Digital Railway

Reference	153821-NWR-REP-ESE-000002
Issue/Ver:	6.0
Date:	19 March 2019

Digital Railway – System of Systems (SoS) System Definition

Prepared By
Thulasi Karunakaran
Systems Engineer

TK-190319-0002 Date: 19/03/2019

Reviewed By
David Nicholson
System Integration and Interface Manager

DJN-19032019-0081 Date: 19/03/2019

Accepted By
Rubina Greenwood
Head of System Requirements & Integration

RNG-190319-0071 Date: 19/03/2019

Working together for a better railway:

Department for Transport
Rail Delivery Group
National Rail
NetworkRail
RFG Rail Freight Group
Rail Supply Group
Railway Industry Association
RSSB

Electronic file reference: https://digitalrailway.ipss-hdms.co.uk/DigitalRail/Search/QuickLink.aspx?n=153821-NWR-REP-ESE-000002&t=3&d=Main%5cDIGITAL-RAIL-Production&sc=Global&r=03&i=view

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.

Document owner: David Nicholson, Systems Integration & Interface Manager

Version History

Issue	Date	Comments
1.0	29.05.17	First issue
2.0	1.11.2017	Minor updates and final issue.
2.1	30.01.2018	Update to align with new strategy [RI9]
2.2	23.02.2018	Update after internal review.
3.0	05.03.2018	Updated after review and comments close out.
3.1	25.04.2018	Updates to reflect received AsBo comments, references and minor clarifications.
4.0	27.04.2018	Issued for signature.
4.1	01.11.2018	Updated to align to SoS BoD and System SDDs.
4.2	08.11.2018	Update after internal review.
4.3	12.11.2018	Update after internal review.
4.4	26.11.2018	Update after internal review.
4.5	28.11.2018	Update after internal review.
5.0	29.11.2018	Formal Issue
5.1	25.01.2018	Update after DRIIAT review.
5.2	01.02.2018	Update after DRIIAT review.
5.3	15.03.2018	Update to add exclusion and updated system architecture.
6.0	19.03.2019	Formal Issue

Exclusions

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

1. Best endeavours have been used during the development of this specification to align it to the DR Integrated Concepts of Operations documents. Where the DR SoS SDD does not align to the DR Concept of Operations, issues have been raised and is currently being resolved. Final assurance of the complete alignment of this specification with the relevant industry-endorsed Concepts of Operations will be achieved in a later version.
2. This document has been submitted for Level 3 assurance in accordance with the System Management Plan [RD12]. At the time of publication, no response has been received. Any comments received will be addressed in a future revision of this document.

Assumptions

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

1. None.

Dependencies

These are items upon which the validity of this document depends. Any changes to the dependencies documents [RD1,RD2,RD3,RD4,RD5,RD6,RD7,RD8,RD9,RD10] may require further changes to this document.

1. Comments have been received from the AsBo on v3.0 of this System Definition document [RD6]. No category 1 comments were received; all comments received that required an update of this document have been addressed accordingly.

Contents

ABBREVIATIONS

Abbreviations and acronyms are contained within the DR Glossary of Terms and Abbreviations [RD7]. They are also explained on first use.

REFERENCES

Dependant References

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

RD1. Digital Railway Programme Director's Remit 000000-NWR-REM-MAN-000001, v1.0
RD2. The Common Safety Method for Risk Evaluation and Assessment (CSM RA) regulation, Commission Regulation (EU) 402/2013, 30th April 2013
RD3. The Common Safety Method for Risk Evaluation and Assessment (CSM RA) regulation amendment, Commission Regulation (EU) 2015/1136, 13th July 2015
RD4. Digital Railway – M9 Significance of Change Assessment, 147883-NWR-ASS-ESS-000001, Ver.1.0, 19th February 2018
RD5. Commission Regulation (EU) 2016/919, 27th May 2016
RD6. Assessment Record No.2 – Digital Railway System of Systems (SoS) System Definition, 153819-NWR-COM-ESE-000001, Issue 3.0, 23rd March 2018
RD7. Generic Outcome-Based Business Requirements for Digital Railway Technologies, 000000-NWR-PRG-MAN-000002
RD8. Digital Railway SoS System Architecture, 153819-NWR-DRG-ESE-000003 Issue 5.0.
RD9. Digital Railway SoS Basis of Design, 153819-NWR-REP-ESE-000002, Issue 2.3, 26th of September 2018.
RD10. Control-Command and Signalling TSI Commission Regulation (EU) 2016/91927 May 2016
RD11. Digital Railway Integrated Concept of Operations, 000000-NWR-PLN-MPM-000005, Issue 1.0
RD12. System Management Plan, 153819-NWR-PLN-MPM-000002, v8.0

Informative References

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

RI1. Digital Railway Ready Signalling Specification, NR/L2/SIG/11711, Issue 2, 03/03/2018
RI2. Network Rail – Security Assurance Framework – Procedures, NRT/SY/2015/036, Ver.2.3, 15 July 2016.
RI3. ETCS Baseline 3 GB Onboard Retrofit Subsystem Requirements Specification (EOSS), NEPT/ERTMS/REQ/0007, Rev.3.0, 31st March 2017
RI4. ETCS Baseline 3 GB Onboard New Trains Subsystem Requirements Specification (ENTOSS), NEPT/ERTMS/REQ/0038, Rev.2.0, 31st March 2017
RI5. DR Level A, Generic Hazard Record, 147883-NWR-LOG-ESS-000001, v0.1
RI6. DR System Safety Plan, 147883-NWR-PLN-MPM-000008, Rev.4.0, 07th September 2018.
RI7. DR SoS RAID log, 153819-NWR-REG-ESE-000001, Version 1.0
RI8. Digital Railway – System of Systems Realignment Strategy, 153819-NWR-STR-SSD-000001, v1.0, 27th November 2017
RI9. Commission Regulation (EU) 2016/919, CCS TSI (as amended)
RI10. Digital Railway, Capability Maturity Model and Programme Capability Report, DRD-PH3-MSP2-TAD-000000-DEL-160503-182456, v1.1, 3rd May 2016
RI11. Digital Railway Traffic Management System Definition Document, 153821-NWR-REP-ESE-000004, v2.0, 30th November 2018
RI12. Digital Railway ETCS Onboard System Definition Document, 153821-NWR-REP-ESE-000005, v2.0, 26th November 2018
RI13. Digital Railway ETCS Trackside System Definition Document, 153821-NWR-

REP-ESE-000006, v2.0, 27th November 2018

RI14. Digital Railway C-DAS System Definition Document, 153821-NWR-SPE-ESE-000009, v2.0, 26th November 2018

RI15. Digital Railway – Glossary of Terms and Abbreviations, 153819-NWR-SPE-ESE-000001

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 main benefits of the Digital Railway are expressed as:

- Improved capacity
- Better connectivity
- Improved performance
- Improved safety and security
- Increased network availability

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 as [RD1] and articulated in [RD8].

This is an industry-wide programme involving Network Rail (as Infrastructure Manager), Train and Freight Operating Companies (as Railway Undertakings), 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 outcomes. These are:

1. Creation of a generic customer requirements for deploying Digital Railway (DR) Systems (using European Train Control System (ETCS) Level 2, Traffic Management (TM), Connected Driver Advisory System (C-DAS) and for interfaces with other systems and enablers).
2. Preparation of business cases that provide input to Route strategic business plans for deployment projects using specific applications of DR Systems.
3. Assisting deployment projects to deploy specific DR Systems as a result of the Business Plan work undertaken in 2 above.
4. Production of guidance notes, rules, processes and templates to help deployment projects. Where remitted, DR will provide support to deployment projects in determining the deltas between the DR System of Systems (SoS), DR System items and their particular deployment.

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 (TM), C-DAS and other systems and enablers).

System of Systems (SoS) refers to the aggregation and integration of the DR Systems in a baseline architecture to enable the full benefits of the digital technologies to be realised.

Both terms include more than just the systems themselves, but also the people, processes and data required to enable operation.

