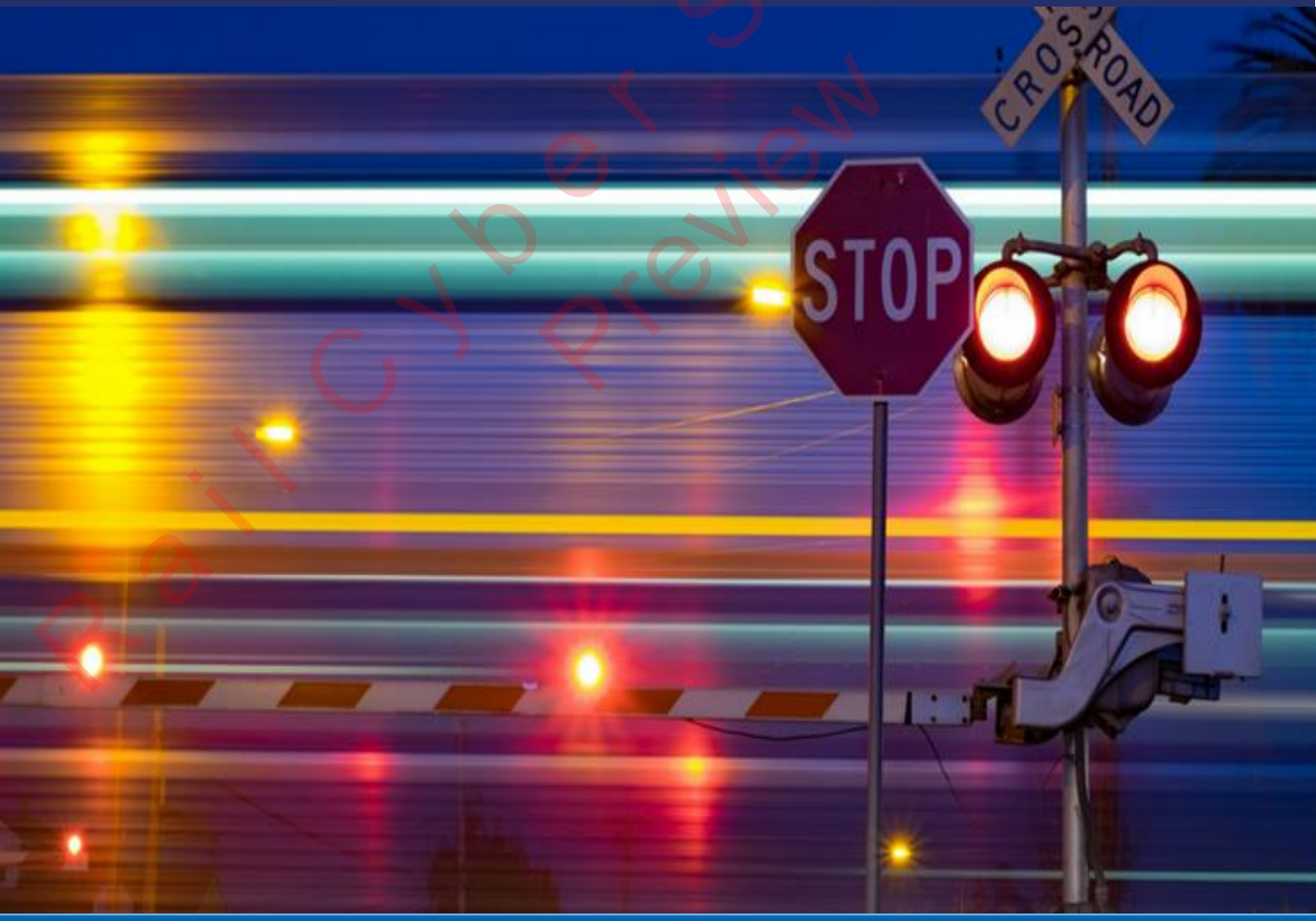
AS 7770:2018

Australian STANDARD®

Rail Cyber Security

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Safety Standard



This Australian Standard® AS 7770 Rail Cyber Security was prepared by a Rail Industry Safety and Standards Board (RISSB) Development Group consisting of representatives from the following organisations:

- Aurizon
- Queensland Rail
- TasRail
- Sydney Metro
- Metro Trains Melbourne
- Roy Hill
- Vic Track
- ASA
- Sydney Trains
- ARTC
- KiwiRail

This Standard was approved by the Development Group and the Safety Integration Standing Committee in June, 2018. On July 10, 2018 the RISSB Board approved this Standard for release.

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

Development of this 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 this 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 this 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.

Paul Daly
Chief Executive Officer
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 can be issued. Australian Standards developed by RISSB can also be withdrawn.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 this 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.

AS 7770:2018

Rail Cyber Security

Document details

First published as: AS 7770:2018
ISBN 978 1 76072 078 0

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

Copyright

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 shall assess whether it meets their Organisation's operational environment and risk profile.

Document control

Document identification

Designation / Title
AS 7770:2018 Rail Cyber Security

Document history

Publication Version	Effective Date	Reason for and Extent of Change(s)
2018 July	July 10, 2018	First Published

Approval

Name	Date
Rail Industry Safety and Standards Board	10/07/2018

Contents

Appendix Contents

1 Introduction

1.1 Purpose

This Standard specifies the requirements for rail transport operators (RTOs) for managing cyber security risk on the Australian railway network.

It has been developed to assist RTOs to establish and maintain a good practice approach to industrial automation and control systems (IACS) and information technology (IT) that is used within their organisations to operate rail systems and protect them from deliberate cyber-attack.

1.2 Scope

This Standard includes the requirements for implementing an effective cyber security management system for rail systems.

In this Standard, rail cyber security is the preservation of the reliability, availability, maintainability and safety (RAMS) of rail control systems and the confidentiality, integrity and availability of data in ancillary systems and the privacy of customer information.

The focus is on cyber threats that can lead to a reduction of reliability, availability, maintainability and safety of railway operations.

1.3 Intended audience

This Standard applies primarily to RTOs and to suppliers, subcontractors, and maintenance contractors, who will need to be aware of changing expectations in the industry that they are supporting.

This Standard has been written for implementation by digital systems engineers or security architects who have a detailed knowledge of rail control systems, critical systems design and cyber security, and for the information of management and all staff who have responsibility for cyber security.

This Standard is not intended to cover urban on-street tramway, light rail networks, or heritage railways operating on a private reservation, but may be applied to such systems as deemed appropriate by the relevant organisation.

1.4 Compliance

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

(a) Requirements.

(b) 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 cannot be able to be applied or other controls could be more appropriate or better.