Digital Railway – European Train Control System (ETCS) Onboard System Definition

Prepared by
Patrick Ndimurukundo
Lead Architect - ETCS Onboard

PN-270318-0003 ....................... Date: 27/03/2018

Reviewed by
Tracey Best
Head of Systems Engineering

TLB-280318-0013 ....................... Date: 28/03/2018

Approved by
Anders Moeller
Head of System Requirements & Integration

ANDM-280318-0014 ....................... Date: 28/03/2018

Working together for a better railway:

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 shall 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 for any purpose other than its stated purpose or for any purpose other than that for which it was prepared except where it can be shown to have acted in bad faith or there has been wilful default.

© Copyright 2018 Group Digital Railway
This document is the property of Group Digital Railway. It shall not be reproduced in whole or in part, nor disclosed to a third party, without the written permission of Group Digital Railway.

Document owner: Patrick Ndimurukundo, Lead Architect - ETCS Onboard

Version History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>07.02.2018</td>
<td>First issue</td>
</tr>
<tr>
<td>0.2</td>
<td>06.03.2018</td>
<td>Scope of the SDD changed: decision System Integration &amp; Interface Manager (e-mail DN 20.02.2018). New Template used.</td>
</tr>
<tr>
<td>0.3</td>
<td>22.03.2018</td>
<td>Updated following Technical Author review</td>
</tr>
<tr>
<td>0.4</td>
<td>26.03.2018</td>
<td>Minor update, reviewed by the System Integration &amp; Interface Manager (JJE)</td>
</tr>
<tr>
<td>0.5</td>
<td>26.03.2018</td>
<td>Reviewed by the Head of Systems Engineering (TB); section 12 Integration Fundamentals Handbook added. Reviewed by the Head of Systems Requirements &amp; Integration (AM)</td>
</tr>
<tr>
<td>1.0</td>
<td>26.03.2018</td>
<td>Formal issue for signature</td>
</tr>
</tbody>
</table>

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 DR Concept of Operations will be updated at a later stage).

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.

