Reference	153821-NWR-REP-ESE-000005
Issue/Ver:	3.0
Date:	26/03/19

Digital Railway – ETCS Onboard System Definition

Prepared by:
John R Senior
Lead Architect - ETCS Onboard

JRS-260319-007 Date: 26 March 2019

Reviewed by:
David Nicholson
System Integration and Interface Manager

DJN-26032019-0093 Date: 26 March 2019

Approved by:
Rubina Greenwood
Head of System Requirements & Integration

RNG-270319-0087 Date: 27 March 2019

Working together for a better railway:

Reference	153821-NWR-REP-ESE-000005
Issue/Ver:	3.0
Date:	26/03/19

Electronic file reference: https://digitalrailway.ipss-hdms.co.uk/DigitalRail/Contents/Objects/6777B3

Disclaimer

Group Digital Railway has used its best endeavours to ensure that the content, layout and text of this document are accurate, complete and suitable for its stated purpose. It makes no warranties, expressed or implied, that compliance with the contents of this document will be sufficient to ensure safe systems of work or operation. Group Digital Railway will not be liable to pay compensation in respect of the content or subsequent use of this document.

Document owner: John R Senior, Lead Architect - ETCS Onboard

Version History

Issue	Date	Comments
0.1	07.02.2018	First issue
0.2	06.03.2018	Scope of the SDD changed: decision System Integration & Interface Manager (e-mail DN 20.02.2018). New Template used.
0.3	22.03.2018	Updated following Technical Author review
0.4	26.03.2018	Minor update, reviewed by the System Integration & Interface Manager (JJE)
0.5	26.03.2018	Reviewed by the Head of Systems Engineering (TB); section 12 Integration Fundamentals Handbook added. Reviewed by the Head of Systems Requirements & Integration (AM)
1.0	26.03.2018	Formal issue for signature
1.1	29.07.2018	Meeting review by DN, AL, RK, JS, AJ (18th July) plus further changes on interfaces and actions to close L2 and L3 reviews Issued for internal DR comment
1.2	02.08.2018	Updated following feedback from DN and AL
1.3	19.09.2018	Updated at DN and AL Onboard and Trackside SDD Review

Issue	Date	Comments
1.4	03.10.2018	Transposed due to formatting / template issues. Minor updates to comments / re-review Issued for L1 review.
1.5	01.11.2018	Updated to L1 comments (153821-NWR-COM-ESE-000005), DRIIAT comments (on v 1.4) and tech author review.
2.0	22.11.2018	Updated to final comments (L1 and DRIIAT) and issued for approval
2.1	22.03.2019	Updated to L3 comments plus minor template updates and revised boundary diagrams
3.0	26.03.2019	Minor update to review comments and issued for approval.

Exclusions

These are items currently missing from this version of the document that should be included in a later publication.

1. Revised DR Concept of Operations. (Note: It is assumed that the existing DR Concept of Operations [RD24] will be updated at a later stage.)
2. This document has been submitted for Level 3 assurance in accordance with the System Management Plan [RD25]. A response has been received showing no Category 1 comments (i.e. there is no issue associated with a fundamental concern, error, omission or question that has a direct bearing on the acceptability of the document). A response has been made to address the comments which is reflected in this version of the document. However, confirmation has not yet been received that these responses are considered to be satisfactory which may result in amendments to a future revision of this document.

Assumptions

These are items upon which the validity of this document relies, and which will be delivered by others. Non-delivery of these items will necessitate a change to this document.

None.

Dependencies

These are items upon which the validity of this document depends. Any changes to the referenced document may require further changes to this document.

1. Digital Railway System of Systems System Definition document [RD1]

CONTENT

ABBREVIATIONS

Abbreviations are explained in full on first use within this document. A comprehensive list of abbreviations and definitions is contained in the Digital Railway Programme (DRP) Glossary of Terms & Abbreviations [RI6].

REFERENCES

Dependent References

An update to one of these references requires a review to identify any potential need for an update to this document.

[RD1] Digital Railway – System of Systems (SoS) System Definition, 153819-REP-DRP-ESE-000002, v6.0

[RD2] Regulation (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union

[RD3] Commission Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009

[RD4] Commission implementing Regulation (EU) 2015/1136 of 13 July 2015 amending implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment

[RD5] Removed

[RD6] ERTMS/ETCS Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, Subset-091, v3.6.0

[RD7] ERTMS/ETCS RAMS Requirements Specification Chapter 2 – RAM, version 6, Reference EEIG: 96S126

[RD8] Removed

[RD9] BS EN 50126-1:2017, Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Generic RAMS Process

[RD10] BS EN 50126-2:2017, Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Systems Approach to Safety

[RD11] BS EN 50128:2011, Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems

[RD12] BS EN 50129:2003, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling

[RD13] Operational Concept for ERTMS, Issue 2, December 2014, RSSB

[RD14] Appendix A (version 4) to Technical Specifications "Operation and traffic management", ERTMS Operational Principles and Rules version 4 dated 30/06/15

[RD15] Operational Concept for the GB Mainline Railway, RSSB-GBMR-OC, Issue 02, March 2014, RSSB

[RD16] GB ETCS Testing Framework strategy, 053821-NWR-PRO-ESG-000001, v1.0 (24 April 2017)

[RD17] ERTMS/ETCS Environmental Requirements, EEIG:97s066, version: 5, 20/11/13

[RD18] BS EN 50125-3:2003 - Railway applications. Environmental conditions for equipment. Equipment for signalling and telecommunications

[RD19] Removed

[RD20] Assignment of values to ETCS variables, ERA_ERTMS_040001

[RD21] Digital Railway – M9 Significance of Change Assessment, 147883-NWR-ASS-ESS-000001, Ver.1.0, 19th February 2018

[RD22] Removed

[RD23] GB Testing Framework, 053821-NWR-PRO-ESG-000001, v2.0

[RD24] Digital Railway – Integrated Concept of Operations, 000000-NWR-PLN-MPM-000005, version 1.0, 15th May 2018

[RD25] DRP System Management Plan DRD-0000-DRSE-PLN-000001. v8.0

[RD26] Commission Regulation (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the 'rolling stock — locomotives and passenger rolling stock' subsystem of the rail system in the European Union

[RD27] Digital Railway Programme - System of Systems Architecture, 153819-NWR-DRG-ESE-000003, v5.0.

[RD28] Digital Railway – European Train Control System (ETCS) Trackside System Definition, 153821-NWR-REP-ESE-000006, v3.0

[RD29] Digital Railway – GB Generic Interface Requirements Specification, 153821-NWR-SPE-ESE-000013, v3.0

[RD30] The Management of Packet 44 Applications, RIS-0784-CCS, Iss 1

[RD31] ERTMS/ETCS DMI National Requirements, GERT8402, Iss 2.

[RD32] The Railways (Interoperability) Regulations 2011, SI 2011/3066

[RD33] Requirements for Data Recorders on Trains, GMRT2472, Iss 2

[RD34] Digital Railway – GB Generic Customer Requirements Specification for Operations & Maintenance, 153819-NWR-PLN-ESE-000014, Ver 2.0

Informative References

These references have no material bearing on the content of this document but are referenced within it. Unless otherwise specified, the latest version should be used.

[RI1] Digital Railway Programme - System of System Hazard Record Report, 153830-NWR-LOG-PRK-000001

[RI2] DR System Safety Plan, 147883-NWR-PLN-MPM-000008

[RI3] Digital Rail Programme Project Level RAID, 153821-NWR-REG-PRK-000001

[RI4] ERTMS/ETCS DMI National Requirements, GERT8402, Iss 2, June 2016

[RI5] The Management of Packet 44 Applications, RIS-0784-CCS , Iss 1, March 2017

[RI6] Digital Railway – Glossary of Terms & Abbreviations, 153819-NWR-SPE-ESE-000001,

[RI7] Digital Railway – GB Generic Customer Requirements Specification for ETCS Onboard, 153821-NWR-SPE-ESE-000008

1. Introduction

1.1 Background

Digital Railway is a rail industry-wide programme designed to benefit Great Britain's economy through more effective train operation, and improved customer experience and industry adaptability, enabled by accelerating the application of digital technologies to the railway. The benefits of the Digital Railway are expressed as:

- More trains
- Better connections
- Improved reliability

These benefits are to be realised by the Digital Railway Programme to GB Rail through the application of modern train control technology. The vision, purpose and objectives have been summarised in the System of Systems (SoS) System Definition Document [RD1] as:

- Increased capacity
- Safer, more secure & environmental railway
- Improved train performance (reliability and availability)
- Improved whole-life cost and sustainable commercial model
- Wider socio-economic benefits (e.g. skills, productivity, housing, exports)

This is an industry-wide programme involving Network Rail (as Infrastructure Manager and maintainer), Train and Freight Operating Companies (as Railway Undertakings), the Rail Safety & Standards Board (RSSB) and the supply chain. It will also engage with the Regulator and the Department for Transport (DfT), as necessary, to secure the required improvements to safety and customer provision, funding and approvals.

