Digital Railway

Reference	153821-NWR-SPE-ESE-000009
Issue/Ver:	3.0
Date:	27/03/2019

Digital Railway – Connected Driver Advisory System (C-DAS) System Definition

Prepared By
Thomas Harrison
Lead Architect C-DAS

TH-260319-0008 Date: 26/03/2019

Reviewed By
David Nicholson
System Integration and Interface Manager

DJN-28032019-0097 Date: 27/03/2019

Approved By
Rubina Greenwood
Head of System Requirements & Integration

RNG-280319-0089 Date: 28/03/2019

Working together for a better railway:

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

Electronic file reference: 153821-NWR-SPE-ESE-000009

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: Thomas Harrison, Lead Architect C-DAS

Version History

Issue	Date	Comments
0.1	19/03/2018	1st Draft
0.2	26/03/2018	Document updated to address review comments
1.0	05/04/2018	Formal issue for signature
1.1	05/10/2018	Update to address Level 2 Assurance comments and to apply revised template
1.2	17/10/2018	Update to address significant omissions in version 1.1
1.3	08/11/2018	Update to address 2nd round of review comments
1.4	15/11/2018	Update to address 3rd round of review comments
1.5	19/11/2018	Update to address Level 2 Assurance 2nd round comments
2.0	22/11/2018	Formal issue for signature
2.1	01/03/2019	Update to address L3 review comments from Ricardo
3.0	26/03/2019	Third formal release

Exclusions

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

1. Revised DR Concept of Operations (Note: It is assumed that the existing DR Concept of Operations [RD7] will be updated at a later stage).
2. This document has been submitted for Level 3 assurance in accordance with the System Management Plan [RD12]. A response has been received with one Category 1 comment (i.e. there is an issue associated with a fundamental concern, error, omission or question that has a direct bearing on the acceptability of the document). The issue in this case was initially that the physical interfaces were not sufficiently clear. After the first revision of the document this was largely fixed, although a small issue remained; the criticality of the interface with the train driver was not sufficiently clear. A response has been made to address this comment which is reflected in this version of the document. However, confirmation has not yet been received that these responses are considered to be satisfactory which may result in amendments to a future revision of this document.

Assumptions

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

None.

Dependencies

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

1. Digital Railway System of Systems System Definition document [RD5]

Contents

References ... 6
1 Introduction ... 7
1.1 Background ... 7
1.2 The Digital Railway Programme (DRP) ... 7
1.3 Context & Purpose of this Document ... 7
1.4 Scope ... 8
1.5 Background to the Generic System of Systems (SoS) ... 8
1.6 Document Maintenance ... 9
1.7 Terms, Abbreviations & Acronyms ... 9
2 System Purpose and Objectives ... 10
2.1 C-DAS Mission and Objectives ... 11
2.1.1 Business Change Consideration for C-DAS ... 11
2.1.2 Business Benefits of C-DAS ... 12
3 System Functions and Elements ... 13
3.1 C-DAS Functionality Overview ... 13
3.1.1 Normal operation ... 14
3.1.2 Degraded mode operation ... 15
3.1.3 Emergency mode operation ... 15
3.2 Enabling Systems: ... 15
4 System Boundary ... 16
4.1 Geographic Boundary ... 16
4.2 System Configuration ... 16
4.3 Interfacing Systems ... 16
5 Physical Interfaces ... 17
5.1 The Deployed System ... 17
5.2 Rail Operating Centre (ROC) ... 18
5.2.1 Building Interior ... 18
5.2.2 Power Supply ... 18
5.3 Telecommunications ... 18
5.4 Rolling Stock ... 18
5.5 Drivers ... 18
5.6 Layered Information Exchange (LINX) ... 18
5.7 Integrated Timetable Planning System (ITPS) ... 19
5.8 Configuration Data ... 19
6 Functional Interfaces ... 20
6.1 People ... 20

6.1.1 Operational & Maintenance Staff 20
6.1.2 Accident/Incident Investigators 20
6.1.3 Non-authorised User 21
6.2 Management Systems 21
6.2.1 Planning, Information & Management Systems 21
6.2.2 External (Third Party) Systems 21
6.3 Traffic Management 21
6.4 Business Systems 21
7 System Environment 23
7.1 Procedures and Rules 23
7.2 Staff Competence and Assessment 23
7.3 Security 23
7.4 Maintenance 23
7.5 Local Environment and Conditions 23
7.5.1 Trackside 23
7.5.2 On-board 24
7.6 Electro Magnetic Compatibility (EMC) 24
7.7 Human Factors 24
8 Existing Safety Measures 25
9 Safety Requirements 26
10 Assumptions 27
10.1 Technical 27
10.2 Environmental 28
10.3 Operational 28
10.4 System Integration 28
10.5 Maintenance 28

References

Dependent References

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

RD1. Digital Railway Programme Directors Remit, 00000-NWR-REM-MAN-000001, Version 2.0, December 2017
RD2. Commission Regulation (EU) 402/2013, 30th April 2013
RD3. Commission Regulation (EU) 2015/1136, 13th July 2015
RD4. Digital Railway – M9 Significance of Change Assessment, 147883-NWR-ASS-ESS-000001, Version.1.0, 19th February 2018
RD5. Digital Railway Programme – System of Systems Definition Document, 153821-NWR-REP-ESE-000002, Version 6.0
RD6. Digital Railway Programme – System of Systems Architecture, 153819-NWR-DRG-ESE-000003, Version 5.0
RD7. Digital Railway – Integrated Concept of Operations, 000000-NWR-PLN-MPM-000005, Version 1.0
RD8. Interface Requirements for Connected Driver Advisory System, RIS-0711-CCS, Issue One, December 2018
RD9. System Management Plan, 153819-NWR-PLN-MPM-000002, Version 8.0
RD10. C-DAS Interim System Requirements Specification, 153821-NWR-REQ-ESG-000001**,** Version 2.2
RD11. Digital Railway – GB Generic Interface Requirements Specification, 153821-NWR-SPE-ESE-000013, Version 3.0
RD12. Digital Railway Programme - System Management Plan, 153819-NWR-PLN-MPM-000002, Version 8.0

