AS 7511:2019

Onboard Train Protection Systems

Rolling Stock Standard

Please note this is a RISSB Australian Standard® draft

Document content exists for RISSB product development purposes only and should not be relied upon or considered as final published content.

Any questions in relation to this document or RISSB's accredited development process should be referred to RISSB.

RISSB Office

Phone:
(07) 3724 0000
Overseas: +61 7 3724 0000

Email:
info@rissb.com.au

Web:
www.rissb.com.au

AS 7511 **Assigned Standard Development Manager**

Name:
Ian Routcliffe

Phone:
0429 432 095

Email:
iroutcliffe@rissb.com.au

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

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	ASA
PTV	RTBU	DPTI

The Standard was approved by the Development Group and the Enter Standing Committee Standing Committee in Select SC approval date. On Select Board approval date 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 Australian Standards developed by RISSB could also be withdrawn.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 7511:2019

Onboard Train Protection Systems

Document details

First published as: AS 7501:2019

ISBN Enter ISBN.

Document history

Publication Version	Effective Date	Reason for and Extent of Change(s)
2019	Select Board approval date	

Draft history (Draft history applies only during development)

Draft version	Draft date	Notes
PC Draft	12/12/2019	Draft for Public Comment

Approval

Name	Date
Rail Industry Safety and Standards Board	Select Board approval date

Copyright

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 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 D.

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 and does not form part of the Standard.

Contents

Appendix Contents

1 Scope and general

1.1 Scope

The scope of this standard is constrained to onboard train protection systems as fitted to new, self-propelled, modified and existing 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).

Rolling stock used on light rail, cane railway and monorail networks are not covered in this Standard.

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.

Onboard train protection systems on fully automated trains are not covered in this standard.

1.2 Normative references

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

- AS 7666 - Train Protection and Control Interoperability.
- AS 7450 - Rail Systems Interoperability.
- AS 7527 - Rolling Stock Event Recorders.
- AS 7770- Rail Cyber Security.
- EN 62290-1 Railway Applications – Urban Guided Transport Management and Command/Control Systems – Part 1: System principles and fundamental concepts.
- EN 50159 Railway Applications – Communication, Signalling and Processing Systems – Safety-Related Communication in Transmission Systems.
- IEEE 1474.1 Communication-Based Train Control (CBTC) Performance and Functional Requirements.
- AS 7722 – EMC management.

- AS 7470 Human Factors integration in engineering design – General requirements.
- EN 50126-1 Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process.
- UNISIG ERTMS/ETCS Class 1 - SUBSET 026 – System Requirements Specification.
- ARTC 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 (ICD)***
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 use 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)***
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 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 the emergency brake (venting air to atmosphere) 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); and

vi. driver only operations.
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.

(i) ***vigilance system***
A system that will react by directly initiating a penalty brake application if an acknowledgement input is not received within a specified time increment.

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) ***ERTMS***
European railway traffic management system.

(h) ***ETCS***
European train control system.

(i) ***GEMS***
greenhouse and energy minimum Standards.

(j) ***HVAC***
heating, ventilation and air conditioning.

(k) ***LRU***
line replaceable unit.

(l) ***MEPS***
minimum energy performance Standards.

(m) ***MTSTGS***
mechanical train stop and trip gear system.

(n) ***OES***
operator enable system.

(o) ***RAMS***
reliability, availability, maintainability and safety.

(p) ***RIM***
rail infrastructure manager.

(q) ***RTC***
rail traffic crew.

(r) ***RTO***
rail transport operator.

(s) ***SFAIRP***
so far as is reasonably practicable.

(t) ***SMS***
safety management system.

(u) ***TPWS***
train protection and warning system.

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 Rolling stock compliance certification, this Standard shall be included in the schedule of Standards in accordance with AS 7501 Rolling stock compliance certification 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 Clauses 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 Rolling stock compliance certification 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 Rail systems interoperability and AS 7666 Train Protection and Control Interoperability.

2.3 Document structure

The document is presented as follows:

(a) Sections 1 & 2: Provide 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 high-level 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 risk of hazards 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: Hazard register.

(i) Appendix E: 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.

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 Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts.

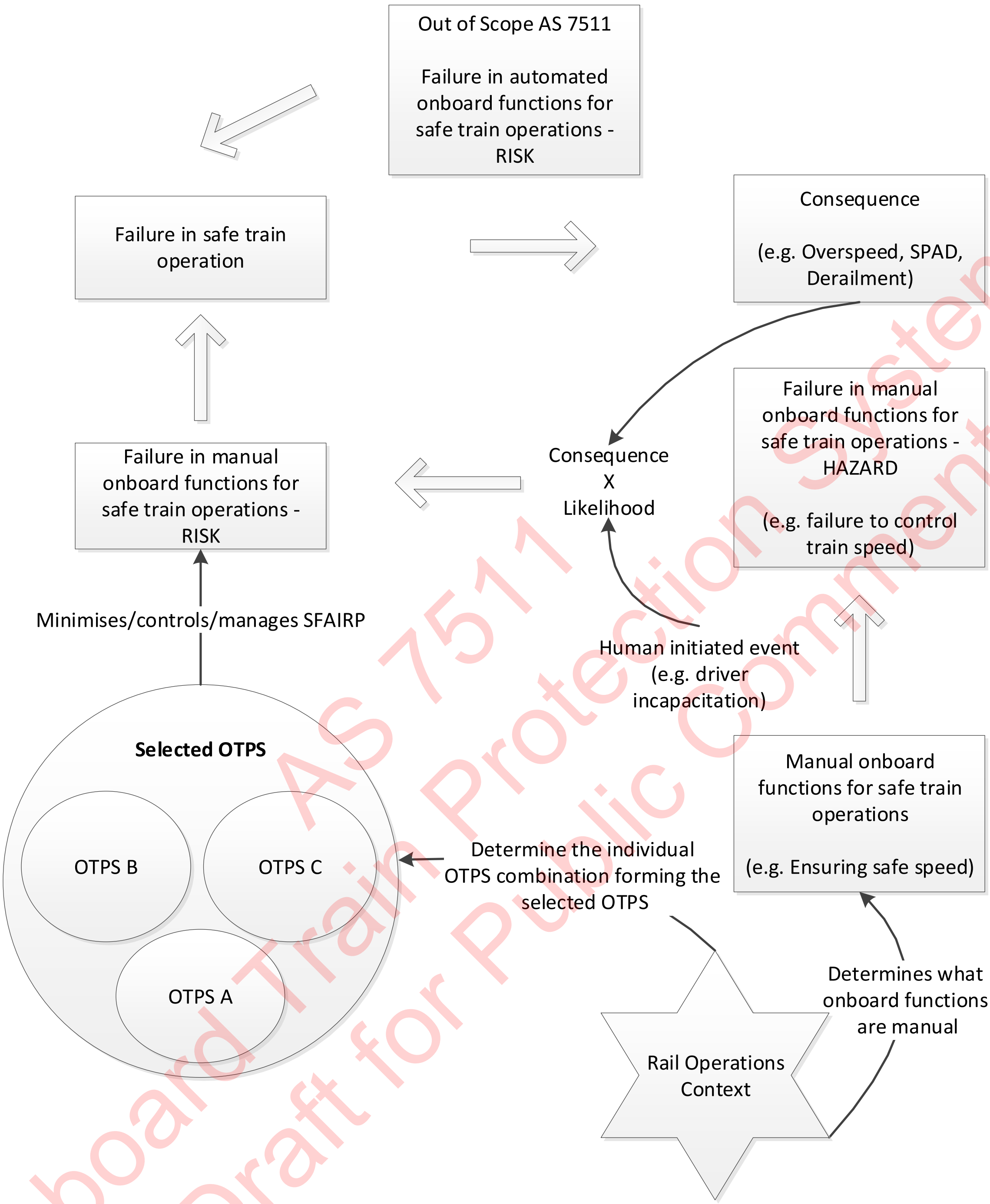

Figure 3:1 Relationship between onboard functions and OTPSs

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 OPTS interfaces

Examples of other OPTS 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.

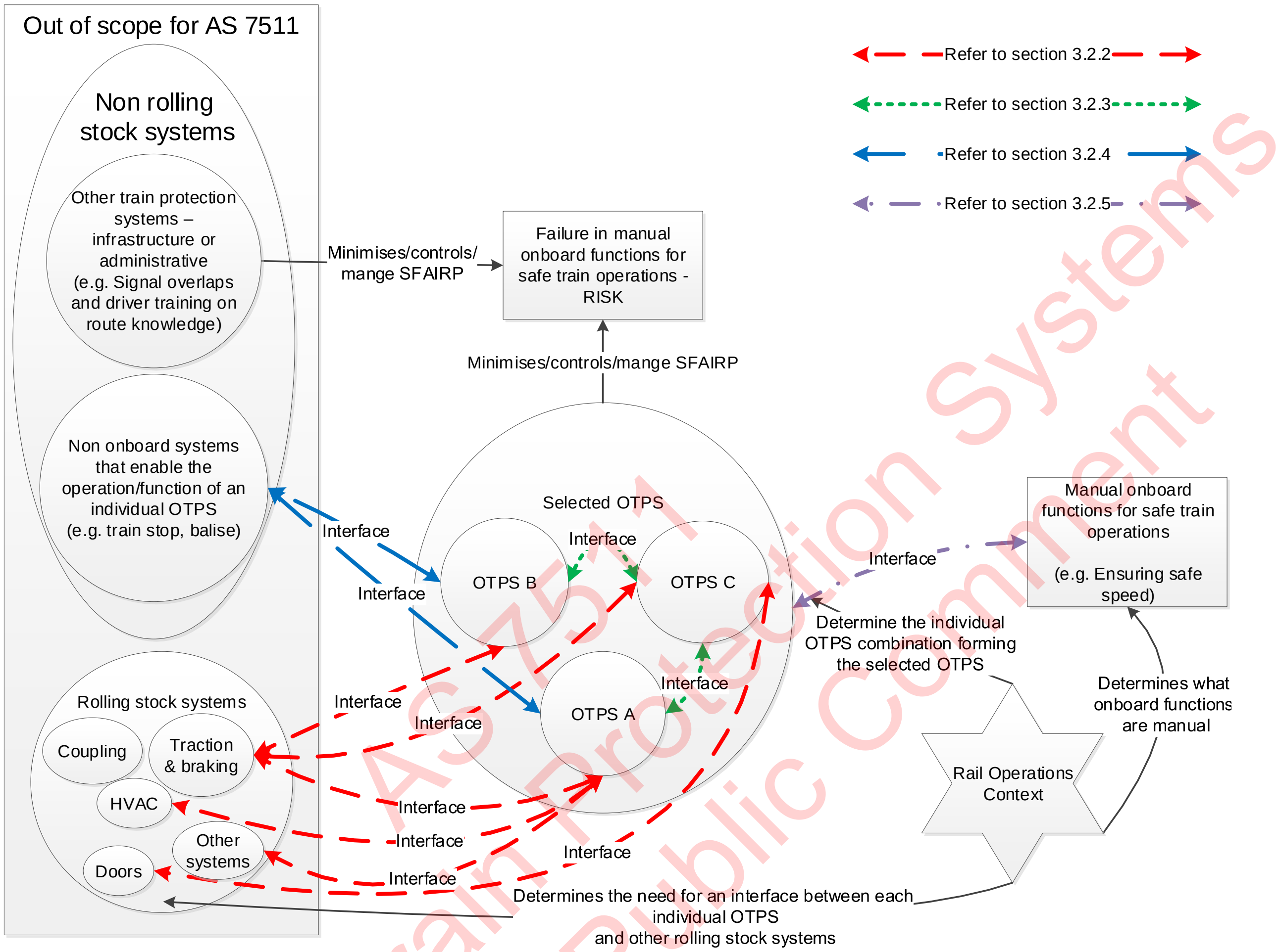

Figure 3.2 OPTSs interfaces and relationships to manage safety SFAIRP

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:

- provide critical information generated by the OTPS; and
- 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.

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 Standard, and any changes are managed through the Standard interface.

4.3 Operational requirements

4.3.1 The selected OTPS shall be fitted to rolling stock to reduce the risk of hazards 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 the ETCS on all RIMs.*
>
> *Note that the selected OTPS shall be safe SFAIRP 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 operator 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 Requirements for design principles and constraints

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 should 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 Rolling stock event recorders.

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. All data recording shall be in line with this standard.

