ETALON

D 3.4 Train Integrity Methods Power Requirements and System Analysis

Due date of deliverable: 01/09/2018

Actual submission date: 15/10/2018

Leader of this Deliverable: David Vincent, Perpetuum

Reviewed: Yes

Document status		
Revision	Date	Description
1	March 2018	Draft
2	Oct 2018	Update following peer and TMT review
3	Oct 2018	Quality 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
David Vincent	Perpetuum	Document leader
Alexander Pane	ISMB	OTI Methods and general document review
Paul Hyde	UNEW	FMEA
Veronika Nedviga	Ardanuy	Safety systems
Roberto Cafferata	SIRTI	General editing revision

Table 1 - List of Acronyms

EXECUTIVE SUMMARY

This report includes an analysis of On-board Train Integrity (OTI) methods in the context of energy harvesting. Actual power requirements and energy balance calculations are included in D3.2 and D4.2 respectively. An FMEA is included for the operating parameters of the platform.

Task 3.3 – On-board Train Integrity Function and Trade-off Analysis

(Task Leader: PER, Task Contributor: ARD, ISMB, UNEW), Starting at month 3– Ending at month 12

Starting from the functional requirements defined in T2.3, this task will deliver an analysis of the functions (what it needs to do) and functionality (how quickly and frequently it will need to do it) within the limitations of power available and reliability (safety integrity) of the system. Alternative methods of meeting each requirement will be analysed. Each component of the system will have minimum power requirements to deliver reliable service, according to the communication systems defined in T3.1 and functional requirements defined in T2.3.

Perpetuum will calculate the power requirements and develop a test platform with a radio output and power demand platform as described by these requirements – this will be used in system testing. An FMEA will be organised with the other task partners to perform an in-depth analysis of the system. Contributors to the task will deliver information on harvester characteristics, power supply and storage technologies, operating conditions of rolling stock and system safety requirements to implement a comprehensive FMEA.

D3.4 – Train Integrity Methods Power Requirements and System Analysis (M12)

A report will be delivered to fulfil the call deliverable 1b), identifying the power requirements of the on-board energy harvester technologies, as defined by the communications specifications defined in T3.1 and T3.2. This report will contain a description of the power requirements (harvesting, storing, supplying) of the lowest power method capable of achieving train integrity as specified in T2, as well as also describing other methods where the power required is within the availability foreseen in T4.2. This report will include a description of the operating parameters of the test platform and the output of the FMEA.

TABLE OF CONTENTS

Report Contributors 2
Executive Summary 3
Table Of Contents 4
List of Figures 5
List of Tables 5
List of participants 6
1. Introduction 7
1.1 List of Acronyms 8
1.2 Train Integrity Fundamental Requirements 9
1.3 Phases of Operation for Train Integrity Functions 10
1.4 Operational Train States Affecting Train Integrity Operation 10
1.5 SIL-4 and How It Affects Energy Requirements 10
1.6 System Components 11
1.7 Function – Energy Balance 11
1.8 FMECA Methodology 12
2. Train integrity methods 12
2.1 X2Rail-2 Proposal – energy Harvester Powered Communication and Explicit Location and Inertial Navigation Unit. 13
2.2 ETALON Developed OTI Method 15
2.3 Alternative Proposal (not developed) 17
2.4 North American End of Train Device 17
3. FMECA 18
4. Discussion 38
5. Conclusions 38
6. REFERENCES 39

LIST OF FIGURES

Figure 1 - Class 2C configuration, X2R2-TSK4.3-T-ANS-003-01_-_X2Rail-2_WP4_Technical_Note_Overview_of_the_Functional_Requirement_Specification 13
Figure 2 - ETALON Developed OTI With VEH 16

LIST OF TABLES

Table 1 - List of Acronyms 2
Table 2: FMECA for ETALON OTI 18

LIST OF PARTICIPANTS

N°	LEGAL NAME	SHORT NAME
2	SIRTI - SOCIETÀ PER AZIONI	SIRTI
3	ARDANUY INGENIERIA SA	ARD
6	ISTITUTO SUPERIORE MARIO BOELLA SULLE TECNOLOGIE DELL'INFORMAZIONE E DELLE TELECOMUNICAZIONI ASSOCIAZIONE	ISMB
7	PERPETUUM LIMITED	PER
8	UNIVERSITY OF NEWCASTLE	UNEW

1. INTRODUCTION

The central output of this deliverable is a system analysis of the train integrity method, based on state diagrams and a Failure Mode, Effects and Criticality Analysis (FMECA) for the OTI system as proposed and described in D3.2 and D4.2. Power consumption and energy balance are included in these other deliverables also. The intention of the deliverable is to show that with the limited energy production and storage available, it is possible to implement a viable train integrity system.

1.1 LIST OF ACRONYMS

EH	Energy Harvester
EoT	End of Train
Dx.y	Deliverable code number x.y
FMECA	Failure Mode, Effects and Criticality Analysis
GNSS	Global Navigation Satellite System
OTI	On-board Train Integrity
PV	Photo-Voltaic
RPN	Risk Priority Number
UIC	Union Internationale des Chemins de Fer
UWB	Ultra-Wide-Bandwidth
VEH	Vibration Energy Harvester
UHF	Ultra High Frequency (around 1GHz in this work)
VHF	Very High Frequency (up to 300MHz)

1.2 TRAIN INTEGRITY FUNDAMENTAL REQUIREMENTS

A set of formal statements describing the train integrity system is contained in D2.2 – "System Requirements Specification". Please refer to that document for details. A summary of train integrity (high level) requirements, as interpreted by the work in D3.2 "On-Train Communication Systems and RF Components Report", is as follows:

1) Train Integrity is the confirmed knowledge that all the vehicles that are understood to be part of the same train by the signalling system are, in fact, still connected and part of the same train. This safety critical information is typically established by counting axles of a train passing into and out of a fixed signalling block.

2) Train integrity is established in this work by checking integrity of all couplings in the train; explicitly by measuring separation distance between vehicles (using UWB radio devices designed for radio location) and implicitly by maintaining regular radio communication with all vehicles (particularly the end of the train) using a short range (sub GHz) radio and customized radio network protocol.

3) Like any electronic system, this technology is subject to a number of potential failure mechanisms. The objective of the FMECA is to demonstrate that all conceivable failure mechanisms are fail safe (i.e. never produce a false positive OTI result). Minimising the number of false negative results (stating that the train has lost integrity when it hasn't) is therefore a problem of reliability, not safety.

4) The objective of this development is to establish a minimum level of communication and sensor activity that is necessary for OTI, in order to establish the minimum amount of energy required to support that activity (applying the usual modern techniques for optimising power consumption). Other methods could be used, but energy harvesting should be able to support the amount of data flow required.

