ETALON

D 2.2 System Requirements Specification

Due date of deliverable: 31/08/2018

Actual submission date: 01/10/2018

Leader of this Deliverable: Giuseppe Caragnano, ISMB

Reviewed: Yes

Document status		
Revision	Date	Description
1	15.01.2018	First ToC shared within the consortium by ISMB
2	07.05.2018	Content update by ISMB
3	07.05.2018	Content update by UNEW
4	16.05.2018	Contents added by SIRTI
5	21.05.2018	Contents added by ARDANUY
6	03.07.2018	Contents added by BUT
7	03.07.2018	Contents added by SIRTI
8	30.07.2018	Update by ISMB, BUT
9	22.08.2018	Contents added by ARDANUY, SIRTI, ISMB, UNEW
10	23.08.2018	Contents added by Perpetuum
11	28.08.2018	Update by ISMB
12	31.08.2018	Contents added by PERPETUUM
12	31.08.2018	Final review and control check

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/09/2017 Duration: 30 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Francesco Sottile	ISMB	Crete the first structure of document
Alexander James Pane	ISMB	Add content about OTI node
Giorgio Giordanengo	ISMB	Add content about communication components of OTI node
Giuseppe Caragnano	ISMB	Insert content overview about functional requirement
Roberto Cafferata	SIRTI	Insert an overview regarding the OTI (including the hazard analysis), some main functionalities regarding control Module and communication module, an introduction to the Safety Integrity Level and an introduction to the design and implementation constraints of the system requirements specification
Marco Giuliari	SIRTI	Integration of some specifications relating ETCS and Safety Integrity Level
Paul Hyde	UNEW	Content Update

Name	Company	Details of Contribution
Veronika Nedviga	ARDANUY	Content Update about Track side architecture and modules descriptions
Alexander James Pane	ISMB	Added Content regarding the OTI node, cleared some comments and also comments. Minor corrections
Zdenek Hadas	BUT	Toc and Content about Trackside Energy harvesting (4.8)
Roberto Cafferata	SIRTI	Added Content regarding the hazard and conceivable consequences of the OTI device
David Vincent	PERPETUUM	Given information about energy harvesting from vibrations
Alexander James Pane	ISMB	Updated various sections for the OTI. Added some comments and updated the Signalling Control Centre terminology to Control Module
David Vincent	PERPETUUM	Inserted WSN functional state description
David Vincent	PERPETUUM	Updated train state descriptions, their analytic description and the possibly aspects of the different phases of transition from one state to another one
Roberto Cafferata & Alexander James Pane	SIRTI	Performed the last editing check and final revision of the entire document

EXECUTIVE SUMMARY

The main objectives of ETALON WP2 – System Architectures, Specifications and Technical Coherence, regarding the activities linked with the WP2 TD 2.4 are:

- Describe details to deliver the “System Requirements Specification” for the “On-board Train Integrity System” solution
- drill down in the details to deliver the “System Requirements Specification” for the “Trackside Energy Harvesting device for Object Controllers”

The main problem for freight trains is that normally no power source is available on a freight wagon. Solutions are limited by the fact that many freight trains may require frequent changes in the train composition, with separation and re-assembling of wagons for different train missions.

These considerations emphasise the importance of developing train integrity solutions based on radio communication between vehicles with locally generated power (energy harvesting on-board).

In order to better define System architecture, the requirements coming from the SIL4 features are taken into account separating into requirements to be implemented in the prototypes of ETALON project and in requirements of future implementation.

This document contains all the output considerations that comes from Functional Requirement Specification Document D2.1 and presents the output of the Feasibility study and Trade-off analysis of the Tasks T3.1 and T4.1. In addition, the results presented in this document are output of the activities of the WP5 and for the tasks T3.2, T3.4, T4.2 and T4.3.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PARTICIPANTS

N.	LEGAL NAME	SHORT NAME
2	SIRTI - SOCIETÀ PER AZIONI	SIRTI
3	ARDANUY INGENIERIA SA	ARD
5	ERGOSE SA	ERGOSE

6	ISTITUTO SUPERIORE MARIO BOELLA SULLE TECNOLOGIE DELL'INFORMAZIONE E DELLE TELECOMUNICAZIONI ASSOCIAZIONE	ISMB
7	PERPETUUM LIMITED	PER
8	UNIVERSITY OF NEWCASTLE UPON TYNE	UNEW
9	BRNO UNIVERSITY OF TECHNOLOGY	BUT

1. INTRODUCTION

The System Requirements Specification report (in the following chapters referred to as “SRS”) describes the functional requirements needed for the next generation “On–board Train Integrity System” and for the new “Trackside Energy Harvesting device for Object Controllers”.

1.1 ACRONYMS AND REFERENCES

1.1.1 Acronyms

This is the list of acronyms used inside this document.

AES	Advanced Encryption Standard
CCS	Command Control and Signalling
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
FRS	Functional Requirements Specification
HMI	Human Machine Interface
kmh	Kilometres Per Hour
OCWC	Object Controller Wireless Communication
OTI	On-Board Train Integrity
RF	Radio Frequency
PME	Power Management Electronic
RSA	Rivest–Shamir–Adleman (public-key cryptosystem used for secure data transmission)
SCC	Signalling Control Centre
SHA	Secure Hash Algorithm
SIL	Safety Integrity Level

SRS	System Requirements Specification
TDMA	Time Division Multiple Access
TEH	Trackside Energy Harvesting
TI	Train Integrity
TMS	Train Management System
TO	Trackside Object
ToF	Time of Flight
UWB	Ultra-Wide Band
TPS	Train Protection System

Table 1 – List of Acronyms

2. GENERAL OVERVIEW OF THE FUNCTIONAL ARCHITECTURE

The SRS defines the system requirements for the European Train Control System (ETCS) of ERTMS. It is the translation of the mandatory functional requirements defined by the Functional Requirements Specification (UIC/A200 FRS version 4.3, in the following chapters referred to as "FRS") into a technical specification for developers.
It is recalled the functional requirements for the TI check system.

2.1 FUNCTIONAL REQUIREMENTS OVERVIEW

In this section is shown the list of Functional Requirements taken from the deliverable D2.1. These requirements are classified as safety relevant or not, according to a preliminary estimation as already explained inside the deliverable D2.1.

TI_FS_1 (safety relevant): Integrity shall be considered not confirmed when the distance between two adjacent vehicles exceeds a specific reference distance by a limit value (to be specified according to hazard analysis and system design).

TI_FS_2 (safety relevant): Integrity shall be considered not confirmed when there are insufficient communication nodes responding to support a communication network that includes the whole length of the train.

TI_FS_3 (safety relevant): Integrity shall be considered not confirmed when insufficient communication nodes remain associated with the convoy for train integrity to be proven (and communication nodes which lose association with the convoy will generate an alert).

TI_FS_4 (safety relevant): Integrity shall be considered not confirmed when the network can not complete data transfer to establish train integrity for all vehicles or the data is incomplete.

TI_FS_5 (safety relevant): Integrity shall be considered not confirmed when the distance between two adjacent vehicles cannot be evaluated.

TI_FS_6 (safety relevant): Integrity shall be confirmed only at the end of a check proving that, within a configurable time period, all distances between adjacent vehicles do not exceed the limit value.

TI_FS_7 (safety relevant): If the check starts at time t_s and ends at time t_f, the confirmation of integrity shall be referred to time t_s.

TI_FS_8 (safety relevant): If for an unknown reason, the integrity check starts but the process is interrupted, then the integrity check will be not confirmed.

TI_FN_1 (not safety relevant): It shall be possible to implement cyclic train integrity confirmation (with configurable time period) or confirmation on–demand by the external user functionality (on–board train protection functions).

TI_P_1 (performance, not safety relevant): It shall be possible to configure the acceptable duration of the train integrity confirmation process.

TI_P_2 (performance, not safety relevant): The time for a single instance train integrity confirmation process to complete should be as short as possible, there should be a maximum time limit for the process which should be configurable and established during train integrity function initialisation. If a train integrity confirmation cannot be completed within the time limit the train integrity status will be considered as “not confirmed”.

TI_P_3 (performance, not safety relevant): The time between consecutive train integrity confirmation processes should be configurable according to the train speed and the category of route. The moving block of the traffic management system and the required line capacity should be considered (according to hazard analysis and system design).

TI_P_4 (performance, not safety relevant): The time between consecutive train integrity confirmation processes should not be lower than the time required for train integrity confirmation.

TI_P_5 (performance, not safety relevant): The system shall be reconfigurable to reflect the initial actual vehicles consist of the train, any intentional changes should exclude all other vehicles it communicates with from the integrity check.

TI_P_6 (performance, not safety relevant): The target time for the system to complete the initialisation process to establish the network, verify the train consist and establish train integrity will be 1 minute, and the time taken to complete this process shall not exceed 5 minutes.

TI_O_1 (operational): The OTI Control Module shall be configurable to take at least three states: (i) active locomotive/vehicle train is being controlled from and communicating with Signalling Control Centre/traffic management system, (ii) active assisting locomotive/vehicle train is not being controlled from and providing traction power, not (principal) communicating with Signalling Control Centre/traffic management system and (iii) inactive locomotive/vehicle not providing traction power and not communicating with Signalling Control Centre/traffic management system. States will only be changeable in initiation stage, NOT changeable whilst part of consist sending train integrity confirmation.

2.2 HIGH LEVEL FUNCTIONAL ARCHITECTURE FOR OTI

2.2.1 *Preliminary hazard analysis*

ETALON is developing a train integrity check system that must be able to be integrated in a Train Protection System respecting the severe safety requirements currently applied in EU railways.

This means that the train integrity check system developed in ETALON shall be able to be implemented in configurations permitting the achievement of SIL 4 (Safety Integrity Level), according to EN 50126 standard, for the functions allocated to it.

The approach of ETALON is providing a prototype that fully implements the functionality required, even if, in the configuration tested in ETALON project, the safety level will not be proven.

Anyway, by suitable configuration of the systems installed on locomotives and vehicles, it will be possible to achieve the required SIL. This is further discussed in section 3.3 of this document.

The hazards that will affect the train integrity check system belong to different categories:

a) Wrong configuration of the system installed on a train composition, as detected at initialisation before the start of train mission

Hazard Conf1: a vehicle, not belonging to a composition, is erroneously considered as part of it.

In principle, as soon as the train moves, the vehicle erroneously considered part of the consist, will not be detected any more as part of it (exceedance of the distance between nodes). This causes an alert of "lost integrity". Therefore, this hazard has no direct safety critical consequences, but represents a severe availability issue, requesting important operational measures, with consequent impact on traffic and implicitly risks of operational errors during the recovery phase.

Hazard Conf2: a vehicle, belonging to a composition, is erroneously not considered as part of it.

If the vehicle is at the end of consist, the train will systematically report integrity confirmed for a train length shorter than the real one. This will have safety critical consequences for interlocking operation and train spacing.

The system is by default unable to ensure that all train's wagons have been detected; although, as reported in the Functional Requirement TI_OR_3, the train driver is provided with enough information (quantity of wagons detected) to ensure that all wagons have been correctly detected.

> *TI_OR_3 OTI Interface module should enable the driver to alter the parameters of the OTI system (provided requirements of TI_OR_4 are respected);*
>
> *(i) switch system between sending train integrity confirmations (such as when travelling on managed network) and not (such as when dissolving network/consist at end of journey),*
>
> *(ii) initiate network/consist discovery, and*
>
> *(iii) update train formation data (list of vehicles expected in consist).*
>
> *The hazards of this category require mitigation measures based on appropriate specification of initialisation functionality, independently on the adopted configuration of equipment in the final application of the train integrity check system on a train.*

b) Errors in data communication between nodes on vehicles and OTI Control Module on the locomotive

This hazard can affect both the initialisation phase (i.e. act as a cause of hazard Conf1 and Conf2 discussed above) and the operation phase, that is discussed below. According to EN 50159, the hazards that need to be considered are:

Hazards Comm1: corruption, i.e. a message is accepted by the intended receiver, that does not recognise that its content is wrong (bit errors, etc.).

Hazard Comm2: deletion. A message does not reach the intended receiver.

Hazard Comm3: delay. A message reaches the intended receiver after a time greater that the planned one.

Hazard Comm4: repetition. A message reaches the intended receiver more than once.

Hazard Comm5: resequencing. Two or more messages reaches the intended receiver in an order different that the planned one.

Hazard Comm6: insertion. A receiver receives a message intended for another one.

Hazard Comm7: masquerade. It is a special case of Hazard Comm6, where a message is intentionally prepared and inserted by an attacker. This is considered a special case due to the dedicated protection measures required (typically, cryptographic techniques).

Mitigation of above listed hazards requires specific measures in communication protocols (coding against corruption, using time stamps or “tokens” against delayed or repeated messages, managing identities of sender/receivers against insertions, etc.) according to the guidelines of EN 50159.

It is also necessary that the parts of the protocols responsible of managing the measures are implemented (in the final configuration of train integrity check system) in such a way that the required SIL 4 is achieved, with respect to the errors in operation of equipment, as discussed below (see also section 3.3 of this document).

c) Errors in operation of equipment (nodes on vehicles and control Module)

This kind of hazards can affect both the initialisation phase and the operation phase, causing all configuration and communication hazards, and also the hazards listed below.

Hazard Eq1: the Control Module considers valid a train configuration that does not correspond to the real one.

Hazard Eq2: the Control Module confirms integrity even if corresponding information has not been sent by the nodes.

Hazard Eq3: the Control Module confirms integrity on the basis of old information from the nodes.

Hazard Eq4: a node confirms the presence of the next one, even if the conditions (distance, reception of data) are not verified.

Causes and mitigation of these hazards is discussed in Table **4** of this document.

2.2.2 *Operational phase of wagon or train*

Using the power output at a given speed, and the time spent when the vehicle is stationary, the operating states can be combined with power consumption of system components to calculate an overall energy balance. In the table below, there is a summary of a state analysis.

	DORMANT	**IDLE**	**STATIONARY**	**SHUNTING**	**SLOW MOVING**	**MEDIUM SPEED**	**NORMAL SPEED**
	Not loaded, not in a consist	Loaded, not in a consist	In a consist, not moving	Slow, intermittent movement, in a yard	25km/h	50km/h	80km/h
TRAIN INTEGRITY STATE							
Confirmed	Off	Off	Off or only 868MHz communication	Communication only	Communication only	Full function	Full function (max. TI check freq.)
Integrity lost	Off	Off	Full function	Full function	Full function	Full function	Full function
Reforming consist	Off	Off	Full function	Full function	Full function	Full function	Full function
Not active	Off	Off	Off	Listen only	Full function	Full function	Full function
Topology discovery	Off	Off	Full function	Listen only	Full function	Full function	Full function

Table 2 – Summary of Train Integrity state analysis

It is important to consider that when the train moves, vibrations induce currents in the energy harvester, and when these appear at the power supply interface circuitry, EH module can generate an interrupt into the processor to wake it from deep sleep. Separate energy storage (capacitors, supercaps, etc.) can supply enough power to get the system up and running until power output from the harvester increases to a level where it starts to recharge the energy storage and supply full function power requirements for communications and sensing.

