Deliverable D 2.3
Case study requirements and specification

Project acronym:	4SECURail
Starting date:	01/12/2019
Duration (in months):	24
Call (part) identifier:	H2020-S2R-OC-IP2-2019-01
Grant agreement no:	881775
Due date of deliverable:	Month 12 (November 2020)
Actual submission date:	25-11-2020
Responsible/Author:	SIRTI / Andrea Piattino
Dissemination level:	PU
Status:	Issued

Reviewed: yes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 881775.

Document history		
Revision	*Date*	*Description*
0.0	30/03/2020	Template creation and Executive Summary
0.1	02/04/2020	First issue
0.2	28/04/2020	Background and Aim, Rationale, Requirements definition
0.3	06/07/2020	Enumerated requirements
0.4	22/07/2020	SUBSET-039 and SUBSET-098 requirements tracking
0.5	05/08/2020	Sect. 10 and Sect. 11 and Annex moved to external excel table
0.6	15/09/2020	Application Layer renamed as Communication Supervision Layer
0.7	29/10/2020	General revision of the wording Chapters Set-Up and Safety moved under chapter 6 Sect. 07 updated with requirements Mapping of requirements on SS-039 and SS-098
0.8	10/11/2020	General revision of the wording Section 6.2 removed Update of Sections 1 and 8
1.0	25/11/2020	Issue for submission

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Andrea Piattino	SIRTI	ToC, Executive Summary, Rationale, Methodology, System Requirements Specifications, Aim and Background
Franco Mazzanti Davide Basile Stefania Gnesi	CNR	Comments on structure and content
Albert Ferrer-Bonsoms	ARD	Internal review
Carlo Vaghi Elisa Sivori	FIT	Internal review

Table of Contents

1 Executive Summary

Workstream 1 of 4SECURail project addresses the topic of the Open Call IP2 S2R-OC-IP2-01-2019 of the Shift2Rail initiative, related to the *Demonstrator development for the use of Formal Methods in railway environment*. Specifically, the project contributes to the objective of the Technical Demonstrator TD2.7 of the MAAP - Formal methods and standardisation for smart signalling systems, to use formal methods in development of railway signalling systems to increase market competition and standardization and to improve interoperability and reliability.

The main objective of WP2 in 4SECURail is to propose a demonstrator of state-of-the-art formal methods to evaluate the learning curve and to perform a cost/benefit analysis of the adoption of Formal Methods in railway industry, with a special focus to the point of view of the railway infrastructure managers, for the uptake of Formal Methods on system requirements definition.
This document is the result of the activities carried out within the 4SECURail Task 2.2, which aims to address one of the objectives of WP2: *identify and describe, using standard interfaces, the railway signalling subsystem intended to exercise the demonstrator prototype of formal methods*. A detailed description of the process and framework constituting the demonstrator prototype will be released in D2.2.

The subsystem identified to exercise the formal methods demonstrator is the RBC/RBC handover interface, as specified by UNISIG into SUBSET-039 - FIS for the RBC/RBC Handover [1] and SUBSET-098 - RBC/RBC Safe Communication Interface [2].

The RBC/RBC case study is based on an already existing and standardized interface, which is however specified in “natural language”. By exercising the formal methods demonstrator, the goal is to provide an even more efficient requirements definition with an augmented usability of the standardized interface, significantly reducing development problems related to residual uncertainties, like missing requirements and not yet detected ambiguities or contradictions. This means an improved interoperability of different implementations, with reduced risk of producing diverging architectures and simplification of the development process.

The choice of the RBC/RBC case study has been supported by a SWOT analysis, which has highlighted the appropriateness of the RBC/RBC case for the validation of the formal methods demonstrator. As underlined in the analysis, RBC/RBC interface relies on public and harmonised requirements that can be a consolidated reference for our study. Although the interface might be complex and its evaluation with Formal Methods might be challenging within the limited duration of 4SECURail, this risk is however manageable, considering that the harmonised specifications already subdivide the interface into a safety layer and a communication layer, permitting the identification of a kernel functionality, sufficient for a significant estimation of Formal Methods advantages. Finally, the RBC/RBC interface is an important example of products from different suppliers that need to communicate within an infrastructure railway system.

A careful review of requirements has been made in Task 2.2, centring the work on the higher application levels and the safety levels of the architecture, in order to have functional interface requirements ready to be handled by Task 2.1 to produce a formal definition of the subsystem. In

particular, a specific Communication Supervision Layer has been introduced to isolate only the needed communication requirements and to be independent from the complete RBC functionalities. The definition of the subsystem will contribute to the identification of the hazards and the clarification of safety requirements by reference to standard EN50159 [3].

The validation activity that will be performed on the RBC/RBC subsystem will provide the necessary inputs for the release of the final version of the demonstrator prototype (D2.5).

2 Abbreviations and acronyms

Abbreviation / Acronyms	Description
CBA	Cost Benefit Analysis
CSL	Communication Supervision Layer
EC	Execution Cycle
ER	EuroRadio
ERTMS	European Rail Traffic Management System
FM	Formal Methods
IM	Infrastructure Manager
MA	Movement Authority
MAAP	Multi-Annual Action Plan (Shift2Rail)
MBSD	Model Based System Design
NL	Non-leading (ERTMS Mode)
NRBC	Neighbour RBC
RBC	Radio Block Centre
SAI	Safe Application Intermediate sub-Layer
SIL	Safety Integrity Level
SFM	Safe Functional Module
SWOT	Strengths Weaknesses Opportunities and Threats
TD	Technical Demonstrator
TSI	Technical Specification for Interoperability
TTS	Triple Time Stamp

3 Background

The present document constitutes the Deliverable D2.3 “Case study requirements and specification” in the framework of Task 2.2 (Requirements definition of a railway signalling subsystem) of the WP2 (Demonstrator Development for the use of Formal Methods in Railway Environment) of 4SECURail project - IP2 S2R-OC-IP2-01-2019 of the Shift2Rail initiative. This activity is linked with the TD2.7 of the MAAP - *Formal methods and standardisation for smart signalling systems* (14/11/2019) [4]. Activities of WP2 are in line with the following technical objectives of TD2.7:

1. Demonstrate state-of-the-art formal methods for specification of requirements
2. Demonstrate improvements to high-level specification thanks to the use of semi-formal languages
3. Demonstrate formal verification of safety requirements to achieve significant reduction of effort and cost compared to traditional safety assessment

As stated in TD2.7, common interfaces are key to increase competition and to enable more efficient use of Formal Methods to reduce cost and time in development, approval and commissioning of signalling systems.
For our purposes, the project scenario considers the Infrastructure Managers (IMs) applying formal and semi-formal methods to build robust and verifiable specifications of system requirements, which will make the procurement of systems and equipment - compliant with legal requirements and needs of operators - possible and suitable for easy integration in the existing railway subsystems. This will contribute to moving towards an open market for maintenance (availability of spare parts) and future enhancements (implementation of new functions and/or performance exploiting open and possibly standardised interfaces). The introduction of Formal Methods in the process of specifying requirements carries the advantage to reduce any possible ambiguity in the requirements definition; this could even introduce some benefits about the uniformity of products architectures and about procurement and maintenance costs.
The idea of IMs is to have modular systems parts and to define standardised interfaces to integrate these modules together (this approach is supported by the Eulynx initiative [5]). In this context of modular systems, the use of Formal Methods is a solid support to the definition of more efficient interfaces and evaluate safety in this specific scenario of a heterogeneous distributed system.

4 Objective/Aim

One of the objectives of 4SECURail project is to evaluate a cost-benefit analysis for the adoption of Formal Methods (FM) in the railway environment, through prototyping a formal method demonstrator to be exercised with a selected case study.

The aim of this document is to define the requirements and specification of a railway case study, the RBC/RBC interface, on which to apply the formal demonstrator prototype (defined in Task 2.1) and evaluate the cost-benefit analysis, compared with a similar process based on "traditional" methodologies of its application.

The RBC/RBC interface definition is aligned with the objectives of TD2.7 of the Shift2Rail MAAP, which focus on applying Formal Methods and Standard Interfaces in application demonstrators and the business case study for using them.

A rationale for the choice of the RBC/RBC interface case study is proposed in the next section.

The ETCS specifications for RBC/RBC interface specify requirements relevant for interoperability. This deliverable integrates the ETCS specifications contained in SUBSET-039 – FIS for the RBC/RBC Handover [1] and SUBSET-098 – RBC/RBC Safe Communication Interface [2] with additional requirements also taking into account the ISO-OSI model, in order to make it possible to realize a feasible case study of the above mentioned protocol by creating a formal specification of the interface. The adapted definition of the subsystem is limited to higher application levels and safety levels (SAI sub-level of SUBSET-098) and will contribute to the identification of the hazards and the clarification of safety requirements by reference to standard EN50159 [3].

5 The RBC/RBC interface case study rationale

The case study to test the FM demonstrator proposed by 4SECURail is the RBC/RBC handover protocol, as specified by UNISIG into SUBSET-039 - FIS for the RBC/RBC Handover [1] and SUBSET-098 - RBC/RBC Safe Communication Interface [2].
A Handover procedure is needed to manage the interchange of train control supervision between two neighbouring RBCs. When a train is approaching the end of the area supervised by one handing over RBC, an exchange of information with the (new) accepting RBC takes place to manage the transaction of responsibilities (Figure 1).
The interface specified in SUBSET-039 [1] has the goal to enable any pair of neighbouring RBCs, compliant with it, to be interconnected, so that RBC/RBC handovers can be performed independently of the functional characteristics, service performance and safety architecture of the concerned RBCs.