5) The complementary project X2Rail-2 TIN_OTI_4 overview of the Functional Requirement Specification includes, in addition to the communication network down the train (harvester powered), a slave module at the back of the train for establishing OTI (proposed harvester power). To supply the energy required for all the potential functions listed for this device (inertial and GNSS navigation) a significantly larger harvester, bogie mounted, may be necessary (power depends on harvester mass). Field trials in WP5 will determine if there is a realistic amount of energy available from this technology to power near-continuous GNSS and inertial navigation (by testing standard size harvesters and measuring vibration). It should be noted that accurate acceleration measurement for the purpose of speed assessment is very difficult from the axlebox, due to the vibrational noise present generated from the wheel-rail interface (the vibration necessary to power the measurement is also responsible for limiting the type of information available). In the OTI scheme from ETALON the functional train integrity is shared between all sensors, thus increasing the amount of energy available to train integrity sensing (more harvesters involved in the task). It is possible that an alternative location for slave OTI functions is in the tail light, which already has a large battery, fitment and maintenance operations with it.

6) If a slave OTI is required, it may be more economical and reliable to use video technology to measure train speed over the tracks. Frequent transmission of speed would not be dependent on availability of GNSS satellites or accumulated speed errors using inertial navigation. Identical devices at both ends of the train may be more reliable than other approaches. Appropriate technology is currently deployed on a passenger fleet in the UK.

1.3 Phases of Operation for Train Integrity Functions

For train operation and system design purposes, the following OTI system states have been defined (these are a superset of states defined by complementary project X2Rail-2):

- Confirmed;
- Integrity lost;
- Reforming consist;
- Not active;
- Topology discovery.

These states correspond to vehicle states covering loaded/not loaded, in/out of a consist, moving/not moving. The challenge for OTI is to establish and maintain an accurate train integrity state for all these conditions, to handle the transitions between these states as smoothly as possible, and to require the minimum amount of manual intervention for the process. Any manual intervention must obviously be fail safe when errors occur.

More details are available in the ETALON WP2 (refer to deliverable D2.1 “Functional Requirements Specification” and D2.3 “System Requirements Specification”).

1.4 Operational Train States Affecting Train Integrity Operation

The major challenge for an energy harvester powered OTI is to maintain the correct OTI state when the train is stationary (no Vibration Energy Harvester (VEH) output), moving slowly (regular updates but low energy available) or establishing OTI (probably slow moving but more activity required). The energy balance for these activities is more deeply analysed in D4.2 “On-board Energy Harvester, Power management and Energy Storage”.

1.5 SIL-4 and How It Affects Energy Requirements

It is not the intention of this work to develop a SIL-4 qualified system, but it is necessary to assess how SIL-4 could be achieved with the tools and technologies described. In the system proposed in

this work, the design of the method for OTI delivers a SIL-4 functionality through fail-safe communication (not possible to transmit a false positive OTI confirmation). Reliability is delivered through ubiquitous installation of energy harvester powered devices and redundant functionality. Harvester power permits multiple transmissions and measurement of the same data without impacting fixed energy constraints (as is the case with battery power). Frequent measurement of the conditions, required to establish OTI, is also enabled by harvester power.

1.6 System Components

System components, including the energy harvester, energy storage, communications and sensors are described in D4.2 “On-board Energy Harvester, Power management and Energy Storage”. Solution, design and predicted performance report for adapted or developed solution and D3.2 “On-Train Communication Systems and RF Components Report” respectively. For the purposes of an OTI implementation, the following points should be noted:

1) Electronics design: Components and electro-mechanical design should be implemented respecting the high vibration environment on the axlebox. Refer to EN50155 for standards defining vibration testing. Large components such as energy storage devices should be supported or encapsulated. PCBs should be supported to avoid significant resonances.

2) Any external antennas should be protected from impacts (ballast strikes etc.).

3) The geometry of a wireless network changes continuously on any journey. Network geometry/routing should take this into account.

4) The availability of external communication links throughout a journey (GNSS and mobile data) is not necessarily guaranteed.

1.7 Function – Energy Balance

The desired frequency of train integrity checks, when powered by energy harvesters and as stated during discussions with complementary project X2Rail-2 (Cola meeting, Genoa, 2017) is a check every 5 seconds for high speed traffic on high use routes, dropping to every 30 seconds minimum requirement acceptable on low use routes (unless the train is running at low speed for very extended periods, a 5 second interval could be maintained). Achieving the correct balance between harvester output, energy storage and energy demand is possible through the use of modern low power communication and a system that shares communication burden between many independent OTI sensors. This is more deeply illustrated in D3.2 “On-Train Communication Systems and RF Components Report” and D4.2 “On-board Energy Harvester, Power management and Energy Storage”. The key to achieve these design aims is to minimise the active, high power usage time.

1.8 FMECA METHODOLOGY

FMECA (Failure Mode, Effects and Criticality Analysis) is a technique for systematically examining the possible failure modes of the components of a system, evaluating the higher-level consequences of failures as well as the range of causes. The simple approach is to break down the system under examination into its component parts, list the possible failure modes then follow through to the consequences by applying an understanding of the component function and the system design. The severity and likelihood of the failure are both used to evaluate the seriousness of any failure mode, and this, in turn, is used to assess the effectiveness of any mitigation that is already in place or the need for further mitigation. At the end of the design process there should be no unacceptable failure modes remaining (the scope of the project will determine).

2. TRAIN INTEGRITY METHODS

The following are examples of possible train integrity methods, either proposed by complementary project X2Rail-2 and developed within ETALON or proposed but not developed by ETALON. All methods discussed here are technically feasible if power consumption is not a factor. In each case the impact of energy harvesting and possible mitigation for power consumption problems is discussed. If a battery supply is proposed, it is in the context of there being a pre-existing battery application and maintenance action required for normal freight traffic.

The fundamental requirement of OTI is to deliver a failsafe report on the presence (or otherwise) of the complete train as a coherent consist. Any loss of vehicles from the train must be detected in a sufficiently short time that any following train has enough headroom to stop. Clearly the signalling system must be capable of stopping a following train, even if there is a false alert from the OTI system, or if the OTI itself fails. The assumption therefore is that only the positive confirmation of train integrity must achieve a SIL-4 confidence. Other failures have an impact on reliability, but not safety. Poor reliability, however, impacts the operational and economic viability so it must be high, although it is a less demanding task to demonstrate fail-safe operation than it is to demonstrate reliability to the same level.

Assessment of OTI methods in this document is focussed generally on the viability of energy harvesting as a source of power. It is not intended that this is an exhaustive assessment of OTI method viability.