If there is no stored energy, the power supply will turn on when there is enough energy in the power storage to sustain volts to the electronics, in which case it all turns on automatically. Careful design is needed to minimise this delay – we can do this by turning off functions when the train is stationary and we still have plenty of energy stored to enable a quick wake up later.

The energy harvester is a coil and magnet connected to a rectifier in the power supply circuit. As soon as it stops moving, the current in the coil collapses into the power supply.

TRAIN STATES Description

- **DORMANT** - wagon waiting to be assigned to a specific use (loaded with containers or equipment), parked indefinitely, unspecified use, empty. The wagons are separated;
- **IDLE** - prepared wagon ready to be assembled with others, assigned to a specific use and loaded;
- **STATIONARY** - wagons belonging to an assembled train, including the locomotive, which is stationary and waiting to be moved;
- **SHUNTING** - wagons moving independently at a very low speed, usually near a station, cargo area or other place where you are travelling at very low speed;
- **SLOW MOVING** – train moving at 25km/h;
- **MEDIUM SPEED** - train moving at 50km/h;
- **NORMAL SPEED** - train moving at 80km/h.

Some key aspects of the different phases of transition from one state to another are described below:

- From IDLE to DORMANT: after 48 hours of inactivity.
- From DORMANT to IDLE: signal generated from the EH to the communication system caused by the slow wagon movement.
- SHUNTING to STATIONARY: no movement, joined consist network.
- From IDLE to STATIONARY: request of topology generation.
- From STATIONARY to IDLE: Lost of network or no incoming request.
- SHUNTING to MOVING: moving more than 25 km/h (if valid distance measurement, join consist network, dynamic topology integration).
- MOVING to STATIONARY: moving less than 25km/h for last 5mins.
- MOVING or STATIONARY to SHUNTING: consist network dissolved by train integrity controller (wagons being redistributed, therefore no current valid network).
- MOVING AT SPEED X -> MOVING AT SPEED Y: detected change in speed.

NODE FUCTIONAL System states:

- Off: System is off – electronics turned off where possible. Motion detection, energy harvester power present wakes the system up. No network connection to maintain.
  - *Power supply to electronics is turned OFF. Consumption reduced to energy storage leakage until fully discharged.*
- Sensors only: Periodic checking for presence of the neighbouring vehicle. Maintain connection with the network, but no transmission of updates. System ready to run when necessary. Minimizes delays between physically assembling wagons and establishing the network topology.
  - *Quiescent state – electronics normally in the minimum power consumption state, with the real time clock (RTC) powered. At the correct interval, the RTC generates an interrupt that wakes up the microprocessor, which then checks the local status and*

turns the sensors on to check for local vehicle presence. If no vehicle present, returns to quiescent state for another interval. If a vehicle is present, it could turn on the radio to look for a communications network.

- Communication only: No sensor function, regular updates returned to the network. Slow response time permits detection of train integrity using radio RSSI and message rates without energy use on distance measurements.
  - *Quiescent state – electronics normally in the minimum possible power state, with the RTC generating an interrupt to start the microprocessor to look for a network at a set interval.*
  - *Active state - the pattern of wake intervals, time spent listening for a network synchronisation pulse, determines the time taken to identify a network and the power required to perform the search. i.e., if the radio is on and listening for a time as long as the network synchronisation interval, it will take one cycle to find the network. If it is only on for 1% of the time, it may take 100x the network synchronisation time to find the network. During this time only the radio and microprocessor are on.*
- Full function: Sensors maintain a record of inter-vehicle distance. Updates transmitted at the rate required by the vehicle speed.
  - *Quiescent state – electronics normally in minimum power consumption state, with the RTC wake up interval set to the shortest necessary for maximum performance of train integrity.*
  - *Active state – sensors and communications functions fully powered to report separation distance at the required interval.*

2.2.3 *Overall system operation*

Operation of train integrity check system can be subdivided in two phases:

a) System initialisation and configuration.

In this phase, before start of train mission, the Control Module collects and checks information on the identities of vehicles belonging to the composition.

According to the preliminary hazard analysis, it is important that in this phase all vehicles belonging to the composition are recognised (safety critical) and that no inappropriate vehicle is taken into consideration (availability critical).

This means that all nodes installed on vehicles must have a unique identity. To ensure safety and availability, the Control Module should be informed about the list of identities belonging to the composition, to perform appropriate checks.

b) Check of integrity during train mission.

Upon request coming from the Control Module (i.e. a “token” that is propagated and returned along the train composition) all nodes confirm their presence at a distance from the next one within the specified range. In figure n. 1 is described the typical composition of the On-board Train Integrity architecture. All the OTI nodes are identical, so that the Control Module can be placed in any position within the railway convoy (both in the passenger service and the freight service).

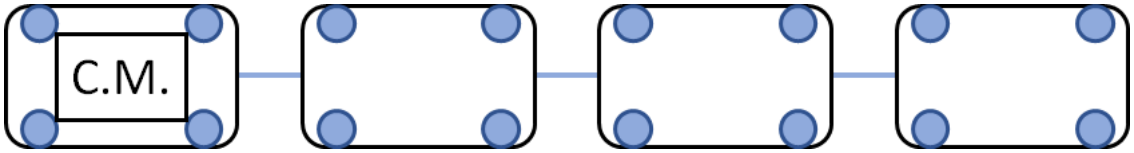

Figure 1 – Overview of the OTI nodes installed on four consecutive wagons
(with the leading unit placed on the left)

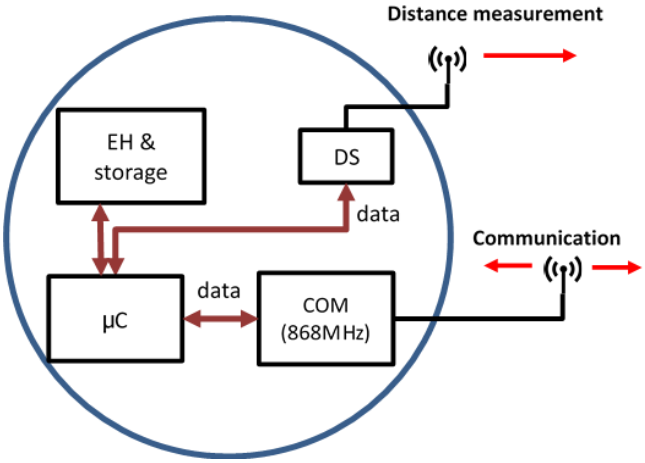

Figure 2 – On-board Train Integrity device’s architecture

2.3 OTI NODE FUNCTIONAL ARCHITECTURE

The On-Board Train Integrity monitoring solution is based on monitoring the inter-wagon distance, by acknowledging all the wagon-to-wagon distance. The solution is able to locate the whole train's length.

In order to perform such monitoring, the architecture is based on placing a certain quantity of nodes per wagon. In the use case scenario, each wagon will be equipped with four OTI nodes, but this is scalable at least up to eight, since each wagon is composed by four axles and each axle can mount up to two devices, one for each end of the latter.

The architecture is capable of communication between nodes through a sub-GHz communication link, while the distance between wagons is measured as the distance between adjacent nodes on the same side of the train. The distance measurement employs UWB (Ultra-Wide Band) technology, based on very high frequency and very short time impulses, the central frequency is in the range of 3 to 10 GHz with a large bandwidth higher than 500 MHz For the use case scenario, a module with a central band of 6.5 GHz and a band of 500 MHz is employed.

Both the sub-GHz and the UWB modules are based on radio communication, but on different frequencies. In order to exploit the functionalities provided by the modules, two separate antennas will be allocated for the OTI node (one for each radio module).

The UWB-antenna identified for this project is a tapered slot antenna since offers a wide band along with a directional pattern. The reason we chosen this type of antenna is that most of UWB built-in antennas provide an almost omnidirectional pattern, thus often unreliable to communicate over long-distances and/or throughout a fading channel. The description of the proposed antenna is discussed in section 2.3.6.

The proposed antenna for the sub-GHz communication system is an axial mode helical antenna which will substitute the current state-of-the-art wire antenna. The axial mode helical antenna will ensure better performance compared to the existing one, while maintaining the same dimension. In particular, the design is optimized to get the maxim radiation directivity in one direction (no loss of radiated energy). Thanks to the higher antenna directivity the communication system (i.e. radio) reaches longer communication distances and/or lower the transmit power which, in turn, reduce the overall consumption. An accurate description is reported in section 2.3.7.

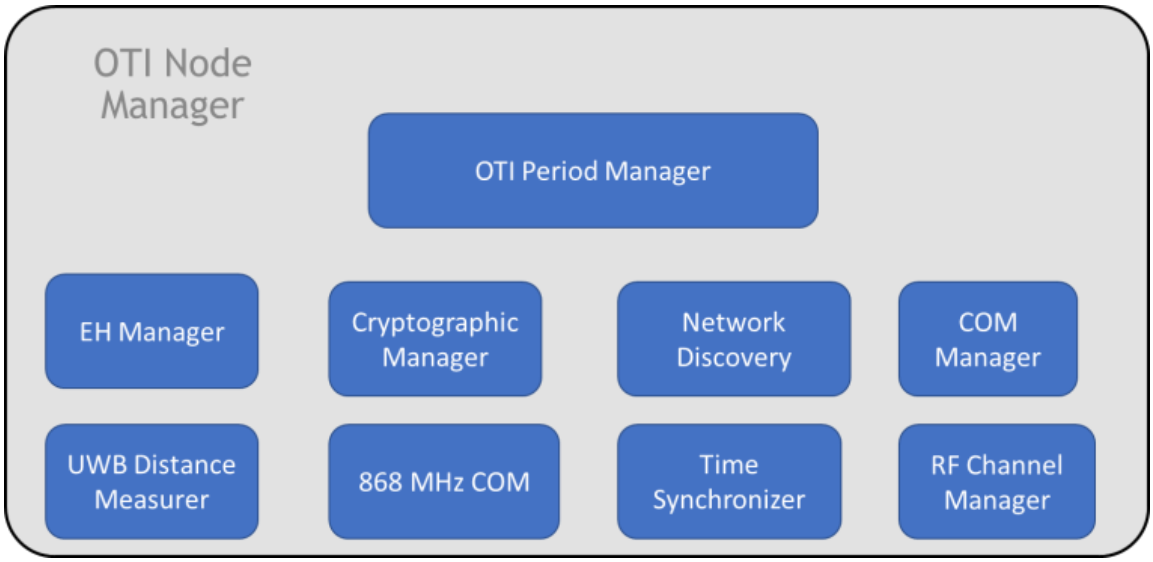

Figure 3 – On-board Train Integrity module configuration

Communication must also respect the high availability standard for communication. This shall contribute to make it extremely rare that a loss of communication is the actual cause of loss of integrity detection. To achieve high availability of communication the antenna design will be choose by the ones with high gain and robustness. Furthermore at each side of the wagon will be placed two identical OTI node (to double the possibility of communication) to improve the availability of the system.

Availability of communication has always be considered in conjunction with other features of the systems allowing it to provide reliable information about train integrity status (in other words: high availability of communication shall not be the only countermeasure for missed detection of train integrity loss).

2.3.1 OTI Period Manager

This module is in charge of managing the correct TI (Train Integrity) frequency checking. The module receives the TI frequency information through the 868 MHz COM module, initialised by the Control Module. Once the frequency is correctly set, the module interacts with the UWB Distance Measurer to correctly check the TI. This module is mainly composed by a clock-based timer that counts the required time until the next TI check time elapses. The clock will continue to be functional even if the module enters a low power mode.

2.3.2 EH Manager

A vibration energy harvester system includes three major components.

The energy harvester, which simply generates electrical energy when vibration is present (starting from a train speed around 15kph). This uses a magnet suspended on a spring to induce current in a coil, which is fixed. The resonant frequency determined by the mass of the magnet and the strength of the spring is designed to match the normal driven frequency of the vibration source, or in the case of a train axle box, a convenient frequency range where substantial vibration is available even at low speeds. For a train this is around 60-70Hz.

The power regulator, which converts the alternating power output (from a coil and magnet, voltage from 1.5V up to 15V or more) into a usable direct current at a convenient voltage (for example, 3.6V is common for many super capacitors and rechargeable batteries).

Energy storage, which must meet competing requirements of cost, usable life, capacity, size, robustness (vibration and temperature ranges can be quite harsh) leakage, output voltage stability (how far does it drop at low temperatures) input and output current limits (how much current is required by the electronics, and how much current can be generated by the harvester). Determining the optimal size for energy storage can only be achieved once the communications (and sensing in this case) power requirements has been established. This will become possible when the data density (packet size, frequency and range) has been established. If the energy storage is oversized it can drive prices high, if it is undersized the system may become unreliable. The amount of energy stored, and the level of activity permitted by the electronics must be carefully managed to ensure that if the vehicle is stationary for a pre-determined period of time, the system will always be capable of maintaining the network or waking up and reforming the network in a guaranteed time limit. This stored capacity must be available under all specified ranges of temperature. Voltage from electrical storage devices tends to drop at low temperature, and leakage increases at high temperature, leading to premature discharge.

2.3.3 Cryptographic Manager

In order to ensure security in the communication between OTI nodes and with the Control Module, the architecture must ensure the three security aspects of:

- Data confidentiality
- Data integrity
- Data availability

Data confidentiality is ensured by data encryption. Nodes will communicate using packets processed by an encryption algorithm. Each architecture will first of all use a private-public (asymmetric key) encryption for the encryption key distribution such as RSA (Rivest–Shamir–Adleman). Once all the nodes are provided with the key, messages will be encrypted using a symmetric key encryption algorithm (such as AES “Advanced Encryption Standard”).

During the first phase of key distribution, each node will generate its own public-private key pairs for the asymmetric encrypted communication. Using this communication link, the key is securely distributed between all the nodes. Once the key is known by all the nodes, communication packets will be sent using symmetric encryption making use of the distributed key.

In order to ensure data integrity, each packet must also contain an integrity meta-data check, this will ensure that data is not compromised or damaged by hostile attempts or by environment disruption. Packets will be sent using error checking methods such as CRC (Cyclic Redundancy Check) or hash functions such as SHA (Secure Hash Algorithm) or MD5.

The Cryptographic Manager module covers all these security aspects. The module is in charge of processing the data before re-transmission, while, regarding incoming messages, the module will process the data before it is passed to the rest of the OTI node architecture.

The Cryptographic Manager module is compliant to EN50159 (see references [1]).

Cryptographic keys are periodically updated to minimize and prevent the system from any long time attack that aims at cracking the current key.

