OCORA

Open CCS On-board Reference Architecture

Modular Safety – SRAC Management

Whitepaper

Document ID: OCORA-TWS07-030

Version: 2.01

Release: R1

Date: 02.12.2021

Revision history

Version	Change Description	Initial	Date of change
1.00	Inherited content from draft “Safety Strategy” version for OCORA Delta Release	PN	01.08.2021
1.01	Definition of the document structure based on the R1 template	PN	03.11.2021
1.02	Update according to member’s review. Complete all section	PN	16.11.2021
1.03	Update according to SRAC and Evolution members reviews	JB	17.11.2021
2.00	Official version for OCORA Release R1	JB	18.11.2021
2.01	Update following Christophe Cassir comments	JB	02.12.2021

Table of contents

Table of figures

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

[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-TWS07-010 – Modular Safety – Strategy

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

1 Introduction

1.1 Purpose of the document

The purpose of this document introduced by Modular Safety Strategy [7] is to describe the management of SRACs within OCORA compliant projects. SRAC is the abbreviation for Safety-related Application Condition.

SRACs establish the safety-related assumptions and conditions that need to be satisfied to mitigate risks when the system under consideration is integrated. The need for a standardized SRAC management within OCORA compliant programs comes from a common return of experience from railway undertakings. Although rules for SRAC writing already exist inside EN 50129 [66], a process design for SRAC management is still outstanding. The sharing of SRACs between different levels of safety cases usually induces misunderstandings due to a lack of communication between SRAC emitters and receivers which can, in the worst case, drive to an incorrect coverage and lead to a safety issue.

The correct definition, processing, and handling of SRACs is essential and a precondition for safe integration. Working with a predefined SRAC management processes is not mandatory, when the current SRAC management process inside the contracting entity (in charge of the overall OCORA compliant project) fully covers its expectations. However, harmonized SRAC management is highly recommended and is one of the key factors for bringing OCORA to success. In this context, OCORA Collaboration has decided to tackle this topic within this document. OCORA provides the opportunity to improve complex SRAC management thanks to its modular architecture. Besides, OCORA architecture needs several requirements to help simplifying the SRAC handling.

More precisely this document shall address the following key aspects of SRAC Management:

- OCORA SRAC management guideline *(*i.e. efficient dialogue and exchanges between SRAC emitters up to final SRAC implementers) (expected to be highly recommended for all OCORA compliant programs)
- OCORA Standardized SRAC list to be deployed on the interaction of different Building Blocks (BB) together and with the external world. These SRAC can be standardized because they will rely on fully defined interfaces (OCORA, ERTMS Subsets, CONNECTA and other European initiatives).
- OCORA Non-standardized SRACs definition rules for defining a framework in which non-standardized SRACs are allowed to be defined within OCORA (SRACs must not go against modularity)
- OCORA SRAC template with strictly defined rules for the documentation of SRACs (expected to be mandatory for all OCORA compliant programs)

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 Applicability of the document

The document is currently considered informative but may become a standard 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 the document

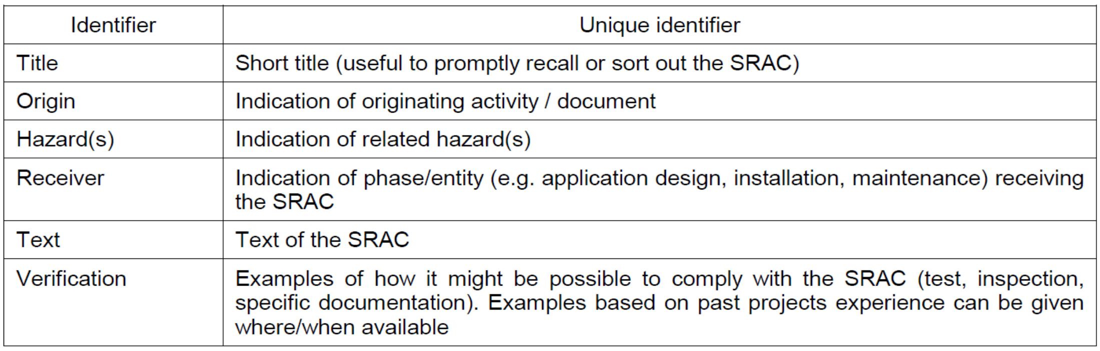
This document is published as part of the OCORA Release R1, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction 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 Pain points of current SRAC application regarding OCORA

In this section existing regulations, process descriptions and templates regarding the current management of SRACs are reviewed and compared with experiences from practice. The goal is to identify current pain points as well as missing or misunderstood information regarding current SRAC management, which must be addressed for SRAC Management within OCORA's modular approach.

