Collaborative Large-scale Integrating Project

OPENCOSS

Open Platform for EvolutioNary Certification Of Safety-critical Systems

Industrial Use cases: Description and business impact D1.2.c Railway Use Case

Work Package:	WP1: Use Case Specification and Benchmark
Dissemination level:	PU
Status:	Final
Date:	03 October 2012
Responsible partner:	Fabien Belmonte (Alstom Transport)
Contact information:	fabien.belmonte@transport.alstom.com

PROPRIETARY RIGHTS STATEMENT
This document contains information, which is proprietary to the OPENCOSS Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the OPENCOSS consortium.

Contributors

Names	Organisation
Laurent de la Beaujardière, Fabien Belmonte, Andrea Palermo	ALSTOM Transport

Document History

Version	Date	Remarks
V0.1	2012-03-14	Template: Contents of the use cases
V0.2	2012-04-15	First draft version including wide coverage, with some incomplete aspects.
V0.3	2012-04-26	First full version
V0.4	2012-06-08	Ready for WP review
V0.9	2012-06-22	Ready for PB review
V1.0	2012-06-28	Approved by PB

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

This document describes the OPENCOSS Railway Industrial Use-Case. This Use-Case will be used as reference proof-of-concept of the certification framework and services offered by the OPENCOSS platform.

The OPENCOSS railway use case presents the certification of an existing and already certified Railway signaling system. This industrial use case describes the certification of a European standardized signalling system provided by Alstom Transport. The Railway use-case chosen is a part of the European Railway Traffic Management System (ERTMS). The ERTMS is intended to replace almost all national legacy mainline signalling and train control systems all across Europe. This Use Case is related to the On-Board Unit Sub-System (OBU) of the ALSTOM solution for the European Train Control System (ETCS) of the European Railway Traffic Management System (ERTMS), known as European Vital Computer (EVC) in the architecture of ERTMS.

The On-Board Unit Sub-System is ALSTOM's solution for ETCS onboard equipment that will be used by ALSTOM ERTMS Application Projects. The main functions of this sub-system are to ensure safe movement of the train and to inform the driver by means of a Cab Display facility. This sub-system contains also railway generic products. This development addresses the both the compositional certification and the reuse of safety argumentation. The industrial use case aims to identify what the OPENCOSS framework should provide to improve certification process efficiency by taking into account the existing approach of generic certification. Since, the specific project applications may be in different countries that have different National Safety Authority requirements, OPENCOSS shall provide support for "cross-country" certification.

The introduction provides the underlying Railway knowledge that help to capture the industrial context of this Use-Case. The European Railway Traffic Management System is described together with basic railway signalling principles. Then the sub-system being studied is described, as are the activities leading to its certification. Finally, relationships with the OPENCOSS technical Work Packages are discussed in order to identify more precisely the reference proof-of-concepts that this particular Industrial Use-Case aims to address in OPENCOSS.

Reference documents

ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS. *FIS for Man-Machine Interface.* ERTMS/ETCS Specifications.
ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS. *FIS for the Train Interface.* ERTMS/ETCS Specifications.
ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS. *System Requirement Specification.* ERTMS/ETCS Specifications.
Artisan. (2012). Consulté le June 20, 2012, sur Artisan Studio - Products - Atego: http://www.atego.com/products/artisan-studio/
CENELEC. (1999). *EN 50126 - Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS).*
CENELEC. (2011). *EN 50128 - Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems.*
CENELEC. (2003). *EN 50129 - Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling.*
EC. *Commission Decision 2012/88/EU on the 25th January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system.*
EC. (1996). Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system. *Official Journal L235* , pp. 6-24.
EC. (2001, april). Directive 2001/16/EC of the European Parliament and of the Council of 19 March 2001 on the interoperability of the trans-European conventional rail system . *Official Journal L110* , pp. 1-27.
EC. (2008). Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community. *Official Journal L191 vol 51* .
OMG. (2012). Consulté le June 8, 2012, sur Website of the Object Management Group - Systems Modeling Language version 1.3: http://www.omgsysml.org/
Ward, P., & Mellor, S. (1985). *Structured Development for Real-Time Systems.* New Jersey: Prence Hall.

Glossary

Abbrev./terms		Definition
ATC	AUTOMATIC TRAIN CONTROL	
ATP	AUTOMATIC TRAIN PROTECTION	A safety system that enforces either compliance with or observation of speed restrictions and signal aspects by trains.
	BALISE	A passive transponder mounted on the track which can communicate with a train passing over it.
	BLOCK	A method of controlling the separation between trains by dividing the line into sections with, normally, no more than one train in each section. The block can either be a fixed block or a moving block.
	BRAKING CURVE	A graphical representation of the braking distance of a train in relation to the gradient of track, and the braking characteristics of the train. The graph normally shows train speed varying against either distance or time.
BTM	BALISE TRANSMISSION MODULE	On board equipment for spot transmission between track and train. It shall be able to receive telegrams from a balise.

Abbrev./terms		Definition
	CONFLICTING MOVEMENTS	Movements that would require trains to occupy the same portion of track over all or part of their length.
	CONTINUOUS DATA TRANSMISSION	Track-to-train or train-to-track transmission that can take place continuously via radio.
	CONTROL CENTRE	A signal box covering a large area, usually incorporating other operational functions.
	CROSS-ACCEPTANCE	The status achieved by a product that has been accepted by one Authority of the relevant European Standards and is acceptable to other Authorities without the necessity for further assessment.
DMI	DRIVER MACHINE INTERFACE	
ERTMS	EUROPEAN RAILWAY TRAFFIC MANAGEMENT SYSTEM	
ETCS	EUROPEAN TRAIN CONTROL SYSTEM	
	EUROBALISE	The group of technical solutions for balises for use in an ERTMS / ETCS installation.
	EUROLOOP	The group of technical solutions for loops for use in an ERTMS / ETCS installation. (see INFILL LOOP)
	EURORADIO	The functions required of a radio network coupled with the message protocols that provide an acceptably safe communications channel between track side and train borne equipment.
FFFIS	FORM FIT FUNCTIONAL INTERFACE SPECIFICATION	_
FIS	FUNCTIONAL INTERFACES SPECIFICATION	_
FRS	FUNCTIONAL REQUIREMENTS SPECIFICATION	_
	INFILL INFORMATION	Data that is transmitted from track to train at locations other than at main signals. Provides, for example, the ability to inform a train that the signal ahead has cleared.
	INFILL LOOP	A loop which is installed at a place (e.g. in rear of a signal) where it is not essential for train safety, but avoids unnecessary delay by transmitting in fill information advising the train at once when the signal clears.
IXL	INTERLOCKING	A general term applied to the controlling of the setting and releasing of “signals” and “points” to prevent unsafe conditions arising, and equipment which performs this function.
JRU	JURIDICAL RECORDER UNIT	Device to record all actions and exchanges relating to the movement of trains sufficient for off-line analysis of all events leading to an incident.
	KERNEL	The core of the ERTMS / ETCS train borne equipment that predicts the safe speed/distance envelope for a train and initiates braking action to prevent the safe envelope being breached.
LTM	LOOP TRANSMISSION MODULE	Train borne equipment that reads the track mounted loop data.
LRBG	LAST RELEVANT BALISE GROUP	
MMI	MAN MANCHINE INTERFACE	
	MOVING BLOCK	A block whose length is defined by the characteristics of the train occupying the section of track. The minimum block length would be from the rear most part of the occupying train to a point on the track where, if the train braked from its current speed, the front of the

Abbrev./terms		Definition
		occupying train would be when the train came to a stand.
OBU	On-Board Unit	The sub-system under study.
	ODOMETRY	The process of measuring the train's movement along the track. Used for speed measurement and distance measurement.
RBC	RADIO BLOCK CENTRE	A centralised safety unit working with an interlocking(s) to establish and control train separation. Receives location information via radio from trains and sends movement authorities via radio to trains.
STM	SPECIFIC TRANSMISSION MODULE	The train borne equipment of the ERTMS / ETCS must be able to be interfaced with the train borne equipment of an existing train supervision system. The Specific Transmission Module shall perform a translation function between these systems and the ERTMS / ETCS.
SyRS	SYSTEM REQUIREMENTS SPECIFICATION	
SyAD	SYSTEM ARCHITECTURE DESCRIPTION	
TIU	TRAIN INTERFACE UNIT	The unit that provides the interface between the train borne equipment and the train. It is likely to be unique to a class of train.

1 Introduction

The OPENCOSS railway use case presents the certification of a Railway signaling system. This document describes the certification of a European standardized signalling system provided by Alstom Transport.

Figure 1: Next generation & cross domain ETCS? (Credit photo www.uic.org)

The Railway use-case chosen is a part of the European Railway Traffic Management System (ERTMS). Europe's railways have developed over the last 150 years within national boundaries, resulting in a variety of different signalling and train control systems, which hampers cross-border traffic. The European Union has decided to improve interoperability for the railway sector. Therefore the ERTMS is intended to replace almost all national legacy mainline signalling and train control systems all across Europe. Eight UNIFE[1] members are developing the ERTMS industrial project including Alstom Transport. The ERTMS contains three main components; the communication system based on Global System for Mobiles – Railway (GSM-R), the Automatic Train Control system (ATC) named European Train Control System (ETCS) and the European Traffic Management Layer (ETML):

- **GSM-R** (Global System for Mobiles - Railway) – the communication element containing both a voice communication network between driving vehicles and line controllers and a bearer path for ETCS data. It is based on the public standard GSM with specific rail features for operation e.g. Priority and Pre-emption (eMLPP) - Functional Addressing Location Dependent Addressing - Voice Broadcast Service (VBS) - Voice Group Call (VGC) - Shunting Mode - Emergency Calls - General Packet Radio Service (GPRS option) - Fast call set-up .
- **ETCS** (European Train Control System) – the signalling element of the system which includes the control of movement authorities, automatic train protection and the interface to interlockings. It allows the stepwise reduction of complexity for train drivers (automation of control activities) - It brings track side signalling into the driver cabin - It provides information to the on-board display - It allows for permanent train control - Train driver concentrates on core tasks.
- **ETML** (European Traffic Management Layer) – the operation management level intended to optimise train movements by the "intelligent" interpretation of timetables and train running data. It involves the improvement of: real-time train management and route planning - rail node fluidity - customer and operating staff information.

