OCORA

Open CCS On-board Reference Architecture

Acceptance of Global Standards:

Cartography of Safety Standards

Document ID: OCORA-BWS09-030

Version: 1.00

Release: R1

Date: 30.11.2021

Management Summary

There are numerous standards addressing the safety subject, each main industrial domain has developed its own vision on safety. Identification of the main industrial domains, where components of the OCORA architecture are today emerging from, may allow us to grasp the gap in standard ecosystem between the first prototypes of CCS on-board as per today and the future CCS on-board subsystem as per tomorrow, in complete conformity with railway regulations. Once the most relevant industrial domains providing components to OCORA have been identified, this study shows how the domains' standards derived from the IEC 61508 or relate to each other, highlighting their relevant differences.

Revision history

Version	Change Description	Initial	Date of change
0.1	▪ Creation + addition of previous work	A.A	2021-10-23
0.2	▪ §3 RAMS standards of the relevant industrial domains from carsten	A.A	2021-11-03
0.3	Review in meeting with C.H, H.AK , A.A, C.G	A.A	2021-11-03
0.4	Conclusion and general modifications.	A.A	2021-11-04
0.5	Finalization review with HAK, AA, CG, JMP, OC	HAK	2021-11-17
0.6	Final review: modification of §2 order of presentation, minor correction in Annex 1 about LOC4Rail	HAK	2021-11-30
1.00	Official version for OCORA Release 1.0	HAK	2021-11-30

Table of contents

Table of figures

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] OCORA-BWS09-10 – Acceptance of Global Standards

[8] OCORA-BWS09-20- Acceptance of Global Standards Focus on Safety in CCS

[9] EN 50126-1:2017-10 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[10] EN 50126-2:2017-10 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[11] EN 50128:2011-06 – Railway Applications – Communication, signalling and processing systems - Software for railway control and protection systems

[12] EN 50129:2018-11 – Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[13] EN 50159:2010-09 – Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[14] TSI CCS: 02016R0919 - EN - 16.06.2019 - 001.001 - 1: COMMISSION REGULATION (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union, amended by Commission Implementing Regulation (EU) 2019/776 of 16 May 2019 L 139I

NOTE 1: IEC 61508-x and IEC 61511-x are parallel 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.

1 Introduction

1.1 Purpose of the document

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

Many RAMS standards used in various industries are a declination of IEC EN 61508 (i.e. ISO 26262 for the automotive industry, IEC 61513 for the nuclear industry). Yet, those standards may diverge from IEC EN 61508. The safety demonstration of future CCS on-board subsystem requires to well assess from which industrial sectors the future OCORA building blocks are emerging from and which certification practices are taken.

This document aims to:

- Identify the sectoral domains where OCORA non-railway components are emerging from
- Compare the uses and habits in safety assessment and standards in different industries

1.2 Applicability of the document

The document is currently considered informative but may become a reference at a later stage for OCORA compliant on-board CCS solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of this document

This document is published as part of the OCORA Release R1, 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].

2 Families of industrial domains for future CCS on-board subsystem

In order to identify the industrial domains where OCORA components may be emerging from, a product breakdown identifying the currently known suppliers within on-going research projects has been constructed. This product breakdown is derived from the OCORA architecture work with some simplifications. It is by no means relevant for SIL allocation, even though our focus remains the overall safety demonstration.

Recognizing that some OCORA components are deemed to be specifically built for the railway sector, the product breakdown structure has been filtered to exclude such products/parts. This is especially the case for components which are already existing in current CCS on-board subsystem or software-part of equipment.

