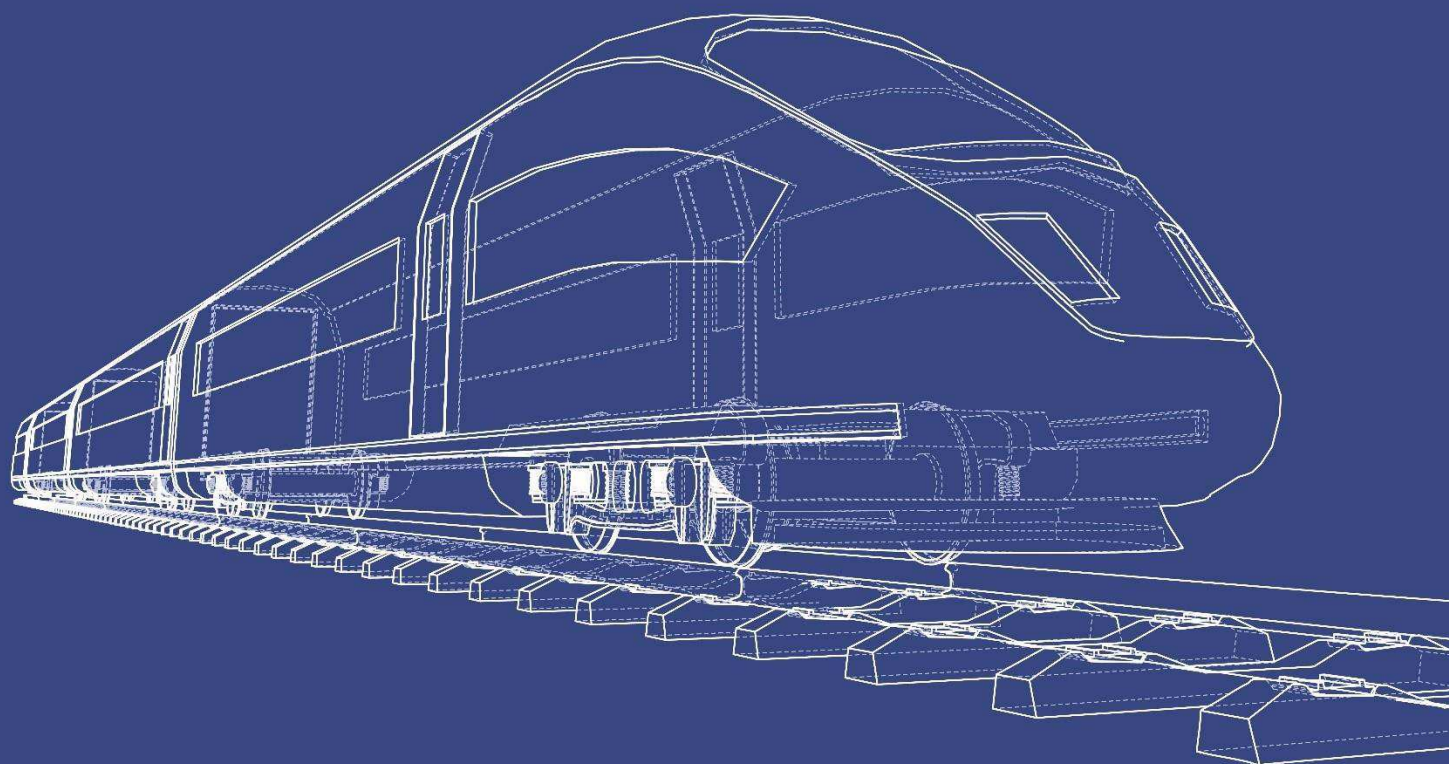


Onboard train protection systems

RiSSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Rolling Stock Standard



This Australian Standard® AS 7511 Onboard train protection systems was prepared by a Rail Industry Safety and Standards Board (RISSB) Development Group consisting of representatives from the following organisations:

Metro Trains Melbourne	Pacific National	TfNSW
Queensland Rail	Aurizon	PTV
RTBU	DPTI	Sydney Trains

The Standard was approved by the Development Group and the Rolling Stock Standing Committee in May, 2020. On June 01, 2020 the RISSB Board approved the Standard for release.

This standard was issued for public consultation and was independently validated before being approved.

Development of the Standard was undertaken in accordance with RISSB's accredited process. As part of the approval process, the Standing Committee verified that proper process was followed in developing the Standard

RISSB wishes to acknowledge the positive contribution of subject matter experts in the development of this Standard. Their efforts ranged from membership of the Development Group through to individuals providing comment on a draft of the Standard during the open review.

I commend this Standard to the Australasian rail industry as it represents industry good practice and has been developed through a rigorous process.



Deb Spring
Exec. Chair / CEO
Rail Industry Safety and Standards Board

Keeping Standards up-to-date

Australian Standards developed by RISSB are living documents that reflect progress in science, technology and systems. To maintain their currency, Australian Standards developed by RISSB are periodically reviewed, and new editions published when required. Between editions, amendments may be issued. Australian Standards developed by RISSB could also be withdrawn.