4.4.5 The equipment of each OTPS shall not adversely 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 Railway applications – communication, signalling and processing systems – safety-related communication in transmission systems.

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 rail transport operator'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.*	

4.5.2 The selected OTPSs 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 it shall continuously execute self-tests to ensure the equipment and functions are capable of operating safely.

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 Rail cyber security.

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 Human factors integration in engineering design – General requirements.

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 coordinated universal time (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.

4.5.13 The equipment of each OTPS shall not adversely impact any pre-existing normal maintenance activity.

> *C4.5.13 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.*
>
> *For example, vehicle washing may be impacted if OTPS components require special disconnection / removal prior to the washing activities.*

4.5.14 Each OPTS shall be designed with minimal maintenance and part replacement.

> *C4.5.14 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.*

4.5.15 The software and configuration updates of each OTPS shall not degrade the safety integrity of the system.

> *C4.5.15 Commentary*
> *Updates to software and configuration needs to consider operation safe operation impact not only to the areas/locations/trains directly affected by the update, but also those indirectly impacted.*

4.5.16 Each OTPS software and configuration update shall only impact operations where agreed to by the RTO(s).

> *C4.5.16 Commentary*
> *Updates to software and configuration need to consider operation not only to the areas/locations/trains directly affected by the update, but also those indirectly impacted.*

4.5.17 Each OTPS shall be supplied with the artefacts that will ensure that the OTPS meets the expected design life requirements.

> *C4.5.17 Commentary*
> *The intent of this requirement is to ensure that the asset owner and operator has all the relevant information to support the asset during operation, including maintenance, supplier details, product update information, obsolescence, etc.*

4.6 Environmental requirements

4.6.1 Each OTPS shall comply with IEC 62236-3 or equivalent EN 50121-3.

> *C4.6.1 Commentary*
> *The intent of this requirement is to ensure there is a consistent and recognised standard approach to ensuring EMC management is considered in the design of the OTPS.*

4.6.2 Each OTPS shall comply with AS 7722.

> *C4.6.2 Commentary*
> *The intent of this requirement is to ensure there is a consistent and recognised standard approach to ensuring EMC management is considered in the design of the each OTPS.*

4.6.3 Each OTPS shall operate reliably as per the predefined performance targets within the electro-magnetic environment of the rail network.

> *C4.6.3 Commentary*
> *The intent of this requirement is to ensure that each OTPS not only complies with EMC standards, but operates reliably within the application environment. The application environment may include legacy equipment which may operate outside the standards.*

4.6.4 Each OTPS shall operate reliably as per the reliability targets specified by the RTO within the environment of the rail network.

C4.6.4 Commentary *The intent of this requirement is to ensure that each OTPS considers the environment in which they are to be operated in, operate in the application environment, taking particular note of heat extremes, and sun loads for example, and not simply compliance to, for example euro-norms.*

4.6.5 Each OTPS generated electro-magnetic interference shall not degrade the operational performance of existing assets.

C4.6.5 Commentary *The intent of this requirement is to ensure that each OTPS considers the generated EMI impact on existing and legacy equipment, and therefore that those systems may be more susceptible than, for example, euro-norms.*

4.6.6 Each OTPS equipment shall meet the minimum energy performance standards (MEPS) of the Australian greenhouse and energy minimum standards (GEMS) regulator, where it is rated by MEPS.

C4.6.6 Commentary *The intent of this requirement is to ensure there is a consistent and recognised standard approach to energy performance in the design of each OTPS.*

5 Individual OTPS types

5.1 General

There are many different types of OTPS (currently in use or being trialled) on different rolling stock in Australia. Each OTPS has different levels of effectiveness and limitation against failures in different manual onboard functions.

Table 5:1 provides the layout for sections 5.2 to 5.7, where these sections provide a detailed description, context diagrams and the high-level requirements of each OTPS. As OTPS are configured for a specific rail operations context there are a number of known variants of these OTPS.

Table 5.1 – Layout of sections 5.2 to 5.7

Section heading	Description
Description	This section defines the OTPS and describes the purpose of the system.
Context diagram	This section includes a context diagram for the OTPS, providing reference back to the interfaces described in section 5. For each interface, the context diagram provides the data flow direction, and a description of the interface data.
Requirements	1. This section includes the high-level requirements for the OTPS, comprising of interface requirements, operational requirements and design requirements. The layout for the requirements in these sections is as follows: 2. ***Clause number*** A unique clause number for the requirement. Note that the clause number is associated with the section. 3. ***Clause text*** Specifies the high-level requirement in terms of 'shall' or 'should' 4. ***Commentary*** A Commentary box is provided below each clause which describes the intent and purpose of the requirement.

Section 5.8 covers proprietary ATP systems and provides reference to applicable known Standards and RIM requirements.

When selecting an OTPS, consideration should be given to anticipate and minimise SFAIRP interoperability issues. These considerations include:

(a) being based on open Standards and interfaces where practical;

(b) aiming to support a multi-vendor competitive market;

(c) being chosen to provide technical harmonisation;

(d) avoidance where possible of modifications to proprietary OTPS;

Where modifications to proprietary OTPS are required due to the rail operations context, selections should be made were practicable to adopt solutions that enhance interoperability. Interoperability component selection guidance is provided in Appendix C, which provides examples of known interoperability issues for OTPS and their implemented (or proposed) solution.

5.2 Vigilance system

5.2.1 Vigilance description

A task based vigilance system monitors the rail traffic crew activity by intermittently checking the status of task linked operated controls for example:

(a) acknowledgement of the vigilance alert button (by pressing a button);

(b) movement of power / brake controller;

(c) sounding the horn;

(d) adjusting the headlights; or

(e) operating the windscreen wipers.

5.2.2 Vigilance context diagram

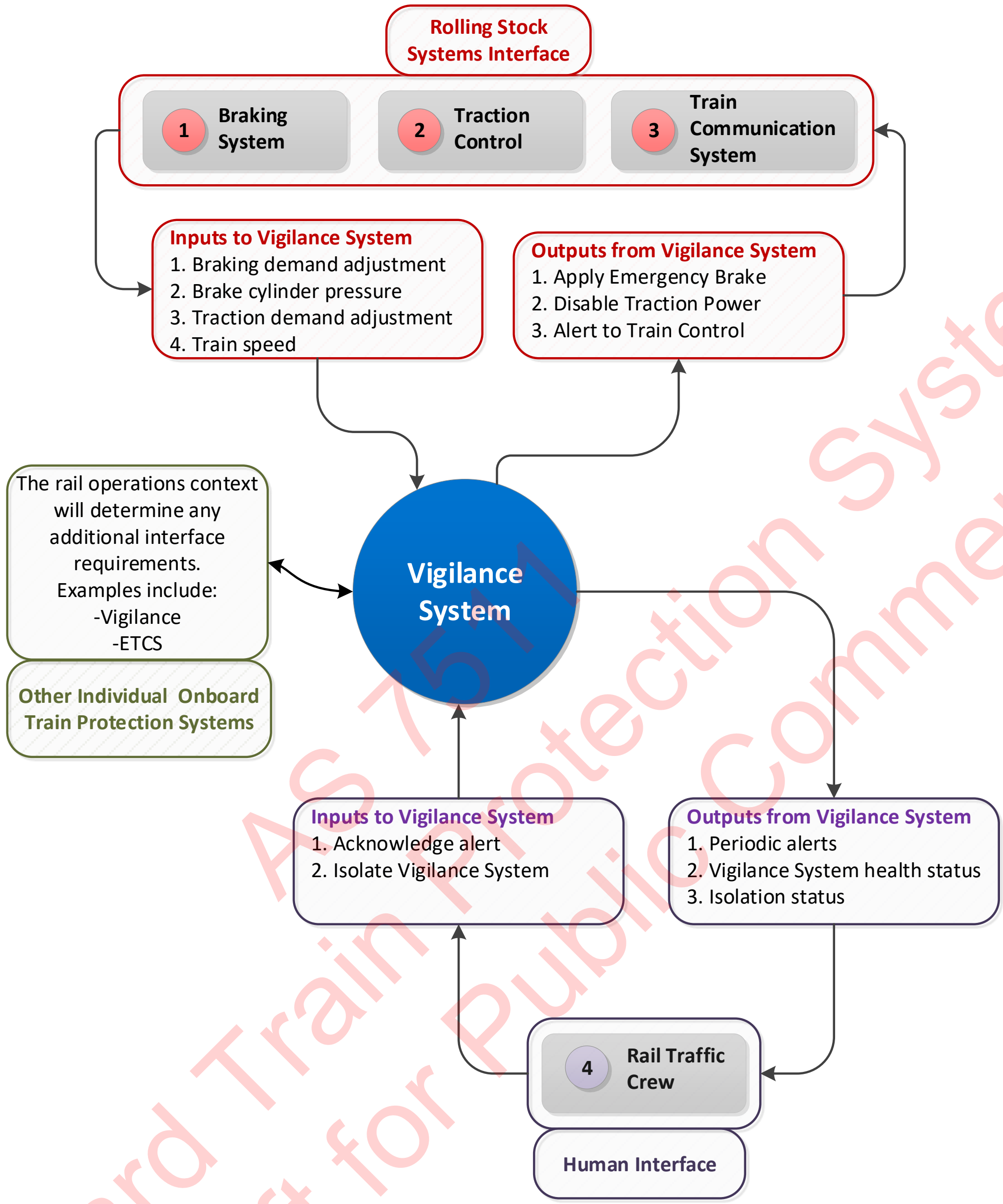

Figure 5:1 Vigilance system context diagram

5.2.3 Vigilance requirements

5.2.3.1 Vigilance interface requirements

5.2.3.1.1 The vigilance system shall periodically alert the rail traffic crew with first a visual alert which if not acknowledged is followed by an audible alert, which requires acknowledgement.

> *C5.2.3.1.1 Commentary*
> *The rail traffic crew are to be alerted to acknowledge the Vigilance system. A two-stage approach is considered best practice from a human factors perspective. The alert duration and tone will be determined by the RTO(s) in consultation with the RIM and consideration to:*
> *(a) rolling stock that operates across different RIMs;*
> *(b) alert tones being easily distinguishable from other alarms / alerts.*

5.2.3.1.2 The vigilance system shall provide the health status of the system to the rail traffic crew.

> *C5.2.3.1.2 Commentary*
> *This is provided to the rail traffic crew, so that if the vigilance system is not healthy appropriate action can be taken such as isolation of the system.*

5.2.3.1.3 The vigilance system shall provide the isolation status of the system to the rail traffic crew.

> *C5.2.3.1.3 Commentary*
> *The status of the vigilance system is to be provided to the rail traffic crew, so that appropriate action can be taken.*

5.2.3.1.4 The vigilance system shall provide a mechanism for the rail traffic crew to acknowledge alerts by either:

(a) manual activation of an acknowledgement mechanism by the rail traffic crew; or

(b) automatically as a result of a linked task.

> *C5.2.3.1.4 Commentary*
> *The rail traffic crew must be able to acknowledge the vigilance system alerts.*
>
> *Linked tasks reduce the number of alerts and acknowledgements generated which diverts rail traffic crew attention when actually performing a train operating related task. For suburban operations it can substantially reduce the number of acknowledgments needed during a run.*
>
> *Linked tasks also help with reducing the opportunity for habitation. Linked tasks may include:*
>
> *(a) movement of any controls that adjust traction or braking demand into or out of any detent positions;*
>
> *(b) meaningful movement of controls that adjust traction or braking demand;*
>
> *(c) operation of the driver's town or country horn;*
>
> *(d) operation of the driver's headlight switch once in succession;*
>
> *(e) operation of the driver's fog light switch once in succession;*
>
> *(f) operation of windscreen wipers.*

5.2.3.1.5 Where an operator enable pedal is used as a form of alert acknowledgement, the vigilance system shall have means to attain the status of the operating range and position in the operator enable pedal.