Within the DR Programme, the System Requirements and Integration (SR&I) team is responsible for producing the outputs 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 (CSM) on risk evaluation and assessment (CSM RA) came into full effect through Regulation 402/2013 [RD2] and 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 significance impact on the operation and organisation of GB rail. A formal assessment of the significance of the

change has been undertaken [RD4] and 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 Regulations is the preparation of a System Definition i.e. this document. The purpose of the System Definition document under CSM RA is to complement the hazard record by bounding the scope of the hazard identification and risk assessment process and 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 defines what is meant by 'System of Systems' and 'System' and its interfaces to ensure successful requirements apportionment. This will result in minimizing integration risk during deployment. This System Definition document will fulfil that need of defining the system, its interfaces and thus minimize integration risks.

The System Definition defines the key details of the baseline System of Systems, its purpose, functions, interfaces and the existing safety measures that apply to it, so that it provides a generic design in support of subsequent development and deployment (i.e. application-specific design and implementation). It also allows the generic specification and design for the SoS and Systems 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 too.

This document has been written to support a high-level understanding of the DR SoS and is also intended to support the early stages of hazard analysis of the proposed solution.

1.4 Scope

This document applies to the outputs of the SR&I team only as listed in section 1.2 above.

These generic requirements only consider the deployment of the core Systems as a SoS and does not consider how a particular section of the railway might operate if only some of the systems are deployed. Any variation from a full deployment of the SoS as described in the DR SoS System Architecture [RD9], 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, or migration stages in the deployment of the core Systems; it deals with the generic SoS design (in its end state) and its associated interfaces (both physical and non-physical (e.g. operators)).

This document does not describe in detail the Systems upon which it is dependent (e.g. ETCS, TM and C-DAS) as they have their own System Definitions [RI11RI12, RI13, RI14, RI15]. The SoS System Definition document must be read in conjunction with the System SDDs to understand the full functionality of the individual DR systems and how they interface with each other within the SoS architecture to achieve the key high level SoS functions. This SDD concentrates on outlining the high level SoS functions that the DR systems collectively deliver as described in detail in the DR SoS Basis of Design document [RD10]. This document has been aligned to the DR Integrated Concept of Operations where possible and where there are differences, it will be resolved by DRP and any consequential agreed changes will be captured in an update to this document in due course.

1.5 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).

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

- ETCS Trackside, incorporating equipment trackside for Level 2 (no signals), modern interlocking technologies, and all trackside equipment necessary for fitted trains running elsewhere on the GB rail network
- ETCS Onboard[1]
- Traffic Management
- Connected-Driver Advisory System (C-DAS)

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 and Key Management
- Operations and Maintenance framework to support the people and process change required
- Timetabling to support the system capacity planning process change required
- LINX

The SoS configuration ensures that the systems within it, e.g. the European Train Control System (ETCS), Traffic Management (TM) etc, 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.

The SoS configuration will be supported by the production of a series of guidance notes, rules, processes and templates to help a specific delivery project to deploy DR Systems.

1.6 Document Maintenance

This System Definition Document is owned by the Systems Integration & Interface Manager. It will be subject to review at least prior to any required stage gate to ensure its ongoing adequacy for progressing to any future stage gate. Other updates may be instigated as necessary when directed by the Head of Systems Requirements and Integration.

This document has presumed a particular baseline technical solution as outlined in the Realignment Strategy [RI9]. 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 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 as needed. All the safety requirements identified from the hazard identification (HAZID) activities and other emergent safety requirements will be managed in the master DOORS database and included in the relevant DR System Requirements specification with a safety related requirement tag to denote it as a safety requirement. Where the HAZID activity identifies a safety functionality this will be updated in the appropriate DR System SDD as needed. The DR SoS SDD is an overview of the high-level functionality of the DR Systems and it is not envisaged that the HAZID outputs will be included in this SDD.

[1] It should be noted the Control-Command Signalling (CCS) Technical Specification for Interoperability (TSI) [RI10] requires that the onboard elements of ETCS supports all ETCS levels, not just Level 2.

2 SYSTEM PURPOSE AND OBJECTIVES

The principal objectives of the DR SoS generic design are to:

- Provide the requirements to allow a successful deployment of an integrated and standard train command, control and safety system on GB rail to deliver the objectives mentioned in 1.2 which includes:
  - Traffic Management System;
  - Connected-Driver Advisory System;
  - ETCS Trackside, incorporating equipment trackside for Level 2 (no signals), modern interlocking technologies, and trackside equipment necessary for fitted trains running elsewhere on the GB rail network
  - ETCS Onboard
- Provide the framework to enable delivery of the Digital Railway Vision and to ensure that all DR delivery activities are aligned against a common understanding and baseline architecture (i.e. maintenance, operations, engineering, people and process etc);
- Provide a foundation (through a common reference data framework) for enabling the systems to be configured and optimised to support the DR technologies;
- Automated control of train paths derived from a planned timetable;
- The safe movement of rolling stock;
- An enhanced safety environment for workers on or about the running lines;
- Increased service reliability and the potential for increased capacity and performance (subject to the specifics of the deployment);
- Secure transmission of command-control information (i.e. KMS).

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 systems and to maximise benefits gained.

After the creation of Customer Requirement Specifications (CRSs) and DR Requirements, application-specific requirements would need to be created so that the DR technologies could be applied to the specific route. Following this, there may be a supply chain development and integration stage for the systems concerned (e.g. TM, ETCS and C-DAS) and the use of test facilities (e.g. suppliers' own test facilities, ERTMS National Integration Facility (ENIF) and Railway Innovation and Development Centre (RIDC)), prior to actual deployment on the operational railway.

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 SoS functional architecture. The diagram shows the Infrastructure and Rolling Stock Systems and their functional inter-relationships.

Generic roles that are integral to the SoS architecture are presented, but these are currently shown in grey as the interfaces between these roles and the Systems are still to be defined. Similarly, interfaces for the Infrastructure and On-board data hub have been omitted pending their development and review by subject matter experts. The architecture is not intended to be read as a physical relationship diagram. A number of Enhancing Facilities and Required Enablers are shown where these directly enable or interface to one of the DR Systems.

Further details of the interfaces shown and the information flowing over them are covered in the document Digital Railway SoS Architecture [RD9].