2.3.4 Network Discovery

At first boot, the device does not have the knowledge of the other surrounding devices to whom it shall communicate. This module has the duty of generating the network topology that will afterwards be employed for communication. The module will communicate with the UWB Distance Measurer in order to discover devices mounted on adjacent wagons. It will also employ the COM Manager to pass on communication data. Once the node has been associated to the network, the module will not be employed until the node needs to be re-associated to the same or another network.

2.3.5 COM Manager

The COM Manager module has the role of managing the networking layer for the communication. The module also provides the node identifier and provides the routing management in order to correctly find the path and communicate to the next device. The module also manages different possible paths in the event that some nodes fail, this means that the communication is not bound to a single path, but a message starting from the Control Module towards the tail of the train (or vice versa) can pass through many paths. In the case that the latter event occurs, the module should also provide details of the failed communication attempts.

2.3.6 UWB Distance Measurer

In order to check TI, a device to check distance between devices has been employed. This duty is covered by the UWB Distance Measurer. The module employs UWB technology to correctly measure the distance between UWB devices. The module provides a software abstraction layer

through which it is possible to interact with the module. Each OTI Node has a unique identifier that describes with respect to which OTI node the distance measurement should be performed.

2.3.7 868 MHz COM

This module is in charge of interfacing the device with the main communication interface in order to be able to establish data transactions with other devices. The module is in charge of managing the 868 MHz radio chip, providing an abstraction interaction layer for the other modules that require the communication routine.

2.3.8 Time Synchronizer

To correctly establish communication between devices, data transactions for the various devices must not overlap. The Time Synchronizer covers the role of synchronizing data using Time Division Multiple Access (TDMA). This avoids inter device interference and potential packet drops that could occur.

2.3.9 RF Channel Manager

To increase data throughput without overlapping data transactions, multiple channels are employed in the architecture, since the 868 MHz communication offer various channels in the bandwidth. The Radio Frequency (RF) Channel Manager covers the role of correctly selecting the wanted communication channel for the data transaction. The module interacts with the 868 MHz COM in order to correctly select the transmission frequency.

2.4 CONTROL MODULE FUNCTIONAL ARCHITECTURE

2.4.1 Control Module

The OTI Control Module is located on the train's leading unit. It acts as the main wireless communication network controller. The module is responsible for initializing the OTI network, to perform requests towards the OTI network and to retrieve data from the train's on-board instrumentation.

The control Module is composed of two independent computational units that perform the same tasks. If at least one unit doesn't confirm train integrity then the train integrity function will not be confirmed.

The first phase that the Control Module performs is the OTI Network formation. It is reminded that the Control Module knowledges the existence of the four OTI nodes on the leading unit and how to communicate towards them. A request is then sent to the OTI nodes that belong to the train's leading unit. The OTI nodes will then search the other OTI nodes that belong to the next wagon, thanks to the OTI Node UWB Distance Measurer Module. The request continues to travel along the train (from the leading unit down to the train's tail) up to the end when no more OTI nodes are found.

Once all OTI nodes have been discovered, the network can now be generated, a unique ID is associated to each OTI Node. The Control Module will retrieve the information of speed by the train's on-board instrumentation, so that it is capable of identifying the correct timing to query OTI checks down the OTI network (faster, if the train speed is high and slower when the train speed is low).

The integrity status of the train is then reported by the OTI Control Module through some typology of HMI (display, sound, lights, etc.). The first phase of network initialization will be initialized by the interaction with a button by the loco-pilot.

All the outlined performed operations are performed using a secure communication link generated thanks to the Cryptographic Manager.

Control Module receives from the nodes the unique ID (that identified each node) and other diagnostic information (distance, speed, SNR, failures, etc.). It elaborates the received data from the nodes to achieve the list of all the devices that belong to the same convoy. To achieve this, it also compare the distance between the nodes (by using UWB distance measurer) to avoid that wrong nodes are linked to the convoy.

Main device is linked to the Train Protection System (TPS) using the same communication bus. Main device is composed by a motherboard with two different computational unit completed with all the functional peripherals needed to connect it to the train bus according to ERA SUBSET-119 (ref. [16]).

Software developed for the Control Module has to be as close as possible to MISRA C rules and is at least completed with the following applications:

- routine application

- train integrity application

- security enhancements token generation application

- security encryption generation application

- communication and data collecting & formatting application

- storage nodes database

- log messages database (status info, warning and alarm messages).

The OTI Control Module is responsible of the following functions:

- Initialization
- Confirmation of Integrity
- Managing interfaces with other train systems
- Monitoring and diagnostic

Each functionality is in detail described in the next pages.

1- Initialisation

Initialisation is activated by the Control Module (upon a request via HMI coming from the train driver). The Control Module sends an “initialization token” (to be propagated and returned along the train composition) and expects that each node returns its identity together with the token, within a programmable time.

The Control Module checks that all expected nodes[1] has correctly reported their identity and that no unwanted node is connected.

The Control Module reports the outcome of initialisation to the Train Protection System (e.g. “OK” or “ID x missing”, “unwanted ID y connected”, etc.).

Note: if the Control Module informs the nodes, sending the expected list of nodes IDs, this will avoid uncertainties in case of initialisation of a train standing close to another one, where it could be difficult for a node to discriminate the right next one (more than one node within the distance range). This means that a node only accepts connection with a node within the distance range and if the identify corresponds to the next node announced by the control module. If there is an error in the list of node identities and this node is on a wagon not attached to the train, as soon as the train starts, integrity will be lost (no safety issue, only availability). If the last node, that should not find any next node,

[1] It seems necessary that the Signalling Control Centre has a list of expected IDs. If the approach of a completely automatic configuration is followed, there will be the risk of a not working node (e.g. because no power available) that will not therefore be detectable, limiting the composition of the train to the first vehicles (shorter than the real one).

finds a node within the distance, this is reported as an alert (because an additional wagon could be attached to the train and not indicated in the train configuration).

It could however be advantageous that the Control Module always reports by showing in the lcd screen (or something like this) the list of “detected IDs” (ad not only “OK”) to allow operators to perform a further cross check, to protect even against the case of a list of IDs communicated to the system, where the ID of the last wagon is missing and the node on this wagon is not working - this would cause the Hazard Conf2 – “a vehicle, belonging to a composition, is erroneously not considered as part of it”. In fact errors in the ID list are the same that occur when a wagon is attached to a train, forgetting the connection of the brake pipe. These errors are not specific of the train integrity check system, but some protection against them should anyway be offered.

2- Confirmation of Integrity

Integrity check is performed cyclically or upon request, according to commands from the Train Protection System.

The Control Module generates a “confirmation token” different for each check (see safety considerations and protection against delayed and repeated messages as described at page n. 14) that is propagated and returned along the train composition (note: a node returns the token, together with its identity, only if the measured distance from the next node is within a given distance).

The Control Module confirms the integrity to the Train Protection System only if all nodes have returned the token, otherwise it sends appropriate diagnostic information (e.g. which node is missing).

The Control Module shall be able to handle intermittent loss of train integrity by without requiring driver to confirm train integrity (if this is possible)[2].

The Control Module shall provide information to Train Management System or other equipment dedicated to management of train (on-board CCS excluded).

The Control Module shall perform a diagnostic check of the overall system in order to detect potential malfunctions which could lead to no detection or undue detection.

3- Managing interfaces with other train systems

[2] Justification: ETCS specifications allow driver to confirm train integrity and provide a specific value of the relevant variable; since some kind of train sets allow provide driver alternative means to ascertain whether a vehicle has been lost or not. This represents a valuable fallback option when handling intermittent loss of integrity. The probability of undue reaction caused by temporary missed communication among detectors is reduced.

The Control Module shall have an interface with the On-board Unit computational unit (vital computer). It shall be able to interact with the Control Module directly by the train driver (through HMI) or by interfacing with the On-board instrumentation. Interaction with the Control Module consists in the request of network topology generation and validation of the latter.

The OTI Control Module sends integrity checks results and diagnostic information to the On-board Unit (vital computer) and on an HMI integrated on the Control Module itself. The HMI should display on the screen:

- the total number of Train Integrity checks completed from the start of the journey

The On-board Unit should obtain some information on-demand:

- the total hours of operation of each OTI device;
- OTI nodes alert messages (communication problem, harvesting failure, low battery level, etc.);
- OTI nodes status information (communication signal strength, harvesting system status, CPU load, link with previous and following wagon, battery level, etc.).

Note: at the initialisation phase the OTI Control Module doesn't have and does not require the list of expected IDs of the OTI nodes in the consist. According to the overall communication system installed on the train, the identification of each OTI node is performed during the topology generation phase, during which each node will be assigned with a unique ID. This information shall then be reported to the On-board instrumentation.

It is therefore advisable that the SW of OTI Control Module is designed in a way that at least one interface is possible according to ERA SUBSET-119 (ref. [16]).

4- Monitoring and diagnostic

Collecting tokens returned by the nodes, the OTI Control Module can inform the Train Protection System when one of them is not answering or not well performing (e.g. data link low signal, cpu high usage, energy harvesting faulty, etc.).

If nodes are able to detect the state of low power and report it to the OTI Control Module, also information about possible outages due to energy harvesting can be anticipated to take to opportune countermeasures (e.g. replace the faulty devices) informing the maintenance staff about it.

2.5 HIGH LEVEL FUNCTIONAL ARCHITECTURE FOR TRACK SIDE

Etalon aims to architect the best solution for energy harvesting the communication system used by the trackside to operate with the Interlocking. Etalon will investigate also the next generation communication system between the smart devices as level barriers, switch, signals and the objects controllers to avoid the use of wired communication.

The economic modelling for the energy harvesting trackside points to use the vibrations as the main power generator used to power the modem.

To achieve to the desired system architecture it's profitable to check for the list of Functional Requirement defined in deliverable D.2.1.

TEH_Definition: Trackside Energy Harvester is a device that provides locally generated energy to power object controller wireless communications system.

TEH_Function: To harvest and store energy derived from the local railway environment to provide a continuous reliable energy source to meet the power requirements of the object controller functionalities and wireless communications.

TEH_Functional Definition: Unit able to collect energy while installed near tracks. The unit, including energy storage, operates (provides power to connected devices) possibly with different efficiency, in all conditions during the entire day.

OCWC_Definition: The Object Controller Wireless Communications is a device or module which provides communications between the Object Controller and the Signalling Control Centre, between the Object Controller and track–side objects when these are installed separately and potentially between neighbour object controllers where necessary.

OCWC_Function: Provides wireless communications capability to enable the Object Controller to communicate wirelessly with the Signalling Control Centre, other object controllers and track–side objects.

OCWC_Functional Definition: A device able to provide wireless communications capability for following interfaces: Signalling Control Centre (interlocking) – object controller – trackside object; object controller – neighbour object controller.

As the safety related functions of object controller (which shall be SIL4 system) are out of the scope of the present document, therefore no Top Hazard is assigned for TEH.

The possible hazardous consequences of communication failure shall be treated and mitigated by the end devices (e.g. interlocking and/or own object controller).

However, achieving high availability is important (see corresponding requirements below) since prolonged operation in degraded modes can decrease the average safety level of the system and

the loss of communication with object controllers must be safely managed by the Signalling Control Centre and not lead to an accident.

Requirements related to the Object Controller Wayside Communication

OCWC_FN_1: It shall be possible to establish the centre – trackside communications when it is required by Signalling Control Centre with defined availability.

OCWC_FN_2: The Signalling Control Centre – trackside communications shall be continuously supervised confirming the availability to perform the required function at defined period of time.

OCWC_FN_3: The loss of communication between Signalling Control Centre and trackside shall be detected.

OCWC_FN_4: The wireless communication system should be suitable for the communication of safety critical commands and information and safeguard against intrusion.

OCWC_FS_5: The possible perturbations, interferences or attenuation of signal, shall be taken in account.

OCWC_P_1: The OCWC shall comply with QoS parameters defined for Signalling Control Centre – trackside communications (e.g., latency, throughput, etc.).

OCWC_P_2: The OCWC shall have sufficient reliable communication range (with minimal power usage) to assure Signalling Control Centre – trackside communications to perform the required function at defined period of time.

OCWC_P_3: The wireless communication system should have sufficient capacity to transfer all of the required commands and data within a required time period.

OCWC_P_4: The time for the wireless communication system to send an individual message/data packet through the communication network should be minimised (although also considering power consumption) and be suitable for the attainment of response times suitable for railway signalling systems and traffic control.

TEH_FN_1: The TEH shall provide the power when it is required by OCWC with defined availability.

TEH_FN_2: The power state of TEH shall be continuously supervised confirming the availability to provide the necessary amount of power at defined period of time.

TEH_FN_3: If the power state reaches a threshold level a small margin above the minimum required for the system to operate for a short period of time a message/alert should be sent to the Signalling Control Centre (or the Signalling Control Centre should create the message/alert based on the power state data).

TEH_FN_4: If the power state reaches the minimum threshold state required for the system to operate, the system shall enter a safe state (and deny requests to change state which it does not have enough energy attain).

TEH_P_1: The amount of power provided shall be enough to support the bidirectional Signalling Control Centre – trackside communications with defined range during the duration of mission.

Requirements related to the Trackside Energy Harvesting

TEH_FS_1: The powering configuration of TEH will correspond to uninterruptible local power supply.

TEH_FS_2: The TEH shall provide the functions of protection, power conversion and back–up.

TEH_FS_3: The voltage and power requirements shall be defined for each TEH unit. The values shall satisfy OCWC demand.

TEH_FS_4: The type of current (AC or DC) shall be defined for each TEH unit. The type shall correspond to OCWC requirement.

TEH_FS_5: when several OCWC are implemented in one area close together, it may be cost effective to centralize their power supply in a cluster powering architecture.

TEH_FS_6: the TEH could be integrated with the OCWC or be installed separately and connected to one or several OCWC by wires.

TEH_FS_7: the operating status of TEH and possibly back–up equipment (battery) shall be known to the Signalling Control Centre to enable appropriate maintenance to be carried out.

TEH_FS_8: the TEH shall be able to report its operating status under request at least, but not limited to “no faults”, “fault” and “too low power”.

TEH_FS_9: the TEH shall be able to report failure events which have to be controlled and the resulting alarms which must be communicated to Signalling Control Centre (e.g. “loss of input power”, “power module 1 failure [in case of redundancy]”, “monitoring unit alarm/fault”, “battery voltage too low”, “battery alarm/battery end of life”).

TEH_P_1: The energy harvesting system shall be sized to provide an average output greater than the average consumption of the devices powered by it.

TEH_P_2: The energy discharge rate from energy storage system should be sufficient to meet the maximum instantaneous energy consumption of the device(s) being powered by the system.

TEH_P_3: The energy discharge rate from energy storage system shall be sufficient to assure the discharging rate during the whole estimated service life of the device (defined for the average operating temperature).

TEH_P_4: The energy discharge rate from energy storage system shall be sufficient to assure the discharging rate the discharging rate at the minimum operating temperature.

