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

Prepared by
John Alexander
Lead Architect ETCS Trackside

Reviewed by
Tracey Best
Head of Systems Engineering

Approved by
Anders Moeller
Head of System Requirements & Integration

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: John Alexander, Lead Architect ETCS Trackside

Version History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>22/02/18</td>
<td>Transfer of Trackside information to new template.</td>
</tr>
<tr>
<td>0.2</td>
<td>28/02/18</td>
<td>Update to Technical Author comments</td>
</tr>
<tr>
<td>0.3</td>
<td>13/03/18</td>
<td>Updated to comments from Lead Architects and stakeholders</td>
</tr>
<tr>
<td>1.0</td>
<td>19/03/18</td>
<td>First issue</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. Alignment with updated Concept of Operations for ETCS.

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. 

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. System of System (SoS) System Definition, [RD5]
# Contents

1 Introduction ...................................................................................................................................... 6
  1.1 Background ................................................................................................................................ 6
  1.2 The Digital Railway Programme (DRP) .................................................................................. 6
  1.3 Context & Purpose of this Document ...................................................................................... 7
  1.4 Scope ...................................................................................................................................... 7
  1.5 Background to the Generic System of Systems (SoS) ........................................................... 8
  1.6 Document Maintenance .......................................................................................................... 8
  1.7 References .............................................................................................................................. 8
    1.7.1 Dependent References ....................................................................................................... 8
    1.7.2 Informative References ....................................................................................................... 9
  1.8 Terms, Abbreviations & Acronyms .......................................................................................... 9
2 System Purpose and Objectives .................................................................................................... 10
3 Overall System of Systems ............................................................................................................ 12
4 ETCS Trackside Functions and Elements ..................................................................................... 13
  4.1 DR System Operation ........................................................................................................... 13
    4.1.1 Normal operation ............................................................................................................... 14
    4.1.2 Degraded mode operation ................................................................................................ 14
    4.1.3 Emergency mode operation .............................................................................................. 15
  4.2 The Deployed System ........................................................................................................... 15
    4.2.1 Business Continuity ........................................................................................................... 16
    4.2.2 Operational Readiness ...................................................................................................... 16
    4.2.3 Training ............................................................................................................................. 16
    4.2.4 Deployment Guide ............................................................................................................ 16
    4.2.5 Integration Fundamentals Handbook ................................................................................ 17
  4.3 Enabling Projects .................................................................................................................. 17
5 System Boundary ........................................................................................................................... 18
6 Physical Interfaces ......................................................................................................................... 19
  6.1 Rail Operating Centre (ROC) ................................................................................................ 19
    6.1.1 Building Interior ................................................................................................................. 19
    6.1.2 Power Supply .................................................................................................................... 19
    6.1.3 Traffic Management .......................................................................................................... 19
  6.2 Telecommunications ............................................................................................................. 19
    6.2.1 Local Area Network (LAN) ................................................................................................ 19
    6.2.2 FTN / FTN-X ...................................................................................................................... 19
    6.2.3 GSM-R .............................................................................................................................. 19
    6.2.4 Data ................................................................................................................................... 20
  6.3 Lineside ................................................................................................................................... 20
6.3.1 Multi Aspect Signalling (MAS) ................................................................. 20
6.3.2 Train Detection ....................................................................................... 20
6.3.3 Automatic Warning System (AWS)/Train Protection and Warning System (TPWS) ...... 20
6.3.4 Management of Trackside Infrastructure ................................................... 20
6.3.5 Signal Controlled Warning System (SCWS) ............................................... 20
6.4 Other Physical Interfaces ........................................................................... 20

7 Functional Interfaces ..................................................................................... 22
7.1 Staff ......................................................................................................... 22
  7.1.1 Operational, Maintenance and Response Staff ............................................. 22
  7.1.2 Maintenance Management ........................................................................ 23
  7.1.3 Operations Staff ...................................................................................... 23
  7.1.4 Train Operating Company (TOC) Station Staff ........................................... 23
  7.1.5 Train Operating Company (TOC) Management and Operational Staff ........... 23
  7.1.6 Trackside Staff ....................................................................................... 23
  7.1.7 Staff engaged in the design and configuration of the ETCS Trackside ............... 23
  7.1.8 Installation staff ...................................................................................... 24
  7.1.9 Testing and authorisation personnel ........................................................... 24
  7.1.10 Incident Investigators ............................................................................ 24

7.2 Command, Control and Signalling Systems .................................................. 24
  7.2.1 Adjacent Systems .................................................................................... 24
  7.2.2 Signalling and Train Control Systems ......................................................... 24
  7.2.3 Level Crossings ....................................................................................... 25
  7.2.4 Interfacing Protocols ............................................................................... 25

7.3 Equipment Monitoring Systems .................................................................... 25
  7.3.1 Infrastructure Monitoring Systems .............................................................. 25