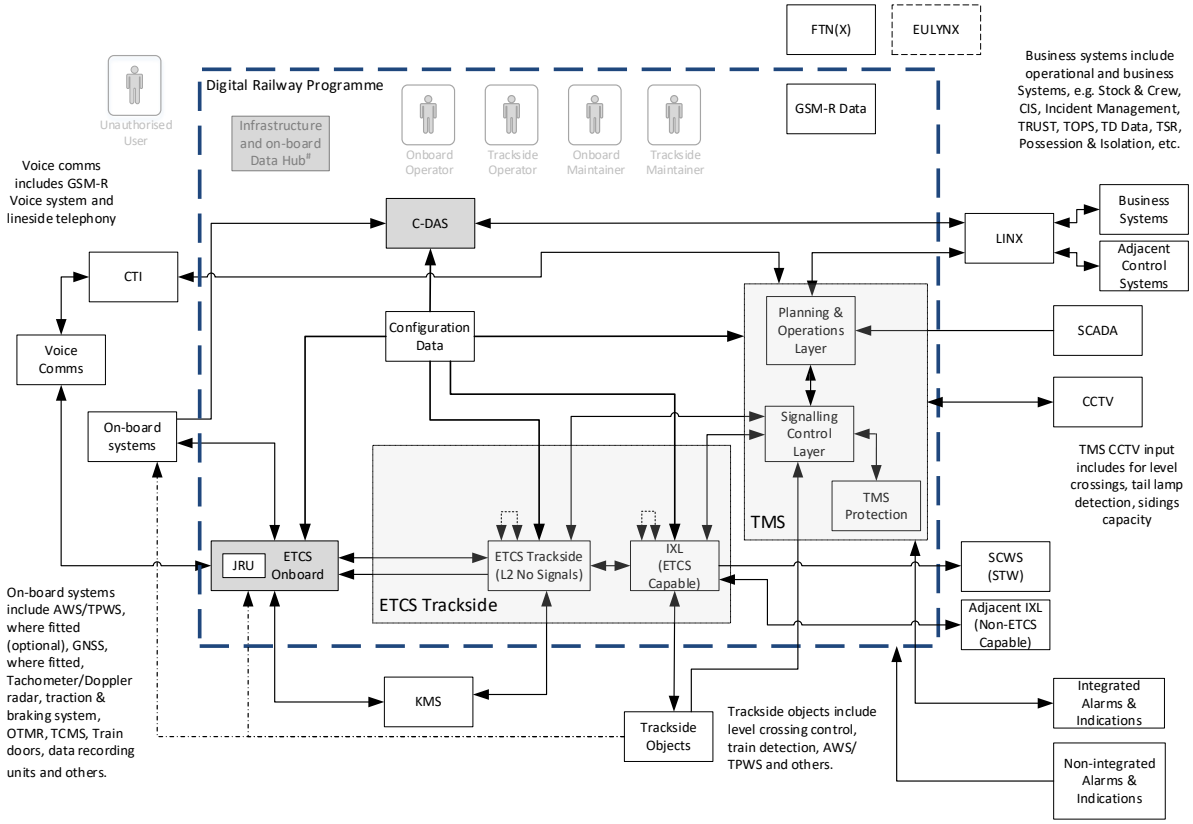

Figure 1 –DR System of Systems architecture

3 SYSTEM OF SYSTEM FUNCTIONS AND ELEMENTS

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

The following are considered essential SoS elements to support deployment:

- Traffic Management (TM), ETCS Trackside, ETCS Onboard and C-DAS (note these are covered by their respective SDDs [RI12], [RI14], [RI13], [RI15])
- Operations and Maintenance
- Enabling Projects (e.g. GSM-R upgrade, Timetabling update, National KMS)

Note that the Operations and Maintenance elements associated with each DR system will be included in the appropriate DR system SDD and will not be provided as a separate SDD.

3.1 DR System of System Operation

The DR Integrated Concept of Operations [RI5], produced for the System of System and its individual DR Systems, will provide greater detail on the SoS operation and the functionality required to deliver the end user needs. However, this section is included to provide a brief summary of how the DR SoS typically operates to aid understanding of other sections of this document.

The high-level functionalities that the SoS will achieve are listed as follows:

- Common reference data
- Safe movement of train
- Optimise the plan
- Service Information for Users
- Safe management of workers
- Service delivery to optimised plan

The DR SoS will support operation in normal, degraded and emergency modes, although the latter two will depend on the cause and scale of the degraded or emergency mode of operation. Regardless of mode, the systems, supported by processes and rules, will ensure adherence to the four fundamental signalling principles of:

- **Safe Spacing**: A train is given a route that is clear of other trains;
- **No Excess Speed**: A train will operate within the speed limits currently in force for the route and train;
- **Route Holding**: The route, once given to the train, is not revoked or altered without some form of assurance that the train is not to make use of that route;
- **No conflicting moves**: The route offered to a train is clear of any other route offered to other trains

The method by which the signalling principles are addressed by SoS will be defined by the DR SoS BoD [RD10].

The following sections describe the functions provided by the SoS, and then describe operations in normal, degraded and emergency modes.

3.1.1 System of System Functions

The SoS functions[2] have been developed in the functional architecture model through a series of Scenarios and Uses case workshops with the engagement of industry stakeholders. The SoS functions being delivered by the DR Systems are articulated in detail in the DR SoS Basis of Design [RD10] are categorised underneath the high-level functionality groupings and listed below (additional functions may yet be identified):

[2] These are extracted from the Enterprise Architect tool used for modelling the SoS Functions. In this tool, these are known as Processes.

3.1.1.1 Common reference data

- **Train Preparation**: Prior to safe operation of a train, the train needs to be configured for the current signalling system. This process involves getting information such as train identity and configuring any required equipment for use. This scenario ends when the train is ready for operation by the driver. Some of this information may require a high degree of integrity.
- **Manage train service data**: Service data is associated with each running train. This includes information such as the train identifier and consist information. This information must be entered prior to a train starting a mission but could be updated at any point. Once entered or updated, this information is then published to interested parties. Some of this information is essential for the train operation.
- **Monitor Digital Railway Health**: Digital Railway system health is monitored to ensure operational safety of the railway. Status information is collected and reported allowing improved operational decision-making including analysing long-term trends, and performance analysis. Potential issues that will prevent the system from operating i.e. latency, system unavailable, errors and saturation.
- **Provide Information to Planning:** Provide the timetable planning function with feedback regarding conflicts within the supplied timetable and actual train movements against the previous day's timetable. This scenario triggers when a new daily timetable is received.
- **Infrastructure Preparation:** Prior to safe use of the infrastructure, the DR trackside elements need to be configured to match the geographic, signalling and operational characteristics. This process involves getting information such as track layout, operable routes and configuring any required equipment for use. This scenario ends when the infrastructure is ready for control by the signaller. Some of this information may require a high degree of integrity.

3.1.1.2 Safe movement of train

- **Safely command a train**: Following the receipt of a control request, this performs the appropriate network operation(s) to allow safe train movements through the use of authorised Movement Authority control messages. **This provides an appropriate safety integrity level for safe movements across the** network. It does not necessarily mean a train will move or a train is even present.
- **Safely operate the train**: Physically operate and move a train between two locations in a safe way. Safe train movement is the responsibility of the driver, using the movement authority and conforming to the rule book.
- **Identify train and location**: Continually determine and publish each train's identity and current location to allow the network to be effectively operated.
- **Interface with mainline entrance/exit**: Once the need for co-ordination with depots, sidings or other third-party infrastructure has been identified, the signaller must ensure that arrangements are made and agreed to (with the interfacing or adjacent signalling control areas), before updating the current plan with any resulting changes.
- **Train Dispatch:** Enable the dispatch personnel with responsibility for train dispatch to safely dispatch the train using the appropriate information. Additionally, provide additional capability to manage Right Away (RA).
- **Transfer Signalling Control:** An area of control needs to be transferred to another signaller, who may well be physically located in a different control centre. This is a "pull" activity, in that the signaller willing to take on the additional area of control initiates the transfer. The actual transfer process should not impact railway operations and typically occurs when a signaller finishes work.

3.1.1.3 Optimise the plan

- **Optimise current plan**: When the current plan is no-longer achievable within the agreed tolerances, it performs a re-plan based on the latest available information and utilising the current objective function. This activity optimises the proposed plan to achieve the desired outcome (e.g. maximum capacity, recover to the original timetable, etc.). Once optimised, the proposed plan is then agreed by relevant parties and published to all concerned systems as the new "current plan".
- **CCS Failure:** Safely operating the Digital Railway System in the event of Service affecting faults and failures of a Digital Railway system or enabling technology. The Digital Railway system continues to operate safely in a restricted manner
- **Control Centre Failure:** Safely operating the Digital Railway System in the event of building fault. Service affecting faults and failures relating to the operating centre building (e.g. ROC) such as power failure, evacuation, terror attack or staff unable to reach work. The Digital Railway system continues to operate safely in a restricted manner
- **Emergency:** Digital Railway system safely dealing with an emergency – For example, a fault or incident which results in a situation where it may be unsafe for trains to continue to the end of already issued movement authority. An unforeseen situation has occurred which endangers life and property requiring immediate action from the Digital Railway System.
- **Infrastructure Fault:** Safely Operating the Digital Railway System when an Infrastructure fault occurs. Service affecting faults and failures relating to the rail infrastructure such as those affecting train detection, points and track. The Digital Railway system continues to operate safely in a restricted manner. Once the fault is corrected, an update is made allowing the system to remove restrictions and optimise the plan to begin recovery of service.
- **Train Based Fault:** Safely operating a train with a fault. Train based faults and failures which affect the operation of a train. These include on board failures such as broken window, DMI failure or network communication failure which may allow restricted movement. Alternatively, other train-based faults such as a freight train being routed towards a bridge with an un-suitable weight limit – essentially providing a train blockage. The Digital Railway system continues to operate safely in a restricted manner. Once the fault is corrected, an update is made allowing the system to remove restrictions and optimise the plan to begin recovery of service.
- **What if Analysis:** At any point the signaller can create a "copy" of the current state of the live railway in order to create a potential plan update. This allows the signaller to make potential modifications to the timetable and have the Digital Railway System provide information regarding the conflicts that would be created and the impact to trains. These updates can then be committed or discarded.
- **Manage Crew and Stock information:** TOCs and FOCs can provide the latest Crew and Stock resource constraints (e.g. a driver constraint on what routes they may be able to drive, due to route knowledge). Following receipt of a change to these constraints the "Optimise Current Plan" function is triggered to ensure these constraints are taken into account in the current plan.