2.1 X2RAIL-2 PROPOSAL – ENERGY HARVESTER POWERED COMMUNICATION AND EXPLICIT LOCATION AND INERTIAL NAVIGATION UNIT.

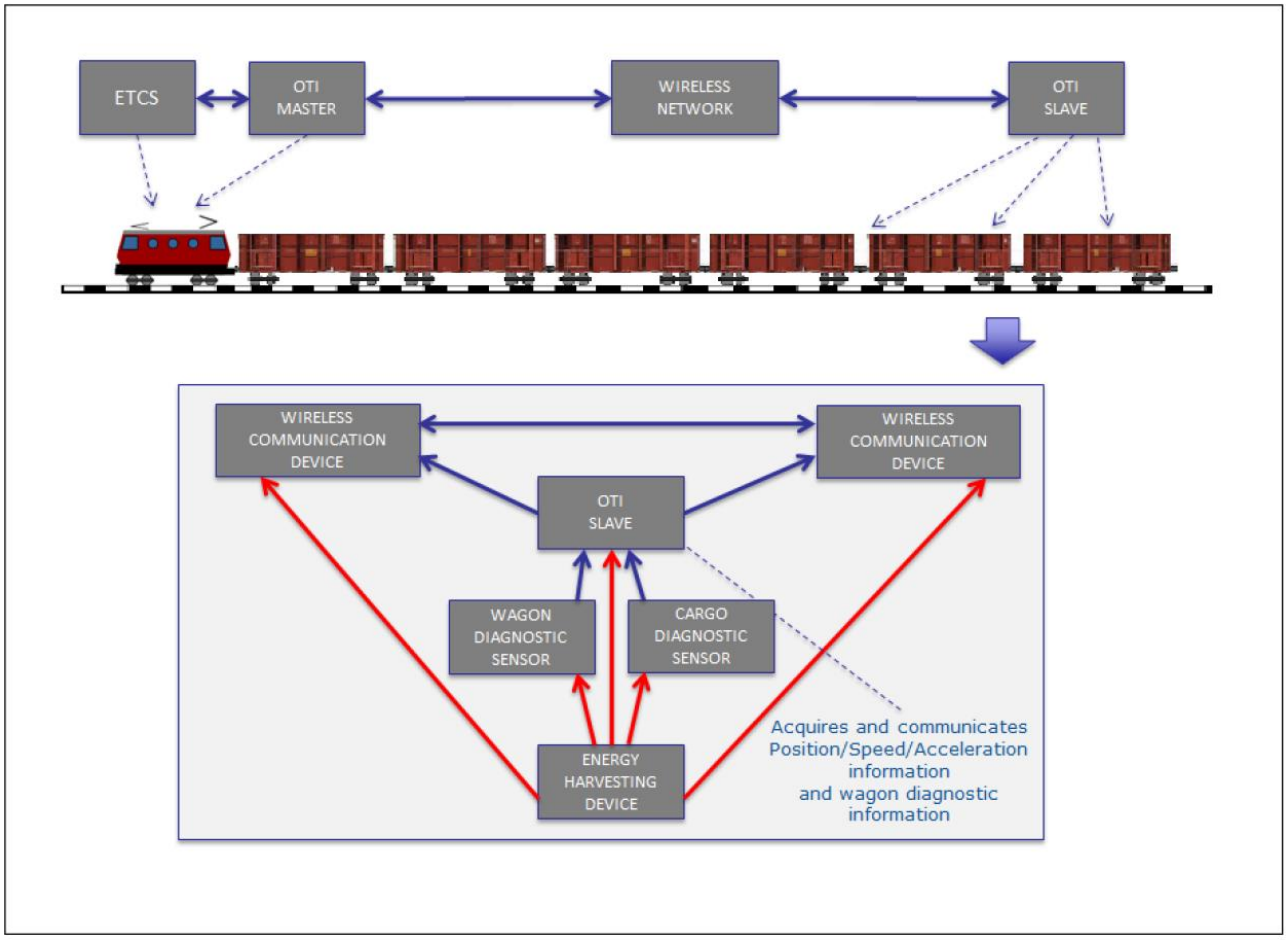


Figure 1 - Class 2C configuration, X2R2-TSK4.3-T-ANS-003-01_-_X2Rail-2_WP4_Technical_Note_Overview_of_the_Functional_Requirement_Specification

The complementary project X2Rail-2 proposal uses a combination of harvester powered, vehicle mounted devices. Some for communications (and additional cargo or vehicle monitoring applications) connecting a multi-functional OTI slave, mounted at the rear of the train. Functionality of the OTI slave is similar to that of an EoT (End of Train) (see section 2.4 below), but in place of a high power, VHF radio (the major power consumption source in these devices), the OTI exploits lower power UHF radio to communicate with the OTI master (indirectly benefitting from axle mounted VEH). Until some freight vibration harvester testing is completed, it remains to be seen if a VEH would be sufficient (as the sole power source) to power an OTI slave, particularly since it would probably be bogie or vehicle mounted (not axle box mounted). Power could be supplemented by solar PV (Photo-Voltaic) and a rechargeable battery, since these devices will be manually placed on the end of the train, and therefore already incur maintenance effort.

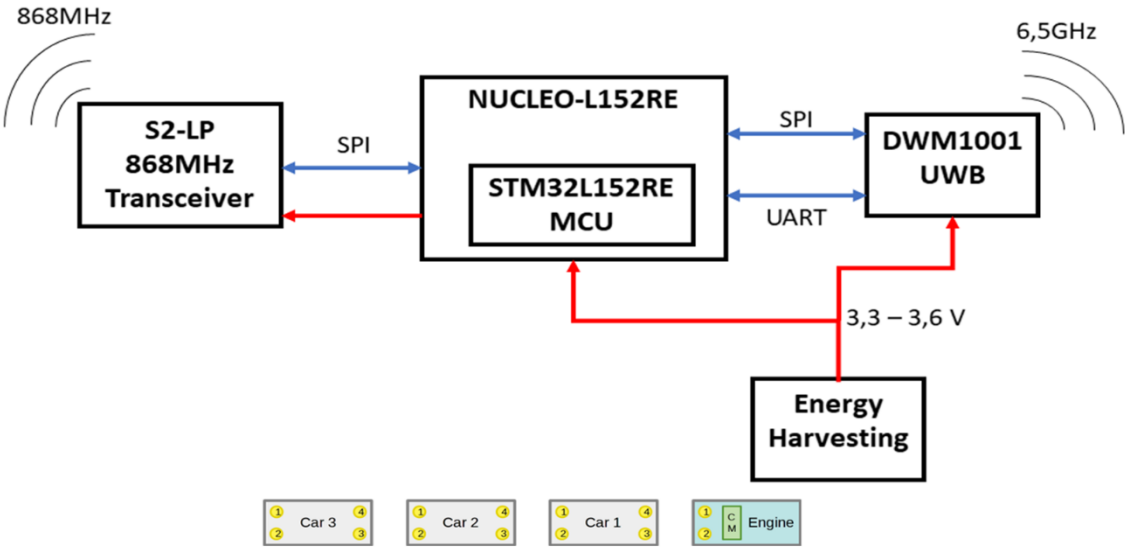
The advantage of this system is that it requires positive identification of a defined EoT device to the OTI master in the locomotive. This removes dependence on completion of individual OTI actions between each vehicle and removes dependence on the correct set of vehicles being identified. The technical risk of this approach is that without an adequate backup power supply, the power requirements of the GNSS and inertial navigation systems may be excessive for reliable operation on long journeys, or intermittent travel in Northern Europe in the Winter.