The ETCS shall replace existing national train control system. The OPENCOSS railway use case is related to parts of the ETCS subsystem. Before developing into more detail the architecture of ETCS, legal requirements governing the ERTMS solution will be briefly discussed, then the ETCS operation levels will be described. Finally, the boundaries of the OPENCOSS railway use case will be defined after having presented the ETCS structural aspects.

1.1 Legal requirements

ERTMS systems are governed by the European commission decision of 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-

[1] The Association of the European Rail Industry, see: http://www.unife.org/

European rail system (EC). It defines mandatory requirement for interoperability. This decision imposes the assessment of the developed ERTMS system (train borne ETCS in particular) with regards to the mandatory standards that are the CENELEC (CENELEC, 1999; CENELEC, 2011; CENELEC, 2003). Furthermore, the manufacturer shall draw up a declaration of conformity with the Technical Specification for Interoperability (EC). Evidences that shall be brought are described in Table 6.1 chapter 6 (EC).

1.2 Operational modes

1.2.1 Basic railway signaling principle

Railway signaling systems are intended to prevent the trains from colliding and from derailing. Since the accuracy of human vision is lower than the braking distance of the trains, the driver shall be notified of any danger on tracks early before entering braking distance zone. This is the role of a signaling system. The basic principle is to define portions of track where only one train is allowed to run. This portion of safe track is called a block. The size of the blocks is calculated with regard to the maximal braking distance of the most restrictive train allowed to run on the line. Sensor installed on the block named track circuit detects the occupancy of the block. This information is used to define the aspect of a line side signal placed before the entrance of the block. This signal aspect is interpreted by the train driver who observes driving operation to stop his train before entering the occupied block. Signals might be traffic lights placed on the side of the tracks or coded information transmitted directly to the train's driver cabin (cab signal). The separation of trains is insured by having always a block not occupied between two trains or to impose speed limitation to a follower train entering the preceding block of an occupied block so that the follower train is able to stop before entering the occupied block. This principle is known as "fixed block" see Figure 2. By improving the accuracy of train localizations it is possible to provide a continuously updated speed limitation to train, this principle is called "moving block".

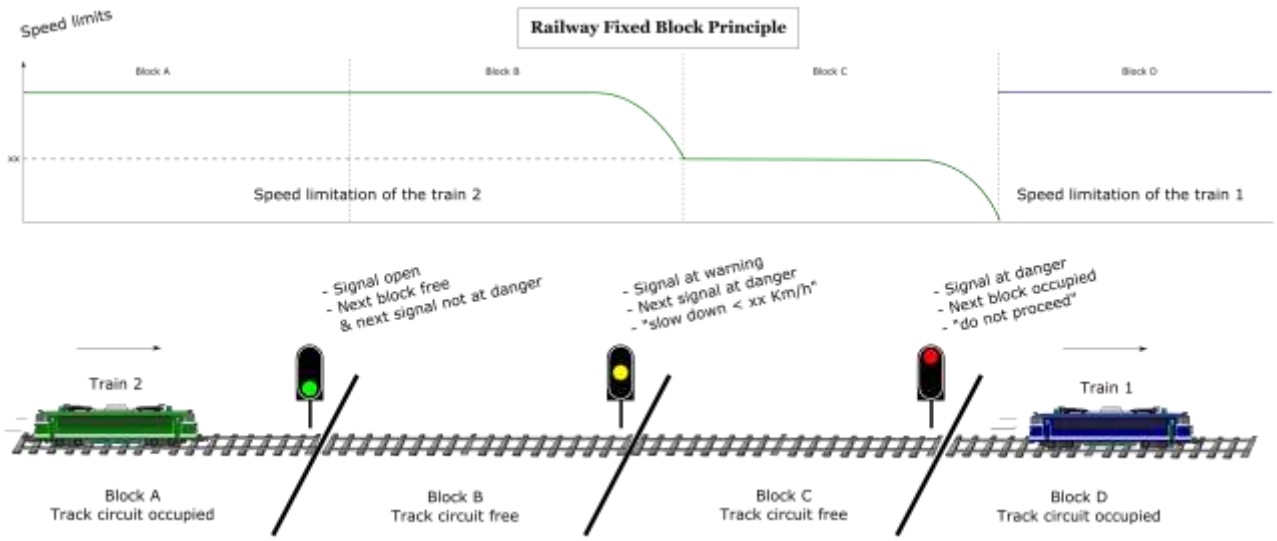

Figure 2: Basic railway principle "Fixed Block"

1.3 Architecture of ETCS

Due to the nature of the required functions, the ERTMS/ETCS system will have to be partly on the trackside and partly on board the trains. The trainborne equipment has been selected by Alstom to be the railway OPENCOSS use case. This section describes briefly the entire ETCS architecture (ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS). The Trainborne equipment will be described further in the next section.

1.3.1 Environment

The environment of ERTMS/ETCS system is composed of:

a) the train, which is considered in the train interface specification (ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS);

b) the driver, who is considered via the driver interface specification;

c) other on-board interfaces, see architecture drawing in Figure 3.

d) external trackside systems (interlocking systems, control centres, etc.), for which no interoperability requirements are established.

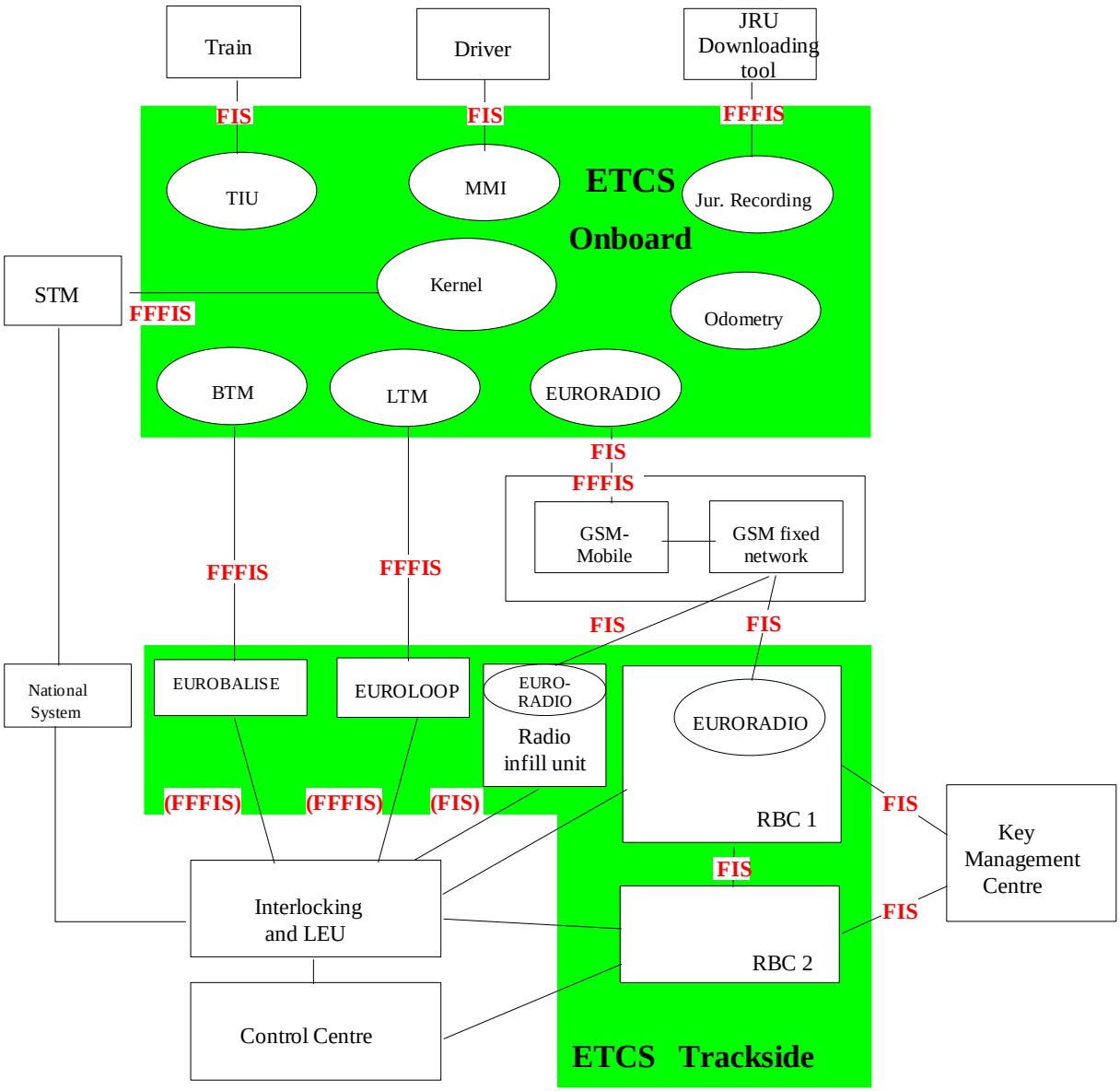

Figure 3: ERTMS/ETCS Architecture – see ref. (ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS)

1.3.2 ERTMS level of operation

The ERTMS/ETCS application "levels" define different uses of ERTMS as a train control system, ranging from limited supervision (Level 0 and Level STM) and fixed block with track to train communications (Level 1) to continuous communications between the train and the radio block center (Level 2). Level 3, which is in a conceptual phase, will further increase ERTMS' potential by introducing a "moving block" technology. Whilst it is commonly acknowledged that to date, ERTMS level 2 offers considerable benefits, the use of level 1 already brings significant advantages for the railways and allows for High Speed travel.