The European Rail Traffic Management System (ERTMS) is a European-led initiative designed to provide a compatible train control system across Europe which enables fitted trains to cross from one member state to another without technical restrictions as part of an interoperable railway. The European Train Control System (ETCS) is the Control, Command part of the ERTMS.

The ETCS is mandated by European Regulation through application of the Control, Command and Signalling Technical Specification for Interoperability (CCS TSI) [RD2], and transposed into UK legislation, railway Interoperability Regulations (RIS) 2011 (as amended) [RD32].

Introduction of the ERTMS will affect on-board systems, trackside equipment, processes for the development of the signalling system, maintenance, and operational procedures.

1.2 The Digital Railway Programme (DRP)

The Digital Railway Programme has several principal outcomes, which are defined in the System Management Plan [RD25].

In the context of the Digital Railway Programme, the term 'System' refers to the various digital technologies to be deployed (i.e. European Train Control System (ETCS) Level 2, a Traffic Management System (TMS), and other sub-systems and enablers);

'System of Systems' (SoS) refers to their integration and deployment to reap the full benefits of the Digital Railway Programme. Both terms include more than just the products themselves, but also the people, processes and data required for operating them.

Whilst the concept is to deploy the System of Systems as a whole, each system may be contracted separately, and the sequence of deployment may reflect the needs of the business for a particular application.

1.3 Context & Purpose of This Document

An EU Regulation on the adoption of a Common Safety Method on risk evaluation and assessment (CSM RA) came into full effect through Regulation 402/2013 [RD3] and was amended by Regulation 2015/1136 [RD4] in August 2015. The CSM RA applies when any technical, operational or organisational change is being proposed to an operational railway. The Digital Railway Programme considered as a whole will bring complex technical changes to the rail infrastructure, resulting in a significant impact on the operation and organisation of GB's railway. A formal assessment of the significance of the change has been undertaken [RD21] and has concluded that the change is significant with a high degree of uncertainty and high consequence.

A key principle of the CSM RA is the preparation of a System Definition, i.e. this document. The purpose of the System Definition document under the CSM RA is to complement the hazard record by bounding the scope of the hazard identification and risk assessment process and to provide sufficient context to facilitate an assessment of the correct application of the process by an independent body (the Assessment Body, or AsBo).

Due to the industry-wide nature of DR, it is also an essential requirement that the DR Programme should clearly define what is meant by 'System of Systems' and 'System' and its interfaces to ensure successful requirement apportionment. This will minimise integration risk during deployment.

This System Definition document defines the ETCS Onboard and its interfaces and thus minimises integration risks. It forms part of a suite of four System Definitions that support the deployment of the DR System of Systems, including the System of Systems Definition Document [RD1].

This System Definition defines the key details of the ETCS Onboard, its purpose, functions and interfaces, and the existing safety measures that apply to it, so that it provides a generic system design in support of subsequent development and deployment (i.e. application-specific design and implementation).

It also allows the generic application specification and design for the ETCS Onboard to be assessed in accordance with the CSM RA in order to provide a basis for a safety case and the associated business change, operational rules and processes to be developed to support it.

This document has been written to facilitate a high-level understanding of the ETCS Onboard and is also intended to support the early stages of impact and hazard analysis of the proposed solution. It is a fundamental requirement that Onboard ETCS systems are CCS TSI compliant. All functions are detailed within this SDD for completeness (as the onboard ETCS system will react if the Trackside provides the relevant messages). However, where there is no current proposal / expectation that the GB network will be configured / allow the respective functions, relevant footnotes are provided within this SDD.

1.4 Scope

This document applies to the ETCS Onboard only.

This definition only considers the deployment of the ETCS Onboard System within the SoS and does not consider how a particular section of the railway might operate if only this system is deployed. Any variation from a full deployment of the SoS will need to be addressed by the particular Deployment Project (i.e. Infrastructure Maintainer and Railway Undertakings) concerned.

This document does not apply to a specific deployment of the core System; it deals with the generic system design and its associated interfaces (both physical and non-physical, e.g. operators).

This document does not describe the Systems of Systems within which it sits as this has its own System Definition [RD1].

1.5 Background of the Generic System of Systems (SoS)

The SR&I team will produce a set of GB rail specifications for system development and integration purposes using a common baseline architecture referred to as the System of Systems (SoS).

The SoS provides a modern integrated railway signalling command and control system based on:

- ETCS Level 2 No Signals
- Traffic Management System
- Connected-Driver Advisory System (C-DAS)
- Modern interlocking technologies

The SoS will be supported by:

- a fixed data network, e.g. the Fixed Telecoms Network (FTN) or the FTN – Next generation (FTNx);
  - a voice and data communications network;
  - data services, systems and protocols, Key Management and EULYNX; and
  - Operational Readiness to support the people and process change required

The SoS configuration ensures that the systems within it, e.g. C-DAS, the European Train Control System (ETCS) and the Traffic Management System (TMS) can be developed by the supply chain with the majority of the interfaces built in to minimise future integration and migration costs for deployment programmes.

1.6 Document Maintenance

This System Definition Document (SDD) is owned by the Lead Architect ETCS Onboard. It will be subject to review at least prior to each Technical Review to ensure its ongoing adequacy for progressing to the next stage gate. Other updates may be instigated, as necessary, when directed by the Head of System Requirements & Integration (SR&I)..

This document has presumed a particular technical solution, as outlined in the SoS System Definition [RD1]. However, if during execution of this plan, a different technical solution emerges that would also achieve the Digital Railway primary objectives (see section 2), then this will be considered. An update to this document may then be necessary.

This System Definition will be updated during this programme to reflect the evolving stages of development in order that it forms an accurate and final representation of the System.

The application of individual DR Systems to a specific section of railway is outside the scope of this System Definition Document. Specific applications will be addressed through a deployment-specific System Definition Document.

2. System Purpose and Objectives

The principal objective of the ETCS Onboard generic design is to provide Automatic Train Protection in conjunction with the ETCS Trackside System.

The Onboard uses data supplied from the Trackside and data entered by the driver to determine the safe envelope in which the train can move. Odometry from the train and geographical referencing via Eurobalise allows the Onboard to monitor the position of the train within the calculated safe envelope. Should the train exceed this envelope, then the Onboard intervenes to control the speed of the train, bringing it to a stand if necessary. Figure 1 below highlights the ETCS Onboard element and its interfaces (i.e. blue lines and boxes) within the DR System of Systems architecture.

Note that two interfaces of Configuration data and Voice Comms in the SoS are not replicated in the Onboard sub-systems architecture (Figure 2). The EuroBalise (aka balise) interface is represented by the single headed arrow interface from 'ETCS Trackside (L2 No Signals)' to ETCS On-board. 'Configuration Data' represents data managed by the supplier during design, data that is only amended by service personnel such as the maintainer and data entered by the driver. (There is not a physical interface on the system labelled 'configuration data')