7.4 Management Systems .................................................................................. 25
  7.4.1 Data Management Capability .................................................................... 25

7.5 Business Systems ........................................................................................ 25

8 System Environment ....................................................................................... 27
  8.1 Procedures and Rules .................................................................................. 27
  8.2 Staff Competence and Assessment ............................................................... 27
  8.3 Security ...................................................................................................... 27
  8.4 Maintenance ............................................................................................... 28
  8.5 Local Environment and Conditions .............................................................. 28
    8.5.1 Trackside ............................................................................................... 28
  8.6 Trackside Equipment .................................................................................. 28
  8.7 Electromagnetic Compatibility (EMC) ........................................................... 29
  8.8 Human Factors ......................................................................................... 29

9Existing Safety Measures .................................................................................. 30
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, 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 for GB Rail through the application of modern train control technology. The vision, purpose and objectives have been summarised as [RD1]:

- 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 and 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.

1.2 The Digital Railway Programme (DRP)

The Digital Railway Programme has several principal objectives. These are:

1. Creation of a suite of generic Customer Requirements for deploying Digital Railway (DR) Systems (using the European Train Control System (ETCS) Level 2, Traffic Management System (TMS), and other subsystems 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 in 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 DR Programme, the term ‘System’ refers to the various digital technologies to be deployed (i.e. European Train Control System (ETCS) Level 2, Traffic Management System (TMS), and other subsystems and enablers); System of Systems (SoS) refers to their integration and deployment to enable the full benefits of the Digital Railway Programme to be realised. Both terms (SoS and Systems) include more than just the products themselves: they also include the people, processes and data required to operate them.

Within the DR Programme, the System Requirements and Integration team is charged with producing the output required under items 1. and 4. above.

The DR Programme is describing as part of the System of Systems four key systems:

- ETCS Onboard,
- ETCS Trackside (including interlocking functionality) – scope of this document,
- C-DAS (Connected Driver Advisory System), and
- Traffic Management.
Whilst the concept is to deploy all of the four systems, 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 (CSM) on risk evaluation and assessment (CSM RA) came into full effect through Regulation 402/2013 [RD2] and was amended by Regulation 2015/1136 [RD3] 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 rail. A formal assessment of the significance of the change has been undertaken [RD4] and it was concluded that the change is significant with high 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 clearly define what is meant by ‘System of Systems’ and ‘System’ and their 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 Trackside and its interfaces, and thus minimise 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 [RD5].

The System Definition defines the key details of the ETCS Trackside, 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 Trackside 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 support a high-level understanding of the ETCS Trackside, 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 Trackside 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 Manager 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 the ETCS Trackside sits as the SoS has its own System Definition [RD5]. Whilst this document may
be utilised to describe the scope of a contract or project, it is intended to be read and applied within the context of the SoS System Definition.

1.5 Background to the Generic System of Systems (SoS)

The System Requirements and Integration (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 Trackside 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 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
- operational readiness to support the people and process change required

The SoS configuration ensures that the systems within it, e.g. C-DAS, ETCS and 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 is owned by the Lead Architect ETCS Trackside. It will be subject to review at least prior to each stage gate to ensure its 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 [RD5]. However, if during delivery of this plan, a different technical solution comes to light that would also achieve the Digital Railway primary objectives (see section 2), then it 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 References

1.7.1 Dependent References

An update to one of these references requires an update to this document:

RD1. Digital Railway Programme – Vision, Purpose, Objectives (DRAFT), issued by email 19th December 2016 by Digital Railway Comms
RD4. Digital Railway – M9 Significance of Change Assessment, 147833-NWR-ASS-ESS-000001, Ver.0.1, 6th November 2017
1.7.2 Informative References

These references have no material bearing on the content of this document:

RI1. DR Level A, Generic Hazard Record, DRD-PH2-NONE-TAD-147833-CSM2-161005-180625.
RI3. ETCS RAID log, 153821-NWR-REP-PRK-000001_01.

1.8 Terms, Abbreviations & Acronyms

Please refer to the DRP Glossary of Terms and Abbreviations [RD6]
2 SYSTEM PURPOSE AND OBJECTIVES

The ETCS Trackside is one of the four core systems within the DR System of Systems. The generic design has been developed as part of that integrated system however the output is equally applicable to:

- deployment of an integrated and repeatable train command, control and safety system on GB rail to meet the objectives mentioned in 1.2, including:
  - Traffic Management System;
  - European Train Control System (both Onboard and Trackside);
  - Connected-Driver Advisory System; and
  - Interlocking, or
- an individual deployment of the ETCS Trackside 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 change) 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 Figure 1 represents the Digital Railway ETCS Trackside architecture.