This resulting analysis provided in annex 1 and shows that the future CCS on-board subsystem can benefit from input of other industries:

- For **CCS Core Computing platform** and **ATO Hardware:** Similarities in the needs and the products can be found with the **aeronautic and nuclear** industries. Those industries are used to develop fail safe components. Depending on the effort needed for being compliant with the railway industry, these companies can provide well proven hardware.
- For **CCS peripherals' train locator and its sensors:** Similarities in the needs and the products can be found with the **aeronautic industry**. The aeronautic industry has a historic background with failsafe and even fault-tolerant localization technologies.
- For **CCS Peripherals' Perception sensors**: Similarities in the needs and the products can be found with the **aeronautic** and **automotive industries**
- For **CCS peripherals' I/O Ports:** Potential similarities can be found with the instrumented systems for the **process industry**
- For **CCS peripherals' CCS add-on for storage of critical data:** the needs are similar with other industries using advanced storage server
- One example for the **CCS peripherals** have been made by NS with their implementation of the **STM ATB** on a commercial hardware platform from the electrical/ electronic/ programable electronics safety related systems.

3 RAMS standards of the relevant industrial domains

This section provides an overview of safety-related standards or normative documents of the industrial domains identified in §2.

- For each of those industrial domains, some information about their **cultural background** is given when available

The link of inheritance, alignment and new version between the different standards are represented in the following paragraphs using the same legend:

- Red arrow: link of inheritance with another existing standard when it was created;
- Blue arrow: new maintenance version of the concerned standard;
- White arrow: link of alignment done at a later stage of the lifetime of a standard.

3.1 Electrical /Electronic and Programmable Electronic

The standards EN IEC 61508-x applying to electrical /electronic and programmable electronic is the “mother” standards. The other safety-related standards are mainly derived from the latter.

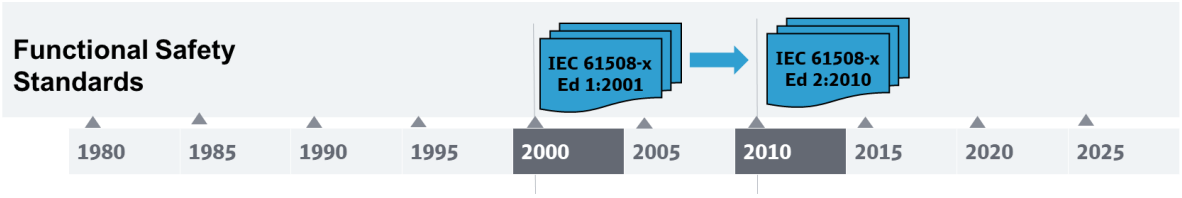

Figure 1 generic industry safety standards

EN IEC 61508-x - Functional safety of electrical / electronic / programmable electronic safety-related systems

Parts 1,2, 3, 4 (definitions),5, 6, 7

- Edition1: 2001
- Edition 2: 2010
- A new edition is under consideration: committee draft from IEC in April 2022