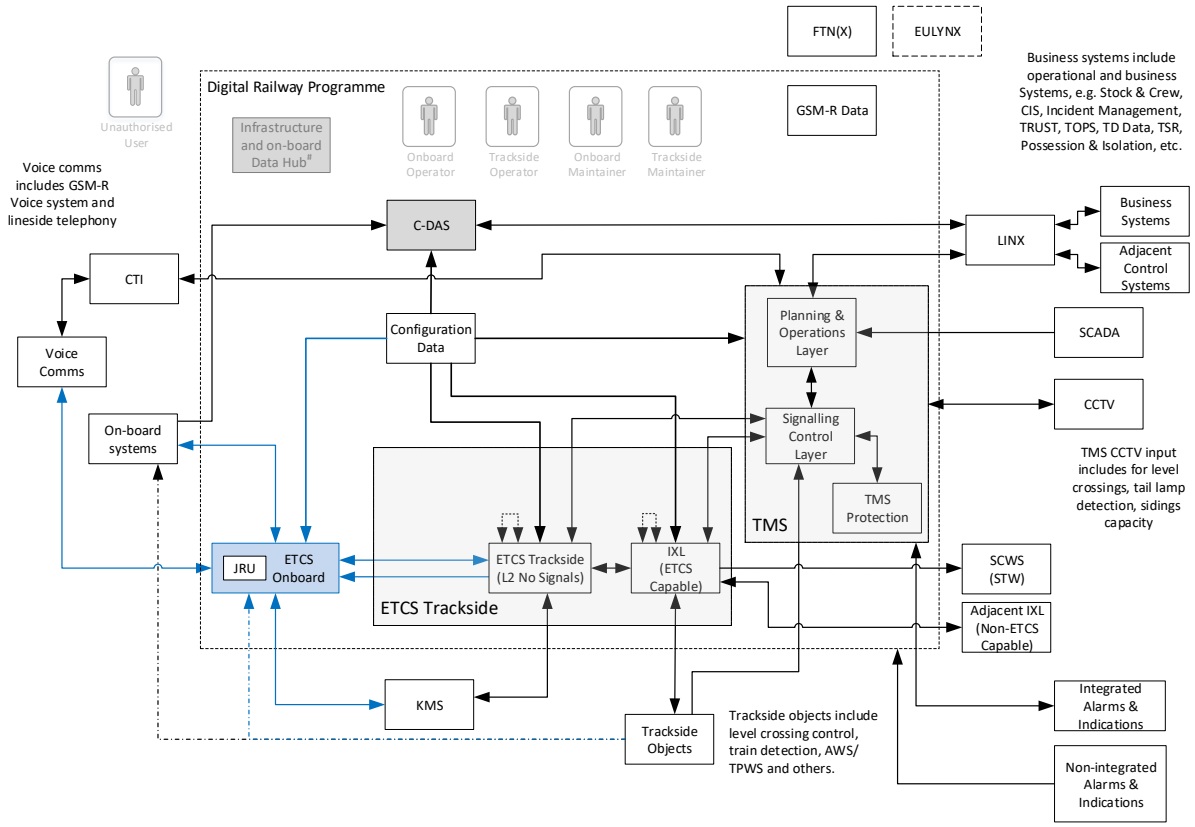

Figure 1. ETCS SoS Architecture / Interfaces - OB Highlighted

The ETCS Onboard comprises hardware and software elements. Hardware elements are installed partly inside the rail vehicle (e.g. European Vital Computer (EVC), Driver Machine Interface (DMI)), and partly on the exterior of the vehicle (e.g. radars, Euro-antennae, GSM-R data antennae, and balise reader).

The ETCS Onboard reference architecture is defined in more detail in Subset-026 v3.6.0, Chapter 2 and it is not repeated here.

2.1 ETCS Mission and Objectives

2.1.1. Business Change Consideration for ETCS

Underpinning ETCS introduction is the need to improve safety and capacity levels and to enhance the performance and reliability of Great Britain's rail network. Aging or obsolete signalling assets need to be replaced by more robust and standardised digital systems. Standardised products and interfaces will support long-term compatibility between products supplied by different suppliers and should reduce costs.

The purpose of the ETCS is to provide signalling information, to the extent advised to the ETCS, which will allow the driver to drive the train safely and to enforce respect of this information. ETCS enables train supervision using cab signalling and provides automatic train protection. ETCS requires a radio system (e.g. GSM-R/GPRS) for signalling data transmission from the ETCS Trackside to the ETCS Onboard. The ETCS Onboard is then capable of transmitting its position and responding appropriately to ETCS Trackside orders. The ETCS will be designed to enable any compliant and compatible train to operate on any compliant and compatible infrastructure by controlling the risks associated with a train travelling too far (i.e. exceeding its Movement Authority) or too fast. The extent to which the ETCS can fulfil aspects of this objective is dependent upon the ETCS Level of application deployed and/or the Mode selected. The ETCS will be designed to cope with degraded modes of operation which may require alternative methods of communication between driver and signaller, such as authority to move based on other visual, verbal and/or written orders.

The introduction of ETCS will necessitate a review of existing safety and operational rules. Staff involved in the management, operation and maintenance of the signalling assets will require training.

With ETCS implementation the number and complexity of signalling assets installed in 'the four foot' will be reduced by the introduction of Eurobalises, which are passive components activated only by the passage of an ETCS-fitted train. The safety risk for staff will be reduced due to fewer active lineside assets (e.g. signals and associated TPWS and AWS), resulting in a reduction in the amount of onsite maintenance activity. Radio Block Centres (part of the ETCS Trackside) will be installed in equipment rooms and connected to existing telecoms and GSM-R systems. GPRS will also be used for transmitting data using packet switching, rather than just using GSM-R for circuit switched calls. This enables functions, such as the transmission of cryptographic keys to RBCs and the ETCS Onboard securing data transmission between them.

2.1.2. Business Benefits of ETCS

The objectives of the ETCS as a Class A system compared to the existing Class B systems (e.g. AWS/TPWS) are to:

- improve safety of the rail system;
- improve reliability and availability;
- improve capacity;
- improve maintainability;
- simplify railway operations;
- improve train driveability;
- reduce the impact of signalling systems on the environment; and
- reduce the life cycle cost of signalling assets (e.g. signals will be decommissioned with their cables and only ETCS markers will be in place to support degraded modes of operation).

The ETCS will replace AWS and existing Class B systems by introducing a harmonised and standardised signalling system. Existing UK Class B systems are: Great Western (GW) ATP, RETB, TPWS, Transmission Voie-Machine (TVM) 430, Chiltern-ATP, Mechanical Trainstops, and Contrôle de Vitesse par Balises (KVB). (Class B systems are those identified within [RD2] as having been notified by member states to provide national train protection).

2.1.3. Business Change Consideration

The introduction of ETCS (both trackside and onboard) will affect several business processes and all staff engaged in the operation and management of trains.

Other processes affected include:

- Definition of signalling projects
- Design of signalling systems
- Installation of equipment (Onboard and Trackside)
- Testing, commissioning and authorisation of systems
- Maintenance and repair of systems
- Management of compatibility and versions
- Renewal and disposal of systems

Personnel affected include:

- Signallers
- Drivers / shunters
- Train managers / guards
- Station dispatch staff
- Onboard maintenance staff
- Trackside maintenance staff
- Accident / Incident investigators
- Operational managers
- Service and timetable planners

3. System Functions and Elements

3.1 ETCS Onboard Functionality Overview

The clear majority of the GB rail network is configured as 'Multi Aspect Signalling '(MAS) utilising lineside signals and legacy track-based train protection systems (Class B). Under the SoS SDD [RD1], the rollout of ETCS for the GB rail network will be Level 2 with no lineside signals. It will need to be ensured that fitment of ETCS systems on board trains (both old and new) does not hinder safe passage of the train.

The CCS TSI lays down ETCS Onboard functionality and interface requirements. The prime ETCS Onboard functionality will be to supervise the train movement safely, in accordance with any received input and data. The Onboard will provide status information to the driver which will, depending on operating mode, alert the driver to potential automatic interactions. When required, the Onboard will automatically intervene, ultimately resulting in the train being braked to a halt if the train travels faster than the most restrictive speed received /calculated by the Onboard. Where able, the Onboard will report its calculated position to the Radio Block Centre.

The ETCS Onboard can support Levels 0, 1, 2 and 3. It can also operate in Level NTC (L-NTC). No Trackside Level 1 configurations are anticipated for the GB application.

Standard ETCS Onboard modes are Full Supervision (FS), Isolation (IS), Limited Supervision (LS), Non Leading (NL), No Power (NP), On Sight (OS), Passive Shunting (PS), Post Trip (PT), Reversing (RV), Standby (SB), System Failure (SF), Shunting (SH), Sleeping (SL), National System (SN), Staff Responsible (SR), Trip (TR), and Unfitted (UN). Use of Limited Supervision and Reversing modes on GB's rail network is not envisaged.

The principle ETCS Onboard functions are to:

- energise balises and receive information from them.
- send train position relative to the detected balises (and confidence level) to the Radio Block Centre.
- request and receive a Movement Authority. Track data, messages, requests and confirmation via the GSM-R data radio.
- select the most restrictive value of the different speeds permitted at each coming location.
- calculate a dynamic speed profile, taking into account the train running / braking characteristics which are known to the Onboard, the track description data, and any section validity timing parameters received.
- compare the train speed with the permitted speed and command a brake application if necessary.
- provide cab signalling and system information to the driver.
- protect the train from undesirable movements.
- command brake application
- manage optional functions, e.g. issuing of commands to lower pantograph, open / close the passenger doors, etc. (if applicable).

Figure 2 provides a detailed diagram of the ETCS architecture and interfaces with the grey area defining the boundary of the OB ETCS system. Further detail on the interfaces can be found in section 6.