It is important that readers assure themselves they are using a current Australian Standard developed by RISSB, which should include any amendments that have been issued since the Standard was published. Information about Australian Standards developed by RISSB, including amendments, can be found by visiting www.rissb.com.au.

RISSB welcomes suggestions for improvements and asks readers to notify us immediately of any apparent inaccuracies or ambiguities. Members are encouraged to use the change request feature of the RISSB website at: <http://www.rissb.com.au/products/>. Otherwise, please contact us via email at info@rissb.com.au or write to Rail Industry Safety and Standards Board, PO Box 518 Spring Hill Qld 4004, Australia.

Notice to users

This RISSB product has been developed using input from rail experts from across the rail industry and represents good practice for the industry. The reliance upon or manner of use of this RISSB product is the sole responsibility of the user who is to assess whether it meets their organisation's operational environment and risk profile.

AS 7511:2020

Onboard train protection systems

Document details

First published as: AS 7511:2020

ISBN 978-1-76072-851-9

Document history

Publication Version	Effective Date	Reason for and Extent of Change(s)
2020	June 01, 2020	First publication

Approval

Name	Date
Rail Industry Safety and Standards Board	1/06/2020

Copyright

© RISSB

All rights are reserved. No part of this work can be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of RISSB, unless otherwise permitted under the Copyright Act 1968.

Published by SAI Global Limited under licence from the Rail Industry Safety and Standards Board, PO Box 518 Spring Hill Qld 4004, Australia

This Standard was prepared by the Rail Industry Safety and Standards Board (RISSB) Development Group AS 7511 Onboard train protection systems. Membership of this Development Group consisted of representatives from the organisations listed on the inside cover of this document

Objective

The purpose of this document is to provide requirements, recommendations and guidance for onboard train protection systems and establishes industry standards for these systems. Onboard train protection systems are implemented to reduce the risk of accidents or incidents due to driver error or incapacity.

Compliance

There are two types of control contained within Australian Standards developed by RISSB:

1. Requirements.
2. Recommendations.

Requirements – it is mandatory to follow all requirements to claim full compliance with the Standard. Requirements are identified within the text by the term 'shall'.

Recommendations – do not mention or exclude other possibilities but do offer the one that is preferred. Recommendations are identified within the text by the term 'should'.

Recommendations recognise that there could be limitations to the universal application of the control, i.e. the identified control is not able to be applied or other controls are more appropriate or better.

For compliance purposes, where a recommended control is not applied as written in the standard it could be incumbent on the adopter of the standard to demonstrate their actual method of controlling the risk as part of their WHS or Rail Safety National Law obligations. Similarly, it could also be incumbent on an adopter of the standard to demonstrate their method of controlling the risk to contracting entities, or interfacing organisations where the risk may be shared.

Controls in RISSB standards address known railway hazards are addressed in Appendix E.

This Standard includes a commentary on some of the clauses. The commentary directly follows the relevant clause, is designated by 'C' preceding the clause number and is printed in italics in a box. The commentary is for information and guidance, it does not form part of the requirements and recommendations of this Standard.

Contents

1	Scope and general	5
1.1	Scope	5
1.2	Normative references.....	5
1.3	Terms and definitions.....	6
1.4	Abbreviations	7
2	General	9
2.1	Application of this Standard	9
2.2	Interoperability principles	9
2.3	Document structure.....	10
3	Onboard train protection system (OTPS)	11
3.1	Onboard train protection systems definition	11
3.2	OTPS interfaces	12
4	Selected OTPS.....	14
4.1	Selected OTPS definitions	14
4.2	Interface requirements	15
4.3	Operational requirements.....	15
4.4	Design requirements.....	16
4.5	RAMS requirements.....	18
4.6	Environmental requirements	20
5	Individual OTPS types	22
5.1	General.....	22
5.2	Vigilance system.....	23
5.3	Mechanical train stop and trip gear system (MTSTGS)	27
5.4	Automatic warning system (AWS).....	32
5.5	Train protection and warning system (TPWS)	37
5.6	Station protection system (SPS)	42
5.7	Operator enable system (OES).....	46
5.8	Automatic train protection (ATP)	48

Appendix Contents

Appendix A	Guidance on the application of OTPS (informative).....	50
A.1	General.....	50
A.2	OTPS application guidance.....	51
Appendix B	Examples of OTPSs used (informative)	57
Appendix C	Interoperability component selection guidance (informative)	59
Appendix D	Guidance on vigilance timing cycle (informative).....	60
Appendix E	Hazard register (informative).....	61
Appendix F	Bibliography (informative)	62

1 Scope and general

1.1 Scope

The scope of this Standard is constrained to onboard train protection systems (OTPSs) as fitted to new, modified or existing self-propelled locomotive, passenger and infrastructure rolling stock.

The document covers the application, design, interface, construction and maintenance of onboard train protection systems.

