ETALON

D 2.1 Functional Requirements Specifications

Due date of deliverable: 01/06/2018

Actual submission date: 31/05/2018

Leader of this Deliverable: Stamatios Eleftheriou, ERGOSE S.A

Reviewed: Yes

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

Document status		
Revision	Date	Description
1	01/12/2017	First draft document
2	22/11/2017	Integration of the contributions relative to the On–board Train Integrity by ISMB
3	27/11/2017	Integration of the contributions relative to the On–board Train Integrity by ISMB
4	03/01/2018	Integration of the contributions relative to the On–board Train Integrity and Track Side energy harvesting system by ISMB and PERPETUUM
5	20/02/2018	Integration of the contributions relative to the On–board Train Integrity Functional Requirements Specification by SIRTI
6	08/03/2018	Integration of the contributions relative to the track–side Energy Harvesting System by University of Newcastle
7	09/03/2018	Reviews by all the Partners during the call conference of 9th March
8	19/03/2018	Reviews by all the Partners during the call conference of 19th March
9	26/03/2018	Integration of the contributions relative to the On–board Train Integrity by ARDANUI and ISMB
10	25/05/2018	Reviews by all the Partners during the call conference of 25th May
11	28/05/2018	Reviews by ARDANUI and ISMB
12	29/05/2018	Final revision by ISMB and SIRTI
13	29/05/2018	Quality check before upload in the Cooperation Tool by UNIFE/RINA

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Stamatis Eleftheriou	ERG	Document generation, integration and review of partner's contributions.
Dimitris Koutsoukos	ERG	Performed a final review of the whole document.
Roberto Cafferata	SIRTI	Added critical comments and content to the document related to the OTI and TEH systems.
Veronika Nedviga	ARD	Added the content for the track–side communication systems and reviewed the OTI system. Updated the content for the track–side communication systems.
Carles Artigas	ARD	Added comments on the on–board and track side communication systems.
Francesco Sottile	ISMB	Added comments and content to the document related to the on–board communication systems.
Alexander James Pane	ISMB	Added comments and content to the document related to the on–board and track side communication systems.
Paul Hyde	UNEW	Added comments and content to the document related to the OTI and TEH systems.
Alexander James Pane	ISMB	Reviewed comments related to the interaction between the OTI system and train driver.
Roberto Cafferata	SIRTI	Final revision before finalisation.
Klevisa Ceka	RINA	Quality Check

EXECUTIVE SUMMARY

The main objectives of ETALON WP2 – System Architectures, Specifications and Technical Coherence, regarding the activities linked with the IP2 TD 2.5 and TD 2.10, are to:

1. Coordinate the technological and scientific orientation of the project and effectively deal with all technical risks and issues as they arise;

2. Liaise with the relevant activities within the S2R JU concerning IP2 TD2.5 and TD2.10;

3. Define the overall Functional Requirements;

4. Collect the System Requirements of the "On–board Train Integrity solution" and "Trackside Energy Harvesting device for Object Controllers";

5. Write the requirements coming from the Engineering Rules and Maintenance needed for the overall System.

ETALON WP2 is responsible for designating the System Architectures, the Functional Requirements Specification, the System Requirements Specification of the ETALON project and to assure the technical coherence and alignment with the activities of the Shift2Rail JU.

This document represents the output of the Task 2.3, where the "Functional Requirements Specification" for the new "On–board Train Integrity solution" and the new "Trackside Energy Harvesting solution for Trackside Object Controller" are defined.

The Functional equirements will be classified by the criticality and required safety level (SIL 4) as well as the operational needs. RAM objectives will be traced at this phase to mark the criteria for the systems performance.

This document will be an input for the activities of ETALON WP3 and ETALON WP4 and for task T2.4 of ETALON WP2.

TABLE OF CONTENTS

LIST OF PARTICIPANTS

NO	LEGAL NAME	SHORT NAME
2	Sirti Società per Azioni	SIRTI
3	Ardanuy Ingineria SA	ARD
5	ERGOSE S.A	ERG
6	Istituto Superiore Mario Boella Sulle Tecnologie dell'Informazione e delle Telecomunicazioni Associazione	ISMB
8	University of Newcastle upon Tyne	UNEW

D2.1 FUNCTIONAL REQUIREMENTS SPECIFICATIONS

1. INTRODUCTION

The Functional Requirements Specification report describes the functional requirements needed for the “On–board Train Integrity System” and for the new “Trackside Energy Harvesting device for Object Controllers”.

1.1 List of Acronyms

CCS	Control command and signalling
EMC	Electro–magnetic compatibility
ETCS	European Train Control System
EU	European Union
FMEA	Failure Mode and Effect Analysis
FRS	Functional Requirements Specification
FTA	Fault Tree Analysis
OCWC	Object Controller Wireless Communication
OTI	Onboard Train Integrity
MITM	Man In The Middle (informatic attack where the attacker secretly relays and possibly alters the communication between two parties)
QoS	Quality of Service
RAC	Risk Acceptance Criteria
RAM	Reliability, Availability, Maintainability
RAC	Risk Acceptance Criteria
SIL	Safety Integrity Level
TEH	Track–side Energy Harvesting
THR	Tolerable Hazard Rate
TSI	Technical Specification for Interoperability
UIC	Union International des Chemins de Fer

2. ON–BOARD TRAIN INTEGRITY SOLUTION

2.1 GENERAL CONSIDERATIONS

The context of the on–board solution for train integrity is the traffic management and supervision, more specifically route interlocking and train protection functions, responsible for ensuring safe spacing and speed, to avoid collisions and derailments [ref 1].

Both interlocking and train protection functions require the knowledge of the positions of train heads and tails.

In modern train movement protection systems (like ETCS – [ref 2]) the knowledge of train head location is achieved by equipment installed on–board and able to locate the train head with respect to fixed reference locations (distance and orientation from reference). This functionality is outside the scope of this project.

In almost all the systems currently implemented in railway lines, the knowledge of the exact location of the train's tail is not necessary, because of the existence of trackside "train detection systems", i.e. equipment that can locate the full train consist inside "block sections" of fixed length. This approach (the so–called fixed block) is sufficient for operational safety; anyway, the poor accuracy of train tail locations (only known with the granularity of the length of fixed sections) has negative impact on line capacity.