C5.2.3.1.5 Commentary *It is possible for rail traffic crew to use the operator enable pedal to acknowledge alerts by depressing the pedal, changing its operating range from released/normal operating range to vigilance acknowledgement.*

5.2.3.1.6 The vigilance system shall have means to receive traction and braking demand adjustments.

C5.2.3.1.6 Commentary *This is to enable the Vigilance system to determine whether the tasked linked activity undertaken by the rail traffic crew is considered meaningful movement (refer to clause 5.2.3.1.4).*

5.2.3.1.7 The vigilance system shall provide a mechanism to suppress alerts based on train operating conditions.

C5.2.3.1.7 Commentary *Vigilance system may want to suppress alerts (that is inhibit) when the vehicle is operating within a safe condition (for example train speed is low enough to be considered stationary and sufficient brakes are applied). This suppression allows the rail traffic crew to focus on the task(s) at hand, minimising distractions. The suppression of alerts should be automatic within the system.*

5.2.3.1.8 The vigilance system shall have means to continuously receive speed and the braking inputs from the traction and braking system.

C5.2.3.1.8 Commentary *The speed and braking information enables the vigilance system to determine whether the train operating condition is safe enough to suppress alerts.*

5.2.3.1.9 Where there is a need identified by the RTO for isolation of the vigilance system by the rail traffic crew, the vigilance system shall provide a mechanism to realise it.

C5.2.3.1.9 Commentary *The isolation of an onboard board train protection system is high risk and hence the RTO needs to determine whether an isolation function is required on the vigilance system is based on an analysis on the rail operations context.*

5.2.3.1.10 The vigilance system shall apply the penalty brake when the alert is not acknowledged within the predefined time.

C5.2.3.1.10 Commentary *The rail traffic crew are required to respond to the Vigilance alert within the predefined time, otherwise the Vigilance system deems the rail traffic crew as unresponsive and stops the train.*

5.2.3.1.11 The vigilance system shall release the penalty brake when the Vigilance System alert has been acknowledged.

C5.2.3.1.11 Commentary *The rail traffic crew has responded to the vigilance alert, this means that the penalty brake can now be released.*

5.2.3.1.12 The vigilance system shall disable traction power when the alert is not acknowledged within the predefined time.

> *C5.2.3.1.12 Commentary*
> *Once the vigilance alert acknowledgement time period has elapsed, the vigilance system applies the penalty brake with the intent of stopping the train. The vigilance system will also disable traction power, so that the penalty brake is effective.*

5.2.3.1.13 The vigilance system should send an alert to the train communication system when the alert is not acknowledged with a predefined time.

> *C5.2.3.1.13 Commentary*
> *The train controller / network controller / signaller is made aware that the vigilance system has determined rail traffic crew unresponsiveness and has applied the penalty brake and cut traction power.*

5.2.3.2 Vigilance operational and design requirements

5.2.3.2.1 When the vigilance system alert acknowledge mechanism remains active for longer than the predefined period, the vigilance system shall provide a visual and audible warning to the rail traffic crew.

> *C5.2.3.2.1 Commentary*
> *The intent of this requirement is to check if the acknowledgement mechanism is:*
>
> *(a) faulty; and*
>
> *(b) is being depressed for too long (suggesting human interface issue).*

5.2.3.2.2 It shall only be possible to isolate the vigilance system whilst the train is stationary.

> *C5.2.3.2.2 Commentary*
> *A stationary train is considered safe with or without an operating vigilance system thus isolation does not degrade train safety integrity in its current state.*

5.2.3.2.3 There shall be a process for the rail traffic crew to isolate the vigilance system.

> *C5.2.3.2.3 Commentary*
> *The isolation process considers and covers how the train operating safety is managed SFAIRP when the vigilance system has been isolated.*

5.2.3.2.4 The RTO shall provide a safe SFAIRP justification for the need to isolate a vigilance system.

> *C5.2.3.2.4 Commentary*
> *The rail traffic crew may need to isolate the vigilance system when it has failed. However, a safe SFAIRP process is required to be in place for train operation to continue whilst the vigilance system has been isolated.*

5.2.3.2.5 At the request of the RTO, the vigilance system shall allow up to one pre-emption in the pre-alert phase of the vigilance cycle. Subsequent pre-emptions will be ignored until the vigilance cycle is reset by another means.

> *C5.2.3.2.5 Commentary*
> *A pre-emption is the rail traffic crew using one of the manual acknowledgement options before the alert (the pre-alert phase).*
>
> *This requirement limits rail traffic crew in building up a pattern of acknowledgement that can be carried without conscious thought (habituation).*
>
> *One pre-emption feature is available in some long-distance passenger rolling stock for the rail traffic crew to use when approaching and stopping at a station.*

5.2.3.2.6 A failure in the vigilance system shall result in an automatic penalty brake application

C5.2.3.2.6 Commentary
This is to ensure that the train is in a safe state while the rail traffic crew determines the appropriate action to resume journey in a safe SFAIRP manner.

5.3 Mechanical train stop and trip gear system (MTSTGS)

5.3.1 MTSTGS description

A mechanical train stop and trip gear system is defined as: "A system involving a trip cock on the vehicle and a trip arm located track side which, when engaged, directly initiates an penalty brake application. The train stop is employed at signals in conjunction with a red aspect and also in areas where train speed is required to be externally controlled".
A MTSTGS can also be configured to check and control excessive train speed, by placing a group of timed train stops together.
The requirements of Clause 5.3.3 are only applicable to the onboard (rolling stock) components of the MTSTGS system.

5.3.2 MTSTGS context diagram

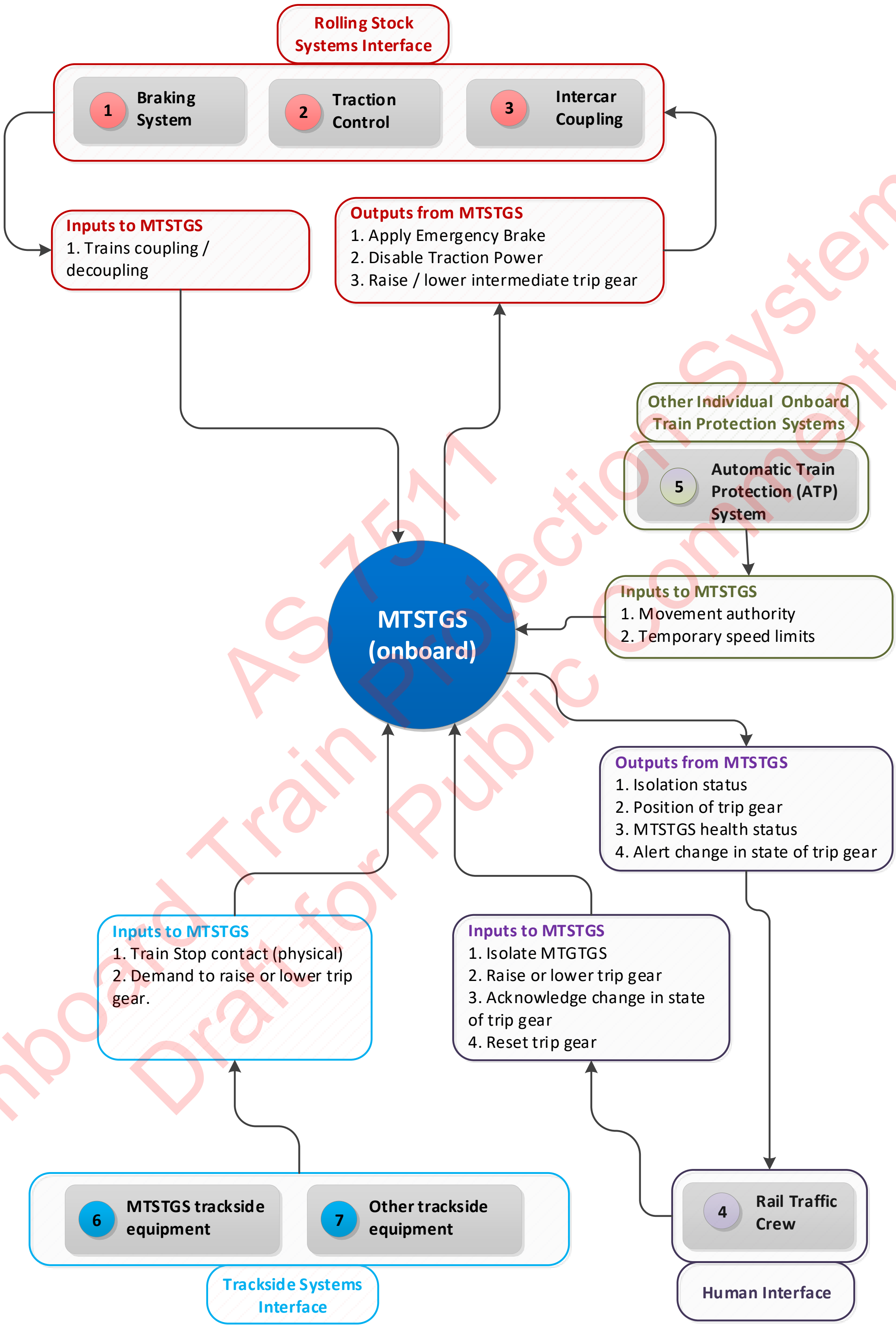

Figure 5:2 Mechanical train stop context diagram

5.3.3 MTSTGS requirements

5.3.3.1 MTSTGS interface requirements

5.3.3.1.1 The MTSTGS shall initiative a penalty brake application when the train has passed a signal at danger.

> *C5.3.3.1.1 Commentary*
> *When a train has passed a signal at danger, the MTSTGS will stop the train. A signal at red/stop will have a raised the train stop arm and the onboard trip gear of the SPAD train will strike the raised train stop.*

5.3.3.1.2 The MTSTGS shall disable (cut off) traction power when the train has passed a signal at danger.

> *C5.3.3.1.2 Commentary*
> *Cutting traction enables the train to be brought to a stop quicker.*

5.3.3.1.3 When configured to protect against overspeed, The MTSTGS shall initiative a penalty brake application when the train has exceeded a predetermined speed limit.

> *C5.3.3.1.3 Commentary*
> *The trip gear on a train travelling in excess of the predetermined speed limit will strike the raised train stop. The MTSTGS will stop to train.*

5.3.3.1.4 The MTSTGS shall disable (cut off) traction power when the train has exceeded a predetermined speed limit.

> *C5.3.3.1.4 Commentary*
> *Cutting traction enables the train to be brought to a stop quicker.*

5.3.3.1.5 The MTSTGS shall provide a facility for the onboard trip gear to be raised and lowered by rail traffic crew.

> *C5.3.3.1.5 Commentary*
> *This is to enable the driver to pass a signal at danger or operate above the predetermined speed limit when authorised to do so.*

5.3.3.1.6 The MTSTGS shall provide a facility for the onboard trip gear to be reset by rail traffic crew.

> *C5.3.3.1.6 Commentary*
> *This is to enable the driver to reset the trip gear after the tripcock is operated.*

5.3.3.1.7 The position of the trip gear (raised or lowered) shall be visually indicated to the rail traffic crew in the cab.

> *C5.3.3.1.7 Commentary*
> *The position of the MTSTGS override must be provided to the rail traffic crew, so that the rail traffic crew are aware of the operational impacts associated with raised trip gear (override).*

5.3.3.1.8 The MTSTGS shall provide a facility to isolate onboard trip gear.

> *C5.3.3.1.8 Commentary*
> *This provides the RTO with the ability to work through equipment failures, and other operational scenarios applicable to their operations.*
>
> *Isolation could be achieved via a safety apparatus isolating (SAI) or trip valve isolating cock.*

5.3.3.1.9 The isolation status of the onboard trip gear shall be visually indicated to the rail traffic crew in the cab.

> *C5.3.3.1.9 Commentary*
> *The isolation status of the MTSTGS must be provided to the rail traffic crew, so that the rail traffic crew are aware of the operational impacts associated with the isolation.*

5.3.3.1.10 Any faults of the onboard trip gear shall be reported to the rail traffic crew.

> *C5.3.3.1.10 Commentary*
> *The rail traffic crew must always be aware of the health of the Onboard trip gear, so that they are able to respond to any faults detected.*

5.3.3.1.11 The MTSTGS shall interface with the Automatic Train Protection (ATP) as agreed with the RTO.

> *C5.3.3.1.11 Commentary*
> *Where the RTO uses both MTSTGS and ATP (e.g. ETCS under limited supervision), the interface must be defined and agreed. This interface may include*
>
> *• Movement authority to proceed at a reduced speed across a train stop.*

5.3.3.2.12 The MTSTGS shall cut traction power if a train is operating on a network fitted with train stops and the trip gear is not lowered.