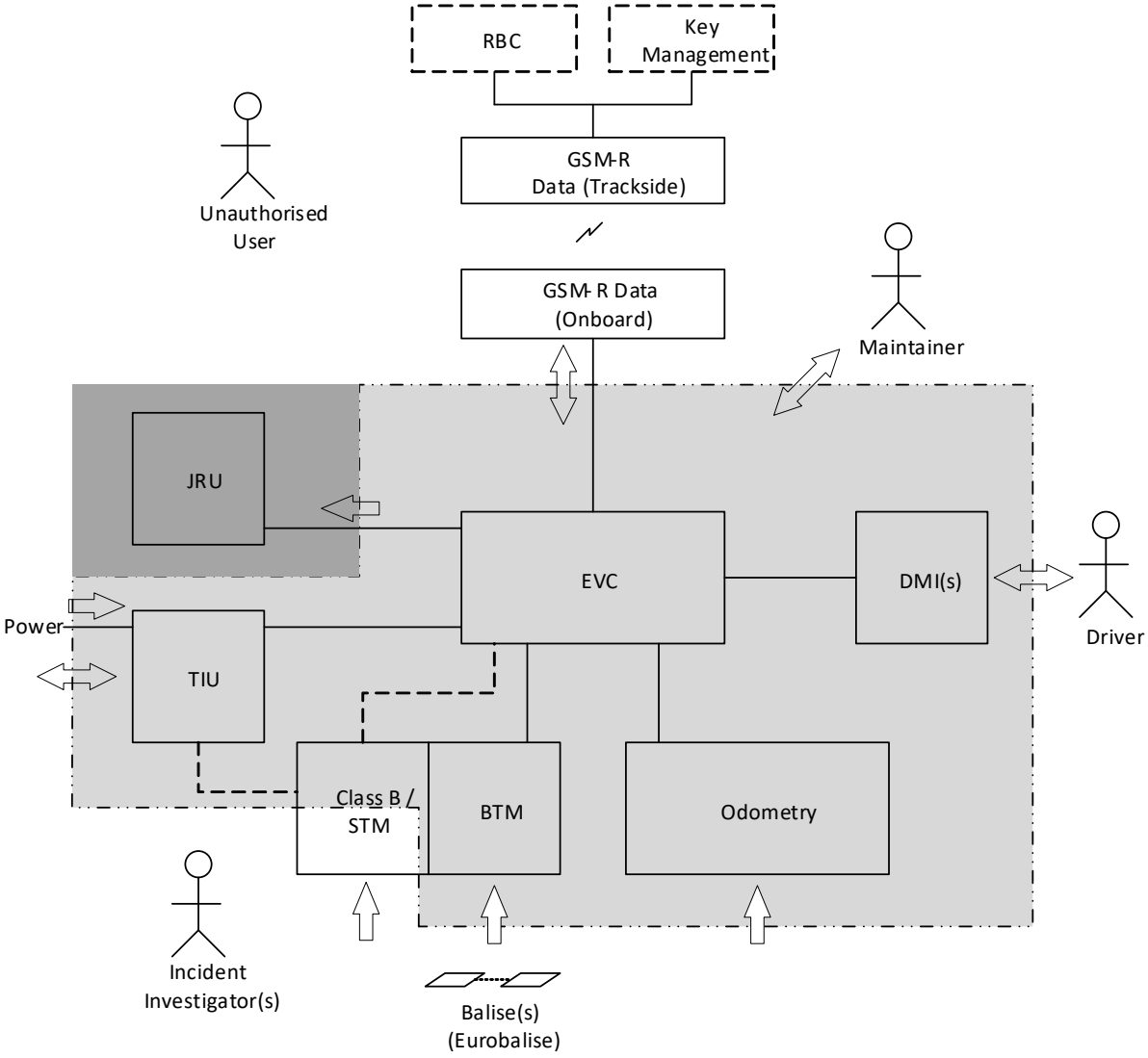

Figure 2. ETCS Onboard Architecture / Interfaces

The Onboard architecture diagram, interfaces and associated tables within this SDD provide an overview of the interfaces to/from the Onboard ETCS plus provide more detail on functionality. These functions will be implemented in accordance with Subset-026, Subset-040 and Subset-091 plus onboard and trackside GB generic constraints (called Digital Rail Requirements). The interface to the JRU is defined by Subset-027 and the CCS TSI details the requirement as the “Interface to Data Recording for Regulatory Purposes”. GMRT2472 [RD33] details the GB requirements for data recorders.

Test and validation requirements are specified in the CCS TSI [RD2] and, more specifically, for the validation of the Onboard application, in Subset-094 and Subset-076. The Interoperability Testing Subsets 110, 111 and 112 will be required for additional testing for compatibility purposes, as required by the GB Testing Framework [RD23].

ETCS equipment identities will be managed in accordance with point 4.2.9 (ETCS-ID Management) in the CCS TSI. For ETCS ID Management, Subsets 026 and 054, and the ‘Assignment of values to ETCS variables’ document [RD20] published on the ERA website will be needed, together with appropriate forms to be completed when submitting new ETCS variables to be coordinated by the ERA.

The GB ETCS application is supported by engineering and operational rules originally identified in the GB ETCS Reference Design. These are included within the Customer Requirements Specification for Operations & Maintenance [RD34], European Operational Rules [RD14], GB Rule Book (GERT8000) and Management of Packet 44 [RD30].

3.1.1. Normal operation

Normal mainline operation (as compared to depots and private lines) for the GB rail application is either operating on a line configured with Class B system (as per the historic norm) or operating on a line configured for ETCS operation / protection. When an ETCS equipped train operates on a line solely equipped with Class B protection systems it operates in Level NTC. (More detail on Levels is provided in section 3.2 but L-NTC (for the GB application) is predominantly the train is operated with pre-ETCS technology aka the sunflower (either on the DMI or standalone), drivers interface with TPWS and speed in mph presented to the driver). The remainder of this section considers normal operation for an ETCS equipped train in start-up and when operating on an ETCS equipped line.

The ETCS Onboard provides cab signalling and train protection in accordance with the data received from the ETCS Trackside configuration. For the GB application trackside application this is Level 2 no signals, enabling train operations in a Digital Railway SoS within the railway system (i.e. SoS, infrastructure, contact systems, etc.). The ETCS Trackside will facilitate a Movement Authority and Track Description (i.e. Speed and Gradient Profiles) to allow the onboard to supervise the train safely in Level 2 Full Supervision (FS) mode. There are other modes of supervision that will support normal operation, including (this is a non-exhaustive list):

- On Sight (OS) – this will support permissive moves, and train joining or splitting
- Non-Leading (NL) – this will support banking movement where a non-leading train provides traction to the whole consist
- Shunting (SH) – in designated shunting areas with trackside protection; this will support train formation, manoeuvres, possessions

An ETCS-fitted train will be able to:

- start in Level 2 and NTC areas;
- move in Level 2 and NTC areas, ideally in FS or OS;
- Execute a Level transition, between Level 2 and NTC areas (in either direction); and
- Communicate with the trackside RBC, including when moving from the control of one RBC to another (RBC-RBC handover within a Level 2 area).

The ETCS start-up process is very similar regardless of initial operating mode with the driver being typically prompted to enter / validate train data and depress "start" on the DM

The Radio Block Centre is the main sub-system sending ETCS Trackside orders to the ETCS Onboard via the GSM-R/GPRS network. ETCS data communication is secured by shared secret authentication keys which are distributed via GPRS to the ETCS entities (i.e. KMAC entities). Normal operation is possible if the correct KMAC keys have previously been installed or updated during the Start of Mission for the ETCS Onboard.

Further details about the type of ETCS procedures are in the CCS TSI, more specifically, Subset-026 and the GB ETCS Reference Design, which gives the operational and engineering context of the ETCS to be deployed on GB's rail network.

3.1.2. Degraded mode operation

The ETCS will be considered to be operating under degraded operating conditions when the designed / intended behaviour cannot be fulfilled by the ETCS Onboard. There are many Trackside and Onboard issues which would result in either the system being unable to supervise the ETCS-fitted train as intended or the driver having to stop the train due to an error leading to a train failure. A failure may also occur during the starting procedure. Further information can be found in European Operational Rules [RD14] and National Technical Rules published on the RSSB website and listed on the ERA website. Running the train in Full Supervision or in On Sight modes is not considered part of degraded operation.

Scenarios in which ETCS degraded operation could occur are given below. (This is not an exclusive list):

- Failure during Start of Mission;
- Authorisation to start in Staff Responsible is required due to loss of valid train position or the Route cannot be set for the train;
- Train is in System Failure (during a mission) due to a failure affecting safety (e.g. Balise Transmission Module is broken);
- Train is tripped (i.e. Trip leads to Emergency Brake application) after passing a Level Transition border or an End of Authority (EOA);
- Breakdown in radio communication, meaning that the Onboard cannot receive or send data from/to the ETCS Trackside (i.e. specifically to the Radio Block Centre).

ETCS also supports degraded railway operations when failures / scenarios external to ETCS occur. For example, when a train has failed such that it cannot move under its own propulsion and is recovered by a following train with working ETCS having to couple and push the failed train to a different location.

3.1.3. Emergency mode operation

The ETCS includes functions enabling users to stop the train movement in case of emergency. Once the signaller has identified the need to stop an ETCS-fitted train in an emergency, the RBC will be able to send an Emergency Stop message to the ETCS Onboard, leading to application of the emergency brake. Further information can be found in European Operational Rules [RD14] and National Technical Rules published on the RSSB website and listed on the ERA website.

Scenario examples when ETCS emergency operations are required are detailed below:

- Train receives an Unconditional Emergency Stop message due to an incident ahead and thus is tripped immediately with emergency brake triggered.
- The ETCS Onboard has failed, the Driver has isolated it (i.e. it is in IS mode), and the train has to be rescued by an assisting train.