Level 0 applies for train equipped with ETCS operating on a line without ETCS or national system or with the ETCS systems in commissioning. ETCS on-board equipment provides no supervision except for the maximum design speed of a train and maximum speed permitted in unfitted areas. No ETCS trackside equipment is used except for Eurobalises to announce level transitions and other specific commands, the on-board equipment is able to read Eurobalises to detect level transitions and certain special commands, all other messages are rejected.

Level STM uses the track-train transmission system from an underlying national system, which is not part of ERTMS/ETCS. For level transition purposes, Eurobalises are used. This level is used to run ETCS equipped trains on lines equipped with national train control and speed supervision systems. The device which allows the ETCS on-board equipment to utilise the transmission system of the national system is called STM.

Level 1 is designed as an add-on or overlays to a conventional line already equipped with line side signals and train detectors. Communication between the tracks and the train are ensured by dedicated balises/beacon (known as "Eurobalises®") located on the trackside adjacent to the line side signals at required intervals, and connected to the train control center. Receiving the movement authority through Eurobalises, the ETCS onboard equipment automatically calculates the maximum speed of the train and the next braking point if needed, taking into account the train braking characteristics and the track description data. This information is displayed to the driver through a dedicated screen in the cabin. The speed of the train is continuously supervised by the ETCS onboard equipment. The main benefits brought by ERTMS Level 1 are interoperability (between projects and countries) and safety, since the train will automatically brake if exceeding the maximum speed allowed under the movement authority.

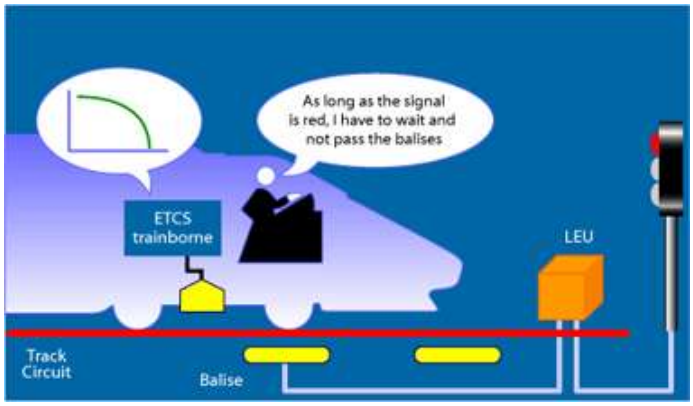

Figure 4: ERTMS level 1 (credit www.ertms.net)

As opposed to level 1, **level 2** does not require line side signals. The movement authority is communicated directly from a Radio Block Centre (RBC) to the onboard unit using GSM-R. The balises are only used to transmit "fix messages" such as location, gradient, speed limit, etc. A continuous stream of data informs the driver of line-specific data and signals status on the route ahead, allowing the train to reach its maximum or optimal speed but still maintaining a safe braking distance factor. Whilst enabling greatly reduced maintenance costs through the removal of line side signals, ERTMS Level 2 also presents the possibility for substantial line capacity increase by enabling higher operational speeds and offering reduced headways: more capacity means more trains moving, thus more benefits.

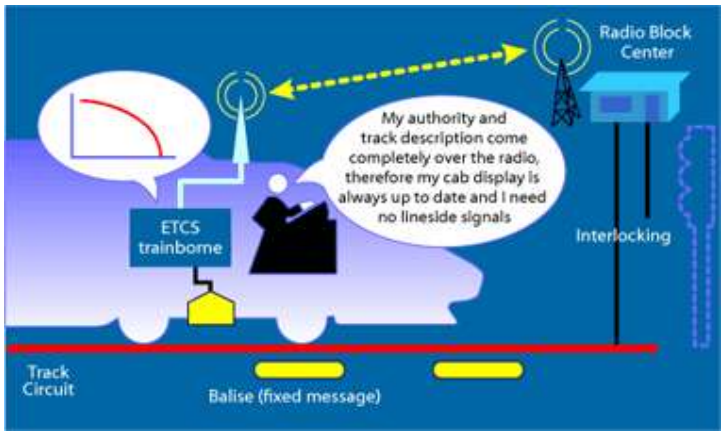

Figure 5: ERTMS Level 2 (credit www.ertms.net)

Level 3, still in its conceptual phase, allows for the introduction of a "moving block" technology. Under ERTMS level 1 and 2, movement authorities are determined using "fixed blocks" - section of tracks between two fixed points which cannot be used by two trains at the same time. With ERTMS level 3, accurate and continuous position data is supplied to the control center directly by the train, rather than by track based detection equipment. As the train continuously monitors its own position, there is no need for "fixed blocks" – rather the train itself will be considered as a moving block.

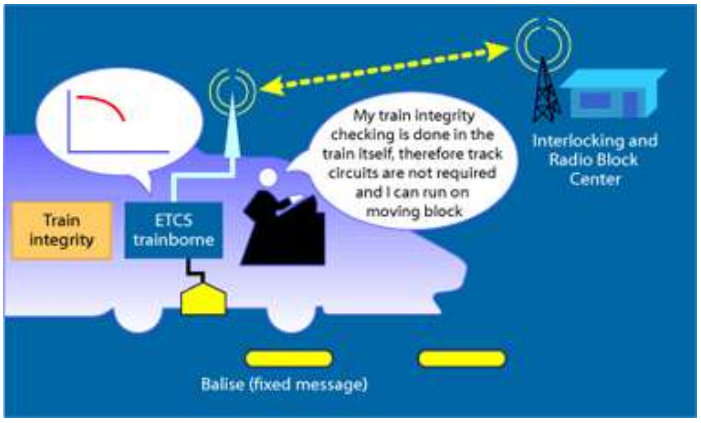

Figure 6: ERTMS Level 3 (credit www.ertms.net)

Interested readers will find didactic videos of the three levels at the following web page:
http://www.ertms.net/ertms/ertms-signalling-levels.aspx

2 System description

This Use Case is related to the On-Board Unit Sub-System (OBU) of the ALSTOM solution for the European Train Control System (ETCS) of the European Railway Traffic Management System (ERTMS).

The On-Board Unit Sub-System is ALSTOM's solution for ETCS onboard equipment that will be used by ALSTOM ERTMS Application Projects. The main functions of this sub-system are:

(a) to ensure a safe movement of the train (*i.e.* the train speed level and braking curve supervisions), applying the "service brakes" or the "emergency brakes" if required, and;

(b) to inform the driver by means of a Cab Display facility, called in the scope of the OBU Project "Driver's Machine Interface" (DMI).

2.1 Industrial Use Case actors and environment

The On-Board Unit subsystem interacts with the following actors, which constitute its environment (

Figure 7):

- The Driver: The driver operates the train command, enters and validates data through the data entry, receives supervision information from the DMI;
- Staff: Configuration, maintenance and investigation:
    - The Maintenance Staff mission is to download all the technical information that has been stored within the Diagnostic Recorder. Downloaded data is necessary for maintenance and diagnostic,
    - The Investigation Staff mission is to download all the technical information that has been stored within the Juridical Recorder. Downloaded data is available to legal authorities for determination of causes of incidents or accidents,
    - The Configuration Staff mission is to modify the system internal parameters in order to configure the system for different tasks. For instance default values, train data, train fitting configuration can be downloaded or uploaded from the On-Board Unit system;
- The Train: The train receives commands from the On-Board Unit (for service brake application, emergency brake application, pantograph control, traction cut-off, etc.) and the train sends state information to the On-Board Unit (state of the brakes, state of the pantograph, train integrity information, etc.);
    - "The train motion", relative to the track, allows the speed and motion sensors of the train to generate odometric signals (wheels sensors, doppler radar, etc.). Those signals will be used by the On-Board Unit to elaborate odometric information such as speed, location, direction and motion.
- The OBU Trackside: the On-Board Unit receives signalling information from the trackside (via GSM-R and Eurobalise). The ERTMS Trackside (*i.e.* eurobalises, euroloops, and RBC radio) sends mainly track profile, technical data, and emergency data. It receives mainly maintenance data, localisation data, or supervision data;
- The STM: The STM is a specific equipment that receives proprietary (non-ERTMS) information from the track and converts it to ERTMS command. It allows ERTMS-equipped train to run on tracks equipped only with national ATP devices;
- UTC Ref: The UTC provider is the external system which provides UTC to the On-Board Unit equipment;
- OBU Scope: Offline tool such as data readers, maintenance and diagnostic tools and configuration and programming tools (may be considered as internal to On-Board Unit).