1. See Section 10 of this document.
Dependencies

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

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

1 Introduction ...................................................................................................................................... 7
  1.1 Background ............................................................................................................................. 7
  1.2 The Digital Railway Programme (DRP) .................................................................................. 7
  1.3 Context & Purpose of This Document ..................................................................................... 8
  1.4 Scope ...................................................................................................................................... 8
  1.5 Background of the Generic System of Systems (SoS) ........................................................... 9
  1.6 Document Maintenance .......................................................................................................... 9
  1.7 Reference ................................................................................................................................ 9
    1.7.1 Dependent References ....................................................................................................... 9
    1.7.2 Informative References ..................................................................................................... 11
  1.8 Terms, Abbreviations & Acronyms ........................................................................................ 12
2 System Purpose and Objectives .................................................................................................... 13
  2.1 ETCS Mission and Objectives ............................................................................................... 14
    2.1.1 Business Change Consideration for ETCS ....................................................................... 14
    2.1.2 Business Benefits of ETCS ............................................................................................... 14
    2.1.3 Business Change Consideration ....................................................................................... 15
  2.2 ETCS Safety Characteristics Relevant to Interoperability .................................................... 15
    2.2.1 Health and Safety of Workers ........................................................................................... 15
    2.2.2 ETCS Health Monitoring and Maintenance ....................................................................... 16
    2.2.3 Safety ................................................................................................................................ 16
  2.3 Reliability, Availability and Maintainability ............................................................................. 16
  2.4 Environmental protection ...................................................................................................... 17
  2.5 Lifecycle Management .......................................................................................................... 17
3 Overall System of Systems ............................................................................................................ 18
4 System Functions and Elements ................................................................................................... 19
  4.1 DR System Operation ........................................................................................................... 19
    4.1.1 ETCS Legal Context ......................................................................................................... 19
    4.1.2 ETCS Onboard Functionality Overview ............................................................................ 20
    4.1.3 Normal Operation .............................................................................................................. 21
    4.1.4 Degraded Mode Operation ............................................................................................. 21
    4.1.5 Emergency Mode Operation ............................................................................................ 22
  4.2 The Deployed System ........................................................................................................... 22
    4.2.1 Business Continuity ........................................................................................................... 23
    4.2.2 Operational Readiness ...................................................................................................... 24
    4.2.3 Training including Simulator ............................................................................................ 24
    4.2.4 Deployment Guide ............................................................................................................ 24
    4.2.5 Integration Fundamentals Handbook ................................................................................ 24
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>Enabling Projects</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>System Boundary</td>
<td>25</td>
</tr>
<tr>
<td>6</td>
<td>Physical Interfaces</td>
<td>26</td>
</tr>
<tr>
<td>6.1</td>
<td>Rail Vehicles / Onboard Systems</td>
<td>26</td>
</tr>
<tr>
<td>6.2</td>
<td>ETCS Trackside</td>
<td>26</td>
</tr>
<tr>
<td>6.3</td>
<td>Key Management System</td>
<td>26</td>
</tr>
<tr>
<td>6.4</td>
<td>Voice Comms (i.e. GSM-R Voice)</td>
<td>26</td>
</tr>
<tr>
<td>7</td>
<td>Functional Interfaces</td>
<td>28</td>
</tr>
<tr>
<td>7.1</td>
<td>Staff</td>
<td>28</td>
</tr>
<tr>
<td>7.1.1</td>
<td>Operational &amp; Maintenance Staff</td>
<td>28</td>
</tr>
<tr>
<td>7.1.2</td>
<td>Drivers</td>
<td>28</td>
</tr>
<tr>
<td>7.1.3</td>
<td>Incident Investigators</td>
<td>28</td>
</tr>
<tr>
<td>7.1.4</td>
<td>Remote Users, TOCs &amp; FOCs</td>
<td>29</td>
</tr>
<tr>
<td>7.2</td>
<td>Command, Control and Signalling Systems</td>
<td>29</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Adjacent Systems</td>
<td>29</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Operational Telecoms</td>
<td>29</td>
</tr>
<tr>
<td>7.2.3</td>
<td>Signalling and Train Control Systems</td>
<td>29</td>
</tr>
<tr>
<td>7.2.4</td>
<td>Interfacing Protocols</td>
<td>29</td>
</tr>
<tr>
<td>7.3</td>
<td>Equipment Monitoring Systems</td>
<td>29</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Traction Supply Control</td>
<td>29</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Vehicle Monitoring Systems</td>
<td>30</td>
</tr>
<tr>
<td>7.4</td>
<td>Management Systems</td>
<td>30</td>
</tr>
<tr>
<td>7.4.1</td>
<td>Data Management Capability</td>
<td>30</td>
</tr>
<tr>
<td>7.4.2</td>
<td>External (Third Party) Systems</td>
<td>30</td>
</tr>
<tr>
<td>7.4.3</td>
<td>Business Systems</td>
<td>30</td>
</tr>
<tr>
<td>8</td>
<td>System Environment</td>
<td>31</td>
</tr>
<tr>
<td>8.1</td>
<td>Procedures and Rules</td>
<td>31</td>
</tr>
<tr>
<td>8.2</td>
<td>Staff Competence and Assessment</td>
<td>31</td>
</tr>
<tr>
<td>8.3</td>
<td>Security</td>
<td>31</td>
</tr>
<tr>
<td>8.4</td>
<td>Maintenance</td>
<td>31</td>
</tr>
<tr>
<td>8.5</td>
<td>Local Environment and Conditions</td>
<td>31</td>
</tr>
<tr>
<td>8.5.1</td>
<td>ETCS Onboard</td>
<td>31</td>
</tr>
<tr>
<td>8.6</td>
<td>ETCS Onboard Environmental Conditions</td>
<td>32</td>
</tr>
<tr>
<td>8.7</td>
<td>Electromagnetic Compatibility (EMC)</td>
<td>32</td>
</tr>
<tr>
<td>8.8</td>
<td>Human Factors</td>
<td>32</td>
</tr>
<tr>
<td>8.9</td>
<td>TOCs &amp; FOCs</td>
<td>32</td>
</tr>
<tr>
<td>9</td>
<td>Existing Safety Measures</td>
<td>33</td>
</tr>
<tr>
<td>10</td>
<td>Assumptions</td>
<td>34</td>
</tr>
</tbody>
</table>
List of figures

Figure 1: ETCS Onboard and interfaces ................................................................. 13
Figure 2: Digital Railway SoS Architecture .......................................................... 18
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 are to be delivered 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 System (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), Train and Freight Operating Companies (as Railway Undertakings), the Rail Safety & Standards Board (RSSB), Yellow plant, 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 the European Commission states (in part) that:

“The fitting of ERTMS/ETCS is mandatory in the case of new installations or upgrade of the train protection part of a Control Command Signalling (CCS) assembly for rail network identified in the Rail Interoperability Directive transposed in UK law as the Railway Interoperability Regulations (RIR) 2011.”

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. These are:

1. Creation of a generic Customer Requirements Specifications (CRS) for deploying Digital Railway (DR) Systems (using European Train Control System (ETCS) Level 2, a Traffic Management System (TMS), and other sub-systems and enablers).
2. Preparation of business cases and strategic business plans for specific routes using specific applications of DR Systems.
3. Assisting the routes in deploying specific DR Systems as a result of the Business Case analysis work undertaken at 2 above.
4. Production of a series of guidance notes, rules, processes and templates to help a specific delivery project to deploy DR Systems.
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 operating them.
Within the DR Programme, the System Requirements and Integration (SR&I) team is
charged with producing the output required under items 1 and 4 above.