> *C5.3.3.2.12 Commentary*
> *This is to ensure that if the trip gear or trip gear raising/lowering is achieved manually, the protection function of the MTSTGS is always enabled where available.*

5.3.3.1.13 The MTSTGS shall provide means for the rail traffic crew to acknowledge the change in operational state of the trip gear whilst the train is moving.

> *C5.3.3.1.13 Commentary*
> *In some rolling stock an audible signal on activation/deactivation and an indicator light is used to indicate to the driver of the operational state of the trip gear. The driver acknowledges the indications by pressing the vigilance acknowledgement button.*

5.3.3.2.14 When two trains are coupled / decoupled, the trip gears on the coupled ends shall be raised / lowered as agreed with the RTO.

> *C5.3.3.2.14 Commentary*
> *This is to ensure that trip gears at terminal ends of the train are always lowered (active) following any amalgamation or separation of trains.*
>
> *The raising of coupled ends trip gears when coupled also reduces the likelihood or an unintended penalty brake application.*
>
> *The train should as far as possible, be capable of safely coupling and uncoupling 2 sets from the driver's cab, without the requirement for personnel at track level.*
>
> *For rolling stock with no automatic or remote trip gear dropping and lifting capability, a manual latch is to be provided on the trip gear to retain the trip lever in the latched-up position on all non-leading vehicles.*

5.3.3.2 MTSTGS operational and design requirements

5.3.3.2.1 The method of applying the MTSTGS initiated penalty brake shall be as agreed with the RTO.

> *C5.3.3.2.1 Commentary*
> *Usually on a train or vehicle with an automatic brake system, a penalty brake application is made by venting the brake pipe to atmosphere.*

5.3.3.2.2 The MTSTGS initiated penalty brake performance shall be as agreed with the RTO.

> *C5.3.3.2.2 Commentary*
> *Passenger and freight trains have different penalty brake performances and the safe braking distance is defined by the infrastructure (signal) design which differs across different networks.*

5.3.3.2.3 Following a penalty brake application, the mechanical train stop and trip gear system shall be reset as agreed with the RTO.

> *C5.3.3.2.3 Commentary*
> *On trains without an automatic brake system, this may be accomplished by reducing brake pipe pressure below a predetermined level (for example 70 kPa), such that the brake pipe will not fall below this level with the brake pipe being charged and with the minimum allowable number of compressors running.*

5.3.3.2.4 The MTSTGS components shall be located within the rolling stock outline (onboard).

> *C5.3.3.2.4 Commentary*
> *Engagement of passing obstructions on track other than a raised train stop should not result in a penalty brake application.*
>
> *The allowable envelope for Trip gear equipment is defined in AS 7507.*

5.3.3.2.5 The trip gear shall be mounted on the left hand leading axlebox beneath each driver or operator compartment.

> *C5.3.3.2.5 Commentary*
> *This is the physical interface location for the Mechanical Train Stop and Trip Gear System to perform its safety function.*

5.3.3.2.6 The trip gear shall be in the lowered position on the leading car in the direction of travel when the train is propelling or reversing.

> *C5.3.3.2.6 Commentary*
> *This is to ensure any SPAD or overspeed is detected and intervened as soon as the first wheel passes the train stop.*

5.3.3.2.7 The MTSTGS shall be capable of striking a raised train stop arm whilst travelling in the forward direction at the train or vehicle maximum design speed without causing trip valve malfunction or damage to the trip gear or train stop mechanism.

> *C5.3.3.2.7 Commentary*
> *This is to ensure that the system (both onboard and trackside components) remain fully functional in between maintenance inspections, following an activation.*

5.3.3.2.8 The engagement of the trip gear and a raised train stop when travelling in the reverse direction shall not activate the trip valve.

> *C5.3.3.2.8 Commentary*
> *The trip lever must be capable of striking a raised train stop arm whilst travelling in the reverse direction at a minimum speed of 25 km/h without trip valve activation or it needs to be latched up on terminal cars when trailing in the direction of travel.*
>
> *Trip gears could be spring loaded to allow passing obstructions such as ballast and other signal trip arms in the reverse travel direction.*

5.3.3.2.9 The onboard trip gear shall maintain the isolation status as agreed with the RTO.

C5.3.3.2.9 Commentary

The isolation of an Onboard Board Train Protection System is high risk and must only be performed under authorisation only. The RTO needs to determine the appropriate characteristics of the isolation taking into consideration the risk of the isolation. The isolation characteristics may need to consider both temporary and full isolation functionality.

Some example scenarios for isolation include:

(a) equipment failure (full isolation);

(b) operating a train with an area of restrictive working (temporary isolation).

5.3.3.2.10 The trip gear shall be automatically raised or lowered without activating a penalty brake application when a train exits or enters a network not fitted with train stops.

C5.3.3.2.10 Commentary

The automatic raising of the trip gear eliminates the possibility of an unintended penalty brake applications due to engagement of the trip gear with passing obstructions on track.

The automatic lowering of the trip gear when it enters a network with train stop infrastructure ensures the train protection function is automatic and not reliant on the rail traffic crew (manual).

5.4 Automatic warning system (AWS)

5.4.1 AWS description

An AWS system is defined as: “A system that provides audible and visual warnings to the driver on the approach to signals, certain level crossings and emergency, temporary and certain permanent speed restrictions. It supervises the driver’s reaction to signal caution aspects and indicates to the driver the passing of a clear aspect. Mostly advisory, however it will cause a brake application to be made automatically if the driver fails to react when approaching a restrictive aspect”.[1]

[1] As defined by RISSB in the RISSB Glossary.

5.4.2 AWS context diagram

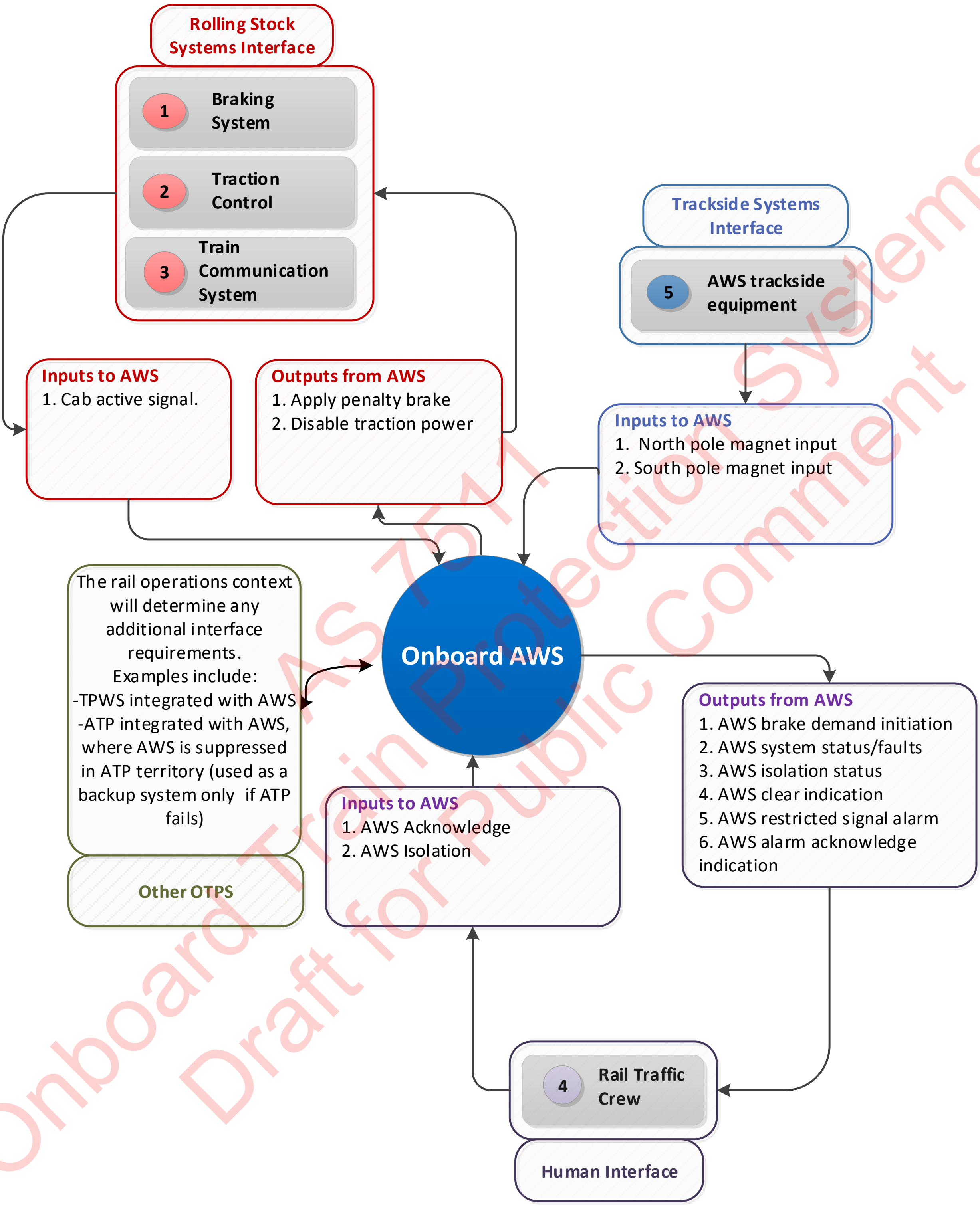

Figure 5:3 Automatic warning system context diagram

5.4.3 AWS requirements

5.4.3.1 AWS interface requirements

5.4.3.1.1 The onboard AWS shall have means to detect the south pole magnetic fields of the AWS trackside equipment.

> *C5.4.3.1.1 Commentary*
> *The AWS onboard equipment distinguishes between the trackside permanent and electromagnets. When both magnetic fields are detected by the onboard AWS system a clear signal aspect ahead is indicated to rail traffic crew which requires no action from rail traffic crew. When the permanent magnetic field only is detected by the onboard AWS, a restricted signal aspect ahead is indicated to rail traffic crew which requires rail traffic crew to acknowledge.*

5.4.3.1.2 The onboard AWS shall have means to detect the north pole magnetic fields of the AWS trackside equipment.

> *C5.4.3.1.2 Commentary*
> *The AWS onboard equipment distinguishes between the trackside permanent and electromagnets. When both magnetic fields are detected by the onboard AWS system a clear signal aspect ahead is indicated to rail traffic crew which requires no action from rail traffic crew. When the permanent magnetic field only is detected by the onboard AWS, a restricted signal aspect ahead is indicated to rail traffic crew which requires rail traffic crew to acknowledge.*

5.4.3.1.3 The onboard AWS shall provide a visual and audible indication to the rail traffic crew when the AWS trackside equipment indicates the approaching signal is displaying a clear aspect.

> *C5.4.3.1.3 Commentary*
> *The rail traffic crew must be informed that the signal ahead is clear, and there are no restrictions.*

5.4.3.1.4 The onboard AWS shall provide a visual and audible warning alarm to the rail traffic crew when the AWS trackside equipment indicates the approaching signal is displaying a restricted aspect.

> *C5.4.3.1.4 Commentary*
> *The rail traffic crew must be informed when there is a restricted aspect ahead to enable action to be taken.*

5.4.3.1.5 The onboard AWS shall provide a mechanism for the rail traffic crew to acknowledge the AWS alarm.

> *C5.4.3.1.5 Commentary*
> *Once informed of the restricted aspect ahead, the rail traffic crew must be able to acknowledge the alarm and drive the train with consideration of the restricted aspect.*

5.4.3.1.6 The onboard AWS shall provide a visual and audible indication to the rail traffic crew when the AWS alarm has been acknowledged.

> *C5.4.3.1.6 Commentary*
> *The rail traffic crew must be informed that the onboard AWS has received the alarm acknowledgement.*

5.4.3.1.7 The onboard AWS shall initiate a penalty brake and disable traction power when the rail traffic crew fail to acknowledge the AWS alarm within a predetermined period of time, as agreed with the RTO.