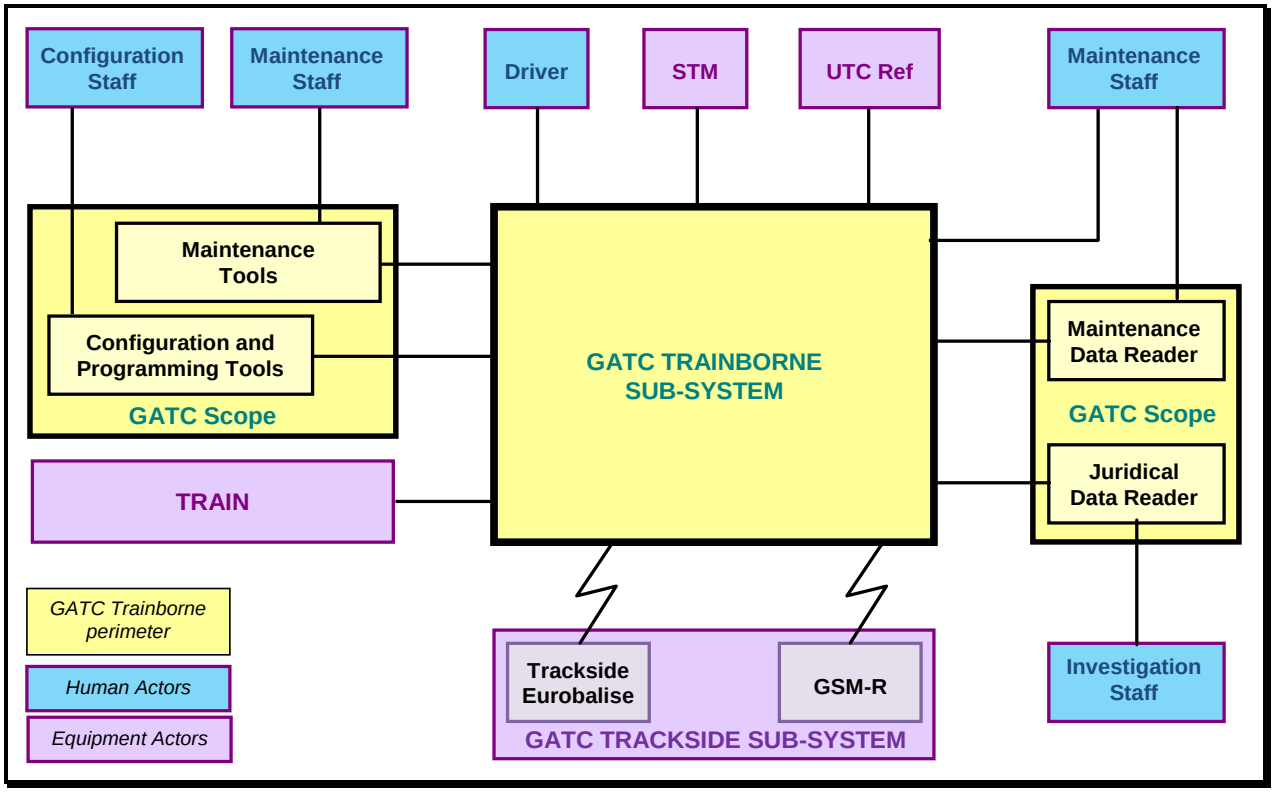

Figure 7: Block diagram of the On-Board Unit environment

To ensure its functions, the On-Board Unit Sub-System uses:

(a) the signaling information received from the trackside via the Trackside Eurobalise Sub-System;
(b) the signaling information received from the trackside via the GSM-R sub-systems (ERTMS Level 2);
(c) the tachometry and odometry data (including the train speed and the train location information) computed internally by the Trainborne Odometer Sub-System on the basis of signals received from sensors and relative to trackside reference points provided on crossing trackside balises;
(d) the information entered by the driver via the DMI Sub-System (e.g. train data, manual movement authority, train composition);
(e) the inputs received from the train (Train Interface);
(f) data about the EVC-Kernel (i.e. Configuration Data such as train braking performances), stored within the EVC internal memories, or the data received from train devices (Train Data).

2.2 Industrial Use case operational scenarios

This use-case is not intended to cover all the operational scenarios of the On-Board Unit subsystem. The following sample scenarios are relevant to the On-Board Unit main activities (note that the operational scenarios depend on the ERTMS level operation of the project *i.e.* the specific application):

- Scenario 1: On-Board Unit performs auto tests before any train movement;
- Scenario 2: On-Board Unit controls safely the movements of the train;
- Scenario 3: On-Board Unit allows maintenance staff to acquire information on equipment's status;
- Scenario 4: On-Board Unit allows configuration staff to insert/update parameters of the onboard equipment;
- Scenario 5: On-Board Unit allows investigation staff to acquire juridical information of the onboard equipment activity in case of accident;
- Scenario 6: On-Board Unit manages the mode and the ERTMS level of operation, it allows the driver to select the proper mode and level and be informed on their status;

- Scenario 7: On-Board Unit acquires and decodes the information provided by the balises;
- …

2.3 Main functions provided by the system

The D1.2 deliverable describes in this section the functions performed by the On-Board Unit system. These functions are the result of Alstom's System Engineering approach. Note: this list of functions is not exhaustive compared to the real functional breakdown structure of Alstom's On-Board Unit system.

2.4 Architecture of the system

The On-Board Unit Sub-System is composed internally of sub-systems/components or single elements (see Figure 8). It includes the following sub-systems/components or single elements:

(a) The EVC-Kernel: core sub-system of the On-Board Unit Sub-System, is responsible for the data processing and the achievement of the ATP Functions allocated to the On-Board Unit Sub-System. Peripheral modules, associated to the EVC-Kernel, for interfacing with the sub-systems external to the EVC-Kernel or with the train signals (Train Interface), are also part of this sub-system. The main ATP functions of the EVC-Kernel sub-system are:

(1) to receive the track-to-train messages via the Trainborne Eurobalise or GSM-R & RTM Euroradio sub-systems;

(2) to compute the relevant target speed and target distance;

(3) to process the signal sent by the Trainborne Odometry Sub-System and to deduce the train speed and the train location;

(4) to provide to the driver, via the DMI, cab signaling information on basis of the computed targets and train location;

(5) to compare the calculated or measured information against the allowed targets (i.e. the train speed level and braking curve supervisions) and then to ensure the Automatic Train Protection Functions (i.e. to apply the "service brakes" or the "emergency brakes" if required).

(b) The Odometry Sub-System is responsible for the measurement of the train speed, the distance covered by the train, the train acceleration/deceleration, the detection of the train direction of movement and the detection of the train standstill position. Odometric Sensors, that provide raw "speed/distance information", are associated to the Odometry Sub-System which processes this information;

(c) The Trainborne Eurobalise Sub-System with one or two Eurobalise Antennas (depending on the configuration - two are used for availability purposes) is responsible for the reception of track-to-train messages transmitted by the Trackside Eurobalises;

(d) The ETCS Trainborne Euroradio Sub-System, composed of a redundant RTM Sub-System connected to GSM-R Mobile Terminals and their associated GSM-R Antennas. The ETCS Trainborne Euroradio Sub-System provides bi-directional radio communications between the On-Board Unit Sub-System and the Trackside Sub-System. Two GSM-R Mobile Terminals are needed to comply with the availability and interoperability requirements;

(e) One DMI Sub-System (i.e. one Cab Display) per cabin providing the interface between the EVC-Kernel and the Driver by means of an LCD display screen and a keyboard. For trains with dual cabins, there is a DMI (a Cab Display) for each driving position. The standard DMI Sub-System configuration is made of one "CPU" module and two LCD Displays for a higher availability;

(f) The Train Recording Unit (TRU) Sub-System composed of:

1) The Juridical Recording Unit (JRU) Sub-System for recording juridical data for later investigation in the event of a train operating incident or accident. The JRU is also responsible for receiving and providing the Trainborne EVC-Kernel Sub-System with the UTC_ reference and the local_time;

2) The Diagnostic Recording Unit (DRU) Sub-System for storing the "diagnostic data" of the On-Board Unit Sub-System and the possible transmission of these data to the trackside;

(g) The Programming Tools, outside the On-Board Unit Sub-System equipment fitted on the train, but in the OBU Scope. These tools enable the "Programming Staff" to upload trainborne parameters or data. The Programming Tools are part of the On-Board Unit Sub-System, although they are not physically and not permanently mounted in the train;

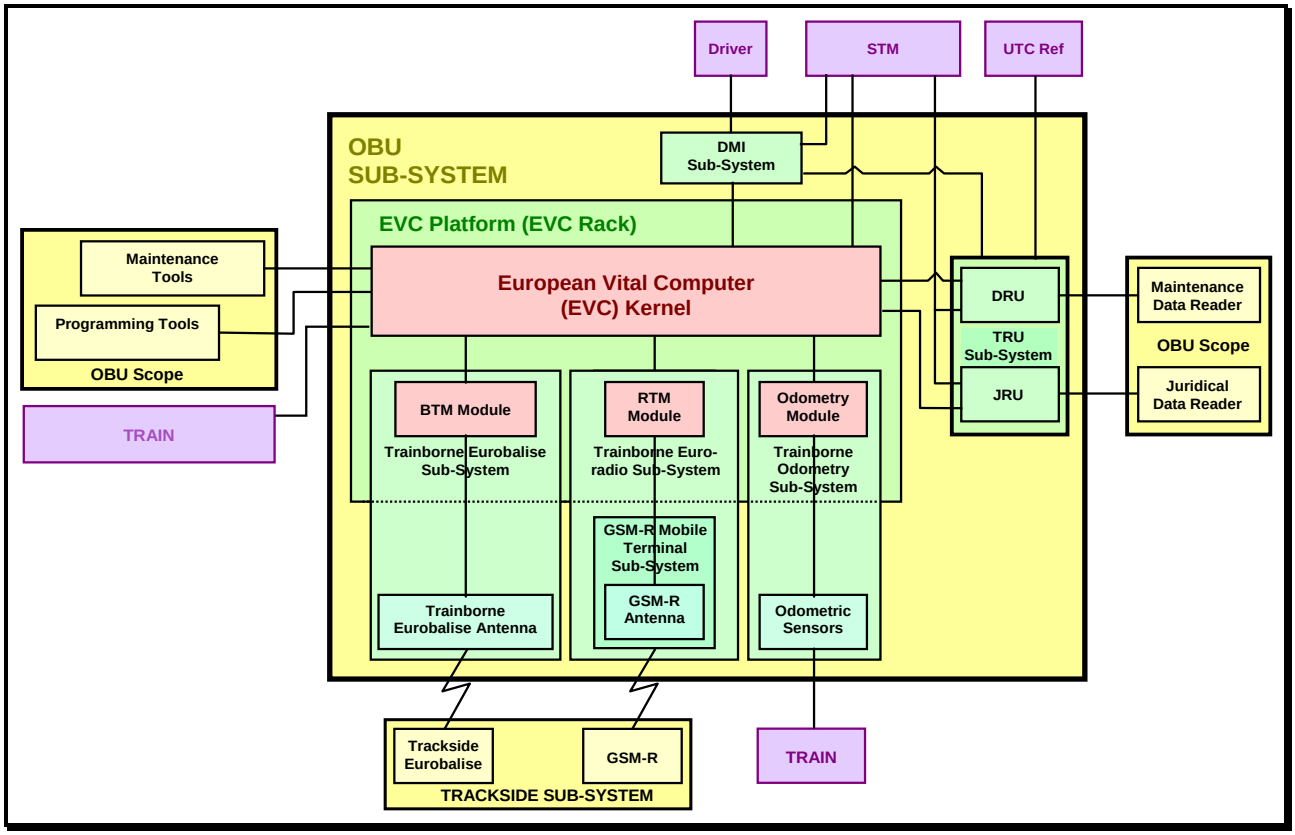

Figure 8: Internal architecture of the On-Board Unit

2.5 General characteristics of the system

For performance purpose only, the On-Board Unit equipment shall operate under specific temperature, EMC/EMI, vibrations, tension, etc., conditions. In case some of these conditions are not observed during operation, the On-Board Unit equipment goes in failsafe mode.