3.2 The deployed system

The ETCS Onboard is a system deployed within the SoS. It needs to be integrated into the rail vehicle to form a complete system running on the rail network. The ETCS Onboard requires orders from the ETCS Trackside and a means of determining the train position along the track. Its configuration can be seen in Figure 2

The ETCS Onboard comprises the following elements:

- European Vital Computer (EVC);
- ETCS Data Only Radio (EDOR);
- Train Interface Unit (TIU);
- Data recording device for juridical and monitoring purposes (the JRU is not formally defined by the Subset, but the interface is);
- Odometry;
- BTM and Antenna;
- DMI

Within the SoS architecture, the following interfaces for the ETCS Onboard have been identified:

- ETCS Trackside;
- Key Management System (KMS)
- Trackside systems
- On-board systems
- Voice comms

and the following are the key enablers:

- GSM-R and GPRS
- Users (e.g. Train Driver, ETCS Onboard operator, Onboard maintainer, etc.)

The ETCS Trackside is described in the ETCS Trackside System Definition Document [RD28] and the System of Systems Architecture [RD27] and, therefore, its description is not repeated here.

The basic ETCS (operating) Levels are as follows:

- Level 1 involves continuous supervision of train movement with non-continuous communication between train and trackside (by means of Eurobalises in GB). Lineside signals are necessary and train detection is performed by trackside equipment, which is outside the scope of the ETCS. The Digital Rail Project remit is for a Level 2 solution with no signals.
- Level 2 involves continuous supervision of train movement with continuous communication (provided by GSM-R/GPRS) between both the train and the Radio Block Centre, which is part of the ETCS Trackside. Lineside signals are optional in this case, and train detection is performed by trackside equipment, which is outside the scope of the ETCS. The retention or provision of lineside signals is outside the scope of this document, although it may be required as an implementation phase for projects. ETCS Level 2 no signals is the version envisaged for operation in a DR SoS area.
- Level 3 is also a signalling system that provides continuous train supervision with continuous communication between train and trackside. The main difference between Level 3 and Level 2 is that, in Level 3, the train location and integrity is managed within the scope of the ETCS, i.e. there is no need for lineside signals or train detection systems at the trackside, only Eurobalises. Train integrity is monitored on board to ensure that the train remains complete and has not split accidentally. This document does not preclude the introduction of Level 3, but it is not part of the core system.

In addition, two more levels are defined:

- Level 0 is intended for trains equipped with ETCS running along non-equipped lines and within the scope of this document it will be used for engineering areas/possessions; Level 0 is likely to be used in degraded modes.
- Level NTC is intended for ETCS-equipped trains running on lines where the Class B system needs to be operated. There can be multiple NTC levels with the labels 'NTC A', 'NTC B', ... replaced by the distinct abbreviations of the concerned National Systems. For the GB onboard application as units are constrained to the GB network only a single NTC level is anticipated. For Level NTC, the ETCS could act as an interface between the driver and the UK Class B system (aka Specific Transmission Module (STM)) or the onboard class B system could be configured as a separate on-board system with which the ETCS interfaces vie the TIU. The provision of a system to enable ETCS-fitted trains to operate on lines fitted with the Automatic Warning System (AWS) and Train Protection and Warning System (TPWS) is within the scope of this document. ETCS Onboards operating in Level NTC or NS require the DMI to display speed in mph. In all other modes the DMI will display it in km/h.

NB Level 3 falls outside scope of SoS specific applications.

Unlike the ETCS levels, which are associated with train-trackside communication, ETCS modes can be considered to be alternative train and/or trackside configurations which are used for managing different operating situations (e.g. Full Supervision (FS), Shunting (SH), Standby (SB), Non-Leading (NL)). The main ETCS mode is Full Supervision (FS). The ETCS Onboard will be in Full Supervision mode when a Movement Authority is available, and all train data (e.g. train length, brake percentage) and track data (e.g. Static Speed Profile, Gradient Profile) which is required for complete supervision of the train is also available on board. In FS, the ETCS Onboard is responsible for train speed supervision and protection (e.g. ensuring movement does not exceed the End of Authority (EOA)).

Full Supervision mode is based on the train holding a Movement Authority, which is also the case for On Sight (OS) mode, the difference being that, with the latter, the speed of the train is limited by the corresponding National Value or the OS Mode Profile data and the driver is responsible for confirming that the track is free of any obstructions.

Other modes are available for different operational situations:

- Shunting (SH) will be used for train formation in a train depot or Possession area.
- Staff Responsible (SR) could be used to pass an End of Authority using the Override procedure, or when the train position information is unknown to the ETCS.

The ERTMS Concept of Operations (ConOps) [RD13] provides more details about the modes and their use in meeting GB Railway operational needs.

3.3 Enabling systems

These are systems that are deemed to be outside of the ETCS Onboard and which are critical dependencies to the operation of the ETCS Onboard. For more details on the systems, see Section 4.3.

- ETCS Trackside;
- On-board Systems
- GSM-R or GPRS Data Radio (for online Key Management);
- Configuration Data
- Key Management System

4. System boundary

4.1 Geographic boundary

As this is a System Definition for a generic System with no specific application in mind, there is no geographical boundary that can be discussed in this section. Railway project geographical boundaries are typically mileage markers and chainages that define the boundary of the lineside project or routes the train will operate on. Alternatively, system boundaries could be used by deployment projects such as the class of vehicles that the ETCS onboard is being fitted too. These will be considered in the System Definition documents for specific DR deployment schemes as and when they occur.

4.2 Train Configuration

The fitment of ETCS Onboards is not dictated by standard and can be applied in a variety of configurations.

As show in Figure 3 a train can be one or more railway vehicles hauled by one or more traction units, or one traction unit travelling alone all running under a given operational number from an initial fixed point to a terminal fixed point. The engine (aka a traction unit) is an association of one or two driving cab(s) of a Rolling Stock unit with one single ERTMS/ETCS on-board equipment i.e. it can be a single cab or dual cab fitment (with a DMI in each cab).

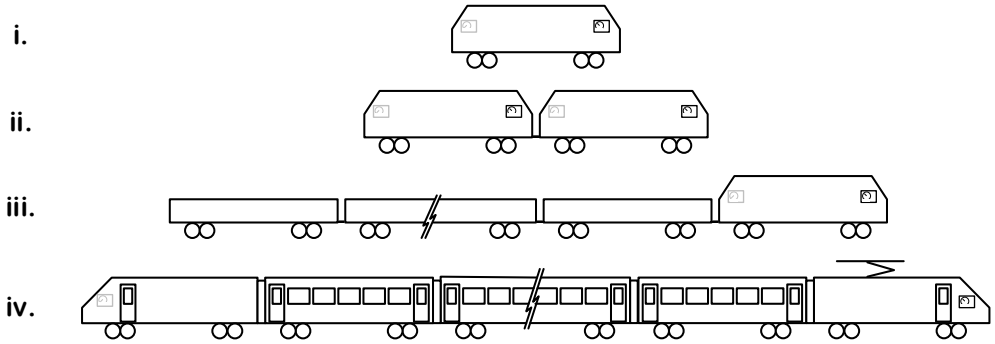

Figure 3. Examples of 'train' configurations.

The application of onboard ETCS is the responsibility of the deployment projects but can be deployed as two single cabs or a dual cab fitment (single ETCS with two cabs/DMI's). The interface with the train ensures that no more than one ETCS on-board system is "in control" (for the train).

4.3 Interfacing Systems

These are systems that are deemed to be outside of the ETCS Onboard System. In some cases, the DR System Requirements and Integration (SR&I) team will be specifying interface requirements for these projects to ensure that they will integrate with the ETCS Onboard. More details on the interfaces, such as subset information, can be found in Section 5 and 6. The Interface Requirements Specification also details [RD29].

- People
- ETCS Trackside;
- Onboard Systems
- GSM-R or GPRS Data Radio Network;

- Voice Comms
- Trackside Objects
- Key Management System

5. Physical interfaces

When deployed in the railway environment, the ETCS Onboard will also interface to other physical systems, as shown in Figure 2 and, where necessary, described in terms of their functionality in Section 6. The functional interfaces are via the defined physical or interoperable air gap interfaces.

The formal ERTMS/ETCS Reference Architecture is described in Subset-026 Chapter 2. It details physical interfaces, including interoperable ones requiring compliance with the CCS TSI. A brief description of the ETCS Onboard physical interfaces is provided in the following sections.

This section will set out the physical interfaces and any protocols used on an interface. Final physical interfaces are defined by the deployment project / supplier / integrator.