TEH_P_5: The storage capacity of the energy storage system should be sized to ensure the required energy output to the system powered by it, despite of fluctuations in the energy input from the harvester.

TEH_P_6: To cover consumption peaks, the TEH can be completed by a local battery which provides an additional power source in operation (discharge) when the traffic increases and stores the locally derived power (in charge) when the powering is sufficient.

TEH_P_7: The minimum energy reserve required over any OCWC shall be defined.

TEH_P_8: The battery (when implemented) shall be sized to provide continuity of supply in case of increased operational load or during the existence of unfavourable conditions for energy harvesting (e.g. low train traffic for vibration/displacement harvester).

TEH_P_9: The autonomy of the battery (when implemented) and the minimum service life of the battery for the back–up power shall be defined for each specific application.

TEH_P_10: The TEH operating in back–up mode shall guarantee normal operation of the OCWC during the autonomy time for a discharge at a constant power level.

TEH_P_11: The TEH and OCWC shall remain in sleeping mode when idle.

TEH_P_12: In case of overproduction of energy it shall be stored by energy storage system.

Comments

Regarding TEH_P_7, when the TEH find itself below the minimum energy reserve required, the alarm (e.g. “too low power”) shall be produced (as per TEH_FS_9). In this case the device status will be treated by the Signalling Control Centre in the same way as “communication loss”.

The safe state should not contradict the previously communicated safe state of the system. That is, the system should not change from one state to another automatically when there is loss of communication or low power event.

If the design of the field element is such that on confirming it is in a safe sate it can be relied on to remain in that state, AND no command to change state has been issued, it might be possible for the Signalling Control Centre to consider the field element to be in a safe state if this is considered appropriate based on a case by case risk assessment.

Regarding OCWC_P_3: the system could be scalable, using different optimisations for high and low communications traffic applications (e.g. if in a particular application an object controller communicated with 20 devices or 4, the power usage optimization and power supply could be altered to suit the application).

Regarding OCWC_P_4: the time taken for communications to pass through the communications network to the destination affects the response times for field elements to receive commands or status requests and respond. This time can be taken into account by the Signalling Control Centre, but for efficient operation it should be as short as reasonable possible.

3. SYSTEM REQUIREMENTS SPECIFICATION FOR THE ON-BOARD TRAIN INTEGRITY SOLUTION

3.1 OTI NODE

The OTI node is identified as a device that has the capability of belonging to a WSN aimed at checking the integrity of the train it is mounted on and being powered by an EH power source.

A group of OTI nodes form a network that has the capability of monitoring the integrity of a train. The system shall be able to confirm the integrity of a train, according to the criteria already outlined in Section 2.1 that refer to D2.1.

3.1.1 General requirements for all modules

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_Definition: “train integrity” means that the whole train is behaving (both when at standstill and when moving) as a single consist whose length remains within known limits.	TI_SR_Definition: The TI WSN must be capable of identifying all wagons that belong to the consist and characterize the status of the train at all time, meaning that each module must be available and cover the corresponding function at any time.
TI_Function: Train integrity confirmation function is responsible to collect, evaluate and send to other train movement supervision functions of the Signalling Control Center updated information about the integrity state (confirmed or not confirmed) of the train.	TI_SR_Function: Each pair of OTI nodes that belong to two adjacent wagons must be capable of measuring the distance between them and report the status of the coupling to the Control Module.
TI_TH: train integrity inappropriately sent a “confirmed” status to the other train movement supervision functions of the Signalling Control Center, when that is not the case, or it cannot certainly be determined to be the case.	TI_SR_TH: Each time a TI check is performed through distance measurement, redundancy must be employed to minimize false positives. Two pair of nodes check the coupling status simultaneously (node redundancy), distance measurement shall be performed multiple times before accepting the result (distance measurement redundancy).

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_RAC: According to the usual principles of railway safety related to Risk Acceptance Criteria (RAC) the Tolerable Hazard Rate (THR) for the occurrence of the "top hazard" TI_TH shall be the one corresponding to SIL 4, i.e. 10^{-9} h-1.	TI_SR_RAC: Both the system network and the single OTI nodes implement redundancy in the operations and in the employed hardware.
TI_FS_1: (safety relevant): Integrity shall be considered not confirmed when the distance between two adjacent vehicles exceeds a specific reference distance by a limit value (to be specified according to hazard analysis and system design).	TI_SR_FS_1: A coupling shall be considered not connected (TI not confirmed) whenever at least one OTI node reports a distance measurement over the defined threshold between two OTI nodes that are monitoring a coupling status.
TI_FS_2 (safety relevant): Integrity shall be considered not confirmed when there are insuficient communication nodes responding to support a communication network that includes the whole length of the train.	TI_SR_FS_2: In order to correctly report TI, the status of all couplings must be reported. If one or more coupling status are not reported, TI shall be considered not confirmed.
TI_FS_3 (safety relevant): Integrity shall be considered not confirmed when insufficient communication nodes remain associated with the convoy for train integrity to be proven (and communication nodes which lose association with the convoy will generate an allert).	Requirement covered by TI_SR_FS_2.
TI_FS_4 (safety relevant): Integrity shall be considered not confirmed when the network can not complete data transfer to establish train integrity for all vehicles or the data is incomplete.	TI_SR_FS_3: Integrity shall be considered not confirmed if the Control Module does not receive a response, within the given time, by the network of the status of the couplings.
TI_FS_5 (safety relevant): Integrity shall be considered not confirmed when the distance between two adjacent vehicles cannot be evaluated.	TI_SR_FS_4: A coupling shall be considered not connected (TI not confirmed) whenever both the OTI nodes that monitor the coupling are unable to measure the distance.

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_FS_6 (safety relevant): Integrity shall be confirmed only at the end of a check proving that, within a configurable time period, all distances between adjacent vehicles do not exceed the limit value.	TI_SR_FS_5: TI shall be considered confirmed if at least one OTI nodes for all couplings confirm the integrity of the latter coupling and the Control Module receive the data within the given time.
TI_FS_7 (safety relevant): If the check starts at time t_s and ends at time t_f, the confirmation of integrity shall be referred to time t_s.	TI_SR_FS_6: The Control Module shall confirm train integrity only if the status of all the coupling is reported within a time t_f.
TI_FS_8 (safety relevant): If for an unknown reason, the integrity check starts but the process is interrupted, then the integrity check will be not confirmed.	TI_SR_FS_7: In case at least one coupling integrity check process is interrupted by all the OTI nodes that are monitoring the latter coupling, then TI shall be considered not confirmed.
TI_FN_1 (not safety relevant): It shall be possible to implement cyclic train integrity confirmation (with configurable time period) or confirmation on-demand by the external user functionality (on-board train protection functions).	TI_SR_FN_1: The CM shall be able of requesting TI checks with variable periods and shall also be able to initialize a TI check by an external request (through HMI).
TI_P_1 (performance, not safety relevant): It shall be possible to configure the acceptable duration of the train integrity confirmation process.	TI_SR_P_1: The TI check process shall require the minimum delay possible for checking all the couplings status.
TI_P_2 (performance, not safety relevant): The time for a single instance train integrity confirmation process to complete should be as short as possible, there should be a maximum time limit for the process which should be configurable and established during train integrity function initialisation. If a train integrity confirmation cannot be completed within the time limit the train integrity status will be considered as “not confirmed”.	TI_SR_P_2: TI check shall require less time than the smallest TI check period, meaning also that a TI check cannot be performed before having the result of the previous check.

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_P_3 (performance, not safety relevant): The time between consecutive train integrity confirmation processes should be configurable according to the train speed, and the category of route. The moving block of the traffic management system and the required line capacity should be considered (according to hazard analysis and system design).	TI_SR_P_3: The CM shall be capable of scheduling TI check processes based on the train's speed, meaning that for higher a higher speed the TI check must be more frequent (smaller period).
TI_P_4 (performance, not safety relevant): The time between consecutive train integrity confirmation processes should not be lower than the time required for train integrity confirmation.	Requirement covered by TI_SR_P_2.
TI_P_5 (performance, not safety relevant): The network controller should be able to compare a list of wagons it should have in the train with the list of wagons in the network that have joined automatically, and reject any wagons that should not be in this train.	
TI_O_1 (operational): The OTI Control Module shall be configurable to take at least three states: • active locomotive/vehicle train is being controlled from and communicating with Signalling Control Centre/traffic management system; • active assisting locomotive/vehicle train is not being controlled from and providing traction power, not (principal) communicating with Signalling Control Centre/traffic management system; • inactive locomotive/vehicle not providing traction power and not communicating with Signalling Control Centre/traffic management system. States will only be changeable in initiation stage, NOT changeable whilst part of consist sending train integrity confirmation.	TI_SR_O_1 (operation): The OTI Control Module shall have two functional states: (i) Active CM: Control Module mounted on the leading locomotive that also provides traction power (ii) Passive CM: Control Module mounted on a NON leading locomotive that might be providing traction power or not. The CM can differentiate the two states by the topology request incoming. Whereas the Active CM will be identified as the one that perform the topology request.

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_E_1 (climate - immunity): The train integrity confirmation system shall operate in the railway environment. All pieces of equipment constituting the system should be able to operate with full nominal performance in relation to the following environmental conditions: 1. Temperature 2. Humidity 3. Rain 4. Snow 5. Exposure to sun 6. Air pressure 7. Altitude	Both OTI nodes and CM must respect the following Environmental & Export Classifications: Temperature operation: from -40 °C to +85°C Humidity: MSL 3 (Moisture Sensitivity Level) compliant to the railway operability EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.
TI_E_2 (vibrations): The train integrity confirmation system shall operate in the environment of railways, both passenger and freight services. The system shall be demonstrated as being able to operate within conditions representative of the railway environment, it shall be suitable for operation with full nominal performance in relation to environmental and vibration conditions either directly or with further ruggedization and development.	TI_SR_2: All components that are integrated in the OTI Node and in the CM must be compliant to the railway operability EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.
TI_E_3: Immunity characteristics of equipment related to environmental conditions and shock/vibrations shall be specified making referring to recognized standards for railway applications.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_E_4 (electromagnetic compatibility - immunity and emissions): The train integrity confirmation system shall operate in the railway environment, where the following traction power supply might be present: 1. 25 kV AC, 50 Hz 2. 15 kV AC, 16 2/3 Hz 3. 3000 VDC 4. 1500 VDC 5. 750 VDC The system should also be immune to, and not interfere with, domestic and industrial power supply and communication systems, which effects are present in the railway environment.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”. EN 61373 for electrical (EMC), vibration qualification and testing respectively.
TI_E_5: Immunity and emission characteristics of equipment related to electromagnetic interferences shall be specified referring to recognised standards for railway applications.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.
TI_E_6: In case of difficulties for the design and manufacturing of equipment, classes of compatibility should be defined; each covering well defined application cases.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.
TI_E_7: Design of equipment shall permit the check of compatibility with laboratory tests.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.
TI_E_8: Equipment constituting the train integrity confirmation system shall not use materials that may be dangerous for the environment and that may be lost during operation, including degraded and accident conditions.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.

FUNCTIONAL REQUIREMENTS	SYSTEM REQUIREMENTS
TI_E_9 (fire): Equipment constituting the train integrity confirmation system shall comply with standards relevant to fire propagation (EN 45545 - railway applications, fire protection on railway vehicles).	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.
TI_E_10 (toxic emissions): Equipment constituting the train integrity confirmation system shall comply with standards relevant to toxic emissions.	Compliant to the railway operability: EN50155:2017 “Railway Applications. Rolling Stock. Electronic Equipment”.

Table 3 – General requirements for all the nodes

3.1.2 Environment

SR_ENV_1: The modules shall withstand the environmental conditions defined in this Section without performance reduction:

a. Low Pressure — 57.2kPa = 0.572 bar

b. Low Temperature — Storage: -40°; Operation: -40° for components, -35° for modules

c. High Temperature — Storage: +71°; Operation: +85° for components, +65° for modules

d. Solar Radiation — 1120 W/m^2

e. Humidity — 95%

f. Salt Fog — 240h salt fog exposure

g. Sand and Dust — Particle size < 150um, concentration 10.6g/m^3

h. Leakage/Immersion — 1m depth for 30min

i. Wind load — up to 90km/h for 1h

j. Snow/ice — up to 68kg/m^2 for 4h

k. Vibration — Axle mounted: Vertical: 144m/s^2 RMS, Transverse: 129m/s^2 RMS, Longitudinal: 64.3m/s^2 RMS: 5 hours (EN61373:2010)

l.	Shock	Axle mounted: 1000m/s^2 for 6ms (EN61373:2010), 3 axes, 3 shocks in both directions on each axis
m.	Electrostatic Discharges	4kV contact and 8kV air as described in IEC 61000-4-2 without damage and performance reduction needed for CE mark

3.1.3 Distance Sensor

SR_DS_1: The DS module shall be capable of measure a distance up to 15 meters (with an maximum error +/- 5 meters) to ensure that integrity is actually lost and not that the module is unable of measuring the distance.

SR_DS_2: The DS module must present one or more interfaces for exposing the APIs for the Microcontroller unit.

SR_DS_3: The DS module shall be able of performing a measurement under 1 second, in order to not introduce a delay that will confirm integrity lost due to timeout.

3.1.4 Microcontroller

SR_MU_1: The Microcontroller unit must present one or more interfaces suitable for communicating with the other modules.

SR_MU_2: The Microcontroller unit shall be capable of managing an ad-hoc communication protocol stack for a WSN.

SR_MU_3: The Microcontroller unit shall be compliant to very low power consumption computing and capable of being powered by an EH solution.

3.1.5 Communication module

SR_COM_1: The Communication module must present one or more interfaces suitable for communicating with the Microcontroller unit.

SR_COM_2: The Communication module must be compliant to the Sub-GHz 868 MHz communication standards of frequency, band and power.

SR_COM_3: The Communication module shall be capable of enhanced features for power consumption and communication reliability adapted to a WSN.

3.1.6 Antenna

SR_AM_1: The Communication Antenna shall be designed for a frequency range from fL = 863 MHz to fH=870 MHz (7MHz bandwidth).

SR_AM_2: The Ultra-Wide Band Antenna shall be designed for a frequency range from fL = 6 GHz to fH=8.5 GHz (2.5GHz bandwidth).

SR_AM_3: The antennas shall be compliant to the IEEE 802.15.4 standard

SR_AM_4: The antennas shall be designed and constructed such that the potential for personal injury during installation, operation and maintenance is minimized.

SR_AM_5: The antennas shall be delivered as a ready to use component, which can by directly connected via the mechanical interface to the other modules.

3.1.7 EH and Storage

Code of system requirement for this component: EH_OTI

SR_EH_OTI 1: For a given operational cycle of the train integrity operation, the total energy output of the energy harvester must be greater than the energy requirements for reliable operation of the OTI.

SR_EH_OTI 2: For a given operational cycle the energy storage capacity provided for the energy harvester must be greater than the total energy requirement for reliable operation of the OTI over the maximum time when energy harvester output is zero (train is stationary or no daylight for vibration or solar PV respectively).

