ATO - GB New Trains Onboard Subsystem Requirements Specification

Prepared By:
Abdalla Allie
Systems Engineer

Date: 21st July 2017

Industry Review By:
ERTMS Systems Body (ESB)

Operational Strategy Group (OSG)

Date: 4th July – 18th July 2017

Authorised By:
Andrew Simmons
Chief Systems Engineer

Date: 31st July 2017

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

Published by:
The STE ETCS Team

© Copyright 2017 Network Rail Infrastructure Ltd
Electronic File Location

Issue record:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>28/04/2017</td>
<td>Initial Draft – for ATO RVE group review</td>
</tr>
<tr>
<td>0.2</td>
<td>09/06/2017</td>
<td>Update after Rail Vehicle Engineer &amp; Control Command Signalling expert review</td>
</tr>
<tr>
<td>0.3</td>
<td>03/07/2017</td>
<td>Update after System Requirements Steering Group review</td>
</tr>
<tr>
<td>0.4</td>
<td>28/07/2017</td>
<td>Update after ERTMS System Body review</td>
</tr>
<tr>
<td>1.0</td>
<td>31/07/2017</td>
<td>First Issue</td>
</tr>
</tbody>
</table>

Disclaimer:

Network Rail 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. Network Rail 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.
Contents

1 Introduction 4
  1.1 Purpose of this document 4
  1.2 Scope 4
  1.3 Context 5
  1.4 Abbreviations 5
  1.5 Requirements Form, Applicability and Identification 5
  1.6 Requirements Assurance 6
  1.7 Requirements Change 7
  1.8 Areas for development 7

2 ATO New Train Onboard Requirements 8
  2.1 Fit For Purpose 8
  2.2 ATO Isolation 12
  2.3 ATO Reset 14
  2.4 Power Supply 15
  2.5 Cab Detection 17
  2.6 Self-Tests 18
  2.7 Key Management System 19
  2.8 Installation Design 20
  2.9 Maintenance 21
  2.10 System Support 27

Appendix A Definitions and Abbreviations 29
Appendix B List of Referenced Standards 31
Appendix C Areas for Development 33
1 INTRODUCTION

1.1 Purpose of this document

This document defines a set of Automatic Train Operation (ATO) requirements for new-build rolling stock, and is intended to promote effective implementation of ATO with the ETCS in new-build rolling stock projects on the GB rail network.

The requirements have been developed using the industry-agreed and issued National ETCS Requirements Management Strategy [RD2] and Plan [RD3], supplemented by a briefing note explaining how ATO fits within these documents [RD28].

These requirements have been developed as part of a suite of ATO requirements [RD9], [RD10] and [RD11] covering all elements required to optimise performance and operation of an ATO over ETCS railway. The ATO requirement suite is intended to be complementary to the GB ETCS requirements suite and should be used in association with these requirements [RD1], [RD4], [RD5], [RD6], [RD7] and [RD8].

These ATO onboard requirements for new build rolling stock have been specifically aligned to work alongside and be complementary to the ETCS Onboard New Trains Subsystem Requirements [RD8].

This Specification for the ATO Onboard solution has been written to complement the European Union Agency for Railways (ERA) specifications for Baseline 3 Release 2 ETCS [RD12], [RD13] together with the proposed amendments to this specification for ATO [RD29]. Every effort has been made to avoid conflict with these European specifications but, in case of conflict, the European specifications take precedence. Nothing in this document obviates any legal requirement to which any of the parties must comply.

The document is set out in the form of standard requirements with the ATO New Trains Onboard Subsystem (ANTOSS) identifier, followed by rationale and guidance notes, where appropriate.

1.2 Scope

This document contains the ATO requirements for new-build rolling stock that are to be implemented alongside the ETCS Onboard Subsystem Requirements for New Trains [RD8].

This specification provides requirements for the following Grades of Automation (GoA):

- GoA1 – Manual driving with ETCS, where the ATO Onboard solution functions as a Connected Driver Advisory System (C-DAS).
- GoA2 – Driver-attended ATO, the ATO Onboard solution controls train movement but the driver remains in the cab and retains responsibility for other operational functions.

Driverless ATO (GoA3) & Unattended ATO (GoA4) are out of scope of this requirements document.

Generic equipment installation requirements are omitted from this specification, unless deemed to be of particular use, on the basis that such requirements will be defined by the procuring agent for all vehicle systems. Equally, system performance requirements are also omitted from this specification, unless critical for ATO over ETCS operation, as any performance requirements for the system may be defined at vehicle level by the procuring agent rather than imposing a specific solution.

Specific requirements and domain knowledge for a particular fleet of trains are not included within this document and will need to be defined by the Contracting Entity or their appointed Agent.

---

1 Note: This document covers new installations; retrofit is covered by the ATO Retrofit Onboard Subsystem Requirements Specification [RD10]
Not all of the requirements within this document will be appropriate for all train procurement activities; the requirements placed upon new rolling stock may differ depending on the intended route, operator, service pattern, train type and supply contract. It is the responsibility of the agent procuring the rolling stock to select the appropriate requirements from this library.

Nothing in this document obviates any legal requirement with which any of the parties must comply. Furthermore, it does not preclude operation of a Technical Specification for Interoperability (TSI)-compliant vehicle on the GB rail network, or a vehicle compliant to this specification operating on TSI-compliant infrastructure outside the GB rail network.

1.3 Context
This document has been developed using information from the European ATO Trans-European Network – Transport (TEN-T) and Shift2Rail ATO development projects, alongside the results of the GB ATO over ETCS development programme and lessons learnt from the Thameslink project. It assumes that ATO will always operate with the ETCS, the ETCS providing the Automatic Train protection (ATP) functionality required to support ATO operation. It enables operation in C-DAS (GoA1) and Driver Attended ATO (GoA2).

1.4 Abbreviations
Other than for standard ATO terminology (e.g. GoA2 etc.), abbreviations are explained in full where used in Requirements. A fuller explanation of Terms and Abbreviations can be found in Appendix A and the ETCS Glossary [RD14].

1.4.1 Specific Terminology
Specific terms are used within the requirements contained within this document:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. rail vehicle and / or train</td>
<td>Installation of the ATO functionality will be expected in all rail vehicles and trains.</td>
</tr>
<tr>
<td>2. on-board</td>
<td>This refers to the functionality on-board the rail vehicle or train that excludes the ATO Onboard solution.</td>
</tr>
<tr>
<td>3. Onboard</td>
<td>This refers to the ATO functionality.</td>
</tr>
</tbody>
</table>

1.5 Requirements Form, Applicability and Identification

1.5.1 Requirement Functionality
Requirements may be functional or non-functional:

- **Functional Requirements** - Technical details that define what a system needs to accomplish, i.e. how suppliers’ equipment will be applied, what it needs to do, and what processes, procedures and rules need to be in place to achieve it.
- **Non-Functional Requirements** - Constraints on the design or implementation, such as performance, security, competence, training, and reliability requirements.

