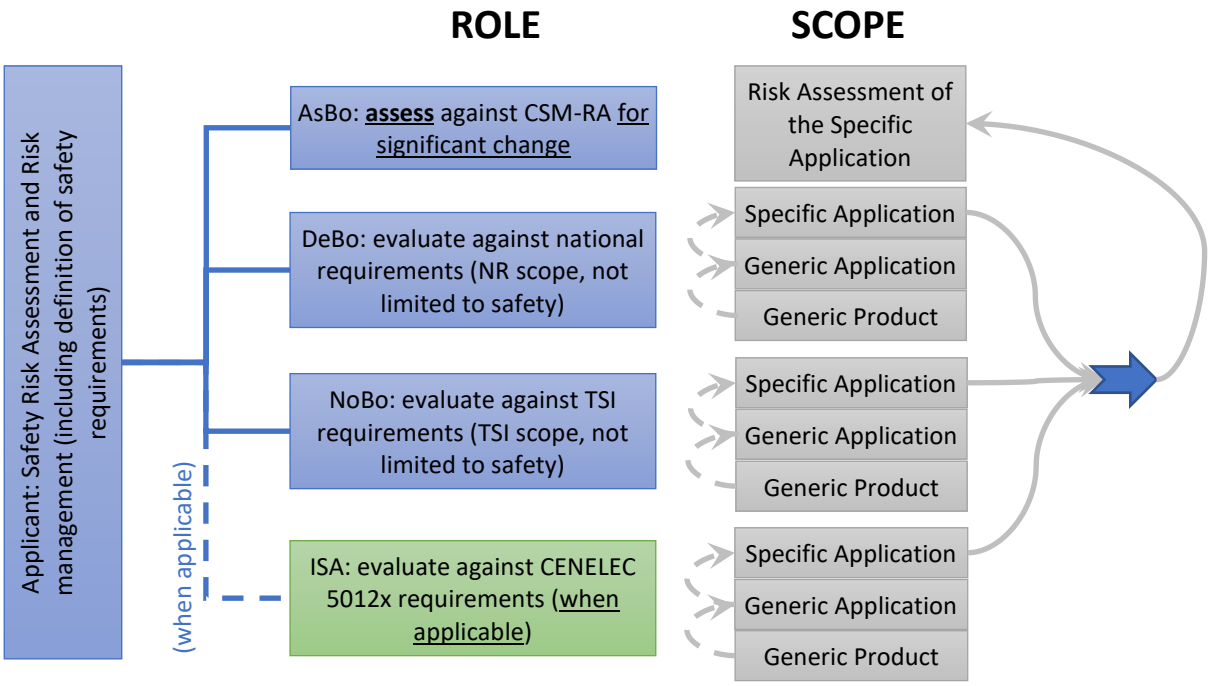

Figure 3 Status of the Assessors in the UE Regulation

Furthermore, a clear division between the roles and responsibilities of the different actors (including the system integrator) are of key importance for the project.

4 Comparison between IEC EN 61508 series and CENELEC EN 5012x

The core activities of cross-acceptance (total or partial), if anticipated and agreed at sectoral level, can reduce the time-to-certification and consequently the time-to-market and thus 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 (CENELEC EN 5012x) and the generic industrial safety standard suite (IEC EN 61508-x).

The CENELEC EN 5012x (RAMS) and IEC EN 61508 standards are grossly comparable, except on several points like for the determination of an acceptable architecture and the way independence shall be proven.

In order to accept the reusability of a Non-Railway Component certified under IEC EN 61508 in the context of system integration under CENELEC EN 5012x, two paths can be taken:

- A linear and systematic comparison of standards for cross-acceptance of products/systems developed according to IEC EN 61508 while the application of CENELEC EN 50126, EN 50128 and EN 50129 standards is required.
- The identification of the all points that the applicant would require to see addressed during the safety demonstration in order, for him, to properly conduct safety risk assessment and risk management.

5 Systematic and linear comparison between IEC EN 61508 and CENELEC EN 5012x

This approach has been manually undertaken on a limited set of clauses and requirements in order to draw our first conclusions on a systematic and linear comparison.

IEC EN Standard	Topic	CENELEC EN equivalent
IEC EN 61508-1	General requirements	CENELEC EN 50126
IEC EN 61508-2	E/E/PE requirements	CENELEC EN 50129
IEC EN 61508-3	SW requirements	CENELEC EN 50128 / EN 50657
IEC EN 61508-4	Definitions/Abbreviation	
IEC EN 61508-5	Methods for allocating SIL	CENELEC EN 5012X
IEC EN 61508-6	Guidelines for Part 2/3	
IEC EN 61508-7	Techniques/measures	CENELEC EN 50128 & 9

Table 1 Equivalence between IEC and CENELEC Standards

Considering the example of software requirements, the table in Annex 1 highlights, in a systematic clause-by-clause approach, the main similarities and differences between IEC EN 61508 and CENELEC EN 50128 version 2011. A systematic approach within the CENELEC EN 50126-1/-2 and CENELEC EN 50129 is required in EN 50128 for functional safety and a mandatory level of requirement had been introduced for the selection of technique and measures.

Despite the fact that a requirement management tool would be more effective to analyse the changes in processes and methods that a shift in standards create for the assessors and the suppliers, the following conclusions could be drawn:

1. A systematic and linear analysis requires RAMS experts with a practical experience in both IEC EN 61508 series and CENELEC EN 5012x. This is globally the case for the experts gathered for conducting this comparison, with of course a greater experience in the railway RAMS standards
2. It must be paid a particular attention to differences in interpretations due to different but similar terminologies and definitions, for instance “functional safety”
3. Differences in a clause-by-clause can only be fully useful by considering the core subjects of differences
4. Through this limited systematic approach, the following areas to be further addressed have been identified so far:

a. the development process,
b. the lifecycle model,
c. the personnel competence,
d. the perimeter of safety integrity level (including SIL0),
e. the organisation and independence of roles.

6 Major points to be addressed for cross-acceptance

The safety demonstration made with CENELEC EN 5012x, at system level benefits from a global consensus from railway RAMS experts.

However, outside of the railway domain, many individual Non-Railway Components are rather certified according to the IEC EN 61508 whose scope is general to all kinds of industry.

In order to accept the reusability of a Non-Railway Component certified under IEC EN 61508 in the context of system integration under CENELEC EN 5012x, the following areas have been identified as major topics to address with respect to the capacity of the applicant to accept a safety demonstration.