It should also be noted that GNSS work best when the antenna has a clear view of all relevant satellites, which in this scenario is not always the case (tunnels, forest, cuttings etc.). When travelling through areas with poor GNSS reception, it may be necessary to revert to alternative methods of TI (axle counting through tunnels) or include a reliable backup location and inertial navigation method (trackside radio beacons). This could increase the complexity of this approach significantly.

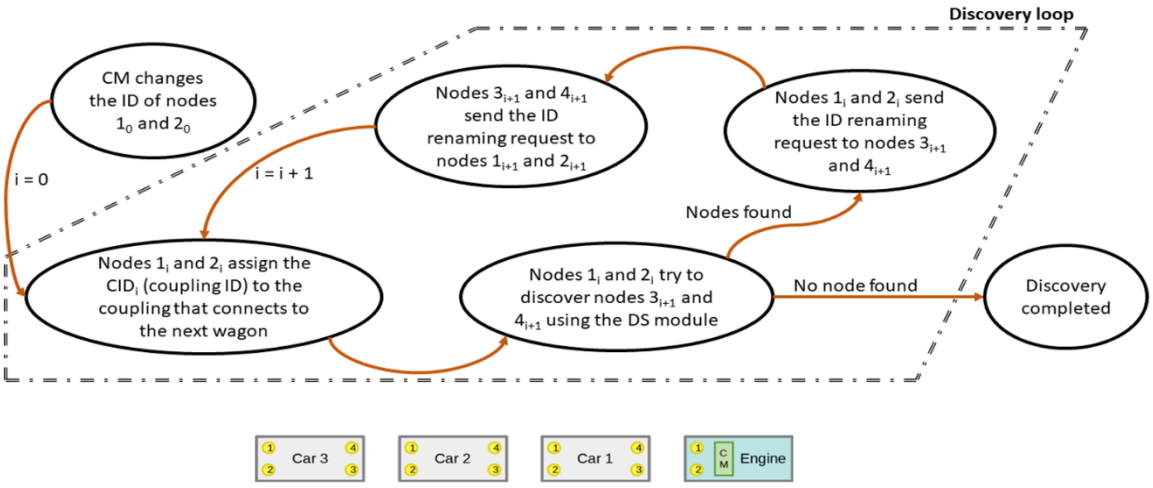
2.2 ETALON DEVELOPED OTI METHOD

The ETALON developed OTI method uses a single sensor type, with no explicit end of train device (OTI slave). Principal, primary (and positive) train integrity confirmation is achieved by reporting the distance between consecutive vehicles in the train. Each node includes a UWB distance sensor that communicates with nodes in the adjacent wagons to establish proximity. By performing this operation from the locomotive to the tail of the train it is possible to both establish the contents of the consist and verify that vehicles are next to each other. Continuous assessment (every 5-30 seconds) of this distance during the journey confirms the integrity status of the train. Continued communication with all nodes in the train can be used as a secondary check of integrity, even if there is a fault with the distance measurement, although the maximum theoretical length of the train would inevitably be greater using this approach, due to the distance uncertainty of this radio link.

Examination of the FMECA for the ETALON developed OTI solution does expose some non-failsafe failure modes. These could be resolved through appropriate extensions to the protocol, including communications strength/communications returns from vehicles to confirm presence even in the absence of distance measurement. This may, however, add unacceptable effective length to the train since radio range can be highly variable.



Each group of 4 OTI nodes that belong to the i^{th} wagon (numbered from 1_i to 4_i) know each others ID beforehand. The CM also knows beforehand the IDs of nodes from 1_0 to 4_0



Loop to check the TI by checking all Coupling Integrity (CI)

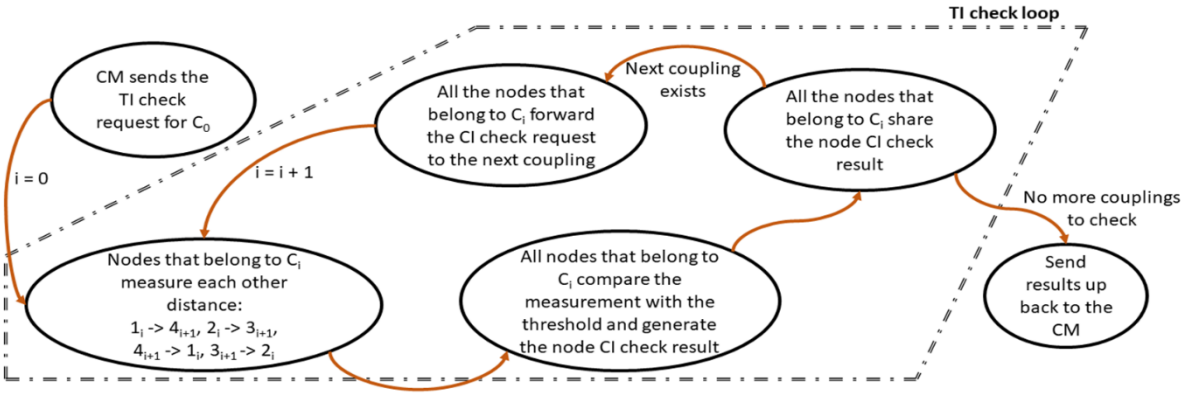


Figure 2 - ETALON Developed OTI With VEH

2.3 ALTERNATIVE PROPOSAL (NOT DEVELOPED)

In place of distance measurement between vehicles combined with communication integrity, or communication to OTI slaves equipped with GNSS and inertial navigation units, an alternative approach could be to report the ground speed of the end of the train using high speed infra-red video technology. This information could be communicated from the slave unit to an identical master unit at the front of the train (communication over harvester powered wireless sensor nodes on the other wagons), with the differential speed being a fast response and accurate indication of the continued attachment of the end of the train. A similar approach is already used to detect roll back on passenger service in the UK [1]. This method would work in areas with poor GNSS coverage, and under all weather conditions. Power consumption is unknown but modern technology should be able to deliver a battery powered device incorporated with the tail light.

2.4 NORTH AMERICAN END OF TRAIN DEVICE

In North America, the use of pneumatic power derived from brake pressure is seen as an acceptable power source for EoTs. This power, in conjunction with a battery supply, is used to power regular GNSS readings and a high power (5W) VHF transmitter (using allocated radio channels) that sends EoT readings directly to the locomotive. An example of this technology is shown in [2] Although this technology is interesting as an alternative approach, neither the long-range VHF radio nor the use of brake pneumatic air to power the device are available in an European application. The aspect of this device that could be applied to Europe, however, is the inclusion of significant functionality in the tail light.