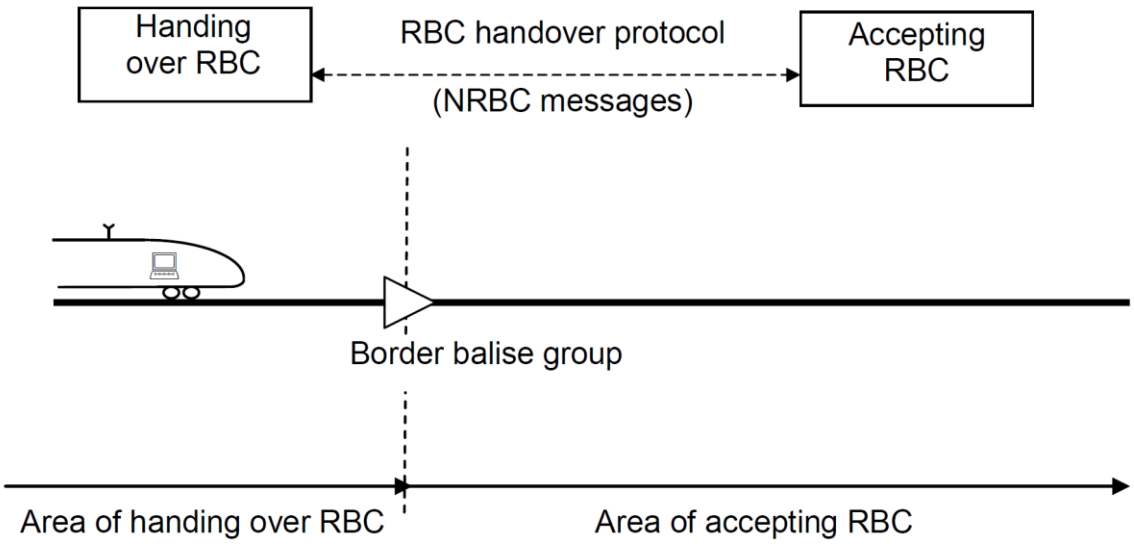

Figure 1 - The RBC/RBC Handover (*source*: SUBSET-039 [1])

This section provides a justification for the choice of RBC/RBC interface as “case study” for the evaluation of a FM demonstrator dedicated to prove feasibility and advantages of this development technique for the development of railway systems and products, with the final objective of performing a cost-benefit analysis against traditional development techniques.

The following guidelines will be considered:

1. Showing compliance of the choice of RBC/RBC interface with the project objectives and the expected results. This will be evaluated through:
   a) Clear declarations of project objectives and expected results;

b) Identification of the "Baseline Scenario" (current development process) for comparison of methodologies and the Cost Benefit Analysis (CBA);

2. Showing advantages deriving from this choice, compared with other possible approaches, according to SWOT methodology. The advantages will be evaluated according to the following criteria:
   a) Level of confidence that the choice is suitable for 4SECURail to achieve the expected results, minimising the risk of project failure. Strengths and Weaknesses considerations will be the basis for this estimation;
   b) Level of confidence that the choice is optimal for the market uptake, inducing positive impact on different aspects of railway system development. Opportunities and Threats criteria will be the basis for this estimation.

It is important to note that SWOT analysis is used in this section of the document only to prove suitability of the choice of RBC/RBC interface as case study for 4SECURail activities, not as a method to prove advantages/disadvantages of FM with respect to "traditional" methods, that will be investigated in the "CBA" part of 4SECURail project (deliverable D2.4 - Specification of cost/benefit analysis and learning curves, 1st release).

5.1 Objectives and expected results

The scope of 4SECURail is not the development of a product but showing the evidence that the use of FM brings advantages with respect to "traditional" processes, identifying such advantages and providing a measure thereof. Precisely, the main objective of WP2 is to propose a demonstrator of state-of-the-art FM to evaluate the learning curve and to perform a cost/benefit analysis of the adoption of FM in the railway industry.
Our selected case study, the RBC/RBC handover interface, contributes to fulfil the second objective of WP2, O2.2: *to identify and describe, using standard interfaces, the railway signalling subsystems to be used as test cases, and exercise with them the formal methods demonstrator*.

The comparison between the use of FM and traditional processes will focus basically on an overall estimation of time to market, taking into consideration that this is strongly dependent on:

- "Linearity" of development process, avoiding recursive steps, due to late detection of errors or unclear initial requirements;
- Simplification of the V&V and certification process, through better structure of documentation and generation of specifications and test reports;
- Improvement of product quality (reduced negative feedback from experience), through formal verification of safety and reliability related properties;
- Possibility of early identification of missing or unclear requirements, possibly leading to inconsistent product development by different suppliers, with compatibility and interoperability issues after installation.

RBC/RBC interface is a typical product where development processes of different supplier meet, and is therefore an optimal choice to investigate how natural language specification may create the possibility of diverging interpretations, leading to interoperability issues.

The fact that RBC/RBC interface already supports well established railway operations offers good opportunities for the elicitation of requirements, especially safety related ones, which can be translated into formally verifiable properties.
The fact that RBC/RBC interface is based on harmonised requirements and is explicitly finalised to connect systems from different suppliers offers a reference case for the estimation of FM advantages that is more significant, and also more accessible for evaluation, than the ones that could be offered by other interfaces (e.g. interface between Interlocking and field objects), the implementation of which is usually proprietary.

5.2 Baseline scenario

The "baseline scenario" is defined as the usual scenario performed by an IM. In the baseline scenario:

- the IM produces system specifications for procurement in the form of documents written in natural language
- suppliers develop systems and products on the basis of these specifications in a traditional way, i.e. without using Model Based Software Development MBSD ("semi"-formal methods) tools and FM.

The baseline scenario is the necessary benchmark situation to be compared with the "project demonstrator scenario", in which:

- system specifications are formalized by IMs using MBSD and FM;
- suppliers use MBSD and FM to assess that their work is compliant with the specifications issued by IMs, taking advantage of the work already done by IMs when formalizing the specifications.

The development phase performed by suppliers is out of the demonstrator scope.
A more detailed description of the "baseline" and the "project" scenario, and its elements relevant as input for the Cost-Benefit analysis, will be given in D2.4 - Specification of cost/benefit analysis and learning curves, 1st release.

5.3 SWOT Analysis

This section provides a SWOT analysis to evaluate the appropriateness of the choice of the RBC/RBC case study for the validation of the FM demonstrator (D2.5 - Formal development demonstrator prototype, final release, D2.6 - Specification of cost/benefit analysis and learning curves, final release).
By performing this kind of analysis, difficulties and risks for the project as well as the possible market uptake have been considered.

5.3.1 Strengths-Weaknesses

Considering difficulties and risks for project, i.e. probability of achieving the expected results and how these results can effectively be applied for future improvements of system and product development methodologies, it can be shown that RBC/RBC interface satisfies these criteria and

is possibly better than alternative choices.

5.3.1.1 Strengths

- RBC/RBC relies on public and harmonised requirements that can be a consolidated reference for analysis.
- The system where RBC/RBC interface is applied is now well known and operational experience exists.
- Compared with other interfaces that may be strongly dependent on implementation strategies of suppliers (e.g. safety architecture solutions), for RBC/RBC interface and its use in operational railway systems there are requirements which are harmonised and not supplier-dependent.

5.3.1.2 Weaknesses

- The RBC/RBC interface might be complex and its evaluation with FM might be challenging within the limited duration of 4SECURail.
- This project risk is however manageable, considering that the harmonised specifications already subdivide the interface into a safety layer and a communication layer. This should permit the identification of a kernel functionality, sufficient for a significant estimation of FM advantages, without mandating unrealistic amounts of work.

5.3.2 Opportunities-Threats

Considering the market uptake of project results, i.e. in which extent the improvement of development methodologies fostered by 4SECURail may positively impact railway systems deployment, it is shown that RBC/RBC interface satisfies these criteria and is possibly better than alternative choices.

5.3.2.1 Opportunities

- RBC/RBC is an important example of products from different suppliers that need to communicate within an infrastructure railway system.
- Strengthening the current specifications and using them as a basis for future efficient approach to product and system development will bring important improvements to the rail system, facilitating future specification of products and interfaces.
- This is also ensured by the compliance of 4SECURail with Eulynx initiative approach.
- Compared with other interfaces, the RBC/RBC interface, being already harmonised at the level of requirements, is an area where limits due to specificities and even confidentiality clauses of suppliers' solutions play a minor role.
- For the same reason it may be expected that resistance to acceptance of 4SECURail outcome will probably be lower.

5.3.2.2 Threats

- Some suppliers have already developed their solutions for the RBC/RBC interface, and therefore 4SECURail outcome could be of little interest for them.
- This threat exists, however, unchanged for all other possible choices, for which it may also be worse, because an outcome related to a not fully harmonised set of functional requirements is even more difficult to accept than an outcome related to specifications that are mandated in a Technical Specification for Interoperability (TSI) [6].
- It must also be taken into account that the object of 4SECURail is not the "product RBC/RBC interface", but the development methodology and cost-benefit analysis.
- This potential weakness will be managed therefore by 4SECURail ensuring that tools, methods, assumptions etc. will be as general as possible and not explicitly linked to the selected case study.

6 Methodology

The RBC/RBC protocol is described according to ISO OSI Layer model. To facilitate the specification activity, the functional requirements, partly in SUBSET-039 [1] and partly in SUBSET-098 [2], are allocated to a specific Communication Supervision Layer (CSL). Requirements related to the safety of the communication are instead allocated in the Safe Application Intermediate sub-Layer of the Safety Functional Module.
The Communication Supervision Layer corresponds to *high level* functionality specifically dedicated to RBC/RBC communication, acting as an interface between communication protocols (Layer 4 and below) and the *User* functions (signalling rules adopted by RBC). The Communication Supervision Layer also allows the definition of communication functionalities not strictly dependent on specific solutions for RBC functions and their implementation (e.g *safety architecture*).
In this context, the *User* includes all application functions (e.g. evaluation of Movement Authorities (MA), communication with on-board units, etc.) and the generation/reception of information to communicate, while protocol Layers are dedicated to formatting and exchanging such information with communication partners. The specification of *User* functions is out of scope of 4SECURail.
The Communication Supervision Layer allows us to separate transport protocols from more applicative functionalities and let us focus on the objectives of WP2 and the FM demonstrator.
Moreover, lower levels (EuroRadio and Communication Functional Module of SUBSET-098) are already well harmonised and should not bring additional information for 4SECURail scope.
Summarising, the scope of the demonstrator will be:

1. Functional requirements allocated in the Communication Supervision Layer (see chapter 7.1 below)
2. Safe Application Intermediate sub-layer (see SUBSET-098).