§ in this document	subject	Short description of the subject
§6.1	Single failure for SIL3 and SIL4	No single random failure should lead to an unsafe state which could lead to a catastrophic accident. It has to be assessed qualitatively and may also need to be done quantitatively.
§6.2	Intrinsic safety	CENELEC EN 50129 needs to be applied when intrinsic safety is required, as no requirements are specified in IEC EN 61508
§6.3	SIL allocation including “safe failure fraction”	In IEC EN 61508, SIL allocation can be made according to two different tables: on-demand use or continuous-use. In CENELEC only continuous-use table exists. To allow SIL allocation, a conversion from on-demand use into continuous-use is necessary. Safe failure fraction is a concept that does not exist in CENELEC EN 5012[6/8/9] standards and which may be used to allocate less requiring SIL than necessary. Its use is therefore unlikely to be accepted in the railway domain.
§6.4	The personnel competency	The competency verification is not explicitly required by the IEC 61508 arrangements. The competency of different involved persons needs therefore a verification.
§6.5	Structuration and contents of the documentation	it is recommended to adopt or confirm the division of the documentation into generic product, generic application and specific application. If this is not the case, we may lose the reusability of the generic product for multiple applications.
§6.6	Cultural approach and associated impact: Terminologies and definitions	Differences in terms and scopes need to be considered and translated into additional requirements for the cross-acceptance.
§6.7	Functional Safety	Two contradicting definitions of functional safety leads to different understanding which can impede the cross-acceptance.
§6.8	Independent assessment by an external party	The Independent Safety Assessor defined in CENELEC EN 5012x and in IEC EN 61508 are defined based on different criteria for SIL3 and SIL4 development.
§6.9	Organisation and independence of roles	The independence in the project organization in EN 5012x and in IEC EN 61508 are based on different criteria depending on the different roles

Table 2 Major points to be addressed for cross-acceptance

6.1 Single failure for SIL3 and SIL4

The main objection from railway experts against the IEC EN 61508 standard, compared to CENELEC EN 5012X, is the acceptance of systems with “hardware fault tolerance” (HFT).

- For railway experts it is unacceptable that, a single fault leads 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 IEC EN 61508 for SIL3/4 even if a single fault might lead to an unsafe state, provided that the risk is sufficiently low.

Therefore, for each Non-Railway Component which certification against IEC EN 61508 is to be cross accepted into an CENELEC EN 50126/8/9 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 Non-Railway Component and whether any of these failures can lead to an unsafe state which could lead to a catastrophic accident.
- 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 → if these exported constraints are not realistic, they will not be put in place, and thus the system will not reach its intended safety target). 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”.

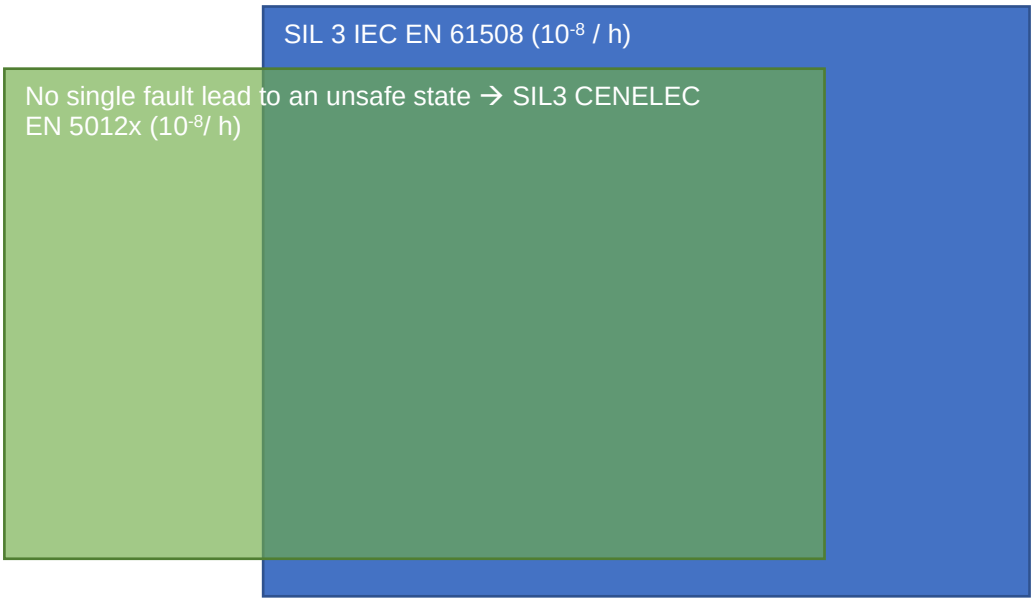

Figure 4 Nesting of SIL Level

The “no single failure” may also be met by using redundancy of Non-Railway Components.

Arithmetical view:

SIL 3 IEC EN 61508 (10^{-8} / h) & No single fault → SIL3 CENELEC EN 5012x

Further relations are to be investigated during the project

6.2 Intrinsic safety

The IEC EN 61508-1 standard mentions the application of intrinsic safety principles as a way to eliminate at source identified hazards. However, no requirements are specified, and no principle of intrinsic safety is described.

Nevertheless, it allows the use of intrinsic safety principles and thus recognizes the application of intrinsic safety standards.

For the IEC EN 61508-1 standard, intrinsic safety principles are part of techniques and measures applicable to safety-related E/E/PE systems in relation to the anomalies or failures to be assumed when quantifying the effect of random equipment failures.

cf. 61508-1 §Introduction and §7.4.2.2.

The CENELEC EN 50129 standard allows the application of intrinsic safety principles.

It is an intrinsic safety standard to which the IEC EN 61508-1 standard directly refers (without mentioning it).

The concept of intrinsic safety is described.

The technique – intrinsic safety – allows a safety-related function to be performed by a single entity, provided that for the Non-Railway Component under study, **no failure** can lead to a catastrophic accident (all failure modes are fail-safe, or lead to non-catastrophic consequences).

The dangerous failure rate of intrinsically safe designed hardware Non-Railway Components is assumed to be zero. As the assumption of zero fault has to be clarified, it means that these failures whose effects have been shown to be negligible can be ignored.

The requirements of intrinsic safety are specified in more details as failure modes and times of occurrence of random hardware failures.

The failure modes of the hardware Non-Railway Components (analogue or numbered electronics) are detailed.

cf. §Annex A3 and §Annex C5

The CENELEC EN 5012x requirements are more prescriptive on intrinsic safety and must be applied for intrinsic safety Non-Railway Components. Otherwise, it is unacceptable.