3.1.1.4 Service Information for Users

- **Provide information to driver**: Following an update to any element of information relevant for the driver (such as movement authority, advisory speed, current speed, train operation mode etc.), and provide that information to the driver in a timely manner. This information is used by the driver.
- **Provide information to the signaller**: Continuously provide the signaller with the latest operational network information and the current plan. This allows the signaller to either effectively supervise or perform the Operate Network to Current Plan function.

3.1.1.5 Safe management of workers

- **Possessions Planning**: Plan access to a track area with the appropriate timetable changes.
- **Managing Possession**: Takes control of an area or zone to enable access and working for a specified time. Persons in Charge are responsible for possessions zone. Prevent unauthorised train movement into a possession. The TMS will support the granting and taking back of possessions remotely. The TMS protection will interact will the other systems within DR SoS as appropriate and allow the signaller to grant and take control of an area of zone.
- **Short notice possessions**: Unplanned event requires an immediate response involving short notice works.
- **Signal Control Warning System**: Detect a train entering a 'warning area' that includes a safe track working site. Alerting all track workers when train movements could impact safe track working. High integrity system(s) maybe required.

3.1.1.6 Service delivery to optimised plan

- **Operate the network to the current plan**: Requests that routes are set in the correct order and at the correct time to allow trains to move across the network safely in order to fulfil the current plan.
- **Manage incidents**: This can trigger at any time when the external incident management system determines CCS activities need to take place. Upon receipt of a task from the incident management system this function steps though a sequence of activities. This optionally provides confirmation that each step has been done in the correct order, before notifying the incident management system of completion. For example, in the event of a station closure, this may involve terminating some services short and re-planning other services. Following completion of the actions, the optimise plan scenario should run to update the plan to take any new perturbations into account.
- **Optimise train movement**: Following the generation of a movement authority, the actual train movement from its current location to the end of the movement authority is optimised. This is performed in line with the current plan and an objective function resulting in a speed profile for the train being created and published. This speed profile aims to ensure the train arrival time will be achieved in line with the current plan. This ensures the objective functions of the railway (e.g. efficiency / throughput) are achieved. When the planned arrival cannot be achieved, provide a notification to relevant parties. The responsible body/system must ensure the safety of this speed profile during the "safely operate a train" scenario.
- **Monitor train movements against the current plan**: Using available information, monitor train movements across the rail network against the current plan, to ensure movements remain within the agreed tolerances. This includes monitoring that routes are set when requested and train movements remain on schedule. Network availability needs to be monitored to detect any failures or potential issues that will prevent the current plan from being implemented within agreed tolerances (e.g. a late arriving terminating train used to start a new service will not be able to leave on time).

3.2 Modes of Operation

The DR SoS will function in normal, degraded and emergency modes.

The DR SoS is characterised as made up of three main constituents which are namely people, systems and processes. By people we mean the users of the DR SoS and are defined as falling in two categories which is Operational Staff and Maintenance Staff. The Operational Staff and Maintenance Staff are further defined below.

Operational Staff are defined as any individual who is 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 contribute to the safe movement of trains through their role, e.g. TOC platform staff undertaking train dispatch duties, Drivers who are responsible for the safe operation of the trains.

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

For the purposes of the DR SoS, the two groups 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 DR Systems. The operational readiness activities should also generate appropriate supporting procedures to allow the staff to operate the DR deployment in a safe and efficient manner.

Interfaces to the DR systems, shall be procedural or technical. The key interface for Operations staff based in the ROCs will be the Traffic Management system. Through the TM System the Operations staff will be able to control ETCS Trackside (including the IXL) and C-DAS. The key interface for Drivers will be the ETCS Onboard and C-DAS. The Maintenance staff will interface with all the DR systems as needed.

3.2.1 Normal operation

3.2.1.1 Optimising the plan

Normal operation will see the TM system import the timetable – the 'agreed plan' - ahead of the day's operations and check it against other available information acquired from the national business systems and other systems such as stock & crew for errors, omissions and conflicts so that these can be addressed ahead of the implementation of the plan.

The Traffic Management System will then use the Current Plan or Forecast plan (beyond the first unresolved conflict) to automatically request routes in a timely manner for all of the trains in its area of control. These requests will be sent to the interlocking which will set routes for those requests that can be actioned, rejecting those that would create conflicting train movements. The ETCS Trackside (L2 No Signals) system will receive a state of the railway from the interlocking on a regular basis which it will use to create the appropriate Movement Authorities (MAs) for the trains within the area of control. Once an MA is issued, the route for the authorised movement will be exclusively reserved until it is safe to release it.

Traffic Management will acquire changes from operational systems as they occur and will support management of events that perturb the delivery of the train service as they happen. Thus, the Current plan for the day's service is dynamically updated with changes to ensure continued train service delivery, wherever possible, in spite of service affecting events.

3.2.1.2 Speed restrictions

Traffic Management will also support the imposition of speed restrictions (as established by an external system outside of DR's scope) and the granting and taking back of possessions remotely. In both cases TM will interact with the operator, and other elements of the DR Systems as appropriate. For speed restrictions as these are applied and removed by an external business system the TM system will disseminate that information to the ETCS Trackside (L2 No Signals) system.

The ETCS Trackside (L2 No Signals) system will take account of any speed restrictions in place as part of its assembly of the MAs sent to the trains in the area of control, thus the speed restrictions are enforced by ETCS for ETCS fitted trains.

3.2.1.3 Shunting/Splitting/Joining

Where shunting needs to take place, the system will not unduly restrict the activities whilst providing appropriate levels of protection to the shunting activity and other train movements.

Trains can split and join as the operational need arises.

3.2.1.4 Possession management

For possessions, the TM system includes a function to provide appropriate protection for lineside staff, locking out the area of track for normal train operations. Lineside staff will be able to interface with the TM through remote possession facilities. Once lineside work is complete, and the railway is in a safe state, lineside staff can request that the possession be handed back to the signaller. A possession will not be removed unless a request is made, and the signaller approves it. The request is made electronically, via remote access. Possessions can be handed back in stages requiring multiple authorisations in cognisance of the risks it poses.

3.2.1.5 Driver machine interface

The Driver will see the MA for the train and other relevant information on the ETCS Driver Machine Interface, as a result of the ETCS on-board system supervising the train's movement based on the received MA from the trackside system. The driver also presses the 'START' button on the ETCS DMI which results in a movement authority request being sent from the ETCS onboard.

Also available will be the advisory speed from the C-DAS system, reflecting updated information received from the trackside element of C-DAS, which is itself receiving updates to the plan and permissible speeds from the TM system as they occur. TSR updates are received by the TMS over LINX from an external system. The driver will use the onboard displays to inform their driving of the train. C-DAS and ETCS onboard systems will not display conflicting speed information, i.e. different maximum speeds will not be displayed on C-DAS and ETCS onboard.

3.2.1.6 Voice communication

The facilities of the GSM-R voice radio system will continue to be available to the driver as they are today.