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 component of the hazard identification and risk assessment process defined in 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 will fulfil that need of defining the ETCS Onboard and
its interfaces and thus minimize integration risks. It forms part of a suite of System
Definitions that support the deployment of the DR System of Systems, including the
System of Systems Definition document [RD1].

The 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 application 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.

1.4 Scope

This document applies to the ETCS Onboard only. The principal output from the System
Requirements and Integration team is the Customer Requirement Specifications for the
SoS, the systems within the SOS boundary, and the Interface specifications.

This definition only considers the deployment of the core 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 Route (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 deliver 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 ETCS Onboard is one of the core systems within this architecture.

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

- ETCS Level 2 No Signals
- Traffic Management
- 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 stage gate 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 Systems Engineering.

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 comes to light that would also achieve the Digital Railway primary objectives (see section 2), and then these 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 and a final update will include the safety requirements identified from the Hazard Identification (HAZID) to form 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.

1.7 Reference

1.7.1 Dependent References

[RD1] Digital Railway – System of Systems (SoS) System Definition, 153819-REP-
[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


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


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


[RD20] Assignment of values to ETCS variables, ERA_ERTMS_040001

[RD21] Digital Railway – M9 Significance of Change Assessment, 147833-NWR-ASS-ESS-000001, Ver.0.1, 6th November 2017

[RD22] Digital Railway – Glossary of Terms & Abbreviations, 153819-NWR-SPE-ESS-000001, V1.0

1.7.2 Informative References

[RI1] DR Level A, Generic Hazard Record, DRD-PH2-NONE-TAD-147833-CSM2-161005-180625, Draft B3, 9/03/2017


[RI3] DR Project RAID log, no reference No, Version 1.0, 16/12/2013
1.8 Terms, Abbreviations & Acronyms

Please refer to the DRP Glossary of Terms and Abbreviations [RD22].
2 SYSTEM PURPOSE AND OBJECTIVES

The principal objectives of the ETCS Onboard generic design are to enable:

- the successful deployment of an integrated train command, control and safety system on GB’s railway to achieve the aims mentioned in 1.2, which includes:
  - Traffic Management System;
  - European Train Control System (both Onboard and Trackside);
  - Connected-Driver Advisory System; and
  - Interlocking.
- the individual deployment of the ETCS Onboard by the industry that would support future integration with the other core systems mentioned above.

To ensure that any future deployment is successful, business change activities (e.g. people and process changes) will also be required to support optimal operation of the system and to maximise benefits gained.

This System Definition (and architecture) is route and solution agnostic; however, it is based around current and emerging technology solutions. The system architecture shown in

The Figure 1 highlights ETCS Onboard and interfaces (i.e. blue lines and boxes) within DR System of System architecture.

represents the Digital Railway ETCS Onboard architecture.

---

**Figure 1: ETCS Onboard and interfaces**

The Figure 1 highlights ETCS Onboard and interfaces (i.e. blue lines and boxes) within DR System of System architecture.

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-
ETCS System Definition V1.0
Reference: 153821-NWR-REP-ESE-000005  Page 14 of 35

antennae, GSM-R data antennae). The ETCS Onboard reference architecture is defined in more details in the 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

The business reason 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 fast (i.e. exceeding its Movement Authority) or too far. 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 using GSM-R voice.

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 exposure of staff will be reduced due to fewer active lineside assets (e.g. signals) and 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. However, GPRS will be required to enable some 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 existing Class B systems by introducing a harmonised and standardised signalling system. Existing UK Class B systems are: GW ATP, RETB, TPWS, TVM 430, Chiltern-ATP, Mechanical Trainstops, and KVB.

2.1.3 Business Change Consideration

The introduction of ETCS will affect a number of business processes and all staff engaged in the operation and management of trains.

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

2.2 ETCS Safety Characteristics Relevant to Interoperability

As stated in the Command, Control and Signalling Technical Specification for Interoperability (CCS TSI),

‘the design, implementation and use of a Control-Command and Signalling On-board or Trackside subsystem shall not export any requirements:

(a) across the interface between Control-Command and Signalling On-board or Trackside subsystems in addition to the requirements specified in this TSI;

(b) to any other subsystem in addition to the requirements specified in the corresponding TSIs.’

Thus, exporting a requirement from another sub-system to the ETCS Onboard or ETCS Trackside is not recommended. However, exchanging data between ETCS and non-ETCS systems is not forbidden, as long as it does not affect interoperability and the standard ETCS interfaces.