C5.4.3.1.7 Commentary *When the rail traffic crew does not acknowledge the restricted aspect ahead, the AWS then initiates a brake application to protect the train.*

5.4.3.1.8 The onboard AWS shall indicate the initiation of a penalty brake to the rail traffic crew.

C5.4.3.1.8 Commentary *The rail traffic crew must be made aware of the reasons for the penalty brake and in turn the automatic application of brakes.*

5.4.3.1.9 The onboard AWS shall provide a facility to isolate Onboard AWS.

C5.4.3.1.9 Commentary *This provides the RTO with the ability to work through equipment failures, and other operational scenarios applicable to their operations.*

5.4.3.1.10 The onboard AWS shall provide a visual indication of the isolation status to the rail traffic crew.

C5.4.3.1.10 Commentary *The isolation status of the AWS must be provided to the rail traffic crew, so that the rail traffic crew are aware of the operational impacts associated with the isolation.*

5.4.3.1.11 The onboard AWS shall report all OTPS faults to the rail traffic crew.

C5.4.3.1.11 Commentary *The rail traffic crew must always be aware of the health of the Onboard AWS, so that they are able to respond to any faults detected.*

5.4.3.1.12 The onboard AWS shall interface with other OTPS as agreed with the RTO.

C5.4.3.1.12 Commentary *Where the RTO uses AWS and other OTPS for example TPWS, the interface must be defined and agreed. This interface may include:* *(a) Combined penalty brake indicator* *Note that: "Where multiple OTPSs are applied, they shall not degrade the integrity and functionality of any other OTPS." This requirement is specified in section 4.3: Operational requirements.*

5.4.3.1.13 The onboard AWS shall interface with the train communication management system to determine the active cab status.

C5.4.3.1.13 Commentary *The AWS must be aware of the active cab status, to manage the isolation status.*

5.4.3.2 AWS operational and design requirements

5.4.3.2.1 The onboard AWS shall maintain the penalty brake for a period to be determined by the RTO.

> *C5.4.3.2.1 Commentary*
> *The RTO must determine how long the penalty brake is active. This can include one or more of the following:*
>
> *(a) a timed period (e.g. 59 seconds);*
>
> *(b) until the train has stopped;*
>
> *(c) acknowledgement by the rail traffic crew.*

5.4.3.2.2 The onboard AWS shall maintain the isolation status as agreed with the RTO.

> *C5.4.3.2.2 Commentary*
> *The isolation of an OTPS is high risk and must only be performed under authorisation only. The RTO needs to determine the appropriate characteristics of the isolation taking into consideration the risk of the isolation. The isolation characteristics may need to consider both temporary and full isolation functionality.*
>
> *Some example scenarios for isolation include:*
>
> *(a) equipment failure (full isolation);*
>
> *(b) operating a train with an area of restrictive working (temporary isolation).*

5.4.3.2.3 When a cab becomes active, the onboard AWS shall remove any isolations.

> *C5.4.3.2.3 Commentary*
> *When a cab becomes active, the status of the onboard AWS must be indicated to the rail traffic crew, to ensure they are aware of the current operational capability of the train.*

5.4.3.2.4 The onboard AWS shall not release the penalty brake by rail traffic crew isolation.

> *C5.4.3.2.4 Commentary*
> *These functions must be planned and applied in advance of a penalty brake. The penalty brake must be released by a different mechanism as agreed with the RTO.*

5.4.3.2.5 Where bi-directional running is configured, the onboard AWS shall only be active for trackside AWS systems installed in the direction of travel.

> *C5.4.3.2.5 Commentary*
> *This is important to avoid unwanted interventions when trains operation in the opposite direction along the same line.*

5.5 Train protection and warning system (TPWS)

5.5.1 TPWS Description

The onboard TPWS is a system that stops a train by automatically initiating a penalty brake application where TPWS trackside equipment is fitted, when a train has:

(a) passed a signal at danger without authority; and

(b) when configured for overspeed protection:

  i. approached a signal at danger too fast;

  ii. approached a specified location at excessive speed.

TPWS can reduce the possibility of a SPAD event by stopping a train when it detects that the train is approaching a signal at danger at a speed that would likely result in a SPAD. This is achieved by interfacing with the TPWS trackside overspeed sensor (OSS) to determine if the train is exceeding the allowed speed. The TPWS trackside OSS can also be used at other locations to protect against excessive speed, e.g. approaches to a diverging/converging route, approaches to a speed restricted area, approaches to a buffer stop.

TPWS can reduce the consequences of a SPAD event by stopping a train when it determines that the train has passed a signal at danger. This is achieved by interfacing with the TPWS trackside train stop sensor (TSS).

5.5.2 TPWS context diagram

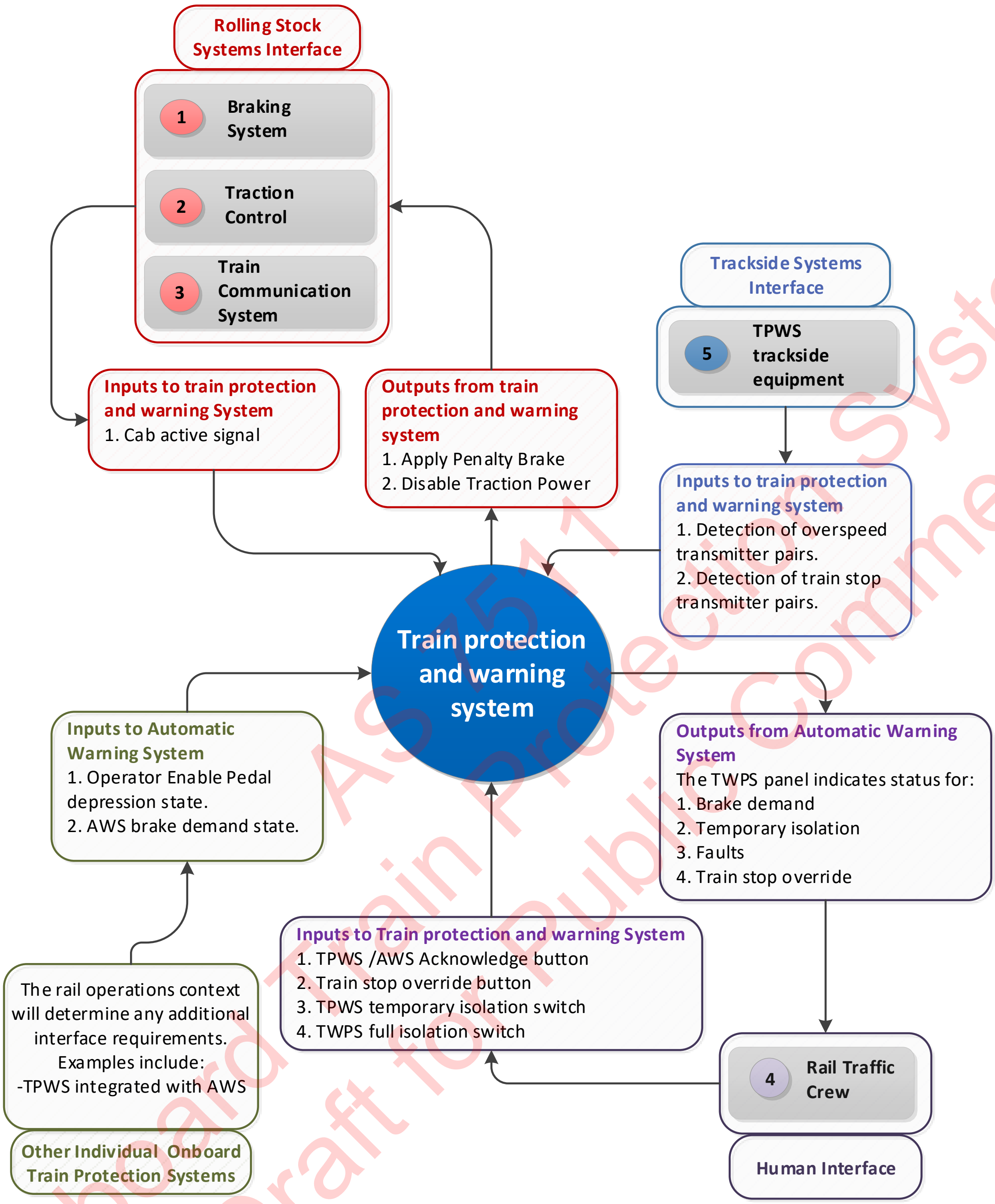

Figure 5:4 TPWS context diagram

5.5.3 TPWS requirements

5.5.3.1 TPWS interface requirements

5.5.3.1.1 When configured to protect against overspeed, the onboard TPWS shall have means to receive the over speed sensor (OSS) transmitter pair input.

C5.5.3.1.1 Commentary *This is to enable the onboard TPWS to determine if the train is exceeding the defined speed.*

5.5.3.1.2 The onboard TPWS shall have means to receive the train stop sensor (TSS) transmitter pair input.

C5.5.3.1.2 Commentary
This is to enable the onboard TPWS to determine if the train has passed a signal at danger.

5.5.3.1.3 The onboard TPWS shall initiate a TSS penalty brake when the TSS indicates the train has passed a signal at danger.

C5.5.3.1.3 Commentary
When the TPWS has determined that the TSS indicates the train has passed a signal at danger, TPWS will stop the train in order to prevent the train from reaching a conflict point ahead of the signal.

5.5.3.1.4 The onboard TPWS shall disable the Traction when the TSS indicates the train has passed a signal at danger.

C5.5.3.1.4 Commentary
The TPWS will also disable the traction, so that the penalty brake is effective.

5.5.3.1.5 When configured to protect against overspeed, the onboard TPWS shall initiate an OSS penalty brake when the OSS indicates the train has exceeded a predetermined speed limit.

C5.5.3.1.5 Commentary
The TPWS will also disable the traction, so that the penalty brake is effective.

5.5.3.1.6 When configured to protect against overspeed, the onboard TPWS shall disable the Traction when the OSS indicates the train has exceeded a predetermined speed limit.

C5.5.3.1.6 Commentary
The TPWS will also disable the traction, so that the penalty brake is effective.

5.5.3.1.7 The onboard TPWS shall provide a mechanism for the rail traffic crew to acknowledge the TPWS penalty brake.

C5.5.3.1.7 Commentary
The purpose of this function is to ensure that the rail traffic crew have acknowledged the TPWS action. This may also play a part in the brake release process.

5.5.3.1.8 The onboard TPWS shall indicate the initiation of a penalty brake to the rail traffic crew.

C5.5.3.1.8 Commentary
The rail traffic crew must be made aware of the reasons for the penalty brake and in turn the automatic application of brakes.

5.5.3.1.9 The onboard TPWS shall provide a facility to override the initiation of a penalty brake in the case where the TSS would indicate the train passed a signal at danger.

C5.5.3.1.9 Commentary
This is to enable the driver to pass a signal at danger when authorised to do so.

5.5.3.1.10 The onboard TPWS shall provide a visual indication of the override status to the rail traffic crew.

C5.5.3.1.10 Commentary
The status of the TPWS override must be provided to the rail traffic crew, so that the rail traffic crew are aware of the operational impacts associated with the override.

5.5.3.1.11 The onboard TPWS shall provide a facility to isolate onboard TPWS.

C5.5.3.1.11 Commentary
This provides the RTO with the ability to work through equipment failures, and other operational scenarios applicable to their operations.

5.5.3.1.12 The onboard TPWS shall provide a visual indication of the isolation status to the rail traffic crew.

C5.5.3.1.12 Commentary
The isolation status of the TPWS must be provided to the rail traffic crew, so that the rail traffic crew are aware of the operational impacts associated with the isolation.

5.5.3.1.13 The onboard TPWS shall report all onboard TPWS faults to the rail traffic crew.

C5.5.3.1.13 Commentary
The rail traffic crew must always be aware of the health of the onboard TPWS, so that they are able to respond to any faults detected.

5.5.3.1.14 The onboard TPWS shall interface with the Automatic Warning System (AWS) as agreed with the RTO.

C5.5.3.1.14 Commentary
Where the RTO uses both AWS and TPWS, the interface must be defined and agreed. This interface may include:

Combined penalty brake indicator

Note that: "Where multiple OTPS are applied, they shall not degrade the integrity and functionality of other OTPS." This requirement is specified in section 4.3: Operational requirements

5.5.3.1.15 The onboard TPWS shall interface with the train communication management system to determine the active cab status.

C5.5.3.1.15 Commentary
The TPWS must be aware of the active cab status, to manage the isolation and override status.

5.5.3.2 TPWS operational and design requirements

5.5.3.2.1 The onboard TPWS shall maintain the penalty brake for a period to be determined by the RTO.

C5.5.3.2.1 Commentary
The RTO must determine how long the penalty brake is active. This can include one or more of the following:

(a) a timed period (e.g. 59 seconds);

(b) until the train has stopped;

(c) acknowledgement by the rail traffic crew.