3.2.1.7 Lineside staff safety

Lineside staff will be warned of approaching trains through an external Signal Controlled Warning System (SCWS) which interfaces with the Interlocking.

3.2.1.8 Train dispatch

At the platform, staff involved in train dispatch will receive indications, and may be provided with controls where appropriate, to assist them in the dispatch of train services.

3.2.1.9 Data logging

Various elements of the on-board and trackside systems will record their respective interactions and operations throughout their service day to support post service analysis, incident investigation and maintenance.

3.2.2 Degraded mode operation

The degraded modes are somewhat more difficult to summarise simply as Digital Railway is a system of systems and thus degraded modes are more complex. That being said there are clearly two types of degraded mode, one that affects individual DR Systems and those that might affect the overall SoS.

The approach to business continuity will address some of the degraded mode operation, as will the provisions within the proposed ETCS deployment design for degraded routes and methods to address GSM-R base station failures.

ETCS supports various levels of train supervision according to any degraded situation. This ranges from a fully supervised train movement with automatic train protection provided, through to driver-supervised train movements using verbal authorities from the signaller.

The system will provide technical solutions to manage degraded modes where these are practicable with the sole use of operational rules being non-preferred.

3.2.3 Emergency mode operation

Emergency controls, indications and functions exist across the DR SoS and all of these will work together to create consistent and coordinated responses to emergency events. For example, the TM operator could assert a function that would cause the associated ETCS Trackside (L2 No Signals) system to revoke all movement authorities within a specific area of infrastructure, and to adjust those for trains approaching the affected area. Additionally, speed restrictions can be applied consistently across the DR SoS to address specific issues.

An alarm management strategy will be developed to ensure a consistent and standard approach will be adopted for DR SoS. All safety functions across DR SoS will be assessed and have a Safety Integrity Level (SIL) assigned to the safety functions to ensure they mitigate the safety risks according to the required SIL targets.

3.3 DR System of System Deployment

3.3.1 Performance, Reliability, Availability and Maintainability (PRAM)

The PRAM targets for the DR SoS has not been developed to provide generic targets that the DR systems need to collectively achieve, and consequentially the individual targets that each DR system has to achieve. There has been work done by others (outside the DRP) for instance on the ETCS L2 to define minimum reliability targets that are to be achieved as a standard when ETCS L2 is deployed, but this has not been formally endorsed yet. The PRAM targets will need to be determined by the individual deployment projects for their specific deployment project.

Business Continuity is the ability of the business to absorb perturbations yet still deliver the service. The level of service can change according to the degree of perturbation. Business continuity requirements will be included where applicable within the SoS CRS.

3.3.2 Data

One of the core capabilities and an integral part of delivering the SoS and its systems 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, Process & Technology. The DRP will be delivering data and data management requirements for the SOS CRS and the system CRSs.

3.3.3 SoS Deployment Guide

The Digital Railway Programme is responsible for producing a deployment guide that will facilitate the implementation of the outputs i.e. specifications and guidance material to assist Deployment Projects in deploying DR Systems.

In addition to DR systems, there will be a need for the industry to develop the following to realize the full potential of deploying Digital Railway Systems:

- **Configuration data:** At each location where DR Systems are 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.
  It is expected that there will be a Test Yard (i.e. an example of a typical track layout) that will be used as a test bed as part of a deployment's system

development and integration activities (e.g. at ENIF and supplier's own facilities) and this will require configuration data.

- **Maintenance Procedures:** The new functionality provided by the Digital Railway Systems 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 various the Systems and on the SoS as a whole.
- **Maintenance tools:** DR Systems will assist maintainers in predicting and identifying faults. Maintenance tools will enable maintainers to predict, identify and rectify faults in the various DR Systems. An assessment on the maintenance impact of all the component parts is to be undertaken and national/industry level ownership and definition is to be defined.
- **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 do this on a live system. Typical training material includes simulators, videos, presentations and course notes.

3.4 External Systems

These are systems that are deemed as being outside of the DR Programme but are dependencies either to or from the DR programme. In some cases, the DR Programme will be specifying requirements for these projects in order to use their outputs.

Some of these projects may be being delivered by other parts of the Digital Railway Group (e.g. GSM-R), some are National Programmes (that may or may not be funded by Digital Railway) and others may be being delivered by external parties.

It is assumed for the purposes of the DR Programme that the Digital Railway Programme will:

- Provide interface specifications for these projects;
- Ensure that the maintenance strategy for the interfacing projects align with the SoS maintenance strategy;
- Promote consistent alarm management system across the projects and Service Level Agreements (SLAs) support arrangements to be agreed with maintenance;
- Get outputs from these projects that will be used to support SoS integration and test and/or deployment (e.g. systems for test);
- Share lessons learned with these projects.

If at a later stage, one or other of these programmes is moved within the scope of the DR Programme then this will be change controlled into the Integrated Programme scope.

The systems are categorised as either being an enabling system for DR SoS (i.e. the system is needed for DR SoS to function as intended) or is a dependant system on DR SoS (i.e. the system needs DR SoS to enable it to function as intended).

3.4.1 DR SoS Enabling Systems

3.4.1.1 Key Management System

The DR System of Systems requires safety critical communication between some of its different systems using open communications and for ETCS (SIL 4), this open communication must be authenticated and secured to comply with European Legislation.

A key management system allows communication across the open interfaces to be secured and authenticated using key encryption.

Both ETCS Trackside and ETCS Onboard Systems need the deployment of a KMS to ensure that the security requirements are met for the overall system, therefore this is a critical system for DRP.

3.4.1.2 Crew & Stock System

This is an external system which will interface to the Traffic Management System. The provision of information over this interface is determined by individual deployment projects.

Crew and Stock system is a decision support tool used in real time to support that the right resources are in the right place at the right time. It combines data from the train service and its actual running diagram and resource information and their associated rolling stock allocations and crew rosters. Data can be interfaced from a wide range of industry and local systems and can also be manually input (dependent on the Crew and Stock system concerned). Dependent on commercially-sensitive access arrangements, it can also allow industry collaboration during times of disruption.

3.4.1.3 Timetable Planning

Digital Railway will be specifying requirements for improvements to the current timetable to maximise the benefits from DR technologies and this project will deliver the Timetable change required to support these Digital Railway requirements.

3.4.1.4 Other Comms: Wireline Comms (FTN(X)) & Wireless Comms (GSM-R)

The backbone of Digital Railway will be the ability to share data and issue command and control instructions. Two basic forms of communications are the wireline communications (using FTN/FTNx) and mobile communications (using GSM-R).

The requirements for communications systems will be of two different forms:

1. Need for particular technologies (e.g. GPRS)
2. Performance requirements (e.g. bandwidth, call channels, protocols…)

Digital Railway will write communications requirements for an interfacing project to provide new/upgraded communications on the mainline and at the test centres.

To address capacity/availability/coverage issues arising from the deployment of ETCS, NRT will be required to upgrade parts of the network to meet this requirement. GSM-R obsolescence is being managed and Future Railway Mobile Communication System (FRMCS) is the proposed replacement for GSM-R. Specifications are currently being developed with implementation anticipated from 2022 onwards.

It is assumed that the delivery of this work will be delivered by a third party (e.g. NRT).

3.4.1.5 Layered Information eXchange (LINX)

LINX is an enterprise service bus architecture that can be used to provide other systems (e.g. TM) with a consistent well-defined set of information services. It can provide an interface between TM, C-DAS and existing business systems (e.g. TOPS, TRUST etc) and an interface between multiple TMs and it performs data conversion to allow different systems to provide data from one to another. Every deployment of TM requires additional interfaces to and from LINX and therefore LINX will require some development work for every deployment until it delivers it's entire catalogue of services.