A condition for fail safe operation in this case would be fitment of the device preventing the addition of further vehicles behind it. There is a protocol established to make sure that the track side maintenance worker fitting the device confirms the correct device number to the driver, thus achieving OTI without being aware of the contents of the consist.

3. FMECA

S = Severity. O = Occurrence. R = RPN.

Following is an example FMECA output for the OTI system developed by the ETALON project as an example application powered by energy harvesting (from vibrations). Clearly this process should be carried out for any proposed OTI system. An assessment of any major flaws in the proposal is included in the discussion, together with an overview of how changes to this approach might resolve the major risks.

Table 2: FMECA for ETALON OTI

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
Energy Harvester	Harvester	EH-1:No output from the harvester	Harvester broken/impact allows water ingress.	Run energy down, stop responding	Node becomes inactive	Node stops reporting status, OTI relies on other nodes/redundancy	Redundant, multiple paths for integrity and communication	Y	1	1	1	Multiple overlapping node failures = TI not confirmed and/or failure to discover network operational failure. Reliability, not safety problem.
	Harvester	EH-2Low energy output	Harvester partially broken/circuit power demand high	Lower communication rate, might not be able to measure distance	Node becomes intermittent, possible loss of topology discovery	Node may report status but not wagon distance	Rely on other nodes nearby for redundancy	Y	1	1	1	Multiple overlapping node failures = TI not confirmed and/or failure to discover network operational failure
Communication Network	Antenna damage	CMN-1: Repetition of old message	Message repeat due to missed acknowledge	Poor OTI comms performance	Slow to confirm OTI	OTI time extended, train longer	Quality antenna, protected, diverse	Y	2	3	6	
	Antenna damage	CMN-2: Loss of message	Antenna misalignment/fading	Poor OTI comms performance	Slow to confirm OTI	OTI time extended, train longer	Quality antenna, protected, diverse		1	4	4	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Antenna damage	CMN-3: Node insertion (other train node, error of network)	Antenna misalignment/ reflexion	Incorrect OTI data	OTI not confirmed	Slow to confirm until train in motion	Distance measurement, vehicle list	Y	2	3	6	
	Antenna damage	CMN-4: Message corruption	Antenna misalignment/ fading	Poor OTI comms performance	Slow to confirm OTI	OTI time extended, train longer	Quality antenna, protected, diverse	Y	1	4	4	
	Antenna damage	CMN-5: Message delay	Fading	Poor OTI comms performance	Slow to confirm OTI	OTI time extended, train longer	Quality antenna, protected, diverse	Y	1	4	4	
	Antenna damage	CMN-6: Intrusion	Deliberate interference	Incorrect messages	Incorrect OTI result	False +ve TI, loss of integrity not detected	Encryption, timestamps	N	**10**	1	10	OTI protocol should be designed to make this practically impossible
	Interference	CMN-1: Repetition of old message	N/A					Y	1	1	1	
	Interference	CMN-2: Loss of message	EMI/thermal noise	Momentary loss of communication	Integrity confirmation time extended	Time between checks extended	Message checksum, acknowledge, repeat	Y	1	4	4	
	Interference	CMN-3: Node insertion (other train node, error of network)	N/A	Incorrect OTI data	OTI not confirmed	Slow to confirm until train in motion	Distance measurement, vehicle list	Y	2	3	6	
	Interference	CMN-4: Message corruption	N/A	Poor OTI comms performance	Slow to confirm OTI	OTI time extended, train longer	Message checksum, acknowledge, repeat	Y	1	4	4	
	Interference	CMN-5: Message delay	EMI/thermal noise	Poor OTI comms performance	Slow to confirm OTI	OTI time extended, train longer	Message checksum, acknowledge, repeat	Y	1	4	4	
	Interference	CMN-6: Intrusion	N/A Environmental	Incorrect messages	Incorrect OTI result	False +ve TI, loss of integrity not detected	Encryption, timestamps	N	**10**	1	10	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Interference	CMN-6: Intrusion - Deliberate	Malicious attack	Cloning, data security compromised,	false +ve or false -ve	Potentially incorrect TI status	Network security measures, intrusion detection?	N	**10**	1	10	OTI protocol should be designed to make this practically impossible
	Software fault	CMN-1: Repetition of old message	Incorrect request from CM/Incorrect data from WSN		Nodes don't respond or data returned invalid/false +ve or false -ve	TI can not be confirmed/Potentially incorrect TI status	Time stamped/checked messages	Y/N	1	1	1	CM/Nodes. Need reliable method to reject out of sequence messages.
	Software fault	CMN-2: Loss of message	Incorrect request from CM/Incorrect data from WSN		false -ve	TI can not be confirmed	Redundancy and comms range usually exceeds node separation		1	4	4	
	Software fault	CMN-3: Node insertion (other train node, error of network)	Incorrect request from CM/Incorrect data from WSN	Incorrect OTI data	OTI not confirmed	Slow to confirm until train in motion	Distance measurement, vehicle list	Y	2	3	6	
	Software fault	CMN-4: Message corruption	Incorrect request from CM/Incorrect data from WSN	Incorrect OTI data	OTI not confirmed	Slow to confirm	Distance measurement, vehicle list	Y	2	3	6	
	Software fault	CMN-5: Message delay	Incorrect request from CM/Incorrect data from WSN	Incorrect OTI data	OTI not confirmed	Slow to confirm	Distance measurement, vehicle list	Y	2	3	6	
	Software fault	CMN-6: Intrusion	Incorrect request from CM/Incorrect data from WSN	Incorrect messages	Incorrect OTI result	False +ve TI, loss of integrity not detected	Encryption, timestamps	N	**10**	1	10	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Impact damage to node	Electronic damage, water ingress	Ballast impact	Loss of sensor, reduced OTI comms performance	Lower communication rate, might not be able to measure distance	Node becomes intermittent, possible loss of topology discovery	Node may report status but not wagon distance Rely on other nodes nearby for redundancy	Y	Y	1	1	1
											0	
Distance Sensor	Antenna	DS-1: DS detects too late the uncoupling of the wagon (safety critical)	Antenna doesn't have enough power/ Incorrect design/ Temperature range has not been taken into account/ Antenna is broken	Incorrect OTI data	OTI not confirmed	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	1	2	2	
	Antenna	DS-2: DS doesn't detect the next coach DS (availability issue)	Antenna doesn't have enough power/ Incorrect design/ Temperature range has not been taken into account/ Antenna is broken	Incorrect OTI data	OTI not confirmed	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	2	2	4	
	Antenna	DS-3: DS doesn't detect the uncoupling of the next wagon (safety critical)	Defective sensor. Incorrect configuration (detects sensor on same vehicle)	Incorrect OTI data	OTI not confirmed. Distance failure	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	**10**	2	20	No distance measurement extends the train
	Radio transmission	DS-1: DS detects too late the uncoupling	Incorrect distance calibration	Incorrect OTI data	OTI not confirmed	Slow to confirm until train in motion	Multiple redundancy, backup from	N	**10**	2	20	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
		of the wagon (safety critical)					communication analysis					
	Radio transmission	DS-2: DS doesn't detect the next coach DS (availability issue)	Faulty antenna. Transmission interruption/bad geometry	Incorrect OTI data	OTI not confirmed	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	1	2	2	
	Radio transmission	DS-3: DS doesn't detect the uncoupling of the next wagon (safety critical)	Incorrect distance calibration	Incorrect OTI data	OTI not confirmed	Slow to confirm until train in motion	Multiple redundancy, backup from communication analysis	N	**10**	2	20	
	Configuration	DS-1: DS detects too late the uncoupling of the wagon (safety critical)	The threshold alert distance is excessive	Incorrect OTI data	OTI not confirmed. Distance failure	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	**10**	2	20	
	Configuration	DS-2: DS doesn't detect the next coach DS (availability issue)	The maximum measurable distance is insufficient to reach the next coach DS	Incorrect OTI data	OTI not confirmed	Slow to confirm until train in motion	Multiple redundancy, backup from communication analysis	N	**10**	2	20	