The ETCS Trackside consists of interlocking functionality (to assure the safe reservation of routes for trains to follow) and the issue of Movement Authorities (primarily, to the ETCS Onboard, but also to lineside assets in boundary areas).

The ETCS Trackside receives and processes requests for train movements from the signaller or automated systems via an interface with the Traffic Management System. Commands to moveable infrastructure, such as points and level crossings, are sent to trackside objects. The status of trackside objects, including train detection, is monitored by the ETCS Trackside. Information is shared with Traffic Management and Safer Track Working systems.

The ETCS Trackside communicates with the ETCS Onboard using fixed balises mounted on the track which are pre-programmed. The ETCS Trackside exchanges information with the ETCS Onboard using messages sent over the Global System for Mobile Communications – Railway (GSM-R) data radio.
Figure 1 – ETCS Trackside Architecture
3 OVERALL SYSTEM OF SYSTEMS

This section provides the context of the ETCS Trackside in relation to the SoS work produced by the Digital Railway Programme. This section summarises the key principles and the definitive text is contained in [RD5].

This work identified a baseline architecture referred to as the System of Systems as follows:

![Figure 2 – The SoS Architecture](image)

Further details of the interfaces shown in Figure 2 (including protocol, bearer and multiplicity) and the information flowing over them are covered in the Digital Railway Programme Interface Description Document [RD7].

Details of the information and data flows required by the ETCS Trackside or from the ETCS Trackside have been developed as part of the generic design and are recorded in the Interface Requirements Specification [RD8].
4 ETCS TRACKSIDE FUNCTIONS AND ELEMENTS

This section provides an outline of the System operations and enablers required to support future deployment of the ETCS Trackside on GB Rail.

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

- ETCS Trackside
- 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, there will be a need 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 deployed, there will be site-specific configuration data (e.g. geographic, functional, etc.) that 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 any transitional arrangements that 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 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 practice the tasks that they will be required to carry out in their role before they have to work on a live system.

4.1 DR System Operation

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

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

The key functions are:

- Recording and sharing the status of the infrastructure (train detection, points, level crossings, etc.),
- Enabling routes to be set when available,
- Locking routes for the exclusive use of a train movement,
- Releasing routes when it is safe to do so including section by section,
- Issuing movement authorities to the correct trains including all supporting static data (speed profiles, gradients),
- Managing emergencies (emergency stop messages, cancelling routes),
- Receiving position reports and other data from trains and sharing with other systems,
- Supporting degraded scenarios.

The ETCS Trackside consists of two core functional elements:

- Interlocking,
- ETCS equipment (often referred to as Radio Block Centre – RBC).
The exact split of functionality is not defined and different configurations are possible. The interlocking is responsible for the control and monitoring of trackside objects. It manages the safe establishment of routes, their proving and locking. The confirmation that a movement authority may be issued may be undertaken by the interlocking, the RBC or both systems.

The communication with the ETCS onboard over the radio connection is the responsibility of the RBC utilising messages specified in the Technical Standard for Interoperability [RD9].

The ETCS Trackside also sends fixed messages to the ETCS Onboard using balises to instruct the train to undertake certain activities, such as connect to the RBC, and provide reference locations which can be reported by the ETCS Onboard for positioning.

Where essential to support the driver, ETCS Stop or Location Markers are provided at the lineside to indicate stopping locations.

4.1.1 Normal operation

The Traffic Management System will pass requests for train movements to be authorised to the ETCS Trackside, which will undertake checks to determine whether it is safe for those movements to be undertaken. The infrastructure required for a movement will be reserved exclusively until it is no longer required for the train movement and commands will be sent to moveable infrastructure. This is a function of the interlocking.

The ETCS Trackside will continually monitor the state of the trackside infrastructure and only issue Movement Authorities when it is safe to do so. In the event of loss of proving of critical trackside elements, the ETCS trackside will issue appropriate commands to the ETCS Onboard. This function may be undertaken by the interlocking, the RBC or jointly.

The Movement Authorities issued to the Onboard will be supported by the correct speed profile information for the train, including any temporary restrictions received from the Traffic Management System. This will enable the Onboard to display all relevant information to the driver. The RBC requires data regarding the infrastructure in order to generate movement authorities.

The ETCS Trackside will provide information on the status of the infrastructure, communicating trains and interlocking functions (e.g. route set and Movement Authority issued) to the Traffic Management System, as required by the signaller. Information will primarily be supplied by the interlocking with supporting data from the RBC.

Security of communications between ETCS Trackside and ETCS Onboard will be maintained in accordance with interoperable standards, utilising authentication data keys obtained from a Key Management System. Communications within the ETCS Trackside (between RBC and interlocking, and between adjacent ETCS Tracksides) will be secured using physical separation, encryption or authenticated messages.

Whilst the preferred normal operation is through the issue of Movement Authorities, the ETCS trackside will support the safe use of other ETCS modes such as Shunting (SH).