A more efficient train spacing (the so–called moving block) requires the accurate knowledge of the train's tail position, with respect to the same reference locations used for the train heads locations. See [ref 3] for a general explanation of fixed and moving block concepts.

Such positions of the train's tail can easily be evaluated from the position of the train's head, if the length of the train is known. While this value can be introduced as a configuration parameter of the interlocking and train protection functions before starting a train mission, the risk remains that, during a trip, the physical connection (coupling) between a couple of wagons is broken and a part of the consist is "lost".

If this event is not advised to the interlocking and to the train spacing functions, it is possible that the traffic management and the train protection functions authorize a train to move on to a track section considered free, but where in reality some lost wagons stay (with the risk of collisions).

The objective of ETALON is to develop a prototype of a system including energy harvesting and on–board train communication network suitable for a train integrity system for freight trains.

2.2 METHODOLOGY AND INITIAL ASSUMPTIONS

The methodology employed for developing the train integrity confirmation system will follow existing standards ([ref 4] and [ref 5]) related to safety critical applications; firstly, a concept definition phase will be taken on, where high level objectives will be outlined. Simultaneously with the adopted technical solutions, the overall system will be developed and integrated starting from the functional and safety aspects.

The project developed within ETALON activities relies on the following assumptions related to the technical solutions that will be adopted:

TI_ASS_1:

1. The train integrity confirmation system is based on communication between pieces of equipment installed on all vehicles[1] and a piece of equipment installed only on the leading unit of a train.
2. Communication occurs at least between equipment installed on adjacent vehicles belonging to the same train and possibly between additional vehicles in communication range.
3. The main sub–functions (collection of information, decision whether train integrity can be considered confirmed or not) and interfaces with other train movement supervision functions, are allocated in the piece of equipment installed on the leading unit of the train.
4. Equipment installed on vehicles only communicates with similar equipment installed on preceding and following vehicles of the same train consist.
5. Equipment installed in each wagon are able to automatically identified equipment not belonging to the same consist.
6. Equipment installed in the last wagon (end of the convoy) communicate with the previous one(s) (a special algorithm will inform the head of the train about it).
7. Equipment installed on vehicles does not require cabling; power shall be made available locally through energy harvesting and storage.
8. All pieces of equipment installed on vehicles are identical; the only differences can be the ones due to configuration data entered during the installation phase.

In addition, regarding the integration in the overall railway system, the following assumptions are made on the way of working of the train protection functionalities that will exploit the information generated by the train integrity confirmation system:

TI_ASS_2:

1. The on–board train protection functions report to the trackside control centre the location of train head, the train length and the state of train integrity (as communicated to them by the train integrity confirmation system).
2. The state of train integrity can be “confirmed” or “not confirmed”. The “not confirmed” state can include different categories such as “integrity lost”, “reforming consist”, “not active”and “topology discovery”, with “not confirmed – integrity lost” being a priority safety alert state.
3. In case no updated information regarding the state of train integrity is received, the on–board train protection functions will report the “not confirmed” state for the train integrity.
4. Upon receiving information from on–board, the trackside control centre functions will update the location of train heads and tails on their maps.

[1] in this paper the term “vehicle” is used with a quite generic meaning. It indicates any vehicle that may be trailed, including locomotives in multiple configurations.

5. If the train integrity is “not confirmed”, the control centre considers that the location of tail is not modified.

The following Chapter 2.3.1 contains the high level functional requirements that do not depend on the technical solutions adopted for the system development.

The high level functional requirements are then refined in the following chapters, where the preliminary assumptions for system development listed above (TI_ASS_1 and TI_ASS_2) are taken into account.

It must therefore be considered that the requirements specified in this document are only valid in applications where TI_ASS_1 and TI_ASS_2 are respected.

Chapter 2.3.2 contains more details on functional and performance aspects.

Chapter 2.3.3 contains general requirements related to the characteristics of equipment.

Chapter 2.3.4 contains general requirements related to the operational conditions referred to the use of train integrity system.

Chapter 2.3.5 summarizes the requirements that have impact on energy harvesting solutions. The reason is that the impact on energy harvesting is “distributed” among all categories of requirements; being energy harvesting one of the key points of ETALON, it is considered advisable to indicate separately all requirements affecting it.

The requirements described in these chapters are the starting point for the system requirements definition. A more precise description of the system architecture, the sub–functionsand their apportionment in pieces of equipment installed on traction units, wagons and the communication between them will be done.

In parallel with the system definition, a second step of safety analysis (other than the preliminary considerations made in Chapter 2.3.1) will be performed, identifying hazards due to failures and errors in equipment and communicationsand apportioning to them the top level requirements, with consequent definition of necessary mitigations, which is the precondition for the final detailed system design.

Legends: in the text of the requirements below

1. “**shall**” means a requirement, the fulfilment of which is essential to achieve the ETALON project goals;

2. “**should**” means a requirement that is advisable and will better investigated during ETALON system design, to achieve a good balance between performance and cost.

2.3 REQUIREMENTS

2.3.1 High level functional requirements

Explanation

Details of interlocking and train protection functions are not in the scope of this project, however it is clear that missing information about loss of integrity of a train can directly cause (without the need of other contemporary faults or errors) collisions of trains against lost vehicles. This is normally considered an accident with catastrophic consequences (i.e. several injuries and deaths). See for example [ref 6].

The usual approach to safety [ref 7] requires that, when accidents may have catastrophic consequences, the probability of occurrence of situations directly causing such accidents must be “incredible”. According to the concepts of EN 50126 [ref 4] and EN 50129 standards [ref 5], the Safety Integrity Level (SIL) of the corresponding functionality must then be 4.

Requirements

In more formal wording, the concepts above can be expressed as:

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_Function: train integrity confirmation function is responsible to collect, evaluate and send to other train movement supervision functions of the trackside control center, updated information about the integrity state (confirmed or not confirmed) of the train.

The “top hazard” for train integrity confirmation function is:

TI_TH: train integrity inappropriately sent a “confirmed” status to the other train movement supervision functions of the trackside control center, when that is not the case, or it cannot certainly be determined to be the case.

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.

Comments

It is necessary that the train integrity confirmation system is designed in a way that permits (following the guidelines of recognized standards, EN 50129 [ref 5] and other of the same series) the proof that the THR for the top hazard is respected.