2.1 Comparison and analysis of existing SRAC processes

Starting point of the analysis was the CENELEC regulation EN 50129 regarding "Safety related electronic systems for signalling". Here a generic definition of SRAC is given and high-level recommendations are defined (for example "SRACs shall be uniquely identifiable" or "Avoid declaring SRACs that could have been avoided through design"). Besides an exemplary categorization for SRACs an example for an SRAC template is given (refer to Figure 1). In general, the EN 50129 distinguishes between SASP ("specific application safety process"), GPSP ("general product safety process") and GASP ("general application safety process"). [64]



Identifier	Unique identifier
Title	Short title (useful to promptly recall or sort out the SRAC)
Origin	Indication of originating activity / document
Hazard(s)	Indication of related hazard(s)
Receiver	Indication of phase/entity (e.g. application design, installation, maintenance) receiving the SRAC
Text	Text of the SRAC
Verification	Examples of how it might be possible to comply with the SRAC (test, inspection, specific documentation). Examples based on past projects experience can be given where/when available

Figure 1 SRAC template example presented in EN 50129

As the SRAC information provided by the EN 50129 are presented in a high-level and generic way, several RU have their own guidelines and templates for handling with SRACs, which must be analysed in the context of this whitepaper. Up to now, the following input documents have been used for recording the status quo of SRAC management:

- CENELEC: EN 50129 - Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
- SBB: I-AT-SAZ Plattform Management – Prozessbeschreibung Anwendungsbedingungen V. 1.0
- SNCF: Extrait de la procédure de gestion des contraintes exportées NExTEO/ATS+] 03/12/2020
- NS: Summary SRAC-process for ERTMS between Railway Undertakings and Infra Manager

For comparing the SRAC information given by the EN 50129 and the specific guidelines of the RU, the information was grouped in the five categories presented in Table 1. The categories represent information regarding the Definition of SRACs, requirements/recommendations for correct SRAC application, involved roles and responsibilities as well as process descriptions, process flow charts or other templates regarding the definition or handling of SRACs.

Definition of SRACs	Requirements for SRAC application	Roles and responsibilities	SRAC processes	Templates

Table 1 Categorization of SRAC information contained in the reviewed documents

The results of the first analysis are shown in the figures in the Appendix of this whitepaper. In the next steps the main content must be consolidated and translated into recommendations and requirements for the handling with SRACS. A SRAC process flow chart must be generated where the process from SRAC emission to its final coverage with different intermediate steps can be defined in the context of OCORA.

2.2 Identification of pain points for OCORA’s modular approach

Main pain points of current SRAC management processes identified by OCORA team members:

- The SRAC doesn’t cover the full lifetime of a system. It happens that a project modifies a part of the system which is covered by a SRAC but the project is no more aware of that. The reason is that the SRAC had been emitted at the very beginning of the project and its coverage has been slightly modified release after release of documentation and at the end, the latest coverage does not fit anymore and hazardous activities (i.e. with critical safety impact) are realized by the project.
- Lack of interaction between SRAC emitters and receivers
- Lack of examples for mechanisms to be deployed to cover the SRAC:
- Insufficient definition of the context of an SRAC.
(required by EN 50129 but not sufficiently challenged by ISA)
- System hazards for SRACs are not clearly identified.
(required by EN 50129 but not sufficiently challenged by ISA)
- Misunderstandings while sharing SRAC between different levels of safety cases, which can, in the worst case, drive to an incorrect coverage and lead to a safety issue.
- No justification of the SRAC; in some cases, RU have to implement SRAC (e.g. for maintenance) without being aware of the expected coverage or the frequency of its realisation.

The last point is related to a general challenge regarding the inheritance and interlinking of SRACs from the ETCS on-board GPSC to the vehicle authorization (i.e. SASC). The example provided in Figure 2 is based on return of experience from manufacturers and contracting entities.