	Configuration	DS-3: DS doesn't detect the uncoupling of the next wagon (safety critical)	The threshold alert distance is excessive	Incorrect OTI data	OTI not confirmed. Distance failure	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	**10**	2	20	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Software	DS-1: DS detects too late the uncoupling of the wagon (safety critical)	Incorrect SW functioning, Incorrect SW version is installed/ SW has not been validated and proven	Incorrect OTI data	OTI not confirmed. Distance failure	OTI slow response	Compliance of EN50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems	N	**10**	2	20	
	Software	DS-2: DS doesn't detect the next coach DS (availability issue)	Incorrect SW functioning, Incorrect SW version is installed/ SW has not been validated and proven	Incorrect OTI data	OTI not confirmed. Distance failure	Coupling integrity/TI not confirmed by that node pair	Compliance of EN50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems	N	2	2	4	
	Software	DS-3: DS doesn't detect the uncoupling of the next wagon (safety critical)	Incorrect SW functioning,Incorrect SW version is installed/ SW has not been validated and proven	Incorrect OTI data	OTI not confirmed. Distance failure	Coupling integrity/TI not confirmed by that node pair	Compliance of EN50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems	N	**10**	2	20	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Internal SPI bus/UART	DS-1: DS detects too late the uncoupling of the wagon (safety critical)	Internal message delay/ corruption/repetition	Incorrect OTI data	OTI not confirmed. Distance failure	OTI confirmation delayed	Compliance with EN 50159:2010 Railway applications: communication, signalling and processing systems: safety-related communications in closed (part 1) and in open (part 2) transmission systems	Y	3	3	9	
	Internal SPI bus/UART	DS-2: DS doesn't detect the next coach DS (availability issue)	Internal message delay/ corruption	Incorrect OTI data	OTI not confirmed. Distance failure	OTI confirmation delayed	Compliance with EN 50159:2010 Railway applications: communication, signalling and processing systems: safety-related communications in closed (part 1) and in open (part 2) transmission systems	Y	3	3	9	
	Internal SPI bus/UART	DS-3: DS doesn't detect the uncoupling of the next wagon (safety critical)	Internal message corruption/intrusion/repetition	Incorrect OTI data	OTI not confirmed. Distance failure	Coupling integrity/TI not confirmed by that node pair	Compliance with EN 50159:2010 Railway applications: communication, signalling and processing systems: safety-related	N	**10**	1	10	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
							communications in closed (part 1) and in open (part 2) transmission systems					
	Suggested Alternate failure (to VN) modes - potential causes would vary with component - Suggested as (see comment) the function of the DS is not to detect uncoupling of a wagon directly but to make a measurement when TI requested. The confirmation or(not) of coupling integrity based on that measurement.										0	
	DS-1: DS Inaccurate distance measurement - measurement lower than actual distance		Damaged/deformed antenna, interference, loss of calibration	Inaccurate distance measurement - measurement lower than actual distance	Inaccurate distance measurement - measurement lower than actual distance	Possible over sensitivity of changes in measurement leading to false reports of loss of coupling/train integrity.	Redundant, multiple paths for integrity and communication	N	**10**	2	20	
	DS-2: Inaccurate distance measurement - measurement greater than actual distance		Damaged/deformed antenna, interference, loss of calibration	Inaccurate distance measurement - measurement greater than actual distance	Inaccurate distance measurement - measurement greater than actual distance	Delay (separation distance between vehicles) in detecting loss of coupling/train integrity	Loss of coupling/train integrity will still be detected after the vehicles separate by a greater number of metres	N	**10**	2	20	
	DS-3: DS doesn't detect the next vehicle in operational range (availability		Damage DS, loss of connection between components	DS fails to make measurement	Coupling integrity/TI not confirmed by that node pair	Coupling integrity/TI not confirmed by that node pair	Redundant, multiple paths for integrity and communication	Y	2	3	6	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
		DS-4: DS reports detection/distance of vehicle in operational range when there isn't one	E.g. Software error, old value not being overwritten		Potential false +ve coupling integrity confirmation. Potential for loss of TI not to be detected	Potential false +ve TI	Redundant, multiple paths for integrity and communication	N	**10**	1	10	
		DS-5: DS reports detection/distance of vehicle on adjacent track not part of the consist	Vehicles in close proximity during network discovery	Incorrect vehicles(s) associated with network	When train (or vehicle(s)) moves, movement of incorrectly associated wagons will not be consistent and TI will be considered lost	TI lost/not confirmed when train/vehicle(s) move inconsistently	Compare vehicle IDs in network with expected consist. Inconsistent movement will result in TI not confirmed, error discovered on investigation				0	
	External interference	DS-6: DS cloned, clone sending false distance measurement	System adversary attaches DS/Node clone to same vehicle which responds to distance measurements	Invalid distance measurement	False +ve coupling integrity confirmation	False +ve TI, loss of integrity not detected	Physical difficulty of introducing clone to vehicle and system security measures preventing cloning and detection of intrusion/duplicates.				0	
Network Manager/ Control	Radio (868MHz)	No radio reception	No connection to antenna, faulty radio, antenna broken, radio misconfiguration	No OTI system	Revert to axle counting	No on-board result	Redundant control module	Y	5	1	5	
	Software	Software crash	Software poorly tested, EMC, poor configuration.	No OTI system	Revert to axle counting	No on-board result	Redundant control module	Y	5	1	5	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Network list	Incorrect node list/vehicle list	Fail to confirm integrity	No OTI system	Revert to axle counting	No on-board result	Redundant control module	Y	5	2	10	
	Coupling list	Incomplete topology/coupling	Fail to confirm integrity	No OTI system	Revert to axle counting	No on-board result	Redundant control module	Y	5	2	10	
	Coupling status	Incomplete coupling list	Fail to confirm integrity	No OTI system	Revert to axle counting	No on-board result	Redundant control module	Y	5	2	10	
	Node status/network status	Missing network nodes	Faulty nodes	OTI system slow to respond	Train longer	Extended on-board result	Redundant nodes	Y	5	1	5	
	Local link	No local output	Cable broken, faulty connector	No local advice to driver	Revert to axle counting	No on-board result	Redundant control module	Y	5	1	5	
	Hardware (electronics/housing)	PSU faulty	Electronic/electrical component failure	No OTI system	Revert to axle counting	No on-board result	Redundant control module	Y	5	1	5	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Power supply	Fuse, relay, wiring, or connection fault	Mechanical fatigue/damage, over current/voltage	No power to CM	Signal/command to release nodes from network can not be sent.	TI can not be confirmed, network discovery can not be initiated	To mitigate inability of failed CM to send signal/command to release nodes from network, as secure procedure could be implemented for another CM to send the command.	Y	5	1	5	In normal operation following network discovery nodes are bound to a network centred on the CM and do not respond to other CMs or network discovery request. A secure procedure (perhaps with special authorisation codes (or obtaining the codes the failed CM was using from the cloud)) would be advisable to enable nodes to be unbound from the network so a new network can be formed with a working CM. This would be failsafe a mistakenly removing a node from an active network would cause it not to confirm TI to that network.