3.2 Railway industry

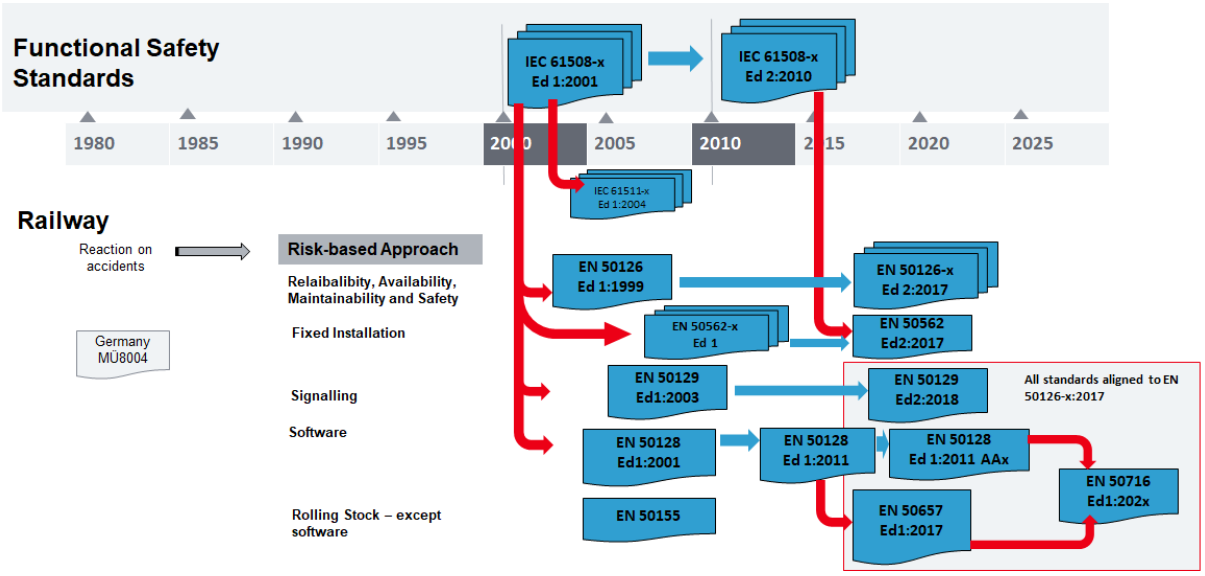

Figure 2 Railway safety standards

Risk-based approach is adopted from IEC 61508-x for the railway domain in the beginning of the 2000 years and adopted also in Common Safety Method regulation in the European Union.

- **CENELEC EN 50126** is based on IEC 61508-x and extended to reliability and availability.
- **CENELEC EN 50155** is mainly related to hardware in Rolling Stock, software is excluded. This standard has no link with IEC 61508-x.
- **CENELEC EN 50129** is focusing on signaling hardware, adopts EN 50126-x and EN IEC 61508-x
- **CENELEC EN 50128** is based on EN IEC 61508-x, several annexes derived from EN IEC 61508-6 and EN IEC 61508-7. Based on EN 50128:2011 the rolling stock version EN 50657:2017 was published.
- **CENELEC EN 50657** considers safety related and non-safety related software.
  CENELEC EN 50617 is the merging of CENELEC EN 50128 and CENELEC EN 50657 as a standard for software, applicable for Signaling and rolling stock. Fixed Installation software applications are excluded, because these applications are close to energy sector and the adopted EN IEC 61508-x in this domain.
- **CENELEC EN 50562 - Railway applications – Fixed installations – Process, protective measures, and demonstration of safety for electric traction systems**
  Annex D (informative) Guidance on software for safety functions on system level