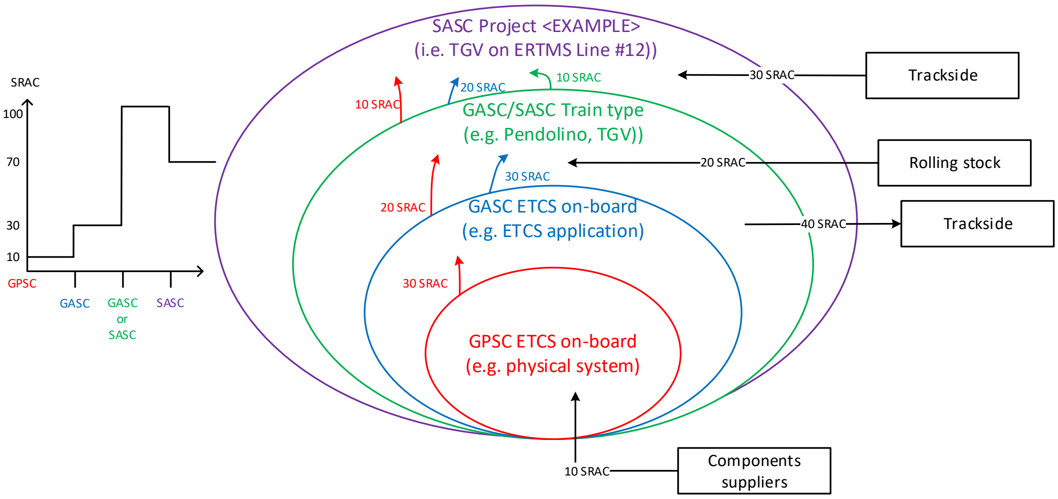


Figure 2: Inheritance of SRACs during integration processes

The SRAC flows presented in Figure 2 are addressed as follow:

- ***10 SRAC*** *coming from safety components used in the ETCS physical system (e.g. FPGA, microcontroller),*
- ***30 incoming SRAC*** *from ETCS physical system to ETCS on-board application (i.e. red circle on Figure 2),*

- *Train type GASC inherits* ***50 SRAC*** *from, both, GPSC (i.e. SRAC not coverable by the ETCS application) and GASC ETCS on-board. In addition, the train exports* ***40 SRAC*** *to the trackside (e.g. RBC, interlocking) (i.e. green circle on Figure 11),*
- *Finally, the final safety case, at vehicle authorization process shall cover* ***40 SRAC***

As presented above, the highest level of safety case uses to deal with very low level SRAC coming from the the ETCS on-board manufacturer (e.g. physical system). The gap between these two levels of engineering management uses to induce troubles when covering this kind of SRAC. Because of the high number of SRACs, their coverage requires a lot of time and resources in engineering and final vehicle authorization process with the assessor. Furthermore, due to the proprietary interfaces within the EVC, this coverage cannot be reused from one ETCS on-board supplier to another. The example provided in Figure 2 , based on existing safety cases from manufacturers and contracting entities, shows the interlinking of SRAC from the ETCS on-board GPSC to the vehicle authorization (i.e. SASC).

To conclude; with both the definition of complex SRAC by the downstream levels of safety cases and their quantity, the risk of wrong coverage of SRAC at the top-level project must be considered.

3 Recommendations for SRAC application within OCORA

Based on the identified pain points of current SRAC management, in this section, the OCORA collaboration provides general high-level recommendations for the application of SRACs within OCORA. The following list of recommendations is the result of a first brainstorming within the OCORA Modular Safety expert group. It will be consolidated, reviewed and expanded. Additional recommendations will be identified after finishing the OCORA architecture design.

The following list of recommendations is elaborated by the OCORA Modular Safety workgroup:

- Deploy interaction between SRAC emitters and receivers as much as possible. Try to involve the future receivers of SRAC into the development loop to start "training" them on the required coverage from the beginning
- Provide typical coverage examples suitable for each SRAC. The emitter should be able to provide examples of mechanisms to be deployed to cover the SRAC (e.g. “verification” field on Figure 1). This should help the receiver at defining its own coverage.
- Clearly identify the system hazard for each SRAC. It is required in EN 50129 but notnot sufficiently challenged by ISA. A complete description shall be provided.
- OCORA must define hazards that are 100% coverable at BB level (i.e. reuse data from Subset-091) to avoid SRAC emission because of non-fitted hazards to the system under consideration.
- OCORA must define a standard list of SRAC to be deployed on the interaction of different Building Blocks (BB) together and with outside onboard CCS scope. These SRAC can be standard because they will rely on fully defined interfaces (OCORA, Subset, CONNECTA and other European initiatives).
- Avoid SRAC linked to "design" choice. This refers to SRAC raised to limit the complexity of safety mechanisms at product level and report it to upper ones. Among others, it concerns safety testing activities (e.g. periodic safety preventive maintenance) that shall be handled by the receiver's maintenance team instead of being intrinsically present in the product’s design. This kind of SRAC are usually agreed between the emitter and the receiver.
- Define a generic definition of a SRAC so that everyone has the same understanding.
- Only one topic per SRAC
- Well-defined SRAC (well described complete contextual information and addressed to a contextual recipient that does exist (SMART))
- Only forward SRACS that are worth forwarding (prevent from forwarding information, which is state of the art or ensured by resp. applied due to common measures or standards)
- They shall have a clear Safety-related context; they are used to protect from or mitigate hazards that would arise, if the SRAC would not exist (e.g. SRACS shall not forward RAM-related or general information of system characteristics)
- A SRAC, which is forwarded shall be feasible to be realized for the receiver (no SRACs that are impossible or unreasonable to apply)
- SRAC must be justified; SRAC receiver shall get all the necessary information to understand why it must be implemented, at which frequency the coverage mean shall be active etc. This information shall be provided by the SRAC emitter.