2.2.1 Health and Safety of Workers

European and UK Health and safety regulations will be applied to the ETCS Onboard. This will mitigate health hazards to people having access to the system and its components.

2.2.2 ETCS Health Monitoring and Maintenance

The ETCS Onboard will be fitted with equipment for health monitoring and degraded mode support. For the ETCS Onboard, this function (i.e. health monitoring) includes:

- initialising the ETCS Onboard functionality;
- providing degraded mode support; and
- isolating the ETCS Onboard functionality.

Data recording for regulatory purposes is required for the ETCS Onboard integrated in the rail vehicle. Where a GB legacy data recording unit is required in addition to the ETCS data recording device, it is possible to combine them.

It should be noted that the CCS TSI (e.g. in section 4.5.1) describes responsibilities for the stakeholders involved in ETCS development, implementation and use.

2.2.3 Safety

The CCS TSI, and more specifically Subset-091[RD6], mandates the safety requirements and Tolerable Hazard Rate (THR) to be achieved by the ETCS Onboard. BS EN 50126 ([RD9] and [RD10]), 50128 [RD11] and 50129 [RD12] outline the processes enabling safety by design of ETCS. Safety processes should be complemented by risk assessment activities in line with the Common Safety Method for Risk Assessment and Evaluation (CSM RA).

Techniques and measures for Safety Integrity Level (SIL) 4 will need to be implemented by the ETCS contractor to achieve safety and performance levels required to run the GB mainline railway safely and reliably. Rigorous techniques will enable the production of high integrity ETCS software (see BS EN 50128:2011, Annex A).

During the ETCS operation and maintenance phase, the system will be monitored to maintain the level of safety and performance confirmed during the Authorisation and Approval process.

2.3 Reliability, Availability and Maintainability

The CCS TSI mandates requirements that are essential to mitigate against the occurrence of failures modes that could cause safety hazards. Infrastructure Managers and Railway Undertakings will be given all the information they need to define appropriate procedures for managing degraded situations. The CCS TSI requires the technical file and the European Commission (EC) Declaration of Verification (DoV) for the ETCS Onboard or the ETCS Trackside system to include calculated availability/reliability values related to failure modes having an impact on the capability of the ETCS to supervise safe movement.

The ETCS Onboard will be compliant to the RAM requirements contained in the ERTMS/ETCS RAM Requirements Specification [RD7] and ERTMS Reliability Specification [RD8]. The CCS TSI mandates the application of BS EN 50126 ([RD9] and [RD10]), BS EN 50128 ([RD11]), and BS EN 50129 ([RD12]) for RAM. In addition, some standards attached to the CCS TSI, such as Subset-036 (i.e. see RAM requirements for Eurobalises) will require demonstration of conformance from ETCS suppliers.

The ETCS Contracting Authority (e.g. Railway Undertaking or Infrastructure Manager) should review all the RAM requirements and, where necessary, add or amend them to align with the level of performance required for the vehicle.

The starting point will be to consider the Reliability specification [RD8]. Each project should then review and complete their RAM requirements as appropriate to the Class of train to be fitted with (an) ETCS Onboard(s).

The ETCS Onboard will not decrease the Mean Time between Service Affecting Failure (MBTSAF) of the existing train system as a basic principle.
2.4 Environmental protection

ETCS Onboard will comply with essential requirements laid down in the CCS TSI and other relevant EU and UK regulations (see CCS TSI, section 3.2.4).

ETCS Onboard equipment will be tested in accordance with testing procedures currently used for trainborne systems.

2.5 Lifecycle Management

The ETCS development life cycle management will need to comply with mandatory standards BS EN 50126, 50128, 50129 and 50159 (see CCS TSI, Table A3). It should be noted that more specific project or programme life cycle management systems could be applied when relevant.
3 OVERALL SYSTEM OF SYSTEMS

This section provides the context of the ETCS Onboard within the System of Systems (SoS) work produced by the Digital Railway Programme.

The baseline architecture, referred to as the System of Systems, is outlined as follows:

---

**Digital Railway Programme**

---

**Figure 2: Digital Railway SoS Architecture**

Further details of the interfaces shown in Figure 2 above (including protocol, bearer and multiplicity) and the information flowing across them are covered in the document Digital Railway Programme Interface Description Document [RD5].
4 SYSTEM FUNCTIONS AND ELEMENTS

This section provides an outline of the System operations and enablers required to support future deployment of the ETCS Onboard in rail vehicles running on GB’s rail network.

The following are considered essential System elements to support future deployments:

- ETCS Onboard
- Operational Readiness
- Enabling Projects (e.g. GSM-R upgrade, National Key Management System (KMS), etc.)