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Software	Complete failure, or failure to confirm TI	Corruption of software, error state, invalid security keys, cyber attack, Failed software installation/update, memory or other hardware fault, failed security key update.	System cannot confirm TI regardless of integrity state	CM not responding or displaying error state	TI cannot be confirmed, network discovery cannot be initiated, AND signal/command to release nodes from network cannot be sent.	Redundant systems/voting	Y	5	1	5	There are multiple failure modes which are failsafe (hard crash, error state, invalid security keys) which would prevent TI confirmation. There are significantly fewer which would cause a false positive TI confirmation and not be failsafe.
	Software	Partial failure false positive TI confirmation	Corruption of software, error state, cyber attack, software defect. Failed software installation/update, memory or other hardware fault.	System capable of indicating TI confirmed, but potentially indicating TI confirmed when not the case (false positive)	CM appears functional, possible false positives	TI can be confirmed, possible false positives.	Redundant systems/voting	N	**10**	2	20	There are multiple failure modes which are failsafe (hard crash, error state, invalid security keys) which would prevent TI confirmation. There are significantly fewer which would cause a false positive TI confirmation and not be failsafe.

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Antenna	Full/partial loss of signal Tx/Rx	Damage, deformation, wiring fault, water ingress	No/partial communications sent/received	Insufficient communication between CM and nodes, Signal/command to release nodes from network can not be sent.	TI can not be confirmed	Redundant control module	Y	5	1	5	In normal operation following network discovery nodes are bound to a network centred on the CM and do not respond to other CMs or network discovery request. A secure procedure (perhaps with special authorisation codes (or obtaining the codes the failed CM was using from the cloud)) would be advisable to enable nodes to be unbound from the network so a new network can be formed with a working CM. This would be failsafe a mistakenly removing a node from an active network would cause it not to confirm TI to that network.

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Touch screen/HMI	Display fault, or loss of touch sensitivity	Mechanical fatigue/damage, electrical fault, Too much force used by operator, too many touch cycles, wiring/connection fault	Touch screen/HMI interface failure	Status can not be displayed visually, result of network discovery can not be displayed, manual input for network discovery can not be entered	TI status can not be displayed and network discovery can not be displayed or confirmed locally	TI system could be arranged so that ETCS could initiate network discovery, confirm result with driver.	Y	5	1	5	If display is integrated into loco systems then the fault is likely to affect other systems preventing the operation of the train/loco. If the TI System display is separate then provided TI confirmation is being sent to ETCS movement authorities provided to the driver will confirm TI is being confirmed, ETCS can notify driver if loss of TI detected. THis would be degraded state working
Configuration database	WSN allocation database	Incorrect asset location (single error)	Operator error	Fail to measure distance to next wagon - rely on other nodes.	Rely on measurements from other wagons. Mark node as faulty	OK, but not robust to further loss of nodes	Automated configuration at fitment	Y	2	4	8	
	WSN allocation database	Incorrect asset location (multiple errors)	Operator error	Fail to establish topology/ measure distance to next wagon	Not possible to establish topology or separation distance	Fail to establish integrity	Automated configuration at fitment		4	4	16	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Expected number of wagons incorrect	Number of vehicles expected in train by database does not match physical number in train	Incorrect input, corruption of software	Inconsistency between number of vehicles found in network discovery and on database	Topology discovery check failed	Train integrity not confirmed	TI check fails, check of actual number of vehicles, vehicles with failed nodes, and database values to find error	Y	4	5	20	
	Software/ configuration fault	Incorrect node/vehicle associations	Incorrect input, corruption of software, Original or replacement node not configured correctly, partial/unsuccessful update of parameters/associations	Node does not try to contact/acknowledge other nodes on same vehicle during network discovery	Topology discovery unsuccessful	Unable to build correct topology	Redundant, multiple paths for integrity and communication	Y	4	5	20	
Train Driver	Check OTI status	False yes interpretation	Human error/DMI error, Driver erroneously interprets the information from DMI/ DMI reproduces erroneous information due to interface fault		Driver interpretation is he is ready to enter signalled network. ERTMS will not authorise move (it has not received TI confirmation)	TI state not confirmed, no ERTMS movement authority given	ERTMS applies brakes on managed rail network. Driver investigates cause of no ERTMS movement authority.	Y	4	5	20	Reliance on ERTMS also receiving the correct OTI result