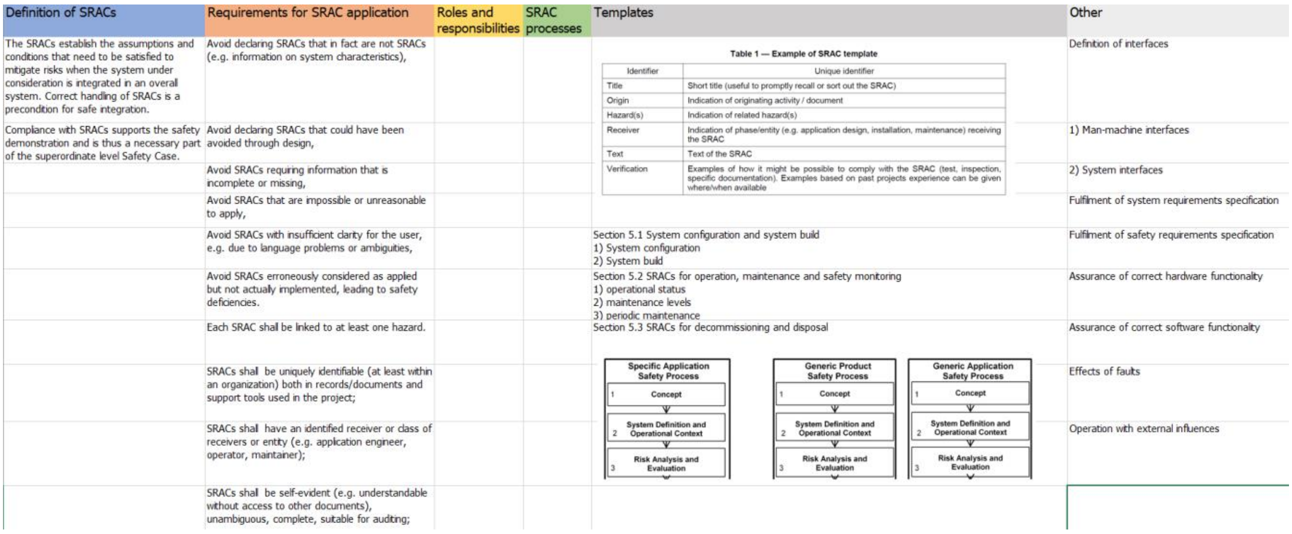
4 Intended future SRAC management within OCORA

4.1 Planned OCORA deliverables

- OCORA SRAC definition
- OCORA SRAC process guideline
- OCORA Standardized SRAC list
- OCORA Non-standardized SRACs definition rules
- OCORA SRAC template