Functional and non-functional requirements have been derived from the ETCS Onboard Sub-system Requirements Specification [RD1].

1.5.2 Basic Requirement Form
All requirements are in the following form:
1.5.3 Safety Requirement
Where a requirement has been associated with a Safety Measure, this is identified.

1.5.4 Provisional Requirements
These are requirements which have been developed to cover areas where there are still open points in the European ATO specifications or further GB Industry discussion is required.

1.5.5 Normative / Application-Specific / Preferred status
Each requirement within this document is identified as one of: normative, preferred, or application-specific. These are defined as follows:

- Normative
  - Necessary to achieve compatibility or optimisation of the system in relation to the GB rail network, or
  - A system feature that is deemed to be cost-effective and universally beneficial.

Satisfaction of normative requirements in compliance with this document is expected to be a requirement of individual delivery contracts.

- Application-Specific
  - A requirement which may not be relevant or applicable to the application of an ATO Onboard to every vehicle. It is expected that where a requirement is applicable, it will be applied.

Satisfaction of application-specific requirements in compliance with this document is expected to be a requirement of individual delivery contracts, as appropriate to the vehicles being considered.

- Preferred
  - A requirement of lower importance which, whilst not essential, the industry would prefer were satisfied. It is expected that where a requirement is applicable, it will be applied.

Satisfaction of preferred requirements in compliance with this document is expected to be a requirement of individual delivery contracts but only if they are considered within individual delivery scope.

1.6 Requirements Assurance
Requirements assurance has been explained in the ATO Requirements Assurance Statement [RD15].
1.7 Requirements Change

Once this specification has been issued, the ETCS Requirements Change Control Process [RD16] will be used to raise Change Requests (CRs).

1.8 Areas for development

Noting that this document represents the best understanding of the needs of GB rolling stock at the time of publishing, it is recognised that there are a number of areas where the document may be deficient. New deficiencies may be identified as understanding of the ATO over ETCS solution develops, as well as areas being closed out through further work being undertaken. Current known areas of deficiency are listed in Appendix C.
2 ATO NEW TRAIN ONBOARD REQUIREMENTS

2.1 Fit For Purpose

The ATO Onboard solution shall be designed to include Automatic Train Operation (ATO) Grade of Automation 2 (GoA2), in accordance with the requirements of the ATO System Requirements Specification (Subset-125).

Status: Normative
Rationale: The ATO must be an interoperable subsystem.
Guidance: In advance of the publication of Subset 125 in the Command, Control, Signalling (CCS) TSI, copies can be obtained from the Digital Railway Programme.

The ATO Onboard solution shall be able to communicate with the ATO trackside using the ATO track/train interface specification (Subset-126).

Status: Normative
Rationale: The ATO must be an interoperable subsystem and must be capable of receiving real-time data.
Guidance: In advance of the publication of Subset 126 in the CCS TSI, copies can be obtained from the Digital Railway Programme.

The ATO Onboard solution shall include the ATO/ETCS Onboard Form Fit Functional Interface Specification (FFFIS) defined in Subset-130.

Status: Application-Specific
Rationale: To allow the ATO Onboard solution to be capable of interfacing with an ETCS Onboard system.
Guidance: To ensure that the ATO Onboard solution is capable of being interfaced to any ETCS Onboard that has the same interface. In advance of the publication of Subset-130 in the CCS TSI, copies can be obtained from the Digital Railway Programme.

The vehicle systems shall be designed to operate in ATO GoA2.

Status: Normative
Rationale: The integration of the ATO in to the train will be simplified by providing the required interfaces and the level of control required.
Guidance: The vehicle control systems will be designed to provide the required interfaces and control granularity needed by an ATO implementation. This will include measures such as:
• providing sufficient brake and traction steps for fine train control.
• smooth blending of braking systems.
• prevention of jerk.
• appropriate application of traction and release of braking (e.g. to avoid rollaway when starting on an uphill gradient).
• using standard / open control interfaces for train systems.
• sufficient capacity in existing data buses and train management systems for ATO related information.

The on-board odometry system shall be capable of providing a stopping accuracy of +/-0.5m for 99.99% of station stopping points.

<table>
<thead>
<tr>
<th>Status:</th>
<th>Normative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale:</td>
<td>ATO is likely to have a more onerous requirement upon the odometry system than would be required for the ETCS. Odometry for ATO can be provided from the ETCS on-board or from another system.</td>
</tr>
<tr>
<td>Guidance:</td>
<td>A high level of positional accuracy is needed to ensure accurate stopping of the vehicle, particularly at station stopping points, where the ETCS System Requirements Specification (SRS) requirement for 5% +/- 5m would be insufficient. Where ATO is integrated within the ETCS Onboard (either from build or as a later upgrade), the ETCS odometry measurement equipment must therefore provide a greater level of accuracy. This figure has been derived from the Thameslink performance requirements as currently no European performance requirements for interoperability exist.</td>
</tr>
</tbody>
</table>

The Train Control Management System shall be capable of determining the loading of the train, and be capable of transmitting that information to external systems including the ATO Onboard solution.

<table>
<thead>
<tr>
<th>Status:</th>
<th>Preferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale:</td>
<td>Calculation of the dynamic weight and loading of a train can be used to improve ATO performance.</td>
</tr>
<tr>
<td>Guidance:</td>
<td>Traffic Management and ATO systems may be able to optimise train movements based upon passenger numbers and locations, thereby improving the efficiency of the railway. Transmission of loading data by the Train Control Management System would support this.</td>
</tr>
</tbody>
</table>

The ATO Onboard solution shall dynamically adjust traction and braking effort to achieve the calculated ATO Operational Speed Profile.

<table>
<thead>
<tr>
<th>Status:</th>
<th>Normative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale:</td>
<td>For optimum ATO performance the ATO needs to follow the ATO Operational Speed Profile calculated by the ATO Onboard solution and limit any impact by external factors.</td>
</tr>
<tr>
<td>Guidance:</td>
<td>The ATO Onboard solution needs to be able to compensate for increased loading of the train, loss of motor(s) on some traction units or environmental conditions and still achieve the required acceleration rate.</td>
</tr>
</tbody>
</table>

The Train Control Management System shall monitor wheel slip and slide activity, and be capable of transmitting that information to external systems including the ATO Onboard solution.

| Status: | Normative |
Rationale: The ATO low adhesion management function requires wheel slip and wheel slide input in order to achieve the required performance.

Guidance: Automatic Train Operation Systems rely on understanding adhesion conditions in order to manage the train performance. The train’s braking performance is dependent upon the available adhesion; the Wheel Slip/Slide Protection System will provide data on changes in adhesion to the Train Control Management System. The Train Control Management System should then be capable of sending the data to the Traffic Management Layer, the ATO Onboard solution, ETCS Onboard, or other systems, so that the traffic patterns and braking curves can be amended.