This requires the consideration of the “sub–functions” into which the global train integrity confirmation function has been split and the relationship between them, to identify the effects of possible failures and errors (e.g. through Fault Tree Analysis (FTA) Failure Mode and Effect Analysis (FMEA) etc.) and allocate tolerable rates for the occurrence of the identified dangerous events in such a way that the top hazard THR is not exceeded.

Of course, a detailed technical analysis as the one shortly described above can only be done after system design and can be finalized only after prototyping and adequate verifications. See the "safety life–cycle" described in [ref 4] and [ref 5].

The analysis should also take into consideration security aspects, i.e. possible intentional attacks that could cause safety relevant consequences (like collisions or derailments) to identify needs of protecting equipment against sabotage and communications against intrusions.

2.3.2 Functional and performance requirements

Explanation

In this document functional requirements are classified as safety relevant or not, according to a preliminary estimation based on expert judgement and taking into account the assumptions on the way this information will be used by train protection functions, as specified in Chapter 2.

This classification will be refined through the hazard identification and analysis.

It has to be taken into account that assumption TI_ASS_2 are essential for the safety analysis. In fact, the safety of train integrity confirmation system cannot be evaluated without reference to the complete operational context.

TI_ASS_2 must therefore be considered as a first set of "exported requirements" that are integral part of the safety analysis of the train integrity confirmation system.

The state of train integrity will be checked through a process, initiated automatically according to a configured cyclic timing or on demand. The following requirements specify conditions for its initiation and duration. Information sent by train integrity conformation system to other train protection functions refer to the outcome of this process.

Requirements

The system shall be able to confirm the integrity of a train, according to the following criteria:

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).

2. 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.

3. 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).

4. 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.

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

6. 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.

7. 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.

8. 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 speedand 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 Signaling Control Centre/traffic management system, (ii) active assisting locomotive/vehicle train is not being controlled from and providing traction power, not (principal) communicating with Signaling Control Centre/traffic management systemand (iii) inactive locomotive/vehicle not providing traction power and not communicating with Signaling Control Centre/traffic management system. States will only be changeable in initiation stage, NOT changeable whilst part of consist sending train integrity confirmation.

Comments

If two vehicles are considered “no more linked” when their distance exceeds a value Dand if the train consists of N wagons, M meter long each; the confirmation of integrity ensures a “safe maximum length of the train” of $N(M+D)$. Allowance shall be made for changes in train length and vehicle separation due to the tensile and compressive forces on the couplings between vehicles, the “safe maximum length of the train” shall include the maximum possible extension of the couplings. This influences the railway performance applications exploiting train integrity (e.g. train spacing in moving block or release of routes in interlocking functions).

Requirement TI_FS_4 takes into account the case of physical links (coupling) between vehicles breaking just after the system has checked their integrity. According to this, the train protection systems will still receive (for the last time) a confirmation of integrity but will evaluate the position of the train tail at the moment of initiation of the check, i.e. less advanced than the one where it should be if the train is still intact. This ensures safety, but also implies that, to avoid degradations of capacity, the duration of the check of integrity should be the shortest possible.

In the event that train integrity is not confirmed, then the last confirmed position of the tail of the train is applied to the traffic management system to determine the extent of the potential location of the tail end of the train, an extra factor should be taken into account. There is an additional hazard to consider that arises when the automatic air brakes fail or leak, this might lead to the unlinked tail moving independently according to its gradient.

The timing requirements of TI_P_1, TI_P_2, TI_P_3 and TI_P_4 are not considered safety relevant, because, as already introduced in Chapter 2, delayed or missing confirmation of integrity can be managed by railway traffic supervision functions in a way that safety is not prejudiced. For example, if a train reports its head position but has not updated integrity confirmation, the interlocking and/or train spacing functions can make the pessimistic assumption that the train tail is still in the last position previously reported. This increases train spacingand could also stop the traffic if no confirmation is possible any more, but this only affects system performance and not railway safety.

It is worth noticing here that, like requirements on acceptable distances between vehicles in a train, also timing requirements have an impact on the capacity of the rail system where train integrity is used. In fact, the position of the train tail can be updated on the control centre map only after reception of an updated train integrity conformation. Therefore, the train tail position will be considered less advanced than in reality, this will increase train spacing.

Considering a cycle of T sec between train integrity confirmations, with a train speed equal to V, the increase can be as high as VT . To evaluate the amount of the degradation of efficiency of train separation in moving block applications caused by train integrity confirmation performance, this value needs to be compared with the typical inaccuracies of train positioning, that currently (see ref [2]) is at least ± 5 m.

Regarding TI_P_1, the acceptable duration must be interpreted as a maximum time, within which the confirmation must be obtained, otherwise the system will declare the train integrity not confirmed. This can be implemented as a timeout for the reception of confirmation by the equipment at the train head. If the timeout expires before receiving confirmation, the integrity is considered not confirmed. The timeout should be a configurable parameter of the system and could be established as a function of the time taken for the initial confirmation of integrity check when the system is initialised during the train formation and network discovery phase.

In “on demand mode” this performance related to duration of the confirmation process can be checked measuring the time between the request from the external user and the sending of confirmation information to the external user.

About TI_P_3 it must be noted that this requirement is closely linked to the power consumption and the energy harvesting efficiency (see also comments in the section on RAM requirements below). There is a need to balance the need to confirm the integrity of the train (and therefore update the location of the tail of the train) frequentlyand the energy consumption of the system. The rate of updates of the location of the tail determines the influence of the system on the network’s capacity, since it determines how often the advancement limit of the moving block of a following train is updatedand the time at which clearance points (such as junctions) can be confirmed as having been cleared by the train. At lower speeds there is less power available from vibration energy harvester to provide to the train integrity system, however the distance the train moves in the interval between updates is less, therefore a lower update rate will have less impact on the interval to a following train. At higher speeds, more power is available for the train integrity system, so updates can be more frequent, which is useful as the train will be advancing at a faster rate, making more frequent updates more significant in terms of the distance covers. When the train has been stationary for a period of time the system would rely on stored power, however there is unlikely to be an unintentional change of train integrity condition and the train should be occupying the same trackand therefore place in the traffic management system, as the previous update, so a longer interval between updates could be acceptable. Also, on less intensively used routes where track occupancy and capacity is less of an issue, configuring the system to update less frequently could save power and have little to no impact on the number of trains using the route.