5 Appendix

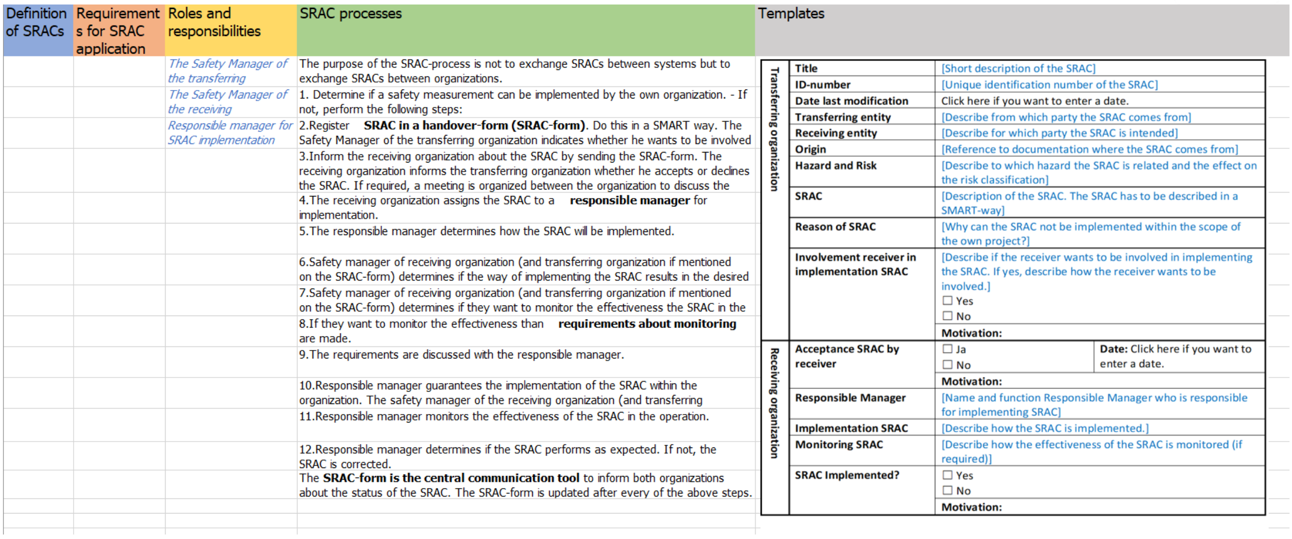
5.1 Extracts of SRAC management documents



Definition of SRACs	Requirements for SRAC application	Roles and responsibilities	SRAC processes	Templates	Other
The SRACs establish the assumptions and conditions that need to be satisfied to mitigate risks when the system under consideration is integrated in an overall system. Correct handling of SRACs is a precondition for safe integration.	Avoid declaring SRACs that in fact are not SRACs (e.g. information on system characteristics),			**Table 1 — Example of SRAC template** Identifier: Unique identifier Title: Short title (useful to promptly recall or sort out the SRAC) Origin: Indication of originating activity / document Hazard(s): Indication of related hazard(s) Receiver: Indication of phase/entity (e.g. application design, installation, maintenance) receiving the SRAC Text: Text of the SRAC Verification: Examples of how it might be possible to comply with the SRAC (test, inspection, specific documentation). Examples based on past projects experience can be given where/when available	Definition of interfaces
Compliance with SRACs supports the safety demonstration and is thus a necessary part of the superordinate level Safety Case.	Avoid declaring SRACs that could have been avoided through design,				1) Man-machine interfaces
	Avoid SRACs requiring information that is incomplete or missing,				2) System interfaces
	Avoid SRACs that are impossible or unreasonable to apply,				Fulfilment of system requirements specification
	Avoid SRACs with insufficient clarity for the user, e.g. due to language problems or ambiguities,			Section 5.1 System configuration and system build 1) System configuration 2) System build	Fulfilment of safety requirements specification
	Avoid SRACs erroneously considered as applied but not actually implemented, leading to safety deficiencies.			Section 5.2 SRACs for operation, maintenance and safety monitoring 1) operational status 2) maintenance levels 3) periodic maintenance	Assurance of correct hardware functionality
	Each SRAC shall be linked to at least one hazard.			Section 5.3 SRACs for decommissioning and disposal	Assurance of correct software functionality
	SRACs shall be uniquely identifiable (at least within an organization) both in records/documents and support tools used in the project;				Effects of faults
	SRACs shall have an identified receiver or class of receivers or entity (e.g. application engineer, operator, maintainer);				Operation with external influences
	SRACs shall be self-evident (e.g. understandable without access to other documents), unambiguous, complete, suitable for auditing;				

Specific Application Safety Process
1 Concept
2 System Definition and Operational Context
3 Risk Analysis and Evaluation
Generic Product Safety Process
1 Concept
2 System Definition and Operational Context
3 Risk Analysis and Evaluation
Generic Application Safety Process
1 Concept
2 System Definition and Operational Context
3 Risk Analysis and Evaluation