3.4.1.6 EULYNX

This is an initiative of a number of European Infrastructure Managers (IMs), including Network Rail. The project aspires to a mutually shared vision toward harmonisation of rail signalling systems, their technical architecture, its functions and interfaces. The work breakdown structure of the EULYNX project includes items like system architecture,

modelling & testing, data preparation, interfaces between interlockings, interfaces to train detection and adjacent interlocking or signalling subsystems. The outcome will be a de facto standard associated with interfaces between various components of the Command, Control and Signalling System. It requires significant stakeholder and supply chain buy-in (some of whom are not within Digital Railway's remit to manage) and is a key enabler for system integration.

The use of EULYNX within the SoS is proposed for the interface between the interlocking and SCWS only. While assumed included at this point, its inclusion is subject to further discussion and development.

3.4.1.7 Business Systems Development

Deployment of the SoS or any of the core Systems may impact on the business systems and therefore to enable successful integration there may be a requirement to:

- Interface to existing IT systems (NR and external) via LINX (e.g. TOPS, TRUST etc);
- Modify existing IT systems;
- Develop new business systems that support the DR implementation of technologies.

At the present time, to enable deployment, a Central Temporary Speed Restriction (TSR) planning and implementation tool and a possession planning system has been identified.

3.4.2 DR SoS Dependant Systems

3.4.2.1 Customer Information System (CIS)

This is an external system to TM which will interface to the Traffic Management System. The provision of information over this interface is determined by individual deployment projects.

This is a customer facing system which provides operational information taken from other railway systems that has been converted into a format that is easily understood by customers (e.g. passengers, freight users). CIS feeds information that is displayed on the electronic arrival and departure screens and displays that can be found on many GB railway platforms.

3.4.2.2 Signal-Controlled Warning System (SCWS)

This is an existing National programme that is delivering a Track Worker Warning System to the industry and is critical to achieving the safety objectives of DRP.

The high integrity Signal Controlled Warning System (SCWS) provides an additional safe system for Track Workers to undertake appropriate non-intrusive inspection and maintenance activities.

It includes a centralised unit in the ROC and portable systems used at the trackside by staff, with telecommunications between the central and mobile unit. The central unit also connects to the Interlocking in order to receive railway state messages in order to function.

3.4.2.3 Incident Management System

This is an external system which will interface to the Traffic Management System. The provision of information over this interface is determined by individual deployment projects.

Incident Management is a decision support tool that can help reduce the impact an incident has on the rail network across the whole incident lifecycle, however the biggest delay minute saving that the tool will have relates to the initial period of an incident and improving the time taken to get required resources to site, and is achieved by:

- Faster identification of incident location;

- Faster access to supporting data (access points etc);
- Targeted communication to those that need it, when they need it;
- Optimising resource utilisation;
- Standardised workflows providing continuity of incident activities and ensuring all key steps are taken at the correct time; and
- Improved information flows from site to control.

4 SYSTEM BOUNDARY

The elements contained within the system boundary are shown in Figure 1 above.

Within its functional system boundary, the SoS includes the people, data and logical systems. The DR System Architecture [RD9] provides an overview of the information and protocols associated with functional interfaces with adjacent logical systems.

The elements contained within the system boundary are shown in Figure 1 above.

4.1 Geographic Boundary

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.

4.2 SoS Configuration

The DR SoS configuration is as described in Figure 1 –DR System of Systems architecture. This is the generic end state architecture for the DR SoS and any variations or migration states to the aforementioned DR SoS configuration is outside the scope of this document. All different migration and configuration states of the SoS will need to be assessed and covered in a separate SDD by the deployment project responsible for that implementation.

4.3 Interfacing Systems

These are systems that are deemed to be outside of the DR SoS. In some cases, the DR SR&I team will be specifying interface requirements for these projects to ensure that they will integrate with the DR SoS, such as Timetabling requirements. For more detail on the interface, see sections 5 and 6.

- External Users
- Key Management System
- Trackside Objects
- Telecommunication network
- Signal-Controlled Warning System
- Adjacent Control Systems
- Adjacent interlocking
- Business Systems
- Integrated and non-integrated Alarm Systems
- Voice Comms including Computer Telephony Interface (CTI)
- LINX
- SCADA
- Rolling Stock onboard systems
- CCTV

5 PHYSICAL INTERFACES

When deployed in the railway environment, DR Systems will also interface to other physical systems as discussed in the following sections. Further details of the architecture, its internal and external interfaces and functions can be found in the DR SoS Architecture [RD9].

5.1 ROC

5.1.1 Building Interior

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

5.1.2 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 require to be undertaken to determine available spare capacity and changes to support deployment as necessary.

5.2 Telecommunications

5.2.1 LAN / WAN

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

The DR System elements within the ROC will communicate with LINX over the wide area networks (WANs).

5.2.2 FTN / FTN-X

The DR Systems will interface to remote equipment (such as CCTV) where it has a functional interface via the Network Rail Fixed Telecommunication Network (FTN / FTN-X).

The CCTV system may be integrated with TM where the operational need is identified to view CCTV images and control the Pan Tilt Zoom functions of the camera.

5.2.3 GSM-R

With the exception of C-DAS systems, the DR Systems will utilise the NR GSM-R network for its wireless connections.

5.2.3.1 Data

The NR GSM-R data system will be utilised for communications between ETCS track-side systems and ETCS on-board equipment. The availability (reliability and coverage) of the GSM-R data system shall be based on the operational requirements introduced by the deployment for ETCS on GB rail infrastructure.

The ETCS on-board equipment interfaces with various rolling stock systems and the rolling stock operator. GPRS/EDGE will be required to support DR deployments that include areas of ETCS with high traffic levels.

5.2.3.2 Voice

The NR GSM-R voice system will be utilised for communications between the signaller, drivers and track-side workers. The availability of the current GSM-R voice system requires

review in light of operational requirements introduced by the deployment for ETCS on GB rail infrastructure.

The TM interfaces with the unified operational telecommunications system using CTI. The TM System is required to link to the CTI in order to replicate a subset of the functionality available on the telecommunications HMI.

The ETCS onboard system interfaces with the onboard voice comms system to provide a common driver login.

5.2.4 LINX

The DR systems will need to interface to adjacent systems, whether other instances of the system itself, existing legacy control systems, or depot control systems. This will be done via LINX.

Source systems – including Conventional Systems and DR Systems – that publish messages or files, are responsible for timely delivery to LINX and the content of the information they send to LINX. LINX is responsible for validation (to the extent defined in the LINX Catalogue), translation (where applicable) and making the information received from the source systems available in a timely manner to the appropriate subscriber(s), as described in the LINX Catalogue. It is the responsibility of each subscribing system using information made available by LINX to appropriately manage functional scenarios relating to the possibilities of non-delivery of messages or out-of-sequence messages (e.g. because of source system outage), and unexpected message content (i.e. any checks required beyond the validation documented in the LINX Catalogue).

5.2.5 EULYNX

The connection between interlockings and trackside objects is currently supplier specific.

The connection between ETCS Trackside and adjacent Interlockings is not standardised and frequently utilises relay interfaces. The desire is to migrate to IP based connections utilising EULYNX protocols.

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

5.2.6 Third-Party Data Network

C-DAS will utilise a Third-Party Data Network to support transmission of C-DAS data between the trackside systems and on-board systems.

5.3 Key Management System

The DR SoS will interface with the Key Management System to receive authentication keys to allow a secure connection to be established between the ETCS Onboard and ETCS trackside systems. This interface will be accordance with the CCS TSI [RD11].

5.4 Trackside

5.4.1 Multiple Aspect Signalling (MAS)/Legacy Signalling

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 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.

There will be other legacy signalling equipment that the DR SoS might interface to at a given deployment area. Drivers will be expected to obey lineside signalling.

5.4.2 Train Detection

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

5.4.3 AWS/TPWS

The IXL system (part of ETCS Trackside) will have an interface to existing AWS/TPWS systems at boundary areas where trains enter and exit DR-fitted infrastructure. This will support the correct removal of the suppression on the onboard AWS/TPWS systems to allow it to operate as required prior to the train entering a section of conventionally-fitted railway and vice versa.