Informative References

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

RI1. Digital Railway – System Hazard Record Report, 147883-NWR-LOG-PRK-000001
RI2. Digital Railway – System Safety Plan, 147833-NWR-PLN-MPM-000008
RI3. DR Tech – System of Systems (SoS) RAID Log, 153821-NWR-REG-ESE-0000001
RI4. Digital Railway – Glossary of Terms & Abbreviations, 153819-NWR-SPE-ESE-000001
RI5. Digital Railway – GB Generic Customer Requirements for Connected Driver Advisory System (C-DAS), 153821-NWR-SPE-ESE-000010
RI6. DR Tech – C-DAS RAID Log, 153821-NWR-LOG-MPM-000002

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 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 (RUs)), the Rail Safety and Standards Board (RSSB) and the supply chain. It will also engage with the Regulator and the Department for Transport (DfT) as necessary to secure the required improvements to safety and customer provision, funding and approvals.

1.2 The Digital Railway Programme (DRP)

The Digital Railway Programme has several principal outcomes that are defined in the System Management Plan [RD9].

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.

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

1.3 Context & Purpose of this Document

An EU Regulation on the adoption of a Common Safety Method (CSM) for 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 principle of the CSM RA is the preparation of a System Definition, i.e. this document. The purpose of the System Definition document under the CSM RA is to complement the

SoS Hazard Record [RI1] 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 C-DAS 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 C-DAS, its purpose, functions and interfaces, and the existing safety measures that apply to it, so that it provides a generic system design in support of subsequent development and deployment (i.e. system-specific design and implementation).

It also allows the generic system specification and design for the C-DAS 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 C-DAS 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 C-DAS only. There are two distinct Connected Driver Advisory System (C-DAS) options under consideration for GB’s railway:

- The provision of C-DAS functionality by an Automatic Train Operation (ATO) over ETCS (AoE) system available in Grade of Automation 1 (GoA1) operation. AoE requirements and architecture are defined in the relevant European specifications currently under development in GB ATO specifications. C-DAS provided by an AoE-based system is sometimes referred to in GB as ‘Interoperable’ C-DAS.
- A non-AoE-based system architecture that can be applied on ETCS-fitted and non-ETCS-fitted trains. This is sometimes referred to in GB as ‘Independent’ C-DAS.

This System Definition document applies to ‘Independent’ C-DAS for ETCS-fitted, fixed and variable formation trains.

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 it sits as this has its own System Definition [RD5].

1.5 Background to the Generic System of Systems (SoS)

The SR&I (System Requirements and Integration) 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 C-DAS is one of the core systems within this architecture.

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

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

The SoS will be supported by:

- A fixed data network, e.g. the Fixed Telecoms Network (FTN) or the FTN – next generation (FTNx)
- A voice and data communications network
- Data services, systems and protocols, Key Management and EULYNX
- 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 C-DAS. It will be subject to review at least prior to each technical review to ensure its ongoing adequacy for progressing to the next technical review. 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 these will be considered. An update to this document may then be necessary.

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 Terms, Abbreviations & Acronyms

Abbreviations are explained in full on first use within this document. A comprehensive list of abbreviations and definitions is contained in the Glossary [RI4].

2 SYSTEM PURPOSE AND OBJECTIVES

The principal objectives of the C-DAS (Connected- Driver Advisory System) are to monitor train speed and location against the current schedule, calculate an optimal safe speed based on the trains specific characteristics and provide the advisory speed to the driver.

Traditionally, the driver is provided with schedule information (timings and calling pattern) for their journey from the timetable or other documentation derived from it. The driver is then responsible for managing the train in such a way as to achieve that schedule as far as is practicable within the constraints imposed by the signalling system. The concept of a Driver Advisory System (DAS) is to provide a support tool to assist the driver in managing the train effectively by providing them with improved information, principally, that reflect the progress of the train and results in an advisory speed.

Initial DAS deployments by some Railway Undertakings (RUs) have been in the form of Standalone Driver Advisory Systems (S-DASs) or Networked Driver Advisory Systems (N-DAS). These provide guidance to the driver on the optimum speed at which to drive their train at any given moment during the journey, based on the schedule for that individual journey (retrieved in advance from a data repository), train position and time. The information is provided to the driver via an in-cab visual display.

An S-DAS or N-DAS configuration has certain limitations, however; in particular, it optimises the performance of a single train in isolation and cannot take account of the impact its guidance could have on the performance of other trains. On a busy and congested network, such as that in Great Britain (GB), this limits the benefits that can be obtained from S-DAS or N-DAS use.

The GB rail industry is therefore pursuing the development of a more sophisticated system which can be interfaced with Infrastructure Manager (IM) Traffic Management systems (TMSs). This interface will enable the provision of information updates to trains in near real time and also offers the potential for the control system to use data received from trains to inform regulation decisions. In this way, the guidance provided has the potential to optimise the performance of the wider network. These system configurations are known as Connected Driver Advisory Systems (C-DASs).