Once a movement has been completed the ETCS Trackside shall release locking on the route to enable other movements. This will require exchange of information between the RBC and interlocking.

The ETCS Trackside will interface with other trackside systems such as level crossings, local control systems and fixed staff protection systems.

4.1.2 Degraded mode operation

The ETCS Trackside will support the safe management of trains in the event of failures of the trackside infrastructure or where insufficient information is available for a Movement Authority to be issued. The objective is that the movement of trains is under the authority of the ETCS Trackside wherever possible and hence degraded classes of route will be provided to enable an On Sight Movement Authority to be issued.
In the event of trackside faults, it may be necessary for the signaller to be able to authorise, via the Traffic Management System, the release of route or point locking and the setting of degraded class routes, resulting in a restricted Movement Authority.

The ETCS Trackside will also respond appropriately to scenarios in which the ETCS Onboard is unable to provide complete location or other information, including informing the driver (via the ETCS Onboard) and the signaller (via the Traffic Management System).

The ETCS Trackside will be designed to manage the risks associated with degraded movements, including those where no Movement Authority can be issued. This will include the issue of information to signaller and driver where movements in Staff Responsible are required. This will include the provision of balises with stop messages and ETCS Stop Markers.

The ETCS Trackside will be designed to support movements in the event of GSM-R data communication failures in a single transmission area.

4.1.3 Emergency mode operation

The ETCS Trackside shall support the driver and signaller where unplanned movements need to be undertaken such as the rescue of a failed train.

In the event that an emergency is detected by the signaller, by the ETCS Trackside or by the Traffic Management System, the ETCS Trackside will send appropriate commands to all trains at risk in order to bring them safely to a stand where required.

4.2 The Deployed System

Combined with ETCS (Onboard), the deployed System provides Automatic Train Protection functionality, including speed supervision, and authorises the train to move through the issuing of Movement Authorities. The ETCS Trackside and ETCS Onboard communicate with each other via GSM-R based data services.

There are two functional elements to the ETCS Trackside System. These are:

- **ETCS Trackside (Level 2 No Signals):** The main component is the Radio Block Centre (RBC), which also interfaces with the Interlocking and the TMS, and is supported by a Key Management System (KMS): the KMS supports the management of cryptographic keys for both the ETCS Trackside and ETCS Onboard. To ensure smooth operation along the route of the railway, this system may also interface with another ETCS Trackside (Level 2 No Signals) System, which may be operated by another IM.

- **Interlocking:** This item fulfils a safety-critical function, managing the movement of trains, keeping them apart, and providing control of specific elements of infrastructure. It achieves this through the presence at the lineside of object controllers which are linked to the central interlocking, usually housed within the Rail Operating Centre (ROC). The reservation of safe routes and Movement Authorities can be issued to the ETCS Trackside (Level 2 No Signals). The link between the Interlocking (IXL) and ETCS Trackside (Level 2 No Signals) is described and specified in the DR Ready Signalling Specification [Error! Reference source not found.]. The Interlocking further interfaces to the Traffic Management System (see section Error! Reference source not found. above) and the Signal Controlled Warning System (SCWS). The SCWS provides enhanced warning and protection facilities for staff working at the trackside, giving advanced warning of approaching trains to enable staff to move to a position of safety before the train arrives.

In order to be able to deploy a compliant DR solution anywhere on the GB Rail Network, the baseline version of ETCS that will be used is Baseline 3 Release 2 (BL3R2 – also referred to as SRS v3.6.0), as defined within the Technical Specification for Interoperability (Regulation 2016-919 [RD9]).
The system is supported by balises and ETCS Stop/Location Markers at the lineside.

4.2.1 Business Continuity

Business continuity refers to the ability of the business to absorb perturbations and continue running the service. The level of service can change according to the degree of perturbation. Where applicable, business continuity requirements will be included within the System CRS.

The configuration should minimise the impact of the failure of a single component and enable quick and efficient recovery from failure.

The ETCS Trackside must be able to re-establish the state of the railway from trackside objects and other systems. The ETCS Trackside must store safety critical dynamic data to avoid safety controls being lost in the event of failure.

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 Trackside CRS.

As a minimum the system shall support the recording of all safety critical and safety related communications between trackside objects and the ETCS trackside/interlocking and between the ETCS trackside and ETCS onboards. All recorded communications must be related to a standard time clock.

The system must enable staff to replay sequences of events to establish whether failures have occurred in the system or operational rules have not been observed.

Procedures must be in place for the proactive monitoring of the system to identify potential issues (such as degraded equipment performance) prior to failures occurring.