3.3 Automation / Process Industry

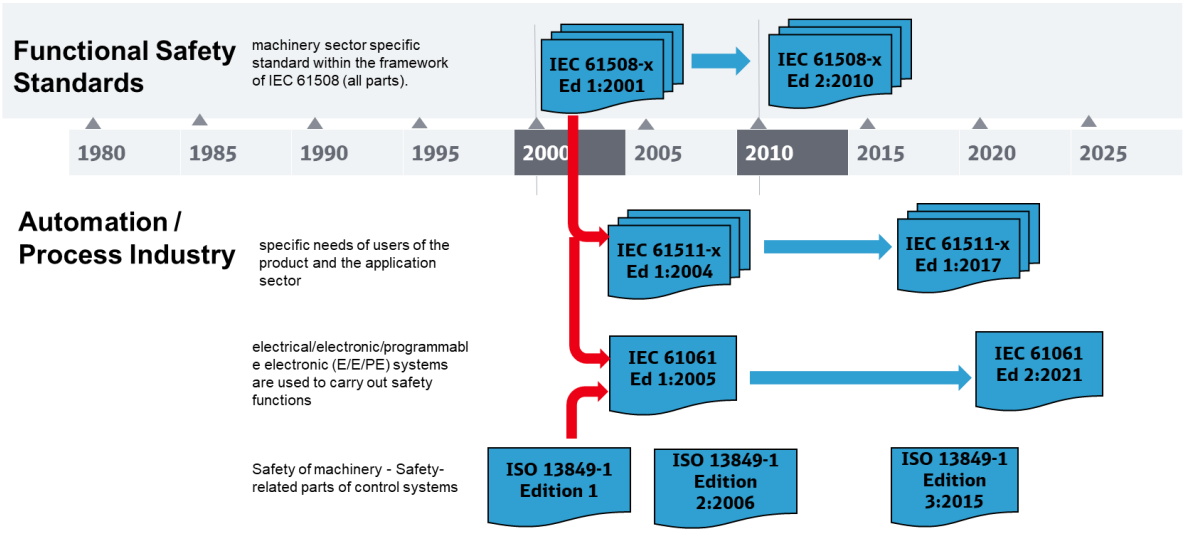

Figure 3 Automation safety standards

EN IEC 61511-x (Part 1, 2, 3) Functional safety - Safety instrumented systems for the process industry sector Part 1: Framework, definitions, system, hardware and application programming Requirements, Part 2: Guidelines for the application of EN IEC 61511-1, Part 3: Guidance for the determination of the required safety integrity levels

- Edition 1: 2004
- Edition 2: 2017

EN IEC 61511-1 has been developed as a process sector implementation of EN IEC 61508.

EN IEC 62061 - Safety of machinery - Functional safety of safety-related control systems

- Edition 1: 2005
- Edition 2: 2021

This document is a machinery sector specific standard within the framework of EN IEC 61508 (all parts). CLC/TR 62061-1:2010 - Guidance on the application of EN ISO 13849-1 and EN IEC 62061 in the design of safety-related control systems for machinery