When C-DAS-equipped trains operate beyond the limits of the control of the Traffic Management area, the C-DAS equipment will provide guidance to the driver based on the last update received prior to leaving the Traffic Management area. For situations where the train starts in a Non-Traffic management area, it will use static data until it reaches the Traffic Management area.

A Driver Advisory System only provides advice to the driver; it does not supersede the safety information received by the signalling system. The driver is required to ignore contradictory information on the DAS if this information contains an advisory speed which is higher than the permissible speed.

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 C-DAS architecture as a singular system for simplicity, further expansion of the configuration of a C-DAS is provided in section 3 of this document.

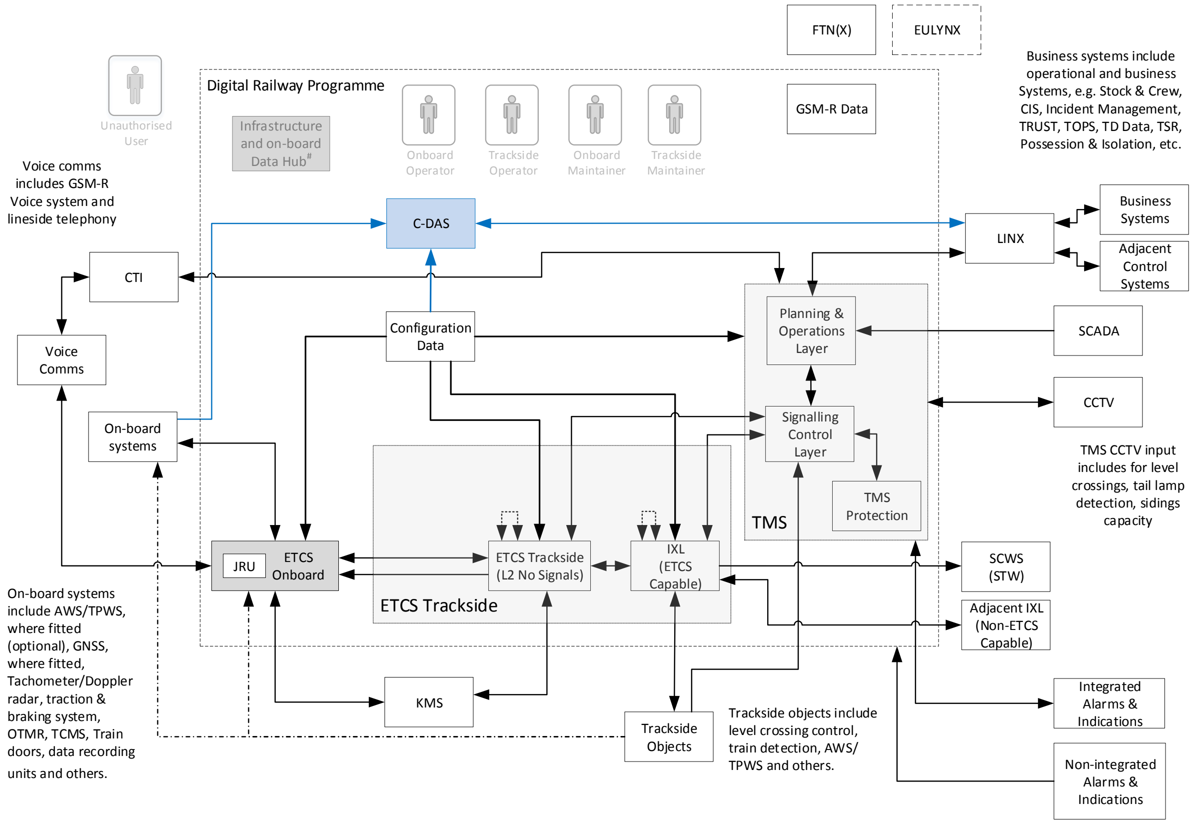

Figure 1 – C-DAS System Boundary

C-DAS is interfaced by three systems (indicated by the blue lines in figure 1); Configuration Data, On-board Systems and LINX. C-DAS interfaces to Business Systems and TMS via LINX. C-DAS comprises hardware and software elements and is broken down into two distinct subsystems; Infrastructure Manager (IM) and Railway Undertaking (RU) subsystems. An IM subsystems primary purpose is to collate data that it receives from business systems and apportions it to the relevant RU. The RU subsystem will be responsible for distributing data to relevant Onboard Units to calculate and display an advisory speed. Due to this distinct line of responsibility between the IM and RU a standard interface is required to ensure a stable connection between the two subsystem elements. This interface is defined in a Rail Industry Standard (RIS) [RD8].

2.1 C-DAS Mission and Objectives

2.1.1 Business Change Consideration for C-DAS

The introduction of C-DAS will affect a number of business processes and all staff engaged in the operation and management of trains:

Processes affected include but are not limited to:

- Maintenance and renewal of systems
- Disposal of systems
- Testing, commissioning and authorisation of trains
- Installation of equipment (on-board and trackside)
- Timetable development including amended timing point locations

Personnel affected includes but is not limited to:

- Drivers

- Vehicle maintenance staff
- Accident / incident investigators
- Service and timetable planners

2.1.2 Business Benefits of C-DAS

Any DAS implementation (S-DAS, N-DAS or C-DAS) would be expected to generate benefits in the quality, cost and efficiency of train operation, while still meeting all times specified in the schedule.