6.1 General Assumptions

The communication between the RBCs is done in compliance with the RBC handover protocol, exchanging NRBC messages (i.e. messages with neighbour RBC), to implement the handover transaction at a functional application level. The safety of the communication is granted by dedicated lower levels.

The following assumptions have been made:

1. Point-to-point communication between two RBCs (only one communication active)
2. The RBC/RBC communication shall provide the exchange of NRBC messages in both directions simultaneously
3. Event driven communication with Triple Time Stamp (**TTS**) option; Cyclic communication with Execution Cycle (**EC**) option.
4. Format of messages according to SUBSET-039 [1] and SUBSET-098 [2].
5. The RBC/RBC communication shall be established according to the Safe Communication Interface SUBSET-098 [2].

Communication Supervision Layer and Safe Functional Module (SFM) sub-Layers specification is based on the compliance to the SIL required by system risk analysis by reference to SUBSET-091 [7]. No special SIL requirement should apply for other Layers.
The RBC User functions, not implemented in our project, are fully responsible of the generation of messages, i.e. of their content, format, syntactical correctness (like length, use of variables values, etc.) and, where necessary, of managing corresponding acknowledgements at User application level, not implemented in our project. The User functions are responsible to generate messages when conditions exist and according to the correct sequence, necessary for safe operations as specified in relevant ETCS specifications.
The interface protocol in 4SECURail scope checks neither the correctness of content and format of messages nor the appropriateness of conditions when they are generated by RBC User functions; the interface protocol is only responsible to send and receive messages generated by RBC User functions, ensuring that the data streams are not affected by communication errors that could generate unsafe conditions. This is done by reference to criteria stated in EN 50159 and preventing the delivery to RBC User application of unsafe messages and/or informing the User application of the potentially unsafe situation, as described in the next chapters.
In particular, the protocol is not responsible of generating acknowledgements or repetition of User messages, which are in any case decided by RBC User functions.

All requirements are structured according to ISO OSI model and most of them are traceable to SUBSET-039 [1] and SUBSET-098 [2]. Some new requirements have been added for implementation reasons.

6.1.1 Logical structure

Figure 2 shows the logical structure adopted in 4SECURail approach. For each RBC, the following functional subdivision is considered. The shadowed part shows the scope of 4SECURail.

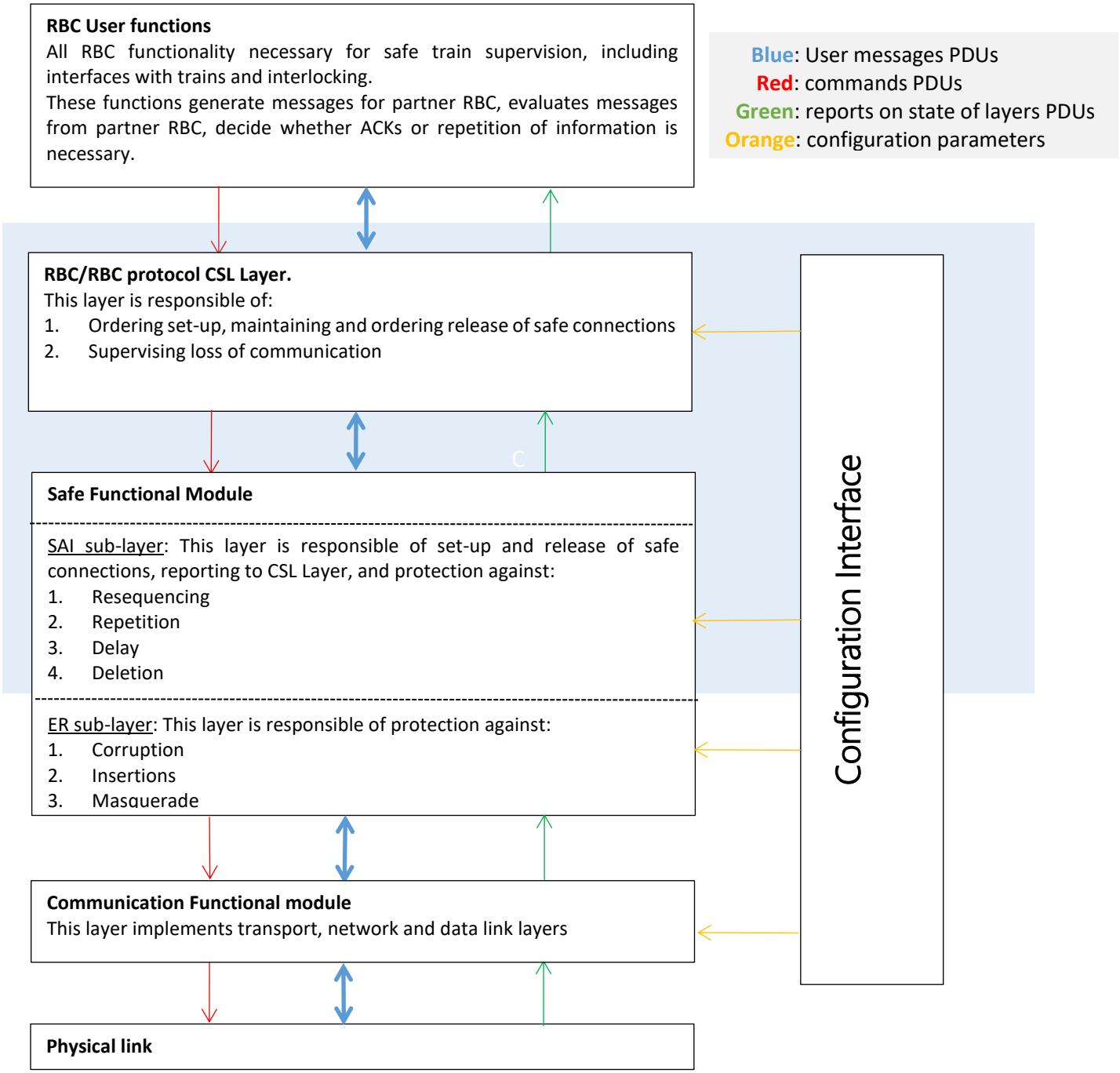

Figure 2 - System overview

6.1.2 Definitions

Valid message: a message is valid if its format and reception conditions (e.g. timing, sequence of message in a stream, etc.) comply with the rules established for the project. The relevant protocol Layers and User application at receiver side are responsible of the verification of compliance.

Correct message: a message is correct when its content corresponds to the operational state of the system. Ensuring correctness of the content is the responsibility of the function generating the message (out of scope of 4SECURail).

Communication error: any event modifying the content and the reception conditions of a message. The following errors are taken into account (definitions as in EN 50159-2 [8]):

1. Deletion (a message is removed from the message stream)
2. Delay (a message is received at a time later than intended)
3. Resequencing (the order of messages in the message stream is changed)
4. Repetition (an already sent message is sent again in the message stream)
5. Corruption (a data corruption occurs)
6. Insertion (an additional message is implanted in the message stream)

Protection: any measure finalised to permit detection of the occurrence of a communication error. A protection ensures, with sufficiently high probability, that a message affected by any of the above mentioned errors becomes formally not valid, and is therefore identified by the receiver that can activate a safe reaction (the safe reaction is out of scope of 4SECURail).

6.1.3 Options

In case of **TTS** (Triple Time Stamp), the User data (messages prepared by RBC User functions) are sent when requested by User functions with an event driven scheduling of processes.
Life sign messages are inserted in the messages stream, to ensure that a message (User or Life sign) is sent before the expiration of a configurable sending timer, which is reset at the sending of a message. The receiver will check the reception of a message before the expiration of a corresponding receiving timer, which is reset at the reception of any message.

In case of **EC** (Execution Cycle), the protocol functionality responsible of sending messages is cyclically scheduled (configurable cycle time).
If, when the functionality is activated by the scheduler, a request from User functions to send a message is pending, the message is sent (only one; if more messages are pending, the queue will be served one message per cycle). If no User message is pending, a Life sign is sent.
In this approach all messages (irrespective if User or Life sign) are uniformly spaced by a time TC.
The receiver will behave in the same way as for **TTS option**.

The 4SECURail requirements include both options. Where not explicitly stated, requirements apply unchanged for both options.

6.2 Safety

As stated in the MAAP, requirements on safety, security and reliability are complex, since they cover a vast state space, and because they use many concepts of multiple domains. Using FM in

specification, development and verification could be the way to ensure that such requirements are satisfied.
The safety requirements of the sub-system selected as our case study, the RBC/RBC interface, are entirely derived by the SUBSET-098 - RBC/RBC Safe Communication Interface [2] and the subsystem is considered at SIL4 level.

Considering that the scope of 4SECURail demonstrator is not the development of a product, but the process to develop an interface specification from the IM point of view, the protection against random "wrong side failures" [9] is out of scope (it will be addressed by suppliers through architectural solutions like "2 out of 2" redundancy or similar), while the application of FM is expected to significantly improve the detection and elimination of systematic failures, representing therefore a major step towards the achievement of SIL4 goals.
Furthermore, protection against consequences of deletion or excessive delay of messages is responsibility of User Application.
Other protection measures according to EN50159 (e.g. authenticity, integrity, etc.) are provided by the RBC/RBC Safe Communication Interface (see [SUBSET-098 [2]]).

The following Table 1 shows the safety threats and their allocation to the levels of the architecture in the scope of 4SECURail:

Threat	**CSL LAYER**	**SFM-SAI**
Deletion (a message is removed from the message stream)	Detection of loss of communication (Life Sign Timeout) Loss of safe connection (reading reports)	Sequence number
Delay (a message is received at a time later than intended)	*(T_RBC in user function)*	Timeout
Resequencing (the order of messages in the message stream is changed)	T_RBC_timestamp >	Sequence number
Repetition (an already sent message is sent again in the message stream)		Sequence number

Table 1 – Protections against threats

7 Requirements

This section contains the requirements related to the RBC/RBC handover used in the 4SECURail project as case study.
As already mentioned, all the requirements are structured according to ISO OSI model: in particular, requirements for the Communication Supervision Layer and for the Safe Functional Module - Safe Application Intermediate sub-Layer are listed. The other layers are out of the 4SECURail scope.
Most of the requirements are traceable to SUBSET-039 [1] and SUBSET-098 [2]. The mapping is shown in 10.2.
Moreover, some new requirements (not traceable to UNISIG subsets) have been added for implementation reasons.