EN ISO 13849-1 - Safety of machinery - Safety-related parts of control systems

3.4 Automotive Industry

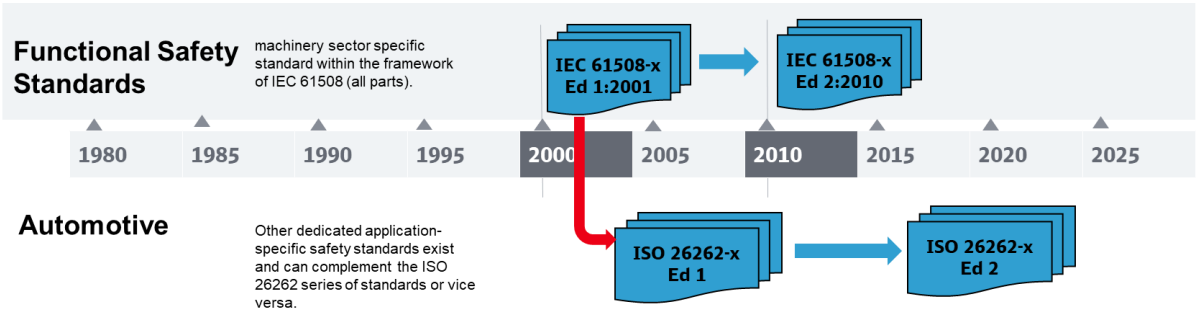

Figure 4 Automotive safety standards

ISO 26262–x - Road vehicles — Functional safety

Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

- Edition 1: 2011
- Edition 2: 2018

3.5 Aeronautics Industry

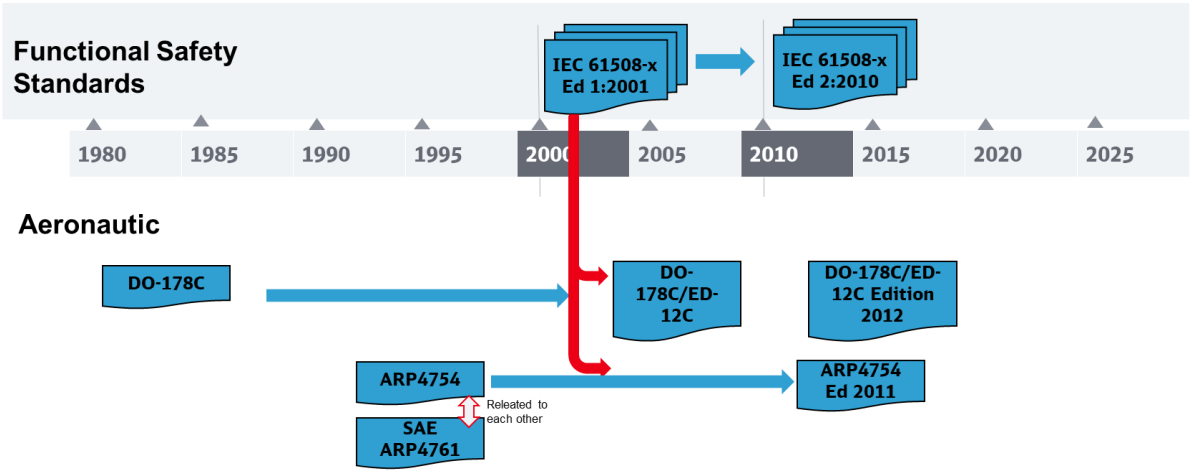

Figure 5 Aeronautics safety standards

DO-178C, Software Considerations in Airborne Systems and Equipment Certification
The **Software Level**, also known as:

- the **Design Assurance Level** (DAL); or
- **Item Development Assurance Level** (IDAL) as defined in ARP4754 (DO-178C only mentions IDAL as synonymous with Software Level),

is determined from the safety assessment process and hazard analysis by examining the effects of a failure condition in the system.

The failure conditions are categorized by their effects on the aircraft, crew, and passengers.

- **Level A - Catastrophic** - Failure may cause deaths, usually with loss of the airplane.
- **Level B - Hazardous** - Failure has a large negative impact on safety or performance or reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload or causes serious or fatal injuries among the passengers.
- **Level C - Major** - Failure significantly reduces the safety margin or significantly increases crew workload. May result in passenger discomfort (or even minor injuries).
- **Level D - Minor** - Failure slightly reduces the safety margin or slightly increases crew workload. Examples might include causing passenger inconvenience or a routine flight plan change.
- **Level E - No Effect** - Failure has no impact on safety, aircraft operation, or crew workload.

ARP4754, Aerospace Recommended Practice (ARP) ARP4754A (*Guidelines For Development Of Civil Aircraft and Systems*)

- a guideline from SAE International, dealing with the development processes which support certification of Aircraft systems, addressing "the complete aircraft development cycle, from systems requirements through systems verification."
- Revision A was released in December 2010. It was recognized by the FAA in AC 20-174 published November 2011. EUROCAE jointly issues the document as ED–79.

It is intended to be used in conjunction with **SAE ARP4761** supported by other aviation standards such as RTCA DO-178C/DO-178B and DO-254.

- This guideline addresses Functional Safety and design assurance processes.
- DAL allocation pertaining to functional failure conditions and hazard severity are assigned to help mitigate risks.
- Functional Hazard Analyses / Assessments are central to determining hazards and assigning DAL, in addition to requirements based testing and other verification methods.
- This guideline concerns itself with Physical (item) DAL and Functional (software/systems integration behavior) DAL and the Safety aspects of systems for the whole life-cycle for systems that implement aircraft functions.