The onboard train protection systems specifically covered in this document are:

- (a) vigilance system;
- (b) mechanical train stop and trip gear system (MTSTGS);
- (c) Automatic Warning System (AWS);
- (d) Train Protection and Warning System (TPWS);
- (e) Station Protection System (SPS);
- (f) operator enable system (OES);
- (g) automatic train protection system (ATP).

The Standard is not specifically intended to cover rolling stock used on light rail, cane railway and monorail networks, but items from this Standard may be applied to such systems as deemed appropriate by the relevant railway infrastructure manager (RIM).

Operation of rolling stock is not covered in this Standard.

The design and operation of wayside elements that interface with the onboard train protection systems is not covered in this Standard.

The design and operation of other rolling stock systems that interface with the onboard train protection systems is not covered in detail in this Standard.

Network operational rules are not covered in detail in this Standard.

The Standard is not specifically intended to cover onboard train protection systems on trains with a grade of automation 2 or above (GoA 2+) as defined in EN62290-1, but items from this Standard may be applied to such systems as deemed appropriate by the relevant RIM.

1.2 Normative references

The following referenced documents are indispensable for the application of this Standard:

- AS 7450 - Rail Systems Interoperability.
- AS 7470 Human Factors integration in engineering design – General requirements.
- AS 7722 – EMC management.
- AS 7527 - Rolling Stock Event Recorders.
- AS 7533 – Driving Cabs.
- AS 7666 - Train Protection and Control Interoperability.
- AS 7770- Rail Cyber Security.

- EN 50126-1 Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process.
- EN 50159 Railway Applications – Communication, Signalling and Processing Systems – Safety-Related Communication in Transmission Systems.
- EN 62290-1 Railway Applications – Urban Guided Transport Management and Command/Control Systems – Part 1: System principles and fundamental concepts.
- IEEE 1474.1 Communication-Based Train Control (CBTC) Performance and Functional Requirements.
- UNISIG ERTMS/ETCS Class 1 - SUBSET 026 – System Requirements Specification.
- ARTC ESD-32-01 Signalling Rolling Stock Interface Procedure.

1.3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

- (a) **conventional signalling**
fixed block signalling. Movement authorities are provided by signals to the driver through the detection of train occupancy in fixed sections of the track (blocks). Each block is only occupied by a single train at any given time.
- (b) **coordinated universal time (UTC)**
UTC is the primary time standard by which the world regulates clocks and time. Previously known as Greenwich Mean Time (GMT).
- (c) **interface control document**
a document defining the different layers of the interface. This document provides full definition of the interface to enable seamless integration.
- (d) **interoperability**
a term used to describe the possibility of uninterrupted movement of trains across differing countries, states or rail networks across international borders, state borders or rail networks managed by various RIMs.
- (e) **onboard train protection system (OTPS)**
a safety system installed on rolling stock that reduces the likelihood of and protects against the consequences of a failure in the manual onboard functions for safe train operation.

OTPSs detailed in section 5 of this Standard monitor the driver (or train) condition or performance and apply the train brakes, and disable traction power when a measured condition or performance parameter violates a required state of limit.
- (f) **penalty brake**
a brake application initiated by the OTPS with a defined brake performance (for example deceleration rate or braking distance from a certain speed). It is common for rolling stock to use:
 - i. the emergency brake (venting air to atmosphere) as their form of penalty brake application.
 - ii. a full service brake application as their form of penalty brake application.

- (g) ***rail operations context***
the operations concept and environment that the Rolling Stock operates under. Rail operations context includes, as a minimum consideration of the following parameters:
 - i. Passenger and freight rolling stock mixing.
 - ii. Traffic density.
 - iii. Train speed.
 - iv. Infrastructure including level crossings.
 - v. Type of train control technology (conventional signalling or communications-based train control operation).
 - vi. Driver only operations.
 - vii. Clause 4.3.1 provides more detail on rail operations context.
- (h) ***selected OTPS***
the combination of one or more OTPSs which work together as an overall system for that train which is determined by the rail operations context.

General rail industry terms and definitions are maintained in the RISSB Glossary:

<https://www.rissb.com.au/products/glossary/>

1.4 Abbreviations

- (a) ***ATMS***
advanced train management system.
- (b) ***ATP***
automatic train protection system.
- (c) ***AWS***
automatic warning system.
- (d) ***CBTC***
communication-based train control.
- (e) ***CTCS***
Chinese train control system.
- (f) ***DIRN***
defined interstate rail network.
- (g) ***EMC***
electromagnetic compatibility.
- (h) ***ERTMS***
European railway traffic management system.
- (i) ***ETCS***
European train control system.
- (j) ***HVAC***
heating, ventilation and air conditioning.
- (k) ***LRU***
line replaceable unit.
- (l) ***MTSTGS***
mechanical train stop and trip gear system.

- (m) **OES**
operator enable system.
- (n) **OSS**
overspeed sensor.
- (o) **OTPS**
onboard train protection system.
- (p) **RAMS**
reliability, availability, maintainability and safety.
- (q) **RIM**
rail infrastructure manager.
- (r) **RTC**
rail traffic crew.
- (s) **RTO**
rail transport operator.
- (t) **SFAIRP**
so far as is reasonably practicable.
- (u) **SMS**
safety management system.
- (v) **SVR**
single voluntary reset.
- (w) **TPWS**
train protection and warning system.
- (x) **TSS**
train stop sensor.