4.2.3 Training

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

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

- training requirements
- a list of training scenarios

Training for maintenance staff shall cover, as a minimum:

- routine inspection, servicing and replacement of components,
- failure analysis using data recordings,
- safety related/critical failure analysis including preservation of evidence,
- application of temporary controls to enable safe operation in degraded situations or during failure analysis,
- restarting the system and precautions to be taken,
- provide an understanding of the key functions and behaviours of the ETCS onboard.

4.2.4 Deployment Guide

The deployment of the ETCS Trackside will be in accordance with development/deployment guides produced by the Digital Railway Programme.

Deployment will be on the basis of ETCS Level 2 without lineside signals with minimal trackside infrastructure.

Deployment will include other related systems including:
• Traffic Management System – this provides the data regarding temporary restrictions on the speed of trains, the instructions for routes to be set and provides the signaller interface.

4.2.5 Integration Fundamentals Handbook

To help enable successful integration of the ETCS Trackside, DRP will be producing a Integration Fundamentals Handbook for programmes to use as best practice guidance when deploying and integration 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 or from the System. In some cases, the DR SR&I team will be specifying interface requirements for these projects to ensure that they will integrate with the ETCS Trackside.

The critical enablers for the ETCS Trackside are:

• Key Management System – this allocates and distributes the authentication keys, enabling secure communication between ETCS Trackside and ETCS Onboards.

• 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.

• GSM_R Data Radio – this provides the essential communication channel between the ETCS Trackside and the ETCS Onboards. The system requires sufficient coverage and capacity and, where necessary, will need to include General Packet Radio Service (GPRS) capability.

For a brief description of the key enabling systems, see the DRP SOS System Definition [RD5] as they are not repeated here.
5 SYSTEM BOUNDARY

The elements contained within the system boundary are shown in Figure 1 above. As this is a System Definition for a generic System with no specific application in mind, there is no geographic boundary that can be discussed in this section. Geographic 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 Trackside will also interface to other physical systems, as discussed in the following sections.

6.1 Rail Operating Centre (ROC)

6.1.1 Building Interior

The principal systems that comprise the DR infrastructure hardware (TMS, ETCS Trackside, ETCS Onboard, C-DAS) will be housed within a ROC building with supporting lineside equipment (noting that: ETCS also has on-board elements). The building provides space in a secure, temperature-stable environment where equipment can be easily accessed by operational and maintenance staff.

6.1.2 Power Supply

Within each ROC, the systems that comprise the DR system are expected to interface to the existing diverse and secure power supplies which are provided within most ROCs. Appropriate survey activities will need to be undertaken to determine available spare capacity and changes to support deployment, as necessary.

6.1.3 Traffic Management

The ETCS Trackside will be connected to the relevant Traffic Management system(s) to receive commands from both automated and manual routes setting, and to supply information to the signaller.

The connection will be a standard physical communications protocol (to be defined) and utilise a common, open source message structure. These will enable products from different suppliers to be connected.

6.2 Telecommunications

6.2.1 Local Area Network (LAN)

The DR System elements within the ROC will communicate with each other (TMS, ETCS, C-DAS, IXL, Data centre, Safe Track Worker (STW) System) via local area Networks (LANs).

Where safety critical or safety related information is communicated over these networks the information shall be secured against loss or corruption. The redundancy and resilience of the network shall take account of the safety risks and business criticality of the information flows.

6.2.2 FTN / FTN-X

The DR Systems will interface to remote equipment where that equipment has a functional interface via the Network Rail Fixed Telecommunications Network (FTN / FTN-X). This will include communications between adjacent ETCS Trackside installations.

Safety critical or related communications over “open” systems such as FTN will be suitably protected through addressing, authentication or encryption.

6.2.3 GSM-R

The DR Systems will utilise the NR GSM-R network. This will be both for the purposes of voice communication between drivers, signallers and site personnel, and for the transmission of instructions and information between the ETCS Trackside and ETCS Onboard(s).
6.2.4 Data

The NR GSM-R data system will be utilised for communications between ETCS lineside systems and ETCS on-board equipment. The availability (reliability and coverage) of the GSM-R data system 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 data flows demand.

The authentication of data messages between the ETCS Trackside and ETCS Onboard(s) will be in accordance with the subsets of [RD9].

6.3 Lineside

6.3.1 Multi Aspect Signalling (MAS)

Although the DR SoS will not utilise (MAS for any given deployment area), it will interface to MAS at the boundary to facilitate the train's transition from and back to legacy control systems. This will require information to be shared between the interlocking functions in the two areas.

To facilitate the transitions it will be necessary for ETCS fitted trains to connect to the ETCS Trackside in areas not fitted with ETCS. Additionally trains will need to connect during maintenance or to obtain replacement authentication keys from the KMS.

There may be locations where some ETCS movements, such as shunting activities, need to be supported by lineside signals or route set indicators.