In addition to these elements, which are described in detail in the following sections – it will be necessary for the industry to develop the following to realise the full potential of deploying Digital Railway Systems:

- **Configuration data:** At each location where a DR System is to be deployed, site-specific configuration data (e.g. geographic, functional, etc.) will define how that specific DR System interacts with the railway it controls and the site-specific functions it applies.
- **Maintenance Procedures:** The new functionality provided by the Digital Railway System will require revised maintenance procedures for areas of the railway where the DR Systems are deployed and transitional arrangements may be required where new and old technology exists.
- **Operator Manuals:** Manuals will contain comprehensive material that supports new and existing skill sets and will define the tasks that operational and maintenance staff will carry out on the various parts of the System.
- **Maintenance tools:** The DR System may assist maintainers in predicting and identifying faults. Maintenance tools will enable maintainers to predict, identify and rectify faults in the DR System.
- **Training material:** Training material will enable operational and maintenance staff to learn and practise the tasks that they will be required to carry out in their role before they operate on a live system.

4.1 DR System Operation

The ETCS Onboard Concept of Operations (ConOps) will provide greater detail on the desired System operation. However, this section is included to provide a brief summary of how the ETCS Onboard typically operates to aid understanding of other sections of this document.

The DR System will support operation in normal, degraded and emergency modes, although operation in the latter two will depend on the cause and scale of the degraded mode of operation.

4.1.1 ETCS Legal Context

The Railway Interoperability Regulations 2011 (RIR 2011) transposes the Rail Interoperability Directive 2008/57/EC into UK law. The RIR describes the Rail system as being composed of structural sub-systems listed below:

- Rolling stock vehicles (external interface to ETCS Onboard)
- Infrastructure (external interface to ETCS Trackside)
- Energy (external interface to ETCS)
- Control, Command and Signalling on board, including ETCS Onboard
- Control, Command and Signalling trackside, including ETCS Trackside extended to include Interlocking for Digital Railway deployments

For each structural sub-system, a Technical Specification for Interoperability outlines the essential requirements to be met, including the interfaces between the sub-systems. The ETCS Onboard requirements are primarily laid down in the Control-Command and Signalling TSI (CCS TSI) and complemented by the GB Generic requirements.
The RIR also describe Functional sub-systems:

- Traffic and Operation Management (external interface to ETCS)
- Maintenance (part- ETCS Onboard and part- ETCS Trackside)
- Telematics applications for passenger trains (out of scope for ETCS)
- Telematics applications for freight trains (out of scope for ETCS)

The interfaces between the ETCS and the wider CCS will require careful consideration during the process of ETCS deployment on the GB rail system.

### 4.1.2 ETCS Onboard Functionality Overview

Introduction of the ETCS Onboard on GB’s rail network will coincide with the procurement of new trains; existing rail vehicles will be modified to accept the ETCS equipment and may also require the alteration or addition of a Train Control Management System (TCMS). The latter is likely to be necessary as the ETCS requires the use of a Train Communication Network (TCN) between equipment in the vehicle.

The CCS TSI lays down ETCS Onboard functionality and interface requirements. The ETCS Onboard main safety function is its ability to supervise a train safely by intervening to prevent the exceedance of speed and distance; this will reduce the risk of collision that could lead a loss of life or a degradation of the railway.

The main safety function of the ETCS Onboard is achieved through Automatic Train Protection (ATP) and Cab Signalling features prescribed in the CCS TSI. These stipulations are complemented by the GB ETCS Reference Design process and the resulting ETCS requirements suite published on the Rail Safety and Standards Board (RSSB) website. To achieve these goals, the following ETCS Onboard functions are required by the CCS TSI:

- setting of train characteristics (e.g. maximum train speed, braking performance);
- selecting of supervision mode on the basis of information from the Trackside (e.g. Full Supervision (FS) mode);
- performing odometry functions;
- locating the train in a coordinate system based on Eurobalise locations;
- calculating the dynamic speed profile for the train’s mission on the basis of train characteristics and information from the Trackside;
- supervising the dynamic speed profile during the mission;
- providing the intervention function (i.e. application of service or emergency brake, when required).

These functions will be implemented in accordance with Subset-026, Subset-040 and Subset-091, and their performance will conform to Subset-040 and additional GB generic engineering rules to be identified at a later stage.

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

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

The GB ETCS application requires additional definition of engineering and operational rules identified generically in the GB ETCS Reference Design.

Applications using Packet 44 application will be integrated to avoid the use of bespoke solutions from suppliers. The role of a GB Industry System Authority will be required to avoid multiplication of bespoke and insufficient documented Packet 44 applications, as one of the main issues that has been identified is the non-harmonised and not properly designed/documented train behaviour.
4.1.3 Normal Operation

The Interoperability Directive defines the ‘Operation and Traffic Management’ system as:

“The procedures and related equipment permitting coherent operation of the various structural subsystems, during both normal and degraded operation, including in particular train composition and train driving, traffic planning and management.”