With any DAS the expected business benefits are:

- Improved Safety:
    - Train regulated to the working timetable encountering fewer restrictive signals.
    - Overall lower sectional running speeds.
    - Advance warning of locations, where speed restrictions change.
    - Lower approach speeds to Permanent Speed Restrictions (PSRs) / stations / known conflict points with extended coasting.
    - Reminder of next station calling point, thus reducing a number of missed stations / overruns.
- Improved fuel efficiency (up to 15% reduction on diesel trains).
- Improved capture of delay attribution data.
- Reduction in wear and tear:
    - Reduced braking / lower speed.
    - Lower running speeds.

However, benefits will not be realised unless trains are on schedule (or nearly so), i.e. typically ~75% of passenger journeys on major routes.

With C-DAS it is possible to 'close the loop'- the revised schedule generated by a Traffic Management Systems can be presented to the driver, and information on train progress against schedule is made available to the Traffic Management System. The expected benefits are therefore all of those anticipated for DAS and in addition:

- Train regulation to revised schedule
- Support for improved recovery from disruption by conveying a consistent set of schedules to trains and corresponding advice to drivers
- Support for regulation to optimise for network capacity or performance (based on fewer delays due to red signals)
- Support for improved conflict resolution (based on trains' predicted running)
- Potential fuel savings on nearly 100% of journeys

In addition, all DAS variants will potentially support future anticipated requirements to optimise energy consumption based on locally available electrical power or power tariffs.

3 SYSTEM FUNCTIONS AND ELEMENTS

3.1 C-DAS Functionality Overview

Driver Advisory Systems include both trackside and on-board elements. The trackside element receives target timing information for each train, calculated by the Traffic Management System's operational forecast and planning function based on the train's current location and the current traffic control priorities. The targets, reflecting the capabilities of the train (mass, traction and braking characteristics etc.) and the constraints imposed by the route (permissible speeds, gradients, speed restrictions etc.), are transmitted to the train. The on-board element calculates the appropriate speed profile for that train, continuously monitors the train's location relative to its targets, displays advisory information to the driver, and also informs the trackside element of the train's progress to pass on to the Traffic Management System so that targets may be updated as appropriate.

A closed-loop Driver Advisory System of this kind is known as a Connected Driver Advisory System (C-DAS). A functional overview is shown in Figure 2.

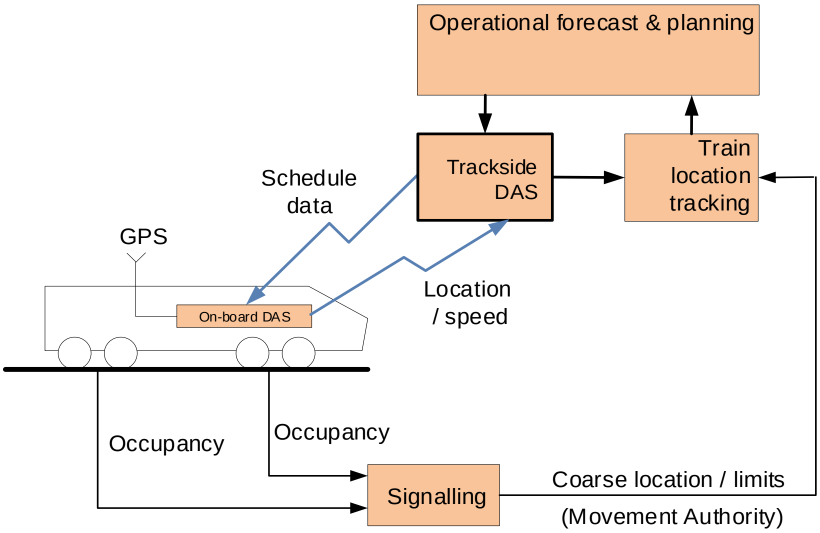

Figure 2 - C-DAS Functionality Overview

C-DAS:

- Calculates recommended energy-efficient speed profiles which allow trains to meet scheduled Timing Points and which are consistent with Infrastructure geography, line speeds (including speed restrictions) for the given train, and the train characteristics and capabilities.
- Collates dynamic information
- Monitors train progress towards the next Timing Point, changing the recommended speed profile as required.
- Determine maximum permissible speed
- Displays advisory information to the driver.
- Receives updates to train schedules and speed restrictions.
- Provides train location, speed information and expected arrival times to the Traffic Management System.
- Notifies the Traffic Management System when a train cannot meet its schedule.

- Provides changes to Train Specific Data to the Traffic Management System.
- Generates data for rail network performance analysis.
- Notifies the Traffic Management system of changes in the operating state of C-DAS on individual trains.

Further detail of the system functionality can be found in the C-DAS Interim System Requirement Specifications [RD10]

3.1.1 Normal operation

C-DAS design is not entirely fixed which promotes innovation from suppliers and provides flexibility for deployment projects whilst remaining within the boundaries of the requirements set out in the C-DAS requirements suite. Where there are functions within this SDD which appear optional, the deployment project team will need to identify a recommended functionality or design decision from the available options.

Before the start of a particular journey, the C-DAS Onboard is primed by trackside systems, with setup information relevant to the train and the journey being undertaken (including infrastructure geography data and permissible speeds). Where multiple on-board systems require input of the same, or a part of the same setup information, the driver should only enter this data once. The driver can input the following at journey start, should the information not be obtainable from other systems:

a) a unique Driver ID, where requested by the RU,

b) the TRN (GB alphanumeric, eight digit or any other future format) to allow journey identification,

c) train consist information,

d) power mode,

e) reduced maximum speed or changes to other performance parameters associated with train defects, if applicable,

f) Route restrictions for vehicle and locomotive, if applicable,

g) Special conditions of travel (RT3973), if applicable.