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Check discovery result	False yes interpretation	Human error/DMI error, Driver erroneously interprets the information from DMI/ DMI reproduces erroneous information due to interface fault		Driver interpretation is he is ready to enter signalled network. ERTMS will not authorise move (it has not received TI confirmation)	TI state not confirmed, no ERTMS movement authority given	ERTMS applies brakes on managed rail network. Driver investigates cause of no ERTMS movement authority.	Y	4	5	20	
	Check OTI status	False no interpretation	Human error/DMI error, Driver erroneously interprets the information from DMI/ DMI reproduces erroneous information due to interface fault		Driver interpretation is he is not ready to enter signalled network. Driver does not request ERTMS movement authority and investigates, or if driver doesn't act on ERTMS movement authority contact made to investigate cause	TI state confirmed, ERTMS movement authority can be requested/given	ERTMS movement authority can be given, driver might stop and/or question validity of ERTMS MA and investigate issue.	Y	4	5	20	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Check discovery result	False no interpretation	Human error/DMI error, Driver erroneously interprets the information from DMI/ DMI reproduces erroneous information due to interface fault		Driver interpretation is he is not ready to enter signalled network. Driver does not request ERTMS movement authority and investigates, or if driver doesn't act on ERTMS movement authority contact made to investigate cause	TI state confirmed, ERTMS movement authority can be requested/given	ERTMS movement authority can be given, driver might stop and/or question validity of ERTMS MA and investigate issue.	Y	4	5	20	
	Command Driver request to check TI	TD request is executed while TI is in Discovery	Driver is unaware of TI state				TI state is not confirmed, error message displayed "network discovery in progress"	Y	4	5	20	
	Command Driver request to check TI	TD request is executed while TI is in Check	Driver is unaware of TI state				TI state is not confirmed and Nodes and CM reset when TI complete/fails. OR: TD request refused and error message displayed, must reset network (release all nodes and CM from network) before starting TD	Y	4	5	20	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Command Driver reset TI device	Reset is executed while TI is in Discovery	Driver is unaware of TI state/Human error				Error/status message displayed, ask for confirmation of rest. If rest confirmed, TD halt command sent and rest all nodes and CM and restart TD	Y	4	5	20	
	Command Driver reset TI device	Reset is executed while TI is in Check	Driver is unaware of TI state/Human error				TI state is not confirmed, nodes and CM reset when TI complete/fails	Y	4	5	20	
WSN energy storage, power supply, electronics	High leakage	Low message rate/fail to power distance measurement sensor	Electronic component defect	Low message rate, no distance measurement.	OTI poor reliability	May fail to complete OTI - rely on other sensors	Redundancy from multiple nodes	Y	1	1	1	
	Low capacity	Only works when train running at high speed	Electronic component defect	Low message rate, no distance measurement.	No topology discovery	May fail to complete OTI - rely on other sensors	Redundancy from multiple nodes	Y	1	1	1	
	No storage	No functionality	Electronic component defect	No running when stationary	No topology discovery/ lose network when train stationary	May fail to complete OTI - rely on other sensors	Redundancy from multiple nodes	Y	1	1	1	
	Voltage regulator to energy storage	Energy storage not working	Electronic component defect	WSN stops responding	OTI poor reliability	May fail to complete OTI - rely on other sensors	Redundancy from multiple nodes	Y	1	2	2	
	Voltage regulator to electronics	No power to circuits	Electronic component defect	WSN stops responding	OTI poor reliability	May fail to complete OTI - rely on other sensors	Redundancy from multiple nodes	Y	1	2	2	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	UHB distance measurement										0	
Mounting Arrangement	Retaining Bolts	Retaining bolts loose	Impact, improper installation/maintenance of device/axlebox cover	Reduction/increase in vibration transmission, degraded antenna alignment	Reduced/increased energy harvesting, reduction in communication/distance measurement capability	Node may report status but not wagon distance	TI: Redundant, multiple paths for integrity and communication. General: Design/approvals and Inspection	Y	**10**	1	10	Mechanical hazard to passengers, derailment possible.
	Retaining Bolts	Retaining bolts failed/missing	Impact, improper installation/maintenance of device/axlebox cover	Device detached from vehicle	Device no longer physically attached to train, destroyed or goes out of range, no further power generated	Node stops reporting status, OTI relies on other nodes/redundancy	TI: Redundant, multiple paths for integrity and communication. General: Design/approvals and Inspection. From TI point of view; N regarding hazard to personnel/assets.	Y,	**10**	1	10	
	Attaching bracket	Bracket cracked, fatigued or damaged	Impact, fatigue	Reduction/increase in vibration transmission, degraded antenna alignment	Reduced/increased energy harvesting, reduction in communication/distance measurement capability	Node may report status but not wagon distance	TI: Redundant, multiple paths for integrity and communication. General: Design/approvals and Inspection	Y	**10**	1	10	

Subsystem	Component		Potential Cause	Failure Mode	Failure Effect	Train Integrity outcome	Mitigation	Failsafe (Y/N)	S	O	R	Notes
	Name & Function	Failure mode										
	Attaching bracket	Bracket failed/fractured	Impact, fatigue	Device detached from vehicle	Device no longer physically attached to train, destroyed or goes out of range, no further power generated	Node stops reporting status, OTI relies on other nodes/redundancy	TI: Redundant, multiple paths for integrity and communication. General: Design/approvals and Inspection from TI point of view; N regarding hazard to personnel/assets	Y	**10**	1	10	

4. DISCUSSION

The key difference between the vehicle distance sensing system developed in ETALON, which has been subjected to examination under an FMECA, and the possible alternate systems either proposed by complementary project X2Rail-2 or in this document, is the presence of an end of train device. Definitive inclusion of an OTI slave, specifically mounted at the end of the train occurred too late to modify the approach taken here. The power consumption requirements placed on the energy harvester with or without an additional distance measurement sensor are still within the power available from a VEH (see D3.2 and D4.2).

Analysis of the FMECA for the OTI developed by ETALON shows that some additional mitigation is required to eliminate all non-failsafe failure modes. This mitigation could be in the form of additional analysis of communication from each of the vehicles, or addition of an OTI slave at the end of the train. A major hazard to the method is the requirement to achieve an accurate configuration of vehicles and nodes in the consist. This process is currently error-prone in normal train operations, where although the total number of axles in a train leaving the yard might be known, the actual identities of all the vehicles might be wrong. The vehicles in the consist could be reliably identified by combining an online database of WSNs on vehicle wheels, with the distance measurement identifying neighbouring vehicles. This method could deliver a reliable list of vehicles for comparison with the intended train content. It is possible that incorrect allocation of WSNs to wheels could break this approach. Inclusion of an OTI slave (irrespective of power source) could deliver OTI that is agnostic to the WSNs used to communicate information down the train.

Slave OTI devices are not proposed by complementary project X2Rail-2 for fitment to all vehicles – only to the EoT is employed. Although these devices may be energy harvester powered, the act of having to fit them manually to each train before departure removes the common driver for energy harvester technology that is zero maintenance. If they are going to be manually moved around, it may be that a more reliable approach is to use rechargeable battery technology to guarantee continuous operation over a minimum length of time, irrespective of the availability of significant ambient energy (either in the form of vibration or sunlight). Battery usage can be reduced by relying on a large number of VEH powered radio devices to carry information to the OTI master, in comparison to the North American EoT devices, which have the high-power VHF radio as the major power drain on their battery supplies.

5. CONCLUSIONS

An assessment of OTI methods is presented, with a FMECA for the system proposed in ETALON, which introduces the novel approach of using UWB distance measurement between vehicles to establish the presence of a continuous train of known vehicles. Extension of this analysis to all other OTI methods is outside the scope of ETALON. The study does show that the method developed is an appropriate model for demonstrating the capability of VEH technology for powering long train communication, passing information down the complete train at a rate compatible with OTI implementation.

The deployment of VEH devices is compatible with a requirement to monitor vehicle condition using the same equipment.

6. REFERENCES

[1] http://www.gobotix.co.uk/guard/

[2] https://w3.usa.siemens.com/mobility/us/en/Events/railway-interchange/Documents/SIE_BRO_End%20of%20Train%20Brochure.pdf