5.5.3.2.2 The onboard TPWS shall maintain the TPWS override until either:

(a) one active TSS has been passed; or

(b) a time period as configured by the RTO has elapsed.

C5.5.3.2.2 Commentary
The overriding of an OTPS is high risk and must only be performed under authorisation for an individual signal. The RTO needs to determine the appropriate amount of time taking into consideration the risk of the override.

5.5.3.2.3 The onboard TPWS shall maintain the isolation status as agreed with the RTO.

C5.5.3.2.3 Commentary
The isolation of an OTPS is high risk and must only be performed under authorisation only. The RTO needs to determine the appropriate characteristics of the isolation taking into consideration the risk of the isolation. The isolation characteristics may need to consider both temporary and full isolation functionality.

Some example scenarios for isolation include:

(a) equipment failure (full isolation);

(b) operating a train with an area of restrictive working (temporary isolation).

5.5.3.2.4 When a cab becomes active, the onboard TPWS shall remove any overrides and isolations.

C5.5.3.2.4 Commentary
When a cab becomes active, the status of the onboard TPWS must be indicated to the rail traffic crew, to ensure they are aware of the current operational capability of the train.

5.5.3.2.5 When configured to protect against overspeed, the onboard TPWS shall be configurable to cater for rolling stock with different braking characteristics.

C5.5.3.2.5 Commentary
The intent of this requirement is to ensure that the TPWS caters for rolling stock with braking characteristics equivalent to that of freight trains, and to rolling stock with braking characteristics equivalent to that of passenger trains.

5.5.3.2.6 The onboard TPWS shall not release the penalty brake by rail traffic crew isolation or override.

C5.5.3.2.6 Commentary
These functions must be planned and applied in advance of a penalty brake. The penalty brake must be released by a different mechanism as agreed with the RTO.

5.5.3.2.7 When configured to protect against overspeed, the onboard TPWS shall be effective between a minimum and maximum speed as agreed with the RTO within a 10% tolerance.

C5.5.3.2.7 Commentary
To be effective, that is, determine excessive speed, the OSS component of TPWS must be able to detect actual speeds. This speed range will be when the TPWS OSS will be in operation.

5.5.3.2.8 Where bi-directional running is configured, the onboard TPWS shall only initiate a penalty brake when it receives input from the trackside TPWS trackside in the correct order.

C5.5.3.2.8 Commentary
This is important to avoid unwanted interventions when trains operation in the opposite direction along the same line.

5.6 Station protection system (SPS)

5.6.1 SPS Description

SPS provides a location-based alert to the driver for the protection of stations or other trackside features.

Station protection alarms are triggered by single north pole track magnets mounted between the rails.

5.6.2 SPS context diagram

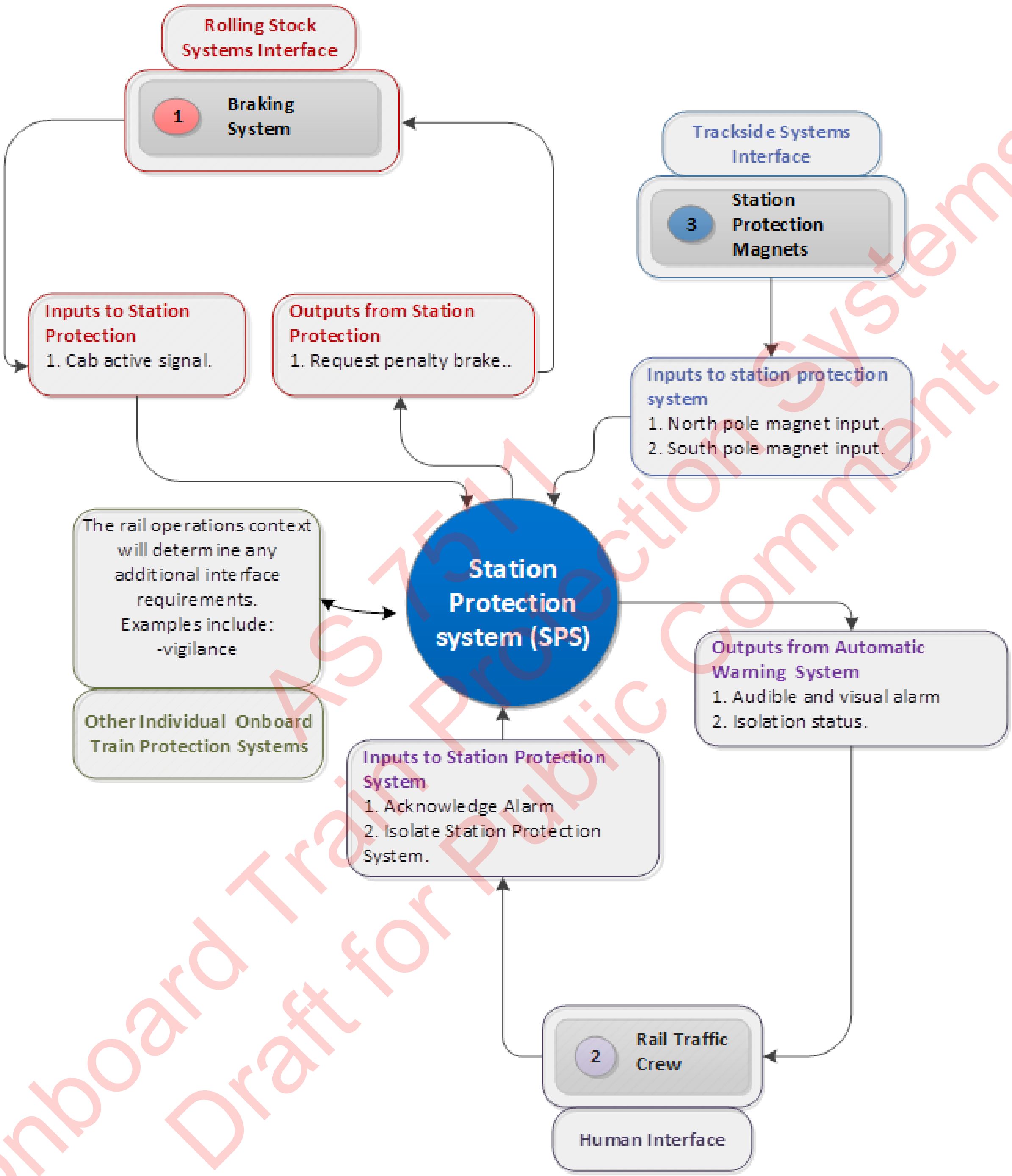

Figure 5:5 Station protection system context diagram

5.6.3 SPS requirements

5.6.3.1 SPS interface requirements

5.6.3.1.1 The onboard SPS shall contain and audible alarm in the cab.

C5.6.3.1.1 Commentary *This component forms a part of the human machine interface for SPS, the audible alarm provides status to the driver.*

5.6.3.1.2 The onboard SPS shall contain and visual alarm in the cab.

C5.6.3.1.2 Commentary *This component forms a part of the human machine interface for SPS, the visual alarm provides status to the driver.*

5.6.3.1.3 The onboard SPS shall contain an acknowledgement button in the cab.

C5.6.3.1.3 Commentary *This component forms a part of the human machine interface for SPS, the acknowledgement button is an input to SPS.*

5.6.3.1.4 The onboard SPS acknowledgement button shall be common with the vigilance system.

C5.6.3.1.4 Commentary *Human factors operational consideration.*

5.6.3.1.5 The onboard SPS shall have a magnet receiver mounted on the vehicle underframe.

C5.6.3.1.5 Commentary *The height of the detector to remain in gauge may vary across fleets. The detector sensitivity must be set to ensure that North Polarity magnets are reliably detected without wrong side failures attributed to false south polarity detections.*

5.6.3.1.6 The magnet receiver arrangement for SPS shall be the same as that used for the AWS.

C5.6.3.1.6 Commentary *Refer to clause's 5.5.3.1.1 & 5.5.3.1.2.*

5.6.3.2 SPS operational and design requirements

5.6.3.2.1 When a north pole track magnet is sensed without a south magnet within 0.5 seconds the station protection system shall sound the audible alarm and flash the visual alarm for three seconds, unless the acknowledgement button is pressed in this time which will cancel the alarms and timing sequence

C5.6.3.2.1 Commentary *If the driver acknowledges the audible and visual alarms within the specified period, SPS will cease to provide the audible and visual alarms and no penalty brake application will occur.*

5.6.3.2.2 If a south pole track magnet is detected within 0.5 seconds after detecting a north pole magnet then the station protection system shall not activate the timing sequence.

C5.6.3.2.1 Commentary *The 0.5 second period allows a train to pass over AWS magnets at 10 km/h and not receive a station protection alarm on a proceed signal.*

5.6.3.2.3 If the acknowledgement button is not pressed within three seconds of the alarm commencing, then the station protection system shall apply a penalty brake.

C5.6.3.2.3 Commentary *If the driver does not acknowledge the audible and visual alarms within the specified period, a penalty brake is applied.*

5.6.3.2.4 If the acknowledgement button is not pressed within three seconds of magnet detection, then the station protection system shall apply a penalty brake.

C5.6.3.2.4 Commentary *If the driver does not press the acknowledgement button within the specified period from magnet detection, a penalty brake is applied.*

5.6.3.2.5 When the station protection applies the brake, the audible alarm shall continue until the acknowledgement button is pressed.

C5.6.3.2.5 Commentary *When a penalty brake application is made by SPS the audible alarm will continue to sound until the acknowledgment button is pressed.*

5.6.3.2.6 When the station protection applies the brake, the visual alarm shall continue flashing until the acknowledgement button is pressed after 60 seconds after the application of the penalty brake application.

C5.6.3.2.6 Commentary *When a penalty brake application is made by SPS the visual alarm will continue to flash for the duration of the penalty brake application.*

5.6.3.2.7 When the station protection applies the penalty brake the penalty brake application shall continue to be applied until the acknowledgement button is pressed after 63 seconds subsequent to the magnet detection.

C5.6.3.2.7 Commentary *When a penalty brake application is made by SPS, the penalty brake will remain active for the specified duration.*

5.7 Operator enable system (OES)

5.7.1 OES description

OES (also known as the deadman system), monitors the presence of a driver at the controls of the vehicle. The OES system will react by directly initiating a penalty brake application if the continuous force, torque or pressure applied the suppression device is removed, however the system itself cannot tell who or what is applying it.

Typical actuation devices include a hand operated device and/or foot pedal.