7.1 Communication Supervision Layer

INFO	SUBSET-039 does not make reference to a specific functional architecture for RBC. It describes RBC functions related to handover without a clear allocation to functional modules. Considering that the scope of 4SECURail is not the development of a full RBC functionality, it has been decided to extract from the whole functionality of SUBSET-039 a functional subset dedicated to RBC-RBC communication, in order to define an "object" that can be modelled and tested independently from the whole system in which it should be integrated. The above mentioned object is the Communication Supervision Layer (CSL) specified through the set of requirements listed below. As stated above, these requirements capture part of SUBSET-039 functionality and are integrated with some additional requirements, to have a self-standing functional module. According to this approach, some requirements of CSL may be directly traced to SUBSET-039 statements, while others will be identified in a different way. CSL is responsible to collect data from the User functions and to deliver received data to the User functions (User messages generated and transmitted by the RBC functions). It cooperates with SFM to ensure protection against deletion, resequencing and insertion of messages by informing the User functions that will take the appropriate reactions (out of 4SECURail scope). CSL is specified with reference to SUBSET-039 requirements and procedures. In the following sections requirements apply unchanged to initiator and called entity, unless otherwise stated. TTS and EC options are not relevant for CSL.

7.1.1 Communication functions

7.1.1.1 Establishment and maintaining of safe communication

INFO	CSL can be configured as initiator or called entity (this role only refers to responsibilities related establishment and maintenance of safe connections and remains unchanged during the whole life of the system, independently of management of transactions):
REQ_001	If configured as initiator, when switched on (communication in state NOCOMMS), the CSL is responsible to send to underlying Layers the command for the establishment of a safe connection with the partner RBC, and to command re-establishment of safe connection when it is considered lost (communication in state NOCOMMS).
REQ_002	After sending the command for the establishment of the connection, a timer shall be started by the initiator. If the timer expires before the connection is established, a new connection request shall be generated.
REQ_003	If configured as called, the CSL shall wait for report from underlying Layers that a safe connection is established.

7.1.1.2 Management of transactions

7.1.1.2.1 Establishment of a transaction

REQ_004	The CSL shall discard any message either from User functions or from partner CSL before a confirmation of successful clock offset estimation (TTS option) or EC initialisation has been received from SAI sublayer.
INFO	It is responsibility of User functions to create an instance of transaction for each ETCS unit connected to the RBC and intended to pass the RBC/RBC borders. The transaction is created by HO RBC User functions before sending pre-announcement message. The transaction is created by the ACC RBC User function upon receiving the pre-announcement message.
INFO	The instance of any transaction is identified by the relevant User functions by means of the identity of the ETCS unit and the identity of the border location.

7.1.1.2.2 Termination of a transaction

INFO	Normal termination of transaction will occur according to Figure 3: - ACC RBC User functions terminate the transaction when receiving announcement message or when informed that train head has passed the border. At termination of transaction a TOR message is sent. - HO RBC User functions terminate the transaction upon receiving TOR message or when informed that the train tail has passed the border.

7.1.1.2.3 Cancellation of a transaction

INFO	Both HO and ACC RBC functions may send a cancellation message at any time to the

	partner RBC to terminate a transaction.
INFO	When a transaction is cancelled by the RBC User functions, the corresponding cancellation message is sent to the partner RBC.
INFO	- reception of pre-announcement with the same train identity of an existing transaction and different border location will always cause the accepting RBC User functions send a cancellation order for this transaction. - reception of pre-announcement with the same border identify of an existing transaction and different train identity will cause the accepting RBC User functions send a cancellation order for this transaction only if more than one on-board unit among the ones directed to the same border location is in a mode other than NL.
INFO	Reception of pre-announcement for a transaction for which a first RRI request has already been received will cause the accepting RBC User functions send a cancellation order for this transaction.

7.1.1.2.4 Repetition of pre-announcements

INFO	The first pre-announcement message can be repeated, with the same identity of ETCS unit and same border location; this will neither affect the on-going transactions nor generate a new transaction.
INFO	The first pre-announcement can be repeated with the same border location and different ETCS unit identities if only one identity is not in NL mode; this will not affect the existing transactions and will create a new transaction for the new train identity.
INFO	Reasons for new pre-announcements or cancellations are not in the scope of 4SECURail.

7.1.1.2.5 Receiving messages

REQ_005	The CSL shall forward a received User message to RBC User functions only if all checks specified in supervision functions (7.2.2) are passed.
INFO	The User functions will ignore messages other than pre-announcements, if the messages are related to ETCS units for which a transaction is not active.

7.1.2 Supervision functions

7.1.2.1 Protection against deletion

INFO	This protection includes both supervision of loss of the safe connection and the supervision that messages are effectively exchanged while safe connection is reported active by underlying Layers. Note: additional protection against deletion is given by SAI sublayer functionality.

7.1.2.1.1 Loss of safe connection

REQ_006	Loss of safe connection shall be detected by the CSL reading reports from the underlying SFM (SAI_DISCONNECT.indication).
REQ_007	If a report from underlying Layers is received that safe connection is lost, the CSL shall consider the communication in state NOCOMMS.

7.1.2.1.2 Detection of loss of communication

REQ_008	TTS option: after reception of report from SAI that the clock offset procedure has been completed, the CSL shall ensure that a message is sent to the partner RBC at the expiration of a configurable transmit time interval (reset at the sending of any message). If no User message needs to be sent, CSL is responsible to send a life sign message (see Figure 4); EC option: After reception of report from SAI that the EC initialisation procedure has been completed, the sending of messages is scheduled cyclically every (configurable) TC. If no request to send messages from User application is pending, a life sign is sent by CSL. If requests are pending, only one message per cycle is sent.
REQ_009	After reception of report from SAI that the clock offset procedure or EC initialisation has been completed, the condition where no valid messages are received within a configurable time shall be recognised by the CSL. This is achieved by means of a configurable receive timer (started at the reception of report from SAI on completion of initialisations and reset at the reception of any message); if no message (User or life sign) is received within such configurable receive time interval, the communication shall be considered in state NOCOMMS.
REQ_010	When communication is in state NOCOMMS, the CSL shall not accept/forward messages neither from its own RBC User functions nor from partner RBC; when switching to NOCOMMS, if the safe connection is still active, the CSL shall send a termination order (SAI_DISCONNECT.request). Note: when informed that the communication is in state NOCOMMS, the User functions will terminate all transactions.
REQ_011	CSL can switch the communication from state NOCOMMs to state COMMS only when underlying Layers confirm the re-establishment of a safe connection. Note: communication in state COMMS is communicated to User functions, that will be able to restart management of transactions.

7.1.2.2 Protection against resequencing

INFO	User functions will ignore received messages, if their time stamp is lower than the time stamp of an already received message. Note: here the time stamp in the User message (T_RBC variable) is meant. This is an additional check with respect to the ones performed by SAI.

7.1.2.3 Protection against delay

INFO	No Application Layer function is dedicated to this protection which is however covered by SAI sublayer and also by the check of time stamps in application messages (variable T_RBC - responsibility of RBC User functions).

7.1.2.4 Protection against insertion

INFO	The User functions will ignore received messages that have been originated by RBCs other than the one involved in the relevant transaction. This is done checking sender ID in the messages (variable NID_RBC).
INFO	Note: additional protection is provided by ER sublayer.

7.1.3 User messages

INFO	Format of messages (payload PDUs) is according to SUBSET-039 [1] and SUBSET-098 [2].

7.1.4 Operations

REQ_012	If configured as initiator, at start-up, and when loss of safe connection is detected, the CSL shall send safe connection init order to SFM (SAI_CONNECT.request).
REQ_013	If configured as initiator, at start-up, and when loss of safe connection is detected, the CSL shall wait for reception of safe connection established confirmation from SFM (SAI_CONNECT.confirm).
REQ_014	If configured as called, at start-up, and when loss of safe connection is detected, the CSL shall wait for reception of safe connection established confirmation from SFM (SAI_CONNECT.indication).
REQ_015	In case loss of communication is detected due to no valid messages received within a configurable time, the CSL shall send a safe connection termination order to SFM (SAI_DISCONNECT.request).
INFO	The User functions are responsible of managing transactions according to messages from partner RBC.
REQ_016	While the safe communication is active (state COMMS), the CSL is responsible of sending User messages received from RBC User functions to partner RBC.
REQ_017	While the safe communication is active (state COMMS), the CSL is responsible of checking User messages received from partner RBC and forwarding (if checks are passed, see 7.2) to RBC User functions.
REQ_018	The CSL is responsible of reading reports from SFM.
REQ_019	The CSL is responsible of sending reports to RBC User functions about state of communication (COMMS/NOCOMMS).

7.1.5 Interface with RBC User functions

7.1.5.1 From User functions

REQ_020	CSL shall receive from User functions the messages to be forwarded to peer RBC User when in state COMMS (RBC_User_Data.request(nrbc_msg)).

7.1.5.2 To User functions

REQ_021	CSL shall forward to User functions the messages received from communication partner (RBC_User_Data.indication(nrbc_msg)).
REQ_022	CSL shall send to User functions the reports (RBC_User_Disconnect.indication) on loss of communication (missing life sign - state NOCOMMS).
REQ_023	CSL shall send to User functions the reports (RBC_User_Connect.indication) on state of safe connection state change (COMMS/NOCOMMS).

7.1.6 Interface with Safe Functional Module

INFO	The interface between Application layer and SAI is specified in compliance with SUBSET-098 5.4.2 and is composed of the following service primitives.