6.3.2 Train Detection

The DR SoS will utilise a train detection system to inform the ETCS Trackside of track occupancy. Modifications to the train detection sections on a specific route may be required to enable the operational and performance requirements to be met.

Train detection information will be through an interface with the interlocking function. The interlocking function will, in conjunction with information from the Traffic Management system, manage the reset of axle counters and associated “aspect” restrictions.

6.3.3 Automatic Warning System (AWS)/Train Protection and Warning System (TPWS)

The ETCS Trackside will not interface with AWS/TPWS equipment. The design of interfaces shall be such that any equipment controlled by the non ETCS signalling interlocking can operate correctly taking account of onboard suppression of Class B systems.

6.3.4 Management of Trackside Infrastructure

The ETCS Trackside will control moveable trackside infrastructure, such as points and level crossings, and release of local controls, such as ground frames and staff protection lockouts.

In addition to releases and controls, the status of trackside infrastructure will be monitored by the ETCS Trackside.

6.3.5 Signal Controlled Warning System (SCWS)

The ETCS Trackside will supply information to the SCWS via a standard information interface utilising EULYNX principles.

6.4 Other Physical Interfaces

There will be interfaces with the trackside signalling objects, such as train detection systems and any legacy lineside signalling required, as mentioned above. The DR Programme does not lead to the development of new systems for the existing as-built
infrastructure (e.g. new Level Crossing technology for safe control of level crossings) and it is assumed that these will be developed by National NR/Industry Programmes.
7 FUNCTIONAL INTERFACES

Digital Railway technology interfaces to the high-level functional systems, as described in the SoS System Definition [RD5].

These interfaces will be implemented taking account 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 Trackside will interact with:

- Trackside objects,
- Traffic Management System(s),
- Adjacent ETCS Trackside(s),
- Adjacent Interlocking(s) controlling non ETCS signalling,
- Key Management System(s),
- Configuration Data System(s),
- Staff Warning System(s) – SCWS,
- ETCS Onboard(s) in accordance with [RD9].

7.1 Staff

Discussion of staff within this document is limited to only those staff that will directly interact with the ETCS Trackside System. This is limited to:

- Operational, Maintenance and Response staff,
- Maintenance management,
- Operations Staff
- Train Operating Company (TOC) staff,
- Train Operating Company (TOC) Management and Operational staff,
- Trackside staff,
- Staff engaged in the design and configuration of the ETCS Trackside,
- Installation staff,
- Testing and authorisation personnel,
- Incident and failure investigation staff.

7.1.1 Operational, Maintenance and Response Staff

Maintenance Staff are defined as individuals who are responsible for undertaking engineering activities on railway infrastructure. This includes those that work trackside and, thus, those that may require protection arrangements to be made by the DR System, primarily the interlocking function of the ETCS Trackside, to ensure that they can conduct their work with appropriate safety measures in place.

For the purposes of the ETCS Trackside, Maintenance Staff defined above sit within the system boundary and, as such, appropriate operational readiness activities will have to take place to enable the successful deployment and operation of the ETCS Trackside. This activity needs to include maintenance management and back room support staff. The operational readiness activities should also generate appropriate supporting procedures to allow the staff to operate the System in a safe and efficient manner.

Operational Staff are defined as any individuals who are authorised, competent and responsible for the movement of trains, e.g. signallers, who interface with the DR System as part of their duties. This includes staff that contribute to the safe movement of trains through their role, e.g. TOC platform staff undertaking train dispatch duties. Whilst not within the ETCS Trackside system boundary, the successful deployment of the ETCS Trackside requires those staff to have revised procedures and rules in order to manage the system safely. Appropriate operational readiness activities will have to take place for these staff and all others involved in management of the railway system.

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

The key interface for Maintenance Management is through the staff undertaking the work. For them to effectively discharge their duties they need to have a knowledge of the ETCS system and its interfaces to other systems.

Experience from other countries is that if management and support staff do not understand the principles of the system there can be a breakdown of communication and support.

7.1.3 Operations Staff

The key interface for Operations staff will be via the Traffic Management System. In order for the ETCS Trackside to operate effectively in all scenarios it will require authorisations or instructions from the signaller. These will be transmitted via the Traffic Management System.

The analysis of operations on an ETCS railway has also identified that signallers will require information relating to the ETCS Trackside, this will be displayed via the Traffic Management System.

7.1.4 Train Operating Company (TOC) Station Staff

The key interface for TOC station staff will be via lineside indicators advising them that the conditions have been met for a Movement Authority to be issued and, hence, train dispatch processes may be commenced.

7.1.5 Train Operating Company (TOC) Management and Operational Staff

The management of delays to the service and incidents will be affected by the introduction of ETCS. Part of the signalling system is transferred to the ETCS Onboard and issues may occur within the Onboard, in the Trackside or at the interface between the two.