Requirement TI_P_2 is also related to power consumption, since it dictates the speed with which the integrity checks between two vehicles should be completed, also it specifies the speed of processing and communicating this information as well as processing other communications. For example, a rapid response might preclude energy saving techniques, such as switching some components to an idle mode, this means that the wake–up time would increase the system response time too much. It should be considered that TI_P_2 and TI_P_3 might vary for different states of the system; for example, there might be a low power mode that can be used when the train is stationary. In this case there is less power available from harvesting, but also an increased time to confirm integrity and time between checks might be acceptable.

2.3.3 Requirements related to characteristics of equipment

Environmental compatibility – see EN50155

Explanation

The following requirements refer to the conditions of the environment, where equipment must operate respecting the safety and reliability/availability requirements.

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

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_E_3: Immunity characteristics of equipment related to environmental conditions and shock/vibrations shall be specified making referring to recognized standards for railway applications.

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 toand not interfere with, domestic and industrial power supply and communication systems, which effects are present in the railway environment.

TI_E_5: Immunity and emission characteristics of equipment related to electromagnetic interferences shall be specified referring to recognised standards for railway applications.

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.

TI_E_7: Design of equipment shall permit the check of compatibility with laboratory tests.

Comments

The environmental conditions of railways are quite different, from mountains in north Europe to deserts in Saudi Arabia. It is not reasonable to mandate, especially at a very early stage of a project, the full compliance to such a wide variety of conditions. It is however essential that the design of equipment permits the check of compliance, to ensure that customers can identify with certainty and procure the products that fit their operational needs.

See [ref 8] and [ref 9] for existing harmonized standards applicable to the requirements exposed in this chapter.

To achieve enough immunity against electromagnetic fields, communication between equipment on adjacent cars should adopt a communication protocol stack implementing (e.g. at data link layer) negotiation of bit rate or repetition of corrupted or lost frames. This could delay the train integrity confirmation process. A good balance between speed of train integrity check and immunity to electromagnetic fields can be the target of on–site tests.

Pollution

Explanation

The following requirements refer to the need that equipment does not negatively affect the environment.

Requirements

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.

Comments

It is not expected that this kind of requirements will be difficult to respect for equipment dedicated to train integrity confirmation.

In particular, it should not be necessary to use consume materials like lubricants, liquids for refrigerators, etc.

It should however be considered that the possible use of batteries, even if small, will require some precautions for their storage and, especially, disposal at the end of life.

Health and safety (for workers and public)

Explanation

The following requirements refer to the protection of personnel against hazard possibly originated or propagated by equipment.

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).

TI_E_10 (toxic emissions): Equipment constituting the train integrity confirmation system shall comply with standards relevant to toxic emissions.

Comments

This kind of requirements are especially critical when trains run in long tunnels.

See [ref 10] for applicable regulations and standards.

Interfaces with other railway systems

Explanation

The following requirements refer to integration of train integrity confirmation equipment with other railway systems.

Requirements in this section refer to:

1. The equipment with which the train integrity confirmation system must cooperate (e.g. train protection) exchanging information according to interfaces and protocols, that must be as far as possible standardized. Thus, facilitating the adoption of the system in different applications world–wide and also support efficient and cost effective evolution following the technological development

2. The coexistence and compatibility of the train integrity equipment installed on a train with other railway systems, including train integrity equipment installed on other trains or isolated vehicles.

Requirements

TI_I_1: The train integrity confirmation system shall be able to receive commands to perform a confirmation process and to send information about the detected state of integrity to other on–board equipment (e.g. Automatic Train Protection).

TI_I_2: It should be possible to design and manufacture different versions of equipment that provide the same train integrity functionality compatible with different standard interfaces. The train integrity detection functionality of the system shall be compatible with other on–board equipment (as an input and/or output).

Note: the requirements above apply to the piece of equipment installed in the leading unit of a train.

TI_I_3: Equipment installed on vehicles shall have no interfaces, other than radio connections to exchange information with similar train integrity equipments on other vehicles and, if needed according to system design, interfaces for configuration at the moment of installation.

TI_I_4: Train Integrity confirmation shall work respecting safety and reliability/availability requirements in all operational conditions of a train, i.e. at standstill and moving in a shunting yard, a station or a line, independently of the presence of other communicating systems, including train integrity confirmation equipment installed on trains on adjacent tracks.

Comments

Requirement TI_I_4 refers to the fact that equipment belonging to the train integrity system on one train must be able to discriminate between messages that are part of normal operation of these systems and “spurious” messages originated by other systems or equipment. Correct operation of the train integrity confirmation system requires in particular that inappropriate communication with similar equipment installed on vehicles belonging to other adjacent trains and on isolated vehicles is recognized and ignored. This can be ensured by registering all the devices on the network during the installation phase.

Onboard Train Integrity interactions with train driver

Explanation

The following requirements refer to the interactions between the OTI system and the train driver.

The OTI system should present information to the train driver regarding the status of Train Integrity. In case of lost of communication between the Signalling Control Center and the OTI Control Module, train driver should be informed to immediately react in case of emergency situations.

TI_OR_1: OTI device, placed in the train’s driver cabin (OTI Interface Module), should inform driver about the state of the Train Integrity (confirmed/not confirmed) using alert messages displayed on the available display.

TI_OR_2: OTI device, placed in the train's driver cabin (OTI Interface Module), should inform driver about the state of the Train Integrity (confirmed/not confirmed) using light signal and/or sound signal (intermittent). Light signal and/or sound signal will be switch on in case of Train Integrity not confirmed.

TI_OR_3 OTI Interface module should enable the driver to alter the parameters of the OTI system (provided requiements 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 disolving network/consist at end of journey),
(ii) initiate network/consist descovery, and
(iii) update train formation data (list of vehicles expected in consist).

TI_OR_4 The OTI Control Module should NOT accept driver inputs from the OTI Interface Module which modify the validity of the train integrity confirmation (such as number of vehicles in cosist or initiate TI network discovery or modify association) if;

(i) the train on a managed part of the network and is moving, and
(ii) the OTI Control Module is part of the consist but is not the master module on the vehcile from which the train is being controlled.