5.7.2 OES Context diagram

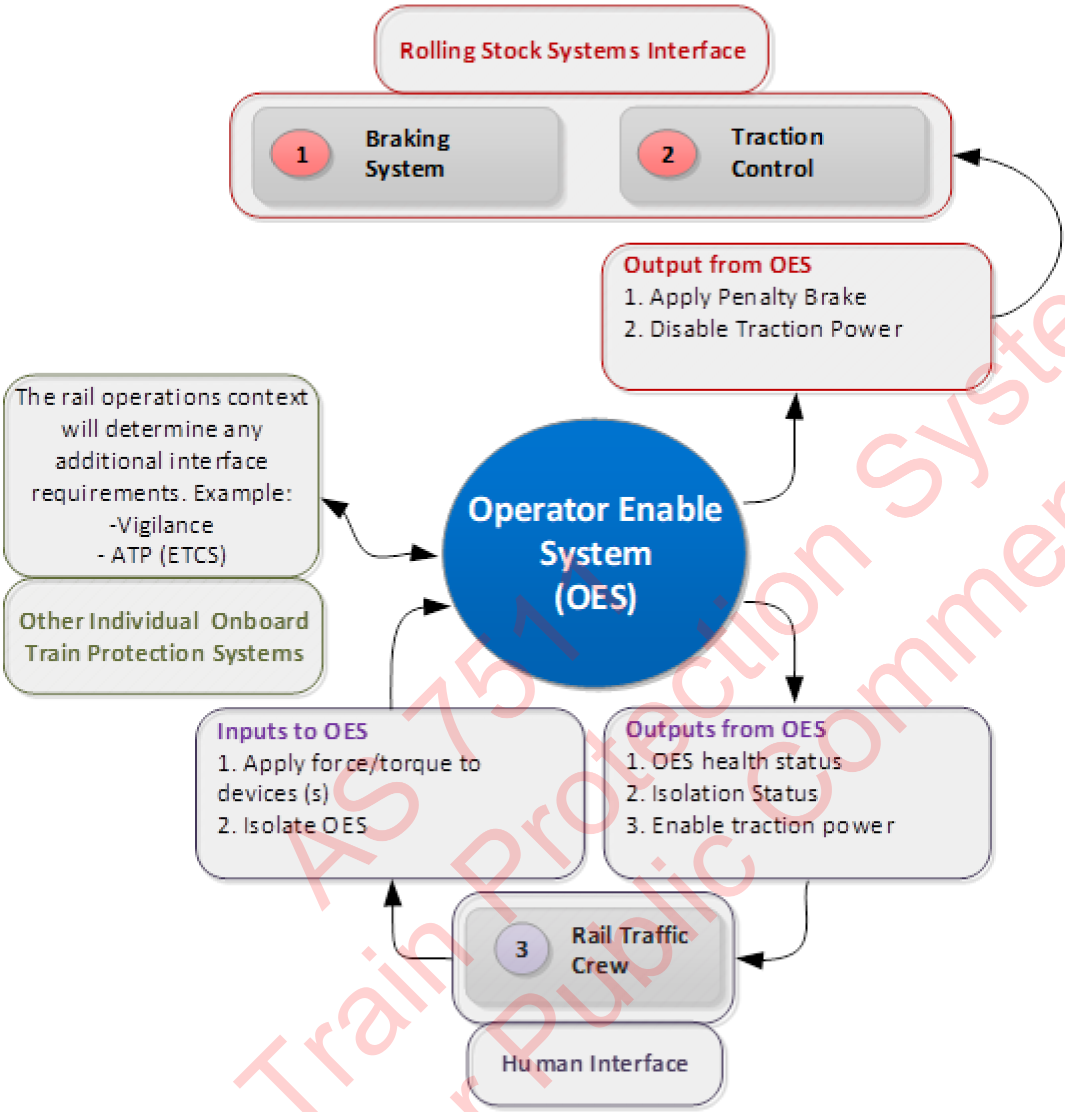

Figure 5:6 OES context diagram

5.7.3 OES requirements

5.7.3.1 OES interface requirements

5.7.3.1.1 If a continuous control input by the driver is interrupted, or not detected for a pre-defined time, while the vehicle is in operating mode, then the OES shall make a penalty brake application.

C5.7.3.1.1 Commentary *System monitors the presence of a driver at the controls of the vehicle and will react by directly initiating a penalty brake application if the driver stops applying force or torque to the device/s (deliberately or unintentionally).*

5.7.3.1.2 The OES shall provide the health status of the system to the rail traffic crew.

C5.7.3.1.2 Commentary *This is provided to the rail traffic crew, so that if the OES System in not healthy appropriate action can be taken.*

5.7.3.1.3 The OES shall provide the isolation status of the system to the rail traffic crew.

C5.7.3.1.3 Commentary
The status of the OES isolation must be provided to the rail traffic crew, so that the rail traffic crew are aware of the isolation status of the OES System.

5.7.3.1.4 Where there is a need identified by the RTO for isolation of the OES by the rail traffic crew, the OES shall provide a mechanism to realise it.

C5.7.3.1.4 Commentary
The isolation of an OTPS is high risk and hence the RTO needs to determine whether an isolation function is required on the OES is required based on an analysis on the rail operations context.

5.7.3.2 OES operation and design requirements

5.7.3.2.1 An OES shall allow the RTC to supress the system using at least two different body parts, contains two activation devices in the driving cab.

C5.7.3.2.1 Commentary
Human factor consideration to avoid RTC muscle strain at one muscle group by allowing to use different muscles groups periodically.

5.7.3.2.2 Transferring between actuation devices by the driver shall be possible, with an overlap prior to release of the initial method.

C5.7.3.2.2 Commentary
To avoid unintended penalty brake application when the driver transfers between devices.

5.7.3.2.3 Actuation devices shall be designed to minimise the risk of drivers in an unconscious state or in various states of incapacitation from keeping the device in the active position.

C5.7.3.2.3 Commentary
The intention is to apply a penalty brake application in the event a driver falls unconscious or becomes incapacitated in some way. The effects of body weight from an unconscious or incapacitated driver on the actuator, whether that be from hand, foot or other need to be well considered.

5.7.3.2.4 Actuation devices shall be designed to minimise the risk of repetitive strain injuries or other physical harm to the driver.

C5.7.3.2.4 Commentary
Human factor consideration for driver operation.

5.7.3.2.5 The OES shall only be able to be inhibited under the following conditions:

(a) When the master controller or direction controller is in the neutral position and the brakes are applied.

(b) When a full service, emergency brake application or penalty brake (by another individual OTPS) has been made.

C5.7.3.2.5 Commentary
The OES need not be operational where:

(a) traction is not enabled (neutral) and brakes are applied as the rolling stock is intended to be stationary under this condition;

(b) a full service, emergency brake application or penalty brake (by another individual OTPS) is already underway.

5.7.3.2.6 The isolation point shall be located away from the rail traffic crew reach while in the driving position.

C5.7.3.2.6 Commentary
This requirement enables OES isolation to only to be carried out if:
(a) the rolling stock is stationary; or
(b) the system to be isolated is not associated with the active cab.

5.8 Automatic train protection (ATP)

5.8.1 ATP description

For the purpose of this Standard, ATP is defined as a system that has the primary purpose of initiating a penalty brake application and inhibiting tractive effort to:

(a) provide overspeed protection; and

(b) provide protection against the exceedance of a movement authority.

5.8.2 ATP selection principles

ATP applications should be focussed on the following three high level principles:

(a) The use of standard off the shelf systems with minimum customization.

(b) The adoption of the applicable international standards where possible.

(c) Interoperability where there is a need for interoperability.

C5.8.2 Commentary
Refer to clauses 4.3.2, 4.4.2 & 5.1

5.8.3 Methods of achieving ATP functionality

(d) ATP functionality can be achieved in a number of ways, for example:

(a) Bespoke ATP systems such as Westect on the Queensland Rail network and PZB in Perth.

(b) ATP functionality within modern train control systems such as ERTMS (ETCS) and CBTC.

C5.8.3 Commentary
Appendix B provides guidance on OTPS fitted across Australia, which identifies some applications of bespoke ATP systems and modern train control systems with ATP functionality.

5.8.3.1 Bespoke ATP requirements

When interfacing with bespoke ATP systems, the RIM(s) for all intended areas of operation shall be consulted to determine the applicable interface, operational and design requirements for the specific system(s).

5.8.3.2 Modern train control systems with ATP functionality

5.8.3.2.1 ETCS requirements

UNISIG ERTMS/ETCS Class 1 Standards shall be used to determine interface, operational and design requirements for ETCS.

5.8.3.2.2 CBTC requirements

(c) IEEE 1474.1 Communication-Based Train Control (CBTC) Performance and Functional Requirements shall be used to determine interface, operational and design requirements for CBTC.

5.8.3.3 ATMS

ATMS is a bespoke modern train control system with ATP functionality that is progressively deployed on the ARTC network.

(d) ARTC ESD-32-01 Signalling rolling stock interface shall be used to determine interface, operational and design requirements for ATMS

5.8.4 Deviations from referenced standards

Where deviations are made from the referenced documentation detailed in clauses 5.8.3.1 & 5.8.3.2 should:

(a) be accompanied by a safe SFAIRP argument;

(b) be made in accordance with clauses 4.3.2, 4.4.2 & 5.1

(c) provide an assessment of equivalency stating how the requirements of this Standard have been met.

C5.8.4 Commentary
Considerations include:

(a) Where customization involves migrating from lineside signalling system to in cab signalling system, consideration to be given to human factors and operational safe working practices.

(b) The implementation of CTCS is one example where assessment of equivalency could be applied.

Appendix C provides example considerations for component selection when adapting existing international OTPS into an Australian rail operations context.

Appendix A Guidance on the application of OTPS

A.1 General

Each OTPS protects against a failure of one, or more, of the manual onboard functions (for example ‘Follow and respond to movement authorities’). Refer to Section 4 for a full list of the functions.

Depending on the rail operations context, the cause of the failure of each manual onboard function may be attributed to one or more to the following:

(a) crew incapacitation (for example, medical event);

(b) human error caused by poor design, fatigue, distraction, inattention, lack of situational awareness and so on;

(c) violations including those of operating rules or requirements or circumvention of safety systems.

When assessing the level of effectiveness of any OTPS against failure, the assessment should consider the system's effectiveness for all of the causes. Most of the existing OTPSs deal with one or more causes in one manual function failure (for example a vigilance system partially covers crew incapacitation, driver fatigue and driver distraction/inattention when a failure in the 'drive train' function occur).

As shown in the guidance tables A.1 and A.2 below no individual OTPS has the capability to cover failures and causes across all manual onboard functions, thus, a set of OTPSs are used together to provide protection against the applicable failures in a particular rail operations context.
It is generally agreed that an ATP system provides protection SFAIRP against a failure in ‘follow and respond to movement authorities’ and ‘ensure safe speed’ but not against a failure in ‘supervise rail corridor’ or ‘supervise passenger transfer’.

Amongst the current proven OTPSs there is little hierarchy between the systems except that some ATP implementations are considered better for speed control and adhering to movement authorities.

It should be noted that the OTPS is only one part of the overall set of safety controls that need to be applied to achieve a safe SFAIRP outcome. Additional levels of safety controls for example infrastructure and administrative systems are required to achieve the desired level of safety performance (See Figure 3.2).

A.2 OTPS application guidance

Tables A.1 & A.2 provide information guiding the application of each type of OTPS, along with the level of effectiveness and limitations associated with each type of OTPS. This information can be used to guide the selection of OTPSs, to form the OTPS(s).

Table A.1 – Table headings and Descriptions for OTPS application Guidance

Table heading	Description
ID	A unique reference for the protection function(s) each type of OTPS.
Protects Against Failures in	Manual onboard functions that an individual OTPS is considered to assist in eliminating the consequences, reducing the severity of the consequences or mitigating the consequences.
Type	The type of OTPS. This can include: 1. vigilance system; 2. mechanical train stop and trip gear system (MTSTGS); 3. automatic warning system (AWS); 4. train protection warning system (TPWS); 5. station protection system (SPS); 6. operator enable system (formerly deadman) (OES); 7. automatic train protection (ATP); 8. door obstruction detection system (DODS); 9. traction interlock system; 10. 10. emerging / future technologies.
Applicable Rail Operations Context	Information relating to the rail operations context where this type of OTPS should be considered.
Effectiveness	How well the OTPS protects against the designated failure of the manual onboard function.
Limitations	Limitations of the individual OTPS in protecting against the identified manual onboard function. Assumes on board equipment is fitted to whole fleet.

Table A:2 - OTPS application, effectiveness and limitation

ID	Protects against failure in	Type	Applicable rail operations context	Effectiveness	Limitations
OES1	Drive train	Operator enable system	All operational areas where rail traffic crew drive the train.	Effective in stopping a train and disabling traction power when driver stops applying force or torque to the device/s (deliberately or unintentionally). Effective in detecting whether a driver is in a driving position.	Only detects a force/torque being applied. It cannot tell who or what is applying it. Requiring people to apply constant force/torque for long durations is a known WHS issue. The suppression force/torque is a compromise between accounting for dead weight (too low) and muscular type injury to the driver (too high). A high force increases the motivation to circumvent the system
SPS1	Drive train	Station protection system	Areas with conventional signalling and the associated trackside equipment (e.g. magnets) is fitted	Effective in stopping a train if the presence of stations or other trackside features are not acknowledged by the driver	Only effective for areas which have trackside equipment installed. Acknowledgement by the driver indicates that the driver has responded to alert. It does not indicate driver is attending to the task appropriately.
VS1	Drive train	Vigilance system	All operational areas where rail traffic crew drive the train.	Effective at stopping the train and disabling traction power when it detects that driver has not performed a linked task or responded to a Vigilance alert.	Driver can be doing task-linked tasks or responding to vigilance alerts from vigilance but not be alert, vigilant or attending to the tasks of driving a train or supervising the rail corridor. Drivers say it can wake them up. There is a time period during which driver response is not being monitored (timing cycle)

Table A:2 - OTPS application, effectiveness and limitation

ID	Protects against failure in	Type	Applicable rail operations context	Effectiveness	Limitations
PVMD1	Drive train	Emerging / future technologies - physiological vigilance measurement devices	All operational areas where rail traffic crew drive the train.	Effective in analysing whether a driver is fatigued or distracted and intervene as required.	Not yet proven technology in rail.
MTS1	Follow and respond to movement authorities	Mechanical train stop and trip gear system	Areas with Conventional Signalling and train stops (trackside) fitted.	Effective in stopping a train in the event of a SPAD.	Does not fulfil function on signals not fitted with compatible trackside equipment. Dependent on a signal overlap design to manage the risk of a collision following a SPAD
AWS1	Follow and respond to movement authorities	Automatic warning system	Areas with conventional signalling and associated trackside equipment (e.g. magnets) fitted.	Effective in stopping a train should a driver fail to respond to a warning aspect.	Only effective where AWS trackside equipment is fitted to the signal. Commonly not fitted to all signals. There is no automatic brake application when a train SPADs.
TPWS1	Follow and respond to movement authorities	Train protection and warning system	Areas with conventional signalling and associated trackside equipment (e.g. TPWS loop) fitted.	Effective in stopping a train in the event of a SPAD.	Dependent on a signal overlap design to manage the risk of a collision following a SPAD. TPWS trackside equipment is not fitted to all signals.