TOC staff will need to co-operate with Infrastructure Manager (IM) staff in the management of incidents and their investigation. The Delay Attribution process will need to be amended to reflect the new causes of delay.

Both parties (TOC and IM) will need to co-operate to identify failure trends and to resolve issues as part of a DRACAS (Defect Recording, Analysis and Corrective Action System) process.

7.1.6 Trackside Staff

The key interfaces for Trackside staff (part of Maintenance staff) will be the maintenance and repair of trackside assets. This includes:

- Point mechanisms and detection systems;
- Train detection systems;
- Level Crossing systems; and
- Lineside signals and indicators.

In addition to conventional signalling equipment, balises and ETCS signs are deployed at the lineside and will require maintenance.

The significant change is the introduction of Eurobalises which will require routine monitoring and occasional replacement.

The lineside signs become more important, in that they replace signals (principally in degraded scenarios) and the visibility and cleanliness of signs will require more robust maintenance processes.

7.1.7 Staff engaged in the design and configuration of the ETCS Trackside

ETCS Trackside is a computer based system with a set of generic core processes which need to be accompanied by application data and configuration.
The key interface is that errors in the process of establishing the operational requirements of a project and configuring the system can lead to safety critical issues (e.g. omitted controls) or safety related issues (e.g. the system not meeting the operational requirements resulting in degraded operations).

7.1.8 Installation staff

The correct positioning and orientation of balises is vital to the efficient safe operation of the system.

A key interface is for installation staff to understand the criticality of positioning equipment and confirming that the correct units are installed.

7.1.9 Testing and authorisation personnel,

The key interface is that the ETCS Trackside needs to be tested as individual components, as an integrated system, with adjacent systems and with the ETCS Onboard via the GSM-R network.

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

It is a requirement that the ETCS Trackside is authorised in accordance with [RD9] have demonstrated that it meets the user needs and satisfies the conditions for interoperability.

7.1.10 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 such an investigation will include voice or data logs from the ETCS Trackside and other DR Systems, which will be stored in a tamper-proof memory.

Others involved (but not limited to) in Incident Investigations include 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, they are crucial interfaces and provision will have to be made to share data across the industry openly and efficiently for incident investigation.

The ETCS Trackside will include sufficient data recording (with replay facilities) with time stamping linked to a defined source. This will support maintenance and incident investigations.

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 Trackside will communicate with adjacent ETCS Tracksides and with other control systems, including lineside signalling controlled by conventional interlockings.

Where there is a boundary with another communication-based system, such as Communication-Based Train Control (CBTC), bespoke interfaces will be required.

7.2.2 Signalling and Train Control Systems

The DR System will be required to interface to existing legacy command and control systems at the boundary of the DR deployment area, enabling handover of operational services.
Such boundaries will require the information provided to the driver to be co-ordinated such that the safe operation of trains may be achieved. At some locations there may need to be an overlap of signalling systems to support the operational requirements for the system.

Where functionality is achieved differently in Traffic Management and legacy control systems, the ETCS Trackside may need to provide or share different information on a bespoke basis.

7.2.3 Level Crossings

DR deployment schemes requiring interfacing to Level Crossings will need to address issues such as Human Factors, update to the existing Level Crossing control systems, and assimilation of control and indication functions.

The ETCS Trackside may be able to provide information to Level Crossing systems in order to manage the flow of road and rail movements better. The ETCS Trackside may be required to respond to information from the Level Crossing system to control train movements, including issuing emergency commands.

7.2.4 Interfacing Protocols

The interface protocol to the Traffic Management System (or legacy control systems) will be defined by the Traffic Management System. The information to be shared is defined in the Digital Railway Programme – Interface Description Document [RD7].

7.3 Equipment Monitoring Systems

7.3.1 Infrastructure Monitoring Systems

Various types of remote condition monitoring systems are provided to monitor key parts of the railway infrastructure. Some of these systems carry alarm and alerts states that are critical to the operation of the railway.

Where equipped and appropriate, alarm monitoring of trackside infrastructure may form input to the ETCS Trackside, resulting in a safe reaction with regard to Movement Authorities.

Where alternative trackside information systems are available, the ETCS Trackside may utilise these for the management of degraded operations.

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.

The ETCS Trackside utilises a series of Eurobalises as references for Movement Authorities and speed profiles. ETCS Onboards report their positions as an offset from these balise locations. There is a need to convert such reports to a geographical model of the railway used by the Traffic Management System and staff, and to convert information, such as temporary restrictions, entered into the Traffic Management System to the ETCS network model.