Manual entry or selection of C-DAS setup data by the driver is performed in a leading cab and when the train is at a stand. When changing ends within the same locomotive, the option to retain train data is available. The solution as to how to achieve retainment of set up data will be by joint agreement between the deployment team and supplier.

The driver is able to confirm that the system has identified the correct details from the information provided.

Where the system has identified incorrect information, the driver is able to correct the error. Where information is downloaded from an external system, the driver can notify the source of that information of any errors and request a correction, this process will be defined under operational rules outside of any C-DAS functionality.

The C-DAS Onboard allows the driver to check and confirm that the current train consist information has been entered / selected / determined / downloaded correctly.

C-DAS operation is enabled if all the following conditions are met:

a) The driver has entered and/or confirmed setup information;

b) The driver has selected and/or confirmed train schedule;

c) Current and correct train specific data is available; and

d) All the data required to be available to the C-DAS Onboard at or prior to journey start has been transferred and confirmed current.

The driver is provided with an indication if the setup process is unsuccessful along with any error messages that will allow for efficient diagnosis and rectification.

The C-DAS Onboard can either be manually or automatically suppressed during normal operation. The scenarios under which manual and automatic suppression and un-suppression occur will be defined by the deployment team.

3.1.2 Degraded mode operation

C-DAS does not provide any additional functionality arising from degraded mode working. The C-DAS Onboard can either be manually or automatically suppressed in cases of degraded operation. The scenarios under which manual and automatic suppression and un-suppression occur will be defined by the deployment team.

Driver training advises drivers to treat information provided by C-DAS as advisory only and will ignore this information if it conflicts with current rules, policies, route knowledge, information from a system with a higher level of authority and/or operational notices.

3.1.3 Emergency mode operation

C-DAS does not provide any additional functionality arising from emergency mode working. The C-DAS Onboard can either be manually or automatically suppressed in cases of emergency mode operation. The scenarios under which manual and automatic suppression and un-suppression occur will be defined by the deployment team.

Driver training advises drivers to treat information provided by C-DAS as advisory only and will ignore this information if it conflicts with current rules, policies, route knowledge, information from a system with a higher level of authority and/or operational notices.

3.2 Enabling Systems

These are systems that are deemed to be outside of the C-DAS boundary 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 C-DAS.

The critical enablers for the C-DAS are:

- Layered Information Exchange (LINX) – This enterprise service bus architecture will serve as means of language unification for data transferred from other systems (including TMS) to the C-DAS IM Trackside Subsystem.
- Capacity Planning / Timetable Planning – Digital Railway may specify improvements to the current timetable including introducing additional Timing Point Locations (TIPLOCS) in order for C-DAS to provide optimal advisory information.
- Traffic Management System
- Configuration Data
- Temporary Speed Profile management
- Telecommunications.

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

4 SYSTEM BOUNDARY

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 System Configuration

The configuration of C-DAS is changeable according to the type of application. It comprises off train and on train elements, but these can be configured in a variety of ways. Typically, off-train (trackside) elements will be responsible for collating and apportioning data received from Traffic Management Systems and Business Systems. On-train (on-board) elements will be responsible for the calculation and presentation of advisory information.

The number of off-train elements will depend on the operational requirements of the deployment. It is envisaged that a single IM subsystem will be responsible for data management and apportionment from external systems to cover a defined geographical area (SoS deployment area) or route. The data will be sent via the standard interface [RD10] to relevant RU subsystems and typically one RU Subsystem will exist for each RU. The off-train RU subsystem will send data to relevant on-board Units. One Onboard Unit will be required in each driving cab.

4.3 Interfacing Systems

These are systems that are deemed to be outside of the C-DAS. In some cases, the DR SR&I team will be specifying interface requirements for these projects to ensure that they will integrate with the C-DAS.

- Staff
- Traffic Management System
- Configuration Data
- On-board Systems
- Layered Information Exchange (LINX)
- Business Systems

5 PHYSICAL INTERFACES

When deployed in the railway environment, the C-DAS will also interface to other physical systems as discussed in the following sections. This section will set out the physical interfaces and any protocols used on an interface. More detailed information on the physical interfaces is provided in the Generic Interface Requirements Specification [RD11].

5.1 The Deployed System

The C-DAS Reference Architecture comprises two subsystems:

- The C-DAS IM Subsystem, which comprises a single or multiple trackside elements (C-DAS IM Tracksides) managed by the Infrastructure Manager (IM);
- The C-DAS RU Subsystem, which comprises:
  - An off-train element (the C-DAS RU Trackside) operated on behalf of a Passenger or Freight operator, referred to as a Railway Undertaking (RU);
  - An on-train element (the C-DAS Onboard) on each C-DAS fitted train in an RU's fleet.

The C-DAS RU Trackside supports the C-DAS Onboards on a set of trains throughout their operational journeys, regardless of the trains' geographical locations and it communicates with its C-DAS Onboards via mobile telecommunications.

The Reference Architecture provided below in Figure 3 shows the relationship between the IM and RU Subsystems and any external systems connected to C-DAS.