6.3 SIL allocation including “Safe failure fraction”

When studying about integrating a **Non-Railway Component** that was developed according to IEC EN61508 into a railway application, the following statements are important to understand and follow:

1. The non-railway standard has been applied at the Non-Railway Component level. However, the integrator will apply the railway standards (CENELEC EN 5012x) for the overall system in which the Non-Railway Component will be integrated (be it a Rolling Stock application (i.e. train or train modification) or signalling application (e.g. level crossing, interlockings, a line that includes several signals, …)).
2. The **safety target** to be achieved is the responsibility of the system integrator, not the supplier of the Non-Railway Component, since the system integrator will in all cases need to demonstrate that the overall system is safe, and in conformity with Regulation (EU) 402/2013 (**C**ommon **S**afety **M**ethod on **R**isk **A**cceptance)
3. To do so, the system integrator will need to rely on the safety development state supported by:
    - Recognised independent assessment reports stating that the Non-Railway Component has been developed in accordance with the adopted standard (IEC EN 61508-x);

- Thorough documentation, tests and structural analyses (including the failure rate of the Non-Railway Component, if possible for each failure mode, and – when applicable – the **S**afety **I**ntegrity **L**evel **applied** for the Non-Railway Component) to estimate the satisfactory fulfilment of the supplementary requirements listed in the future cross-acceptance guideline (corresponding to the adopted standard IEC 61508) in regard to the railway safety target intended.

This process related to pre-existing Non-Railway Component can be understood as in compliance with CENELEC EN 50126-1 section 7.6.2 requiring:

- the demonstration of the implemented quality (in accordance with a standard) [→ Item 3.a]
- *and in case of safety-related functions, possible failures will not jeopardize the defined safety requirements [→ Item 3.b]*
- and justified in the system architecture (without impacting the defined system safety requirements) [→ role of the system integrator].

4. If the expected criteria listed in 3.a and 3.b cannot be met, this should be considered as a non-compliancy with CENELEC EN 50126 requirement, unless an entire safety demonstration in accordance with railway standards is ensured by the system integrator or the supplier.

When using the aforementioned inputs, the following blocking points have to be treated:

- Regarding the SIL:
  - The allocated SIL of a Non-Railway Component (and the way it has been allocated) may not be the most important issue, in particular when the sole Non-Railway Component does not perform a safety function, but is part of a larger overall system which performs the function with a specific safety target: As the Non-Railway Component is anyway integrated in a larger overall system with a specific safety target, the SIL level should be redefined without reference to the original SIL level. This redefinition is performed according to the railways standards and is based on the available information provided by the supplier. Then this redefined SIL is compared to the requirements resulting from the safety apportionment in the overall system (along with the achieved failure rate, which is compared with the safety target from the CSM)
  - In the case of a Non-Railway Component performing a function to which a SIL has been allocated by the integrator, there are two possibilities:
    - Either the SIL allocated by the integrator is low enough (i.e. SIL2 at maximum) to cross-accept, with the railway-specific supplementary verifications, then the SIL proven by the provider under the IEC standard can be used. These supplementary verifications will be concentrated on railway specifics: e.g. vibrations, EMC, etc. which are not dealt in the CENELEC EN 5012[6/8/9].
    - Or, the safety requirement is too high to achieve cross-acceptance (i.e. SIL 3 or SIL4). Then a complete re-demonstration is required due to the important differences between IEC and CENELEC standards.
  - Be careful though that the methodology for allocating a SIL is largely different between IEC EN 61508 & CENELEC EN 5012x about the following specific issues:
    - THR to be achieved: the THR to reach is different in IEC EN 61508-1 depending on the type of solicitation of the Non-Railway Component: low-demand vs high demand/continuous. This can lead to bad use of the supplier which will decide to use one table or the other depending on the chosen outcome.

      Therefore, the CENELEC EN 50126-2 (§10.2.2) states "*In the case that failure probabilities on demand are given, they can be transformed into appropriate continuous mode models.*"

      - Thus, when using IEC EN 61508 Non-Railway Component, the THR to be reached shall only use table 3 of IEC EN 61508-1.
      - The supplier will precise the exact calculation that was used to convert the on-demand probability in failure rate.

- This failure rate will be compared to the THR required in the aforementioned table 3, to confirm whether the claimed SIL is applicable in the railway domain.

- "Failure fraction": tables 2 & 3 of IEC EN 61508-2 provide "maximum level of SIL" depending on the failure proportion. This is misleading and not conform to the requirements of CENELEC EN 5021x: instead of the "failure proportion", only the **achieved** failure rate is to be used.
    - The failure rate achieved, taking into account **all failures that can lead to an unsafe condition** (and thus all possible failures if the supplier does not know how the product can be integrated) will cover both the "failure proportion" and the "fault tolerance" concepts of tables 2 & 3 of IEC EN 61508-2
    - Therefore: a Non-Railway Component with a failure rate of $5x10^{-8}$ / h can be considered SIL2 **if and only if** it applied the qualitative measures of table A.15 regarding SIL2.
    - It could also be considered SIL3 **if and only if** it applied the qualitative measures of table A.15 regarding SIL3 **and** no single failure can lead to an unsafe condition (see 6.1 for this last part).
- SIL combination: this concept is forbidden in CENELEC EN 5012x.
    - The supplier may combine products and systems to achieve a better failure rate (the integrator may also do the same)
    - However, this combination will not achieve a higher SIL in any case, as the qualitative requirements behind SIL will not have been reached (table A.15 of IEC EN 61508-2)
    - This is explained in CENELEC EN 50126-2: *"SILs should be assigned at the level of the last independent function only after a risk analysis in the appropriate life-cycle phases according to one of the risk acceptance principles or equivalent derivation. It is meaningless to assign SILs prior to completing such an analysis"* (§10.2.12)

- Regarding the failure rate:
    - The failure rate calculated for the Non-Railway Component should take into account all failure modes (and combination thereof) that can lead to an unsafe state.
    - If such a detail is not possible (e.g. if the supplier does not know how its product will be integrated), then the overall failure rate (sum of all possible failure modes) shall be produced.
    - This failure rate shall not take into account external condition(s) outside of the Non-Railway Component under consideration (e.g. the failure rate of the fire detector shall not take into account the probability of a fire) → the failure rate shall be strictly limited to the technical failures of the product.
- Regarding intrinsic safety: see previous clause §6.2

6.4 The personnel competency

If the core of the two standards might be stated as globally equivalent with respect to their RAMS requirements, the correct and efficient implementation of the normative requirements are essential and shall be guaranteed in the goal of cross acceptance.