It shall be possible, based on the wheel slip and wheel slide activity for the Train Control Management System, to report an increase or decrease in adhesion conditions.

ANTOSS-9

Status: Normative

Rationale: The ATO Onboard solution needs to be aware of adhesion conditions to dynamically adjust traction and braking calculations when applying traction or braking effort. Small instances of WSP activity, which do not affect performance, need not give rise to a change of traffic regulation, or adjustment of the ATO / ETCS braking curves. It is for the Train Control Management System to report only those incidents of low adhesion which warrant a re-definition of the traffic regulation or brake curves.

Guidance: It is preferable to have at least three classifications of wheel slip/slide activity - none, minor and major - to allow Traffic Management systems to determine braking strategies for following trains and for ATO to adjust its low adhesion management accordingly.

The Train Control Management System shall provide the ATO Onboard solution with any traction force limits.

ANTOSS-10

Status: Normative

Rationale: Based on the train consist and the loading of the train the ATO Onboard solution will take into consideration any limits with regard to the amount of traction force that can be applied.

Guidance: The Train Control Management System can calculate the safe limits of traction that can be applied for a particular train consist and train loading. It will also ensure that this limit is never passed.

The ATO Onboard solution shall be capable of operating in GoA1 providing Connected Driver Advisory System (C-DAS) information when the ETCS Onboard is in Level NTC with NID_NTC = 20 or 21.

ANTOSS-11

Status: Normative

Rationale: The train cannot be driven automatically when operating under TPWS/AWS but it will still be possible to provide the driver with driver advisory information.

Guidance: The ATO Onboard solution can operate as a driver advisory system in GoA1 for ETCS Levels 1, 2 and 3. When operating over Level NTC for Class B systems, e.g. TPWS/AWS, the ATO Onboard solution can also...
operate as a driver advisory system, but this needs to be properly configured to the Class B system.

The ATO/C-DAS information to be displayed to the driver shall be integrated onto the ETCS Driver Machine Interface (DMI) in accordance with the updated DMI specification.

ANTOSS-12

Status: Normative

Rationale: From an ergonomic point of view it is better for the driver advisory information and the information displayed when driving automatically to be displayed on the same screen as the ETCS information.

Guidance: In advance of the publication of the updated CCS TSI, copies for the DMI specification can be obtained from the Digital Railway Programme. The system should take account of the ergonomics and human factors principles outlined in [RD21] to [RD26] and the DMI National Requirements [RD27].

There shall be no additional train data entry required for ATO.

ANTOSS-13

Status: Normative

Rationale: The driver has to input considerable amounts of data for ETCS already; the introduction of ATO will not increase the workload of the driver in this respect. The ATO Onboard solution will receive all train data either from the ETCS Onboard or from the Traffic Management System.

Guidance: The ATO specifications will specify that train data can be provided to the ATO Onboard solution and, therefore, to the ETCS Onboard via the ATO communication channel. Traffic Management Systems or Railway Undertaking business systems can provide this information to the ATO Trackside.

The ATO Onboard solution shall be capable of commanding the automatic opening and closing of the train doors.

ANTOSS-14

Status: Normative

Rationale: The ATO Onboard solution will be able to automatically command the train doors to open and close but the door control system on-board the train will be responsible for managing the safe authorisation for opening train doors and the safe confirmation that train doors are closed and locked. The ATO Onboard solution can be configured to command the doors to open automatically when the train has stopped accurately at the planned stopping point. The ATO Onboard solution can also be configured to command the doors to close automatically when the dwell time has elapsed.

Guidance: The ATO is not a safety-critical system. Safety requirements for door control will be managed by the door control system on the rolling stock. Opening and closing of the doors by ATO can be configured to be manual or automatic.

[Provisional] As a minimum, the ATO Onboard solution shall meet the on-board performance requirements specified in the ERTMS reliability specification (NR/AM/SA/SPE/00147).
Status: Normative

Rationale: If the train performance on a route is going to rely on ATO operation there should be a clear specification on the reliability required from the system. The ERTMS reliability specification NR/AM/SA/SPE/00147 will be updated to include the ATO reliability specification.

Guidance: The ATO reliability specification, which includes the Onboard and Trackside elements of the system, defines reliability and availability targets for the ATO.

The labelling containing the part number, serial number and modification version of all line-replaceable units shall be sited in a position where it can be easily read with the unit installed in its normal working position.

ANTOSS-16

Status: Normative

Rationale: Recording the modification version on line-replaceable components should assist in distinguishing between units during replacement activities or during storage.

Guidance: The modification version of a unit will relate to its software, firmware, hardware and parameter versions, as appropriate.

The part number, serial number and modification version of all software-driven line-replaceable units shall be available to be viewed electronically.

ANTOSS-17

Status: Preferred.

Rationale: The ability to view electronically the configuration of the line-replaceable units of the system allows for rapid verification of the modification state; this is particularly of use during a modification programme.

Guidance: Such functionality could be provided by the system in question; however, an integrated solution using the on-board Train Management System may be preferable. Software-driven’ line-replaceable units include all equipment that can feasibly report its status to the train, but excludes ‘hardware-only’ line-replaceable units without such intelligence.

2.2 ATO Isolation

An ATO isolation facility shall be provided for the driver to isolate the ATO system.

ANTOSS-18

Status: Normative

Rationale: The ATO will sometimes need to be isolated physically from the traction / brakes and other on-board equipment / systems.

Guidance: The isolation facility may be a switch, button, Train Management System function, or other facility of the appropriate safety and security integrity level.

The isolation facility should meet the requirements set out in GM/RT2185 for visibility and operation, in particular, that an indication should be provided in each cab. Although GM/RT2185 is for safety systems it is seen as good practice for ATO.

Some trains use a ‘Safety systems isolated’ indicator in the cab to comply with the requirements set out in GM/RT2185 for visibility of
isolation status. The means of isolating the ATO should be visible to the driver but not in such a way as to make the train unfit for service. GM/RT2185 requires that it not be possible to isolate the system whilst the vehicle is moving. This may be achieved by placing the isolation facility out of the reach of the driver in their normal operating position, or inhibiting the function when the vehicle is moving.

The ATO isolation facility shall be available in each driving cab.

**ANTOSS-19**

**Status:** Application-Specific

**Rationale:** The driver needs to be able to isolate the ATO without leaving the cab.

**Guidance:** Though provision should be made to allow the isolation of the ATO from any cab, it should only be functional in the active cab. The isolation facility will be located beyond the reach of the driver when in the normal driving position.

The ATO isolation facility shall only act upon a single ATO Onboard solution.

**ANTOSS-20**

**Status:** Status: Normative

**Rationale:** Rationale: In most cases, the need to isolate the ATO should be limited to a single ATO Onboard solution.

**Guidance:** Where a vehicle is fitted with more than one ATO Onboard solution (e.g. long trains where the economics dictate that to be the most effective option), then operation of the isolation facility should only act upon a single ATO Onboard solution. This retains the ability for ATO operation from the remaining non-isolated cab.