For inputs which modify the validity of train integrity to be made (such as when intentional changes to train integrity are made or at the end of a journey) the OTI Control Module must NOT be sending train integrity confirmation.

Comments

Regarding Operating Requirement Ti_OR_1, OTI should interface with the available display connecting by bus and/or Ethernet protocol or be a separate display.

Note that TI_OR_1 and TI_OR_2 are Requirements related to managing situation of unavailable communication for broken link with Signalling Control Centre, or before link with Signalling Control Centre is established prior to entering the managed network.

Requirements TI_OR_3 and TI_OR_4 are guidelines; there is the requirement that the driver must be able to make modifications to the system in order to carry out normal operational functions. There is also the requirement that the control logic behind those functions and the sending of train integrity confrimation must ensure that the system is safe and that the system can not send train integrity confirmation signals which do not reflect the true state of the train/vehicles. The intention here is not to set out the exact logic of the system which ensures safety.

Compliance with EU and national laws (e.g. radio spectrum use)

Explanation

The possibility of placing equipment on the market and using it in railway application depends on compliance with applicable legislation.

Especially the selection of frequencies for radio communication need to be managed carefully, because there are important national responsibilities and it is possible that certain ranges are regulated in different ways in different countries. This is important for EU application and is even more critical if technical solutions that are acceptable in a wider area are envisaged.

Requirements

TI_L_1: Train Integrity confirmation equipment shall comply with EU legislation for placing on the market and integration in railway subsystems.

TI_L_2: Frequencies for radio communication shall be available for use in all EU countries.

Comments

Requirement TI_L_1 needs to be interpreted in a proactive way. Currently, EU legislation (ETCS specifications referenced in CCS TSI, see ref [2]) already provides concepts and requirements for the use of train integrity in interoperable train protection applications, however it does not provide yet any indication related to equipment necessary for its implementation. The results of ETALON must therefore permit the identification of subjects for standardization and the identification of new legal requirements (where they are necessary) in a format suitable for their inclusion in the existing legal framework (mainly the CCS TSI, in regard of ETCS system).

Installation

Explanation

The train integrity confirmation system needs to be installed on existing vehicles. In this context, it is critical for the success of the project that no major modification of the vehicles is required, installation must be as simple and cost effective as possible.

Requirements

TI_C_1: The train integrity confirmation system shall make use of pieces of equipment that can easily be installed:

1. On vehicles or units that can be used at the head of a train (specifically those vehicles that have the designated task of communicating with the traffic management system).

2. In suitable positions (to be specified during system design) of wagons or, in general, any kind of vehicle that can be trailed (including locomotives used in multiple configurations).

TI_C_2: Equipment installed on trailed vehicles shall not require cable connections of any kind with equipment on other vehicles.

TI_C_3: Train Integrity equipment shall be installed for long term periods on vehicles.

Comments

None.

Reliability Availability Maintainability (RAM)

Explanation

Train Integrity confirmation will be an essential functionality for the operation of a railway system.

The final objective is the elimination of expensive trackside train detection systemsand this implies that the operation of the railway system will completely rely on determination of train integrity.

Any loss of functionality (unavailability) of the train integrity confirmation system installed on a train, while not preventing the continuation of the mission of that train, will prevent the possibility for the control center to evaluate safe movement authorities for the other trains. As a matter of fact, from the point of view of traffic management, loss of confirmation of train integrity is equivalent to placing an obstacle on the tracks, blocking movement of trains.

Another important aspect of RAM is related to economic aspects.

Even where the targets for system availability can be achieved also in presence of equipment failures (implementation of adequate redundancies) a failed piece of equipment need in any case to be repaired. Keeping a good level of reliability and ensuring easy and cost–effective maintenance is therefore a key factor for the success of the project.

Requirements

TI_A_1 (availability): Unavailability of the train integrity confirmation system installed on a train shall not exceed the typical unavailability of on–board systems, whose failures can cause the blocking of the train (e.g. traction, braking).

TI_A_2 (availability): The architecture of the system should allow a scalable implementation, to adapt the availability to the real needs of different applications, avoiding unjustified high costs.

TI_R_1 (reliability): To evaluate equipment reliability, all failures requiring maintenance actions shall be considered, irrespective of their impact on operation (i.e. whether operation can be continued because of fall back equipment or not).

TI_R_2 (reliability): Failure rate of the train integrity confirmation equipment shall not exceed the typical failure rates of both on–board and track–side systems responsible of train protection.

TI_R_3 (reliability): The system should include options and procedures for degraded working whilst still ensuring safety.

TI_R_4 (reliability): There must be no operational degradation. The system shall not wear out over time.

TI_M_1 (maintainability): Failure conditions should be indicated as soon as possible.

TI_M_2 (maintainability): Equipment should provide as far as possible guidance to identification of defective parts.

TI_M_3 (maintainability): All equipment shall consist of parts easily removable.

TI_M_4 (maintainability): Substitution of failed parts and check of functionality after repair shall not require the moving of the vehicle into a maintenance facility with specialised equipment. Normal tools, such as those needed for normal mechanical operations on a bogie (torque wrench etc.). may be needed.

TI_M_5 (maintainability): Repair and check of functionality should be supported by specific easy to use tools.

TI_M_6 (maintainability): Equipment shall provide an indication “No Fault” for each of the parts when performs correctly.

TI_M_7 (maintainability): Equipment shall provide/storage maintenance–related information (faults and status records).

Comments

Requirement TI_A_1 refers to system non–availability due to the occurrence of equipment failures or loss of functionality and time to repair. The case of loss of functionality includes missing power or power too low to support communication between equipment installed on vehicles; this requirement needs therefore to be taken into account in the design of energy harvesting solutions for train integrity equipment.

The energy balance must ensure that the amount of harvested energy is sufficient to compensate the energy necessary for “stand by” operation and periodic data communication (see also requirements on performance TI_P_3 and operational requirement TI_O_4).

Other requirements that can be considered complementary to TI_A_1 and contribute to specify the full “operational availability” of the system can be found in the section related to operational conditions.

Quantitative values for TI_A_1 may be differentiated and tailored to system application, according to TI_A_2.

Requirement TI_R_3 refers to situations where the system is not operating within normal parameters, but can be operated in a mode which applies different rules to the status of the equipment that allow full or limited operations to continue whilst still ensuring safety.