3.6 Nuclear Industry

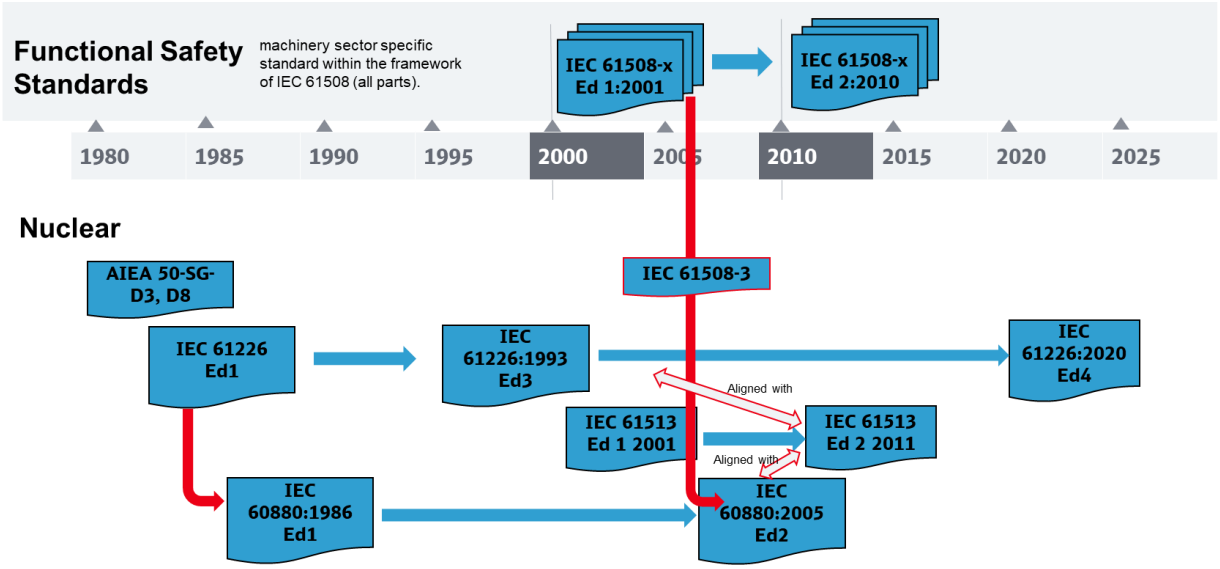

Figure 6 nuclear safety standards

IEC 61513
Certification practices

EN IEC 61226 - Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems
EN IEC 61226:2020

- a method of assignment of the functions specified for the plant into categories according to their importance to safety. Subsequent classification of the I&C and electrical power systems performing or supporting these functions, based on the assigned category, then determines relevant design criteria.
- The design criteria, when applied, ensure the achievement of each function in accordance to its importance to safety. In this document, the criteria are those of functionality, reliability, performance, environmental qualification (e.g. seismic) and quality assurance (QA).

This edition includes the following significant technical changes with respect to the previous edition:

- to align on IAEA requirements, recommendations and terminology, particularly to take into account the replacement of NS-R-1 by SSR 2/1 and publication of SSG 30.
- to extend the scope to electrical power systems.
- to move the detailed requirements applying to functions and I&C systems to a normative annex, which will be removed after updating EN IEC 61513.

EN IEC 61513 - Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
Instrumentation and control (I&C) systems important to safety may be implemented using conventional hard-wired equipment, computer-based (CB) equipment or by using a combination of both types of equipment. IEC 61513:2011 provides requirements and recommendations for the overall I&C architecture which may contain either or both technologies. The main technical changes with regard to the previous edition are as follows:
- alignment with the latest revisions of IAEA documents;
- alignment with new editions of **EN IEC 60880, EN IEC 61226, EN IEC 62138, EN IEC 62340 and EN IEC 60987**;
- alignment with significant advances of software engineering techniques;
- integration of requirements for staff training.

EN IEC 60880 - Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions

- This International Standard provides requirements for the software of computer-based I&C systems of nuclear power plants performing functions of safety category A as defined by EN IEC 61226.
- Provides requirements for the software of computer-based instrumentation and control (I&C) systems of nuclear power plants performing functions of safety category as defined by EN IEC 61226.
- Provides requirements for the purpose of achieving highly reliable software. Addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation.

Comparison between EN IEC 60880 and EN IEC 61508 for Certification Purposes in the Nuclear Domain

- In the nuclear domain, regulators have strict requirements for safety critical software.
- The nuclear domain software standard EN IEC 60880 provides requirements for the purpose of achieving highly reliable software.
- The standard is similar to the part 3 of EN IEC 61508 standard in the sense that it covers requirements for all software lifecycle activities.
- The Common Position document “Licensing of safety critical software for nuclear reactors” states the requirements from the perspective of European nuclear regulators.
- The use of EN IEC 60880 alone seems to be not sufficient for software certification.