5.1 Trackside

5.1.1. ETCS Trackside

The ETCS Onboard will be able to communicate with the ETCS Trackside via the EuroRadio protocol defined in the CCS TSI and, more specifically, in Subset-037 and Subset-098. The ETCS Onboard will be able to read the Eurobalises using the Eurobalise airgap protocol defined in the CCS TSI and, more specifically, in Subset-036.

5.1.2. Non ETCS Trackside

The ETCS Onboard manages, where required, the suppression of any on-board AWS and TPWS systems. Also, Packet 44 is a defined means of transmitting data for national applications (other than ETCS) between train and track and vice versa. For GB applications, where the value of the parameter NID_XUSER = 9, indicating that RSSB is the identity of the user system, the management of Packet 44 is defined by [RD30]. The ETCS Onboard has no other interfaces to non- ETCS trackside systems.

5.2 Rolling Stock

5.2.1. Overview

The prime consideration when integrating the ETCS Onboard will be whether it is being applied as a retrofit or to new rolling stock:

- Retrofit trains typically have lower-level ETCS detailed requirements (i.e. EOSS) which are published on the RSSB website.
- ETCS detailed requirements for new trains (i.e. ENTOSS) are also published on the RSSB website.

Integration of the ETCS Onboard will require compliance with some Rolling Stock characteristics, such as environmental conditions, EMC, etc. For new trains, Rolling Stock will need to comply with the Locomotives and Passenger rolling stock Technical Specification for Interoperability (LOCPAS TSI) [RD26] which includes some GB-Specific Cases (e.g. GB Loading Gauge). Successful ETCS Onboard integration will depend on the application of best practice, such as adherence to international standards requiring the harmonisation of interfaces between the ETCS Onboard and rail vehicles.

It should be noted that both non-TSI compliant and TSI-compliant vehicles will be fitted. This encompasses Passenger trains, Freight trains and On Track Machines.

Depending on the rail vehicle configuration, the ETCS Onboard could be connected to the rail vehicle and the Train Communication Management System (TCMS) via a Train Communication Network. Examples of protocols usually used in the vehicle to interface with the ETCS Onboard and other on-board systems in the vehicle are listed below:

- PROFIBUS (Process Field Bus) – this is a standard for fieldbus communication in automation technology
- Ethernet
- Multifunction Vehicle Bus (MVB)
- Controller Area Network (CAN)

The ETCS Onboard will be able to send commands to the rail vehicle (e.g. Emergency Brake command) and receive the status of train interfaces (e.g. Active leading cab, Traction status). It will interface with Class B systems, either bespoke via the Train Interface Unit or Specific Transmission Module Form Fit Functional Interface Specification (STM FFFIS), enabling level transitions to take place between Level 2 and Level NTC areas. Depending on the rail vehicle, configuration, and the supplier of onboard ETCS equipment the onboard Class B interface will either be via the TIU or managed by a STM.

The ETCS Onboard includes physical interfaces / functions that can trigger other on-board systems to manage a specific rolling stock function, for example, Automatic Selective Door Operation (ASDO). The ETCS Onboard could transfer orders to enable doors on one side of the train via the Train Interface. However, the ETCS Onboard will never be responsible for managing the doors as they are part of the rail vehicle. The deployment projects will define what 'Control of Train Functions' outputs are required to be configured for each class of rail vehicle.

5.2.2. Power Supply

The systems that make up the DR system are expected to interface to the existing diverse and secure power supplies which are provided within most rolling stock. Appropriate survey activities will need to be undertaken to determine available spare capacity and changes to support deployment, as necessary.

5.3 Telecommunications

5.3.1. Data Radio Network;

The NR GSM-R data radio network will be utilised to exchange data between ETCS lineside systems and ETCS on-board equipment during operation and maintenance. The availability (reliability and coverage) of the GSM-R data radio network will be based on the operational requirements introduced by the deployment for ETCS on GB rail infrastructure.

The system will support the use of packet switching in those areas where online key management is required.

The ETCS requires sufficient radio coverage and capacity and compliance to the CCS TSI (i.e. set of specifications #3).

5.3.2. Voice Comms (i.e. GSM-R Voice)

The ETCS Onboard will have an interface to the Operational communications systems so that, within the DR System, a subset of the Human Machine Interface (HMI) functions can be provided to the operator for convenience.

It is envisaged that an interface from the DMI part of the ETCS Onboard to the GSM-R voice cab radio will share the Train Running Number between the on-board systems to avoid the driver having to enter the data twice or more during a Start of Mission or following a Joining or Splitting operation leading to train configuration change.

NB: The UK introduced a National Technical Rule (NTR) to enable the use of alphanumeric Train Running Numbers if needed by the users. It also details considerations on the interface [RD31].

5.4 Key Management System

Key Management, the principle of 'secret' keys to support / ensure safe communication over open networks can be managed manually but for the national GB application would be impracticable. Online key management which allows remote management requires the radio network to support packet switching i.e. GPRS.

The ETCS Onboard will request authentication keys over the EuroRadio airgap (i.e. GSM-R/GPRS), in accordance with online Key Management principles outlined in the CCS TSI and Subset-137. The ETCS Onboard will be capable of storing correct authentication keys transmitted by the Home Key Management Centre.

5.5 Configuration Data System

The ETCS Onboard requires certain data sets which need to be managed by a process controlled by others, such as the TOC Safety Management System.

Data managed by the train operator is:

- Train category
- Train length
- Traction / brake parameters
    - Traction model
    - Braking models or brake percentage
    - Brake position
    - On-board correction factors
    - Nominal rotating mass
- Maximum train speed
- Loading gauge
- Axle load category
- Train fitted with airtight system
- Radio Network ID
- RBC-ID/Phone number (if any) / EIRENE short code

Data which is required by the ETCS Onboard but cannot be amended by the train operator is:

- Traction system(s) accepted by the engine
- List of National Systems on board
- Axle number
- NID_ENGINE – The ETCS Onboard Identity
- Home KMC Identity

It is essential that the configuration data be prepared and configured within the system in a controlled manner.

6. FUNCTIONAL INTERFACES

Digital Railway technology interfaces to the high-level functional systems, as described in the DR SoS System Definition [RD1].

These interfaces will be implemented taking due cognisance of the required service level, presentation, capacity, quality of service, availability, integrity, security, etc. appropriate to each one. Some interfaces may also entail some provision for confidentiality where commercially sensitive data is being exchanged between systems.

The ETCS Onboard will interact with users and the following systems as shown in Figure 2 and listed below.

- ETCS Trackside
- Key Management System
- Onboard Systems
- Trackside Objects

The interfaces are described in terms of their functionality in the following sub-sections.

6.1 People

Discussion of staff within this document is limited to only those personnel that will interact directly with the ETCS Onboard. Thus, users of supporting operational information systems, such as the Integrated Train Planning System (ITPS), Total Operations Processing System (TOPS), Train Running Under System TOPS (TRUST), etc. are excluded.

6.1.1. Operational & Maintenance Staff

Operational staff are defined as any individuals who are authorised, competent and responsible for the movement of trains who interfaces with the DR System as part of their duties, e.g. signaller. This includes staff that contribute to the safe movement of trains through their role, e.g. TOC platform staff undertaking train dispatch duties. In the context of the ETCS Onboard, the interface is the driver.

Maintenance staff are defined as individuals who are responsible for undertaking engineering activities on railway infrastructure and vehicles. This includes those who work on or about the line and, thus, who may require protection arrangements to be made by the DR System to ensure that they can conduct their work with appropriate safety measures in place.

For the purposes of the ETCS Onboard, the two groups defined above sit within the system boundary and, therefore, appropriate Operational Readiness activities for drivers and the Onboard maintainer will have to take place to enable the successful deployment and operation of the ETCS Onboard. The Operational Readiness activities should also generate appropriate supporting procedures to allow these personnel to interface to, manage and interpret the System in a safe and efficient manner.

6.1.1.1. DMI / Train Operator Interface

The DMI provides cab signalling information to the driver and status messages from the RBC as summarised in Table 1. It also provides the driver input interfaces to the EVC.

Table 1:DMI/Train Operator Interface

Type	Description	Functionality
Input	Driver Selection	The driver can make mode requests, request a starting Movement Authority, check status, and configure reminders / set ability to ignore specific balises. Driver requests/input includes: Start, Override, ERTMS Level, Isolation, Acknowledgement, Continue Shunting, Adhesion, Virtual Balise Covers, and/or System Version.
	Driver options	The driver can adjust the visual and audio interface from the DMI. The driver can select: Luminance Adjust, Loudspeaker Adjust, Toggle Speed/Distance Information, and/or Zoom function.
	Data Entry	The driver can enter and/ or confirm train parameters. These parameters are: Train Running Number, Driver ID, Radio Network ID, RBC Data, Language, Track Clear, SR Speed/Distance, Train Category, Length, Traction / Brake Parameters, Maximum Train Speed, Loading Gauge, Axle Load, and/or Airtight system.
Output	Audible & Visual	The DMI provides an audible & visual alert when commanded to for Feedback and Warning alerts to the driver.
	Signalling Status:	The DMI provides cab-signalling status to the driver as calculated on board. Status can be: Normal, Overspeed, Warning, Intervention, Brake command, Target Speed Monitoring, and/or Release Speed Monitoring.