It should be noted that ERTMS Operational Principles and Rules are contained within Annex A of the Operation and Traffic Management TSI and in UK Notified National Technical Rules (available through the ERA and RSSB websites, respectively).

The ETCS Onboard provides cab signalling and train protection with Level 2 no signals, enabling train operations in a Digital Railway SoS within the railway system (i.e. SoS, infrastructure, contact systems, etc.). It requires a Movement Authority and Track Description (i.e. Speed and Gradient Profiles) 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, train joining or splitting
- Non-Leading (NL) – this will support banking movement where a non-leading train provides traction effort 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 execute procedures such as:

- Starting in Level 2, ideally in FS or OS;
- Executing a Level transition, either leaving a Level NTC area or entering into a Level 2 area;
- Performing an RBC-RBC handover within a Level 2 area.

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 the GB rail network.

4.1.4 Degraded Mode Operation

The ETCS will be considered to be operating under degraded operating conditions when it cannot to supervise the ETCS-fitted train safely or the driver has 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 UK Notified 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.

Examples of ETCS degraded operations are given below:

- Failure of self-test 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 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).
4.1.5 Emergency Mode Operation

The ETCS includes functions enabling the 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 UK Notified National Technical Rules published on the RSSB website and listed on the ERA website.

Examples of ETCS emergency operations are given 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. IS mode) and the train has to be rescued by an assisting train.

4.2 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 trackside orders from the ETCS Trackside and a means of determining the train position along the track.

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;
- Odometry unit;
- Speed sensors;
- DMI;
- GSM-R mobiles, etc.

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

- ETCS Trackside;
- Key Management System (KMS).

and the following are the key enablers:

- GSM-R and GPRS;
- Users (e.g. Train Driver, ETCS Onboard operator, Onboard maintainer, etc.);
- Business Continuity;
- Configuration Data;
- FTN and FTNx.

The ETCS Trackside is described in the ETCS Trackside System Definition Document and the DR Interface Description Document ([RD19]) and, therefore, its description is not repeated here.

The levels and operational modes are basic concepts of the ETCS system. A short definition of each follows:

- Level 1 involves continuous supervision of train movement with non-continuous communication between train and trackside (by means of Eurobalises in UK). Lineside signals are necessary and train detection is performed by trackside equipment which is outside the scope of the ETCS. Apart from transitions into Level 2, operation in Level 1 is outside the scope of this document.
- 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 system. Lineside signals are optional in this case, and train detection is performed by trackside equipment.
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 the 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 on 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. ETCS Level 3 offers a migration path where the benefits will be identified in the future.

In addition, two more levels are defined:

- Level 0 is meant 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 meant for trains equipped with ETCS running on lines where the Class B system needs to be operated. For Level NTC, the ETCS could act as an interface between the driver and the UK Class B system. The provision of on-board equipment to enable ETCS-fitted trains to operate with the Automatic Warning System (AWS) and Train Protection and Warning System (TPWS) is within the scope of this document.

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), Stand By (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 supervision and protection (e.g. ensuring movement does not exceed the End of Movement Authority).

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 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.

There are also other modes for different operational situations:

- Shunting (SH) will be used for train formation in a train depot or in 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 by the ETCS.

The Operational Concept for ERTMS [RD13] provides more details about the modes and their use in meeting GB Railway operational needs.

4.2.1 Business Continuity

Business Continuity concerns the ability of the business to absorb perturbations and continue to run the service. The level of service can change according to the degree of perturbation. Business continuity requirements will be included, where applicable, within the System CRS.
4.2.2 Operational Readiness

This will ensure that the systems to be deployed are ready to enter into service, i.e. they can be installed, operated and maintained by competent personnel.

Operational Readiness requirements will be produced for inclusion in the ETCS Onboard CRS.

4.2.3 Training including Simulator

The purpose of the DR programme is to enable successful deployment of new technology and operations on the rail network and there will thus a significant training and capability activity will be required to underpin deployment of the Digital Railway.

The following are expected to be produced, where applicable, for the system:

- A training simulator specification
- Training requirements
- A list of training scenarios

4.2.4 Deployment Guide

The Digital Railway Programme will produce a deployment guide, where felt necessary, that will facilitate the implementation of the system by the deployment programmes.

4.2.5 Integration Fundamentals Handbook

To help enable successful integration of the ETCS Onboard, DRP will be producing an Integration Fundamentals Handbook for programmes to use as best practice guidance when deploying and integrating DR technologies.