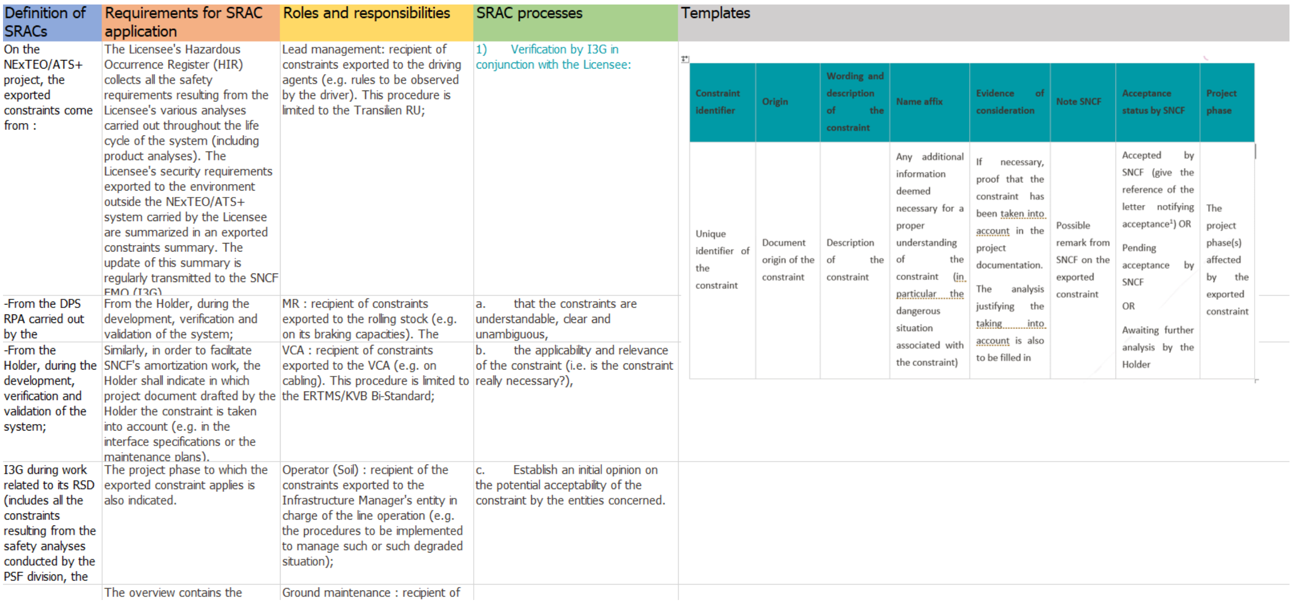
Figure 3: Extract of SRAC information within CENELEC EN 50129



Definition of SRACs	Requirements for SRAC application	Roles and responsibilities	SRAC processes	Templates
		The Safety Manager of the transferring	The purpose of the SRAC-process is not to exchange SRACs between systems but to exchange SRACs between organizations.	
		The Safety Manager of the receiving	1. Determine if a safety measurement can be implemented by the own organization. - If not, perform the following steps:	
		Responsible manager for SRAC implementation	2.Register **SRAC in a handover-form (SRAC-form)**. Do this in a SMART way. The Safety Manager of the transferring organization indicates whether he wants to be involved	
			3.Inform the receiving organization about the SRAC by sending the SRAC-form. The receiving organization informs the transferring organization whether he accepts or declines the SRAC. If required, a meeting is organized between the organization to discuss the	
			4.The receiving organization assigns the SRAC to a **responsible manager** for implementation.	
			5.The responsible manager determines how the SRAC will be implemented.	
			6.Safety manager of receiving organization (and transferring organization if mentioned on the SRAC-form) determines if the way of implementing the SRAC results in the desired	
			7.Safety manager of receiving organization (and transferring organization if mentioned on the SRAC-form) determines if they want to monitor the effectiveness the SRAC in the	
			8.If they want to monitor the effectiveness than **requirements about monitoring** are made.	
			9.The requirements are discussed with the responsible manager.	
			10.Responsible manager guarantees the implementation of the SRAC within the organization. The safety manager of the receiving organization (and transferring	
			11.Responsible manager monitors the effectiveness of the SRAC in the operation.	
			12.Responsible manager determines if the SRAC performs as expected. If not, the SRAC is corrected.	
			The **SRAC-form is the central communication tool** to inform both organizations about the status of the SRAC. The SRAC-form is updated after every of the above steps.	