Type	Description	Functionality
Output	System Status[1] [2]	The DMI provides the following status messages to the driver (when on-board conditions require it): Balise read error, Trackside malfunction, System status message, Communication error, Entering FS, Entering OS, Runaway movement, SH refused, SH request failed, Trackside not compatible, Train data changed, Train is rejected, Unauthorized passing of EOA / LoA, No MA received at level transition, SR distance exceeded, SH stop order, SR stop order, Emergency stop, No track description, Route unsuitable – loading gauge, Route unsuitable – traction system, Route unsuitable –axle load category, Radio network registration failed
	Information	The DMI provides cab-signalling information to the driver as calculated on board, or as requested from the RBC (via the EVC). Presented information can be: Current train speed, Current ERTMS Mode, ERTMS Level Announcement, Planning (Area), Permitted Speed, Distance to Target, Target Speed, Release Speed, Text Messages, 'Lowest Supervised Speed within the Movement Authority' (LSSMA), Time to Indication (TTI), Track Ahead Free information, Slippery Rail, Level Crossing 'not protected', Gradient Profile, Speed Profile discontinuity, Safe Radio Connection, Reversing permitted, Local time, and/or Geographical Position
	Information: Track Conditions	The following statuses and/or commands can typically be announced/ordered and/or indicated as received via the EVC from the RBC: Air conditioning intake, Pantograph (Raise / Lower), Neutral Section, Non-Stopping area, Radio hole, Magnetic Shoe Brake, Eddy Current Brake, Regenerative Brake, Traction System(s), Sound horn and/or Tunnel Stopping Area

[1] As the UK will not authorise Reverse Mode, it is not expected that 'RV distance exceeded' will ever be displayed.

[2] The following message could be displayed if the UK Class B systems are delivered by an STM. The messages would be: [name of NTC] is not available, [name of NTC] needs data, [name of NTC] failed, [name of NTC] brake demand.

6.1.2. ETCS Onboard Maintainer

No specific functional requirements are detailed for the maintainer. Each Onboard system is bespoke to the supplier and it is the supplier's responsibility to ensure that the supplied interface fulfils the generic maintainer requirements. Where required the ETCS Onboard maintainer will update wheel diameter as a function of the odometry after reprofiling on the wheel lathe.

6.1.3. Installation staff

The correct positioning of ETCS Onboard equipment is vital to the efficient and safe operation of the system.

It is essential that installation staff understand the criticality of positioning equipment precisely (e.g. balise reader) and confirming that the correct units are installed.

6.1.4. Testing and authorisation personnel

it is absolutely essential that the ETCS Onboard be tested as individual components, as an integrated system, in conjunction with adjacent systems, and with the ETCS Trackside via the GSM-R network and balises.

The majority of testing will be undertaken in a laboratory environment and the risks of using simulated products, particularly at boundaries and interfaces, need to be understood.

It is a requirement that the ETCS Onboard be authorised in accordance with [RD2] and that it should have demonstrated that it meets the user needs and satisfies the conditions for interoperability.

6.1.5. Accident / Incident Investigators

Formal investigations into serious railway safety incidents are carried out by the Rail Accident Investigation Branch (RAIB). Examples of such incidents include: train overspeed, exceedance of Movement Authority, derailment, collision, and passenger / workforce fatality. Evidence for an investigation will include voice or data logs from the DR System, which will be stored in a tamper-proof memory. More specifically, the Juridical Recording device (whose interface is detailed in CCS TSI, Subset-027) will record all juridical data related to ETCS operation. Investigators will need access to the recorded juridical data.

Others involved in Incident Investigations include (but are not limited to): British Transport Police, the Centre for Protection of National Infrastructure, Office of Rail and Road (ORR) and the Health and Safety Executive, all of whom require access to infrastructure and control system data records in the event of an incident. Although they sit outside the boundary of the System, provision will need to be made to share data openly and efficiently across the industry for incident investigation.

6.1.6. Remote Users, TOCs & FOCs

The ETCS Onboard may also be required to supply information-only displays to other remote users at various locations. Remote access will require cooperation and interface agreement with the Asset Manager owning or managing the rail vehicle into which the ETCS Onboard is integrated. There is no interface for authorised remote users, i.e. no such interface exists, but

there is an established requirement that unauthorised users be prevented from accessing the system.

6.1.7. Non-authorised User

The person(s) is/are recognised in that all interfaces are required to ensure that non-authorised users or systems are unable to access the system.

6.2 ETCS Trackside

6.2.1. RBC Interface

The ETCS Trackside interface provides the continuous communication path (as against intermittent communication when passing over balises) for commands, status and updates between the two systems as summarised in Table 2.

Table 2: RBC Interface

Type	Description	Functionality
Input	Movement Authority	The RBC details information that allows the on-board EVC to permit the movement of the train within the (calculated envelope) without intervention.
	Emergency Messages	The RBC transmits information that requires the EVC to shorten the LoA and / or 'trip' the train to a halt
	Requests and Confirmations	The RBC transmits information that requires the driver to acknowledge the message. The RBC also confirms acceptance of certain requests from the EVC.
	Static Speed Restrictions and Gradients	The RBC transmits information about permitted speed profiles to the EVC; the EVC can then take the most restrictive, depending on the train states.
	Track Conditions and Route Suitability	The RBC transmits information about track conditions for either consideration and action by the EVC, or for the display of respective status to the driver.
	Mode profile	The RBC transmits commands as to the mode in which the train should be operating.
	Level Crossings	The RBC transits information to the EVC on the status of upcoming level crossings.

Type	Description	Functionality
Input	RBC Version	The RBC transmits to the EVC the operating system version.
	Session Management	The RBC (and the EVC) manage communication sessions between each other, including the request to communicate or terminate the session.
Output	Train Position Report	To a timing parameter detailed via the RBC, the EVC transmits position updates of the position relating to the estimated front and rear of the train.
	Train Data	The EVC provides, on request, data relating to how the train is configured.
	Requests and Acknowledgements	The EVC communicates requests for Movement Authority plus requests and acknowledgements from the driver to the RBC
	Onboard Version	The EVC transmits to the RBC the onboard supported system version.
	Session Management	The EVC (and the RBC) manage communication sessions between each other, including the request to communicate or terminate the session.

6.2.2. Balise

The BTM/Balise provides data to the EVC when the on-board Balise antenna passes over the Balise. In L2 solutions, the message content is typically fixed. In Level 1 solutions, the Balise is connected to the interlocking and Movement Authority is received via the balise. Table 3 provides a summary based on Level 2 functionality.

Table 3: BTM / Balise Interface

Type	Description	Functionality
Input	Virtual Balise Cover Marker	'Cover Marker' indicates to an EVC that the telegram can be ignored according to a VBC status from the driver or and 'order' to remove a VBC status from the driver.
Input	System Version Number	Data advising the ETCS OBU which is the operated system version
	Linking	Provides data on where the next set(s) of Balises (and messages) should be found
	Virtual Balise Cover Order	An instruction to implement / remove a VBC configurations
	Track Condition	Provides information, type and distance on upcoming track conditions. These can be: Change of traction system, Change of allowed current consumption, Big Metal Masses, Track Condition, Track Condition Station Platforms, Track Ahead Free up to Level 2/3 transition location.
	Level Transition Order	An instruction for the EVC to change the operating Level. Instructions can be: Level Transition Order, Conditional Level Transition Order, Danger for Shunting Information, Stop Shunting on Desk opening, and/or Stop if in Staff Responsible.
	Session Management	An instruction to the EVC on how to manage a communication session with the RBC. Commands can be Session Management, Radio Network Registration, and/or RBC Transition Order.
Output	Energise Balise	Provide power to balise to enable it to transmit data.

6.3 Onboard Systems

6.3.1. TIU / Train Interface

The TIU provides the interface between the train and the EVC as summarised in Table 4. Its application/connectivity is specific to each project / train type. Depending on how the interface

to Class B systems is determined by the deployment projects / supplier, the TIU may need to include an interface to manage any Class B on-board systems,

Table 4: TIU / Train Interface

Type	Description	Functionality
Input	Mode Control	Data from the train concerning what state the EVC may operate in. These are namely Sleeping, Passive Shunting and/or Non-leading
	Status	Data from the train confirming the status of on-board systems. This data can be: Brake Pressure, Special Brake, Additional Brake, Cab status, Direction Controller, Traction Status, Set speed and/or National System Isolation
	Train Data	Data detailing the train parameters - Type of, Train Data (optional)
	Power	Power for the ETCS Onboard is supplied by the train.
Output	Brake Control	ETCS-commanded interventions as calculated by the EVC, i.e. Service Brake, Emergency Brake, Special Brake
	Mode Control	Data indicating ETCS Isolated
	Control of Train Functions	EVC data to control specific train functions, i.e. Change of traction system, Pantograph raise / lower, Air tightness, Station platform status, Powerless section, Main Power Switch, Traction Cut Off (TCO), and/or Change of allowed current consumption

6.3.2. TOC / FOC Train Systems.

The Train Operating Companies (TOCs) and Freight Operating Companies (FOCs) staff co-located with Network Rail staff to operate parts of the DR System may have both DR equipment and their own employer's proprietary systems and equipment. For the ETCS Onboard that is expected to be in relation to:

- Juridical data;
- Diagnostic data; and
- On Train Monitoring Recorder (OTMR) data.