3.7 FPGA for Nuclear and Railway Industries

From the experience of a manufacturer involved in both nuclear and railway sectors, the following conclusions can be drawn:

- The requirements on FPGA are similar between CENELEC EN 50129 for railway and EN IEC62566 for nuclear plants.
- The safety level Cat.A for function and class 1 for systems are equivalent to railway SIL level 4.
- For the software: both nuclear EN IEC 62566 and railway CENELEC EN 50128 (to be confirmed in the EN 50716 who will supersede the EN 50128) require the same development process and independence requirements.
- the manufacturer can develop the same combined testing protocol whatever the target industry for which its component will be used.

The notable difference between both sectors lies in the certification framework and the safety assessment. In nuclear industry the safety assessment is done by the Nuclear National Safety Authority, while in the EU railway industry, the safety assessment is performed by an independent safety assessor following EU regulation which can be different than the Railway National Safety Authority.

4 Conclusion and next steps

The first results from this cartography show that:

- The most relevant sectoral industries as source of non-railway components for OCORA are the Automation/Process, Aeronautics, Nuclear and Automotive industries
- As for the railway domain, the safety-related standards in use in different sectoral industries historically originate from the generic EN IEC 61508-x series.

In the coming years, a new version of the EN IEC 61508 will be drafted by the responsible committee, IEC TC 65 / SC 65A (Committee draft for all parts is foreseen for the 2nd quarter of 2022), this revision could be a perfect opportunity to better align the different industries with the standard.

Next steps:

- No comparison and projects have been made yet at the system integrator level. The next step could be to go deeper in the study at system level.
- In order to simplify the cross-acceptance of a product, system or process, comparison methods exist and are developed by manufacturers. We therefore envisage to have a deeper look at those methods
- Continue exchange with manufacturers and system integrators
- Consider the opportunity of the revision of EN IEC 61508 to align requirements and methods between sectors.

Annex 1: Product breakdown provided

This product breakdown shows, by CCS subsystem, the following elements:

- Cross sectorial opportunities: 0 (grey) or X whether we consider or not to introduce new safety related component from other industry.
- Identified technical or sectorial areas: list of already foreseen industries where railway companies can obtain supplies from.
- Related CCS interoperability constituent: precision if the CCS subsystem component is related to an interoperability constituent
- Supplier example: example of suppliers producing features that can fit with the railway industry

CCS Core/ Peripheral or external	*"CCS Subsystem Component"*	*Comment on PBS*	*Cross sectorial opportunities*	*identified technical or sectorial areas*	*related CCS interoperabilty constinuant (IC)*	*supplier example*	*comments*
CCS	**On-board CCS**	**overall on-board CCS including all elements below**					
CCS Core	**Core CCS**						
CCS Core	Core CCS - ATP (ETCS Core)	Suppose all ETCS funct.blocks (VS and other ATP related modules : STM-C,**ODO,** Mode mngt..) are running **on the same** dedicated HW Core CCS ATP is seen as a Software abstraction of the CCS Core	0		Train protection and odometry equipment (functional layer)		
CCS Coré	Computing platform	In case the Computing platform is the CCS core hardware abstraction. Safety critical (SIL-4), must comply with the safety requirements according to CENELEC EN 50126, EN 50128, EN 50129 and EN 50159	X	Aeronautics, nuclear, avionics, processing automation, petrochemical	Train protection and odometry equipment	- Wind River, Arcys(nuclear) - OCORA TWS03 (computing platform) has approached a number of companies. These should be referenced for BWS09.	Supports safety critical functions
CCS Core	CCS addon - NTC-STM	In case of embedded NTC-STM	0	Railway specific			example BI-standard architectures
CCS Core	CCS addon - ATO soft	Suppose ATO Vehicle software is running on a dedicated HW	0				We are considering ATO GOA 1-2 for the software part
CCS Core	CCS addon - ATO HW		X	Aeronautics, nuclear, avionics, processing automation, petrochemical	ATO OB IC is foreseen	- Wind River, Arcys(nuclear) - OCORA TWS03 (computing platform) has approached a number of companies. These should be referenced for BWS09.	ATO up to GoA4 is assumed here not to be SIL 4 , the driverless railway system is to be SIL4 - this has to be confirmed at a later stage. If ATO is assumed to be for GoA 1-2 then it