Isolating the ATO Onboard solution shall be recorded on a vehicle Data Recording Unit.

**ANTOSS-21**

**Status:** Normative

**Rationale:** Isolating the ATO has operational implications and needs to be recorded.

**Guidance:** In this context ‘Data Recording Unit’ may be the Juridical Recording Unit (JRU), On Train Monitor Recorder (OTMR), or combined JRU / OTMR equipment.

A controlled method of de-isolating the ATO Onboard solution shall be employed.

**ANTOSS-22**

**Status:** Normative

**Rationale:** The ATO functionality will have been isolated physically from the traction / brakes and other on-board equipment / systems and a controlled method is required for de-isolation.

**Guidance:** This is normally required for safety systems but is seen as following best practice for ATO. In this context, a controlled method is one where only those with authority to de-isolate the ATO functionality are able to do so. This may involve the use of a reset code or special key; the use of a standard T key or driver’s key would not be advised. The decision as to who is authorised to de-isolate the ATO, and is
De-isolation of the ATO Onboard solution shall not require complex procedures.

**Status:** Normative  
**Rationale:** Complex procedures could result in mistakes.  
**Guidance:** A mechanical or electronic key or a reset code could be used to de-isolate the ATO functionality. De-isolation procedures that require configuration or take time to perform (for example, using a laptop computer) are not advised. The mechanism for de-isolating the ATO functionality should be no more complex than that used to de-isolate any Class B safety system.

It shall be technically possible to operate the rail vehicle or train indefinitely with the ATO Onboard solution in isolation.

**Status:** Normative  
**Rationale:** To minimise unnecessary service disruption where trains can continue to operate normally under the control of a driver.  
**Guidance:** To facilitate or support continued service operation with ATO isolated on infrastructure equipped with a signalling system that supports and protects manual driving.

### 2.3 ATO Reset

It shall be possible for the driver temporarily to remove power only to the ATO Onboard solution through an ATO reset facility and then reinstate it in order to force the system to reset.

**Status:** Normative  
**Rationale:** This function provides an efficient means of resetting the ATO Onboard solution in the event of a failure, without the need to shut down and restart other systems on the traction unit.  
**Guidance:** This will not be a Miniature Circuit Breaker (MCB) but a dedicated reset switch. It could be part of the ATO selector.

No special tools or equipment shall be required to reset the ATO Onboard solution.

**Status:** Normative  
**Rationale:** This will ensure that the ATO is immune to any prohibitive methods preventing a necessary reset.

Resetting the ATO Onboard solution shall not necessitate the operation of other vehicle systems.

**Status:** Normative  
**Rationale:** The resetting of ATO needs to be achieved without impacting other on-board systems.
Guidance: A dedicated ATO reset facility needs to be provided. This facility could be provided by a switch, button, Train Management System option, or other option that exists to remove power from the ATO alone. Use of other functions or operations which remove power from the ATO and other systems simultaneously (e.g. which open the battery switch or power master switch) are not preferred.

The ATO reset facility shall be protected against accidental use.

**Guidance:**

**Status:** Normative

**Rationale:** Accidental resetting of the ATO has operational implications and needs to be avoided.

**Guidance:** In the case of a physical switch, this may be achieved by placing it under a safety cover. A virtual control could prompt for confirmation to prevent accidental use.

The ATO reset facility shall be placed in each driving cab within reach of the driver.

**Guidance:**

**Status:** Normative

**Rationale:** The driver needs to be able to reset the ATO on the move.

**Guidance:** Though provision should be made to allow the ATO to be reset from any cab, it should only be functional in the active cab. The ATO reset facility could be on the driver’s desk as part of the ATO selector.

Each ATO Onboard solution shall be reset independently.

**Guidance:**

**Status:** Normative

**Rationale:** In most cases, the need to reset the ATO should be limited to a single ATO Onboard solution.

**Guidance:** Where a vehicle is fitted with more than one ATO Onboard solution (e.g. long trains where the economics dictate that to be the most effective option), then the ATO reset facility should only act upon a single ATO Onboard solution.

Operation of the ATO reset facility shall be recorded on a vehicle Data Recording Unit.

**Guidance:**

**Status:** Normative

**Rationale:** Resetting the ATO has operational implications and needs to be recorded.

**Guidance:** In this context ‘Data Recording Unit’ may be the Juridical Recording Unit (JRU), On Train Monitor Recorder (OTMR), or combined JRU / OTMR equipment.

### 2.4 Power Supply

**Guidance:**

**Status:** Normative
Rationale: It is feasible that electronic train systems may be de-energised temporarily during start-up / shutdown sequences or power supply disturbances, meaning that they do not go through their full power-up sequence.

Guidance: The ATO Onboard solution will need to be prevented, within the vehicle design, from being de-energised temporarily during start-up / shutdown sequences or power supply disturbances, or, alternatively, the equipment will need to be designed to tolerate such scenarios without being damaged or causing it to fail.

The ATO Onboard solution shall energise automatically only when the primary source of power is available.

ANTOSS-33

Status: Normative
Rationale: This function removes the need for a separate ‘ATO ON’ button. The means of achieving automatic energisation will be specific to the vehicle design.
Guidance: An automatic energisation should occur when, and only when, primary power is available, so that the risk of the unsupported back-up power being discharged by the ATO Onboard solution is minimised. The ATO Onboard solution should not start automatically if only unsupported back-up power is available.

It shall be possible to energise the ATO Onboard solution manually without the primary source of power being applied.

ANTOSS-34

Status: Normative
Rationale: This function provides the ability to energise parts of the ATO Onboard solution manually for some maintenance activities, as well as giving further scope for vehicle rescue in the event of engine / electric failure.

The ATO Onboard solution shall remain active for at least 10 minutes after loss of primary power before being load-shed.

ANTOSS-35

Status: Normative
Rationale: Loss of primary power should not cause the ATO Onboard solution to de-power immediately; this is to allow the vehicle to continue in operation without disruption, and to allow the driver to select the stopping position for the train when the primary power is lost.
Guidance: The ATO Onboard solution is not expected to de-power as soon as primary power is lost (e.g. during traction gaps, temporary Overhead Line Equipment (OLE) trips, temporary shutdown of engine etc.). A delay of 10 minutes is considered to be sufficient to mitigate the performance risk from the majority of unplanned interruptions in electrical power supply or vehicle engine operation. Failures of the primary source of power that last significantly longer than 10 minutes are judged to be less frequent where the additional delay of restarting the ATO Onboard solution is less critical.
In the event of a loss of primary power, the ATO Onboard solution shall be load-shed before the vehicle’s unsupported back-up power voltage becomes critically low.