Indeed, the On-Board Unit Safety Case is valid only within the specified range of external influences, as defined in the sub-system requirement specification. Safety is not guaranteed outside these limits. Nevertheless, the general safety principles of the EVC Platform combining composite fail-safety, reactive

fail-safety and inherent fail-safety principles enable the On-Board Unit Sub-System to remain safe even if subjected to external influences outside the specified limits.

These conditions under which the On-Board Unit subsystem works are defined in the “Operation with external influences” section of the safety case.

The trainborne equipment enters a fail-safe state (shut-down) in case of higher environmental constraints than specified, e.g. EMC/EMI or temperature.

Technical validity conditions, under which the On-Board Unit subsystem shall operate are described in the Safety Related Applicable Conditions (SRAC) section of the Safety Case, see section 3.2.1.3 for more detail.

3 Development Lifecycle Activities

From a general point of view, the development phases of the On-Board Unit Sub-System life-cycle can be viewed as a "top-down" process followed by a "bottom-up" one of a "V" diagram.

3.1 Engineering and certification stakeholders

3.1.1 Project Management

The Project Manager has the overall project responsibility, including Quality, Safety and RAM, Verification and Validation.

From a Safety Assurance point of view, the Project Manager is responsible for the following activities:

(a) the issuing of the "Project Quality Plan" and/or "Project Organisation Description";

(b) the approval of this Safety Plan, the Project Development Plan, the Project Verification & Test Plans and the Safety Case;

(c) the implementation of scheduled activities;

(d) the management of the Design, Verification and Testing activities;

(e) the approval of the ERTMS Core Project Safety Cases.

3.1.2 Project Safety Assurance Manager (PSAM or Validator)

The Project Safety Assurance Manager is responsible for the management of the following activities:

(a) Safety Assurance and Safety Validation;

(b) RAMS Engineering.

The Project Safety Assurance Manager is responsible for both the Safety and Quality aspects of the project. Therefore he is also to be considered as the Project Validator.

The Project Safety Assurance Manager (i.e. the Validator) has the responsibility for ensuring the compliance of the OBU Sub-System against the CENELEC standards EN 50126, EN 50128 and EN 50129.

Safety Assurance and Safety Validation Management include the following activities:

(a) Safety Assurance activities:

  (1) to set up with the Project Manager a project organization and the development process in order to comply with the Safety Assurance Requirements;

  (2) to set up the Safety Plan;

(3) to ensure the interface between the Safety Assurance Team and the Development Team;

(4) to ensure the interface between the external Independent Safety Assessor (ISA) and the ERTMS Core Project;

(5) to manage the Safety Case (i.e. Proof of Safety) according to the CENELEC standard EN 50 129;

(6) to manage the "RAMS interface and requirements" with other Alstom sites or sub-contractors involved in the ERTMS Core Project;

(7) to perform with the Project Quality Manager external (i.e. of sub-contractors) Safety and Quality audits in order to ensure the compliance with the Alstom plans and procedures;

(8) to take part to the Change Control Board (CCB) - (i.e. change request assessment);

(9) to interface with the Project Safety Assurance Managers of the ERTMS Application Projects;

(b) RAMS Engineering activities: the Project Safety Assurance Manager is responsible for the management and the driving of the RAMS and Safety Validation activities. This includes the management of the following activities:

(1) to set up and carry out a RAMS Program and Plan in accordance with the CENELEC standards;

(2) to define the safety requirements at various stages of the development process;

(3) to set up and manage the Hazard Log;

(4) to perform safety reviews of all development and test activities and documents;

(5) to write the Safety Management and Technical Safety Report sections of the Safety Case according to the Safety Plan and to the CENELEC standard EN 50 129;

(6) to attend Design Reviews from the technical point of view;

(7) to co-ordinate RAMS and Safety Validation activities, in order to:

(i) verify RAMS aspects (e.g. remarks and critics when reading the design documents) throughout the whole development process;

(ii) verify the RAMS requirement achievement through analyses;

(iii) assess proposed design alternatives;

(iv) request additional tests enabling to validate the safety assumptions made in the scope of the OBU System/Sub-System Safety Studies (e.g. in PHAs, FMECAs, FTA, etc.).

3.1.3 RAMS Team/Engineers

The RAMS Engineers are directly responsible for the carrying out the following RAMS activities:

(a) to verify the RAMS requirements through RAMS analysis/studies;

(b) to assess design alternatives proposed by the Design Team;

(c) to review relevant design documentation;

(d) to attend design reviews;

(e) to participate to ISA Audits and/or to meetings when necessary.

3.1.4 Verification and Testing

Although from the target achievement point of view, the Verification and Testing is the responsibility of the Project Manager, this is actually independent from the Design Team. The required independence is achieved by the Test Specification activity and by the Validation Audits/Reviews of the test procedures and activities.

3.1.5 Project Quality Assurance

The Quality Manager of the ERTMS Core Project is responsible to define with the Project Manager, the Project Safety Assurance Manager, the Platform Director and the Department Heads the various processes and tools to be applied, as well as to monitor and control their application.

3.1.6 Site Safety Officer

The Site Safety Officer has the responsibility for evaluating the Safety Management System of the site in compliance with the Alstom Transport Information Solutions instructions and the prescriptions of the Product Safety Manual.

The Site Safety Officer:

(a) has the power to prevent the delivery of any System/Sub-System or equipment the safety level of which is not judged sufficient;

(b) is the only person allowed to sign the internal authorization (i.e. the formal permission) to put a System/Sub-System or an equipment into service within specified application constraints;

(c) approves the Safety Cases and Safety Reports.

3.1.7 External Independent Safety Assessor and/or Notified Body

As defined by the CENELEC standards, a Safety Integrity Level 4 System/Sub-System requires a third party assessment. This assessment takes place from the early stage of the ERTMS Core Project in order to deal with the applied process.

In a first step, the ERTMS Core Project is subjected to an Independent Safety Assessment.

In a second step, a Notified Body (NOBO) is appointed to the ERTMS Core Project reusing the results of the ISA assessment but performing the certification of predefined Interoperability Constituents, which are subjected to the European Directive 2008/57/EC (EC, 2008)(i.e. on the interoperability of the rail system) replacing both the European Directive 96/48/EC (EC, 1996) (i.e. on the Interoperability of Trans European High Speed Lines) and the European Directive 2001/16/EC (EC, 2001) (i.e. on the Interoperability of Conventional Lines) from 19 July 2010.

The Interoperability Constituents are not treated as standalone products during NoBo assessment, but are certified when integrated in the context of the On-Board Unit Application. While the role of the NoBo is interoperability, this also includes Safety among the essential interoperability requirements (UNISIG subset-091, quoted in the TSI, gives the safety requirements for the ETCS levels 1 and 2). We note also that in the general case the NoBo and ISA are not necessarily different bodies.

3.1.8 Other Intervening Parties

In the scope of the ERTMS Core Project, some products are developed either in other Alstom units or by sub-contractors. These other intervening parties follow their own Safety and Quality Process. By this way the "sub-contractors" are able to use their own process rather than being forced to use the OBU Process. The OBU team allocates requirements at the contract definition stage and performs follow-up during contract execution.

3.2 Activities executed by stakeholders

3.2.1 Safety Management Activities

The EN standards require a safety management process, for the reduction of the incidence of safety-related human errors throughout the life-cycle, in order to minimize the risk of safety-related systematic faults. These are performed by the Project Safety Assurance Manager. Each section below presents the elements of the safety management process.

3.2.1.1 Organisation

The organization used to execute the safety management process presented in section 3.1 above.

3.2.1.2 Safety Plan

The OBU Project Safety Plan was produced in order:

(a) to describe the Safety Management Process set up by ALSTOM;

(b) to give details on the management of the activities of Sub-System Safety Management and Sub-System Safety Engineering that are required to identify, evaluate and/or eliminate hazards, or reduce the associated risk to an acceptable risk level;

(c) to explain the role and the activities performed by the Safety Assurance team for the validation of the OBU development activities.

3.2.1.3 On-Board Unit Sub-System Hazard Log

The purpose of the Hazard Log is to document and to track all the On-Board Unit Sub-System Hazards and their related safety mitigation measures from their identification until their elimination or until the associated risk is reduced to an acceptable level.

Safety related hazards are identified at the overall ERTMS application level (System Risk Analysis and System Hazard Analysis) and are cascaded to sub-systems (Trainborne, Trackside) which most control for them. During Sub-System Risk Analysis and Hazard Analysis, the measures of protection are determined.

A Hazard describes the unwanted consequence of a failure condition, including for example:

- Collision
- Train on wrong track
- Overspeed
- Failure of distance measurement
- Derailment

The full hazard list also includes some hazards not linked to train movement, such as:

- Fire
- Electrocution

Each entry in the Hazard Log is characterized by:

(a) the description of the hazard;
(b) the traceability of the hazard to the safety study where it has been identified;
(c) the risk associated to the hazard (severity, probability);
(d) the status of each hazard (open, closed, cancelled...);
(e) the hardware and software elements responsible for the hazard;
(f) the measures to be taken related to the Design, Manufacturing, Verification and Validation in order to be able to accept the hazard;
(g) Evidence of satisfaction of the measures.

Some hazard log items are safety requirements that come from the generic products. They are usage constraints that must be satisfied by the On-Board Unit sub-system.