SR_EH_OTI 3: The maximum charge rate of the energy storage device must be greater than the maximum peak output of the energy harvester.

SR_EH_OTI 4: The energy storage device must have appropriate protection devices to prevent under/over voltage and current conditions.

For example:

- Capacitors/super capacitors: Over voltage protection
- Hybrid Layer Capacitors (HLC) / rechargeable batteries: Over/under voltage protection (under voltage protection via a primary battery), over current protection (excess charge current may cause damage).

SR_EH_OTI 5: Design life of the energy storage and harvester shall both be matched to the design life of the vehicle.

SR_EH_OTI 6: Lifetime cost/benefit assessment of the system will include any maintenance and subjective degradation mechanisms:

Vibration energy harvester – extreme vibration robustness (no maintenance)

Storage capacitor – capacity degradation over time, susceptibility to vibration

Solar PV – contamination, seasonal and geographical variations

Batteries/HLC – capacity loss over time, degradation with temperature, susceptibility to vibration

SR_EH_OTI 7: Reliability and safety assessment of energy harvester performance is permitted to include improved performance through multiple (redundant) installations.

3.2 OTI CONTROL MODULE (OTI CM)

3.2.1 Microcontroller

The Microcontroller unit for the OTI CM must respect the same requirements outlined in the OTI Node Microcontroller System requirements (Section 3.1.4).

In addition to the requirements of Section 3.1.4 the Microcontroller for the OTI CM must also respect the following requirements:

1. SR_MU_4: The Microcontroller shall be able of controlling one or more HMI interfaces (display, sound actuators, LEDs, etc.).

2. SR_MU_5: The Microcontroller shall be capable of communicating with the train's on-board instrumentation through an already present interface.

3.2.2 Communication module

The Communication Module for the OTI CM must respect the same requirements outlined in the OTI Node Communication Module System requirements (Section 3.1.3).

3.2.3 Transmit/receive antenna

The TX/RX antenna of the Communication Module for the OTI CM must respect the same requirements outlined in the OTI Node antenna System requirements section 3.1.6.

3.3 SIL4 ENABLE

3.3.1 SIL4 Principles

The achievement of SIL 4 is based in any case on the correct and complete identification of hazards.

A consequence analysis shall provide, for each hazard, the conceivable consequences, while a cause analysis shall provide the events that can generate the hazard.

Through evaluation of severity of consequences and probability of their occurrence (on the basis of causes and “barriers” already existing) the residual risk is evaluated.

If this risk is judged not acceptable, additional measures need to be implemented, either to reduce the severity of the consequences or to reduce the probability of occurrence.

As described in section 2.2.1 of this document (preliminary hazard analysis), the mitigation of identified hazards will require:

1. adequate specification of functionality and operational procedures, to address all the risks that can occur in the configuration of the system and in the check of integrity during a train mission;
2. specification of appropriate communication protocols, to protect against communication errors;
3. implementation of measures to ensure that equipment correctly performs the requested functionality.

Points 1 and 2 above are part of ETALON project and will be the basis for the development of the prototype.

Point 3 will not be part of ETALON project, that will however put a disposal the principles and the “modules” that, appropriately combined in a “safety architecture”, will permit the achievement of SIL 4 operations.

List of hazards are divided into two different groups: hardware and software issue. Hardware issue are mostly due to the malfunction of the OTI device (power failure/hardware malfunction) while software issues are due to any hacking actions made by external entity (all the possibly events are described by the EN50159). Software malfunctions - as bugs and programming mistakes - are avoided by simulation software used before the prototype has begun fully operational.

LIST OF HARDWARE HAZARDS AND THE CONCEIVABLE CONSEQUENCES	
LIST OF HAZARDS	POSSIBLY CONCEIVABLES
OTI NODE: no power / module faulty (one device placed on a single side is out of service and one device is properly working)	➔ One OTI node device is switched off. Train Integrity is still confirmed by the other OTI node in the same side, that is properly working
OTI NODE: no power / module faulty (both devices placed on a single side are out of service, but not in the last wagon)	➔ OTI node devices are both switched off. Train Integrity is still confirmed by the OTI node device in the previous wagon side
OTI NODE: all the devices placed in the last wagon are in power failure state	➔ Train Integrity is not confirmed
OTI NODE: no power / module faulty (all the devices placed in one wagon, not the last)	➔ Train Integrity is still confirmed by the first OTI device that if capable of measuring the distance
OTI NODE: no power / module faulty (all the devices placed in two or more adjacent wagons)	➔ Train Integrity is still confirmed by the first OTI device that if capable of measuring the distance
OTI CONTROL MODULE: one CPU module is faulty (out of order)	➔ Train Integrity is not confirmed: the other CPU is working correctly
OTI CONTROL MODULE: all the CPU are out of order	➔ Train Integrity is not confirmed

Table 4 – List of Hazard and Conceivable Consequences (hardware)

LIST OF SOFTWARE HAZARDS AND THE CONCEIVABLE CONSEQUENCES	
LIST OF HAZARDS	POSSIBLY CONCEIVABLES
DATA PACKET REPETITION	➔ Repetition of an old message in appropriate situation
DATA PACKET DELETION	➔ Delete a message or part of this
DATA PACKET INSERTION	➔ Insertion of data packet inside data stream
DATA PACKET RE-SEQUENCING	➔ Change the sequence of data packets
DATA PACKET CORRUPTION	➔ Packet change his content to another formally correct message
DATA PACKET DELAY	➔ Insertion of bogus messages that causes big transmission delay or the service to stop
DATA PACKET MASQUERADE	➔ Type of inserted message in which a non-authentic message is designed to appear to be authentic

Table 5 – List of Hazard and Conceivable Consequences (software)

Regarding the hazard related to software conditions, system will auto mitigate itself by using special routine features that permits to auto detect corrupted packets and hackers attempts to modify wireless data contents.

Note: Train Integrity not confirmed is a safe condition because railway traffic is blocked immediately in the corresponding track where there is an hazard.

3.3.2 Safety features

No single failure of the OTI Control Module shall cause missed detection of train integrity loss.

No single failure shall cause undue detection of train integrity loss by the OTI Control Module.

3.4 DESIGN AND IMPLEMENTATION CONSTRAINTS

Achievement of SIL 4 implies putting in place measures able to ensure that, during the life of a system, the rate of occurrence of errors possibly leading to “catastrophic consequences” is lower than 10^{-9} h^{-1} per train.

The measures to be taken belong to different types, according to the dangerous situation that need to be taken under control, as explained below.

Systematic errors

These are the errors that can be done during all the phases of the development of products, such as inappropriate software design, causing unwanted system behaviour under some particular condition.

These errors are mitigated before commissioning of a system, through appropriate development methodologies (see for example EN 2019 and EN 50128) and extensive verifications in as many conditions as possible.

Random errors

These errors occur during the life of a system, because of malfunctioning of some of its components.

In case of electronic equipment (that are not subject to wear) the distribution of probability of occurrence of such kind or errors is usually described through a constant failure rate. This is the reason why, for signalling and train protection equipment, safety is mandated in terms of respecting the target of rate not higher than 10^{-9} h^{-1} for failures directly leading to catastrophic consequences (and less stringent targets for less severe consequences).

Strategies normally adopted to achieve SIL 4 are based on redundant operation with a “safe” check between the two (or more) elaboration “channels”.

With this concept in mind, ETALON will provide, as prototype, the implementation of one elaboration channel, consisting of:

- a variable number of vehicles nodes, each able to communicate with preceding and following one through antennas mounted on the two “sides” of the vehicle;
- a OTI Control Module, starting and checking system configuration and collecting train integrity information to be forwarded to Train Protection System.

The implementation of a full SIL 4 system requires therefore the duplication of parts that can be affected by random failures leading to dangerous situations, with safe comparison of their operations and outputs.

ETALON will analyse two possibilities.

The first assumes that errors in any of the pieces of equipment may remain undetected within the corresponding “channel”; safety requires therefore:

- installation, on each vehicle, of two nodes, with corresponding antennas. This will permit the creation of two independent “communication chains” along the train composition;
- installation, on the locomotive, of two OTI Control Modules, each managing a “communication chain”.

A second possibility could exploit the structure of data generated by each node. If each node is able to confirm the correct distance to the close one, sending back to the OTI Control Module (along the linear communication network of the vehicles nodes[3]) a message containing:

- identity of the node;
- token[4] generated by the OTI Control Module Node (different for each cycle of integrity check) re-sent back.

The probability that a node is able to generate, because of a random failure, also the message that should be generated by another node, is negligible[5]. It is therefore reasonable that an OTI Control Module can assume that, if all nodes of a chain have returned correctly the token, this means that the chain is full.

Regarding safety is then necessary to take into consideration only failures of OTI Control Module itself. This means that the two communication chains can be exploited to increase system availability (it is sufficient that one of them works correctly, to confirm train integrity).

The protection against failures of the OTI Control Module requires that it is duplicated and that the outputs of the two instances are compared. The safe comparison of the two OTI Control Modules will be possible, according to specific implementation decisions, either by software modules inside the train protection equipment, or by a specific “2 out of 2” computer, placed between the OTI Control Modules and the Train Protection System.

---

[3] Here it is also necessary that a node managing the antenna on the front side of a wagon generates a confirmation message, and that the node managing the antenna on the rear side of the preceding wagon forwards it back to the Signalling Control Centre, only if both nodes check that the distance between said antennas is within the allowed range.

[4] Resending the token used by the Signalling Control Centre to initiate the integrity check cycle is better than using a time stamp, because no timer is required in nodes (lower energy demand).

[5] The concept here is that a message is complicated enough to assume that it cannot be replicated by another node. This means that a node shall not be “too intelligent”... The safest approach would be to use digital signature, but this would require secret and public keys for each node...

The efficacy of the safe comparison of the resulting overall “2 out of 2” architecture is in any case strongly depending on the capability of fast self detection of failures, to reduce to zero the probability that the two channels continue to operate when both are affected by equivalent failures.

In this context, it is important that the system design is such that latent failures are avoided and that each failure becomes detectable in a short time.

This is taken into account in the design of the ETALON prototype, through the following measures:

- cyclic operation, to avoid long time without exchange of data;
- easy and safe distinction between old and new pieces of information (for example, different tokens to be propagated and returned for each integrity check).

Certification

Every product intended for use in rail systems need to be certified, and this is especially true for pieces of equipment performing SIL 4 functions.

Certification is not planned for prototypes developed in ETALON project, however the structure of documentation prepared (functional and system requirements specification with preliminary hazard analysis, etc.) will be ready to be completed with all other evidences.

Prototype

Prototype developed by ETALON project is not SIL4 but the documentation has been written by respecting SIL4 principles: so ETALON project is SIL4 capable.

3.4.1 Technical Specifications for Interoperability

Final production design of the system(s) would need to be compliant with the Technical Specifications for Interoperability (TSI) issued by the European Union Agency for Railways, relevant to the application, these indicate the standards which it is mandatory that a system/component is compliant with and the standards referenced in the TSI. The prototype developed within ETALON need not be fully compliant with the TSI but should be; operable safely in the test environment, not utilise technology which is fundamentally non-compliant with the TSI, and therefore be suitable for production versions to be made compliant with the TSI.

Technical Specifications for Interoperability (TSIs)	Decision / Regulation number	Date adopted by EC	Date published in OJEU	Entry into force	Links to TSIs and other associated documents
Control Command and Signalling (CCS TSI)	2016/919 (Regulation)	27/05/16	15/06/2016	**05/07/2016**	Commission Regulation (EU) 2016/919 of 27 May 2016
Locomotive & Passenger (LOCPAS TSI)	1302/2014 (Regulation)	18/11/2014	12/12/2014	**01/01/2015**	Commission Regulation (EU) No 1302/2014 of 18 November 2014 Corrigenda to Commission Regulation (EU) No 1302/2014 Application Guide LOC&PAS TSI
Operation and Traffic Management (OPE TSI)	2015/995 (Regulation)	8/06/2015	30/06/2015	**01/07/2015**	Commission Regulation (EU) 2015/995 of 8 June 2015
Rolling Stock (Freight Wagons) (WAG TSI)	321/2013 (Regulation)	13/03/2013	12/04/2013	**01/01/2014**	Commission Regulation (EU) 321/2013 of 13 March 2013
Telematic Applications for Freight (TAF TSI)	1305/2014 (Regulation)	11/12/2014	12/12/2014	**01/01/2015**	Commission Regulation (EU) No 1305/2014 of 11 December 2014
Safety in Railway Tunnels (SRT TSI)	1303/2014 (Regulation)	18/11/2014	12/12/2014	**01/01/2015**	Commission Regulation (EU) No 1303/2014 of 18 November 2014 Application Guide SRT TSI
TSI Conformity Assessment Modules	2010/713/EU	9/11/2010	04/12/2010	**01/01/2011**	Decision 2010/713/EU

Table 6 – List of Technical Specifications for Interoperability relevant to on-board train integrity solution, as at March 2018

4. SYSTEM REQUIREMENTS SPECIFICATION FOR TRACKSIDE OBJECT CONTROLLERS

4.1 TERMS AND DEFINITIONS

4.1.1 Usage of the words “shall”, “will” and “should”

Throughout this Chapter the word “shall” indicates an absolute requirement. It is incumbent to implement a design that complies with requirements stated using the word “shall”.

The word “will” indicates that although the stated need is not absolute, it is a design goal and is highly desirable or it is a goal or requirement levied on an external system.

The word “should” indicate the recommendation or desirable feature to be implemented to improve system performance or user experience.

4.1.2 Terms and definitions for trackside

Following the explanation of the used terms inside this chapter:

OCWC – Object Controller Wireless Communications

SCC – Signalling Control Centre

TEH – Trackside Energy Harvester

TO – Trackside Object

OCWC: provides wireless communications capability to enable the Object Controller to communicate wirelessly with the Signalling Control Centre, other object controllers and TOs.

TO: an apparatus installed on rail track that participates in train circulation management and are commanded from SCC. In the present document two main apparatus are considered: switches (including point machines) and level crossing barrier.

OCWC unit: a single device installed on field, mounted on TO or installed on wayside that provides wireless communication interface to SCC and is capable to transmit data regarding the state of TO to SCC and the commands from SCC to TO.

OCWC network: a communication network that contain a number of OCWC units that shall de capable to communicate with SCC and will be able to communicate among them if necessary. OCWC network is controlled by OCWC network control unit.

OCWC network control unit: a unit installed on SCC building and commanded by SCC, that shall be capable to provide an interface from SCC to OCWC network. This unit is out of the scope of the ETALON.

OCWC system: OCWC system contains the OCWC network and the OCWC network control unit.

TEH: is a device that provides locally generated energy to power object controller wireless communications.

TEH function: used to harvest and store energy derived from the local railway environment to provide a continuous reliable energy source to meet the power requirements of the object controller functionalities and wireless communications.