**Status:** Normative  
**Rationale:** The aim should be to maintain only essential services for as long as possible after loss of primary power.  
**Guidance:** In the context of this requirement, critically low unsupported back-up power voltage means there would be an inability to power other higher priority vehicle systems for the required duration, for example, emergency lighting, voice radio, or the ability to re-start the vehicle engine etc.  
ATO is less critical than the ETCS so could be load shed if this would keep the ETCS energised when the vehicle’s back-up power becomes critically low. Critically low’ is a vehicle-specific definition. This could occur before the 10 minutes have elapsed as specified in ANTOSS-35.

### 2.5 Cab Detection

**[Provisional]** It shall be possible to close the desk remotely from the opposite end of the vehicle, unit or train, subject to certain conditions being met.

**Status:** Application-Specific  
**Rationale:** This will avoid the need for the driver to walk the length of the train.  
**Guidance:** The ability to perform an automatic turnaround of the train is needed. This will allow the driver to leave the cab while an Automatic End of Mission is performed for the ATO and the ETCS. In the event that the desk is not closed by the driver upon leaving the cab, it will be possible to close the desk from the opposite end of the train, subject to certain conditions being met, for example:  
• enabling the cab active signal within another cab of the train.  
• operating the driving controls within another cab of the train.  
Likewise, certain circumstances may prevent the cab active being remotely cancelled, for example:  
• the vehicle is moving.  
• a direction is still selected in the original cab.  
Such a method of remotely closing the desk means that the ‘cab open’ function may be better served by a push button or Train Management System option, rather than a physical switch or key that cannot be reset remotely.

**[Provisional]** Subject to certain conditions being met, a desk shall automatically close after a configurable time delay.

**Status:** Application-Specific  
**Rationale:** Whilst desk closure is beneficial for security, there are operational benefits to leaving it open in certain circumstances.  
**Guidance:** The active ATO desk will automatically close after a vehicle-specific delay if it can be inferred that the driver has left the cab. Such signals may be that:  
• the vehicle is stationary.  
• no direction is selected.
• there has been no driver interaction with the DMI or controls during that period.
A typical delay may be 30 minutes to account for the driver leaving the cab to attend to an incident elsewhere on the vehicle, although this will depend upon the preference of the Railway Undertaking.

It shall be possible to secure a rail vehicle or train from unauthorised operation whilst retaining the cab active signal.

ANTOSS-39

Status: Normative
Rationale: The driver may be required to attend to issues on the rail vehicle or train, which would preferably be done without losing the Journey Profile. The driver should be able to secure the rail vehicle or train from movement by unauthorised persons whilst still retaining the cab active signal.

Where there is only one ATO Onboard solution, the driver shall be able to see an indication in their cab that the ATO Onboard solution has been isolated from the other cab.

ANTOSS-40

Status: Application-Specific
Rationale: The driver needs to be aware of the ATO status.
Guidance: This could be displayed on the integrated ETCS/ATO Driver machine Interface (DMI).

Where two ATO Onboard solutions exist, an indication as to the status of both shall be displayed (or indicated) in both cabs.

ANTOSS-41

Status: Application-Specific
Rationale: This applies to a single vehicle where two ATO Onboard solutions are present.
Guidance: Indication should make clear which ATO on-board is isolated.

2.6 Self-Tests

The ATO Onboard solution shall automatically inform the driver that the ATO is functioning correctly before being used to control rail vehicle or train movements.

ANTOSS-42

Status: Normative
Rationale: The driver needs to be aware of the status of the ATO.
Guidance: This can be displayed using the integrated ETCS/ATO DMI during the Start of Mission (SoM) procedure.

Where two ATO Onboard solutions exist on-board, an indication as to the status of both ATO Onboard solutions shall be displayed (or indicated) in both cabs.

ANTOSS-43

Status: Application-Specific
Rationale: This applies to a single vehicle where two ATO Onboard solutions are present.
Guidance: This can be displayed using the integrated ETCS/ATO DMI in each cab.

The ATO Onboard solution shall be capable of performing any ATO initialisation or self-test routine without the presence of specific ATO trackside infrastructure.

**Status:** Normative

**Rationale:** This will prevent any ATO initialisation failure that could result from performing the self-test on routes without ATO capability.

The ATO Onboard solution shall be capable of performing any ATO initialisation or self-test routine without the presence of an operator during the course of the test.

**Status:** Normative

**Rationale:** This supports remote vehicle starting, allowing the unit to be prepared for operation ahead of the driver’s arrival.

The results of any ATO initialisation or self-test shall be displayed in a succinct, intuitive form.

**Status:** Normative

**Rationale:** Providing the driver with information on faults upon which they cannot act provides no benefit, and may overload the driver with unnecessary information.

**Guidance:** It is envisaged that information would be provided in plain English at all times; use of foreign languages which the driver would have to interpret would not be deemed to meet the requirement. Provision of data as a series of fault codes which have to be interpreted by the user would also be deemed unsatisfactory.

### 2.7 Key Management System

[Provisional] Each ATO Onboard solution belonging to the GB Key Management (KM) Domain shall be able to accept an upload of offline encrypted authentication keys via transfer media, as appropriate.

**Status:** Normative

**Rationale:** To provide a fallback mechanism for the secure and efficient distribution of authentication keys.

**Guidance:** Transfer media covers compact disks, memory sticks, etc.

[Provisional] Each ATO Onboard solution belonging to the GB Key Management (KM) Domain shall be able to receive keys in accordance with Subset-137 without interruption to service.

**Status:** Normative

**Rationale:** The upload of online encrypted authentication keys will not impact the operational performance of the vehicle.
[Provisional] Each ATO Onboard solution belonging to the GB Key Management (KM) Domain shall be able to support unique transport keys for their KMC – ATO entity relationship (e.g. Key Management Centre (KMC) – ATO-OBU).

**Status:** Normative  
**Rationale:** This reduces the consequences of a compromised key.

[Provisional] Each ATO Onboard solution belonging to the GB Key Management (KM) Domain shall be able to support unique authentication keys for each relevant ATO trackside.

**Status:** Normative  
**Rationale:** This reduces the consequences of a compromised key.

[Provisional] The ATO Onboard solution shall store and action downloaded key data in accordance with its validity period.

**Status:** Normative  
**Rationale:** Downloaded keys will have a validity period that needs to be actioned by the ATO Onboard solution.

[Provisional] The maintainer shall be able to set the periodicity for online update requests from an ATO Onboard solution belonging to the GB Key Management (KM) Domain.

**Status:** Normative  
**Rationale:** The periodicity of online update requests needs to be modifiable by an authorised person.

### 2.8 Installation Design

The ATO Onboard solution shall incorporate modularity and the facility to upgrade or replace parts of the system separately.

**Status:** Preferred  
**Rationale:** As with most on-board electronic components, the ATO Onboard solution should be easily replaceable and modular in design.

All equipment shall be tolerant of cleaning using the typical range of cleaning materials and processes used in the railway environment.