Transferring organization	**Title**	[Short description of the SRAC]	
	ID-number	[Unique identification number of the SRAC]	
	Date last modification	Click here if you want to enter a date.	
	Transferring entity	[Describe from which party the SRAC comes from]	
	Receiving entity	[Describe for which party the SRAC is intended]	
	Origin	[Reference to documentation where the SRAC comes from]	
	Hazard and Risk	[Describe to which hazard the SRAC is related and the effect on the risk classification]	
	SRAC	[Description of the SRAC. The SRAC has to be described in a SMART-way]	
	Reason of SRAC	[Why can the SRAC not be implemented within the scope of the own project?]	
	Involvement receiver in implementation SRAC	[Describe if the receiver wants to be involved in implementing the SRAC. If yes, describe how the receiver wants to be involved.] ☐ Yes ☐ No	
		Motivation:	
Receiving organization	**Acceptance SRAC by receiver**	☐ Ja ☐ No	**Date:** Click here if you want to enter a date.
		Motivation:	
	Responsible Manager	[Name and function Responsible Manager who is responsible for implementing SRAC]	
	Implementation SRAC	[Describe how the SRAC is implemented.]	
	Monitoring SRAC	[Describe how the effectiveness of the SRAC is monitored (if required)]	
	SRAC Implemented?	☐ Yes ☐ No	
		Motivation:	

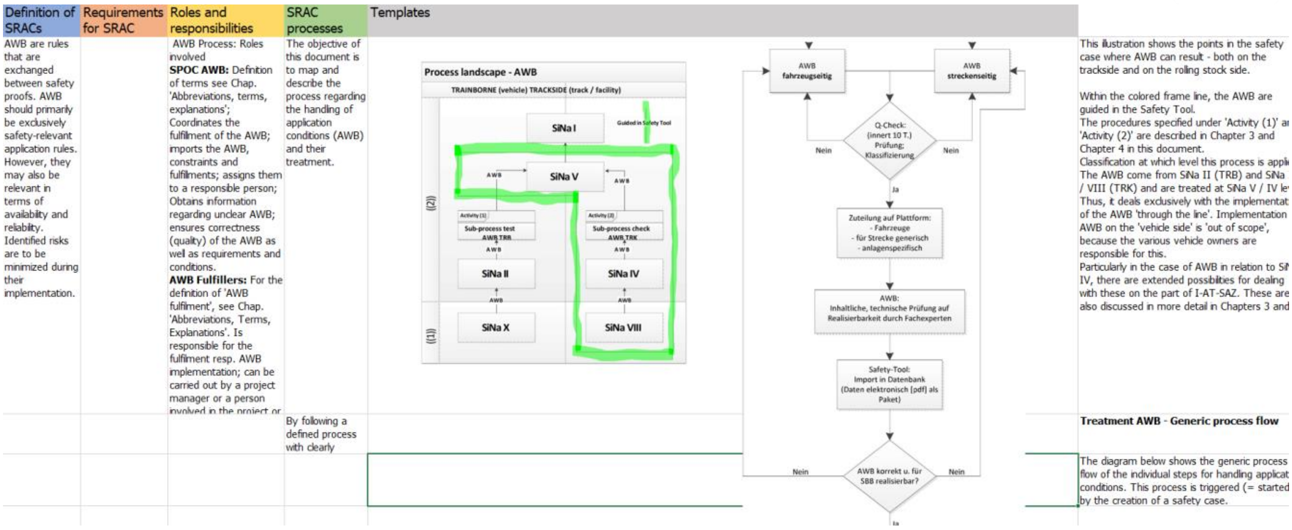
Figure 4: Extract of NS SRAC management documents



Definition of SRACs	Requirements for SRAC application	Roles and responsibilities	SRAC processes	Templates
On the NExTEO/ATS+ project, the exported constraints come from :	The Licensee's Hazardous Occurrence Register (HIR) collects all the safety requirements resulting from the Licensee's various analyses carried out throughout the life cycle of the system (including product analyses). The Licensee's security requirements exported to the environment outside the NExTEO/ATS+ system carried by the Licensee are summarized in an exported constraints summary. The update of this summary is regularly transmitted to the SNCF FMO (I3G)	Lead management: recipient of constraints exported to the driving agents (e.g. rules to be observed by the driver). This procedure is limited to the Transilien RU;	1) Verification by I3G in conjunction with the Licensee:	
-From the DPS RPA carried out by the	From the Holder, during the development, verification and validation of the system;	MR : recipient of constraints exported to the rolling stock (e.g. on its braking capacities). The	a. that the constraints are understandable, clear and unambiguous,	
-From the Holder, during the development, verification and validation of the system;	Similarly, in order to facilitate SNCF's amortization work, the Holder shall indicate in which project document drafted by the Holder the constraint is taken into account (e.g. in the interface specifications or the maintenance plans).	VCA : recipient of constraints exported to the VCA (e.g. on cabling). This procedure is limited to the ERTMS/KVB Bi-Standard;	b. the applicability and relevance of the constraint (i.e. is the constraint really necessary?),	
I3G during work related to its RSD (includes all the constraints resulting from the safety analyses conducted by the PSF division, the	The project phase to which the exported constraint applies is also indicated.	Operator (Soil) : recipient of the constraints exported to the Infrastructure Manager's entity in charge of the line operation (e.g. the procedures to be implemented to manage such or such degraded situation);	c. Establish an initial opinion on the potential acceptability of the constraint by the entities concerned.	
	The overview contains the	Ground maintenance : recipient of		