The correctness of this implementation can be achieved by proper quality process (e.g. through compliancy with ISO 9001 or equivalent – as required by both standards).

However, competency (including duties) of the key actors implicated in the assessment process should not be underestimated without compromising any mutual recognition.

Both standards require the necessary competency of the relevant parties to carry out the activities for which they are accountable, asking for proper justifications to be documented. However, the verification of these justifications is not managed in the same way.

If both standards seem to rely on the assessment activity to do so, the competency verification is not explicitly required by the IEC EN 61508 arrangements.

The IEC EN 61508 just refers to a person in charge of this assessment, approved by the functional safety manager, but not detailing this latter role and corresponding duties. On the other hand, CENELEC EN 50126 requires an Independent Safety Assessor with statutory roles (in some cases, it also needs to be accredited due to specific regulation, generally at the national level).

These differences could be particularly damaging to future cross acceptance.

It is then recommended to identify in a cross-acceptance guideline the additional requirements compared to the IEC EN 61508 in order to facilitate the global equivalence in regard to this topic.

This could be achieved thanks to:

- the completion of the assessment plan;
- some specific requirements related to the acceptance process of the selected Safety Assessor.

6.5 Structuration and content of the documentation

The division of the documentation into generic product (GP), generic application (GA) and specific application (SA) documentation is explicit in standard CENELEC EN 5012x. In CENELEC EN 50129 §8.1 and CENELEC EN 50126-2. §6.2, the overall documentary evidence for safety acceptance are explicitly defined for the 3 aforementioned categories.

CENELEC EN 50129 §8.1 describes the following steps:

- the system requirements specification;
- the risk assessment outcomes;
- the safety requirements specification;
- the safety case;
- the independent safety assessment report.

In addition, CENELEC EN 50126-2 §6.2 describes the necessary parts of the safety case for both the physical implementation and the application design:

- Part 1: Definition of the system;
- Part 2: Quality Management Report;
- Part 3: Safety Management Report;
- Part 4: Technical Safety Report;
- Part 5: Related safety cases (if applicable);
- Part 6: Conclusion.

The overall documentation structuration is more flexible within IEC EN 61508-x providing examples of the documentation structuration covering the overall safety life cycle for the system, an E/E/PE system and a software (c.f. IEC EN 61508-1 Annex A). The overarching structuration between GP/GA/SA is not captured within the IEC EN 61508-x.

In order to facilitate the cross-acceptance of an IEC EN 61508-certified product:

- it is recommended to adopt or confirm the division of the documentation into generic product, generic application and specific application.

- If this is not the case, we may lose the reusability of the generic product for multiple applications.

The important aspect remains the design and validation of the product and the evidences provided in the safety report.

6.6 Cultural approach and associated impact: Terminologies and definitions

Implementation of standard requirements is totally framed by the sense of the terms used and their understanding in the occupational field concerned: that's the weight of the cultural approach.

In the evaluation process related to the cross-acceptance of a Non-Railway Component developed in accordance with another standard, it is essential therefore to be convinced that terminologies, definitions and corresponding interpretation of the implemented standard are the same, or at least equivalent, to those of the original standard. Otherwise ambiguities or even contradictions may occur with potentially dire consequences.

This undesirable situation may occur, if:

- one of these issues relies on the existence of terms only used by one of the two considered standards (as for instance "generic product/generic application and specific application" used by the sole CENELEC EN 5012[6/8/9] standards);
- terms are identical but with different meaning or interpretation. This could be implicit, particularly emphasised by the translation of standards (the "evaluation" / "assessment" are translated in some language by the same term; not to mention errors in translations), and/or explicit with different definitions or scopes. For the purpose of this document, the sole latter case will be addressed with examples presented at the end of this section.

Of particular interest to this cross-acceptance approach, special attention has to be paid on (non-exhaustive list):

- the general terms such as systems, subsystems, redundancy, element….;
- the safety terms such as independency, certification, approval, accident / harm / hazard, evaluation / assessment, authorisation, …;
- the major development milestone such as verification, validation, testing process, ….

These categories and items will have to be detailed in the future cross-acceptance guideline.

Examples

Given the above this can be shown thanks to the following sample: **verification** and **validation** are two terms broadly used and well understood by all parties. What would be the consequences in case of mismatches?

Comparing the IEC EN 61508 and CENELEC EN 50126-x standards, it can be noted the following definitions:

❖ **Verification**

Term	CENELEC EN 50126 definition	IEC EN 61508 definition
Objectives	*"The objective of verification is to demonstrate that the deliverables of each phase meet in all respects the requirement of that phase. Within the scope of verification, it may also be necessary to consider the input and process of a phase."*	*"The objective of the requirements of this subclause [verification] is to demonstrate, for each phase of the overall, E/E/PE system and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase."*
	These two definitions seem to be equivalent but with slightly different or added wordings.	
Scope	*"In each life-cycle phase, the verification tasks shall include the following:* *a) evaluation of the correctness and adequacy of the safety analysis;* *b) verification of the deliverables of the phase for compliance with the deliverables of former phases;* *c) verification of the deliverables of the phase for compliance with the requirements for this phase defined in this standard;* *d) assessment of the adequacy of the methods, tools and techniques used within the phase;* *e) evaluation of the correctness, consistency and adequacy of test cases and executed tests."*	*"The E/E/PE system verification planning shall specify the activities to be performed to ensure correctness and consistency with respect to the products and standards provided as input to that phase.* *The E/E/PE system verification planning shall consider the following:* *a) the selection of verification strategies and techniques;* *b) the selection and utilisation of the test equipment;* *c) the selection and documentation of verification activities;* *d) the evaluation of verification results gained from verification equipment direct and from tests.* *In each design and development phase it shall be shown that the functional and safety integrity requirements are met."*
	Comparing these two scopes, the first one (CENELEC EN 50126) seems to be more prescriptive than the second one (IEC EN 61508) that remains at higher level, just specifying objectives to be met. **All of this can be considered as equivalent, provided that the implementation of the objectives raised by the IEC EN 61508 standard complies with the CENELEC EN 50126 prescriptions…**	

Table 3 Comparison of the definitions of Verification between the IEC EN 61508 and CENELEC EN 50126 standards