An example might be that if a unit in the middle of a train fails completely but communications between vehicles either side of the one with the failed unit can be confirmed, thencompatibility the system enters a mode where the communication is used to confirm that the vehicles are within a specified distance and therefore the position of the tail of the train can be confirmed as being with a maximum distance of the nominal length of the train, which is added to the position of the tail of the train to increase the separation distance for following trains or clearance points. If communication is lost then the lower level of integrity is not confirmed and the last confirmed maximum position of the end of the train is used for traffic control. This would allow trains with failed units on vehicles to continue to the nearest yard or station and other trains to follow at a reduced speed and increased interval within safe limits until the defective train can be confirmed as having cleared the path for other trains. This would reduce the impact of a failure as it would prevent the train having to be stopped for a manual check of integrity and/or a manual inspection of the track to see if it is clear.

In the system design phase, regarding availability, intentional attacks causing “denial of service” (like damages of equipment or disturbance to communication) should be considered, in order to identify protections at least against the most common hazards (e.g. vandalism).

Encryption shall be sufficient to avoid brute force attacks.

The authentication method shall be safe to avoid MITM attacks

Replay attacks should be as well taken in account.

It shall respect CIA triad policy [ref11].

2.3.4 Requirements related to operations

Explanation

This is one of the most critical aspects for the introduction of train integrity confirmation systems and their acceptance by the railway operators.

The most important area for application of train integrity confirmation is the one of freight traffic, that is characterized by severe operational constraints that cannot be modified without economic consequences that would make the rail freight transport less competitive.

The first aspects to consider are related to operational procedures for the preparation of trains, these are already quite complex and should not be made more critical: requiring additional operations would increase costs, decrease efficiencyand would probably also increase the probability of human errors, thus decreasing system safety.

The second aspect is that the current way of working implies that a freight wagon is attached to different locomotives for different missions and can remain at a standstill even for several days (and quite far from its “home depot”).

In addition after the start of a mission, a freight train can be forced to stand still (waiting authority to proceed) for long periods of time, up to numerous hours.

Requirements

TI_O_1: Use of the train integrity confirmation system during operation (from beginning of train preparation to return to depot) shall not require:

1. Increase of staff for both on–board and trackside.

2. New complex staff competences.

3. New procedures that could delay the normal operations (from train preparation to recovery after end of mission) as performed today in systems without train integrity equipment.

TI_O_2: Train Integrity equipment shall not need operational intervention other than:

1. Switch on, switch off and entry of configuration data at start of mission, for equipment at train head.

2. Switch on and switch off for equipment installed on vehicles, if requested by energy management.

TI_O_3: Need of charging the energy storage unit should be limited as far as possibleand only in case of very long stops of vehicles between train missions or of failures. Ideally, there should be no external charging required at any time.

TI_O_4: The train integrity confirmation system shall be able to continue normal operation without any intervention for the whole mission, including a planned or not planned stop, between start and end of the mission.

TI_O_5: The train integrity confirmation system for each vehicle should contain the necessary information and vehicle parameters for that vehicles, initiate and configure the system. The system should be able to communicate the information and parameters throughout the network during initiation.

TI_O_6: The train integrity system shall be scalable (does not matter how many wagons the train has, it shall be possible to detect all the wagons and report the train integrity confirmation in a reasonable time).

Comments

During the system development phase, the requirement TI_O_4 will be further detailed, including the case of several stops (duration of each of them, time between consecutive stops, etc.). This requirement is strongly related with energy harvesting solutions.

Requirement TI_O_5: Information for the configuration of the system might include vehicle identification, vehicle length and vehicle maximum speed.

Requirement TI_O_6: In the scenario of a consist composed by multiple locomotives (passive and/or active), only the leading unit will be in charge of managing the train integrity confirmation process. The other locomotives will present the confirmation system but will be deactivated.

2.3.5 Summary of requirements affecting energy harvesting

All previous requirements must be respected during the development of the train integrity confirmation system.

All requirements have impact on the design of equipment. In the context of ETALON, it is important to identify in a special way the requirements affecting the energy harvesting solutions that are one of the most innovative aspects of the project.

Such requirements are:

1. TI_ASS_1
2. TI_P_3
3. TI_A_1
4. TI_O_2
5. TI_O_3
6. TI_O_4
7. TI_R_3
8. TI_E_8

3. TRACKSIDE ENERGY HARVESTING SOLUTION FOR OBJECT CONTROLLERS

3.1 GENERAL CONSIDERATIONS

Research on energy–harvesting applications has gained importance in the last decade, mainly because of the need to power wireless devices. The research in this area has increased the efficiency of devices in converting ambient free energy into usable electrical energy. The railway industry faces numerous challenges which will require autonomous radio communication units and innovative power sources often in hostile environmental circumstances.

The aim of energy harvesting technology in the railway industry is to avoid the placement of an expensive wiring structure to feed electronic devices on the track side, which have high installation and maintenance costs.

In order to be cost effective for the different applications, these radio communication units must be low cost and low maintenance. This presents challenges in terms of radio communication units calibration, packaging for survival in harsh environments and, particularly, the efficient supply and utilization of power. In addition, the performance of battery technology is gradually improvingand the power requirement of electronics is generally dropping.

Energy harvesting provides numerous benefits:

- ✓ Reduce installation cost: self–powered wireless sensor nodes (field elements to objects controllers and object controllers to interlocking) do not require power cables. They are easy to installand this allows to reduce the heavy installation and test cost.
- ✓ Provide long–term solutions: a reliable self–powered field element will remain functional as long as the ambient energy is available.
- ✓ Reduce maintenance cost and cost of equipment replacement (e.g. adjustments and concordance test in the field for cable replacement).

One objective of ETALON is to develop a prototype of an energy harvester to power the track–side object controllers and its associated communication system which forms part of the safety critical communications between the track–side and the trackside control centre. The aim is to enable a system which reduces the use of wiring.

The specifics objectives of this project are:

- ✓ Contribute to the deployment of Smart radio–connected track–side objects.
- ✓ Locally derived power supply for the communication system.
- ✓ Reduction of power consumptions by the communication system.
- ✓ Reduction of power cabling between interlocking and track–side object controllers.
- ✓ Availability of Maintenance Data.