Example: “Constraint exported from the DMI to the On-Board Unit”

> When the EVC wants to stop the totality of the safety controls executed by a DMI, the data "Cycle Number", sent through the Safety layer , has to be compliant with these following SIL2 requirements :
> - The data "CycleNumber" is defined equal to "-1" only for the cycles of safety inhibition . (CycleNumber value Integrity)
> - The DMI which has to be inhibited is selected in safety . (DMI Id Authenticity)

The status of a hazard log entry is closed when all of the measures associated with that hazard are implemented and verified:

- The action is “implemented” if evidence can be found in a document from the descending phase of the V cycle (typically in a design document)
- The action is “verified” if evidence can be found in a document from the ascending phase of the V cycle (typically in a test report)

The Hazard Log is managed by using the HALOMAT (HAzard LOg MAnagement Tool) software tool (internal to ALSTOM), which is based on Microsoft Access.

The following sample illustrates a typical Hazard Log entry (only a selection of the entry fields is represented):

MeasRef : OBU_ANT_REC_24 **Implemented :** Yes **Verified :** Yes
Measure :
The on-board equipment shall ensure safe operation in case of transmission of a corrupted message

Implementation :
Reference :
OBU_BSI_RAMS_0050
Paragraph reference :
Section 4.4.2
Verification
Reference :
OBU_BSI_VIT_0050
Paragraph reference :
Section 5.3.6

3.2.1.4 Verification of Requirements Traceability

A simplified V-diagram is represented in Figure 9. It shows traceability links for functional, technical and safety requirements through the descending phase of the development cycle, and indicates the Hazard analysis carried out at each step. These protection measures elaborated by Hazard analysis are the "Safety Requirement Specifications" to be implemented in the design of the On-Board Unit Sub-System.
A top-down traceability table is produced in order to demonstrate that the requirements of the previous phase are taken into account by each phase of the V cycle.
An initial set of Safety Requirements for the On-Board Unit Sub-System are derived from the ERTMS Application Projects. The safety requirements from UNISIG (SUBSET 091) are included in this set.

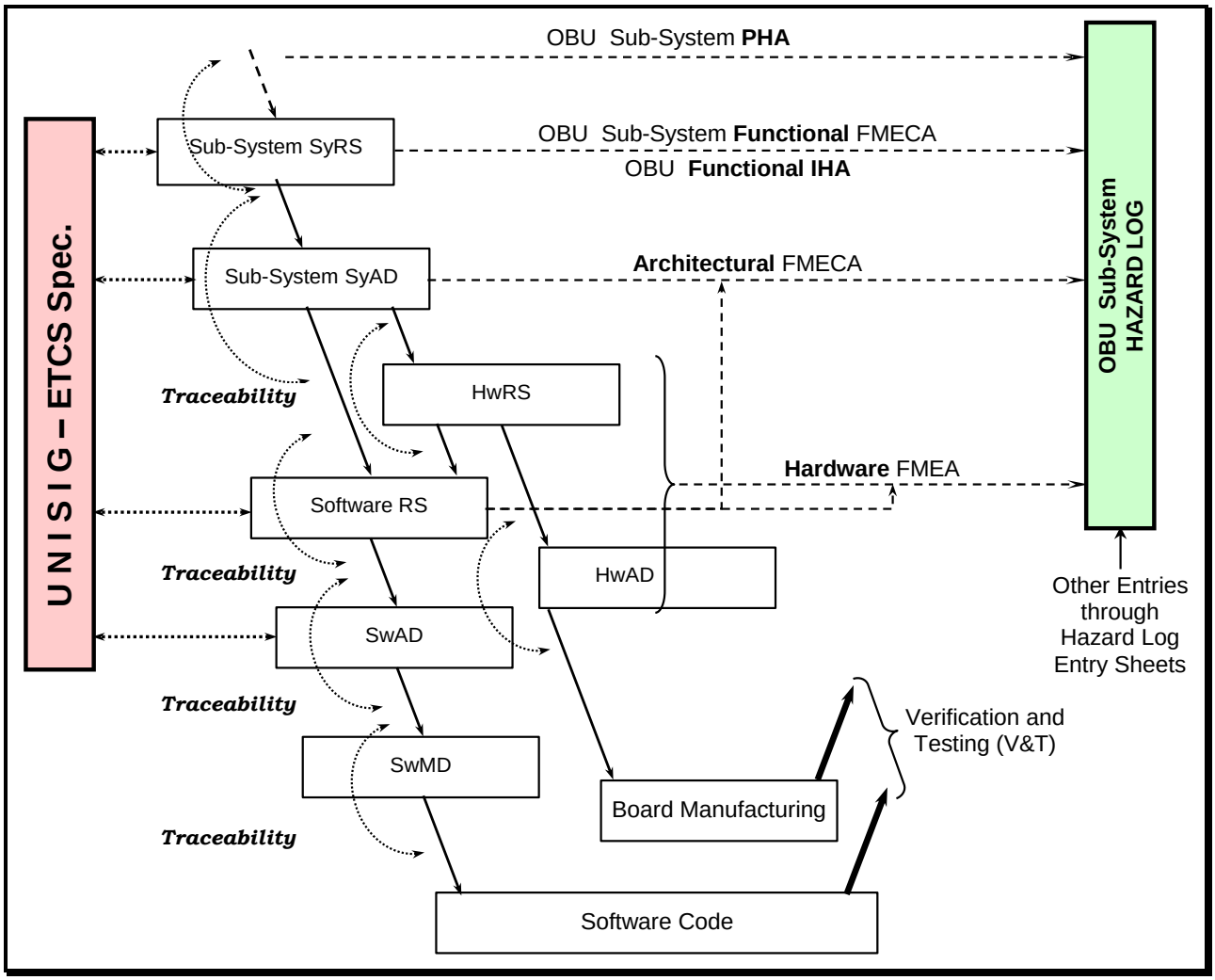

Figure 9: Traceability of Requirements and Hazard Analysis steps

3.2.1.5 On-Board Unit Sub-System Hazard Analysis

The purpose of this Hazard Analysis is to specify the safety requirements of the On-Board Unit Sub-System. This consists in identifying:

(a) the safety functions of the On-Board Unit Sub-System, and;
(b) the Safety Integrity Level of these functions.

The methodology is summarized by the following steps:

(1) evaluate the technical solutions proposed in the Design documents;
(2) identify possible hazards related to these solutions;
(3) identify mitigation measures/safety requirements in order to:
  (i) eliminate the hazard if an appropriate design alternative exists, or

(ii) prevent the hazard from occurring, or
(iii) protect against the effects of the accident;
(4) enter and manage the identified hazards in the On-Board Unit Sub-System Hazard Log.

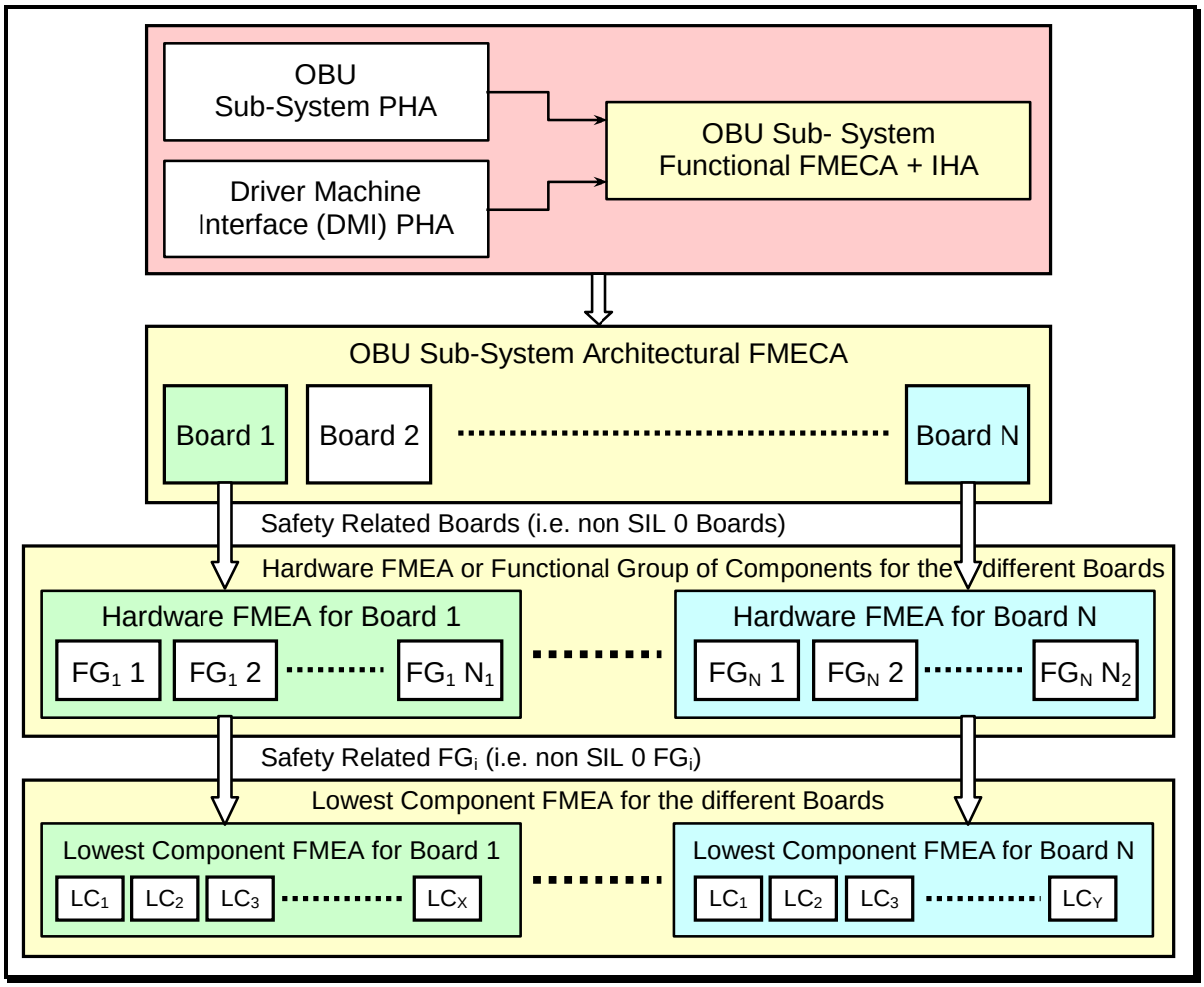

Figure 10: Hierarchy of the On-Board Unit Sub-System Hazard Analyses

Relation between these Hazard Analyses of the On-Board Unit Sub-System:

The hierarchy of the On-Board Unit Sub-System Hazard Analyses shown in Figure 10 indicates the "top-down" indenture levels of the On-Board Unit Sub-System FMEA. The top three levels of Figure 10 have been carried out:

(a) the purpose of the Functional FMECA (including the IHA) and of the PHA (at an early stage of the OBU Project for the PHA) is:

(1) to list the Trainborne Sub-System functions and their safety severity (including the Functional Inputs/Outputs of the EVC);
(2) to raise mitigation measures applicable to the Trainborne Sub-System and to record them in the Hazard Log of the On-Board Unit Sub-System;
(3) to trace the identified mitigation measures (i.e. Safety Requirements) with regard to the UNISIG mitigation measures raised in the SUBSET 091;
(4) to identify the mitigation measures (i.e. Safety Requirements or Application/Re-use Constraints) that are to be implemented at the ERTMS Application Project level.