							should be non-SIL (SIL0) according to SubSet-125.
CCS Core	**CCS addon - other functions/services**	**All other functional blocks running on a dedicated HW (e.g. Digital Map)**					
CCS peripherals	**Communication and interfaces**						
CCS peripherals	STM		X example NS: STM ATB	E/E/PE (electronical / electronic / programable electronics) used in different domains	Train protection and odometry equipment	- Texas Instruments: Hercules. - Microchip: AVR & PIC - Synopsys: ARC EM - ST Microelectronics: STM8 & STM32 - NXP: MPC564 - Renesas: RX, RA	In the ATB example only one component / chip was procured, not the complete PCBA. Depending on the needed functions procurement of PCBA or computer could be possible.
CCS peripherals	I/O Ports		X	Instrumented systems for the process industry		- MEN/Duagon - Siemens automation - schneider Electric - Rockwell	INPUT and OUTPUT sil2
CCS peripherals	Functional Vehicle Adapter (FVA)	Logical adaptation to I/O (wired or serial TCMS)	0				The FVA might provide safety functions up to SIL2. This means that it has to run on an appropriate computing unit that could be used from other sectors.

CCS peripherals	CCN (CCS Communication network) ex UVCC	Only Bus specific access for EVC "as is"	0				the safety layer is foreseen to be a part of CCN , at a final stage CCN will be specified in IEC 61375. The CCN is not foreseen to be safety relevant - to be confirmed. Network components like cables, switches, routers could be used from many other sectors.
CCS peripherals	Gateway		0				assumingly no safety critical function supported
CCS peripherals	MCG (GSM-R, FRMCS…)		0		VRC / DRC		
CCS peripherals	SIM card		0				
CCS peripherals	**Sensoring**						
CCS peripherals	ETCS Sensoring (eg Odo, BTM, LTM)		0				
CCS peripherals	Train Loc (GNSS, Inertial…)	Vehicle Locator and its sensors	X	aeronautics, defense, industrial, aerospace	Train detection	- iXblue (Loc4Rail project) - iMAR Navigation not SIL - Swift Navigation - inertialsense - Analog Devices - Sensonor - TAMAGAWA SEIKI - Bosch Sensortech	

CCS peripherals	CCS addon-server storing critical data	ex digital Map server	X	aeronautics, defense, industrial, aerospace		Advanced storage server manufacturer	- Assumingly no safety critical function supported, to be confirmed. - When using a safety platform or processor the memory is already integrated and designed to suite the application.
CCS peripherals	Perception sensoring (other sensors)	E.g. perception devices	X	aeronautics, defense, industrial, aerospace		- Renesas - Security & Safety Things - Bosch: INTEOX - Pilz - Safety Camera Systems - and many others…	- Example: IP video …, automotive to be confirmed, Renault? - more details are needed the purpose of the perception system, otherwise the market too broad.
CCS peripherals	DMI		0	Rail sector			
CCS tools	**Tools**						
CCS tools	Testing tools (eg test bench, simulator)	For test and integration purpose (eg TCMS)	0				
CCS tools	Maintenance tools		0				
CCS tools	Training tools	For test and integration purpose (eg TCMS)	0				
RST	**Rolling Stock CCS related components**						
RST	TCMS		0				
RST	Time service on board		0				
RST	**recording device including JRU**		0				
RST	Train networks interfaced to CCS (eg ECN)		0				
RST	Specific STM network	E.g. Profibus	0				

RST	CCS related RST parts (bogies, cabinet…)	Including RST mechanical bodies to be adapted for CCS devices mounting	0				
RST	Other CCS related devices & sensors	RST devices interfacing CCS	0				