2 General

2.1 Application of this Standard

2.1.1 New and repurposed rolling stock

For new rolling stock, existing rolling stock being proposed for operation on a network on which the class of rolling stock has not previously operated or rolling stock that has been deemed to require certification as determined by AS 7501, this Standard shall be included in the schedule of Standards in accordance with AS 7501 Section 2.

2.1.2 Rolling stock upgrades and modifications

This Standard shall be applied to the addition or removal of any individual OTPS to existing rolling stock.

This Standard shall be applied when upgrades or modifications are made to OTPSs.

All upgrades and modifications to OTPS(s) shall be accompanied by a safety SFAIRP argument.

Where a Standards compliance register exists as per the requirements of AS 7501, upgrades and modifications shall trigger an update of the Standards compliance register to reflect the changes.

2.1.3 Use of alternative standards

Standards outside of the RISSB rolling stock series of Australian Standards (e.g. international standards) may be used where specifically called up by RISSB rolling stock standards as is the case for Clause 5.8 of this Standard or where a RISSB rolling stock standard has not been issued.

Where alternative standard(s) are used, relevant certification documentation shall be issued according to the alternative standard(s) and be accompanied by:

- (a) a safety SFAIRP argument which provides a list of and justification for all alternative standards to be used;
- (b) a statement that clearly details:
 - i. any deviations made from the alternative standard(s) that:
 - (A) are required to adapt system(s) to the rail operations context; or
 - (B) have been made for any other reason; and
 - ii. why the standard is equivalent and its applicability.

Where a Standards compliance register exists for the rolling stock, it shall be updated in accordance with AS 7501 to record details of any statement made as per clause 2.1.3 (b) of this Standard.

2.2 Interoperability principles

The selection of OTPS is largely influenced by the need for interoperability. Interoperability planning should support the safety and business needs of RIMs and RTOs as detailed in AS 7450 and AS 7666.

2.3 Document structure

The document is presented as follows:

- (a) Sections 1 & 2: Provides the outline for the standard.
- (b) Section 3: Provides a definition of OTPSs, including system functionality, system context, system components and interfaces.
- (c) Section 4: Provides the requirements for OTPSs. This section includes functional and non-functional requirements applicable to all OTPSs.
- (d) Section 5: Provides detailed requirements for each type of OTPS.
- (e) Appendix A: Provides guidance on the application of different levels of OTPSs. This section provides rationale for application of each type of OTPS based on the risks attributed to the Rail operations context.
- (f) Appendix B: Provides examples of OTPS fitted to locomotives and passenger rolling stock throughout Australia.
- (g) Appendix C: Provides interoperability component selection guidance.
- (h) Appendix D: Guidance on vigilance timing cycle.
- (i) Appendix E: Hazard register.
- (j) Appendix F: Bibliography.

3 Onboard train protection system (OTPS)

3.1 Onboard train protection systems definition

An onboard train protection system (OTPS) is a safety system installed on rolling stock that reduces the likelihood of and protects against the consequences of a failure in the manual onboard functions for safe train operation.

OTPSs protect the train through the automatic activation of other rolling stock systems to render the train to a safe condition in the event of a failure in the manual onboard functions for safe train operation.

The selected OTPS is usually made up of a number of OTPSs. The composition differs across rail networks due to differences in the rail operations context (for example type of rolling stock, route and traffic mix), which determines its risk profile. Refer to Section 4 for further details.

Usually a minimum of two independent engineering defences (OTPSs) are used to minimise the risk of derailment or collision in the event of RTC incapacitation (Recommendation 31 - Special Commission of Inquiry into the Waterfall Rail Accident Final Report).

Figure 3.1 shows the relationship between manual onboard functions for safe train operation and how the selected OTPS manage the risks associated with the failure of these manual functions.

For the purpose of this Standard, manual onboard functions and automatic onboard functions are defined as per EN 62290-1.