7.1.6.1 Connection Set-up

REQ_024	• SAI_CONNECT.request shall be used by initiator CSL to command the establishment of a safe connection • SAI_CONNECT.indication shall be used by called SAI to notify to the CSL the connection establishment request • SAI_CONNECT.response shall be used by called CSL to accept the connection request. • SAI_CONNECT.confirm shall be used by the initiator SAI entity to inform the CSL about the successful establishment of the safe connection.
INFO	SUBSET-098 does not specify any mandating use of the SAI_CONNECT.response. In our model we will not implement this primitive and will see if the model is consistent. The SAI_CONNECT.response signal would be sent after the TTS/EC initialization procedure that requires the use of an already established connection.

7.1.6.2 Data Transfer

REQ_025	• SAI_DATA.request shall be used by CSL to transmit data to the peer entity. • SAI_DATA.indication shall be used to indicate to the CSL that data have been received successfully from the peer entity.

7.1.6.3 Connection release

REQ_026	• SAI_DISCONNECT.request shall be used by the CSL to enforce a release of the safe connection • SAI_DISCONNECT.indication shall b used to inform the CSL about a safe connection release.

7.1.6.4 Error detection

REQ_027	SAI Error Report shall be sent from SAI to CSL in case of errors detection by SAI (deletion, resequencing, delay, repetition).

7.2 SFM-SAI sublayer

INFO	This Layer is responsible of establishing and releasing safe connections. It is responsible of protection against delay, resequencing, deletion, repetition. The SAI is specified with reference to SUBSET-098 [2]. In the following section, requirements apply unchanged to initiator and called entity, unless otherwise stated.

7.2.1 Communication functions

7.2.1.1 Establishment and maintaining of safe connection

REQ_028	If SAI receives a command to establish a safe connection from CSL (CSL configured as initiator), SAI shall forward this order to ER Layer.
REQ_029	In case initiator, when SAI receives a confirmation of safe connection established from ER Layer, SAI shall start the initialisation procedure (initial clock offset estimation for TTS option or initialisation for EC option).
INFO	To simplify the implementation (and according to SUBSET-098 [2] Fig 7), we consider that any connection request is always accepted by SAI without any authorization from upper layers. This means that SAI level will automatically reply to incoming connection requests forwarded from ER Layer.
REQ_030	In case called, if SAI receives a safe connection establishment indication from the ER Layer, SAI shall send a confirmation to ER Layer and wait for the start of the initialisation procedure (initial clock offset estimation for TTS option and initialisation for EC option).
REQ_031	Robustness requirement: considering that the communicating RBCs might be affected by loss of communication at different time, the called RBC protocols shall accept the re-establishment of a safe connection even if they are still considering the communication not lost.

7.2.1.2 Clock offset estimation (for TTS option)

INFO	The format of messages mentioned in this section is according to SUBSET-098 [2], estimation of offset are according to Figure 17.
REQ_032	When ER sublayer reports the successful establishment of safe connection, SAI initiating the safe connection establishment (initiator) shall send an OffsetStart message.
REQ_033	At the reception of an OffsetStart message the responder SAI shall answer with an OffsetAnswer1 message.
REQ_034	At the reception of the OffsetAnswer1 message the initiator shall estimate the offset between clocks, and send a message OffsetAnswer2.
REQ_035	At the reception of the OffsetAnswer2 message the responder shall estimate the offset between clocks, and send a message OffsetEst.
REQ_036	At the reception of OffsetEst message the initiator shall compare the offset estimations. If the difference between estimation is lower than a configurable value, the initiator shall send a message OffsetEnd with value “OK”, otherwise with value “notOK”.
REQ_037	When OffsetEnd message is sent, the initiator SAI shall report the corresponding termination to CSL.
REQ_038	At the reception of OffsetEnd message the responder SAI shall report the corresponding termination to CSL.
REQ_039	After sending OffsetStart, OffsetAnswer1, OffsetAnswer2, OffsetEst messages, the sender SAI shall start a timer with configurable time out. If the time out expires without the reception of a new message, the procedure shall be cancelled and the error reported to the CSL. Note: after sending OffsetEnd the initiator CSL starts the management of life sign messages; when OffsetEnd is received, the responder CSL starts the management of life cycle messages.
REQ_040	When the initiator SAI is informed about cancellation of clock offset estimation, it shall initiate a new estimation procedure.

7.2.1.3 Periodical update of clock offset (for TTS option)

INFO	The following procedure may be applied with a configurable period, independently by each communicating party:
REQ_041	With a configurable period, by each communicating party, SAI shall send a ClockOffsetUpdateRequest message and start a configurable timer.
REQ_042	At the reception of the ClockOffsetUpdateRequest the partner SAI shall send a ClockOffsetUpdateAnswer message.
REQ_043	Receiving the ClockOffsetUpdateAnswer message, the SAI shall check that it refers to the last ClockOffsetUpdateRequest sent (check of time stamps). If the timer has not expired the SAI shall update the clock offset according to SUBSET-098 [2] Figure

	21; if the timer expires the SAI shall report the error to CSL and a new ClockOffsetUpdateRequest shall be sent.

7.2.1.4 Initialisation procedure (for EC option)

REQ_044	When ER sublayer reports the successful establishment of safe connection, SAI initiating the safe connection establishment (initiator) shall send an ExecutionCycleStart message containing its initial value of EC counter and the EC period.
REQ_045	The responder SAI shall answer to an ExecutionCycleStart message with an ExecutionCycleStart message containing its initial value of EC counter and the EC period and report to the CSL that the initialisation procedure has been completed.
REQ_046	After sending any of the above listed messages, the SAI shall start a timer with configurable time out. If the time out expires before the reception of a new message (that is a User message or a life sign, in the case of the responder SAI) the procedure is cancelled and the error is reported to the CSL.
REQ_047	At the reception of the message from the responder, the initiator SAI shall inform the CSL that the initialisation procedure has been completed.

7.2.1.5 Detection of transmission delays (for EC option)

REQ_048	With a configurable period, by each communicating party, SAI shall ensure that an application message with request of ACK is sent and start a timer (note: here the ACK specified in message type is meant, not the ACK managed at User application level inside the User messages).
REQ_049	At the request of an ACK, the responding SAI shall ensure that an application message with ACK is sent.
REQ_050	If the application message with ACK is not received before expiration of the timer an error is reported to the CSL.

7.2.1.6 Sending and receiving messages

REQ_051	For TTS option: No User message shall be accepted by SAI neither from CSL nor from ER sublayer if the clock offset estimation has not been completed (report from SAI to CSL). For EC option: No User message shall be accepted by SAI neither from CSL nor from ER sublayer if the initialisation procedure for EC parameters has not been completed (report from SAI to CSL).

7.2.1.6.1 Sending

REQ_052	For messages sent by CSL (including life sign messages), SAI shall recognize the

	destination of the message from the content of request received from CSL.
REQ_053	Messages originated by SAI itself (e.g. clock offset estimation) shall contain indication of destination.
REQ_054	Messages originated by SAI itself (e.g. clock offset estimation) shall comply with SUBSET-098 [2].
REQ_055	The SAI shall add a message type to User data to be sent. See SUBSET-098 [2] section 5.4.6.
REQ_056	The SAI shall add a sequence number to User data to be sent; the sequence number shall be increased by one at any new message sent (irrespective of its type).
REQ_057	For TTS option, the SAI shall add to User data to be sent: 1. A time stamp set at the current value of sender clock (sender time stamp TS_sender); 2. The time stamp (receiver time stamp TS_receiver) of the last received message; 3. The value of sender clock at the time of reception of last message (T_reception). See SUBSET-098 [2] Figure 5
REQ_058	For EC option, the SAI shall add to the User data to be sent the current value of the cycle counter EC. **No requirement to send max 1 msg per cycle**

7.2.1.6.2 Receiving

REQ_059	A received User message shall be forwarded to CSL only if all checks specified in Supervision functions are passed.

7.2.1.7 Termination of a safe connection

REQ_060	When an order for termination is received from CSL, SAI shall forward it to ER sublayer.
REQ_061	When an indication of disconnection is received from ER sublayer, SAI shall forward it to the CSL.

7.2.2 Supervision functions

7.2.2.1 Protection against deletion

7.2.2.1.1 Check of sequence number

REQ_062	The receiver SAI shall accept any value for the sequence number of the first message after establishment of safe communication.
REQ_063	If N (configurable) consecutive messages are missing in the sequence of the received messages, i.e. if a message whose sequence number is greater that the sequence number of the last correctly received message + N, the message shall be ignored and the SAI shall send an order to terminate the safe connection to ER sublayer and

	report its state to CSL.
REQ_064	In case the sequence number of a received message is greater than the sequence number of the last correctly received message + 1 and lower than the sequence number of last correctly received message + N, the message shall not be discarded and SAI shall report to CSL the occurrence of the communication error.
REQ_065	If the sequence number of the received message is lower or equal to the sequence number of an already received message, the new message shall be discarded and SAI shall report to CSL the occurrence of the communication error.

7.2.2.2 Protection against resequencing

INFO	User functions will ignore received messages, if their time stamp is lower than the time stamp of an already received message. Note: here the time stamp in the User message (T_RBC variable) is meant. This is an additional check with respect to the ones performed by SAI.

7.2.2.3 Protection against delay

REQ_066	The SAI of the receiver entity shall recognise a message that, after sending, has been delayed in the communication channel for a time greater than a configurable value.
INFO	Such message will not be forwarded to RBC User functions.[1]
REQ_067	For TTS option, a received message shall be accepted by SAI only if the difference between the current value of receiver clock and the transmission sender time stamp of the message (taking clock offset into account) is not greater than a configurable value (see SUBSET-098 [2] Figure 20). In case a message is rejected, a report is sent to CSL.
REQ_068	For EC option the acceptance of a message shall be checked according to SUBSET-098 [2] Figure 24.
REQ_069	For EC option the corrections specified in SUBSET-098 [2] section 5.4.9.5.2 shall be applied.

7.2.2.4 Protection against repetition

INFO	Check of sequence number of received messages as above.

7.2.3 User messages

INFO	Format of messages (payload PDUs) is according to SUBSET-039 [1] and SUBSET-098 [2].

[1] In 4SECURail the error is visible in the model but no special information to CSL is necessary because the project does not include user functions able to react to it.