(b) based on the Trainborne functions and their safety severity allocated by the Functional FMECA, the purpose of the Architectural FMECA is:

(1) to list the functions of the different modules/components of the On-Board Unit Sub-System and;
(2) to perform a first determination of the SIL allocation per component;
(3) to raise mitigation measures/Safety Measures applicable to the different modules/ components of the On-Board Unit Sub-System, and to record them in the On-Board Unit Sub-System Hazard Log.

(c) based on the Safety Integrity Allocation to the On-Board Unit Sub-System modules/components by the Architectural FMECA, the purpose of the Hardware FMEA is:

(1) to list the functions of the different Functional Groups of Components (FG 1, FG 2, etc.) of the associated hardware module/board, as well as the safety severity of those functions and then Functional Groups of Components;
(2) to raise mitigation measures/Safety Requirements applicable to the considered Functional Groups of Components and to record those mitigation measures in the Hazard Log of the On-Board Unit Sub-System;
(3) to provide an indication of the testability of the hardware module/board against the considered failure modes of the group of components (and/or individual components, i.e. the fourth indenture FMEA level identified in the OBU Project Safety Plan);
(4) to determine for the Functional Groups of Components:

(i) the single point failure tolerance;
(ii) the operational impact of the considered failure mode at the level of the hardware module/board;
(iii) the testability, fault detection period and designed fault mitigating capability.

3.2.1.6 HW & SW Component SIL Allocation

The safety related functions identified by the Hazard Analyses are managed by both hardware and software components of the On-Board Unit Sub-System. This leads to define SIL requirements to be fulfilled by the hardware and software components of the On-Board Unit Sub-System.

In addition to those requirements for components, two off-line processes are identified as being related to safety, and lead to additional requirements:

- the Data Entry Procedure for DMI shall be suitable for a SIL4 application;
- the Data Preparation Process shall be suitable for a SIL4 application.

3.2.1.7 Safety Reviews

The safety reviews are meetings involving the project staff and the site safety officer, the purpose is to perform a review of open points affecting safety.

3.2.1.8 Safety Verification and Validation

The Safety Verification and Validation activities performed on the On-Board Unit Sub-System, in order to comply with the SIL 4 Development Process Requirements, are pictured in Figure 11.

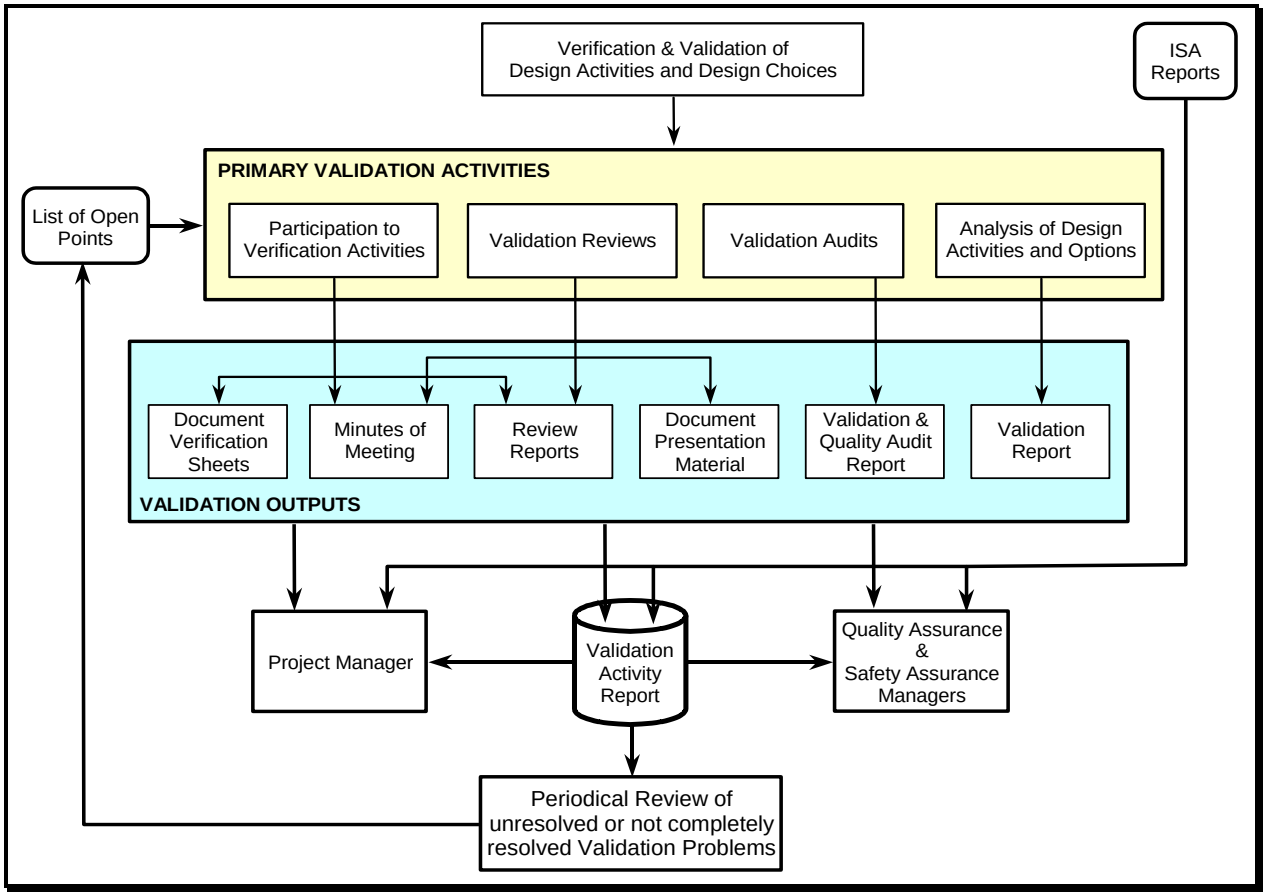

Figure 11: Safety Validation Process

The following table gives the compliance of Verification and Validation techniques/measures used on the On-Board Unit Sub-System to the techniques/measures that are recommended by Table E9 (Recommendations for System and Product Design V & V) of the CENELEC Standard 50 129 for SIL 4 Sub-Systems.

Table 1: Verification and Validation on the On-Board Unit Sub-System (Table E9 of CEN 50 129).

Techniques/Measures	SIL4	Compliance / Description (chapter references apply to On-Board Unit Sub-system Safety Case)
1. Checklists	R	All End of Phase Reviews and (Critical) Gate Reviews are carried out by going through prepared detailed checklists
	Compliant	Yes
2. Simulation	R	
	Compliant	Yes
3. Functional testing of the system	HR	Yes. Comprehensive functional tests are carried out on the bases of well defined test cases to demonstrate the specified characteristics and safety-requirements are fulfilled
	Compliant	
4. Functional testing under environmental conditions	HR	Yes. EVC Platform functional testing under environmental conditions.
	Compliant	

5. Surge immunity testing	HR	Yes. Surge immunity are tested higher / higher limit than the boundary values of the real operation conditions
	Compliant	
6. Inspection of documentation	HR	The review process of design documents throughout Quality Process.
	Compliant	Yes. Inspection and assessment of design documents throughout Safety Analyses.
		The verification of (software) design documents throughout independent Verification & Validation activities
7. Ensure design assumptions are not compromised by manufacturing process	HR	Yes. Specified manufacturing requirements and precautions, plus audit of actual manufacturing process by safety organisation.
	Compliant	
8. Test facilities	HR	Designer of the test facilities are independent from the designer of the system or product.
	Compliant	Yes
9. Design Review	HR	When necessary, Design Reviews are carried out at the different stages of the life-cycles in order to confirm that the specified characteristics and safety requirements are achieved by the On-Board Unit Sub-System.
	Compliant	Yes. The review process of design documents throughout Quality Process
10. Ensure design assumptions are not compromised by installation and maintenance processes	HR	Yes. Installation and maintenance procedures/manuals are produced in order to guarantee that design assumptions are respected during the installation and the maintenance operations.
	Compliant	
11. High confidence demonstrated by use (optional, where some previous evidence is not available)	R	1 million hours operation time, at least 2 years experience with different equipments including safety analysis, detailed documentation also of minor changes during operation time
	Compliant	Yes

3.2.1.9 ISA & ISA Report - Safety Endorsement

The Independent Safety Assessor Audits of the On-Board Unit Sub-System cover the assessment and compliance checks with regard to the CENELEC Standards 50 126, 50 128 and 50 129 for the following topics:

(a) the Quality Management Process;

(b) the Safety Management Process;

(c) the Technical Safety and Safety Principles of the EVC Platform as a SIL 4 equipment;

(d) the SIL 4 Software Development Process;

(e) Safety Cross-Acceptance of some already assessed components;

3.2.2 Quality Management Activities

The following Quality Assurance activities are performed

(a) to establish with the Project Manager and the Safety Assurance Leader the Project Management and Project Quality Plans;

(b) to support the development and the application of the different plans and procedures of the ERTMS Core Project;

(c) to organize Design Reviews requested by the Project Manager or the Project Safety Assurance Manager in order to ensure the correct application of processes defined in plans (Design, Management, Configuration, Change Control, Planning, Safety Assurance, etc.);

(d) to support, in the Alstom Organization, the "End of Phase" and "Gate Reviews";

(e) to report the Quality Assurance activities, the project problems and non-conformances to the Management (TIS CRL Quality Manager, Project Manager and Project Safety Assurance Manager);

(f) to elaborate the Software Quality Plan, defining the quality assurance activities to put in place in order to control the software development;

(g) to support internal or external quality and safety audits (by ISA and/or Customer);

(h) to follow-up from the quality aspect point of view the sub-contractors.