TEH functional definition: unit able to collect energy while installed near tracks. The unit, including energy storage, operates (provides power to connected devices) possibly with different efficiency, in all conditions during the entire day.

4.1.3 Trackside Operational parameters

Operation	No circulation	Check alive	Establishing link	Sending the state of TO	Receiving the command from SCC	Message size	Data rate	Max end-to-end delay	Time period
	Controlled by SCC	Automatic periodic check	Under request from SCC at train approach	Under request from SCC	Receiving	Type: 1. ACK SCC Command 3. TO state	Type: Safety critical Non-safety critical	Type: Safety critical 2. Non-safety critical	Type: Defined period Train traffic
OCWC state									
Dormant	On	Off	Off	Off	Off	n/a	n/a	n/a	No circulation
Idle	On	On	On	Off	Off	n/a	n/a	n/a	No circulation
Path searching	Off	On	On	Off	Off	54 bytes	1 Kbps/kbitps	Check alive: 20 s	Check alive: Low density line: each 30 min Medium- high density: each 15 min
Receiving	Off	Partial function	Partial function	Full function	Full function	256 bytes	5 kbitps	100 – 400 ms	Low density line: less or equal to 2

Operation	No circulation	Check alive	Establishing link	Sending the state of TO	Receiving the command from SCC	Message size	Data rate	Max end-to-end delay	Time period
	Controlled by SCC	Automatic periodic check	Under request from SCC at train approach	Under request from SCC	Receiving	Type: 1. ACK SCC Command 3. TO state	Type: Safety critical Non-safety critical	Type: Safety critical 2. Non-safety critical	Type: Defined period Train traffic
Transmitting	Off	Partial function	Partial function	Full function	Full function	256 bytes	5 kbitps	100 – 400 ms	trains/hour in both directions. Medium density line: 3 -11 trains/hour in both directions High density line: more than 11 trains trains/hour in both directions

Table 7 – Trackside Operation Parameters

4.2 FUNCTIONAL REQUIREMENTS OVERVIEW

OCWC_FN_1: it shall be possible to establish the centre- trackside communications when it is required by Signalling Control Centre with defined availability.

OCWC_FN_2: the Signalling Control Centre-trackside communications shall be continuously supervised confirming the availability to perform the required function at defined period of time.

OCWC_FN_3: the loss of Signalling Control Centre-trackside communications shall be detected.

OCWC_FN_4: the wireless communication system should be suitable for the communication of safety critical commands and information, and safeguard against intrusion.

OCWC_FS_5: the possible perturbations, interferences or attenuation of signal shall be taken in account.

OCWC_P_1: the OCWC shall comply with QoS parameters defined for Signalling Control Centre-trackside communications (e.g., latency, throughput, etc.) [ref. 13]

OCWC_P_2: the OCWC shall have sufficient reliable communication range (with minimal power usage) to assure Signalling Control Centre-trackside communications to perform the required function at defined period of time.

OCWC_P_3: the wireless communication system should have sufficient capacity to transfer all of the required commands and data within a required time period.

OCWC_P_4: the time for the wireless communication system to send an individual message/data packet through the communication network should be minimised (although also considering power consumption) and be suitable for the attainment of response times suitable for railway signalling systems and traffic control.

TEH_FN_1: the TEH shall provide the power when it is required by OCWC with defined availability.

TEH_FN_2: the power state of TEH shall be continuously supervised confirming the availability to provide the necessary amount of power at defined period of time.

TEH_FN_3: if the power state reaches a threshold level a small margin above the minimum required for the system to operate for a short period of time a message/alert should be sent to the Signalling Control Centre (or the Signalling Control Centre should create the message/alert based on the power state data).

TEH_FN_4: if the power state reaches the minimum threshold state required for the system to operate, the system shall enter a safe state (and deny requests to change state which it does not have enough energy attain).

TEH_P_1: the amount of power provided shall be enough to support the bidirectional Signalling Control Centre-trackside communications with defined range during the duration of mission.

4.3 METHODOLOGY AND INITIAL ASSUMPTIONS

In the present document the System Requirements Specifications (SRS) will be provided for the trackside communication system, consisting in:

- High Level system requirements: including the requirements regarding main network parameters for safety critical data and non-safety critical data;
- OCWC device architecture including the main components responsible for communications, computing, measurement and control and interfaces;
- SRS for OCWC device hardware and software;
- TEH device architecture including harvester and storage units;
- SRS for TEH device hardware and software.

4.4 HIGH LEVEL SYSTEM REQUIREMENTS FOR OCWC

System Requirements in this table are high level requirements for the equipment that shall be complied to satisfy Functional

Requirements Functional REQ	System REQ
OCWC_FN_1: It shall be possible to establish the Signalling Control Centre-trackside communications when it is required by Signalling Control Centre with defined availability.	SYS_OCWC_COM_1: System shall be able to receive and decode messages from SCC. SYS_OCWC_COM_2: The message structure shall be clearly defined for each type of communication. SYS_OCWC_COM_3: The total number of messages that can be interchanged between OCWC and SCC shall be limited. SYS_OCWC_COM_4: OCWC system shall have a support data base with a list of defined messages. SYS_OCWC_COM_5: If OCWC system receives a message that doesn't correspond to any from the list of defined messages it must be discarded.
OCWC_FN_2: The Signalling Control Centre-trackside communications shall be continuously supervised confirming the availability to perform the required function at defined period of time. OCWC_FN_3: The loss of Signalling Control Centre- trackside communications shall be detected.	SYS_OCWC_COM_6: OCWC system shall respond with ACK message to each received from SCC message. SYS_OCWC_EXP_1: Three intents will be performed from SCC to setup the communication link with OCWC. SYS_OCWC_EXP_2: The loss of communication link between SCC and OCWC shall be confirmed if OCWC doesn't respond to SCC after performing three requests. See section 4.2

Requirements Functional REQ	System REQ
OCWC_FN_4: The wireless communication system should be suitable for the communication of safety critical commands and information, and safeguard against intrusion. OCWC_FN_5: The possible perturbations, interferences or attenuation of signal shall be taken in account.	SYS_OCWC_SEC_1: OCWC shall satisfy EN50159 requirements for open transmission systems. SYS_OCWC_HW_1: OCWC antenna and RF transceiver shall be robust to external negative perturbations. SYS_OCWC_HW_2: OCWC antenna and RF transceiver shall be dimensioned to provide defined communication range considering signal attenuation. See section 4.1
OCWC_P_1: The OCWC shall comply with QoS parameters defined for Signalling Control Centre-trackside communications (e.g., latency, throughput, etc.), [ref. 13]. OCWC_P_2: The OCWC shall have sufficient reliable communication range (with minimal power usage) to assure Signalling Control Centre-trackside communications to perform the required function at defined period of time. OCWC_P_3: The wireless communication system should have sufficient capacity to transfer all of the required commands and data within a required time period.	SYS_OCWC_HW_3: OCWC antenna and RF transceiver shall be dimensioned to comply with defined performance parameters with minimum power consumption. See section 4.5.1
OCWC_P_4: The time for the wireless communication system to send an individual message/data packet through the communication network should be minimised (although also considering power consumption) and be suitable for the attainment of response times suitable for railway signalling systems and traffic control.	SYS_OCWC_HW_4: OCWC network configuration shall be dimensioned to comply with maximum end-to-end delay considering normal and degraded operational parameters of the system. See section 4.6.

Table 8 – High level system requirements for OCWC

4.4.1 Quality of Service Requirements

The Quality of Service requirements are derived from OCWC_P_1, OCWC_P_3 and OCWC_P_4 functional requirements.

Data bandwidth

Safety critical data

Minimum data bandwidth	1 kHz

Non-safety critical data

Minimum data bandwidth	240 Hz

Data rate

Safety critical data

Minimum data rate	5 kbitps

Non-safety critical data

Minimum data rate	1 kbitps

Data throughput

Safety critical data

Minimum data throughput	1 kbitps

Non-safety critical data

Minimum data throughput	40 bitps

End to end latency

Safety critical data

Maximum latency	Low 100 ms Normal 400 ms

Non-safety critical data

Maximum latency	20 s

Packet loss

Safety critical data

Packet loss	Ultra-low 99.9999% Low 99.9%

Non-safety critical data

Maximum packet loss rate	99%

Reliability

Safety critical packet loss

Reliability	High 99.9999% Normal 99.9%

Non-safety critical packet loss

Reliability	99.9%

4.5 OCWC COMPONENTS ARCHITECTURE

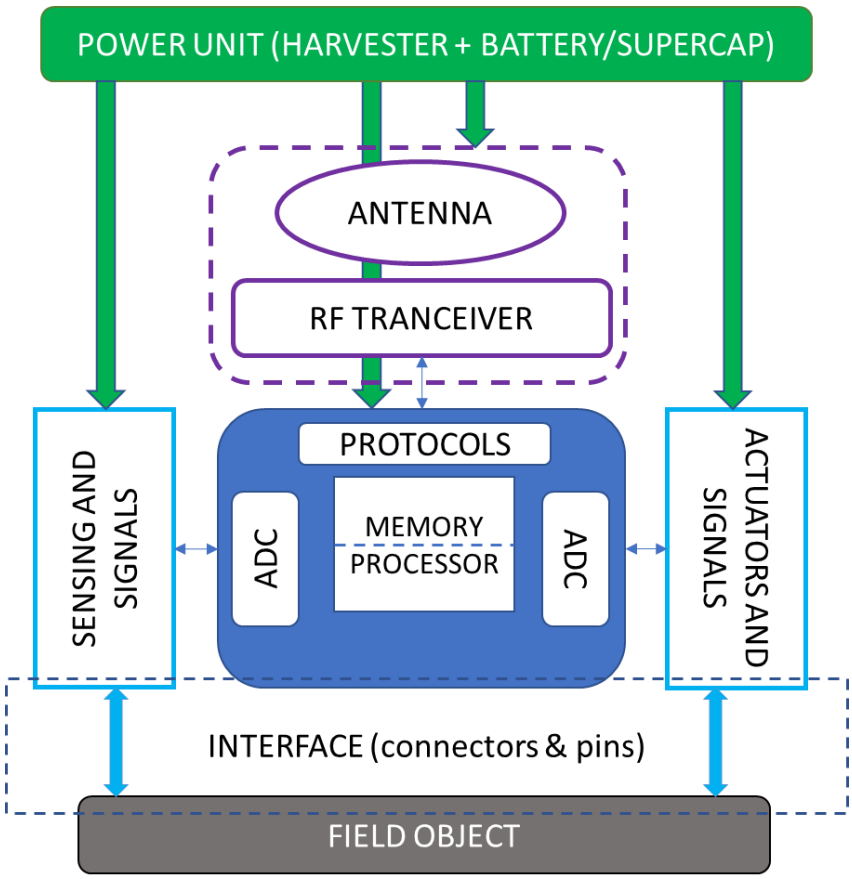

Figure 4 – OCWC unit architecture

4.5.1 Communications

RF transceiver

RF transceiver is the critical part of the device from the point of view of power consumption. The trade-off between power consumption and communications quality shall be found based on the given transceiver characteristics.

RF transceiver parameters

Parameter	Value
Frequency range (Hz)	Minimum value (to calculate according to maximum antenna size) Maximum value (according to path loss and range)
Receiver sensitivity (dBm)	Minimum value (according to QoS, see 4.4.1)
Receiver current (A)	Maximum value (interface with TEH)
Transmit current (A)	Maximum value (interface with TEH)
Output power (dBm)	Minimum value (according to communication range)
Communications range (m)	Minimum 200 m
Data rate (bps)	Value (according to required value, see 4.4.1)

Table 9 – RF transceiver parameters

Architecture considerations

There are different techniques to perform modulation and demodulation of RF signal and accordingly a variety of possible architectures.

The main characteristics that need to be considered are:

- the complexity of the scheme
- sensitivity of the receiver
- performance factors (throughput)
- power consumption

Usually as more complex as the scheme the better sensitivity and performance could be achieved but a greater implication of the active devices will be necessary and consequently the power consumption, complexity of the development and cost will be higher.

The OCWC device is characterized by low demand regarding performance factors (data rate, throughput) but high demand in terms of reliability, latency and availability (refer to section 4.4.1).

The communication range of the device is also a restrictive factor for the deployment since a dense communication network with high number of nodes will be difficult to maintain and will require high Capex and Opex costs.

To increase availability and reliability a redundancy factor shall be foreseen.

Antenna

The antenna is a part of the device that transmits and receives radio waves and it shall be installed on the trackside close to field objects which means that it will be surrounded by metalwork and shall be specifically designed and tested for hostile environments. It shall be robust to external conditions (static and dynamic) while keeping its own properties. It is also open-air environment and an adequate shelter shall be foreseen for the antenna to avoid its contamination and negative weather effects.

Consequently, the most restrictive conditions for the antenna selection are:

- Robustness and resilience to be able to work in harsh railway's conditions
- Antenna size

Antenna shall work with the defined frequency and be able to transmit and receive the radio waves in the defined directions with determined range.

Antenna parameters

Parameter	**Value**
Antenna type (radiation pattern)	Omnidirectional
Antenna type (technology chosen)	Shall be defined for specific application Recommended types: dipole, helical.
Dimensions	Shall be defined for specific application Recommended maximum height x width x depth: 480x310x310 mm (including the shell)

Table 10 – List of antenna parameters

4.5.2 Computing

Microprocessor

The microprocessor main functions are the radio data packetization and protocol management, as well as security related processes (e.g. encryption of data). Microprocessor and RF transceiver could be integrated in one module with hot swap redundancy, and need to satisfy RF transceiver characteristics.

4.5.3 Measurement and control

Sensing and signals

This component is responsible for gathering the data regarding the state of trackside objects.

Trackside Object	State
Point machine	Activated Not activated Left position (position locked) Right position (position locked) Position not detected No signal
Switches heating (optional)	Activated Not activated No signal
Level crossing barriers	Activated Not activated Closed (position locked) Open (position locked) Position not detected No signal
TEH	Power system is ON Power system is OFF Power system is OK Insufficient Energy (TRESHOLD ALERT) No signal

Table 11 – Track side Object and states

Actuators and signals

This component is responsible for transmitting control signal from SCC to TOs:

Trackside Object	Command
Point machine	Connect power to the motor Disconnect power Check the position
Switches heating (optional)	Connect power Disconnect power
Level crossing barriers	Connect power Disconnect power Check the position

Table 12 – Commands transmitted from SCC to TO

4.5.4 Interfaces

The main functional internal interface of OCWC is the one to trackside energy harvester (TEH).

The main functional external interfaces that shall be considered for OCWC are the wired interface to field object and wireless interface to SCC. Both interfaces are not in the scope of ETALON and only general indications are provided.

Wired interface to TEH

OCWC and TEH shall include the necessary number of I/Os to assure the correct powering of OCWC according to TEH_FN_1, and the correct supervision of state of the power system and storage according to TEH_FN_2.