4.3 Enabling Projects

These are projects that are deemed to be outside of the DR System but which are critical dependencies to/from the 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.

The critical enablers for the ETCS Onboard are:

- GSM-R and GPRS network availability: the radio system is required to enable ETCS functionality as the ETCS Onboard will exchange data during operation and maintenance, if necessary. The ETCS requires sufficient radio coverage and capacity and compliance to the CCS TSI (i.e. set of specifications #3).
- Key Management System: this allocates and distributes the authentication keys, enabling secure communication between ETCS Trackside and ETCS Onboard. 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)).
- Configuration Data: this is the static information regarding the railway network that is used to provide Movement Authorities to trains and as a reference for temporary restrictions and degraded scenarios.

Please refer to the DRP SoS System Definition [RD1] for a brief description of the key enabling systems as they are not repeated here.
5 SYSTEM BOUNDARY

The elements contained within the system boundary are shown in the

The Figure 1 highlights ETCS Onboard and interfaces (i.e. blue lines and boxes) within
DR System of System architecture.

above. 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. Geographical boundaries will be considered in the System Definition documents for specific DR deployment schemes as and when they occur.
6 PHYSICAL INTERFACES

When deployed in the railway environment, the ETCS Onboard will also interface to other physical systems, as discussed in the following sections.

The ERTMS/ETCS Reference architecture is described in Subset-026 Chapter 2. It shows 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.

6.1 Rail Vehicles / Onboard Systems

The ETCS Onboard will be integrated into two types of train configuration:

- retrofit trains, for which lower level detailed requirements (i.e. EOSS) are published on the RSSB website; and
- new trains for which lower level detailed requirements (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 (LOC&PAS TSI), which includes some GB-Specific Cases (e.g. UK Loading Gauge). The success of 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.

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 or Specific Transmission Module Form Fit Functional Interface Specification (STM FFFIS), enabling level transitions to take place between Level 2 and Level NTC areas.

The ETCS Onboard includes functions that can trigger other on-board systems to manage a specific rolling stock function. A good example is the Automatic Selective Door Operation (ASDO). The ETCS Onboard could transfer orders to open the doors on one side to the trackside via the Train Interface Unit. However, ETCS Onboard will never be responsible for managing the doors as they are part of the rail vehicle.

6.2 ETCS Trackside

The ETCS Onboard will communicate with the ETCS Trackside via the radio airgap (i.e. GSM-R/GPRS) in compliance with the CCS TSI.

6.3 Key Management System

The ETCS Onboard will request authentication keys over the radio 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 then be capable of storing correct authentication keys transmitted by the Home Key Management Centre if an update is needed.

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

The only interface that could be considered is the one enabling entry of the Train Running Number (i.e. Headcode) from one place only: i.e. the DMI. If the interface is not provided, then the driver will have to enter the Train Running Number more than once into the GSM-R voice interface, DMI and, potentially, into the C-DAS, where fitted. This is not ideal from a performance point of view.
NB: The UK introduced a Notified National Technical Rule (NNTR) to enable alphanumeric Train Running Numbers, if needed by the users. See GERT8402 “ERTMS/ETCS DMI National Requirements”.

7 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.

7.1 Staff

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

7.1.1 Operational & Maintenance Staff

Operational Staff are defined as any individuals who are authorised, competent and responsible for the movement of trains, e.g. signaller, who interfaces with the DR System as part of their duties. This includes staff that contributes to the safe movement of trains through their roles, e.g. TOC platform staff undertaking train dispatch duties.

Maintenance Staff are defined as individuals who are responsible for undertaking engineering activities on railway infrastructure and vehicles. This includes those who work track side 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 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 staff to operate the System in a safe and efficient manner.

Interfaces to the system will be procedural or technical. Details for specific groups of staff are described in the following sections.

7.1.2 Drivers

The ETCS Onboard will have functional interfaces with the driver as follows:

- Driver Machine Interface
- Isolation capability

7.1.3 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 over-speed, 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 (see 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, 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 have to be made to share data openly and efficiently across the industry for incident investigation.
7.1.4 Remote Users, TOCs & FOCs

The DR System 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 in which the ETCS Onboard is integrated.

7.2 Command, Control and Signalling Systems

7.2.1 Adjacent Systems

The DR System will need to interface to adjacent systems, whether other instances of the system itself, existing legacy control systems or depot control systems.

The ETCS Onboard of a leading train with its leading active cab could be connected to:

- multiple ETCS Onboards in single or multiple formation; or
- other ETCS Onboards in Sleeping (SL) mode requiring Sleeping input.

7.2.2 Operational Telecoms

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 between the DMI part of the ETCS Onboard and GSM-R voice cab radio will share the Train Running Number between 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.