Context of ETALON: describe a typical trackside architecture based on trackside control centre and object controllers to operate different pieces of equipment installed along the line.

Connections between object controllers and trackside control centre are critical for the safe and efficient operation of the railway network. These connections are currently implemented with wires and cables which have disadvantages due to costs of cabling, costs for maintenance of electronic equipment along the lineand substitution of cables in case of damage or theft.

Complete elimination of cabling seems impossible at the present stage: e.g. power required to operate switches. On the other hand, use of radio communication should eliminate cabling for communication and it seems also realistic to feed radio communication units through energy harvesting.

3.2 METHODOLOGY AND INITIAL ASSUMPTIONS

System concept: develop an energy harvesting solution, consisting in a unit that can be installed in sections close to stations or along a railway line and able to provide a reliable power supply for object controllers.

Assumptions on energy harvesting units:

- ✓ The unit must operate in typical railway environment, without requiring complex protective measures.
- ✓ Units should not require significant modifications of the existing infrastructure to enable them to harvest power.
- ✓ The unit should require minimal maintenance once installed.
- ✓ Units or modules should be easily replaceable on site.

Assumptions on equipment to be fed by energy harvesting:

- ✓ Radio Communication equipment, with a range up to several km, keeping the functionality of current wired communications between track side and trackside control centre Performance requirements can and should be adjusted to provide comprehensible parameters, adequate for wireless communications.
- ✓ The energy requirements to be supplied by the energy harvester is assumed to be the maximum power requirement of current object controllers, this could potentially reduce for new generations of smart track–side object controllers.

The project developed within ETALON activities relies on the following assumptions related to the technical solutions that will be adopted:

TEH_ASS_1:

1. The energy–harvesting system and the energy storage unit shall be sized depending on the power requirements of the components that are being fed by the system.

2. The energy–harvester shall operate in a wide range of conditions (Humidity, Temperatureand Weather).

3. All the connections (at least when referring to communication) between interlockings and objects controllers shall be unwired in order to reduce material cost, installation cost, maintenance cost, energy costand impact of cable theft.

TEH_ASS_2:

1. The object controller shall be able to communicate with the interlocking any time, no matter humidity, temperature, weather or other environmental conditions.

2. The object controller shall be able to communicate any time with its connected field elements.

3. The communication between object controllers and field elements shall be bidirectional to get field information and send orders.

4. The communication between interlocking and objects controllers shall be bidirectional.

5. The radio interface of the field elements, interlocking and objects controller should be in a licensed frequency band. This frequency band should be defined as soon as possible.

6. The field element shall send state information to its object controller.

7. The object controller should send field element and its own state information to the interlocking/control centre.

8. The object controller shall be potentially able to communicate to its neighbour object controllers when necessary.

9. The object controller operational state and communication traffic, processing and protocols should be optimised to minimise power consumption, whilst maintaining the required communication link.

Comments

None

3.3 REQUIREMENTS

3.3.1 High level functional requirements

Definitions

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

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_Deffinition_C: The Object Controller Wireless Communications is a device or module which provides communications between the Object Controller and the control center, 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 control centre, other object controllersand track–side objects.

OCWC_Functional definition: A device able to provide wireless communications capability for following interfaces: trackside control centre (interlocking) – object controller – trackside object; object controller – neighbour object controller. For the sake of simplicity these interfaces will be referred under the collective term control centre– trackside communications along the Chapter 4.

Top hazard

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.

Exported Safety related requirement: loss of communication with object controllers must be safely managed by the trackside control centre and not lead to an accident.

Requirements

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

OCWC_FN_2: The 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 communications between 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 informationsand 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 control centre– trackside communications (e.g., latency, throughput, etc.) (ref. [12])

OCWC_P_2: The OCWC shall have sufficient reliable communication range (with minimal power usage) to assure 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 control centre (or the 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 control centre–trackside communications with defined range during the duration of mission.

Comments

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 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 optimisation 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 control centre, but for efficient operation it should be as short as reasonable possible.

3.3.2 Functional and performance requirements

The energy harvesting solution shall at least ensure power for the object controller and the radio communication inputs, outputs and the supervision of the state of communication system.

Other types of equipment which are to be powered should be defined during system design.

OCWC Requirements

OCWC_FS_1: The services for the transmission and reception of messages shall be defined.

OCWC_FS_2: The reception service shall be able to confirm the reception of messages to the transmission service.

OCWC_FS_3: The connection and disconnection services shall be defined. These services shall be able to engage and to release the connection whenever necessary under the request of end devices (e.g. interlocking and object controllers).

OCWC_FS_4: The device shall be able to report its state under request at least, but not limited to “idle”, “busy” and “fault”.

OCWC_FS_5: The device shall be able to report its state under request at least, but not limited to “idle”, “busy” and “fault”.

OCWC_FS_6: The device shall possess a unique identifier to be able to discriminate between devices connected to the same communication network.

OCWC_FS_7: The interfaces to external communication network shall be considered and implemented correctly where necessary.

OCWC_FS_8: The time sequence and the flow of control data shall be considered.

OCWC _FS_9: It shall include CIA triad policy [ref. 11].

OCWC_P_1: The bandwidth needed for the communication between devices should be properly sized and taken into account when designing the system.

OCWC_P_2: The distance between relays (where present) to propagate the signal between field elements or/and interlocking, should be taken into account (e.g. attenuation, delay).

OCWC_P_3: The communication protocols employed should be energy aware in order to minimize the energy consumption.

OCWC_P_4: the antenna shall be selected to minimize the energy consumption, radiated powerand the interference of the signal.

OCWC_P_5: Data concerning the status of the track and field elements have to be transmitted close to real time [with max delay ≤ 0.5 seconds].

OCWC_P_6: It shall be possible to configure the acceptable interval of the trackside communication confirmation process.

OCWC_P_7: A multipath structure should be taken into account in the design in order to increase reliability in case of failure.

TEH requirements

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 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 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 control centre in the same way as "communication loss".

3.3.3 Requirements related to characteristics of equipment

Environmental compatibility

Explanation

The following requirements refer to the conditions of the environment, where equipment must operate respecting the safety and reliability/availability requirements.