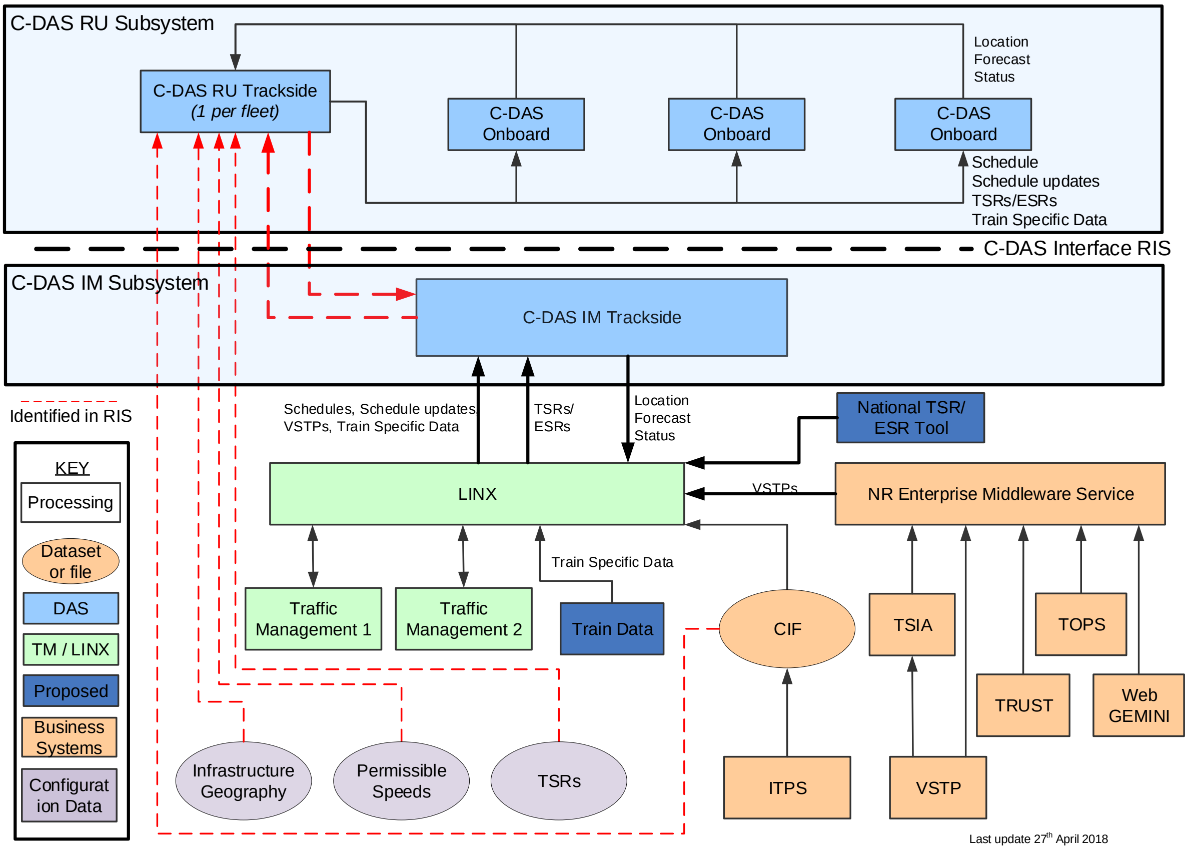

Figure 3 - C-DAS Reference Architecture

5.2 Rail Operating Centre (ROC)

5.2.1 Building Interior

The principal systems that comprise the DR infrastructure hardware (TMS, 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.

5.2.2 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, as necessary, to determine available spare capacity and changes to support deployment as necessary.

5.3 Telecommunications

C-DAS will utilise a third-party data network to support transmission of C-DAS data between trackside and on-board systems. The deployment teams' quality of service, volume of data and frequency at which the data is sent and received will drive the selection of an appropriate data communication solution.

5.4 Rolling Stock

Rolling Stock will require fitment of radio equipment for the purposes of sending and receiving C-DAS data as well as providing system interfaces for the Driver (Human Machine Interface HMI)).

Deployment of C-DAS will introduce the following interfaces into the rolling stock:

- The C-DAS Onboard will interface to the train power supply.
- Data interface to commercial data radio for C-DAS equipment.

5.5 Drivers

A C-DAS Human Machine Interface (HMI) will be provided in the driving cab to display advisory information. It will be necessary for the driver to input some relevant information to ensure that the C-DAS operates correctly if the information cannot be sent and the system populated automatically.

5.6 Layered Information Exchange (LINX)

The Layered Information Exchange (LINX) is not part of the DR SoS but is a vital interface which connects the C-DAS, TMS and Business Systems. LINX is Network Rail's strategic solution for providing a single source of planning and operational information required to operate the GB train and rail services. Currently, existing conventional systems form a disparate set of services that require consuming systems projects to negotiate for access, implement and maintain multiple, complex network routes and services; in order to access multiple data sources, often with manual recovery processes.

As NR's strategic solution, LINX is implemented using a Service Bus messaging technology which supports a catalogue of message flows and a reliable message delivery system. Message consumption and production systems only require a simple, single network connection to the one system rather than to multiple systems. LINX also provides facilities for consuming systems that require automated recovery of data.

5.7 Integrated Timetable Planning System (ITPS)

C-DAS will interface with the Capacity Planning function to receive a daily timetable file to use at start up for the following day. This will be in the form of a CIF (Common Interface File) and will be used as the base plan that C-DAS will work to up until any perturbation occurs, at which point the timetable will no longer be current.

The file will be transmitted via means which accommodates both the quality of service and the capabilities of the ITPS.

5.8 Configuration Data

The C-DAS will need to be configured with the necessary data that describes the physical railway in such a manner that it can successfully monitor the train progress against the schedule and provide a safe optimal advisory speed. This data will be sourced externally; the protocol and procedures required to ensure correct configuration are to be defined.