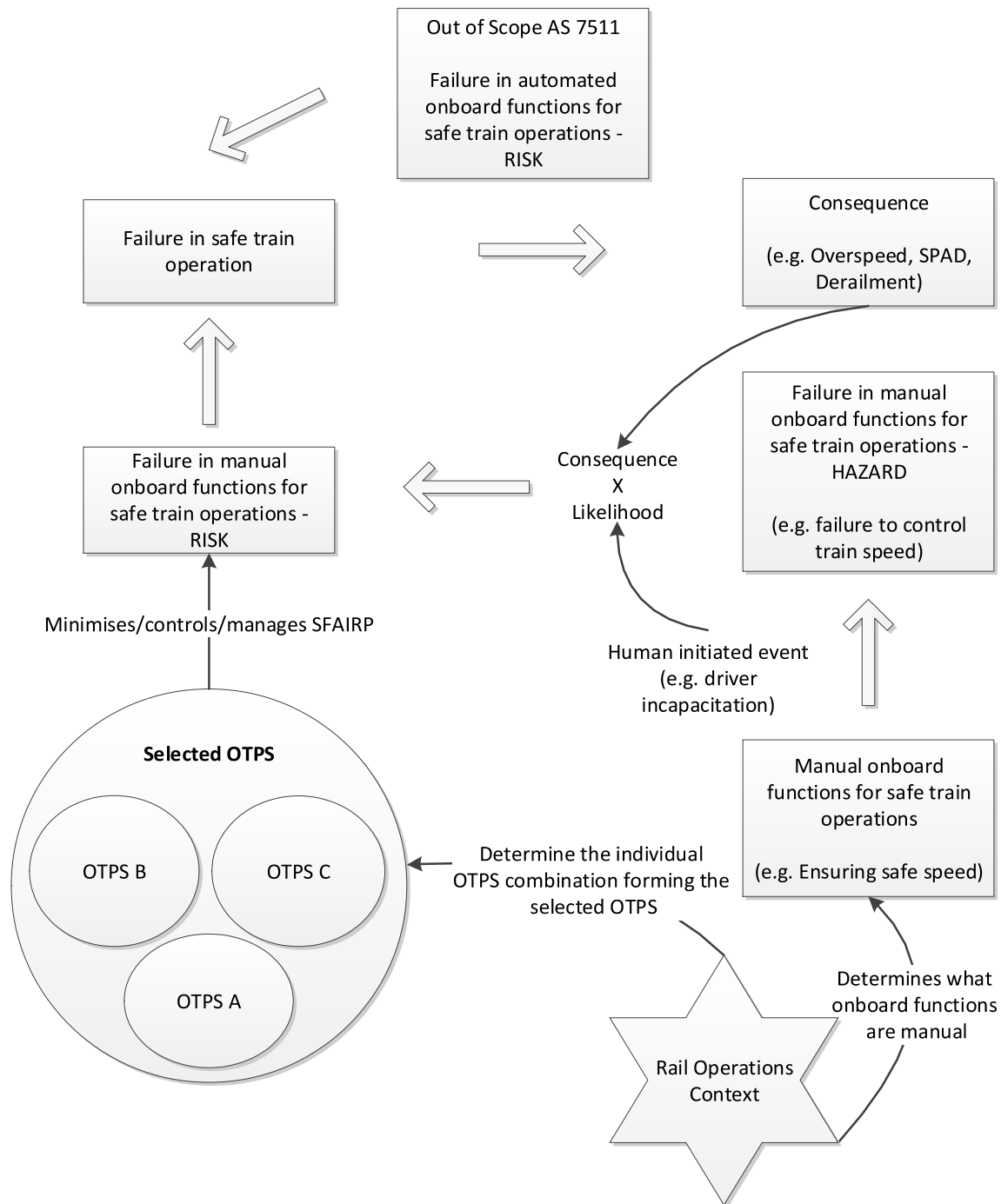


Figure 3:1 Relationship between onboard functions and OTPSs

3.2 OTPS interfaces

3.2.1 General

There are 4 categories of interfaces to an OTPS. Whether or not an individual OTPS has an interface with the other systems listed below is dependent on the rail operations context.

A full definition for all the interfaces associated with each OTPS is provided in section 5.

3.2.2 Rolling stock systems interfaces

Examples of rolling stock systems interfaces include:

- (a) traction and braking system;
- (b) doors system;
- (c) fire & emergency system;
- (d) HVAC system;
- (e) train control and monitoring system;
- (f) coupling system;
- (g) train / passenger communication system.

3.2.3 Other OTPS interfaces

Examples of other OTPS interfaces include:

- (a) vigilance system with OES;
- (b) vigilance system with ATP system;
- (c) ATP system with AWS system;
- (d) ATP system with OES.

3.2.4 Trackside systems interfaces

Examples of trackside systems interfaces include:

- (a) trip gear (onboard) with train stop (trackside);
- (b) trip gear (onboard) with magnets (trackside);
- (c) AWS (onboard) with magnets (trackside);
- (d) TPWS (onboard) with transmitters (trackside);
- (e) ATP systems (onboard) with balises (trackside);
- (f) ATP systems (onboard) with other radio infrastructure (trackside).

3.2.5 Human interfaces

Human interfaces, often referred to as human machine interface (HMI) or driver machine interface (DMI) provide functionality including:

- (a) indicate status of individual OTPSs;
- (b) where required alerts human to intervene to maintain safe train operation;
- (c) allow isolation for degraded operations / recovery;
- (d) control the OTPS (e.g. vigilance pushbutton and operator enable device).

Figure 3.2 shows the relationships between manual onboard functions for safe train operations, the associated risks, how selected OTPS can manage these risks SFAIRP and the interfaces for the OTPSs.