7.2.4 Operations

REQ_070	At start-up, and when loss of safe connection is detected (Sa_DISCONN.indication), the SAI, if configured as initiator, shall wait for order from CSL.
REQ_071	At start-up, and when loss of safe connection is detected (Sa_DISCONN.indication), the SAI, if configured as called, shall wait for reception of safe connection established confirmation from ER sublayer (Sa_CONN.indication).
REQ_072	In case loss of safe connection is detected, the SAI shall send a safe connection report to CSL (SAI.DISCONN.indication).
REQ_073	The SAI shall be responsible of Sending User messages received from CSL (SAI_DATA.request) to partner RBC (through Sa_DATA.request).
REQ_074	The SAI shall be responsible of Checking User messages received from partner RBC (through Sa_DATA.indication) and forwarding (if checks are passed) to CSL (SAI_DATA.indication). Note: CSL might ignore messages if its state is NOCOMMS.
REQ_075	The SAI shall be responsible of Reading reports from ER sublayer (Sa_DISCONNECT.indication).
REQ_076	The SAI shall be responsible of Sending reports to CSL (SAI.DATA.indication, SAI.CONNECT.indication and SAI.DISCONNECT.indication).

7.2.5 Interface with SFM-EuroRadio sublayer

INFO	The interface between SAI and EuroRadio is specified in compliance with SUBSET-037 [10] and is composed of the following service primitives:

7.2.5.1 Connection set-up

REQ_077	• Sa_CONNECT.request shall be used by initiator SAI to command the establishment of a safe connection • Sa_CONNECT.indication shall be used by called ER to notify to the SAI the connection establishment request • Sa_CONNECT.response shall be used by called SAI to accept the connection request. The response shall always be sent automatically without any authorization from upper layers. • Sa_CONNECT.confirm shall be used by the initiator ER entity to inform the SAI about the successful establishment of the safe connection

7.2.5.2 Data transfer

REQ_078	• Sa_DATA.request shall be used by SAI to transmit application data to the peer entity. • Sa_DATA.indication shall be used to indicate to the SAI that data have been received successfully from the peer entity

7.2.5.3 Connection release

REQ_079	• Sa_DISCONNECT.request shall be used by the SAI to enforce a release of the safe connection • Sa_DISCONNECT.indication shall be used to inform the SAI about a safe connection release.
INFO	For an explanation of the connection procedure see Figure 5.

7.3 SFM-ER sublayer

This sublayer is according to SUBSET-037 [10]out of 4SECURail scope.

For testing of Communication Supervision Layer and SAI, the ER sublayer will be simulated with a "stubbed" object, receiving messages as specified above and with the possibility of answering with expected messages or simulating degraded conditions, like:

1. No answer;
2. Delayed answer;
3. Corrupted answer
4. ...

7.4 CFM Layer

According to standard specifications, and it is out of 4SECURail scope

7.5 Physical Layer

Not relevant for the scope of 4SECURail.

8 Conclusions

This deliverable is the outcome of the Task2.2 - Requirements definition of a railway signalling subsystem of the 4SECURail project. This system will be used in the project as a case study on which to apply the formal demonstrator prototype and develop the cost-benefit analysis of its application among IMs.
The system selected is the RBC/RBC handover interface. The choice has been supported by a SWOT analysis, which has highlighted the appropriateness of the RBC/RBC case study for the validation of the FM demonstrator, whose scope is not the development of a product, but the process to develop an interface specification from the IM point of view.
A detailed description of the process and framework constituting the demonstrator prototype will be released in D2.2, and will show, in particular, how all the identified components will be integrated and used.
With reference to SUBSET-039 and SUBSET-098, a minimum set of requirements was composed to kick off the FM development process: with the goal of producing a usable case study for the demonstrator, a specific Communication Supervision Layer has been introduced to isolate only the needed communication requirements and to be independent from the complete RBC functionalities.
The collection of requirements written in natural language, as performed in the current document, is the first step to produce a specification for a railway system, common to both the processes, with and without the adoption of FM.
In the next steps of the 4SECURail projects the requirements defined in this deliverable will be used to validate how the adoption of FM could improve the process of writing a specification for a railway subsystem. Therefore, the demonstrator is expected to raise and help solving possible ambiguities and lacks due to the human process and, on the other hand, the cost-benefit analysis will evaluate the costs and advantages, in terms of time, resources and effort due to the adoption of FM to create a specification, as well as evaluating the impact of FM adoption on rail safety.

9 References

[1] UNISIG - FIS for the RBC/RBC Handover - SUBSET-039 - 17-12-2015 (Issue 3.2.0)
[2] UNISIG - RBC/RBC Safe Communication Interface - SUBSET-098 - 21-05-2007 (Issue 1.0.0)
[3] CENELEC-EN 50159:2018 “Railway applications – Communication, signalling and processing systems - Safety related electronic systems for signalling”
[4] Shift2Rail - MAAP – Multi-Annual Action Plan - 14-11-2019
[5] https://eulynx.eu/
[6] https://www.era.europa.eu/activities/technical-specifications-interoperability_en
[7] UNISIG - Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 – SUBSET-091 – 01-12-2015 (Issue 3.4.0)
[8] CENELEC-EN 50159-2:2001 “Railway applications - Communication, signalling and processing systems - Part 2: Safety related communication in open transmission systems”
[9] https://en.wikipedia.org/wiki/Wrong-side_failure
[10] UNISIG - EuroRadio FIS - SUBSET-037 - 17-12-2015 (Issue 3.2.0)

10 Annexes

10.1 Annex 1 – Data Flow and operating sequences

10.1.1 Normal data flow

INFO	The message sequence chart in Figure 3 is a complement to the state diagram in SUBSET-039 [1] section 4.6.2. It shows the normal flow of messages for managing a handover transaction once the connection has been established. Figure 3 only shows User messages sent by CSL on demand of RBC User functions and does not show the life sign messages, possibly generated by the CSL when necessary.

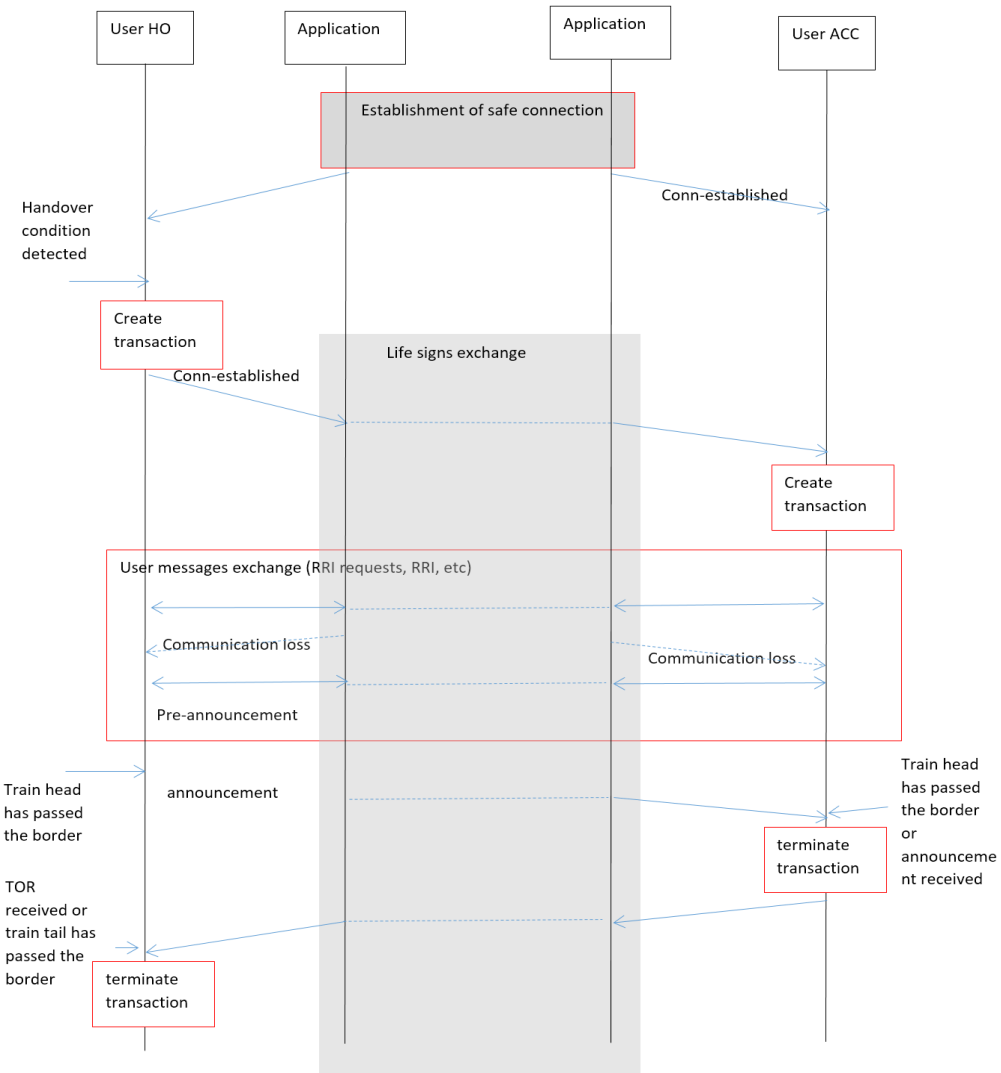

Figure 3 Normal Data Flow

10.1.2 Message flow with TTS option

INFO	Figure 4 shows the message flow from RBC 1 to RBC 2 (TTS option); the flow in the opposite direction is the same (timers may have different values for RBC 1 and RBC 2).