It is essential that the Configuration Data is prepared and downloaded into the systems in a controlled manner both the IM and RU subsystem owners will be responsible for the reception and management of configuration data. The types of data and the controls required need to consider:

- Data sources
- Data consumption
- Derivation of resolution and accuracy requirements
- Derivation of safety integrity requirements
- Assurance of Data for SIL level processes
- Security classification of data and derived information
- Storage and management of data throughout the life cycle
- Sharing of data in operational service

6 FUNCTIONAL INTERFACES

Digital Railway technology interfaces to the high-level functional systems as described in the DR SoS System Definition [RD5]. These interfaces will be implemented taking into account 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 C-DAS will interact with people (i.e. users), and the functions listed below:

- Management Systems
- TMS (via LINX)
- Business Systems (via LINX)

6.1 People

Discussion of staff within this document is limited to only those staff who will interact directly with the DR System. Thus, users of supporting operational information systems are excluded.

6.1.1 Operations & Maintenance Staff

Operations staff are defined as any individuals who are authorised, competent and responsible for the movement of trains, e.g. signaller, who interfaces with the DR System as part of their duties. In the context of the C-DAS, the HMI of the driver with the On-board DAS is the critical interface as it allows for the provision of advisory information to the driver, the main goal of the C-DAS. There is currently no interface for operations staff with the IM element and RU Trackside element of the C-DAS.

Maintenance Staff are defined as any individual who is responsible for undertaking engineering activities on railway infrastructure and rail vehicles. C-DAS will require maintenance staff to interface with the IM and RU subsystems for maintenance and diagnostics purposes both onboard (RU) and trackside (both IM and RU). There will also be an internal interface between IM maintenance staff and RU maintenance staff to manage the communication between the two off-train subsystems.

For the purposes of C-DAS, the two groups defined above sit within the DR System boundary and as such, appropriate operational readiness activities will have to take place to enable the successful deployment and operation of C-DAS. The operational readiness activities should also generate appropriate supporting procedures to allow the staff to operate the System in a safe and efficient manner.

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

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

6.1.2 Accident/Incident Investigators

Formal investigations into serious railway safety incidents are carried out by the Rail Accident Investigation Branch (RAIB). Examples of such incidents include: train 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 DR System, which will be stored in a tamper-proof memory.

Others involved in Incident Investigations (but are not limited to) include British Transport Police (BTP), Centre for Protection of National Infrastructure (CPNI), Health and Safety Executive (HSE) all of whom require access to infrastructure and control system data records in the event of an incident which will require the support of identified, competent

IM operational and maintenance staff. Although they sit outside the boundary of the System – they are crucial interfaces provisions will have to be made to openly share data across the industry efficiently for incident investigation.

C-DAS will include sufficient data recording facilities to support maintenance and incident investigations.

6.1.3 Non-authorised User

The user is recognised in that all interfaces are required to ensure that a non-authorised user or system is unable to access the system.

6.2 Management Systems

6.2.1 Planning, Information & Management Systems

DR deployment requires 'transient' information to execute its functions and national systems, such as the 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, Total Operations Processing System (TOPS), R2, Train Running Under System TOPS (TRUST) and ELLIPSE.

C-DAS will acquire relevant information for a number of business systems via an interface with LINX either directly from the systems themselves or via a Traffic Management System.

6.2.2 External (Third Party) Systems

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

6.3 Traffic Management

The C-DAS will be connected to the relevant Traffic Management System(s) to receive schedule updates following both automated and manual routes setting, and to supply information to the signaller.

The interface protocol to the Traffic Management System (or legacy control systems) will be defined by the TMS. The information to be shared is defined in the Digital Railway Programme – Interface Description Document [RD6]. The desire is to migrate to IP based connections utilising LINX protocols.

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.

6.4 Business Systems

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

- interfacing to existing IT systems via LINX (e.g. TOPS, TRUST etc);
- 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; and
- developing new business systems that support the DR deployment of technologies and/or offer additional benefits to the industry.

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

- Central Temporary Speed Restriction (TSR) planning and implementation tool.

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

7 SYSTEM ENVIRONMENT

The system environment will be different for each deployment. Therefore, the DR SoS Operating Model will need to be defined and implemented for each specific deployment. The Operating Model is a high-level representation of how IMs and RUs can best execute the DRP Strategy. Moreover, it provides a common understanding of how to operate and maintain the DR System by allowing people across the industry to visualise it from a variety of perspectives as every significant element of business activity should be represented. The development of this Operating Model will require a detailed analysis of roles, responsibilities and accountabilities in using the deployed DR SoS. The DR SoS Operating Model will potentially result in changes to, and the splitting of, roles and responsibilities within the industry.

7.1 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.

C-DAS deployment will cause changes to the Rule Book and other longstanding practices.

7.2 Staff Competence and Assessment

In line with existing accident investigation recommendations, staff will be trained 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 C-DAS equipment appropriately and safely, and their competence will require ongoing assessment.

7.3 Security

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

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

7.4 Maintenance

The C-DAS deployment 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.

7.5 Local Environment and Conditions

Relevant environmental conditions and their compliance criteria will be defined on a deployment-specific basis. Sections 7.5.1 and 7.5.2 list the main expected considerations for trackside and on-board respectively.