Constraint identifier	Origin	Wording and description of the constraint	Name affix	Evidence of consideration	Note SNCF	Acceptance status by SNCF	Project phase
Unique identifier of the constraint	Document origin of the constraint	Description of the constraint	Any additional information deemed necessary for a proper understanding of the constraint (in particular the dangerous situation associated with the constraint)	If necessary, proof that the constraint has been taken into account in the project documentation. The analysis justifying the taking into account is also to be filled in	Possible remark from SNCF on the exported constraint	Accepted by SNCF (give the reference of the letter notifying acceptance[1]) OR Pending acceptance by SNCF OR Awaiting further analysis by the Holder	The project phase(s) affected by the exported constraint

Figure 5: Extract of SNCF SRAC management documents



Definition of SRACs	Requirements for SRAC	Roles and responsibilities	SRAC processes	Templates	
AWB are rules that are exchanged between safety proofs. AWB should primarily be exclusively safety-relevant application rules. However, they may also be relevant in terms of availability and reliabilty. Identified risks are to be minimized during their implementation.		AWB Process: Roles involved **SPOC AWB:** Definition of terms see Chap. 'Abbreviations, terms, explanations'; Coordinates the fulfilment of the AWB; imports the AWB, constraints and fulfilments; assigns them to a responsible person; Obtains information regarding unclear AWB; ensures correctness (quality) of the AWB as well as requirements and conditions. **AWB Fulfillers:** For the definition of 'AWB fulfilment', see Chap. 'Abbreviations, Terms, Explanations'. Is responsible for the fulfiment resp. AWB implementation; can be carried out by a project manager or a person involved in the project or	The objective of this document is to map and describe the process regarding the handling of application conditions (AWB) and their treatment.		This illustration shows the points in the safety case where AWB can result - both on the trackside and on the rolling stock side. Within the colored frame line, the AWB are guided in the Safety Tool. The procedures specified under 'Activity (1)' ar 'Activity (2)' are described in Chapter 3 and Chapter 4 in this document. Classification at which level this process is appli The AWB come from SiNa II (TRB) and SiNa / VIII (TRK) and are treated at SiNa V / IV le Thus, it deals exclusively with the implementat of the AWB 'through the line'. Implementation AWB on the 'vehicle side' is 'out of scope', because the various vehicle owners are responsible for this. Particularly in the case of AWB in relation to SiN IV, there are extended possibilities for dealing with these on the part of I-AT-SAZ. These are also discussed in more detail in Chapters 3 and
			By following a defined process with clearly		**Treatment AWB - Generic process flow**
					The diagram below shows the generic process flow of the individual steps for handling applicat conditions. This process is triggered (= started by the creation of a safety case.

Process landscape - AWB
TRAINBORNE (vehicle) TRACKSIDE (track / facility)
SiNa I
Guided in Safety Tool
SiNa V
AWB
AWB
Activity (1)
Sub-process test AWB TRB
Activity (2)
Sub-process check AWB TRK
AWB
AWB
SiNa II
SiNa IV
AWB
AWB
SiNa X
SiNa VIII
((2))
((1))
AWB fahrzeugseitig
AWB streckenseitig
Q-Check: (innert 10 T.) Prüfung; Klassifizierung
Nein
Nein
Ja
Zuteilung auf Plattform: - Fahrzeuge - für Strecke generisch - anlagenspezifisch
AWB: Inhaltliche, technische Prüfung auf Realisierbarkeit durch Fachexperten
Safety-Tool: Import in Datenbank (Daten elektronisch [pdf] als Paket)
AWB korrekt u. für SBB realisierbar?
Nein
Nein
Ja

Figure 6: Extract of SBB SRAC management documents