The alerts that shall be generated when the power available in TEH is below the established threshold, can be generated either by the system or by the SCC according to the data provided.

Wired Interface to field object

OCWC shall include the necessary number of I/Os to assure that the connections with field object allow to transmit the signals corresponding to the state od TO (sensing) and commands to TO from SCC (control). The conversion from analogy to digital signal shall be performed with required reliability.

Wireless Interface to Signalling Control Centre

So far, no specific form fit Functional Interface Specification have been developed for purely trackside radio communications on Railways.

The applicable standard that shall be considered for the implementation of the interface is UNE-EN50159.

The most prominent features to be implemented in the OCWC are:

- the standardisation of the interface and its implementation in OCWC
- each OCWC shall have a unique identification code and be registered in the network
- define message type and structure to be interchanged between OCWC and Signalling Control Centre
- define safety policy and protection against hazards and intrusions
- define protocol of connection establishment
- define priority police

4.6 SYSTEM OPERATION

In the present section the system operation on field will be described, which includes operation in normal conditions (nominal) and the operation in degraded conditions (single faults).

System design shall assure fail safe operation in both normal and degraded scenarios, and the possibility of multiple faults shall be reduced to the acceptably low level.

The description is related to the operation after installation and commissioning assuming that these activities are out of the scope of the present document as well as maintenance and repair activities.

4.6.1 Normal conditions

The normal conditions of the system suppose:

- the communication network of OCWC is deployed according to the defined specifications, respecting the range, power consumption requirements, interface requirements, performance and security requirements;
- the communications network has been tested and proved to comply with assigned functionality (i.e. verification and validation are complete);
- all the nodes are registered in the system and could be perfectly identified by SCC.

The main functionalities of the system correspond to:

1. provide under request to the SCC the data regarding the state of TOs connected to the network;
2. send the control commands from SCC to TOs when it is required by exploitation program and actual train circulations;
3. provide to SCC the data regarding the state power system (TEH).

Note: the functionality derived from OCWC_FN_3 related to the supervision of the state if communication link between each network node and the SCC will be performed by SCC.

System operation under normal conditions

According to the exploitation program belonging to railway exploitation where the network is deployed, it shall be possible to set the TOs (switches and level crossings) to defined states according to the circulations.

Operation with switches

When the train is approaching to a switch, its state shall be checked in advance by SCC (left position, right position, position not proven), once it is checked and if it doesn't match the required position for the next circulation, a command will be send to power the point machine and move the switch to required position, after that the position will be checked and if it is correct the circulation will be allowed over the switch.

Operation with level crossings

When the train is approaching to a level crossing, its state shall be checked (open, closed, position not detected), if the level crossing is closed and protected the circulation will be allowed, if it is open, Signalling Control Centre will send a command to close it (after implementing the necessary safety measures to protect it).

It shall be noted that in both situation SCC is completely responsible for the decision about the required state of the TO and about the movement authority issue to the train.

OCWC equipment is responsible to provide OT state data and transmit the command under request from SCC.

The next Message Sequence Chart depicts SCC - OCWC communication (**Error! Reference source not found.**).

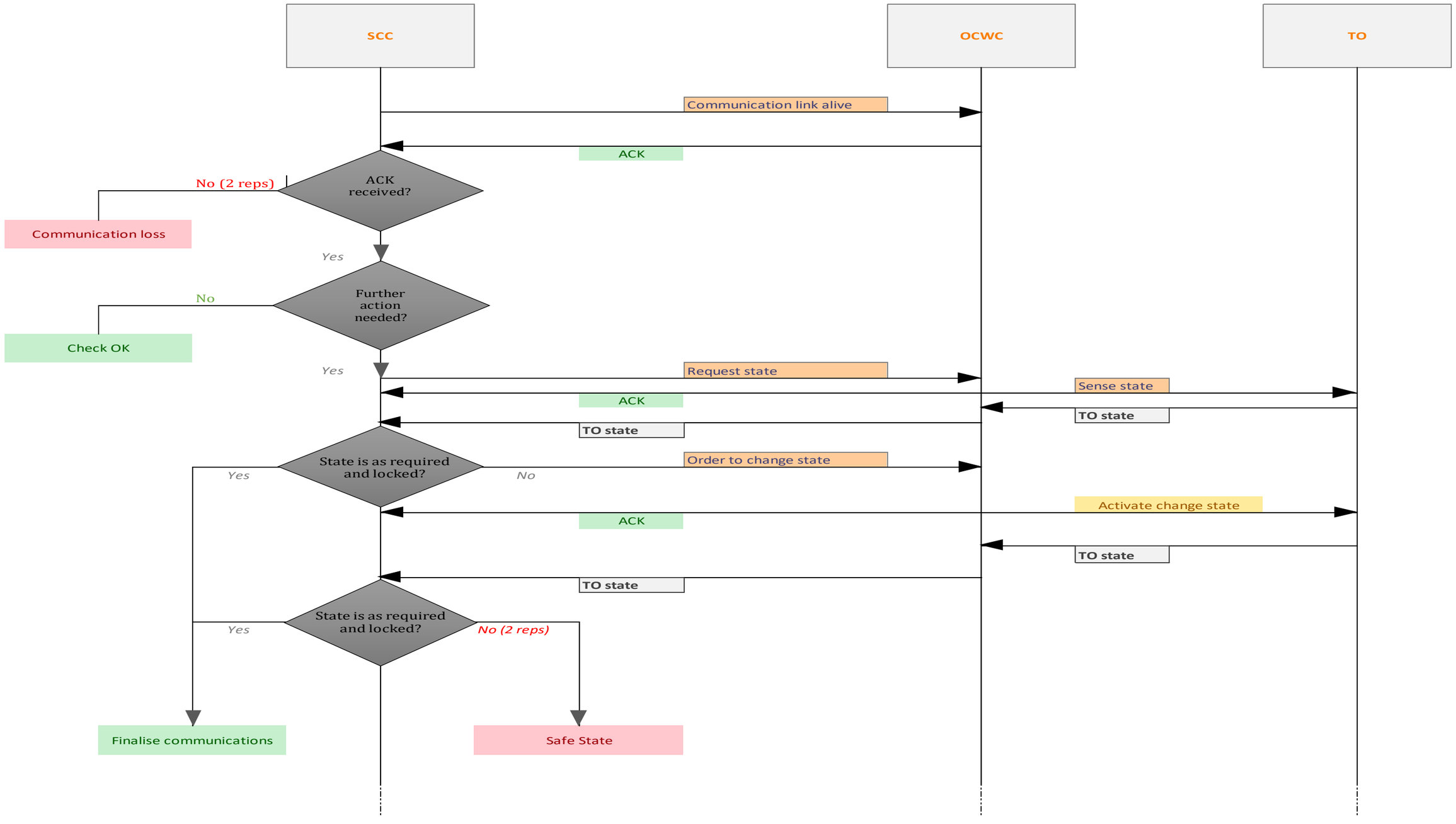
SCC
OCWC
TO
Communication link alive
ACK
ACK received?
No (2 reps)
Communication loss
Yes
Further action needed?
No
Check OK
Yes
Request state
Sense state
ACK
TO state
TO state
State is as required and locked?
Yes
No
Order to change state
Activate change state
ACK
TO state
TO state
State is as required and locked?
Yes
No (2 reps)
Finalise communications
Safe State

Figure 5 – Message Sequence Chart for SCC - OCWC communication

The message interchange depicted in the MSC diagram correspond to the following:

1) SCC starts the communication with chosen OCWC to verify the communication link is available (message *Communication link alive*).

2) once OCWC receives the request it shall send the ACK message to SCC.

3) if SCC doesn't receive the ACK message in 400 ms, it will repeat the cycle 2 times more.

4) If after 3 cycles the ACK message is not received the communication link will be considered lost.
5) If ACK message is received, SCC can either:

   a) finalise communications (Check OK) in case it is a periodical check;
   b) proceed to further actions in case the chosen TO will form part of a route.

6) in case of 5b, SCC sends the request about chosen TO state[6].

7) Once OCWC receive the request, it shall send ACK message to SCC and sense the state of TO.

8) after acquiring TO state, OCWC will send the data to SCC.

9) SCC will check whether the received state correspond to the required one for the next circulation (*State as required and locked*):

   a) If true, the communication will be finalised;
   b) If false, SCC will send the order to change the state of TO.

10) once OCWC receives the command it shall send ACK to SCC; transmit the command to TO (through the actuators); sense the state of TO and forward the new TO state to SCC.

11) SCC will check whether the new state is as required and locked:
   a) If true, the communication will be finalised;
   b) If false, two more intents to change the state of TO will be performed[7].

12) If three intents to change the state of TO fail, the system will enter the safe mode.

---

[6] The overall delay for signalling system shall be counted starting from the point 6 (state request) since the first 5 steps correspond to checking the communication link which can be performed periodically and in advance to the programmed circulations.

If during the process corresponding to the steps 5- 12, ACK message is not received by SCC in due time (max. 400 ms) the communication failure shall be reported.

[7] The time of waiting the TO state once the command "change state" is sent shall be configurable for each specific application and well as number of repeats (corresponding to line speed, density and trackside object properties).

4.6.2 Degraded conditions

For OCWC system the following degraded conditions of operation are possible:

1. loss of communication with SCC.

SCC will consider the communication with a system node is lost if it doesn't respond to the request during 3 intents to set the link.

2. state of the TO cannot be detected and the message "position not detected" is generated.

State of the TO will be considered "not detected" when:

- the communication with OCWC is lost;
- the message describing the state of the elements doesn't correspond to message structure from data base.

Three intents to obtain the state of the element will be performed from SCC until declare it as "not detected" and generate an alert.

Note: the interface OCWC- TO shall be implemented in safe and reliable way to assure the data about TO state can be trusted (out of the scope of ETALON).

3. TEH power storage is below the established threshold and the data/alerts is provided to SCC;

   TEH power storage will be considered to be below the threshold when:

   - The energy left will not allow to perform transmission/ receiving of data during the time to next recharge of the harvester.

4. TEH power unit is out of service;

   TEH power unit will be considered out of service if after "threshold alert" receipt the communication with node is lost.

In all the cases the SCC is responsible to safely manage the operation in degraded conditions based on fail safe principle.

When one of these conditions is not detected and Signalling Control Centre doesn't recognize it, a hazardous situation is generated. These hazardous situations are analysed in the following chapter 4.7.

4.7 SAFETY ANALYSIS

In the table below the degraded conditions of OCWC network are analysed in the case when the fault is detected and known to SCC and, in the case when it is not detected and consequently not known. The severity of the consequences is evaluated according to the signalling system top hazard (impact on system availability[8]; railway accident).

ID	Fault	Detected/Not detected	Consequence/ Failure	Severity	Mitigation
1	Loss of communication between SCC and OCWC	Detected	SCC orders safe state	Marginal (availability affected)	None
		Not detected	The previous known state of element is considered valid by SCC but it is not the required one.	Catastrophic (derailment/ collision)	Protection measures such as time- stamping, authentication protocol, message numbering, message acknowledgment, etc. shall be implemented.
2	State of the TO cannot be detected (OCWC-TO communication fault; message corruption/lost)	Detected	SCC will not allow circulations	Marginal (availability affected)	None
		Not detected	The previous known state of element is considered valid by SCC, but it is not the required one/ SCC takes into account the incorrect message	Catastrophic (derailment/ collision)	Time stamping; define secure codification/decodification algorithm; protection against intrusions.
3	TEH power storage is below the established threshold	Detected	SCC will take into account the necessity to recharge/replace the TEH.	Insignificant. System will rely on redundant nodes.	None
		Not detected	The TEH will be in use until it is out of service. Communication delays.	Marginal (availability affected)	OCWC should know the state of power storage of the TEH and transmit this information to the system.
4	TEH power unit is out of service	Detected	SCC will take into account the necessity to recharge/replace the TEH.	Marginal (availability affected)	None
		Not detected	System will rely on redundant node until its depletion	Critical (availability affected)	OCWC should know the state of the TEH and transmit this information to the system.

Table 13 - Degraded conditions of OCWC network

[8] Even though system availability decrease cannot be considered a hazard itself, it is a negative factor that, when maximized, impedes the compliance with other railway requirements (maximum service delay, reliability and average safety). Moreover, degraded operational mode cannot remain as safe as a normal operation.

It can be concluded that the most critical system failures correspond to undetected communications faults, for this reason the implementation of appropriate protocols with protections measures such as time stamping, acknowledgement messages, message counting, and adequate c codification/decodification algorithm must be foreseen.

4.8 ENERGY HARVESTING SOLUTIONS

The power unit to supply energy to the OCWC consists of the TEH module, the Power Management Electronics module, the Energy Storage module, and the interface between the power unit and OCWC.

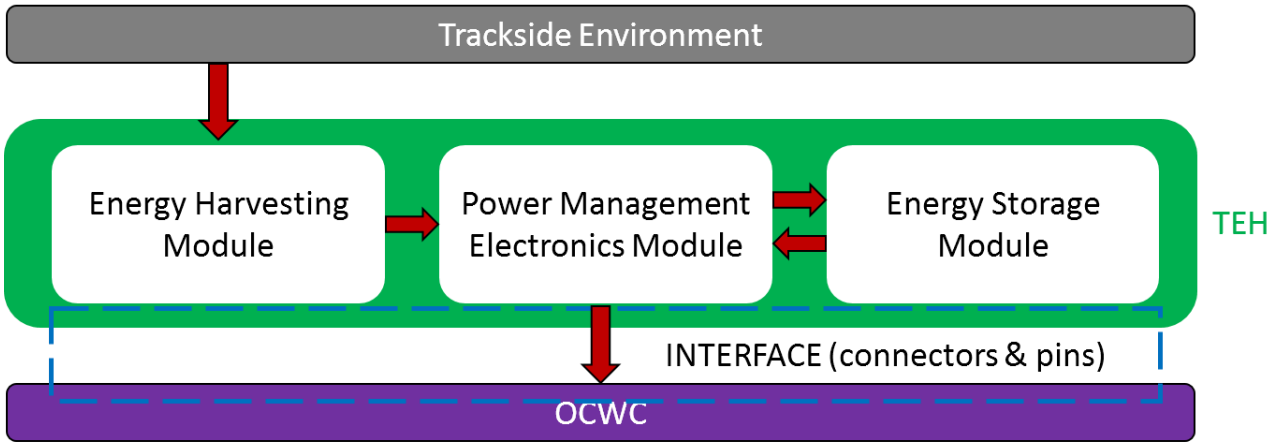

Figure 6 – TEH architecture

4.8.1 TEH Module

Trackside Energy Harvester (TEH) module is the key component responsible for production of electricity to power up the OCWC hardware. A number of different energy harvesting systems have been identified as suitable for deployment in the trackside environment, based on different energy transduction principals and each with different energy harvesting characteristics. In Functional Requirements Specification D2.1 these potential energy harvesting systems have been identified and characterized, a number of the energy harvesting techniques have been selected as particularly suitable for trackside energy harvesting in different situations. Depending on the characteristics of the selected TEH module the appropriate electronics and storage shall be selected. The TEH module selections shall be based on educated review of the ambient energy conditions and multiple energy harvesting devices of the same or different types might be specified to meet the power requirements of the application.