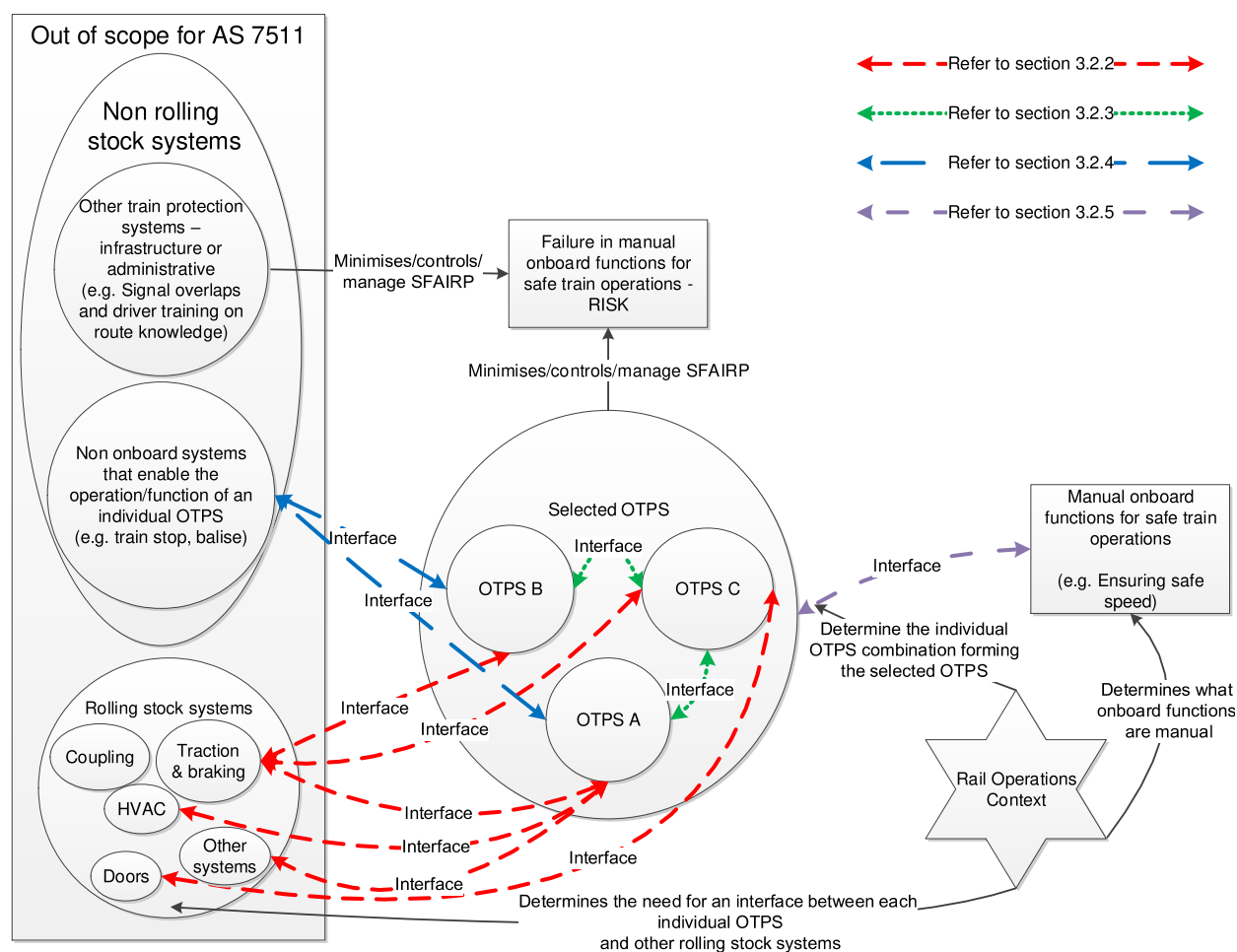


Figure 3:2 OTPSs interfaces and relationships to manage safety SFAIRP

4 Selected OTPS

4.1 Selected OTPS definitions

This section defines the requirements applicable to the selected OTPS, and each individual OTPS.

The high-level requirements are presented within the subsections of clauses 4.2 through 4.6 inclusive. For each subsection, the requirements are presented as follows:

- (a) **Clause number**
A unique clause number for the requirement. Note that the clause number is associated with the section.
- (b) **Clause text**
Specifies the high-level requirement in terms of 'shall' or 'should'
- (c) **Commentary**
Describes the intent and purpose of the requirement. The commentary also includes any supporting information to provide context for the requirement.

Appendix A provides additional guidance on the application of OTPSs.

4.2 Interface requirements

4.2.1 Each OTPS shall interface with the driver to:

- (a) provide critical information generated by the OTPS; and
- (b) process authorised controls/commands.

C4.2.1 Commentary

The intent of this requirement is to define the interface with the driver in the cab. The interface to the driver includes:

- (a) status information, alarm information; and
- (b) driver acknowledgement, equipment isolation.

AS 7533 provides requirements for alarms and controls in driving cabs.

4.2.2 All OTPS interfaces shall be defined in an interface control document.

C4.2.2 Commentary

The intent of this requirement is to capture the specifics of the interfaces, so that the interface is an adopted standardized definition, and any changes are managed through the interface.