5.4.4 Level Crossings

DR SoS interfaces to Level Crossings in the Area of Control. Some level crossing controls will be routed directly from the TMS to the level crossing, whereas others are routed via the ETCS Trackside.

A DR deployment scheme 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 DR Programme does not lead 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 delivered by National NR/Deployment Programmes.

5.5 Rolling Stock

The DR Systems will require fitment of radio equipment for the purposes of sending and receiving data over GSM-R as well as ETCS and C-DAS equipment for all rolling stock operating in the chosen DR application areas and will provide system interfaces to the Drivers. In addition, ETCS Onboard will require an interface to voice radio systems and train braking, in addition to power supply needs. A fitted train will run on non-fitted infrastructure, so this creates an interface that will need managing.

The train fitment programme to support ETCS deployment is being managed within the DR programme with implementation via the National Joint ROSCOs Project (NJRP) and this will continue, and the DR programme will support the specification, integration and testing of on-board equipment. Additional equipment will be required for implementation of DR Systems.

Where a fitted train is expected to operate on the conventional network, it will need to retain APC magnets for neutral sections (if electric traction is used) and any existing safety systems such as AWS/TPWS. These will need to be confirmed as operational prior to the train leaving DR-fitted infrastructure.

Within each Rolling Stock, the systems that comprise the DR System are expected to interface to the existing diverse and secure power supplies which are provided within most Rolling Stocks.

6 FUNCTIONAL INTERFACES

Digital Railway technology interfaces to the high-level functional systems shown in Figure 1 –DR System of Systems architecture. These interfaces will be implemented with appropriate 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.

6.1 Users

Discussion of users within this document is limited to only those users who are external to the DR System of Systems but who will directly interact with the DR System(s), i.e. external user interfaces. Users within the DR System of Systems boundary will be defined in the respective System Definition documents. The, users of supporting external operational informational systems, that has a direct interface with the DR System of Systems will be included within this section.

6.1.1 TOC station staff

TOC station staff with duties involving train dispatch may interface with DR Systems through indicators such as 'Right Away' (RA) and /or 'Train Ready to Start' (TRTS) controls where these are provided.

6.1.2 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 such an investigation will include voice or data logs from the various DR Systems, which will be stored in a tamper-proof memory. Others involved (but not limited to) in Incident Investigations include British Transport Police, Centre for Protection of National Infrastructure, 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 SoS – they are crucial interfaces provisions will have to be made to openly share data across the industry efficiently for incident investigation.

6.1.3 Remote Users, TOCs & FOCs

The DR SoS may also be required to supply information-only displays to other remote users at various locations. Where this is the case, then this will be achieved through web-based displays accessible from the users' own existing computing environment. Information will be sent to the user from the relevant DR System via the existing Network Rail Information Management network.

Finally, it may be necessary to deploy remote information terminals to operational staff in other existing control centres during the period of migration to a DR deployment to assist with train running management. In this case, such an interface would utilise network technology and dedicated connections over the FTN or the FTN-X.

6.1.4 Unauthorised User

As DR SoS enables remote and external users to access the SoS environment to support the operations of the DR deployment, this gives rise to the threat of unauthorised access into the DR SoS environment. To mitigate this threat DR SoS will specify and implement the necessary security systems and protocol to ensure that any unauthorised users do not gain access or interface with the DR Systems in any manner that causes a detrimental effect to the DR operations, reputation or safety.

6.2 Command, Control and Signalling Systems

6.2.1 Adjacent Control Systems

The DR SoS will need to interface to adjacent railway control systems, whether other instances of TM/ETCS Trackside (L2 No Signals), existing legacy control systems or depot control systems. Typically, such interfaces will support transfer of train description information for trains entering / leaving the area of control. The interface may also need to support site specific acceptance or signal 'slotting' arrangements via which an adjacent signaller or shunter accepts a train from the DR area of control or asks acceptance for a train to enter the DR area of control.

The DR Systems noted above will be required to interface existing legacy command and control systems at the boundary of the DR deployment area, enabling handover of operational services. The information interfaces between the signalling and traffic management systems at route boundaries are assumed to be at the Traffic Management and Interlocking system level.

6.2.2 Level Crossings

DR SoS will monitor and control level crossings in the Area of Control. The ETCS Trackside will monitor the status of the level crossing (including failure status) and command the level crossing to go to a protected state or return to an unprotected site.

The TMS will be able to control level crossings where the functionality to do so exists in the level crossing. Some level crossing controls will be routed directly from the TMS to the level crossing, whereas others are routed via the ETCS Trackside

6.2.3 Operational Telecoms (including Voice Comms)

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

There is also an interface between the ETCS Onboard System and the GSM-R Voice communication systems for sharing of data.

6.3 Key Management Systems (KMS)

The ETCS system within DR SoS will interface with the Key Management System to receive authentication keys to allow a secure connection to be established between the ETCS Onboard and ETCS trackside systems.

6.4 Signal-Controlled Warning System(s) – SCWS

The SCWS with interface with the ETCS trackside system to determine the location of trains, position of the points and route status, so that it can provide enhanced warning and protection facilities for staff working at the trackside. The SCWS gives advanced warning of approaching trains to enable staff to move to a position of safety before the train arrives.

6.5 Equipment Monitoring Systems

6.5.1 Traction Supply Control

It is the intention that the TM system will interface with the SCADA systems in order to be able to isolate and re-energise either overhead or third rail traction supplies to the railway infrastructure.

TM will also interface to the traction supply control system(s) to import traction supply status information which will be used both within train route suitability decisions and also displayed to the operator. Traction section 'live' and 'dead' states along with traction supply status information are to be acquired and used / displayed.

6.5.2 Infrastructure Monitoring Systems

There are various types of remote condition monitoring systems that 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. However, it is important to note that the information required is the understanding of the operational implication of the failure, not necessarily the failure message itself.

An example of such a system would be the monitoring of signalling power supplies which are monitored by a system called the Signalling Power Alarm System (SPAS), which reports states to the maintainer. The TM System will interface with such systems to acquire the operationally relevant alarms.

Other systems, such as airport or rock fall trip wires, may be connected directly to the underlying signalling system as activation of such systems indicates an immediate need to protect train movements. The activation of these systems, and any associated activities to protect train movements, are then reported to TM by the Interlocking system. This approach replicates existing alarm reporting functionality via interlocking.

CCTV systems are connected to the TMS to view images and control the PTZ cameras and the wiper blade(s).

6.5.3 Vehicle Monitoring Systems

The DR Systems (specifically TM) will interface to rail vehicle monitoring systems like Hot Axle Box Detectors (HABD), and Wheel Impact Load Detectors (WILD) where the area of infrastructure under control requires this.

Note that projects that deploy DR Systems (and therefore will re-control the railway to TM from the existing signal boxes signalling centres to ROCs) will be required to undertake an assessment of the freight traffic in the area and the need to deploy additional HABD sensor sites in mitigation of the removal of lineside observation, where local and regularly staffed signal boxes are being closed.

6.5.4 Alarms and Indication

There are currently multiple systems which provide alarms and indications to the signaller which are not a part of the DR SoS like tunnel ventilation systems etc. This interface receives alarms and alerts from such systems and displays it through the TMS to the signaller.

6.6 Rolling Stock – Onboard Systems

SoS onboard technologies will need to be integrated into both new and legacy Rolling Stock. These technologies will introduce the following interfaces into the rolling stock:

- The on-board ETCS interfaces to the train power supply, GSM-R Voice[3] and Data (CSD & GPRS) and the train braking systems.
- The on-board C-DAS will interface to the train power supply and the train commercial data radio system (non-GSM-R).

6.7 Business Systems

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

- Interfacing to existing IT systems via LINX (e.g. TOPS, TRUST etc);

[3] The GSM-R Voice mobile exists on all stock but a new link between this and the ETCS system is introduced

- Requiring modifications to existing IT systems including those related to timetable improvements and capacity planning to ensure the benefits of DR Systems are fully realised.
- Developing new business systems that support the DR implementation of technologies and/or offer additional benefits to the industry (e.g. DRACAS).