Architecture considerations

There are multiple options for TEH modules. Their feasibility depends heavily on the traffic and environmental conditions in the expected application location and on the power requirements of the OCWC. The main factors affecting energy harvesting capability to be considered include:

- Traffic density and speed profile
- Railway track quality
- Railway formation and alignment characteristics (tunnel, straight track/curve, regular track/switch, trackside space…)
- Geographical location and alignment (latitude, longitude. and compass heading of track alignment)

Vibration

The TEH vibration module produces electrical energy from vibrations of the track or sleeper during the passage of trains. The mechanical energy of vibrations induced by a passing train is converted into electricity through an electromechanical transducer exploiting one of the available physical effects. The power output of the vibration harvester is dependent on TEH mass, operating frequency and electrical load. It is also dependent on the shape of the input accelerations (vibrations and shocks waveforms).

Parameter	Value
Dimensions	volume integrated inside sleeper/between sleepers
Weight	seismic mass shall not affect dynamics of the track
Output voltage range	Minimum-Maximum value with respect to dimensions and other factors
Energy per train range	Minimum-Maximum value with respect to dimensions and other factors

Table 14 – General characteristics of the Trackside Energy Harvesting vibration module

Architecture restrictions

The restrictions placed on the vibration TEH usage are due to the principle of its operation and include following points:

- vibration TEH will not function well on high quality track where the vibration levels are low;
- vibration TEH will operate very well in switch sleepers where track stiffness is significantly changed and wheel-rail impacts at discontinuities in the rail provides high sleeper vibrations from passing trains;
- vibration TEH cannot be used in ballast-less tracks, since the sleepers are fixed by concrete and vibration is restricted;
- mass of the mechanical oscillator part of the vibration TEH shall not significantly affect the dynamic parameters of the track, thus the maximum power output of the vibration TEH on any given track is limited.

Reluctance

The TEH reluctance module generates electricity from the changes of magnetic circuit reluctance due to train wheels passing. The power output of the variable reluctance TEH depends on the speed of the passing train, number and design of its wheels and on the distance between the wheels and the TEH in the moment of passing.

Parameter	Value
Dimensions	approx. 0.1 x 0.1 x 0.2 m
Weight	up to 2 kg
Output voltage range	Minimum-Maximum value with respect to dimensions and other factors
Energy per train range	Minimum-Maximum value with respect to dimensions and other factors

Table 15 – General characteristics of the THE reluctance module

Architecture restrictions

Variable reluctance restrictions are given by the physical energy conversion principle and by the device design as follows:

- variable reluctance TEH cannot be used with non-ferromagnetic train wheels and rails;
- variable reluctance TEH cannot be kept in place during track maintenance (tamping, grinding);
- variable reluctance TEH cannot be used near devices, that could be affected by its magnetic field.

Displacement

Selected displacement based energy harvesting principal was linear electromagnetic generators actuated either by the wheels of passing trains or the relative motion of the track to the ground when a train passes:

- actuation of the energy harvester shall not produce a significant effect on vehicle or track dynamics and must not reduce safety levels below thresholds;
- energy harvester shall be easily installed securely on track structure and require minimal adjustment upon installation and throughout its operating life;

- energy harvester shall fit within the geometric constraints of the track infrastructure and not obstruct the passage of trains (except any intended contact of the actuator with the wheel).
- energy harvester (except actuator activated by wheel) must not impinge on the structure gauge for the route. EN 15273-3 Railway applications - Gauges - Part 3: Structure gauges, or any other structure gauges in use on the route.
- energy harvester shall not obstruct track maintenance activities or shall be easily removable to allow track maintenance activities to take place;
- geometric and activation force constraints will limit the energy harvesting capacity of an individual unit; multiple units might be required to meet the power requirements of connected devices.

Solar

The selected continuous or intermittent energy harvesting principal for harvesting energy from the environment (as opposed to the passage of trains) is photovoltaic solar panels.

- The nominal maximum power output of a solar panel (with full intensity sunlight acting normal to the panel) is 150 W/m^2. Taking into account the passage of the sun throughout the day and statistics for average sunshine variations due to weather, the average power output of a panel in central Europe, fixed at the optimal angle, is approximately 0.4kWh/m^2/day, or 12.4kWh/m^2/month. To achieve the energy harvesting requirements for a specific application, the total area of solar panel(s) must be sufficient for its average energy harvesting capacity to meet the average energy consumption of the connected devices, with allowances made to ensure an excess of energy harvesting capacity and for the efficiency of the energy storage equipment;
- Output voltage and current of solar panels depends on incident solar energy and panel/array design, voltage and current range of solar panels shall be suitable for input to power management electronics.
- Tools for taking into account the difference in daily/monthly/annual solar panel output of different geographic locations and local weather patterns should be used to estimate the average energy harvested by solar panels, or size the installation, for each location.
- Solar panels must have as unobstructed field of view of the sky as possible, the effect of any fixed obstructions on the energy harvesting capacity of the panels must be taken into account when determining the size of installation required to supply the energy consumption of the connected devices.
- Secure fixing arrangement that orientates the solar panels in the desired relationship with the passage of the sun and is resistant to effects of wind and aerodynamic effects of passing trains.
- Fixing arrangements must also be compliant with rules and standards regarding trackside structures.
- Solar installations require an energy storage system capable of supplying the requirements of the connected devices overnight and for a number of days when climactic conditions result in little or no energy being harvested.

4.8.2 Power management electronics

- Power Management Electronics (PME) must be able to cope with the maximum theoretical momentary and instantaneous energy harvester output, and dissipate it if necessary.
- PME must limit or buffer the input to the energy storage. In some cases energy harvesting capacity might be specified to ensure adequate energy harvesting in sub-optimal harvesting conditions, which means that in optimal harvesting conditions excess energy might be harvested above what the energy storage can accept.
- PME must be able to provide the charge status of the energy storage (amount of available energy) and should provide energy usage and harvesting data for the connected devices.
- PME must include an interface to output the energy data to other connected devices and/or central control and maintenance centres (via data interface with systems communications equipment (not independent communications).
- PME must be able to convert variable and fluctuating harvested electrical energy to a voltage and current output suitable for charging the energy storage and (optionally) supplying the attached equipment directly.
- The PME shall regulate and monitor the power supply from the energy harvester(s) and energy storage to the OCWC.
- The PME shall be capable of simultaneously supplying the connected equipment and charging the energy storage if sufficient energy is being harvested.
- The PME will be tailored for given energy harvester, optimal load should be set up for maximal power extraction.
- The maximal power point tracking function should be included in the PME.
- The PME shall operate in a guaranteed time at given ambient conditions.
- The PME shall regulate and monitor the charging of the energy storage, shall be included battery charging and protection electronics for controlling undervoltage and overvoltage levels.
- The PME shall transfer alternating current to direct current from energy harvester.
- Lead based solder shall be used for higher reliability of soldered electronics.

4.8.3 Energy storage

- During design of each installation:
    - the capacity, and discharge rate, should be specified to meet the requirements of the connected devices;
    - the charge rate should be specified to accept enough of the charge from the energy harvesting to meet the long term consumption of the attached equipment (and shall be protected from overcharging);
    - the physical parameters of the energy storage should be specified to meet the restrictions of the location;
    - the type of energy storage should be specified to meet the requirements of application;

  - the charging cycles and cycling performance should be specified to meet the requirements of application.

- Energy storage must have sufficient capacity to supply the requirements of the connected equipment for a number of days, from partially charged, without energy harvesting input.
- Energy storage maximum discharge rates must be sufficient to supply the worst case of maximum energy consumption/requirements of the connected equipment.
- Energy storage maximum charge rate must be sufficient to accept the maximum charge supplied by the PME.
- Energy storage shall operate in a guaranteed time at required ambient conditions.
- Energy storage will operate with nominal voltage to meet the requirements of OCWC.
- Energy storage will have self-discharge as low as possible.

4.8.4 Interface

Both TEH and OCWC shall include matching interfaces with sufficient number of I/Os to assure the correct powering of OCWC, and the correct supervision of state of the power system and storage. The interface shall include an output providing condition data on the available stored energy. Alerts regarding the available stored energy falling below a threshold (configurable for the application) may be generated locally by the Power Management Electronics Module of the TEH system, or at the signalling and maintenance Signalling Control Centres based on the condition data.

4.9 TEH SYSTEM REQUIREMENTS SPECIFICATIONS

Identifier	Parameter	Requirement
TEH		
SRS-TEH-001	Power output	Power output shall cover the OCWC power requirements
SRS-TEH-002	Dimensions	Maximum height x width x depth shall be defined
SRS-TEH-003	Clearance	TEH shall not obstruct the passing train or its parts
SRS-TEH-004	Housing	TEH should be covered or hidden from vandals and casual mechanical damage.
SRS-TEH-005	Installation	The TEH installation shall meet the requirements of the standards relating to track side equipment and structures

Identifier	Parameter	Requirement
Vibration TEH		
SRS-TEH-V-001	Working frequency	Working frequency shall be set to match the exploitable frequency in the excitation spectra
SRS-TEH-V-002	Bandwidth	Bandwidth shall be designed to allow for wide range operation
SRS-TEH-V-003	Sensitivity	The vibration TEH shall be able to produce electricity from low level vibrations
SRS-TEH-V-004	Applicability	The power output of vibration TEH shall provide sufficient power under specified excitation conditions

Identifier	Parameter	Requirement
Variable reluctance TEH		
SRS-TEH-VR-001	applicability	Variable reluctance TEH shall generate output power when ferromagnetic train wheels are passing through its magnetic circuit
SRS-TEH-VR-002	Wheel clearance	The wheel clearance of the variable reluctance TEH shall be within specified limits

Identifier	Parameter	Requirement
Displacement TEH		
SRS-TEH-D-001	Dimensions and configuration	The displacement TEH shall not impinge on the structure loading gauge of the route (except for the actuating arm of wheel activated devices)
SRS-TEH-D-002	Installation	The displacement TEH shall not obstruct track maintenance OR shall be removable for track maintenance

Identifier	Parameter	Requirement
Solar TEH		
SRS-TEH-S-001	Installation	The solar panel components shall be exposed to the sky and mounted to optimise incident solar energy throughout the year

Identifier	Parameter	Requirement
Power management electronics TEH		
SRS-TEH-PME-001	Operating conditions	The power management electronics shall not be affected by humidity and dustiness in operating area.
SRS-TEH-PME-002	Reliability	The power management electronics shall be soldered by lead solder for a higher reliability of connections.
SRS-TEH-PME-003	Working temperature	The power management electronics shall operate in range of temperatures in area of the local railway environment.
SRS-TEH-PME-004	Inputs	The power management electronics shall operate in range of voltages, currents and power generated by TEH module.
SRS-TEH-PME-005	Outputs	The power management electronics shall output electrical energy in the range of voltages, currents required/accepted by the energy storage and the connected equipment (converting input voltages/currents where necessary)
SRS-TEH-PME-006	Outputs	The power management electronics shall limit the range of voltages and currents applied to the energy storage and connected equipment, and dissipate the excess energy if necessary.

Identifier	Parameter	Requirement
Energy Storage TEH		
SRS-TEH-ES-001	Capacity	The power density of the energy storage shall be appropriate with respect to the demands of connected equipment.
SRS-TEH-ES-002	Working temperature	The energy storage shall operate in range of temperatures in area of the local railway environment.
SRS-TEH-ES-003	Output	Range of Range of voltages, currents shall be usable by PME

Identifier	Parameter	Requirement
Interfaces		
SRS-TEH-I-001	Connectivity	The interface of TEH solution shall match the OCWC interface

Table 16 – General requirements for TEH

4.10 DESIGN AND IMPLEMENTATION CONSTRAINTS

Final production design of the system(s) would need to be compliant with the Technical Specifications for Interoperability (TSI) issued by the European Union Agency for Railways relevant to the application, these indicate the standards which it is mandatory that a system/component is compliant with and the standards referenced in the TSI. The prototype developed within ETALON need not be fully compliant with the TSI but should be; operable safely in the test environment, not utilise technology which is fundamentally non-compliant with the TSI, and therefore be suitable for production versions to be made compliant with the TSI.

Technical Specifications for Interoperability (TSIs)	Decision / Regulation number	Date adopted by EC	Date published in OJEU	Entry into force	Links to TSIs and other associated documents
Control Command and Signalling (CCS TSI)	2016/919 (Regulation)	27/05/16	15/06/2016	05/07/2016	Commission Regulation (EU) 2016/919 of 27 May 2016
Infrastructure (INF TSI)	1299/2014 (Regulation)	18/11/2014	12/12/2014	01/01/2015	Commission Regulation (EU) No 1299/2014 of 18 November 2014 Application Guide INF TSI
Operation and Traffic Management (OPE TSI)	2015/995 (Regulation)	8/06/2015	30/06/2015	01/07/2015	Commission Regulation (EU) 2015/995 of 8 June 2015
Telematic Applications for Freight (TAF TSI)	1305/2014 (Regulation)	11/12/2014	12/12/2014	01/01/2015	Commission Regulation (EU) No 1305/2014 of 11 December 2014
Telematic Applications for Passenger Services (TAP TSI)	1273/2013 (Regulation)	06/12/2013	07/12/2013	08/12/2013	Commission Regulation (EU) No 1273/2013 of 06 December 2013
Safety in Railway Tunnels (SRT TSI)	1303/2014 (Regulation)	18/11/2014	12/12/2014	01/01/2015	Commission Regulation (EU) No 1303/2014 of 18 November 2014 Application Guide SRT TSI
TSI Conformity Assessment Modules	2010/713/EU	9/11/2010	04/12/2010	01/01/2011	Decision 2010/713/EU

Table 17 – List of Technical Specifications for Interoperability relevant to trackside energy harvester systems (as at March 2018)

5. CONCLUSIONS

The system requirements and specifications document presents the main indications to be adopted for the correct design of the system planned for the Etalon project. In task 2.4, the discussions on the architectural definition were the focus of the activities. The detailed analysis of the architecture modules and their operation played a key role in achieving the task's goal: Starting with a high-level definition of the architecture, the partners gradually focused on the individual components and how to achieve the train integrity.

Numerous detailed ideas emerged during the analysis, including a hazard list, the status table, as well as the technical specifications of each component.

6. REFERENCES

[1] STANDARD: CENELEC - EN 50159: Railway Applications - Communication, Signalling And Processing Systems - Safety-Related Communication In Transmission Systems *Link*

[2] SUBSET-119 Train Interface FFFIS, ERA, ISSUE: 0.1.13, DATE: 2014-10-16.