❖ **Validation**

Term	CENELEC EN 50126 definition	IEC EN 61508 definition
Objectives	"During phase 9 – System validation, the objectives of this phase are to: a) validate that the system, product or process in combination with its application conditions complies with the RAMS requirements; b) confirm or update the safety case for the system, product or process appropriate to the results of the validation; c) prepare the acquisition and assessment of operational data. Note: There is also a validation activity in regard to the specification of system requirements (phase 4)."	"The objective of the requirements of this subclause [validation] is to validate that the E/E/PE safety- related system meets in all respects the requirements for safety in terms of the required safety functions and safety integrity (see 7.2 above and 7.10 of IEC EN 61508-1)."
Scope	"A RAMS validation plan shall be established. This RAMS validation plan should include: A) Identification of the system, product or process subject to validation; B) identification of the steps necessary to demonstrate the adequacy of the deliverables of each phase of the system, product or process to be validated, in fulfilling the specified requirements; C) Identification of the steps necessary to demonstrate the adequacy of planned testing activities against the specified requirements; D) Justification of the validation and testing strategy under consideration of the required safety integrity; E) The RAMS tests and analysis to be carried out for the validation including details of the required environment, tools, facilities etc.; F) the validation management structure including requirements for personnel independence; G) procedure for dealing with non-compliance."	"Planning for the validation of the E/E/PE safety-related system shall consider the following: A) all of the requirements defined in the E/E/PE system safety requirements specification and the E/E/PE system design requirements specification; B) the procedures to be applied to validate that each safety function is correctly implemented, and the pass/fail criteria for accomplishing the tests; C) the procedures to be applied to validate that each safety function is of the required safety integrity, and the pass/fail criteria for accomplishing the tests; D) the required environment in which the testing is to take place including all necessary tools and equipment (also plan which tools and equipment should be calibrated); E) test evaluation procedures (with justifications); F) the test procedures and performance criteria to be applied to validate the specified electromagnetic immunity limits; NOTE Guidance on the specification of electromagnetic immunity tests for elements of safety-related systems is given in IEC/TS 61000-1-2" G) policies for resolving validation failure.
The requirements for the attended validation are quite expressed differently, CENELEC EN 5012[6/8/9] being more prescriptive than the required specified by IEC EN 61508. Identifying at this stage whether both phrasings are equivalent is quite difficult. Statement might be made at the objective level but with clear doubts at the implementation one.		

Table 4 Comparison of the definition of Validation between the IEC EN 61508 and CENELEC EN 50126 standards

In the context of comparing the IEC EN 61508 and CENELEC EN **5012[6/8/9]** standards, these two simple samples clearly reveal risks of misleading (at the implementation level) that may occur when definitions are quite different, or at least lying at various levels (objective / prescriptive). If it would be possible to conclude on the cross-acceptance between standards, the main issue is rather the manner in which the implementation of the corresponding normative requirements is carried out and deemed as acceptable means of equivalence.

And the independent safety assessment process will not be able on his own to clearly state on this equivalence without any recognized guideline since they just assess the correct implementation of the applied standard.

It is therefore necessary that the appropriate definitions and scopes are clarified in a cross-acceptance guideline and that the independent assessor recognizes and applies this guideline.

6.7 Functional Safety

We are facing two contradicting definitions of the functional safety concept:

1/ In IEC EN 61508, functional safety is defined as the part of the overall safety of a Non-Railway Component that depends on automatic protection operating correctly in response to its inputs or failure in a predictable manner (fail-safe). The automatic protection system should be designed to properly handle likely human errors, hardware failures and operational/environmental stress.

The objective of functional safety is freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly (through damage to property or to the environment) by the proper implementation of one or more automatic protection functions (often called safety functions). A safety system (often called a safety-related system) consists of one or more safety functions.

In the case of the integration of a Non-Railway Component, the functional safety shall not be limited to this Non-Railway Component but should consider the entire automatic protection function of the system under consideration. Functional safety standards focus on electrical, electronic, and programmable equipment (E/E/PE).

Even though the IEC EN 61508-x is applicable to E/E/PE, the same RAMS methodology needs to be applied to all Non-Railway Components including non E/E/PE Non-Railway Components. The SIL concept remains specific to E/E/PE Non-Railway Components since the technical annexes for IEC EN 61508-x are only application to those Non-Railway Components.

2/ In **CENELEC EN 50126-1** 3.26, functional safety is defined as **'**part of the overall safety that depends on functional and physical units operating correctly in response to their inputs'

Railway operators usually perform a "functional analysis" at the first step in the system design. In principle, it takes no assumption on how the contemplated function will be technically implemented (e.g. it can be mechanical, electronic, human procedure, etc.). At that level, a safety analysis is possible, identifying the effects of generic functional failures on the overall railway system. The generic functional failures usually considered are the following:

- not functioning,
- function lost when functioning,
- function continues when should stop,
- inadvertent, unintentional start-up,
- wrong function delivered or error,
- delay.

At that early stage, these failures are considered irrespective to their concrete causes, because these causes are unknown as the system is not technically designed yet.

Such an analysis helps for defining high level safety requirements, that can be refined and apportioned in following steps when the system is defined more in detail with precise technological choices.

6.7.1 Essential difference of understanding IEC EN 61508-x versus CENELEC EN 5012x / EN 50657

The understanding of functional safety principle according IEC EN 61508-x series is divided between:

- Control Unit (CU) which fulfils the safety requirements
- Equipment under Control (EuC) that is controlled by the CU

Safety according CENELEC EN 5012x is:

- If a system is identified as “safety-related”, the system has to fulfil safety requirements
- the safety requirements have to cover both the Control unit and Equipment under Control, but this is not exclusive.

The **Figure 5** depicts the essential difference in understanding the overall safety between IEC EN 61508 and CENELEC EN 5012[6/8/9] with respect to safety.