7.5.1 Trackside

The system will be deployed trackside with the following provisions:

- Suitable accommodation for equipment including C-DAS IM and RU trackside subsystems

- Secure access, both into the building compound and within the building to access C-DAS IM and RU trackside subsystems

7.5.2 On-board

C-DAS equipment installed on board the rolling stock will require the following:

- Cable routes between equipment locations and the driving cab
- Secure electrical supply equipment (diverse and UPS backed)
- Earthing points
- External mounting points for antennae
- Interconnection capabilities along the length of the train

7.6 Electro Magnetic Compatibility (EMC)

It is reasonable to assume that the EMC environment for the Trackside equipment 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 GB's rail network it is also reasonable to assume that some units will not comply with current EMC standards. Additional work may, therefore, be necessary to ensure that any risks posed to the new on-board equipment caused by lack of compliance are fully mitigated.

7.7 Human Factors

For C-DAS, there is likely to be a significant change to the HMI for the operators and maintainers.

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

8 EXISTING SAFETY MEASURES

As the CSM process is applied to the system, all safety measures and associated requirements will be listed in the SoS Hazard Record and associated safety requirements specifications.

Within a current (conventional) railway command and control system the Interlocking contain the safety-critical functionality that ensures route integrity and provides Movement Authority. Since The C-DAS is used by the driver in a purely ‘advisory’ way it is neither a safety critical nor a safety related system. However, the operator interface will require careful design to ensure that, for the driver, the advisory speed is clearly separated from the Movement Authority and braking profile information.

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

Existing safety measures identified by the risk assessment process and any previous risk assessment work will be captured in the SoS 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 SoS Hazard Record [RI1] and the 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].

9 SAFETY REQUIREMENTS

Safety Requirements are contained within the specifications which are an export from the configuration managed DOORS database and included in the C-DAS CRS [RI5]. Safety requirements are tagged as such within the configuration managed DOORS database and with the word ‘Safety’ in the CRS.

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

10 ASSUMPTIONS

The assumptions listed here are additionally captured in the Technical RAID Logs for C-DAS [RI6] and for the SoS [RI3] in case the assumption relates to multiple DR systems. The RAID Log is used only to manage the assumption and track it until it is closed and not as the master record of the assumptions. The master record of the assumptions remains here in this document and set out in the following sections.

10.1 Technical

1. There will be no interface between C-DAS and ETCS in a System of Systems (SoS) deployment and therefore functionality which could exist if this interface were present is omitted from this system definition.
2. Existing power supplies are sufficient for the C-DAS application or will be upgraded as required.
3. Commercial communications networks will be suitable for C-DAS applications in both capacity and quality of service. No requirement exists to utilise the GSM-R network.
4. C-DAS RU and C-DAS IM subsystems make up C-DAS as a system and will be considered as one system within the DR SoS. Projects will need to understand the functionality of the individual subsystems which will be detailed in the C-DAS requirements suite.
5. C-DAS is not a sole (or primary) source of information, and does not provide safety information, or supersede the safety information.
6. The primary function of C-DAS is to provide advisory speed information; any additional information provided to the driver is considered optional and will be configured by the project deployment team.
7. The “Advisory information” function is capturing speed in the format of numbers or actions, e.g. “25mph” or “Increase Speed”
8. C-DAS uses its own internal GPS to track and broadcast its location.
9. C-DAS internal clock is synchronized with local trusted time source.
10. Schedule updates are sent to C-DAS from TMS.
11. Train performance information is sent (downloaded or exported) to C-DAS from TMS and is based on the running performance of the C-DAS fitted train.
12. C-DAS display complies with Human Factors standards and specifications, and minimises impact on the driver, e.g. fatigue, glare, confusion, etc.
13. Cab design will undergo an ergonomic assessment to minimise the impact to the driver following the introduction of a C-DAS display.
14. The driver is able to suppress C-DAS if incorrect information is presented / displayed on C-DAS display.
15. When C-DAS is unavailable longer-term performance will be indirectly impacted as no feedback of train performance against the timetable can be provided to Capacity Planning.
16. In Auto Suppression areas, the driver is likely to need to concentrate on additional tasks and pay attention to surrounding environment. If C-DAS presents a display when it shouldn’t, and driver is in ETCS mode OS, there is a risk that the driver misses an impending hazard (trespasser, obstruction, etc.).
17. C-DAS only has one source of power supply, sourced from the Train Main power supply (no redundant power supply).
18. C-DAS is used during Normal, Degraded and Emergency modes of operation.
19. The technical outputs from C-DAS are specified as data sent to TMS, data presented on C-DAS display (to the driver), and/or data presented to the C-DAS maintainer, if they are using separate device(s) for maintenance.
20. The interfaces identified were Data, Physical, Electrical and Environmental.

21. The Cyber Security breach can happen at any point in time and is either related to Data, Physical and Electrical inputs and Data and Physical outputs, and can be intentional or unintentional.
22. The interface protocol to the Traffic Management System (or legacy control systems) will be defined by the TMS.

10.2 Environmental

None

10.3 Operational

1. It is assumed that ETCS Level 2 operation will be undertaken using metric units, therefore C-DAS will be required to display information in the same format whilst the train is operating in an ETCS Level 2 area.

10.4 System Integration

1. C-DAS will be deployed as part of a DR System of Systems, however if, for instance, Traffic Management is not implemented by a project then equivalent functionality will not be available and C-DAS will operate as a standalone DAS product.

10.5 Maintenance

None

Digital Railway

Working together for a better railway:

Department for Transport

Rail Delivery Group

National Rail

NetworkRail

RFG Rail Freight Group

Rail Supply Group

Railway Industry Association

RSSB

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