**Status:** Normative  
**Rationale:** This applies to all cab equipment (including the DMI and all other controls and indicators) and saloon-mounted equipment. Cleaning these items should not be an issue or require additional provisions to the ones currently used.

**Guidance:** Exterior equipment is subject to acid and/or alkaline cleaning chemicals applied at pressure, or forcibly through brushing action. High pressure hot water with or without detergent, or steam might also be applied.
The ATO Onboard solution shall be designed to afford protection from vandalism and accidental damage by drivers, train crew, other staff and members of the public.

**Status:** Normative  
**Rationale:** The equipment needs to be robust and tolerant of misuse.

### Externally mounted ATO equipment

Externally mounted ATO equipment shall be designed to continue to function when subjected to the conditions and impacts reasonably expected in normal service operation.

**Status:** Normative  
**Rationale:** Any additional ATO component that needs to be mounted externally should function as seamlessly as any other external train component.  
**Guidance:** For ATO this is currently limited to any additional antenna required, but could apply to other supplementary systems such as external obstacle detection devices.

## 2.9 Maintenance

[Provisional] The ATO Onboard solution shall, as a minimum, meet the on-board Mean Active Repair Time (MART) requirements for underbody mounted equipment specified in the ERTMS Reliability Specification (NR/AM/SA/SPE/00147).

**Status:** Normative  
**Rationale:** The MART requirements are considered best practice to date.  
**Guidance:** NR/AM/SA/SPE/00147 defines reliability and availability targets for the ETCS, which are then apportioned to the respective elements of the Onboard and Trackside.

ATO line-replaceable units shall be clearly delimited and marked to prevent subdivision, loss of configuration, or traceability.

**Status:** Normative  
**Rationale:** This is important for equipment where staff may exchange components during fault-finding, resulting in loss of configuration and traceability.

It shall take no more than fifteen minutes for an integrated ETCS/ATO Driver Machine Interface (DMI) to be replaced, configured and tested by a single trained person.

**Status:** Application-Specific  
**Rationale:** DMIs are expected to need replacing more regularly than other components. This should be a quick operation performed by a single trained person.  
**Guidance:** Whilst most components will be changed at maintenance depots, it is feasible that DMIs will be swapped out by station-based maintenance staff while the train or other rail vehicle is in service. Because of this, the requirements for changing a DMI are much more stringent than those for other components.
Specialist anti-static, bench test or clean room precautions shall not be required to maintain the ATO Onboard solution.

**Status:** Normative

**Rationale:** The low failure rate required of the ATO Onboard solution should not precipitate a need for specialist equipment or facilities in depots.

**Guidance:** A separate clean and dry store for electronic equipment is, however, justifiable.

Failure of ATO Onboard solution elements shall be easily identifiable during maintenance.

**Status:** Normative

**Rationale:** It is common practice to use switches and contacts (in serial or parallel, depending upon the implementation) to reduce the chance of a single switch failure causing a hazard or immobilizing failure of the rail vehicle or train. If latent failures of equipment in such circuits are not identified then it may eventually lead to a hazard or a system failure.

**Guidance:** This function may be achieved through monitoring of back contacts (either by the Train Management System or separate ‘tell-tale’ indicators), or ATO Onboard solution test cycles that independently test any parallel output at an appropriate juncture. A dedicated test tool may be deemed acceptable if it is simple to operate and requires limited intrusion into the vehicle systems.

Diagnostic tools shall be simple to operate and interpret.

**Status:** Normative

**Rationale:** Complex diagnostic tools can lead to error or delay in determining faults.

**Guidance:** Diagnostic tools include maintenance download, fault finding, interrogation and performance analysis tools.

Software-based diagnostic tools shall be designed for use on standard modern operating systems.

**Status:** Preferred

**Rationale:** This is to allow the software to be installed and used seamlessly.

**Guidance:** The software should not rely on legacy operating systems for its operation; it should function correctly within modern, commercially available operating systems. This may include, but is not limited to, Windows, iOS, Linux and Android systems.

Software-based diagnostic tools shall not require complex procedures for manual input and recording of output.

**Status:** Normative

**Rationale:** A software diagnostic tool should not require complex use or specialist knowledge to input data or record the output.
Software-based diagnostic tools shall not cause data or software corruption during download.

**Status:** Normative

**Rationale:** Corruption during download can lead to error or delay in interpretation.

Software-based diagnostic tools shall use modern, universally available interfaces for communicating with the ATO Onboard solution.

**Status:** Preferred

**Rationale:** Ethernet, USB, Wi-Fi and other common interfaces will be utilised to avoid potential obsolescence issues with the device hardware.

**Guidance:** RS232, RS485 and other legacy interfaces should be avoided.

Functionality shall be provided to download remotely ATO diagnostic information stored onboard while the rail vehicle or train is in service.

**Status:** Application-Specific

**Rationale:** The ability to identify faults within the ATO Onboard solution from locations remote to the vehicle is deemed to be beneficial.

**Guidance:** This may be facilitated through exporting system fault logs at defined intervals, or on demand via a remote communication medium.

The Data Recording Unit shall be provided with a channel for ATO

**Status:** Normative

**Rationale:** ATO can use the same Data Recording Unit as the ETCS, the JRU, or a separate Data Recording Unit.

**Guidance:** GM/RT2472 specifies the minimum requirements for on-train monitoring and recording.

Functionality shall be provided to download data from the Data Recording Unit remotely whilst the vehicle is in service.

**Status:** Application-Specific

**Rationale:** The ability to download data from the ATO Onboard solution from locations remote to the vehicle is deemed to be beneficial. It may be considered acceptable for only a subset of the data to be available for download whilst the vehicle is in motion if it can be shown to be sufficient for the needs of the operator.

**Guidance:** This may be facilitated through exporting data logs at defined intervals, or on demand, via a remote communication medium.

Authorised people shall be provided with diagnostic information sufficient to confirm that the complete ATO Onboard solution is operational and functioning correctly.

**Status:** Normative
**Rationale:** Confirmation of correct functionality is particularly important after corrective or preventive maintenance has been carried out.

**Guidance:** Authorised people include: competent personnel (technicians, fitters, drivers, maintainers, etc.) appointed by the Railway Undertaking or company responsible for the rolling stock and its safety management system.

Authorised people shall be provided with diagnostic information sufficient to allow the diagnosis of faults to a single ATO line-replaceable unit.

ANTOSS-71

**Status:** Normative

**Rationale:** Clear indication of defects aids efficient corrective action.

**Guidance:** Authorised people include: competent personnel (technicians, fitters, drivers, maintainers, etc.) appointed by the Railway Undertaking or company responsible for the rolling stock and its safety management system.

ATO Onboard solution diagnostic information shall be displayed to authorised persons without the need for equipment other than access keys.

ANTOSS-72

**Status:** Preferred

**Rationale:** As with most electronic equipment, a maintainer must be able to interrogate the ATO diagnostic information from displays / interfaces integrated within the ATO Onboard solution.