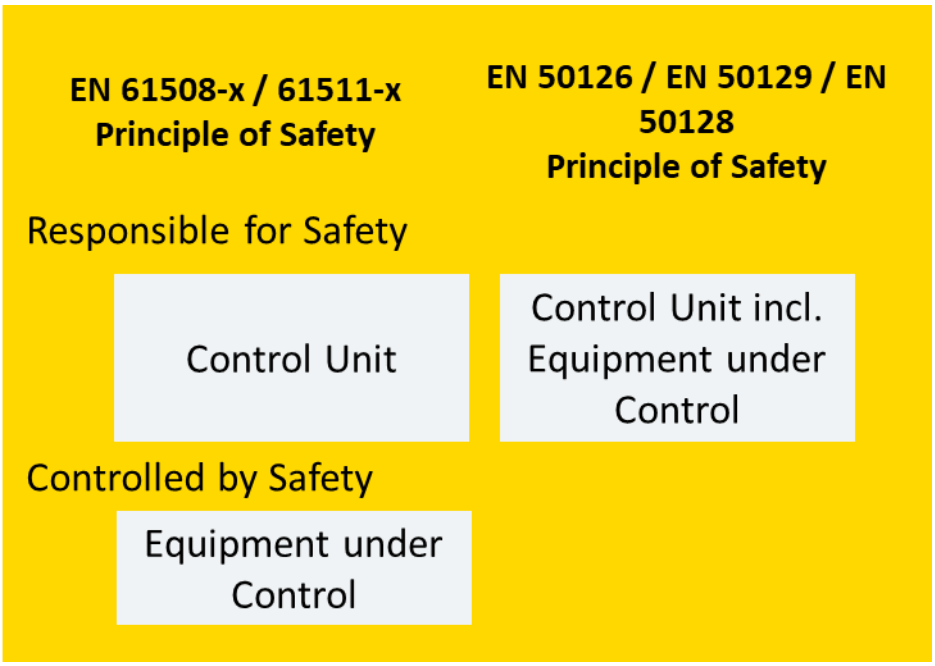

Figure 5 Essential differences in the understanding overall safety

6.8 Independent assessment by an external party

The Independent Safety Assessor defined in CENELEC EN 5012x and in IEC EN 61508 are defined based on different criteria for SIL3 and SIL4 development.

This subject will be addressed in a subsequent release of this document.

6.9 Organisation and independence of roles

The independence in the project organization in CENELEC EN 5012x and in IEC EN 61508 are defined based on different criteria depending on the different roles.

This subject will be addressed in a subsequent release of this document.

Annex 1. Example of a clause -by -clause analysis of IEC EN 61508-3 and CENELEC EN 50128 version 2011

Similarities are underlined while differences are in bold and in red.

IEC EN 61508-3, Ed 2	CENELEC EN 50128:2011
7.1.2 Requirements 7.1.2.1 A safety lifecycle for the development of software shall be selected and specified during safety planning in accordance with Clause 6 of IEC EN 61508-1.	
7.2 Software safety requirements specification 7.2.1 Objectives 7.2.1.1 The first objective of the requirements of this subclause is to specify the requirements for safety-related software in terms of the requirements for software safety functions and the requirements for software systematic capability. 7.2.1.2 The second objective of the requirements of this subclause is to specify the requirements for the software safety functions for each E/E/PE safety-related system necessary to implement the required safety functions. 7.2.1.3 The third objective of the requirements of this subclause is to specify the requirements for software systematic capability for each E/E/PE safety-related system necessary to achieve the safety integrity level specified for each safety function allocated to that E/E/PE safety-related system.	Introduction *(Comment by author: CENELEC EN 50128:2011 address issues, not specification in CENELEC EN 50128)* … CENELEC EN 50126-1 and CENELEC EN 50129 require that a systematic approach be taken to a) identify hazards, assessing risks and arriving at decisions based on risk criteria, b) identify the necessary risk reduction to meet the risk acceptance criteria, c) define an overall System Safety Requirements Specification for the safeguards necessary to achieve the required risk reduction, d) select a suitable system architecture, e) plan, monitor and control the technical and managerial activities necessary to translate the System Safety Requirements Specification into a Safety-Related System of a validated safety integrity.
7.4 Software design and development 7.4.3 Requirements for software architecture design	7.3 Architecture and Design
7.4.4 Requirements for support tools, including programming languages	6.7 Support tools and languages
Annex A (normative) **Guide** to the selection of techniques and measures	Annex A (normative) **Criteria** for the Selection of Techniques and Measures
See IEC EN 61508-7 for an overview of the specific techniques and measures referenced in Annexes A and B.	
With each technique or measure in the tables there is a recommendation for safety integrity levels 1 to 4. These recommendations are as follows. HR R -- NR	With each technique or measure in the tables there is a requirement for each software safety integrity level (SIL). In this version of the document, the requirements for software safety integrity levels 1 and 2 are the same for each technique. Similarly, each technique has the same requirements at software safety integrity levels 3 and 4. These requirements can be **M** HR R '-' NR
Table A.1 – Software safety requirements specification (See 7.2)	Table A.2 – Software Requirements Specification (7.2)

IEC EN 61508-3, Ed 2	CENELEC EN 50128:2011
NOTE 1 The software safety requirements specification will always require a description of the problem in natural language and any necessary mathematical notation that reflects the application. NOTE 2 The table reflects additional requirements for specifying the software safety requirements clearly and precisely.	Requirements: 1) The Software Requirements Specification shall include a description of the problem in natural language and any necessary formal or semiformal notation. 2) The table reflects additional requirements for defining the specification clearly and precisely. One or more of these techniques shall be selected to satisfy the Software Safety Integrity Level being used.
Table A.2 – Software design and development – software architecture design (see 7.4.3)	Table A.3 – Software Architecture (7.3)
2 Error detecting codes | C.3.2 | R R **R** HR	4. Error Detecting Codes | D.19 | - R R **HR** HR
* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. It is intended the only one of the alternate or equivalent techniques/measures should be satisfied. The choice of alternative technique should be justified in accordance with the properties, given in Annex C, desirable in the particular application. ** Group 11, “Structured methods”. Use measure 11a only if 11b is not suited to the domain for SIL 3+4.	Requirements: 1) Approved combinations of techniques for Software Safety Integrity Levels 3 and 4 are as follows: a) 1, 7, 19, 22 and one from 4, 5, 12 or 21; b) 1, 4, 19, 22 and one from 2, 5, 12, 15 or 21. 2) Approved combinations of techniques for Software Safety Integrity Levels 1 and 2 are as follows: 1, 19, 22 and one from 2, 4, 5, 7, 12, 15 or 21. 3) Some of these issues may be defined at the system level. 4) Error detecting codes may be used in accordance with the requirements of CENELEC EN 50159.