4 Engineering environment

The methodological framework of Alstom Transport includes regulation of the design processes and the engineering environment (i.e. the tools). The specification of the systems follows internal instructions in which several approaches may be applied depending on the nature of the system being developed. For example, until recently the specification of complex signalling systems used the Structured Analysis SA/RT (Ward & Mellor, 1985). Specific tools have been used to apply this technique, but the result of the design used to be described into Microsoft Word Document.

Alstom recently adopted a model-based system engineering approach. This approach allows the specification of the system with a set of models. These are supported by a standardized notation called System Modelling Language (OMG, 2012) (SysML is standardized by the Object Management Group - OMG). The tool actually used in Alstom to model the system within SysML is Artisan Studio developed by Atego (Artisan, 2012). The models are recorded into an SQL server database and an Atego proprietary API (Applied Programming Interface) is required to access these models from outside Artisan Studio.

Traceability evidences may be performed with the Rectify tool (Dassault Systèmes). However some system development uses IBM Rational Doors. Rectify and Doors bridges are available to trace information within Microsoft Word and Excel files, Artisan SysML models and source code.

The safety plans are defined in natural English with Microsoft Word. There is no mandatory project management support tool.

The Failure Mode and Effect Analyses (FMEA) are conducted in Microsoft Excel files. The Hazard Log is managed by using the HALOMAT (HAzard LOg MAnagement Tool) software tool (internal to ALSTOM), which is based on Microsoft Access. The fault-tree analyses are modelled with specific tools such as Risk Spectrum, Item Toolkit, Aralia, RAM Commander or Safety-Designer. The results of the fault tree analyses are described within a Microsoft Word document.

The content management systems (document, models, etc.) are home made. There are several content management systems within Alstom Transport. These tools have generally a web-based user interface. The content (document in general) is uploaded to the content management system. The contents are stored in specific databases.

The configuration management is performed by IBM Rational ClearCase, the change requests are managed by IBM Rationale ClearQuest.

5 Summary of main argument for safety

From the general point of view, the fail-safety of the On-Board Unit Sub-System is ensured by both composite and reactive fail-safety of its most important item called the "EVC Platform or EVC Rack".

6 System lifetime events

The project execution is regimented by events called Gate Reviews, which consist of the satisfaction at a given date of formal checklists to ensure the next phase can be started without significant risk of rework.

Table 2: Gate reviews definition

Name	Abbr.	Objective of the Review
Specification Gate Review	SGR	All contractual requirements have been translated into an approved specification of user needs.
Preliminary Gate Review	PGR	The basic architecture of the technical solution has been approved by the director of the related product line.
Critical Gate Review	CGR	Detailed design has been completed.
First Equipment Inspection	FEI	Integration tests have been successfully passed.
Initial Quality Approval	IQA	Factory activities of functional validation and formal verification are completed sufficiently to start on-site sub-system tests and customer acceptance.
Validation Gate Review	VGR	The system is ready for revenue service : • On-site validations and verifications are completed; • On-site dynamic testing are completed; • Sub-system acceptance testing is completed; • The Safety Case is approved.
Final Quality Approval	FQA	Partway through the warranty phase, performance objectives have been met and accepted by the customer; all contractual deliveries have been performed; Return Of Experience has been formalized.

7 Relationship to conceptual and technical work packages and expected results

The certified On-Board Unit subsystem presented above will support the description of the Railway domain expectation for OPENCOSS. This section deals firstly with the general vision in which OPENCOSS shall improve the certification engineering process. Issues related to the European Railway certification context are discussed. These issues are related with the Use-Case information contained in the On-Board Unit description above. Secondly, the specific objectives of the technical Work Packages are discussed with the point of view of the On-Board Unit.

7.1 Overview and general issues

7.1.1.1 Transversal goals

The main objective of this Use-Case is to provide industrial knowledge on how a typical railway signaling system is developed and certified. This knowledge aims at supporting the OPENCOSS developments to improve the safety engineering activities performed by both manufacturers and Independent Safety Assessor. The general idea is to build progressively the case for safety, build incrementally the argumentation and to support its assessment. The application of the following would contribute to this goal:

- To have support for intertwined system engineering and safety engineering processes (to be able to access and to link to the information of each stake-holder),
- To support the incremental build (progressive refinement) of the design,
- To provide support for re-certification when performing product and system revisions,
- To support the traceability (*e.g.* between requirements and test cases and test results, between change orders and engineering impacts),
- To provide workflow support for the project safety engineer,
- To provide support for the ISA to assess the case for safety,
- To manage the Question & Answer process with the ISA.

Sections 3 to 6 of this document describe the engineering activities to support.

7.1.1.2 Certification in divergent regulatory context

Despite the effort achieved by the European Standardization committee (CENELEC), national authorities can impose their own safety constraints to the certification of a system. These safety requirements are divergent from one country to another. This issue raises major difficulties for manufacturers to obtain the “cross-acceptance” of a system certified for a country A in a country B. OPENCOSS platform shall provide a facility allowing to identify for each European country the differences between normative safety requirements. The objective is to remove the barriers set by each country to apply cross-acceptance from one country to another. This issue is similar to the OPENCOSS problem addressed in cross-domain certification (See Avionics Use-Case).

7.1.1.3 Compositional certification

The On-Board Unit Use-Case describes three cases of compositional certification for the generic products used by the On-Board Unit: BTM, DMI and Odometry. See section **Error! Reference source not found.**.

Compositional certification shall be supported without the pitfalls related to the proliferation of usage constraints exported in the safety case contract: redundant, superfluous and incomprehensible constraints

must not outweigh the benefits of the composition. The exported constraints are described in section 4.5 of the safety case (CENELEC, 2003). The hazard log integrates these exported constraints for the application and generic product; see §3.2.1.3.

7.2 Specific Work Package goals

7.2.1 WP2: Requirements and Architecture Design

The expected results presented in this section 7 are basis for the OPENCOSS platform requirements capture and refinement (*i.e.* Railway User needs).

7.2.2 WP3: Platform Integration and Validation

The task T3.1 "Analysis of safety certification data of industrial use case" will perform real data capture. This data will illustrate the engineering activities and the transversal issues rose in the section 7.1.

7.2.3 WP4: Common Certification Language

The CCL will be in our vision the modeling language of the evidences and the argumentation. Another highlighted aspect of the CCL is to provide support for the convergence of certification for both cross-domain certification (to align the constraints coming from one to domain to another) and for divergent regulatory context ("cross-country" certification).

Arguments are included in the Hazards Analysis and in the Technical Safety Report chapter of the Safety Case.

Evidences are included in:

- the Hazard Analysis worksheets including FMEAs,
- the Verification and Validation reports,
- the evidence contained in the safety case of a reused product.

Certification constraints differences shall be analyzed within the specific domain standards (DO178B, ISO26262, CENELEC).

Divergences of railway regulatory contexts shall be analyzed within the national authority regulations.

The CCL shall also provide support to drive the ISA in its assessment.

7.2.4 WP5: Compositional certification

The Railway Use Case proposes an application example of compositional certification. Indeed, the On-Board Unit uses several generic products (DMI, Odometry, BTM, etc.). The compositional certification will be used to improve the cross-acceptance approach for the generic products used by the On-Board Unit.
It shall allow the safety manager of a generic product to identify and express the contract that a product consumer has to accept when integrating the product into its system architecture

7.2.5 WP6: Evolutionary Evidential Chain

The evolutionary evidence chain will be used to store the progressive building of the case for safety (Hazard Analysis and Safety Requirements management). Since the Hazard Log presented above (section 3.2.1.3) is

a report based on the content of the evidences repository, the Evolutionary Evidential Chain is the infrastructure of this repository, where the evidence, the safety requirements and SRAC's are stored.

7.2.6 WP7: Transparent Certification and Compliance-aware process

This WP shall support the certification stakeholders to assess where they are with respect to their duties to conform to safety practices and standards, and still to motivate them to see the effective progress of the work and level of compliance. Additionally, this management infrastructure shall take into account the collaborative aspect of the processes. It shall provide means to record certification stakeholder interactions that drive the process such as

- System Lifetime events (Gate Reviews), see section 6,
- ISA Questions & Answers log,
- ISA agreements.

8 Conclusions

The OPENCOSS Railway Industrial Use-Case has been described in this document. It is based on an existing and certified ERTMS subsystems developed by Alstom Transport. This subsystem and the methodology that led to its certification have been presented. Relationships with the technical work packages of OPENCOSS define the industrial needs that this particular Use Case aims to address in OPENCOSS. These are summarized below:

- to build progressively the case for safety, to build incrementally the argumentation and to facilitate its assessment;
- to provide support allowing to overcome the barriers set by each country to apply cross-acceptance from one country to another;
- to support and generalize compositional certification;
- to capture emergent properties related to constraints of use of a certified generic product.