Subset-027 details 49 classes of data that should be transmitted to the JRU within five seconds of the occurrence of the event which triggered the message. The list, which is clearly detailed within a single table in Subset-027 is not replicated here. It is envisaged that the Incident Investigator(s) will use the data stored in the JRU as the need arises.

Requirements for diagnostic interfaces and OTMR (above the JRU requirements) are the responsibility of the deployment projects.

6.3.3. Power, Odometry and Other

ETCS Onboard sources its power from the vehicle. Deployment projects will manage the interface to ensure that due consideration is given to power fluctuations, range and interruptions of power to the ETCS Onboard.

Deployment projects will manage the odometry interface from tachometers including who supplies what and the resultant interface

All ETCS Onboard requires physical, electrical and environmental integration with the rail vehicle of both the bespoke components and all connecting cables. Allocation of responsibility for this integration will be determined by the deployment project(s).

6.4 Key Management System

Key Management facilitates communication between Onboard Units (OBUs), lineside RBCs and other related equipment, ensuring that Identification and Authentication Dialogues (I&As) and resultant data streams that use Messenger Authentication Codes (MACs) are secure. This security is based on defined cryptographic techniques using keys which contain secret information only known to the communicating equipment. This interface is recognised here for completeness, but it is not discussed further as its formally part of the UNISIG EuroRadio Specifications.

The Key Management policy needs to be clear and the GB Key Management Domain must be defined as, currently, there are isolated projects using their own offline Key Management Systems that are compatible with older system versions (i.e. Baseline 2 (2.3.0d), Baseline 3 (3.3.0 + specific features) and Baseline 3 Maintenance Release 1 (3.4.0)).

6.5 Trackside Objects

Great Britain's Existing rail network deploys two track-to-train systems of AWS and TPWS. These remind drivers of trackside signalling status and intervene in certain circumstances. In an L2 area these trackside systems are not fitted. The ETCS Onboard manages any associated on-board systems so that they do not interfere with the operation of the train in L2 areas. In areas where ETCS Trackside is not operational, the AWS and TPWS are required to be operational and ETCS must not interfere with their functionality. The method of interfacing with the ETCS Onboard is the responsibility of the deployment project / supplier.

7. SYSTEM ENVIRONMENT

7.1 Procedures and Rules

The majority of DR deployments will take place in existing mature operating environments and will provide new functions, facilities and shared information sources, and Operational procedures will be modified to reflect the new processes, roles and responsibilities.

ETCS deployment will cause changes to the Rule Book and other longstanding practices.

7.2 Staff Competence and Assessment

In line with existing accident investigation recommendations, training will be provided for train staff in the new roles in normal, degraded and emergency modes of operation, with a realistic portrayal of the Area of Control and the traffic (both trains and communications) within it.

It is expected that maintenance staff will need to be trained or retrained to be able to maintain and find faults on any new equipment appropriately and safely, and their competence will require ongoing assessment.

7.3 Security

Appropriate physical and cyber security requirements and arrangements will need to be implemented for the ETCS Onboard. These will be made in the context of the wider NR organisation, Network Rail Telecoms (NRT), and railway industry security and cyber security policies, procedures and provisions.

Cyber security for Network Rail and Digital Railway is overseen by the DfT (Security – Transport (Rail) division) as the Regulator and implemented by the Security Assurance Framework process.

7.4 Maintenance

Deployment of the ETCS Onboard will introduce new maintenance requirements.

The DR system will be provided with suitable maintenance support, both tools and local and remote facilities, to assist maintainers in monitoring, understanding, and repairing the system.

Maintenance work will normally be expected to take place outside operational hours, but this may not always be possible.

7.5 Local Environment and Conditions

ETCS Onboards will be required to comply with environmental conditions specified for their installation location on or within rail vehicles. These conditions will be confirmed through the acceptance / First-in-Class validation of the application to each class of vehicle.

The ETCS Onboard system will need to use the available on-board electrical power supply without affecting the power use of other on-board systems or being affected by the power use of other on-board systems.

The ETCS Driver Machine Interface (DMI) will need to meet human factors and ergonomics considerations when integrated into the driving desk.

The minimum system-specific environmental requirements for the operation of the ETCS Trackside and train-mounted equipment have been specified in [RD17] and [RD18].

7.6 Electromagnetic Compatibility (EMC)

It is reasonable to assume that the EMC environment for the system should be compliant with the latest standard and this assumption will be validated as part of the DR deployment validation activities.

Given the range of age of rolling stock operating on the GB rail network, it is also reasonable to assume that some units will not comply with current EMC standards; additional work may therefore be necessary to ensure that any risks posed to the new on-board equipment caused by lack of compliance are fully mitigated.

Deployment Projects and suppliers will be responsible for the duty of care to assure the appropriate level of electromagnetic integration activities and management of risk.

7.7 Human Factors

For the ETCS Onboard, there is likely to be a significant change to the HMI for operators (e.g. drivers, train preparers) and maintainers. Therefore, ergonomics assessment work will be required to ensure that HF requirements are met. Managed by the Deployment Projects Human Factor Plans will set out the methodology and assurance activities for this assessment work and management of risk.

8. EXISTING SAFETY MEASURES

The CSM RA process will be applied to the system. Therefore, all safety measures and associated requirements will be listed in the Hazards record and associated safety requirements specifications.

Railway Undertakings and Vehicle Owners will be responsible for managing, through their own processes, all necessary changes to their standards, or the introduction of new standards, as a result of fitting any on-board systems. For ETCS Onboard systems guidance, documentation and processes will be provided by the DRP. Again, due to the evolving nature of the DRP, it is anticipated that new Onboard System Requirements or standards will be necessary, or existing ones will need to be revised.

In operational terms, the existing safety measures include the applied maintenance regime, TOC & FOC operating practices, Railway Rule Book, and compliance with Group and Network Rail Standards, all of which will require review, update and implementation as part of the deployment of the DR System.

Existing safety measures identified by the risk assessment process will be captured in the DR SoS Hazard Record and will be assessed to determine their effectiveness based on engineering change and whether special arrangements / additional procedures and standards, etc. may be required during the implementation period of the change.

Further information with respect to Safety Measures and Requirements is contained in the DR System Safety Plan [RI2].

9. SAFETY REQUIREMENTS

Safety Requirements are contained within the specifications which are an output from the DOORs database and included in the ETCS Onboard CRS [RI7]. Safety requirements are tagged as such within the configuration managed DOORs database and with the word 'Safety' in the CRS.

Safety Requirements that emerge from the hazard identification and risk assessment process will be cross-referenced to the source of the requirement, e.g. DR SoS Generic Hazard Record [RI1] and System Safety Plan [RI2].

10. Assumptions

The assumptions listed here are additionally captured in the Technical RAID Log [RI3]. The RAID Log is used only to manage the assumption and track it until it is closed and not as the master record of the assumptions. The master record of the assumptions remains here in this document and set out in the following sections

10.1 Technical

1. Trackside and Onboards will implement a set of ETCS specifications #3 (Baseline 3 release 2), including the CR solutions identified as part of the Article 10 Technical Opinion).

10.2 Environmental

None.

10.3 Operational

1. It is assumed that ETCS Level 2 operation will be undertaken utilising metric units, including:

   i. entry of metric distances and speeds by the driver
   ii. display of metric distances and speeds to the driver.

10.4 System Integration

1. The procurement/development of the On-line Key Management System and the publication of any protocols and interfaces will not necessitate an update to this document.

2. Parties (Deployment projects / integrators / suppliers) shall ensure that integration of the ETCS Onboard to the train is correct electrically, functionally and environmentally considering all possible physical coupling permutations and all methods of train operation.

3. Trains will be fitted with AWS and TPWS until it is formally determined they will only operate in ETCS fitted areas.

10.5 Maintenance

None

Digital Railway

Working together for a better railway:

Department for Transport

Rail Delivery Group

National Rail

NetworkRail

RFG Rail Freight Group

Rail Supply Group

Railway Industry Association

RSSB

digitalrailway.co.uk @DigitalRailway

Group Digital Railway, Network Rail, 4th Floor, One Eversholt Street, London, NW1 2DN