New business systems will be identified as the requirements are developed. At the present time, the following has been identified:

- Central Temporary Speed Restriction (TSR) planning and implementation tool.
- Possession Planning System.
- Common Infrastructure Model.

To deliver the new Business Systems required to support deployment, there will be an interfacing project to deliver these.

6.7.1 Planning, Information & Management Systems

DR deployment requires 'transient' information to deliver its functions and national systems, such as TPS, are the source of this information. DR Systems will communicate with various National systems to acquire timetable, rolling stock data, train consist, possession, maintenance management systems and other types of information. These systems include but are not limited to: TPS, TOPS, TRUST and ELLIPSE.

The DR SoS also 'exports' information to National Systems. The information exported will typically be as a result of any changes made to the 'operational plan' as it approaches service delivery, and also as a result of train movements that occur as the service is delivered. These systems include but are not limited to: TRUST, TOPS and TSIA.

DR will interface to these third-party systems via the LINX layer and its provision of 'message brokering services'.

6.7.2 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. Other external sources of 'transient' information are the TOC Crew and Stock allocation systems, and the FOC crew allocations systems[4]. These provide planned and updated allocations before and during train service delivery.

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. Such systems could include Crew and Stock allocation systems.

DR Systems will also 'export' information to external systems such as DARWIN for the publication on Customer Information Systems.

DR Systems will interface to these external systems via the LINX layer and its provision of 'services'. There is a project outside the DRP to develop a standardised Crew and Stock system which might introduce an interface change to the DR system such as TMS.

[4] Noting that TOPS currently provides freight stock allocation / consist information

7 SYSTEM ENVIRONMENT

7.1 Procedures and Rules

SoS technologies will be integrated into existing mature operating environments and will provide new functions, facilities and shared information sources to the rail operating environments. The Operational procedures will also be modified to reflect the new processes, roles and responsibilities. SoS deployments will be either complete 'green field' or 'brown field' where there will be no existing infrastructure systems to interface to (that provide command and control functionality).

The deployment of DR Systems will cause changes to the Rule Book and other longstanding practices. Guidance on this will be contained in the SoS deployment guide.

7.2 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 any new equipment appropriately and safely, and their competence will require ongoing assessment.

Training needs to extend to the Users who are interfacing to the DR Systems as described in Section 6.1.

7.3 Security

Appropriate physical and cyber security requirements and arrangements will need to be implemented for both the DR specification phase and any DR deployment. These will be made in the context of the wider NR, NRT and railway industry security and cyber security policies, procedures and provisions. DR deployments represent a significant departure from traditional railway practice in the sense that there will be much greater connectivity between different data driven systems and therefore a greater need for cyber security measures than previously where physical isolation was often relied upon.

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

Also noted is the linkage between security risk and safety case and the need to integrate the security risk assessment with the safety case production[5].

7.4 Maintenance

The deployment of DR will introduce a number of new systems and networking products that will require maintenance. Whilst the day to day maintenance is likely to present a lower level of demand, the large number of interfaces and services being transacted across some of those interfaces will create a high level of demand for the maintainer when things do fail. Similarly, frequent changes to the railway controlled by any of the DR systems and / or adjacent systems are likely to require frequent updates to the configuration data of these systems.

The DR systems will require suitable maintenance support, both tools and local and remote facilities, to assist the maintainer in monitoring, understanding, and repairing the system. These needs will be stated in the deployment guide.

[5] The Department for Transport's Rail Executive is developing a Code of Practice to support the development of" Cyber Security informed Safety Cases for the Rail Industry"

Note that the deployment of DR continues the general shift towards a more IT-orientated set of competences for the maintainer and also requires that competence in cyber security is established and maintained in line with the industry's evolving policies on this subject.

7.5 Local Environment and Conditions

7.5.1 ROC

The systems will generally be deployed within the ROCs and it is assumed that these buildings provide a common and stable environment which includes the following:

- Suitable accommodation for equipment
- Suitable accommodation for staff
- Secure access systems, both into the building compound and within the building
- Fire protection systems

7.5.2 On-board

The ETCS and C-DAS systems will require installation of equipment on board the rolling stock, this will require:

- Temperature stable environment and waterproof environment with lighting and ventilation
- Odometry
- Cable routes between equipment locations, the driving cab and other 'sensor' locations (balise antenna, GPS antenna, GSM-R antenna etc.)
- Secure electrical supply equipment
- Earthing points
- External mounting points for antenna
- Interconnection capabilities along the length of the train

7.5.3 Trackside

DR Systems will have equipment located in trackside locations, this is expected to comprise of the following or their associated component parts; IXL, ETCS Trackside (L2 No Signals) as well as associated interfaces to Level Crossing and point control. They will be provided with the appropriate power supplies and communication networks and physical and environmental protection.

7.6 Electro-Magnetic Compatibility (EMC)

DR Systems will comprise products that are suitable for the ROC, on-board and trackside environment(s). Given that the ROCs are not anticipated to contain legacy equipment that pre-dates the EMC directive, it is reasonable to assume that the EMC environment should be compliant to 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 UK rail network it is reasonable to assume that some units will not comply with current EMC standards, additional work may therefore be necessary to ensure any risks posed to the new on-board equipment caused by lack of compliance are fully mitigated.

7.7 Human Factors

For DR deployments, there is likely to be a significant change to the HMI for the operators and maintainers. The workloads for the integrated DR Systems will also require further HF investigation. Therefore, ergonomics assessment work will be required to ensure that requirements are captured in the DR specifications and that for any given deployment the workload for the various users is appropriate under normal, emergency and abnormal modes of operation. Section 6.1 discusses the users impacted by these changes in more detail.

8 EXISTING SAFETY MEASURES

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

Railway Undertakings and Vehicle Owners will be responsible for managing, through their own processes, all necessary changes to their standards, or the introduction of new standards, as a result of fitting on-board systems. They will be guided by documentation and processes provided by the DRP. Again, due to the developmental nature of the DRP, it is anticipated that new on-board system requirements or standards will be necessary, or existing ones will need to be revised.

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

Existing safety measures identified by the risk assessment process will be captured in the DR 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.

Further information with respect to Safety Measures and Requirements is contained in the DR System Safety Plan [RI7].

9 SAFETY REQUIREMENTS

Safety Requirements are contained within the specifications which are an output from the configuration managed DOORs database. Safety requirements are tagged as such within the configuration managed DOORs database.

Safety Requirements that emerge from the hazard identification and risk assessment process will be cross-referenced to the source of the requirement e.g. DR SoS Generic Hazard Record [RI6] and DR System Safety Plan [RI7].

10 ASSUMPTIONS

All risks, assumptions, issues and dependences are recorded in the Digital Railway SoS RAID log document [RI8]. These are regularly reviewed by technical leads to ensure compliance with this System Definition.

Current assumptions are:

- Comms connections, such as FTN/FTN(X), are available at the required locations.
- The development of training requirements is delivered by 3rd party.
- A maintenance strategy for any enabling projects will align with the maintenance strategy for DR technologies.
- A consistent alarm management system across the projects and Service Level Agreements (SLAs) support arrangements will be provided.
- The use of EULYNX within the SoS is proposed for the interface between the interlocking and SCWS only. While assumed included at this point, its inclusion is subject to further discussion and development.
- Configuration and operational data will be stored in a Data Centre provided by a 3rd party.
- National NR / Deployment programmes will lead the development of new systems for any existing as-built infrastructure (e.g. level crossings, depots, stations).
- Interfacing at the boundary of any DR deployment area (to enable handover of operational services) are at the Traffic Management and Interlocking system level.
- Buildings used to house DR technologies provide a common and stable environment, compliant to EMC requirements.

Digital Railway

Working together for a better railway:

Department for Transport

Rail Delivery Group

National Rail

NetworkRail

RFG Rail Freight Group

Rail Supply Group

Railway Industry Association

RSSB

digitalrailway.co.uk @DigitalRailway

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