Table 5 Comparison IEC EN 61508-3, Ed 2 vs CENELEC EN 50128:2011

Bibliography of techniques: Comparison IEC EN 61508-7 vs CENELEC EN 50128:2011

IEC EN 61508-7, Ed 2	CENELEC EN 50128:2011
Annex B (informative)	Annex D (informative)
B.2.5 Checklists … Description: A set of questions to be answered by the person performing the checklist. Many of the questions are of a general nature and the assessor must interpret them as seems most appropriate to the particular system being assessed. Checklists can be used for all phases of the overall, E/E/PE system safety and software safety lifecycles and are particularly useful as a tool to aid the functional safety assessment. To accommodate wide variations in systems being validated, most checklists contain questions which are applicable to many types of system. As a result, there may well be questions in the checklist being used which are not relevant to the system being dealt with and which should be ignored. Equally there may be a need, for a particular system, to supplement the standard checklist with questions specifically directed at the system being dealt with. In any case it should be clear that the use of checklists depends critically on the expertise and judgement of the engineer selecting and applying the checklist. As a result, the decisions taken by the engineer, with regard to the checklist(s) selected, and any additional or superfluous questions, should be fully documented and justified. The objective is to ensure that the application of the checklists can be reviewed and that the same results will be achieved unless different criteria are used. The object in completing a checklist is to be as concise as possible. When extensive justification is necessary this should be done by reference to additional documentation. Pass, fail and inconclusive, or some similar restricted set of responses should be used to document the results for each question. This conciseness greatly simplifies the procedure of reaching an overall conclusion as to the results of the checklist assessment.	D.7 Checklists … Description A set of questions to be completed by the person performing the checklist. Many of the questions are of a general nature and the Assessor shall interpret them as seems most appropriate to the particular system being assessed. To accommodate wide variations in software and systems being validated, most checklists contain questions which are applicable to many types of system. As a result there may well be questions in the checklist being used which are not relevant to the system being dealt with and which should be ignored. Equally there may be a need, for a particular system, to supplement the standard checklist with questions specifically directed at the system being dealt with. In any case it should be clear that the use of checklists depends critically on the expertise and judgement of the engineer selecting and applying the checklist. As a result, the decisions taken by the engineer, with regard to the checklist(s) selected, and any additional or superfluous questions, should be fully documented and justified. The objective is to ensure that the application of the checklists can be reviewed and that the same results will be achieved unless different criteria are used. The object in completing a checklist is to be as concise as possible. When extensive justification is necessary this should be done by reference to additional documentation. Pass, Fail and Inconclusive, or some similar restricted set of tokens should be used to record the results for each question. This conciseness greatly simplifies the process of reaching an overall conclusion as to the results of the checklist assessment.
C.2.2 Data flow diagrams	D.11 Data Flow Diagrams

IEC EN 61508-7, Ed 2	CENELEC EN 50128:2011
NOTE This technique/measure is referenced in Tables B.5 and B.7 of IEC EN 61508-3. **Aim:** To describe the data flow through a program in a diagrammatic form. **Description:** Data flow diagrams document how data input is transformed to output, with each stage in the diagram representing a distinct transformation. Data flow diagrams have three aspects: - annotated arrows – represent data flow in and out of the transformation centres, with the annotations documenting what the data is; - annotated bubbles – represent transformation centres, with the annotation documenting the transformation; - operators (and, xor) – these operators are used to link the annotated arrows. Each bubble in a data flow diagram can be considered as a stand-alone black box which, as soon as its inputs are available, transforms them to its outputs. One of the principal advantages is that they show transformations without making any assumptions about how these transformations are implemented. A pure data flow diagram does not include control information or sequencing information, but this is catered for by real-time extensions to the notation, as in real-time Yourdon (see C.2.1.4). The preparation of data flow diagrams is best approached by considering system inputs and working towards system outputs. Each bubble must represent a distinct transformation – its output should, in some way, be different from its input. There are no rules for determining the overall structure of the diagram and constructing a data flow diagram is one of the creative aspects of system design. Like all design, it is an iterative procedure with early attempts refined in stages to produce the final diagram.	**Aim** To describe the data flow through a program in a diagrammatic form. **Description** Data Flow Diagrams document how data input is transformed to output, with each stage in the diagram representing a distinct transformation. The basic components of a data flow diagram include - functions, represented by bubbles, - data flows, represented by arrows, - data stores, represented by open boxes, - input/output, represented by special kinds of boxes. Data flow diagrams describe how an input is transformed to an output. They do not, and should not, include control information or sequencing information. Each bubble can be considered as a stand alone black box which, as soon as its inputs are available, transforms them to its outputs. One of the principle advantages of data flow diagrams is that they show transformations without making any assumptions about how these transformations are implemented. The preparation of data flow diagrams is best approached by considering system inputs and working towards system outputs. Each bubble shall represent a distinct transformation – its output should, in some way, be different from its input. There are no rules for determining the overall structure of the diagram and constructing a data flow diagram is one of the creative aspects of system design. Like all design, it is an iterative process with early attempts refined in stages to produce the final diagram.
C.2.4.5 LOTOS Aim: LOTOS is a means for describing and reasoning about the behavior of systems of concurrent, communicating processes. **Description:** LOTOS (language for temporal ordering specification) is based on CCS with additional features from the related algebras CSP and CIRCAL (circuit calculus). It overcomes the weakness of CCS in the handling of data structures and value expressions by combining it with aspects of the abstract data type language ACT ONE. The process description aspect of LOTOS could, however, be used with other formalisms for the description of abstract data types.	D.28.4 LOTOS Aim LOTOS is a means for describing and reasoning about the behavior of systems of concurrent, communicating processes. Description LOTOS (Language for Temporal Ordering Specification) is based on CCS with additional features from the related algebras CSP and CIRCAL (Circuit Calculus). It overcomes the weakness of CCS in the handling of data structures and value expressions by combining it with a second component based on the abstract data type language ACT ONE. The process definition component of LOTOS could, however, be used with other formalisms for the description of abstract data types.

IEC EN 61508-7, Ed 2	CENELEC EN 50128:2011
C.2.4.6 COBJ C.2.4.7 Temporal logic	Content of sub clauses identically 61508-7: D.28.5 OBJ D.28.6 Temporal logic
C.2.4.8 VDM, VDM++ – Vienna Development Method	D.28.7 VDM – Vienna Development Method Content partially taken from 61508, C.2.4.8, in this case unchanged.

Table 6 Examples of identic content (not complete)

Annex 2. The STM ATB example

The STMATB performs the ATBEG class B function. Based on a risk analysis, the required safety integrity level is calculated to be SIL3. The interfaces of the system consist of:

- An analogue track signal representing the current through the track.

  The information is in a current injected in the rails (75Hz track circuit currents) which are coded (switched on/off or switched between a high and a low level).

  The safety of the signal is included in the modulation and the phase relation between the left and right rail signal.

  Disturbances in the signal can in no way simulate a valid signal due to the requirements concerning the phase relation and further requirements concerning the signal levels.

Safety coding: modulation, phase relation and added test signals.

- A profibus connection with the ETCS on-board which is protected as specified in subsets 056/057 (“safety layers”)

  Safety coding: safety layers

- Digital input signals which are antivalent available (only relevant for SIL1 functions)

The “safety coding” of the signals is only removed in the central processor. This way only the subsystem including the processing has to comply with SIL3 requirements (except for the quantitative requirements equal to SIL4 requirements).