7.2.3 Signalling and Train Control Systems

The DR System will be required to interface to existing legacy command and control systems at the boundary of a DR deployment area, enabling handover of operational services.

7.2.4 Interfacing Protocols

The ETCS Onboard will be able to communicate with the ETCS Trackside and KMS 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. 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 protocol 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).

7.3 Equipment Monitoring Systems

7.3.1 Traction Supply Control

The ETCS Onboard is connected to the rail vehicle via the Train Interface Unit. It has the capability to command the cutting of traction to pass a neutral section area, for example, and to obtain the traction status from the rail vehicle. Subset-034 of the CCS TSI, prescribes the functional interface specifications for integrating an ETCS Onboard into a rail vehicle.
7.3.2 Vehicle Monitoring Systems

The ETCS Onboard will include a Juridical Recording device which can be combines with an On Train Monitoring and Recording (OTMR) or an On Train Data Recorder (OTDR). Timestamping of recorded data will need to be synchronised to avoid discrepancies within recorded data/events. Synchronisation of clocks is important in the wider DR SoS.

7.4 Management Systems

7.4.1 Data Management Capability

In deploying a successful Digital Railway system, one of the core capabilities will be managing and exploiting data as a business-critical asset. Achieving this means transforming the way that data and information is perceived and used by the industry requiring changes across People, Processes & Technology. This forms one of the core building blocks of the Programme, transforming the technology and processes involved in running the railway by integrating the underlying data.

It should be noted that ETCS data will be pre-designed and pre-programmed and will thus not be changed during its operation. It will be possible to superimpose specific data in a controlled manner related to Temporary Speed Restrictions applicable for a limited time only. Any other change to the infrastructure will require rigorous data preparation processes (i.e. to be certified as Safety Integrity Level – SIL 4), usually undertaken by a competent ETCS supplier (e.g. part of UNISIG).

7.4.2 External (Third Party) Systems

As well as the national systems, the DR Systems will also necessarily acquire their transient information from systems outside of the Network Rail suite of information and business systems. Both Train and Freight Operating companies have their own internal systems and some of these hold data that will need to be acquired by DR Systems in order to deliver their functions.

Remote download and sharing of data recorded in the vehicle may be needed by users in the future.

As mentioned in section 7.3.2, it is envisaged that the project will require a Train Control Management System. Business Systems

The rail industry relies on a wide range of Business Systems to run its existing operations and the ETCS Onboard will potentially impact on these by:

- data entry using external systems such as TOPS; and
- developing new business systems that support the DR implementation of technologies and/or offer additional benefits to the industry (i.e. DRACAS).

7.4.3 Business Systems

The rail industry relies on a wide range of Business Systems to run its existing operations and the ETCS Onboard will potentially impact on these by:

- data entry using external systems such as TOPS; and
- developing new business systems that support the DR implementation of technologies and/or offer additional benefits to the industry (i.e. DRACAS).
8 SYSTEM ENVIRONMENT

8.1 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.

Deployment of the ETCS Onboard will cause changes to the Rule Book and other longstanding practices.

8.2 Staff Competence and Assessment

In line with existing accident investigation recommendations, training facilities 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 and retrained to be able to maintain and fault-find any new equipment appropriately and safely, and their competence will require ongoing assessment.

8.3 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, Network Rail Telecom (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.

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

8.5 Local Environment and Conditions

8.5.1 ETCS Onboard

ETCS Onboards will be required to comply with environmental conditions specified for their installation location on or within rail vehicles. This will be confirmed through the normal Approval process.

ETCS Onboards will need to be EMC-compliant within limits specified for their installation location on or within rail vehicles. This will be confirmed through the normal Approval process.

ETCS Onboards 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 in the driving desk.
8.6 **ETCS Onboard Environmental Conditions**

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

8.7 **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.

8.8 **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.

8.9 **TOCs & FOCs**

The Train Operating Companies (TOC) and Freight Operating Companies (FOC) 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;
- On Train Monitoring Recorder (OTMR) Data.
9 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.

Within a current (conventional) railway command and control system, the Interlocking contains the safety-critical functionality that ensures route integrity and provides Movement Authority.

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 Generic 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.

The Safety Requirements that emerge from the hazard identification and risk assessment process will be cross-referenced to the DR SoS Generic Hazard Record [RI1] and the DR Systems Generic Hazard Records for each DR System (where applicable).

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

All risks, assumptions, issues and dependences are recorded in the Digital Railway Project RAID log document [RI3]. They are regularly reviewed by Lead Architects to ensure compliance with this System Definition.
Digital Railway

Working together for a better railway:

Rail Delivery Group
Network Rail
Rail Freight Group
Rail Supply Group
Railway Industry Association
RSSB
London Underground