4.3 Operational requirements

4.3.1 The selected OTPS shall be fitted to rolling stock to reduce the risk SFAIRP associated with failure in the manual functions of train operations, dependent on the rail operations context.

C4.3.1 Commentary

The rail operations context will define the level of risk for hazards associated with the failure in the manual functions of train operation. For example, a rural environment with minimal trains would have a significantly different risk profile to an urban system. The safe SFAIRP argument and strategic approach to the makeup of the selected OTPS, should consider as a minimum:

- (a) type of operation, such as suburban, intercity, regional, interstate;
- (b) fleet size of the proposed train;
- (c) operational parameters, such as route, speed, frequency, travel distance, trip time, operating hours, closed or mixed traffic;
- (d) current and proposed infrastructure centred and administrative centred risk controls;
- (e) operation staff (e.g. shift durations, number of crew, cross or mixed fleet operations);
- (f) rolling stock type;
- (g) operational modes, including normal and degraded/emergency mode of operation.

4.3.2 Where rolling stock is required to operate across multiple RIM territories, the selected OTPS shall be interoperable.

C4.3.2 Commentary

The intent of this requirement is to ensure interoperability, that is, where trains are fitted with a particular OTPS, e.g. ETCS, that this system will have the same operational interface between RIMs and function correctly on all infrastructure fitted with associated wayside elements of ETCS on all RIMs.

Note that 4.3.1 is applicable for all RIMs that the rolling stock is required to operate across. This could mean that there are multiple OTPSs on the rolling stock, some of which operate only under one RIM, some which operate only on another RIM, and some which operate across both RIMs. The human interface with respect to interoperability and safety will need careful consideration where:

- (a) different OTPS are required over multiple RIMs (hence some are de-activated);
- (b) operation of a particular OTPS is different across RIMs.

4.3.3 Where multiple OTPSs are applied, they shall not degrade the integrity and functionality of other OTPS.

4.3.4 Each OTPS shall validate its own inputs where practicable.

C4.3.4 Commentary

The intent of this requirement is to ensure that each onboard train control system acts on a valid set of inputs, therefore protecting the train when necessary. These inputs will vary on the type of OTPS, examples include:

- (a) mechanical input (e.g. force or pressure of a switch or pedal);*
- (b) electrical input, e.g. the signal is only valid between a defined range of voltages;*
- (c) data e.g. manually entered data such as driver codes from a valid list or between a specified range.*

4.3.5 Each OTPS shall only be operable in the active cab.

C4.3.5 Commentary

The intent of this requirement is to ensure that the OTPS which would be installed in all cabs only become operable, when the cab is active. This ensures that in the cab where the driver is operating the train includes the protection from the OTPSs.

4.3.6 Where required by operations, each OTPS shall have its own isolation function.

C4.3.6 Commentary

The intent of this requirement is to ensure that in the case of OTPS failure, the driver is provided a facility to isolate where deemed necessary given the operational context. Examples include isolating for recovery purposes in the event of a failure.

4.3.7 The isolation status of each OTPS shall be indicated to the driver.

C4.3.7 Commentary

The intent of this requirement is to ensure that the current driver and future drivers (after crew change) are aware that the OTPS is isolated, so that they can take the appropriate actions where necessary.

4.4 Design requirements

4.4.1 Each OTPS should be based on proven technologies, designs and assets configured for the localised application.

C4.4.1 Commentary

Increased service reliability and introduction of new technology are reliant on confidence in the capability of the system and products and thus brand new never used elements are not consistent with achieving those outcomes. New technologies can be proven in trial sites, test tracks etc.

4.4.2 Each OTPS shall where practicable be capable of interfacing to open industry standards that are non-proprietary and established.

C4.4.2 Commentary

The intent of the requirement is to ensure that each OTPS solution is capable of interfacing to open industry standards, which provides a path for future integration and interfacing with new/updated products and technology using the open industry Standards.

4.4.3 Each OTPS shall where practicable:

- (a) use common architectures and components;
- (b) use modular designs;
- (c) minimise the number of variants of line replaceable units (LRU) and thus spares;
- (d) minimise the impact where an LRU becomes obsolete; and
- (e) minimise the need for special tools.

C4.4.3 *Commentary*

Introduction of any new system or product aims to reduce, not increase, cost of ownership and whole of life costs. This is a strategic requirement to support that aim. All of the identified list aim to simplify and standardise maintenance across equipment.

4.4.4 All OTPS parameters shall be recorded in compliance with AS 7527.

C4.4.4 *Commentary*

AS 7527 covers the specification of an onboard driving data recording system for the purpose of recording data about the operation of the train. The data refers both to the driver behaviour and the onboard systems behaviour to support systematic safety monitoring as a means of preventing incidents and accidents.

4.4.5 The equipment of each OTPS shall not infringe upon the kinematic envelope specified for the application environment.