Several architectures were investigated, especially:

- 2oo2 system with two standard processors
- 2oo2 system with one ARM-9 processor and a soft-core processor built in an FPGA at the same chip (Xilinx Zynq)
- 1oo1D system (or 2oo2 according to CENELEC EN 5012x definitions) with a lock step processor and advanced safety functions (mainly implemented in hardware) provided by TI (Hercules microcontroller series).

Using a (standard) 2oo2 solution would lead to the need to develop a lot of software based diagnostic functions for the selected processor(s) (STM series were envisaged) which gives a much poorer coverage compared to the hardware diagnostics available in the TI processors. In addition, a comparison between the two channels could only be made at application level every calculation cycle (every 10 to 100ms) on a small range of values.

The solution based on the Xilinx Zynq is very robust. The diversity (two different processors) and simple self-testing of the FPGA are promising. However diagnostic functions for the ARM-9 were not available and no IEC 61508-2 certification is available. (IEC 61508-3 certification concerning the software tooling to implement functions at the FPGA and soft-core processor is available)

The TI Hercules provides the simplest solution. Hardware diagnostics are available which check the processor and on chip peripherals at run-time up to transistor level. The diagnostic functions can be sliced to execute a next step every cycle. The whole set fits within the STMATB system safety time.

In addition, a redundant on-chip CPU is available which is time shifted (2 cycles) and has a different orientation compared to the prime CPU. Data and address bus generated by the CPU’s are compared every 5ns. Both the coverage and the frequency of the comparison is orders of magnitude better compared to a classical 2oo2 system.

The internal design is not available in detail to the user, however the safety performance is assessed and certified by TÜV-Süd against IEC EN 61508-2.

Based on the above the TI RM48x micro controller (further the processor) was selected for the SIL3 compliant subsystem of the STMATB.

As most widely used components, the TI Hercules series (and Xilinx Zynq) are not certified against CENELEC EN 5012x. This is because these standards differ from more widely used standards, and the railway market is extremely small compared to the industry, medical and automotive sectors. The railway market size doesn't justify putting a lot of effort in certification of a 25-dollar product.

The IEC EN 61508-2 has more severe requirements. A standard 2oo2 architecture which is acceptable for SIL4 according to CENELEC EN 50129 if the channels are independent (see discussion below) and if a first fault is detected in time to guarantee the quantitative safety target, is not always accepted as SIL4 according to IEC EN 61508-2. This standard requires in addition:

- The safe failure fraction of the elements shall at least be 90%, i.e. > 90% of the faults shall not lead to an unsafe state (2oo2 implies HFT =1). **Do refer to §6.3 *SIL allocation including "Safe failure fraction"* for further warnings on the use of failure fraction and hardware fault tolerance**.

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Figure 6 extract of Table 3 of IEC EN 61508-2

- At least one of the redundant channels shall be certified against SIL3 requirements, not using further redundancy to achieve SIL3. See the extract IEC EN 61508-2 §7.4.4.2.4 below:

  7.4.4.2.4 In an E/E/PE safety-related subsystem where an element safety function is implemented through a number of channels (combination of parallel elements) having a hardware fault tolerance of N, the maximum safety integrity level that can be claimed for the safety function under consideration shall be determined by:

  a) grouping the serial combination of elements for each channel and then determining the maximum safety integrity level that can be claimed for the safety function under consideration for each channel (see 7.4.4.2.3); and

  b) selecting the channel with the highest safety integrity level that has been achieved for the safety function under consideration and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of the subsystem.

  These are requirements to which most SIL4 railway systems do not comply. (Also not the STMATB which is certified to CENELEC EN 5012x SIL3/4 requirements, however only complies with SIL3 requirements in the IEC EN 61508-2).

Nevertheless, cross acceptance of IEC EN 61508 certified Non-Railway Components for use in CENELEC EN 5012x certified systems is not possible. Therefore, the CENELEC EN 5012x (especially the CENELEC EN 50129) requirements had to be proven for the STMATB.

The key requirements are:

- no single fault shall lead to an unsafe state;
- if multiple faults can lead to an unsafe state then those faults may not have any common cause;
- if multiple faults can lead to an unsafe state then the occurrence of those faults shall be detected and negated in time to comply with the safety target;
- the quantitative safety requirements shall be proven.

Point 1. The TI Hercules series complies with this requirement, although this cannot be derived from the IEC EN 61508-2 certificate. As SIL3 according to IEC EN 61508-2 can be achieved when the safe failure fraction of the elements is > 99% (not 100%).

The IEC EN 61508-2 never considers a diagnostic function having 100% coverage. CENELEC EN 5012x based solutions which are called 2oo2, but with the second channel only used for comparison with the main channel, are according to the IEC EN 61508-2 categorized as 1oo1D. This implies a HFT ("hardware fault tolerance") = 0 while if the second channel covers 100% of the faults a single fault cannot lead to an unsafe state.

All elements in used from the Hercules processor for the STMATB application are either redundant (e.g. CPU's) or coded (memory). The memory has been a concern for which mitigating measures have been discussed with the assessor.

Point 2. The diagnostics implemented in hardware (and controlled from software) perform diagnostics on all safety relevant elements and diagnostic circuits with a coverage and frequency which are both orders of magnitude better than common in railway 2oo2 systems. Therefore, this requirement is fulfilled. However, as the conclusion could not be based on cross acceptance of the IEC EN 61508-2 certificates, the proof had to be based on the limited technical details of the product provided by TI to customers. (while TI developers have built the dossier for certification against IEC EN 61508-2 having all technical details available).

Point 3. Common causes are also an issue for certification against IEC EN 61508-2. However, for this standard the requirement is not "no common cause may lead to…." but common causes have to be taken into account when the quantitative safety requirements are proven.

The STMATB has been developed within the ERTMS program funded by the Ministry of Transport (I&W). It became clear in an early stage that the ERTMS introduction would delay and the alternative (buying an STM at the market) was available until the development has been finished. Therefore, it was acceptable to take risk in time and money during the development.

The chosen route is not practicable for industrial parties having a commercial contract with deadlines and penalties. Therefore, Non-Railway Components like the TI Hercules series and the Xilinx Zynq (and many others) with safety certifications for industry, medical and automotive (big markets) cannot be used for the railway market. However, these Non-Railway Components provide a high safety level at much lower costs compared to standard solutions in the railway market.