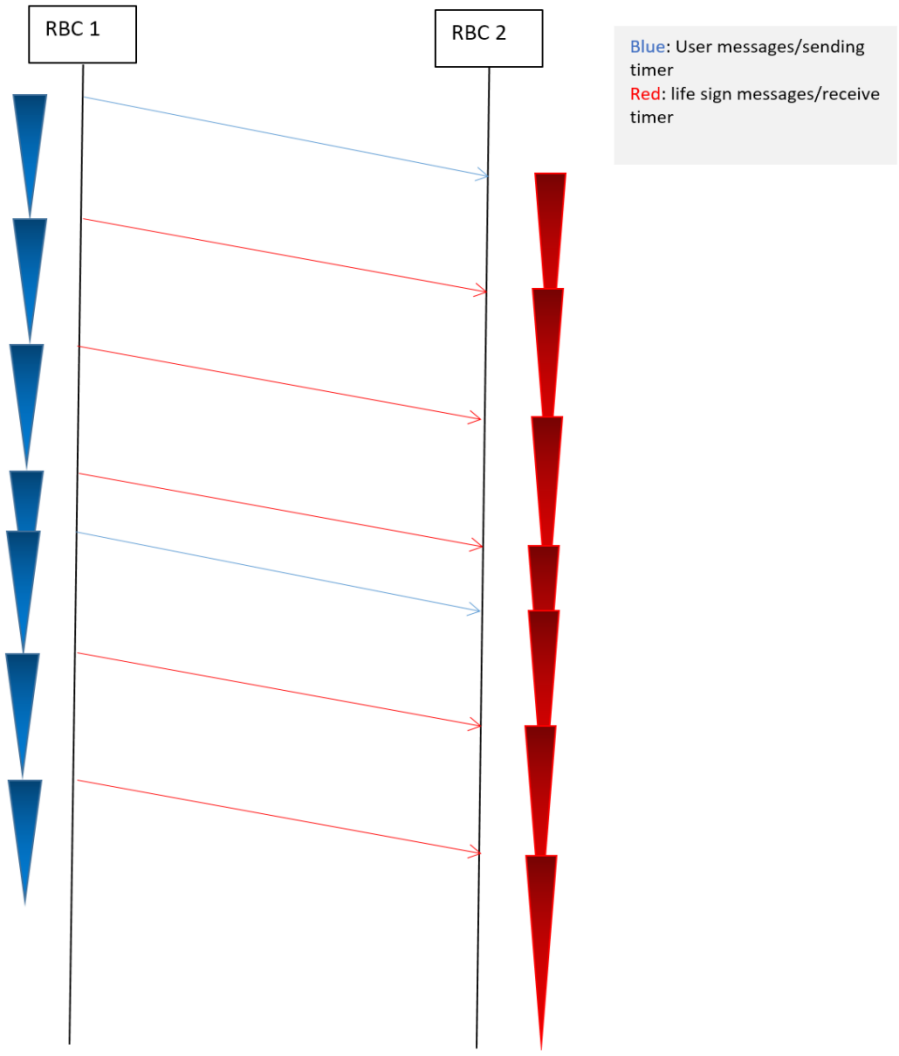

Figure 4 Message flow with TTS option

10.1.3 Safe connection establishment

INFO	According to the above mentioned requirements, the sequence for the establishment of a connection is as follows (see Figure 5): 1. CSL requests the establishment of the safe connection (REQ_001).

	2. SAI request the establishment of the safe connection at ER level; called SAI always, upon receiving Sa_CONNECT.indication, answers with Sa_CONNECT.response, without performing any check (REQ_077). 3. When SAI on the side of initiator receives Sa_CONNECT.confirm, it starts the initialisation of TTS or EC (REQ_032, REQ_008). 4. When called side SAI detects successful end of initialisation, it sends SAI_CONNECT.indication to called CSL (REQ_038). 5. When called CSL receives SA_CONNECT.indication, it answers always with SAI_CONNECT.response. NOTE: we keep step 5 for compliance with SUBSET-098 but we do not implement the SAI_CONNECT.response. This will not affect the normal flow of operation and the results of 4SECURail. See NOTE for REQ_024. 6. When initiator side SAI detects successful end of initialisation, it sends a SAI_CONNECT.confirm to initiator CSL REQ_024.

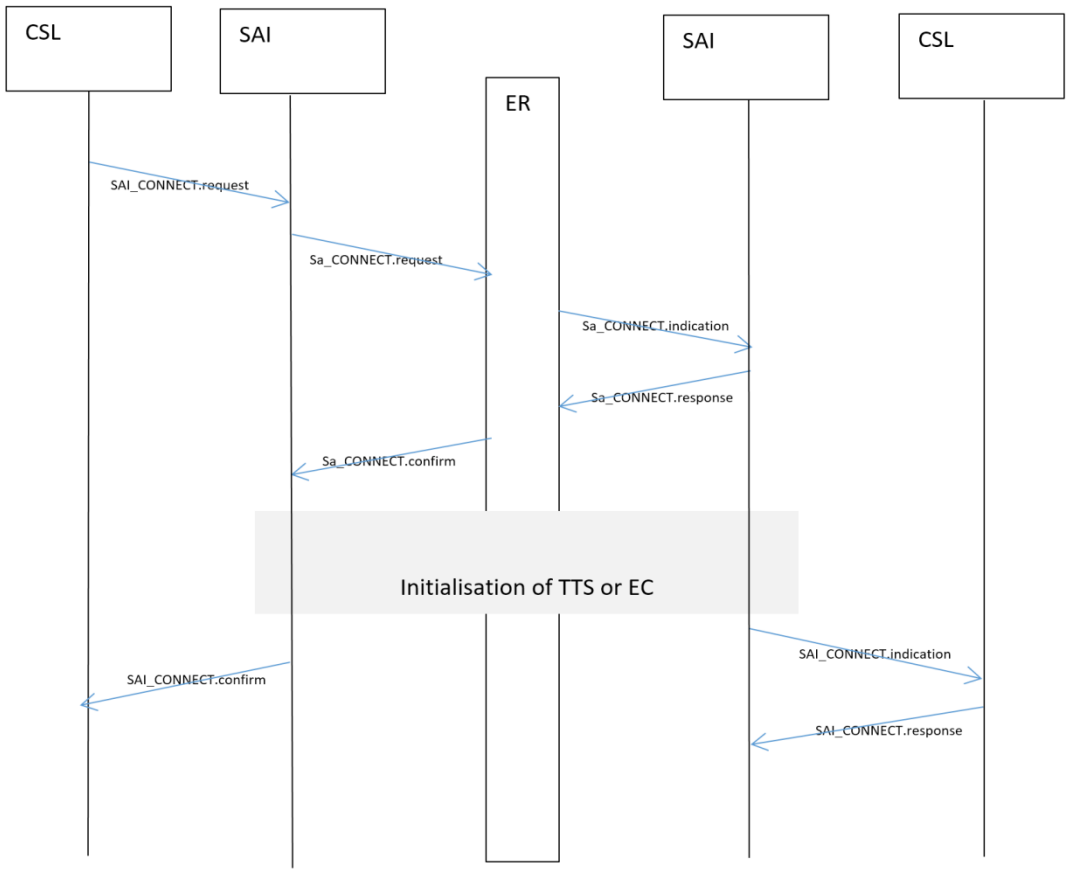

Figure 5 Safe connection establishment

10.1.4 User messages exchange

INFO	The chart in Figure 6 applies to all user messages, including pre-announcements, cancellations, ACKs, etc. CSL does not check the type of user messages, which are interpreted and cause reactions only in User functions.

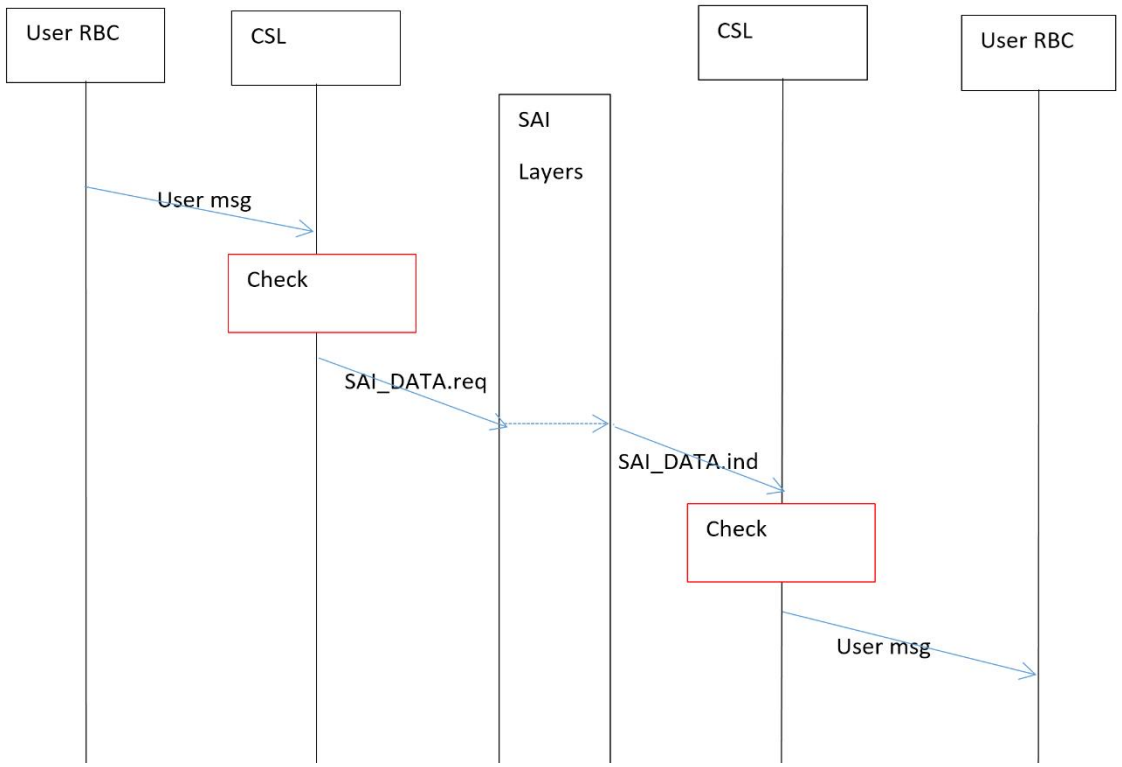

Figure 6 User messages exchange

10.1.5 Loss of safe connection

INFO	Figure 7: initiator side; called side CSL after sending “NOCOMMS indication” waits for SAI_CONN.indication