C4.4.5 *Commentary*

Generic requirement for any system which has equipment fitted to rolling stock. Note that the kinematic envelope is the outline of the space occupied by a rail vehicle when in motion, including the effects of tilt, sway, track cant, etc.

4.4.6 Each OTPS shall ensure that the communication system for safety related data is designed in accordance with EN 50159.

C4.4.6 *Commentary*

The intent of this requirement is to ensure that the safety related communications is safe, which can be achieved by designing in accordance with EN 50159. The details of the category need to be determined, taking into consideration the overall approach to security and the associated risks.

4.4.7 The selected OTPS(s) shall be designed for an expected design life as agreed by the RTO(s).

C4.4.7 *Commentary*

The intent of this requirement is to ensure that each OTPS is designed so that they won't need replacing for a significant period of time, typically this is 35 years. Replacing systems is a costly business both in monetary, time and network performance measures, therefore providing systems with a substantial design life provides a better whole of life outcome.

4.5 RAMS requirements

4.5.1 Each OTPS shall comply with the RTO's safety management system.

C4.5.1 *Commentary*
Each RTO that operates a network is accredited by the Office of the National Rail Safety Regulator. As part of the accreditation, the RTO(s) must have a safety management system which defines processes and procedures to be applied to all modified and new operations on the network. This applies to the overall system, and its constituent parts. Evidence of compliance is acceptance by the RTO of project design against their SMS.

4.5.2 The selected OTPS design shall mitigate hazards SFAIRP.

C4.5.2 *Commentary*
The design of the overall system, including the constituent parts, must consider hazards from all aspects of engineering. These hazards must be identified and managed to ensure the best low risk outcome.
Speciality engineering encompasses:
(a) *reliability, availability and maintainability;*
(b) *human factors integration;*
(c) *security engineering;*
(d) *electromagnetic interference / electromagnetic compatibility;*
(e) *system resilience;*
(f) *manufacturing and producibility;*
(g) *environmental engineering.*
Hazard mitigation describes the actions taken to reduce the risk associated with the hazard or eliminate the hazard.

4.5.3 On start-up, each OTPS shall be tested to determine whether the equipment and functions are capable of operating safely and are fit for service.

C4.5.3 *Commentary*
Tests on start-up, ensure that the integrity of the system and its equipment is healthy and can function safely prior to being put into functional operation on the rail network.

4.5.4 Where the overall OTPS(s) is capable of self-test it shall not allow a train to move when any OTPS start up self-test has failed.

C4.5.4 *Commentary*
Self-tests on start-up, ensure that all pieces of electronic equipment are healthy and can function safely prior to being put into functional operation on the rail network. Therefore, if a test fails, it is important to resolve the issue prior to allowing the train into service.

4.5.5 During operation, where the OTPS is capable of self-test, the system shall monitor its own operation and ensure the train is placed in a safe state where the system is unable to perform its function.

C4.5.5 *Commentary*
Self-tests during operation, ensure that electronic equipment remains healthy and safe for operation, as it continues to operate on the rail network.

4.5.6 The data of each OTPS shall be protected against unauthorised physical access.

C4.5.6 Commentary

The intent of this requirement is to provide an overarching security need. This is specifically aimed at physical access.

4.5.7 Each OTPS shall be resilient against both unauthorised electronic access and unauthorised radio frequency access in accordance with AS 7770.

C4.5.7 Commentary

Each OTPS must ensure that they are resilient against these types of access in order to provide a safe and reliable system.

4.5.8 The specification and demonstration of human factors integration for each OTPS shall be in accordance with AS 7470.

C4.5.8 Commentary

The intent of this requirement is to ensure there is a consistent and recognised standard approach to ensuring humans are considered in the design of each OTPS.

4.5.9 The specification and demonstration of RAMS engineering for each OTPS shall be in accordance with EN50126.

C4.5.9 Commentary

The intent of this requirement is to ensure there is a consistent and recognised standard approach to ensuring RAMS is considered in the design of each OTPS.

4.5.10 Each OTPS shall minimise the risk of a single point of failure SFAIRP and demonstrate this through systems analyses.

C4.5.10 Commentary

RAMS requirements for the specific application, and the associated process governing RAMS do not preclude single points of failure. Whilst it is possible to demonstrate achievement of targets with single points of failure the resultant solution is more vulnerable. This is a strategic requirement to set the emphasis towards removal of single points of failure and thus tends towards a higher level of resilience.

4.5.11 The human interaction in each OTPS shall be designed to discourage circumvention.

C4.5.11 Commentary

The intent of this requirement is to ensure that the "easy way is the correct way". That is, the user will perceive required tasks to be easy to perform, preventing them from seeking to circumvent the system where tasks are perceived as being difficult. For example, high forces will be perceived as difficult, which may encourage circumvention.

4.5.12 Each OTPS should record system events and system interactions over external interfaces with a consistent time and date stamp synchronised to UTC in accordance with AS 7527.

C4.5.12 Commentary

The intent of this requirement is to ensure all logging or recording is able to be analysed with respect to a common time source; all systems and products, not just OTPSs, are specified with this requirement.