**Guidance:** There should be no need to use maintenance tools or laptop-based interrogation software, other than access keys, if located in a secure area.

ATO Onboard solution diagnostic information shall be recorded with a time stamp with sufficient resolution to identify all events accurately.

ANTOSS-73

**Status:** Normative

**Rationale:** A time stamp enables correlation of all recorded information.

**Guidance:** The ATO Onboard solution should use the same clock for time stamps as the ETCS Onboard solution.

The details and nature of faults within the ATO Onboard solution shall be recorded on-board the vehicle.

ANTOSS-74

**Status:** Normative

**Rationale:** All faults need to be downloaded for later evaluation.

The ATO Onboard solution shall be able to identify malfunctioning ATO line replaceable units to an authorised person before they cause a service failure.

ANTOSS-75

**Status:** Preferred

**Rationale:** Failures in unmonitored hardware (wiring degradation, sticking relays, etc.) cannot reasonably be expected to be identified before failure.
Guidance: Partial failure of redundant systems or tolerable but unusual activity are examples of faults which a system may reasonably identify before it results in a failure (e.g. abnormal data errors, dropped connections, inconsistent ATO input and software watchdog resets etc.).

Faults reported that relate to trackside ATO equipment issues shall be supported with information on the location and nature of the failure.

Status: Normative
Rationale: Full details of faults are required for later evaluation.
Guidance: Location information may be derived from the Last Relevant Balise Group and distance, or other relevant co-ordinates, if supported.

Information about ATO faults that require immediate driver attention shall be presented in an unambiguous, operationally meaningful manner.

Status: Normative
Rationale: Fault information will be presented in a way that minimises the likelihood of driver error.
Guidance: The acknowledgement of supplier-specific text messages informing of faults within the ATO Onboard solution is not specified. The requirement is for these text messages informing the driver of ATO faults that require immediate attention to be acknowledged by the driver. If the ATO fault leads to an unplanned transition to manual driving then the driver taking control of the traction brake lever is seen as acknowledgement of this transition.

Information about ATO faults that require immediate driver attention shall require acknowledgement.

Status: Normative
Rationale: Acknowledgement confirms that the driver has received the necessary information.
Guidance: The acknowledgement of supplier-specific text messages informing of faults within the ATO Onboard solution is not specified. The requirement is for these text messages informing the driver of ATO faults that require immediate attention to be acknowledged by the driver. If the ATO fault leads to an unplanned transition to manual driving then the driver taking control of the traction brake lever is seen as acknowledgement of this transition.

Information about ATO faults that require immediate driver attention shall persist after acknowledgement.

Status: Normative
Rationale: Persistence should ensure that the driver does not forget the fault.
Guidance: ‘End of display’ determines whether the message is deleted after acknowledgement or is retained in a list that can be scrolled. It is proposed that, owing to the message requiring immediate attention by the driver, it is appropriate for it to persist in the scrolling list of text messages.

Detailed maintenance information about the cause of ATO faults and appropriate remedial action shall be provided by the on-board systems.

Status: Preferred
Rationale: An ATO fault should be reported in relevant train management systems which can be accessed by the driver and/or maintainers.

Guidance: When the vehicle is fitted with train control systems which report faults directly to drivers, and/or to maintainers remotely, the ATO fault logging system should be integrated with the vehicle system if it is economical to do so. The failure of one system in an integrated solution should not affect the fault logging of other systems.

An access control system for ATO configuration settings and data shall be provided.

ANTOSS-81

Status: Normative

Rationale: An access control should prevent either malicious or accidental modification of the configuration settings and data.

Guidance: Access control should incorporate user identifications and appropriate access levels. This access control system will need to extend to the Train Management System, where it can be used to amend and upload revised configuration management settings. ‘System Security’ refers to security against unauthorised access to the ATO Onboard solution settings, configuration data, cryptographic keys, and software. Rigorous mechanisms and procedures should be adopted to avoid the ATO being compromised by malware. These should extend to the whole system, including maintenance and diagnostic equipment and all removable media. Before entering service, the ATO Onboard solution should have ATO cryptographic keys installed that are compatible with any ETCS Level 2 or Level 3 infrastructure on which it is required to operate. Subset-037 sets out how the keys are used.

The ATO Onboard solution shall be designed to reduce the risk of cyber-attack upon the ATO to an acceptable level.

ANTOSS-82

Status: Normative

Rationale: Cyber security is becoming increasingly important as modern protection systems become more and more software-based.

Guidance: Risks to consider may include the possibility of malicious remote operation of the ATO Onboard solution, remote editing of data within the ATO Onboard solution, remote disabling of the ATO Onboard solution, or unauthorised use of access keys to ATO Onboard solution equipment.

The level of risk from a cyber-attack will be determined and agreed with the Centre for the Protection of National Infrastructure.

Any ATO equipment not contained within a secure enclosure shall be failsafe in the event of tampering.

ANTOSS-83

Status: Normative

Rationale: Any non-enclosed equipment should not fail in a way that affects safety in the event of tampering.

Exclusive access to the ATO Onboard solution equipment enclosure shall be provided for staff via use of the relevant tool.

ANTOSS-84
Reference: STE/ATO/REQ/001
Issue: 1.0
Date: 31st July 2017

Status: Normative
Rationale: An access control will prevent either malicious or accidental entry to the equipment enclosure. The access tool should be the same as that for the ETCS to limit the number of tools required.

Guidance: The ‘relevant tool’ will vary depending on the fleet being fitted, but should be selected to align with the existing access arrangements for the particular fleet. For example, one fleet may use items from the ‘Southco’ product line, or equivalent compatible products which include:
• gated 8mm hex recess - maintainers (access to equipment cabinets)
• gated 8mm square driver - drivers (access to circuit breakers)
• gated 7mm triangle - driver manager (access to DMI)
Where maintainers and drivers / train preparers require access to equipment, two separate locked areas can be provided to allow them access only to the appropriate parts of the system. Each such area can be accessed by a separate key which is common for maintainers or for drivers / train preparers, as appropriate.

Status / fault indicators and download ports necessary for ATO maintenance and fault-finding shall be accessible only with access keys.

Status: Normative
Rationale: Maintenance and fault-finding indications may distract the driver unnecessarily.

Guidance:

Status or fault indicators necessary for ATO operations shall be visible without the need to gain entry using access keys.

Status: Normative
Rationale: Drivers or other operational staff may need to view fault indicators in service (e.g. for basic fault diagnosis in the event of failure). Such indicators need to be easily accessible to the driver.

Guidance: If personnel need to observe an indicator in an unauthorised area, a window should be used that allows visibility from an authorised area.

2.10 System Support

The ATO Onboard solution shall be supported by a lifecycle management plan which is in place on first authorisation of the rail vehicle or train.

Status: Normative
Rationale: A lifecycle management plan is part of the acceptance and strategy process on the GB railway.