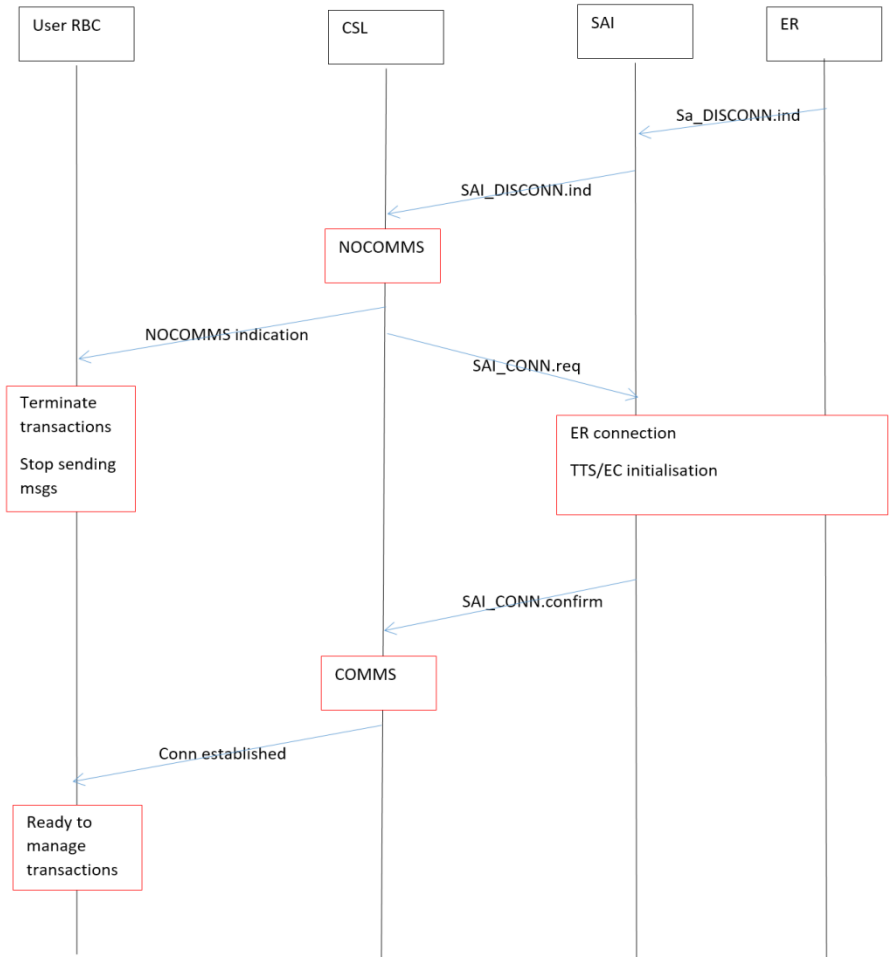

Figure 7 Loss of safe connection

10.1.6 Loss of communication

INFO	Figure 8: initiator side; called side CSL after sending NOCOMMS indications and, if necessary, SAI_DISCONN.req, waits for SAI_CONN.indication
INFO	Notes to “Loss of communication”. CSL (both initiator and called side) sends SAI_DISCONN.req only if the safe connection is released, i.e., if SAI_DISCONN.indication has been received. It might be useful that CSL keeps memory of the current state of safe connection, considering that SAI only reports changes of state.

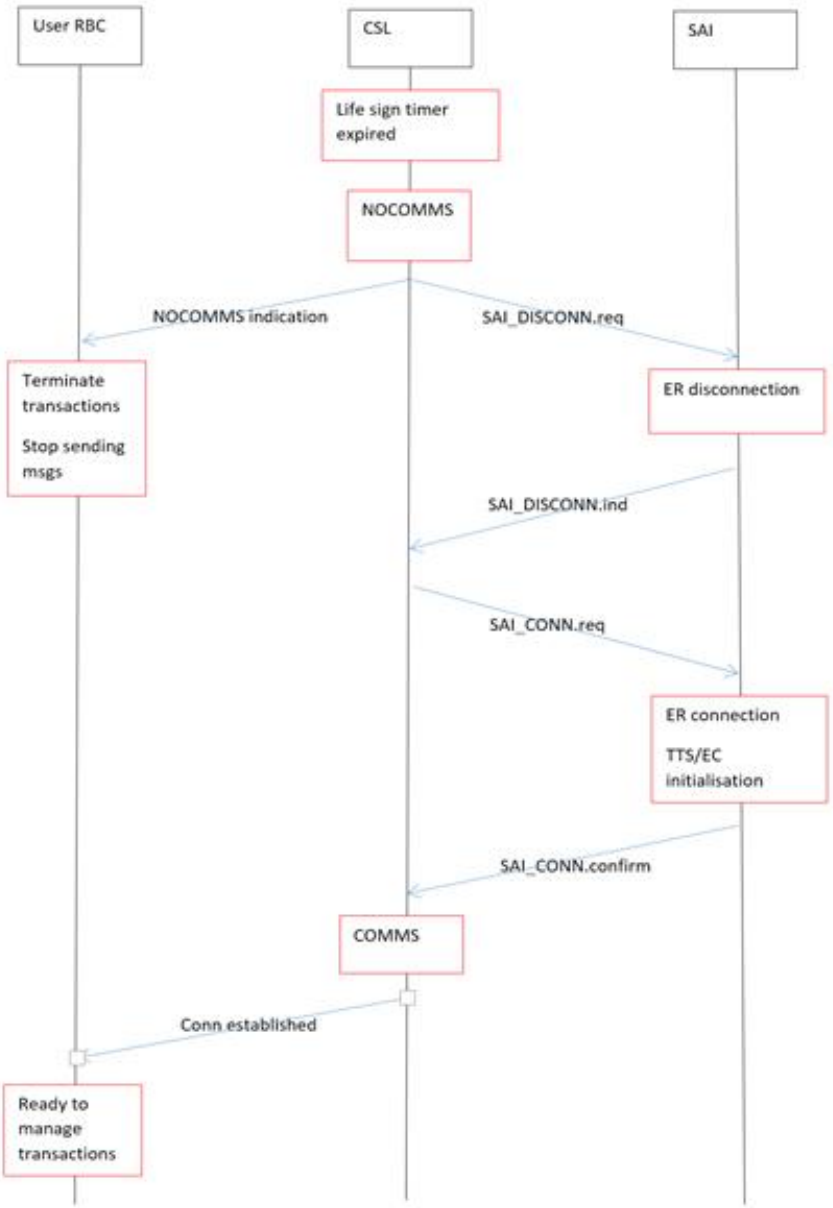

Figure 8 Loss of communication

10.2 Annex 2 – Mapping of requirements

The following table shows the mapping of the project requirements towards SUBSET-039 and SUBSET-098.

REQUIREMENT NUMBER	SS-039	SS-098
REQ_001	4.4.1.2	
REQ_002		
REQ_003		
REQ_004		
REQ_005		
REQ_006		
REQ_007	4.4.1.2 state diagram in 4.6.4	
REQ_008	4.4.1.1 4.4.1.5 4.4.1.6	
REQ_009	4.4.1.1 4.4.1.7 4.4.1.7.1 state diagram in 4.6.4	
REQ_010	4.4.1.3	
REQ_011	state diagram in 4.6.4	
REQ_012	4.4.1.2	
REQ_013	4.4.1.2	
REQ_014	4.4.1.2	
REQ_015	4.4.1.3	
REQ_016		
REQ_017		
REQ_018		
REQ_019		
REQ_020		
REQ_021		
REQ_022		
REQ_023		
REQ_024		5.4.2
REQ_025		5.4.2
REQ_026		5.4.2
REQ_027		
REQ_028		5.4.5.1
REQ_029		5.4.1.1.10 5.4.5.1

		5.4.8.1.1 5.4.8.3.3
REQ_030		5.4.5.1
REQ_031		
REQ_032		5.8.5
REQ_033		5.8.5
REQ_034		5.8.5
REQ_035		5.8.5
REQ_036		5.8.5
REQ_037		5.8.5
REQ_038		5.8.5
REQ_039		5.8.5
REQ_040		
REQ_041		5.4.8.1.8 5.4.8.7
REQ_042		5.4.8.7
REQ_043		5.4.8.7 Fig 21
REQ_044		5.4.9.3
REQ_045		5.4.9.3
REQ_046		5.4.9.3
REQ_047		5.4.9.3
REQ_048		5.4.9.6
REQ_049		5.4.9.6
REQ_050		5.4.9.6
REQ_051		5.4.8.1.1 5.4.8.3.2
REQ_052		5.4.5.3.3 Fig 9
REQ_053		5.4.5.4
REQ_054		5.4.5.4 5.4.8.4
REQ_055		5.4.4.1.4 5.4.5.3.4 Fig 9 5.4.6
REQ_056		5.4.4.1.4 5.4.5.3.4 Fig 9 5.4.7
REQ_057		5.4.1.1.6 5.4.1.1.7 5.4.4.1.4 Fig 5

		5.4.5.3.4 5.4.8.6
REQ_058		5.4.1.1.8 5.4.4.1.4 Fig 6 5.4.5.3.4 Fig 9 5.4.9.2
REQ_059		5.4.5.3.9 to 5.4.5.3.15 Fig 9
REQ_060		5.4.5.2
REQ_061		5.4.5.2
REQ_062		5.4.7.1.4
REQ_063		5.4.7.2.3 to 5.4.7.2.9
REQ_064		5.4.7.2.3 to 5.4.7.2.9
REQ_065		5.4.7.2.3 to 5.4.7.2.9
REQ_066		5.4.1.1.3
REQ_067		5.4.1.1.4 5.4.8.1.5 5.4.8.1.6 5.4.8.6 Fig 20
REQ_068		5.4.9.4
REQ_069		5.4.9.5.2
REQ_070		
REQ_071		
REQ_072		
REQ_073		
REQ_074		
REQ_075		
REQ_076		
REQ_077		5.4.3 5.4.5.1
REQ_078		5.4.3 5.4.5.3
REQ_079		5.4.3 5.4.5.2