Requirements

TI_E_1 (climate – immunity): The trackside energy harvesting 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

TEH_E_2 (vibrations): The trackside energy harvesting system shall operate in the railway environment. The system shall be demonstrated as being able to operate within conditions representative of the railway environmentand be considered suitable for operation with full nominal performance in relation to environmental/vibration conditions either directly or with further ruggedization and development.

TEH_E_3: Immunity characteristics of equipment related to environmental conditions and shock/vibrations shall be specified making reference to recognized standards for railway applications.

TEH_E_4 (electromagnetic compatibility – immunity and emissions): The trackside energy harvesting 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, which affect or are present in the railway environment.

TEH_E_5: Immunity and emission characteristics of equipment related to electromagnetic interferences shall be specified making reference to recognised standards for railway applications (EN 50121–4 and EN 61000–6–2).

TEH_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.

TEH_E_7: Design of equipment shall permit the check of compatibility in the lab.

TEH_I_1: All pieces of equipment, field elements shall be interoperable, different products from different vendors/manufacturers shall be able to work together seamlessly.

Reliability Availability Maintainability – RAM

TEH_A_1 (availability): Unavailability of the object controller due to loss of power or communication shall not exceed the typical unavailability of object controllers due to loss of power or communication.

TEH_A_2 (availability): The architecture of the system should permit scalable implementation, to adapt the availability to the real needs of different applications, avoiding unjustified high costs.

TEH_R_3 (availability): There must be no operational degradation. The system shall not wear out over time.

TEH_R_1 (reliability): In the evaluation of equipment reliability, all failures requiring maintenance actions shall be taken into account, irrespective of their impact on operation (i.e. whether operation can be continued because of fall back equipment or not).

TEH_R_2 (reliability): Failure rate of the object controller due to power loss, or loss of communication shall not exceed the typical failure rates for object controller power and communication. Also it shall not exceed the typical unavailability of railway radio communications which failures provoke the system entering safe state.

TI_M_1 (maintainability): Failure conditions should be indicated as soon as possible.

TI_M_2 (maintainability): Equipment should provide as far as possible guidance to identification of defective parts and power faults.

TI_M_3 (maintainability): All equipment shall consist of components/modules which are easily replaceable in the field.

TI_M_4 (maintainability): Repair and check of functionality should be supported by specific easy to use tools.

TI_M_5 (maintainability): Equipment shall provide an indication “No Fault” for each of the parts when performs correctly.

TI_M_6 (maintainability): Equipment shall provide/storage maintenance–related information (faults and states records).

3.3.4 Requirements related to the operations

The energy harvesting (and storage) unit shall be able to deliver sufficient power without interruption for the operation of the powered devices. This should take into account:

- ✓ Power requirements for normal operations.
- ✓ Power requirements for short periods of exceptional operations (e.g more trains than usual).
- ✓ Variation in harvested energy through the daily and yearly cycle.
- ✓ Variation in interval between passing trains.

The units should not require additional maintenance or other operations requiring site visits than the current system, or at least, the benefits of the units should exceed the operational disadvantages of them.

Explanation

It is important for the introduction of energy harvesting and wireless communication for object controllersand the acceptance by the railway operators that the system does not require additional operators. Requiring additional operations would increase costs, decrease efficiencyand would probably also increase the probability of human errors, thus decreasing system safety.

Requirements

TEH_E_1: The power consumption of the equipment shall be as low as possible.

TEH_O_1 The use of energy harvesting for object controllers shall not require:

1. Increase staff on trackside.

2. New complex competences of staff.

TEH_O_2 Trackside elements should decrease:

1. Maintenance..
2. Cost.
3. Set up complexity.

TEH_O_3 Need of changing or charging batteries manually should be limited as far as possible, only in case of bad weather conditions (ex. too much cold) sabotage and unpredictable events.

TEH_O_4 The energy harvesting and wireless communication elements of the object controller should have similar or longer life than current systems.

TEH_O_5: All modules of the object controller or field elements (e.g. radio interface) shall be interchangeable without the replacement of all the equipments (cost reduction).

Health and safety (for workers and public)

Explanation

The following requirements refer to the protection of personnel against hazard possibly originated by or propagated by equipment.

Requirements

TEH_HS_1: The radiated energy of the radio interface shall be compliant to the European standards and not be dangerous to the health.

TEH_HS_2 (fire): Equipment constituting the energy harvesting, storage and communications for the object controller shall comply with standards relevant to fire propagation.

TEH_HS_3 (toxic emissions): Equipment constituting the energy harvesting, storageand communications for the object controller shall comply with standards relevant to toxic emissions.

TEH_HS_4: All the edges of the equipment will be rounded to avoid injuries during the manipulation.

4. REFERENCES

[1] A general description of railway signalling functions with further references can be found at: https://en.wikipedia.org/wiki/Railway_signalling

[2] ETCS specifications can be found in the website of the European Union Agency for Railways: http://www.era.europa.eu/Core–Activities/ERTMS/Pages/Current–Legal–Reference.aspx

[3] A general explanation of fixed and moving block concepts can be found at: http://www.railway–energy.org/static/Moving_block_81.php

[4] EN 50126 – Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[5] EN 50129 – Railway Applications – Communication, Signalling and Processing Systems – Safety Related Communication in Transmission Systems.

[6] Railway accidents classification can be found in the "Definitions of UIC safety data–base" (http://uic.org/forms/IMG/pdf/definitions_en.pdf) and in the documents on "Common Safety Indicators" issued by the European Union Agency for Railways (http://www.era.europa.eu/Core–Activities/Safety/Safety–Performance/Pages/Common–Safety–Indicators.aspx)

[7] EU Regulation 402/2013

[8] European Standard for environmental compatibility EN 50125

[9] European Standard for EMC EN 50121

[10] COMMISSION REGULATION (EU) No 1303/2014 of 18 November 2014 concerning the technical specification for interoperability relating to 'safety in railway tunnels' of the rail system of the European Union

[11] CIA triad (Confidentiality, Integrity and Availability) is a model designed to guide policies for information security within an organization: (http://whatis.techtarget.com/definition/Confidentiality–integrity–and–availability–CIA)

[12] X2R–WP03–D–SIE–005–01– X2Rail–1 (H2020–S2RJU–CFM–2015–01–1) Deliverable D3.1 User & System Requirements (Telecommunications) 01/09/2016.