Guidance: The ATO Onboard solution Lifecycle Management Plan will need links into a lifecycle management strategy for ATO over ETCS as a system on the rail network to enable effective configuration and reliability management through industry Data Recording, Analysis and Corrective Action System (DRACAS) processes. The System Authority (ESB) is able to provide further guidance in this area. Standard lifecycle support arrangements are also expected to be included and may include, but not be limited to:
• arrangements for update of equipment, including for obsolescence;
• spares provided;
• test equipment;
• endemic and epidemic faults;
• warranty support;
• ongoing training;
• repair processes;
• documentation updates;
• decommissioning and disposal;
• support for DRACAS processes;
• configuration management (including use of existing train operator systems, e.g. component tracker);
• reliability; and
• monitoring and trend analysis for all relevant applications of the supplier's ATO equipment and interoperable constituents.

The ATO Onboard solution system shall have its software updated with ATO Baseline releases in a reasonable timescale following the instruction for their implementation.

**Status:** Normative

**Rationale:** If requested by the owner / operator the ATO Onboard will be updated with the latest ATO Baseline release; this will require only a software update. This will allow the owner / operator to take advantage of enhancements and error corrections, while reducing the cost of upgrading the system.

**Guidance:** ATO is a software based system defined by a core European specification, and the GB Programme is deploying the first baseline of this specification. During the life of the system, system updates or maintenance releases will be required to fix errors, implement compatible functionality, and act upon feedback from other projects. This means that the system version deployed on an installation will need to change during the lifetime of the system to allow incorporation of the updates, and should be formalised contractually between owner / operator and supplier. A 'reasonable timescale' will be agreed between operator and supplier, after assessment of the content of the release and consideration of its impact on individual fleet operation. Compliance to this requirement would be judged on when first authorisation took place, when maintenance releases were issued, whether they had been deployed and, if not, checking that plans were in place to deploy, supported by the appropriate contracts and processes.
Appendix A  Definitions and Abbreviations

The following definitions are supplementary to those set out in reference document [RD12].

ANTOSS  ATO New Train Onboard Sub-System
ATO      Automatic Train Operation
ATP      Automatic Train Protection
AWS      Automatic Warning System
CCS      Control, Command and Signalling
CCS TSI  Technical Specification for Interoperability relating to Control, Command and Signalling
C-DAS    Connected Driver Advisory System
CR       Change Request
DMI      Driver Machine Interface
DRACAS   Data Recording, Analysis and Corrective Action System
EC       European Commission
ENTOSS   ETCS Onboard New Trains Sub-System
ERA      European Union Agency for Railways
ERTMS    European Rail Traffic Management System
ESB      ERTMS Systems Body
ETCS     European Train Control System
EVC      European Vital Computer
FFFIS    Form-Fit Functional Interface Specification
GB       Great Britain
GoA1, GoA2 Grade of Automation 1, Grade of Automation 2
JRU      Juridical Recording Unit
KM       Key Management
KMC      Key Management Centre
KMS      Key Management System
MART     Mean Active Repair Time
MCB      Miniature Circuit Breaker
OBU      Onboard Unit
OLE      Overhead Line Equipment
OTMR     On Train Monitoring Recorder
RAM      Reliability, Availability and Maintainability
SRS      System Requirements Specification
TCMS     Train Control Management System
TEN-T    Trans-European Network - Transport
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPWS</td>
<td>Train Protection and Warning System</td>
</tr>
<tr>
<td>TSI</td>
<td>Technical Specification for Interoperability</td>
</tr>
<tr>
<td>WSP</td>
<td>Wheel Slip Protection</td>
</tr>
</tbody>
</table>
Appendix B  List of Referenced Standards

Note: Unless otherwise stated, reference should be made to the most recent authorised version of the document.

[RD3] ETCS Requirements Management Plan, NEPT/ERTMS/REQ/0001
[RD12] COMMISSION REGULATION (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the ‘control-command and signalling’ subsystems of the rail system in the European Union
[RD13] Baseline 3 Release 2 (TSI CCS Annex A set of specifications #3)
[RD14] ERTMS Programme Glossary of Terms, NEPT/ERTMS/ADM/0002
[RD15] ATO Requirements Assurance Statement, CCMS No: TBC
[RD17] ERTMS Reliability Specification NR/AM/SA/SPE/00147 Issue: A07 – expected to be updated to include ATO
[RD20] GM/RT2185, Train safety systems
[RD22] GM/RT2161, Requirements for Driving Cabs of Railway Vehicles


[RD27] GE/RT8402, ERTMS/ETCS DMI National Requirements

[RD28] ESB ATO requirements plan briefing note 18/04/17

[RD29] European ATO specifications comprising Subset 125, Subset 126, Subset 130
### Appendix C  Areas for Development

<table>
<thead>
<tr>
<th>No.</th>
<th>Issue</th>
<th>Description</th>
<th>Identified in version</th>
<th>Closed in version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RAMs specification for ATO</td>
<td>ERTMS Reliability Specification NR/AM/SA/SPE/00147 Issue: A07 currently excludes ATO and needs updating to include it.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Status of European ATO specifications in the CCS TSI</td>
<td>These documents (SS125, 126, 130) are currently in final draft versions being processed for acceptance into the next version of the CCS TSI. This issue will remain open until final versions have been agreed by the European Union Agency for Railways for publication in the CCS TSI.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Interface to the ENTOSS</td>
<td>This document is aligned with version 2.0 of the ENTOSS as published on the 31/03/17 plus a CR containing ATO interface requirements. This issue will remain open until the ENTOSS has been updated to include contents of the CR.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>KMS and ATO secure communications</td>
<td>The issue of secure ATO communication is still an open point in the European ATO over ETCS specifications. It is assumed this will be handled by the KMS currently specified for ETCS. All requirements are therefore prefixed as provisional until this open point is closed.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Subset 139</td>
<td>This subset specifies the ATO Onboard solution interface to the train planned for future development; it will be possible for some of the ATO requirements in this document to be removed once this is published.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Adhesion Level</td>
<td>It is stated that there will be at least three classifications of wheel slip/slide because this is the minimum number required to be able to calculate if the adhesion factor needs to be increased or decreased. It needs to be determined if it would be acceptable that the way adhesion was managed for ATO would be train / supplier-specific. This is an ATO performance issue and not for safety.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>C-DAS operation in Level NTC (TPWS/AWS)</td>
<td>How C-DAS operates when the system is operating in ETCS Level NTC has not been fully defined e.g. issues regarding positioning.</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Automatic Turnaround/Turnback</td>
<td>The functionality of Automatic Turnaround (i.e. Automatic End of Mission in the cab to be closed and Automatic Start of Mission in new active cab); and Automatic Turnback (i.e. the ability of the ATO to operate the</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>train without operational staff in designated areas in order for next service preparation) still need to be added to the European Specifications. Until then it is listed here as an open point.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>