Table A:2 - OTPS application, effectiveness and limitation

ID	Protects against failure in	Type	Applicable rail operations context	Effectiveness	Limitations
ATP1	Follow and respond to movement authorities	Automatic train protection	Operational areas where rail traffic crew drive the train and associated trackside equipment (e.g. balise) fitted.	Effective in automatically stopping a train before the end of a movement authority.	ATP braking performance is based on worst case track conditions.
MTS2	Ensure safe speed	Mechanical train stop and trip gear system	Areas with conventional signalling and train stops (trackside) with timing feature available.	Effective in proving the speed of the approaching train is suitably reduced to the defined speed limits.	The speed checking/proving function is only available when the raised or lowered status of train stops is programmed to interlock with occupancy of the berth track circuit (not available to all train stops). Does not achieve the best operational outcome and hence not a preferred type of protection against a failure in ensuring safe speed (in particular high speeds).
TPWS2	Ensure safe speed	Train protection and warning system	Areas with Conventional Signalling and associated trackside equipment (e.g. TPWS loop) fitted.	Effective in stopping a train if its speed approaching a signal, speed sign or end of line is too fast.	TPWS trackside equipment is not fitted to all signals.
ATP2	Ensure safe speed	Automatic train protection	Operational areas where rail traffic crew drive the train and associated trackside equipment (e.g. balise) fitted.	Effective in enforcing speed if train travels in excess of the allowable speed.	ATP braking performance are based on worst case track conditions.

Table A:2 - OTPS application, effectiveness and limitation

ID	Protects against failure in	Type	Applicable rail operations context	Effectiveness	Limitations
SPS2	Supervise rail corridor	Station protection system	Areas with Conventional Signalling and associated trackside equipment (e.g. magnets) fitted.	Effective in stopping a train if the presence of stations or other trackside features are not acknowledged by the driver.	Only effective for areas which have trackside equipment installed. Acknowledgement by driver indicates driver has responded to alert. It does not indicate driver is attending to the task appropriately.
VS2	Supervise rail corridor	Vigilance system	All operational areas where rail traffic crew drive the train.	Effective at stopping the train and disabling traction when it detects that driver has not performed a task-linked task or a request to respond and stopping the train.	Driver can be doing task-linked tasks or responding to requests from vigilance but not be alert, vigilant or attending to the tasks of driving a train or supervising the rail corridor. Drivers say it can wake them up. There is a time period during which driver response is not being monitored (timing cycle).
COD1	Supervise rail corridor	Emerging / future technologies - corridor obstruction detection	All operational areas where rail traffic crew drive the train.	Effective in detecting obstructions on track and stop train as soon as possible.	Emerging technology in rail (currently trialled on light rail systems). Current systems inaccurate under heavy rain or fog conditions.
TI1	Supervise passenger transfer	Traction interlocking	All operational areas where the doors are not manually opened and closed by rail traffic crew.	Effective in ensuring all doors are closed prior to train departure from station.	Dependent on door obstruction detection System to fully manage the risk of dragging passengers do to trapped objected.

Table A:2 - OTPS application, effectiveness and limitation

ID	Protects against failure in	Type	Applicable rail operations context	Effectiveness	Limitations
DOD1	Supervise passenger transfer	Door obstruction detection	All operational areas where the doors are not manually opened and closed by rail traffic crew.	Effective in preventing doors from closing while passengers are alighting/board the train.	Small and flexible obstruction material such as clothing, handbags and fingers cannot be detected.
OES2	Other operational functions	Operator enable system	All operational areas where rail traffic crew drive the train.	Effective in stopping a train and disabling traction power when driver stops applying force or torque to the device/s (deliberately or unintentionally). Effective in detecting whether a driver is in a driving position.	Only detects a force/torque being applied. It cannot tell who or what is applying it. Requiring people to apply constant force/torque for long durations is a WHS issue. The suppression force/torque is a compromise between accounting for dead weight (too low) and muscular type injury to the driver (too high). A high force increases the motivation to circumvent the system

Appendix B Examples of OTPSs used

Appendix D provides a summary of the combination of OTPS to form the OTPS(s) fitted on trains operating on different networks in Australia.

Table B:1 - Locomotive rolling stock OTPSs used

Rail Network		DIRN	QLD		NSW			VIC			SA	NT	WA
RIM		ARTC	QR	Aurizon	Sydney Trains	CRN	ARTC	ARTC	Metro Trains	V/Line	DPTI	GWA	ARC Infrastructure
Area of Control		Interstate standard gauge	Passsenger	Freight	Metropolitan	Regional branch lines	Heavy rail/ intrastate	Intrastate	Metropolitan	Regional	Passenger	Freight / Passenger	Freight
Locomotive rolling stock onboard protection systems	ATP	Yes @	Westect	Yes - North Coast & Mt Isa lines	Yes * XPT power cars only								
	Vigilance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Station Protection		Yes	Yes									
	OES (deadman)		Yes - Driver only operations		Yes - Driver only operations	Yes - Driver only operations	Yes - Driver only operations				Yes - Driver only operations	Yes	Yes
	AWS												
	TPWS									Yes Loco's hauling passengers			
	Trip gear and train stop				Yes XPT power cars only				Yes				

@Progressively implementing ATMS | * Progressively implementing ETCS L2 | ^ Progressively implementing CBTC

Table B:2 - Self-propelled rollingstock OTPSs used

Rail Network		DIRN	QLD		NSW			VIC			SA	WA	
RIM		ARTC	QR	Aurizon	Sydney Trains	CRN	ARTC	ARTC	Metro Trains	V/Line	DPTI	ARC Infrastructure	PTA
Area of Control		Interstate standard gauge	Passsenger	Freight	Metropolitan	Regional branch lines	Heavy rail/ intrastate	Intrastate	Metropolitan	Regional	Passenger	Passenger	Passenger
Self-propelled rolling stock onboard protection systems	ATP	Yes @	Westect	Yes - North Coast & Mt Isa lines	Yes *				Yes ^		Yes	^	PZB
	Vigilance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Station Protection		Yes - Outside Brisbane										
	OES (deadman)		Yes - Brisbane suburban	Yes	Yes	Yes	Yes		Yes EMU only		Yes	Yes	
	AWS	Yes	Yes - Brisbane suburban								Yes		
	TPWS									Yes Loco's hauling passengers			
	Trip gear and train stop				Yes				Yes EMU Only				
@Progressively implementing ATMS		* Progressively implementing ETCS L2				^ Progressively implementing CBTC							

Appendix C Interoperability component selection guidance

C.1 Interoperability component selection guidance

Table C.1.1 provides example considerations for component selection when adapting existing international OTPSs into an Australian rail operations context.

Table C.1.1 - Interoperability selection guidance

OTPS	Component	Proposed Change	Justification for Change
ETCS	Train radio	Train radio frequency 1800Mhz	European train radio operates on 900MHz. Change required due to ACMA spectrum licensing
	HMI	Alphanumeric train data entry	To allow compatibility with existing train management system

Appendix D Hazard register

Hazard number	Hazard
5.6	Out of Control Trains
5.9	Signals Passed at Danger
5.16	Train protection system failure
5.20	Driver Fatigue
5.21	Driver being distracted
5.22	Overspeed
5.23	Track Failure
5.46	Excessive acceleration
5.2.1.3	Derailment
5.2.1.7	Out of gauge train causing collision with wayside structures
5.9.1.8	In-cab signal failure
5.14.1.3	System being isolated
5.14.1.3	Alarms lacking visibility and audibility
5.15	Failure of deadman
5.16	Train Protection System Failure
7.1.1	Human factors collision or derailment
7.3.1	Human factors damage to rolling stock and or infrastructure

Appendix E Bibliography

The following referenced documents are used by this Standard for information only:

(a) AS 4292 Railway Safety Management.

(b) AS 7503 Train operation interface.

(c) AS 7504 Brake Blocks.

(d) AS 7505 Signalling detection interface.

(e) AS 7722 EMC Management.

(f) AS 7530 Electrical Systems.

(g) AS 7510 Braking systems.

(h) AS 7704 Train Control Systems Change Management.

(i) AS 7532 Audible Warning Device.

(j) AS 7718 Signal Design Process Management.

(k) AS 7715 Train Detection.

(l) RSSB GM/GN2572 Guidance on the provision of Automatic Train Protection Space Envelopes on Rail Vehicles.

(m) RSSB GE/RT075 AWS and TPWS Interface Requirements.

(n) IEC62625-1 Electronic Railway Equipment On-Board Driving Data Recording System Part 1 System Specification.

(o) TfNSW Standard T HR RS 00840 ST RSU Appendix D – Train (Driver) Safety Systems.

(p) TfNSW Standard T HR RS 13001 ST Train Safety Systems.

(q) AS ISO 31000 - Risk management – Guidelines.

(r) UNISIG ERTMS/ETCS Class 1 – SUBSET 027 – FFFIS Juridical Recorder.

(s) UNISIG ERTMS/ETCS Class 1 - SUBSET 033 – FIS for the Man-Machine Interface.

(t) UNISIG ERTMS/ETCS Class 1 – SUBSET 034 – FIS for the Train Interface.

(u) UNISIG ERTMS/ETCS Class 1 - SUBSET 036 – FFFIS for EuroBalise.

About Rail Industry Safety and Standards Board

The Rail Industry Safety and Standards Board is a not for profit company limited by guarantee. Wholly owned by its funding members, RISSB is required to apply the whole of its income and assets to achieving the objects listed in its constitution.

RISSB is responsible for the development and management of Standards, Rules, Codes of Practice and Guidelines for the Australian rail industry.

For further information, visit www.rissb.com.au

RISSB Australian Standards Development Process

The Standards development process is rigorous and transparent.

Authors work with RISSB's Standards Development Managers and Development Groups to ensure that products are acceptable to industry. Standing Committees oversee this work and ensure that proper governance and process is followed. The products are exposed to the public and industry for comment and validated by an independent validator.

Once agreed by the Development Groups, Standing Committees and Validator, the drafts are passed to the RISSB Board for approval.

The same process is used in developing other RISSB products, although Guidelines are not exposed to the public for comment or validated, given their non-binding nature.

Standards Development and Accreditation Committee

RISSB is accredited by the Standards Development and Accreditation Committee (SDAC), and all Standards produced by RISSB since 31 July 2007 are published as Australian Standards.

The Standards Development and Accreditation Committee audits RISSB annually to ensure that RISSB's processes are in accordance with SDAC accreditation requirements.

Sales and distribution

Australian Standards developed by RISSB are sold and marketed through SAI Global. For further information, please visit www.saiglobal.com.

Financial members of RISSB are granted access with membership.

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN 58 105 001 465

For information regarding the development of Australian Standards developed by RISSB contact:

Rail Industry Safety and Standards Board

Brisbane Office
Level 4, 15 Astor Terrace
Brisbane, QLD, 4000

Melbourne Office
Level 4, 580 Collins Street,
Melbourne, Vic 3000

PO Box 518
Spring Hill, QLD, 4004

T +61 7 3274 000
E Info@rissb.com.au

For information regarding the sale and distribution of Australian Standards developed by RISSB contact:

SAI Global Limited
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@saiglobal.com
http://infostore.saiglobal.com/store

ISBN: Enter ISBN.