7.5 Business Systems

The rail industry relies on a wide range of Business Systems to run its existing operations and the ETCS Trackside will potentially impact on these by developing new
business systems that support the DR implementation of technologies and/or offer additional benefits to the industry (i.e. DRACAS – see 7.1.5).
8 SYSTEM ENVIRONMENT

8.1 Procedures and Rules

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

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

Particular areas of operation affected are:

- Start of a journey, entry of train data and management of indeterminate train location
- Possessions
- Shunting
- Management of infrastructure failures
- Management of train failures
- Train dispatch processes
- Driver training and professional driving principles
- Management of restricted routes

The processes for management of signalling maintenance (e.g. Signalling Maintenance Specifications) will need to be amended or augmented to reflect the additional equipment and changes in functionality.

The processes for investigation of failures and their rectification (including safety critical/related failures) will need to reflect the additional functions and the partial transfer of signalling from the trackside to the ETCS Onboard. This will include the rating of safety related failures.

Processes for the consistent design of ETCS schemes, their development, proving and authorisation will be produced which need to address the legal process of authorisation in accordance with [RD9].

8.2 Staff Competence and Assessment

In line with existing accident investigation recommendations, training facilities will be provided to 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 on any new equipment appropriately and safely, and their competence will require ongoing assessment.

Particular areas to be addressed include:

- Routine monitoring of data logging systems to identify potential issues and signs of system degradation,
- Maintenance and routine renewal of ETCS Trackside components,
- Investigation and rectification of failures,
- Management of safety critical or safety related failures including preservation of evidence,
- Design and testing of ETCS Trackside.

8.3 Security

Appropriate physical and cyber security requirements and arrangements will need to be implemented for the ETCS Trackside. These will be made in the context of the wider NR, NRT and railway industry security and cyber security policies, procedures and provisions.
All ETCS Trackside systems shall be housed in secure buildings with physical security and restricted access. Consideration shall be given to the availability and security of support systems such as:

- Power supplies,
- Communication systems to Traffic Management and other ETCS Trackside within the same building,
- Communication systems to Traffic Management and other ETCS (or non ETCS) Trackside in adjacent areas,
- Communication systems to trackside objects,
- Communication with the GSM-R system,
- Remote access and remote monitoring systems.

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 Trackside will introduce new maintenance requirements.

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

Where possible, common maintenance procedures will be adopted, however it is recognised that individual products may have specific requirements or not provide some facilities.

Prior to entry into service a fully documented maintenance regime shall be authorised by the Professional Head(s) including:

- Routine maintenance tasks and frequencies,
- Component replacement instructions,
- Interrogation of, and extraction from, data recording systems,
- Management of safety related or critical failures,
- Reset and restart procedures,
- Proactive maintenance techniques such as data logger analysis.

The procedures for working on an ETCS controlled railway and the management of operational incidents for use by all railway disciplines and parties will be updated and authorised in accordance with industry practices (e.g. Rule Book, incident investigation processes, delay attribution).

8.5 Local Environment and Conditions

8.5.1 Trackside

The ETCS Trackside comprises systems which will be housed in control centres in controlled environments. The system will connect to other systems at the trackside.

The two “functional” systems are the interlocking and the Radio Block Centre, however it should be emphasised that whilst it is anticipated these will be separate physical entities there is no reason why they may not be combined.

8.6 Trackside Equipment

The ETCS Trackside will be supported by lineside equipment with controls located in trackside locations which are outside the system boundary.

The new or affected systems deployed trackside includes:

- Points – used to route trains, no anticipated change to current practices.
• Train detection – used to detect the location of trains, no anticipated changes to current practices with the exception that aspect restriction following axle counter reset will be through “sweeping” moves utilising degraded routes and On Sight mode.

• Level Crossings – used to manage road/rail interfaces. No changes have been confirmed to date however there may be opportunities for the ETCS Trackside to share information on the location and speed of trains for a level crossing control system to safely combine with train detection to improve the road/crossing user experience.

• Lineside signals – these will be restricted to those locations where it is not possible to provide all the required information to the driver on the DMI, typically for shunting.

• Staff protection systems – used to lockout parts of the signalling system to reserve a work area, these will remain unchanged.

• Staff warning systems – the information for these systems will be available from the ETCS Trackside, principally the interlocking function.

This equipment will be provided with the appropriate power supplies and communication networks, and physical and environmental protection.

DR will place an emphasis on safety by design and remote diagnostics and, where possible, locate trackside equipment in a safe position that does not require trackside working.

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.

ETCS Trackside equipment will be tested for the environment in which it is deployed, the principal equipment being within the ROC.

8.8 Human Factors

For the ETCS Trackside, there is likely to be a significant change to the Human machine Interface (HMI) for the maintainers.

Therefore, ergonomics assessment work will be required to ensure that HF requirements are captured in the DR specifications.
9 EXISTING SAFETY MEASURES

As the CSM RA process is applied to the system, all safety measures and associated requirements will be listed in the Hazard 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 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 the 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]. These are regularly reviewed by Lead Architects to ensure compliance with this System Definition.
Digital Railway

Working together for a better railway: