TS 05327:1.0

T HR SC 01257 SP

Specification

Traffic Management Systems

Issue date: 28 May 2024

Effective date: 28 May 2024

Disclaimer

This document has been prepared by Transport for NSW (TfNSW) specifically for its own use and is also available for use by NSW public transport agencies for transport assets.

Any third parties considering use of this document should obtain their own independent professional advice about the appropriateness of using this document and the accuracy of its contents. TfNSW disclaims all responsibility and liability arising whether directly or indirectly out of or in connection with the contents or use of this document.

TfNSW makes no warranty or representation in relation to the accuracy, currency or adequacy of this document or that the document is fit for purpose.

The inclusion of any third party material in this document, does not represent an endorsement by TfNSW of any third party product or service.

For queries regarding this document, please email Transport for NSW Asset Management Branch at standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

Document information

Owner: Director Signals and Control Systems Engineering
Asset Management
Safety, Environment and Regulation

Mode: Heavy rail

Discipline: Signals and control systems

Document history

Revision	Effective date	Summary of changes
1.0	July 2017	First issue as T HR SC 01257 SP, superseding T HR SC 01257 SP, version 1.0.
1.0	28 May 2024	First issue as TS 05327. Version number recommenced in line with new designation. Changes include adding a section on ETCS L2 interface and removing digital system project requirements.

Preface

This Specification is the first issue as TS 05327 and supersedes T HR SC 01257 SP *Traffic Management System*, version 1.0.

This document sets out the minimum generic operational, functional and non-functional requirements for traffic management systems (TMS).

A TMS plays a key role in the management of railway traffic operation across the TfNSW heavy rail network. It controls and automates train operations such as timetable management, train movements and infrastructure management, minimises delays, and allows increased traffic capacity with reduced operational costs.

A TMS optimises and improves the quality and safety of train services and automates management tasks for operators, including performance analytics. It also provides monitoring of freight and passenger train movement, dynamic timetable editing, rail network access management and automatic route setting. These functions in turn enable more up-to-date, detailed and accurate train information, and better customer service.

By combining the use of automation with manual tasks, a TMS should provide effective and optimal system performance in all foreseeable operating conditions using current and emerging technologies.

Changes from the previous version include the following:

- the incorporation of a technical note on generic workstation and display requirements
- axle counter reset operations have been updated
- ETCS L2 interface has been added
- digital system project requirements have been removed.

Table of contents

1 Scope

This Specification sets out the minimum operational, functional and non-functional requirements for traffic management systems within the TfNSW heavy rail network. It also provides guidance on implementing these requirements.

This document aims to promote the safe, efficient and reliable operation of signalling and train management systems in NSW while encouraging automation and the use of new technologies.

It also outlines relevant requirements for system safety assessment, security assessment and human factors integration (HFI) covered by other standards.

This document does not cover system engineering requirements for a TMS such as development, verification and validation, integration and commissioning. These tasks are addressed during the TAO assessment process or tender evaluation phase.

Nor does it cover other types of signalling control systems such as hardwired mimic panels, which are to be phased out.

2 Application

This document applies to new or existing TMS on the TfNSW heavy rail network for the whole asset life cycle.

It is not applicable to European Train Control Systems Level 2 operations, except when a TMS interfaces with such systems, as specified in this document.

The system safety, security and HFI assessments covered in Section 7 apply to TMS.

Any conflict between this document and other standards will be resolved by TfNSW's Asset Management Branch (AMB).

3 Referenced documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

International standards

CLC/TS 50701 *Railway applications – Cybersecurity*

EN 62264-1 *Enterprise – Control system integration – Part 1: Models and terminology*

IEC 62278 *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*

IEC 62279 *Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems*

IEC 62290-1 *Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts*

IEC 62290-2 *Railway applications – Urban guided transport management and command/control systems – Part 2: Functional requirements specification*

AS/NZS IEC 61709:2019 *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC 62425 *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

IEC 62443 (all parts) *Industrial communication networks – Network and system security*

ISO 9241-210 *Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems*

ISO 11064 (all parts) *Ergonomic design of control centres*

Australian standards

AS 2700 *Colour standards for general purposes*

AS ISO 8601 *Data elements and interchange formats – Information interchange – Representation of dates and times*

AS ISO/IEC 25051 *Software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing*

AS/NZS 1680.2.2 *Interior and workplace lighting, Part 2.2: Specific applications – Office and screen-based tasks*

AS/NZS 2107 *Acoustics – Recommended design sound levels and reverberation times for building interiors*

Transport for NSW standards

TS 00003.1 (T MU MD 00011 ST) *Concessions to Transport Standards, Part 1 – Concession Process*

TS 00031.1 *OT10 Threat-Based Cyber Security Controls, Part 1: Controls and Implementation Requirements*

TS 00096 *Redundant or Staged Signalling Assets Management Requirements*

TS 01471 (T MU AM 06006 ST) *Systems Engineering*

TS 03947 (T MU TE 21001 ST) *Equipment Rooms and Cubicles for Programmable Electronic Systems*

TS 04976 (T MU HF 00001 GU) *Guide to Human Factors Integration*

TS 04978 (T MU HF 00001 ST) *Human Factors Integration – General Requirements*

TS 04981 (T MU MD 20001 ST) *System Safety Standard for New or Altered Assets*

TS 04990 (T MU SY 10010 ST) *Cybersecurity for ICAS – Overview*

TS 04991 (T MU SY 10012 ST) *Cybersecurity for ICAS – Baseline Technical Cybersecurity System Requirements and Countermeasures*

TS 04992 *Surface Transport Fixed Infrastructure Physical Security Standard*

TS 04993 (T MU SY 10013 PR) *Cybersecurity for ICAS – Cyber Risk Management Procedure*

TS 05257 (T HR SC 00719 SP) *Computer-Based Interlocking Equipment*

TS 05258 (T HR SC 01000 SP) *Common Signals and Control Systems Equipment Requirements*

TS 05260 (T HR SC 01250 SP) *Signalling Interlocking and Traffic Management System Interface*

TS 05261 (T HR SC 01251 SP) *Signalling Control Systems Interface Requirements*

TS 05262 (T HR SC 01254 SP) *Signalling Control System Serial Train Information Interface*

TS 05365:0.00 *Signalling Operator Interface* (Obsolete)

TS 05377 (T HR SC 01256 ST) *Telecommunication Transmission Systems for Signalling and Control Systems*

TS 06178 (T MU MD 00005 GU) *Type Approval of Products*

TS 06208 (T MU TE 61007 ST) *Time Synchronisation of Industrial Automation and Control Systems*

TS 06305 (T MU SY 10014 GU) *Application Guide to NSW Cyber Security Policy for Operational Technology*

Legislation

State Records NSW, *Functional Retention and Disposal Authority: FA403*

Other referenced documents

EEMUA Publication 191, *Alarm systems – A guide to design, management and procurement*

Internet Engineering Task Force, RFC 5905 *Network Time Protocol Version 4: Protocol and Algorithms Specification*

RailSafe NPR 700 *Using a Local Possession Authority*

RailSafe NPR 701 *Using a Track Occupancy Authority*

RailSafe NTR 432 *Protecting Activities associated with In-service Rail Traffic*

RailSafe NWT 308 *Absolute Signal Blocking*

RailSafe NWT 312 *Infrastructure Booking Authority*

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document.

ARS automatic route setting

EEMUA Engineering Equipment and Materials User Association

ELCP emergency local control panel

ERP eye reference point

ETCS European Train Control Systems

FMECA failure mode, effects and criticality analysis

GOA grade of automation

HFI human factors integration; the formal process of integrating human factors into the system engineering life cycle. To do this it applies a systematic and scientific approach to the identification, tracking, and resolution of human-system related issues to ensure the balanced development of both the technological and human aspects of operational capability to deliver good overall system performance

interlocking an electrical, electronic or mechanical means of making the operation of one piece of apparatus dependent upon certain predetermined conditions being fulfilled by other apparatus. The logic by which routes that conflict are prevented from being set at the same time

metropolitan rail area the area bounded by Newcastle (in the north), Richmond (in the northwest), Bowenfels (in the west), Macarthur (in the southwest) and Bomaderry (in the south), and all connection lines and sidings within these areas, but excluding private sidings

RAM reliability, availability and maintainability

RAMS reliability, availability, maintainability and safety

RBD reliability block diagram

RCP remote control panel

RIM Rail Infrastructure Manager

SIL safety integrity level

SOE standard operating environment

SPAD signal passed at danger

system safety concurrent application of a systems-based approach to safety engineering and of a risk management strategy covering the identification and analysis of hazards and the elimination, control or management of those hazards throughout the life cycle of a system or asset

TAO Technically Assured Organisation

TfNSW Transport for NSW

TMS traffic management systems

5 Generic architecture

This section explains the context of generic TMS infrastructure and TMS functional requirements specified in this document.

TMS components and configurations can vary from one supplier to another. Figure 1 illustrates the common components of generic TMS structures. This kind of architecture does not consider safety or security-related issues.

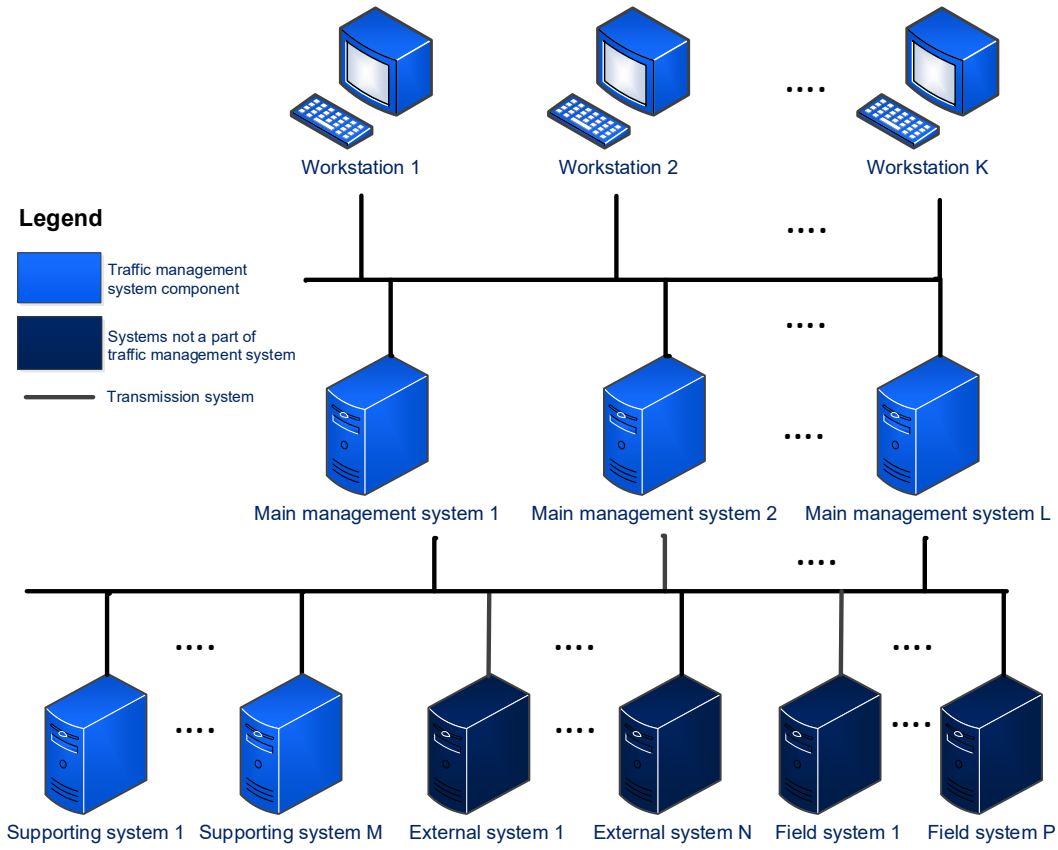

Figure 1 – Generic TMS architecture

A TMS generally has the following six distinct generic subsystem components, which can be implemented on the same or different hardware platforms using various technologies:

- Main management systems – most TMS functions are performed on these systems. They include signalling systems, train management, alarm handling and safety functions (if the TMS has allocated safety functions). They also cover incident management functions and supporting tools.
- Supporting systems – these systems provide functions such as logging, reporting, monitoring and maintaining the TMS and managing timetables, as well as system-wide

functions and supporting tools. They do not normally include real-time or safety-related functions, though there may be exceptions.

- Field systems – these systems provide interfaces to the field assets through various types of systems such as interlocking, telemetry systems and condition or asset monitoring systems. Telemetry systems can interface with the old railway infrastructure or other supporting systems such as tunnel management systems. Interlocking provides safe signalling operation and prevents conflicting train movements to ensure safe train operations. Field systems are not considered to be a part of the TMS.
- External systems – these systems facilitate the exchange of information with the TMS to perform functions such as web interfaces, asset or condition monitoring systems, electrical management systems, external rolling stock and crew information systems. They are not considered a part of the TMS.
- Workstations – these are the user interface to signallers, maintainers and managers of the TMS. Users are assigned different access and operational privileges depending on their roles. Workstations can be used at remote sites or for overview purposes. Based on the outcomes of the HFI assessment, TMS workstations can be used by other systems such as voice communication systems.
- Transmission systems – these systems provide information exchange between applications located on any system or subsystem, as described in TS 05377. Depending on the system design, interfaces, configuration and usage, transmission systems are considered a part of the TMS.

The physical location of each component is determined according to RAMS and disaster recovery requirements.

All performance requirements in this document shall apply to TMS components, including interfaces between the TMS and external and field systems, as shown in Figure 1.

6 General requirements

6.1 Application to existing systems

Existing type-approved traffic management systems used on TfNSW's network do not fully comply with the requirements in this document. They do not need to be modified to fulfil those requirements.

If an existing type-approved TMS needs to be modified or updated, compliance with this document shall be assessed using the complete asset life cycle modelling.

If the modification or update changes the TMS functionality or performance contrary to the requirements in this document, the TAO shall apply for a concession in line with TS 00003.1.

If the changes have no impact on the existing TMS functionality or performance, the functions shall have ‘grandfather rights’, as defined in TS 06178.

Requirements in TS 00096 shall apply if the TMS needs to be updated or upgraded, or if deployment requires staging.

If existing hardwired mimic panels need to be updated, modified or extended, then replacing them with the TMS should be factored into the asset life cycle analysis. If the outcome of this analysis is to keep the existing hardwired mimic panels, then Section 10 of TS 05365:0.00 shall be used as the applicable standard, even though obsolete.

The requirements shall apply to all subsystems or components of the TMS, according to its particular design and implementation, so that the whole system fulfils the requirements.

6.2 Type approvals

TMS hardware and software components as well as supporting products require type approval, as specified in TS 06178.

Type approvals shall be generic product type approval. Functional and performance requirements, interfaces and risks shall be generic enough to cover all site specific configurations.

Site specific type approval shall be allowed if there is supporting evidence.

When the type-approved component needs to be deployed to an operational site, a site specific system assurance shall provide site specific risks and requirements for the configuration changes.

6.3 Compliance with international standards

Based on the identified GOA level, all functional requirements specified in IEC 62290-1 and IEC 62290-2 shall apply. If a conflict exists between the requirements in this document and those of IEC 62290-1 or IEC 62290-2, then this document shall take precedence.

The default GOA shall be GOA 1, which is manual train operation.

The TMS and its components shall be classed as ‘industrial automation and control systems’ in line with IEC 62443 (all parts). This classification shall apply to all TMS components whether located remotely or in the cloud hosting or cloud storage.

The TMS and its components shall be classed as either a level 2 or a level 3 system according to EN 62264-1.

7 Supporting assessments

TMS shall comply with the requirements for supporting assessments specified in TS 01471.

The TMS shall be supported primarily by the following three assessments, as part of the overall safety case:

- system safety assessment
- HFI assessment
- security assessment.

These three assessments shall be used and kept up-to-date during the life cycle of the TMS.

7.1 System safety assessment

The system safety assessment shall comply with TS 04981.

Safety signalling systems such as interlockings, which are part of the field systems illustrated in Figure 1, provide safety using various train detection mechanisms including axle counters or track circuits. If signalling systems cannot reduce all hazards identified with train operations, then these risks can be transferred to the TMS for further mitigation or vice versa.

The following hazards shall be considered during the system safety assessment, as a minimum:

- derailment
- loss of separation between rail vehicles
- loss of separation between rail traffic and road vehicles
- loss of separation between rail vehicles and worksites
- a person in the path of the rail vehicle
- gauge infringements due to misrouting
- loss of structural integrity due to misrouting
- overcrowding
- exposure of moving parts such as points
- loss of balance
- risks transferred or allocated to the TMS from other system safety assessments
- risks allocated to the TMS from the overall system safety assessment.

7.2 Human factors integration assessment

The HFI assessment shall comply with TS 04978. For further guidance on complying with these requirements, refer to TS 04976.

The design of the user interface to the TMS is critical for the effective and efficient operation of the system. The interface shall be designed using established human factors design principles and human computer interaction guidelines.

This document specifies the inputs that shall be considered during the HFI assessment.

If those parameters cannot be fulfilled or the principles and guidelines cannot be applied, then a justification for such deviation shall be provided with supporting evidence.

7.3 Security assessment

The security assessment shall comply with the following standards:

- TS 00031.1
- TS 04990
- TS 04991
- TS 04993.

8 Failure requirements

A failure is a loss of at least one of the following integrities in any component of the TMS and associated controls, as detailed in Section 13:

- signalling assets
- train
- safety operations
- display
- alarm
- transmission system.

The TMS shall be modelled as one entity when calculating its RAM requirements. Non-availability of any TMS function that is essential to signalling and train operations shall be taken as a failure of that function – whether or not it is required by the whole TMS. For example, if a function such as a route setting has a failure only in one part of the TMS, it will still be considered a complete failure.

The following shall not be considered as failures:

- planned activities with assessed and approved controls in place for safe and reliable signalling and train operations
- failure of systems that are not part of the generic TMS architecture shown in Figure 1, such as failures at field systems
- performing a failed function in an alternate way within the TMS without compromising the integrity and safety.

Failure analysis shall include common cause failures as required by IEC 62278. The TMS shall fulfil the RAM requirements for all safety or non-safety functions as specified in IEC 62278.

Appendix F provides additional information on the concept of integrity.

9 Availability requirements

The TMS shall be available 24/7, to provide safe, reliable and efficient signalling and train operations. The TMS availability requirements in this document have been apportioned from customer service business requirements, such as on-time running requirements for advanced train control systems, and rail operation centre availability requirements. They are also based on measured failure data for existing control systems.

The operational availability of TMS as a whole shall be 99.99% or better, based on the failures listed in Section 8.

The availability requirements of the components and subsystems of the TMS shall be apportioned from the overall TMS availability requirements and supported with evidence-based analysis. Depending on the characteristics of the TMS functions, components or subsystems, such as SIL, different availability requirements can be set.

Availability calculations for random failures shall be based on techniques such as FMECA or RBD, or on the prediction methods specified in AS/NZS IEC 61709: 2019. The analysis shall also cover common cause failures and redundancy.

Systematic failures of safety or non-safety functions shall be identified and mitigated using relevant engineering techniques, procedures and standards, such as IEC 62279.

Appendix E provides additional information on availability requirements.

10 Reliability requirements

The mean time between failures or mean time for failure of the TMS as a whole shall be greater than 50,000 hours based on the failures detailed in Section 8.

The reliability requirements of the components and subsystems of the TMS shall be apportioned from the overall TMS reliability requirements, and supported with evidence-based analysis.

Depending on the kinds of functions, components or subsystems such as SIL, different reliability requirements can be set.

Reliability calculations for random failures shall be based on techniques such as FMECA or RBD, or on the prediction methods specified in AS/NZS IEC 61709:2019. The analysis shall also cover common cause failures and redundancy. Multiple or secondary failures that can occur due to a failure within the TMS, or repair delays, shall be considered.

If the required reliability information can be extracted from existing site applications and the amount of information is statistically justifiable, then the empirical reliability information shall be used for the reliability calculations.

Systematic failures of safety or non-safety functions shall be identified and mitigated using appropriate engineering techniques, procedures and standards, such as those outlined in IEC 62279.

Appendix E provides additional information on reliability requirements.

11 Maintainability requirements

The mean down time of the TMS as a whole shall not be greater than 52.5 minutes per year on average based on the failures detailed in Section 8.

The maintainability requirements of the components and subsystems of the TMS shall be apportioned from the overall TMS maintainability requirements and supported with evidence-based analysis. Depending on the kinds of functions, components or subsystems of the TMS, such as SIL, different maintainability requirements can be set.

The following parameters shall be set for the TMS so its availability and reliability requirements can be met, supported with evidence-based analysis:

- mean time between maintenance, both corrective and preventative
- mean time to maintain, both corrective and preventative.

The scope of the maintainability shall also cover the impact of failures, and the potential for multiple failures.

The TMS shall provide at least the following maintenance functionalities:

- fault detection facilities
- fault isolation facilities
- secure remote management
- predictive and preventative maintenance based on the performance history of the assets.

Appendix E provides additional information on maintainability requirements.

12 Safety operations

Safety operations should normally be performed within the signalling safety systems, such as interlocking. Depending on the results of the system safety assessment, the TMS can have various allocated safety functions, some of which may be transferred from other systems. Each safety function shall be assessed and its SIL allocated using the processes defined in IEC 62425 and IEC 62279.

These safety functions shall include, at least:

- applying, maintaining or removing a restriction
- providing integrity between the display and field systems and train traffic by including the following:
  - not losing situational awareness
  - not leading incorrect safety, operational and maintenance decisions
- controls to cancel routes and to set signals to stop
- controls to set routes and clear signals
- alarms or warnings to enable the signaller to effectively respond to unexpected events
- axle counter reset operation.

12.1 Safety requirements

System safety assessments for all functions of the TMS shall comply with TS 04981.

If only some safety functions or a part of the safety functions are apportioned to the TMS, then a gap analysis shall be conducted to identify other safety requirements the TMS must comply with.

Requirements for all safety operations shall be based on the outcomes of system safety and HFI assessments.

Alternatives that achieve a similar operational concept and provide the same level of safety may be considered.

12.2 Restrictions

The following three types of restrictions shall be applied by the TMS:

- Total block – this shall apply to different types of assets. If an asset is blocked, then no asset operation shall be performed, without exception, by preventing the issue of controls to the blocked assets. The assets shall be in the following states prior to the application of the restriction:

  - train detection assets – all associated routes are normal
  - moveable assets – in desired state and locked
  - signals – all associated routes are normal and automatic operations are disabled
  - other assets – their operations are disabled or they are in normal state.
- Stop and block – this shall apply to controlled signals, allowing the signal to clear under special conditions. It shall prevent controls being issued to set routes from the signal unless an explicit stop and block override command is executed and acknowledged. All associated routes shall be normal and automatic operations disabled.
- Reminder notice – a comment that can be attached to different types of assets in case a user attempts to issue a control that changes the asset from the safe state. The notice shall not obstruct any asset operation.

12.2.1 Restriction operations

The following restriction operations, at least, shall be considered for the TMS.

The TMS shall be capable of applying:

- the same restrictions on multiple assets and different asset types
- multiple restrictions on one asset
- different types of restrictions on one asset

If more than one restriction is applied on an asset:

- removing a restriction shall not affect remaining restrictions
- the asset shall be restricted until the last restriction is removed
- the asset’s behaviour shall be determined by the most restrictive restriction type
- one restriction shall be removed at a time.

The TMS shall be capable of propagating the blocks to other assets automatically if they are affected, or required for integrity or completeness.

The propagated blocks shall not be modified individually. However, if the originating block is modified, then the propagated blocks shall be updated automatically.

In addition:

- A restriction shall only be applied or removed in response to an explicit user command.
- The effectiveness of a restriction shall not be affected by any other operation.
- The TMS shall prove that the restriction is active and effective before providing feedback to its requester.

- A mechanism shall be provided to prevent removal of the restriction without confirmation from site personnel.
- TMS shall maintain integrity of restrictions between multiple users.
- Subject to the outcomes of the HFI assessment, applying, modifying and removing a restriction shall have a confirmation process.

12.2.2 Worksite protections

The TMS shall be capable of applying the following worksite protections using the restriction types listed in Section 12.2:

- absolute signal blocking (ASB) based on RailSafe NWT 308
- protecting activities associated with in-service rail traffic based on RailSafe NTR 432
- local possession authority (LPA) based on RailSafe NPR 700
- infrastructure booking authority (IBA) based on RailSafe NWT 312
- track occupancy authority (TOA) based on RailSafe NPR 701.

The TMS shall provide the following functionalities, as a minimum, which will be analysed during the HFI assessment:

- The TMS shall use workstations to determine the boundaries of the worksite protection. It shall then determine the optimal way of applying the worksite protection using the restrictions without compromising the safety of the worksite protection. For example, with minimum impact on signalling and train operations on other lines or areas.
- Users with adequate privileges shall be able to modify the existing worksite protection boundaries with the TMS providing feedback on any safety implications.
- The TMS shall manage user conflicts and coordinate and facilitate worksite protections.
- The TMS shall support administrative procedures for setting and releasing worksite protections by replacing paper-based forms with digital forms and pre-filling them with worksite protection information.
- The TMS shall provide a mechanism so that a field person such as a protection officer shall be in control of creation, modification and removal of worksite protection while the TMS operator manages the process.
- The TMS shall be capable of handling multiple worksite protections without compromising safety when:
    - managed by multiple operators
    - in overlapping areas
    - in areas with different protection requirements.

The TMS shall not set a worksite protection in the following situations, and users will be notified to manage such situations:

- when all approaching trains cannot be proven capable of stopping before entering the area
- when trains inside the area cannot be proven to be at a standstill, yet are not authorised to move.

12.3 Signal cancelling operations

The TMS shall provide the following types of signal cancelling operations:

- single signal
- emergency replacement group
- unconditional emergency stop order.

12.3.1 Single signal

The TMS shall be capable of setting controlled signals that support a cancel control, or automatic signals that support an emergency replacement control to stop at any time, regardless of their current states.

12.3.2 Emergency replacement group

The TMS shall be able to set a group of controlled signals to stop when it is required.

Signals shall be grouped according to the operational requirements. This operation shall be available at all times and take priority over other operations. All pending controls for signals within the group shall be discarded.

The cancelling of signals shall be handled in accordance with the field systems requirements, such as pacing of cancellation operation for each interlocking.

> Note: If the field system provides an emergency replacement function as a control, then the TMS can use this function.

Subject to the outcomes of the HFI assessment, this operation shall have a user confirmation process to prevent unintentional operation.

The cancel operation shall be reissued periodically if a previous cancel control has failed. The repeat period shall be determined according to the characteristics of the field system.

12.3.3 Unconditional emergency stop order

The TMS shall have the capability to safely manage unconditional emergency stop order operations if this functionality is allocated to the TMS.

Users with adequate privileges shall be capable of issuing an unconditional emergency stop order to a selected train or all trains within the preconfigured area.

Each train shall indicate its emergency stop status on the workstation.

Subject to the outcomes of the HFI assessment, users shall be able to perform the following operations:

- send an unconditional emergency stop order:
    - to stop a specific train – users shall be able to select the train to be stopped by selecting the train from the workstation or from a list
    - to stop all trains within the preconfigured area – when users select the preconfigured area, the TMS shall issue an emergency stop order to each train within the selected area automatically. The TMS shall continue to issue emergency stop orders when any train enters the selected preconfigured area
- revoke an unconditional emergency stop order:
    - an emergency stop order shall be revoked for each train individually, not within a group or area
    - when an emergency stop order is revoked for any train within a preconfigured area, the TMS shall not issue an emergency stop order when a train enters that area.

A confirmation or review mechanism shall be in place to prevent unintentional or incorrect operations.

12.4 Axle counter reset operations

The TMS shall be capable of safely managing an apportioned part of the axle counter reset operations.

Based on the axle counter and safety signalling systems capabilities, the TMS shall be able to distinguish the axle counter failures that can and cannot be reset and present this information to the user.

The TMS shall be able to reset the axle counter failures if the nature of the failures allows the reset operation. This shall be identified during the hazard analysis as well as the HFI assessment.

The following shall apply to all reset types:

- A one-step acknowledgement process shall be followed before the reset command is sent to the field.
- The TMS shall display an indication for any counting zone being affected by a reset operation.
- The TMS shall not initiate the reset operation automatically.

- The TMS shall raise alarms related to axle counters, including associated information, when it detects alarm conditions, or when the safety signalling system reports the alarm condition.
- The TMS shall present an identical indication and command interface for different axle counter products if the axle counter system provides such a function.
- The TMS shall allow to select, de-select or modify a group of axle counters as reset operations.
- All reset operations shall have supporting safety procedures.

Interface details between the TMS and interlocking for the axle counter operations are covered in TS 05260.

12.4.1 Types of reset operations

The TMS shall support the following types of reset operations, subject to availability in the axle counter system:

- Preparatory reset – the section shall be reset to unoccupied after the passage of a sweep train. There shall be an acknowledgement of the completion of the sweep train passage.
- Unconditional reset – the operator shall give permission to reset the axle counter section manually by the maintenance personnel at the location.

13 Integrity requirements

13.1 General

The TMS provides an interface between a number of systems and users. The TMS should be able to assure the user that the information it presents in visible form is accurate and timely. Failure to do this will lead to a loss of integrity. Information on the concept of integrity used in this document is included in Appendix F as well as in IEC 62425.

Integrity of a system or part of a system shall meet all allocated requirements within specified boundaries under all stated operating conditions. The TMS shall provide integrity in the following situations, as a minimum:

- start up or shut down
- if the system has redundant configuration before, during and after the changeover operation
- switching to or from disaster recovery sites
- inconsistency or unavailability of interfaces
- race conditions

- inactivity
- configuration changes
- maintenance activities
- hardware, software, SOE, configuration or environmental failures
- synchronisation or backup or restore processes
- security threats including cyber attack
- stress and disruptive conditions.

13.2 Loss of integrity

All users affected by the loss of integrity of the TMS shall be informed.

When integrity is lost, the TMS shall restrict or disable all affected signalling and train operations until all compromised integrities are restored, to allow safe and reliable signalling and train operations. A system safety assessment shall be performed to identify all affected operations for each integrity type.

Integrity shall be deemed compromised for all integrity types identified in Section 8 when:

- integrity within the related application or between applications is compromised
- integrity with the interfaced systems, subsystems or products is compromised
- integrity of configurations is compromised
- the TMS loses its integrity, for example, with application or hardware failures
- the transmission system used between applications is compromised
- security is compromised.

If the connection between applications or interfaces can have a non-activity period of longer than 20 seconds, then a mechanism to detect the availability of application shall be devised, such as a heartbeat mechanism.

If there is a non-activity period of more than 20 seconds, integrity between the applications or interface shall be assumed as compromised.

The following sections list the specific failures for each integrity type. Other failures that can compromise the specific integrity type shall be identified using appropriate failure analysis methodologies.

13.3 Signalling asset integrity

The TMS shall assure that all components within the TMS have integrity with the following field systems:

- telemetry systems in line with TS 05260
- interlocking systems in line with TS 05260
- other field systems that provide indications or accept controls based on approved interface specifications.

13.3.1 Indication integrity

Indication integrity shall cover the following situations as a minimum:

- not indicating asset status correctly within a set period of time after the asset status changes at the field
- indicating asset status incorrectly after the asset status changes at the field
- indicating asset status incorrectly while asset status is not changed at the field.

13.3.2 Control integrity

Control integrity shall cover the following situations as a minimum:

- not sending the right control to the right asset when it is required within the set period of time
- sending the wrong control to right asset when it is required
- sending the control to the asset when it is not required.

13.3.3 Compromised signalling asset integrity

The signalling asset integrity shall be deemed compromised in the following situations:

- the field system indicates that it loses its integrity with the signalling assets, including indication and control
- the field system fails
- the integrity of communication between the TMS and the field system is compromised
- the field system indicates that the asset information received has an integrity problem, such as a health bit
- the TMS detects the signalling asset has lost its integrity while field systems report otherwise.

When signalling asset integrity is lost, the last known states of signalling assets shall not be lost. Instead they shall be presented to the user with an associated special indication that can be used for an operational decision.

13.4 Train integrity

The TMS shall determine the train details accurately and in a timely manner based on the timetable information and asset status, namely train detection systems.

The following situations, at a minimum, shall be taken into account for the demonstration of train integrity:

- track is unoccupied unexpectedly, so the train disappears
- track is occupied unexpectedly, so a train appears
- detection of unsafe separation between trains

  Note: Safe separation between trains is normally the responsibility of signalling systems.
- detection of wrong train movement against its planned direction, characteristic, route and other parameters.

Train integrity shall be deemed compromised when:

- signalling asset integrity is compromised
- integrity with other systems related to train operation is compromised.

13.5 Safety operation integrity

The following shall be considered as safety operation functions at the TMS level:

- restrictions and worksite protections
- axle counter reset operations.

Safety operation integrity shall cover at least the following situations:

- applying and maintaining an ineffective safety function when it is required
- applying and maintaining an effective safety function when it is not requested
- removing a safety function when it is not requested
- not removing a safety function when it is requested.

The safety operation integrity shall be deemed compromised when the signalling asset integrity is compromised.

13.6 Display integrity

The TMS shall provide the user with information that is accurate and has integrity by ensuring:

- the display is active, up to date, functional and ready to take command
- display characteristics are within their expected parameters, such as colours.

No more than one incorrect object in 50,000 hours shall be displayed on any human machine interface (HMI) such as workstations, due to a systematic failure, irrespective of the number of HMI configured.

No more than one incorrect control in 50,000 hours shall be sent to field systems because of a systematic failure, irrespective of the number of HMI configured.

When a failure is detected, the root cause analysis shall include events leading to incorrect presentation or operation, such as indication factors or selection of objects, preconditions and circumstances.

13.7 Alarm integrity

The TMS shall ensure alarms or warnings are generated or cleared in real time when the defined conditions are fulfilled. Audible and visual components shall be part of the alarm integrity.

Alarm integrity shall cover the following situations:

- not generating or clearing the right alarm for the right conditions within the set period of time
- generating or clearing the wrong alarm for the required conditions
- not generating or clearing the alarm for the required conditions.

Alarm integrity shall be deemed compromised when signalling asset integrity is compromised.

13.8 Interface integrity

The TMS shall detect and act when any interface it uses is compromised including, as a minimum:

- security as detailed in Section 17.4
- inactivity as detailed in Section 13.1
- transmission system outlined in TS 05377
- conditions detailed in the relevant interface control document (ICD).

14 Redundancy requirements

A number of technical solutions exist to support or improve the RAM requirements of the system. Redundancy is one technique that can be incorporated into the TMS to improve its reliability. Different redundancy techniques are detailed in Appendix G. Some of the redundancy requirements in this document are based on that information.

The redundancy of each TMS component shall be determined according to the overall system availability modelling and outcomes such as using RBD.

The analysis shall include the following factors, as a minimum, according to their importance in terms of reliability, availability and safety:

- status of hardware components
- status of software components including third party components
- status of SOE
- status of security environment
- status of interfacing systems or components
- status of transmission systems
- status of configurations.

When the redundant side becomes the active side, all components of the new active side shall be in a state so that safe, efficient and reliable signalling and train operations are ensured. This shall include the component's configuration, integrity and staleness of the dynamic information. If this cannot be achieved, then the situation shall be presented to the maintenance personnel for a solution. The component shall not operate signals and trains until its operation can be performed safely and reliably.

The TMS and all of its components shall be free from common cause failures, supported with technical evidence. If there is a common cause failure, it shall be mitigated, and RAMS analysis as well as operational and maintenance impact assessments conducted.

The use of disaster recovery sites as redundant systems for the main sites, or vice versa, shall be justified with evidence-based analysis.

14.1 Main management systems

The default redundancy configuration for main management systems shall be 'hot standby' (see Appendix G). Other proposed configurations shall be justified with supporting evidence, including common cause failures analysis and RAM analysis.

Note: Systems can be implemented on servers with various configurations. One server can host more than one system or one system can compromise more than one server.

For redundant system configurations, the synchronisation process shall not impact the system performances. It shall be performed automatically and on demand. When the TMS detects any synchronisation issue, it shall assess the impact on safe and reliable signalling and train operations. Maintenance personnel shall be informed of this issue.

The changeover process shall be seamless and automatic if the redundancy configuration is different from ‘hot standby’. That is, the safe, efficient and reliable signalling and train operations shall not be disrupted from the user’s point of view.

14.2 Workstations

The default redundancy configuration for workstations shall be ‘spare workstation’ (see Appendix G). Other configurations proposed shall be justified with supporting evidence, including common cause failures analysis and RAM analysis.

The total number of spare workstations, at a minimum, shall be 1 + 20% of the total number of workstations located at each operational site. Any deviation to these spare workstation numbers shall be justified according to evidence-based RAM analysis.

A spare workstation shall become completely operational, controlling a workstation for safe, reliable and efficient signalling and train operations in less than two minutes 95% of the time, over a period of the rolling year. This excludes the user’s movement between two workstations, though this period shall be a part of the availability calculation.

If a workstation is configured as a redundant workstation (see Appendix G), then it shall become completely available for safe and reliable signalling and train operations in less than 30 seconds 95% of the time, over a period of the rolling year.

Availability of enabling systems such as voice communications at the spare workstation shall be taken into account to avoid any impact on safe, reliable and efficient signalling and train operations.

When an active workstation fails:

- any unfinished operations on the failed workstation shall not be completed automatically
- the automatic operation that enables the train movements, such as ARS controlled on the failed workstation, shall be disabled.

When the spare workstation is activated and logged on by the user:

- it shall automatically configure according to the user’s latest configuration, as detailed in Section 19
- all incomplete operations shall be discarded.

14.3 Other systems

The redundancy configuration of systems other than workstations and main management systems shall support the functional and non-functional requirements of the TMS. Their redundancy configuration shall be equal to or better than the interfaced systems' redundancy configuration. For example, the hot-standard system should have diverse transmission systems, as specified in TS 05377. Otherwise, the proposed configurations shall be justified with supporting evidence, including common cause failures analysis.

15 Disaster recovery requirements

The redundant TMS configuration can handle most failures and problems smoothly. However, it cannot handle larger problems or disasters, such as fire, malicious attacks and natural disasters. These can affect both the main and redundant components. In such an event, it can take longer to put the system into a safe and reliable operational state at the original location. The disaster recovery configuration and supporting processes can reduce a non-operational period to a more manageable one.

Disaster recovery sites should be located at alternative locations to the main site and be configured in different ways, as shown in Appendix H.

The failed main site shall become the new 'disaster recovery site' when it becomes functional and certified for safe and reliable signalling and train operations after a disaster. Therefore, all disaster recovery requirements and functionalities shall apply to both the disaster recovery and main systems.

Each site shall have its own redundancy arrangement as detailed in Section 14. The components located at disaster recovery sites shall not be used as redundant components by the main site, or vice versa.

The default disaster recovery configuration shall be 'mirrored disaster recovery'. Both the main site and disaster site shall synchronise their dynamic information automatically, including restrictions, axle counter statuses and worksite protections. If such a mechanism is absent, another mechanism that is tested and proven shall be put in place.

Supporting systems and field systems that are not located at the main and disaster sites shall have connections to those sites, without requiring configuration changes such as patching, or modifying the data configuration. If they are located only at the main site or disaster recovery site, their availability after the disaster shall be assessed.

An automatic mechanism shall be present to detect the differences between the main site configuration and disaster site configuration, including as a minimum:

- site specific configuration data, excluding system configuration data such as IP addresses
- application software versions

- dynamic configuration data, such as restrictions.

The two sites shall maintain identical configuration, preferably through automation. If there are differences between them, the disaster recovery site shall not take over automatically without an acknowledgement of those differences by a user with adequate privileges and knowledge.

15.1 Testing and performance

The site shall not be used for any signalling or train operations until it is certified for safe and reliable signalling and train operations. The time period between disasters, that activate the disaster recovery site and the site used for signalling or train operations, shall not be counted as 'down time' for the availability calculation. This period shall not exceed the minimum time between two peak periods.

The system shall be configured so that the disaster recovery configuration can be tested regularly, without impacting on safe and reliable signalling and train operations or performance requirements. When the disaster recovery systems and main systems are operational at the same time, then the TMS shall not provide unsafe, duplicated, conflicted, incorrect or stale information to supporting systems and field systems.

All performance requirements including RAM requirements shall be fulfilled within the disaster recovery configuration. If this is not possible, all shortcomings shall be identified and justified and adequate controls such as processes and procedures put in place.

16 Interface requirements

The TMS interfaces with the following systems:

- Interlocking systems – these systems are safety signalling equipment and have built-in capabilities to communicate directly with the TMS. TS 05260 covers this interface.
- Telemetry systems – these systems provide an interface between the TMS and the safety signalling equipment, which do not have the capability to communicate directly with the TMS. TS 05260 covers this interface.
- Time servers – these servers synchronise all components of the TMS to a common time, in line with the TfNSW time system, as detailed in Section 16.4.
- Another TMS – more than one TMS can be present within the TfNSW environment, from different suppliers. They are covered in the following documents:
    - TS 05262 for serial interfaces, which require AMB permission to use
    - TS 05261 for interfaces between control systems
    - ETCS L2 for boundary interfaces as detailed in Section 16.3.1.

- Web systems – these systems interface with less secure systems such as passenger information systems. TS 05261 covers this interface.
- Timetable systems.
- Long-term storage systems.

  Note: Occasionally new interfaces are developed and covered by international standards. In that case, further details may be available from the AMB.

The TMS should interface with the following systems, when they are available for safe, reliable and efficient signalling and train operations and distribute to other systems for their operations:

- power management systems
- safety and infrastructure management systems
- communication systems
- customer-related systems
- condition monitoring systems
- asset monitoring systems.

16.1 Interface performance

Interface and its performance requirements to all connected systems shall be developed and risks identified. Based on the identified failure modes of the interface, a safety analysis shall be conducted and proper controls implemented.

All TMS communications that take place through the transmission systems shall comply with the requirements of TS 05377.

To integrate the requirements of transmission systems, including their categorisation as detailed in TS 05377, each protocol used by the TMS shall determine the following:

- safety functions performed using the protocols
- failure criteria
- protocol parameters and characteristics
- all threats and protocol defences
- use of redundant transmission system configuration with similar or better redundancy and diversity than the connected systems
- other performance requirements of the transmission systems according to protocol and seamless changeover requirements included in Section 14 and Section 15.

Interfaces to safety signalling systems shall be analysed as part of the system safety assessment.

If the interface is based on serial communication, then the serial communication shall be converted to IP-based communication to implement disaster recovery functionalities. If this is not possible, the consequences shall be analysed and mitigated.

To implement the disaster recovery functionalities, all interfaces shall be available at the main site and disaster site. They shall be designed to fulfil the performance requirements in Section 15.

The TMS shall use the identical name and naming conventions used for assets and systems within the TfNSW environment.

Each interface shall comply with the requirements in TS 05258, unless specified differently in this document, which takes precedence. If any interface requirement is not included either in this document or TS 05258, then the relevant Australian and international standards shall apply.

Cybersecurity requirements concerning interfaces with other systems are detailed in Section 17.4.1.

16.2 Telemetry and interlocking systems

Interfaces to telemetry and interlocking systems include the protocols and digital input received or digital output sent to the field systems, as shown in Figure 1. While analogue input and output are not covered in this document, they can be used for future functionalities.

All telemetry and interlocking interfaces shall comply with the requirements in TS 05257 unless they differ to requirements in this document, which take precedence.

16.2.1 Performance

The TMS shall have real-time systems characteristics, which respond to externally generated inputs within a finite and specified period as follows:

- After the TMS detects the change of field indication at the telemetry or interlocking interface boundary, the display shall accurately reflect the signalling asset status within two seconds, for 99% of all signalling asset status updates within the period of a rolling year.
- For display elements derived from field indications, the time lag for updating the displays shall accurately be less than 2.5 seconds, for 99% of all affected item updates within the period of a rolling year. This shall apply to a display element directly derived from field indications, such as stepping train descriptions and raising alarms. It shall also apply to the time allowed for processing field indications to produce updated status information on screen, such as predicted train running conditions.
- Transient events shorter than a predetermined period shall be identified for each display element and shall not be indicated to the user. The default period shall be 0.2 seconds.

- After a command is issued, the TMS shall issue the first control at the telemetry or interlocking interface boundary within two seconds, for 99% of the time within the period of a rolling year. A command such as setting a route can be initiated by the user using a workstation, or automatically by the TMS such as with ARS.
- Delays shall include delays in transmission systems as well as encryption and changeovers. That is, delays shall be validated end-to-end, not for individual components.
- The TMS shall handle incompatible performance and interface characteristics of adjacent field systems to provide consistent operations and interfaces, such as delays and response times.
- TMS shall interface to adjacent interlockings to handle boundary conditions if required.

16.2.2 Protocols

The TMS shall implement all protocols detailed in TS 05260, including identifying and implementing all deviations and configurations. Interlocking or telemetry systems can use only a subset of the specified protocols.

Note: Some protocols may be subject to intellectual property.

All protocols shall be assessed using TS 05377. All required defences shall be in place.

16.2.3 Interfaces

The TMS shall interface with interlocking and telemetry systems as detailed in TS 05260.

16.2.4 Indications

The asset indication requirements and health indication requirements shall apply for digital indications.

16.2.4.1 Asset indication

Different field systems can provide different indications and status for the same asset type, for example:

- different sets of indication bits
- different indication states, such as high or low
- a combination of indications to make asset state.

The TMS shall handle different sets of indications for the same asset type so each asset type or other system components are presented to the user as a unified asset type. The TMS shall handle all indications set out in TS 05260.

Note: Sometimes new indications may be added to TS 05260, that the TMS must be able to handle to interface and integrate with more systems in the future.

The TMS shall receive individual indications and groups of indications from the field systems in the fastest way, depending on the protocol allowed. This shall be supported with evidence-based analysis of the usage of each protocol.

The TMS shall not load the telemetry and interlocking systems with unnecessary processing. Where possible, processing shall be done within the TMS to determine the actual asset state based on the indications.

The TMS shall detect integrity issues with the field system in less than 20 seconds. If the protocol allows silent periods, then the TMS shall be able to send ‘heartbeat’ messages based on the protocol capabilities, such as requesting changed indications.

Indications detailed in TS 05260 shall be determined according to the outcomes of the HFI assessment.

Appendix A provides examples of indications used in TfNSW.

16.2.4.2 Health indication

The TMS shall use any health bit information indications the field systems provide for the integrity of the associated asset indications. The following indications can provided, as a minimum:

- dedicated indications that do not change its state and are usually connected directly to voltage supply
- equipment status indications provided for the subsystems of field systems, usually generated by the server based on its internal processes.

If the field system is configured as a redundant system, then the TMS shall handle the health bit within the redundant configuration. For example, if the health indication at one side of the field system indicates an integrity issue has been detected but the corresponding health bit at the redundant side indicates otherwise, then the TMS shall use the redundant side’s indications to determine the asset status. If both sides of the field system have integrity issues for the same assets, then the TMS shall assume that the preconfigured signalling assets have lost their integrity.

The TMS shall have the capability to configure the health indication that affects the integrity of signalling assets.

16.2.5 Controls

Different field systems may provide different controls for the same asset type, for example:

- different sets of control bits

- control states like high or low.

The TMS shall handle different sets of controls for the same asset type so the user is presented with each asset type or other system components as a unified asset type. The TMS shall handle all controls specified in TS 05260.

Note: Sometimes other controls may be added to TS 05260 that the TMS must be able to handle, to interface and integrate with more systems in the future.

The TMS shall handle the following types of controls as a minimum:

- steady ON – initial state shall be turned ON
- steady OFF – initial state shall be turned OFF
- pulse ON – steady state output shall be turned OFF. When the control is sent, it shall be turned ON for the configured period of time. It shall then be turned OFF
- pulse OFF – steady state output shall be turned ON. When the control is sent, it shall be turned OFF for the configured period of time. It shall then be turned ON.

16.2.5.1 Pacing and asserting controls

The TMS shall pace controls so there is a minimum period of time between sending controls. The TMS shall configure the pace for each interlocking and assets, such as route controls.

The TMS shall not continuously assert control on the interface to the signalling safety system. All exceptions shall be identified. A risk analysis shall be completed.

If the field system has redundant configuration, then the TMS shall deliver control to one side or both sides of the field system, depending on the requirements of the field system.

TMS shall not send control to the interface of the signalling safety system in the following situations as a minimum:

- the function is not available, except when required to test the operation of the signalling safety system
- the asset is already in the selected state, with the exception of controls to place the asset in its safest state
- the asset is blocked
- the asset is locked by the train movement
- the control can create a hazard
- there is a loss of signalling integrity, with the exception of controls to place the asset in its safest state.

16.2.5.2 Unnecessary or incorrect controls

The TMS shall not send spurious, unnecessary or incorrect controls in the following instances, as a minimum:

- normal system operation
- system start-up or shutdown
- failure conditions, including hardware, software or communication failures
- changeover process
- configuration changes.

16.2.5.3 Unsent controls and user privilege

The TMS shall discard all unsent controls when it detects that integrity with the signalling assets is compromised. If the redundant TMS maintains the integrity, then it can deliver those unsent controls when it becomes the active side.

The user with adequate privilege level shall be able to perform the signal control functions detailed in TS 05260.

Appendix B provides examples of controls used in TfNSW.

16.2.6 Test mode

The TMS shall have a test mode that allows all controls to be passed to the field systems without any integrity or availability checking, so that the signalling safety system can be tested.

Entry to the test mode shall be protected against unauthorised use. This shall be determined during the HFI assessment. If the TMS is in the test mode, it shall be clearly indicated to the user based on the outcomes of the HFI assessment.

16.3 Other systems

The TMS shall be capable of exchanging the following information with other systems or with an adjacent TMS at the fringe or boundary areas:

- train information such as cancelled or restored trips, train locations, train path or route sets, estimated arrival and departure times, and expected order of arrival or departure
- signalling asset status
- other conditions required to control the signalling assets at the boundary including restrictions and worksite protections.

  Note: Occasionally new interfaces are developed and covered by international standards. In that case, further details may be available from the AMB.

The interface between the TMS and other systems shall provide the following functionalities, as a minimum:

- inputs to each other so that functions of each system such as ARS shall perform as specified
- inputs to each other so that they shall not:
    - create a new hazard or modify an existing hazard
    - impact on a signaller's situational awareness or on safety and operation related decisions.

16.3.1 ETCS L2 interfaces

While this document does not cover requirements for ETCS L2 systems, the TMS shall have interfaces to other systems with ETCS L2 capabilities. ETCS L2 systems use marker boards instead of conventional signals. This may create a risk when marker boards and line side signalling need to be indicated on the same display, such as at the boundary between these systems. Confusion may arise in communication between signallers, drivers and workers on-track. For example, if a signaller gives a 'signal' as a reference point when it is actually a virtual marker board.

The TMS shall be able to show the following ETCS L2 modes:

- full supervision
- onsite supervision
- unfitted.

16.3.1.1 ETCS assets

The TMS shall distinguish between ETCS assets such as marker boards and equivalent line side signalling assets, including when display features such as asset names have been turned off.

ETCS L2 may have two different marker boards:

- virtual
- physical.

The TMS shall distinguish between virtual marker boards and physical marker boards.

The movement authority mode such as full supervision or onsite supervision does not need to be distinguishable from route types, as long as the signaller can identify the type from a protecting signal or marker board.

16.4 Time synchronisation

The TMS is a distributed system as shown in Figure 1. To facilitate an investigation process, all time-related activities and recording of events at different sources should be accurately synchronised.

The TMS shall comply with the requirements in TS 06208 as well as the following requirements:

- All equipment within the TMS shall be synchronised with specified stratum time servers using the network time protocol specified in RFC 5905. The TMS shall connect to other time servers to allow redundancy, if the current time server becomes unavailable or unreliable according to the network time protocol specification. All interfaced systems including transmission systems should be synchronised to the same time source – to present cohesive and easily traceable information.
- If there is a failure to connect to the server at any time, the TMS shall synchronise the time internally so that all TMS components are synchronised until an external time server becomes available. This shall be presented as an alarm and logged.
- If there are any issues with time synchronisation or daylight saving time, the maintainers shall be notified in line with the outcomes of the HFI assessment.
- The TMS shall handle the daylight saving time automatically. If this mechanism has a problem, then the TMS shall adjust the daylight saving time manually on all of its components without impacting on operations.
- Time information in all TMS components shall have an accuracy of +/- one millisecond and a precision to one millisecond.

Any departure from these requirements, such as equipment incapable of synchronising time, shall be supported with evidence-based analysis. The analysis shall include the impact of any non-compliance on the logging, reporting, incident and fault management of the TMS as a whole.

17 System configuration

A system can be designed and implemented in a number of ways. It can also consist of various hardware components such as servers, workstations and networking equipment as shown in Figure 1.

17.1 Hardware

All equipment used within the TMS shall fulfil the requirements of TS 05258 unless specified differently in this document, which takes precedence. If any equipment requirement is not covered in either this document or TS 05258, then the relevant Australian and international standards shall apply.

To encourage innovation, this document provides only performance requirements and recommended configuration for a TMS.

The following performance requirements apply to TMS equipment:

- The number of servers shall be kept to a minimum where possible by using appropriate technical solutions, such as virtual machines. Other emerging technologies such as cloud hosting or storage may be used, if safety, security and non-functional requirements are met and supported by evidence.
- The workstations shall be able to support the outcomes of the HFI assessment, for example by incorporating touch screen technology or a stylus.
- If any TMS component is remote-controlled, performance, functionality and security assessments shall be done. All differences against equivalent local control configurations shall be identified, analysed, mitigated and accepted by the asset custodian and asset operator.
- The system equipment including cabling shall not cause losses of quality, performance or function for other equipment operating within the TfNSW network electromagnetic environment.
- The system equipment, including cabling, shall operate without degradation of quality, performance or loss of function within the TfNSW network electromagnetic environment.
- The system components shall be able to perform a self-test and provide diagnostic facilities. These functions shall be part of the maintenance tool as detailed in Section 18.1.
- Systems components and applications running on them shall be organised so that safety-related and real-time functions are not affected by other functions.
- Operating systems and third-party software including firmware shall be sourced from reputable suppliers as detailed in AS ISO/IEC 25051.

  Note: Open-source products should be preferred.

Equipment rooms and cubicles shall fulfil the requirements of TS 03947.

Scalability and spare capacity shall be considered as part of the life cycle of the TMS, such as staging. Overall configuration of the TMS shall have the following spare capacities, as a minimum, beyond normal operations or exceptional situations:

- 20% performance reserve
- 10% expansion of assets coverage.

17.2 Upgrades

17.2.1 Configuration changes

The TMS shall allow the following configuration changes, as a minimum, without impacting the system availability requirements:

- hardware upgrades
- SOE upgrades
- software upgrades, including third party components.
- site data configuration changes
- design changes, including scaling
- cyclic updates
- security updates
- interface changes.

17.2.2 Integrity, safety and reliability

During the upgrades, the integrity of the TMS including the main site, the disaster recovery site and the supporting systems, shall not be compromised.

When required, the rollback operation shall be available to restore the system to its previous configuration without losing its integrity. The synchronisation between the system components shall not be affected due to configuration differences.

The safety and reliability of signalling and train operations may be affected during software updates and upgrades to SOE and site data configuration, impacting on the availability of the TMS. The design of the TMS should therefore incorporate automated upgrade operations. If automation is not possible, manual procedures, interventions or operations should be minimised and optimised.

The TMS shall be able to identify the differences between the approved site configuration and actual site configuration. This capability shall be activated automatically when:

- an application is restarted
- an upgrade is completed.

The user who has adequate privileges shall be able to check the site configuration any time without affecting the TMS operations or performances. Unauthorised configuration modification should be detected automatically to support the integrity requirements.

The TMS shall check and present the following configuration items as a minimum:

- hardware and SOE versions, including firmware
- software versions
- interface versions
- site and system configuration versions.

If the TMS detects any differences in configuration, at least one of the following actions shall be taken:

- The application or system shall be terminated according to the outcome of the risk-based assessments.
- The TMS shall not perform any operation and the user will be notified to resolve
- The system shall provide a means of continuing its operation with a configuration deviation, after a user with the privilege to make such a decision acknowledges the deviation.

Any TMS component shall be able to be constructed from the bare metal configuration to a complete and up-to-date working state in the minimum time between two peak periods, which is five hours for competent personnel.

17.3 Backup

The TMS shall restore any TMS components to the previous or currently approved configuration if either of the following occurs:

- roll back to the previous version during the upgrades
- set up of a new component, after failure or cyber-attack or disaster or renewal.

The content of the backup shall be determined so that the TMS component is functional, as specified in Section 17.2.2.

To fulfil reliability and availability requirements, the TMS shall perform regular backup operations without impacting the safe and reliable signalling and train operations. Backup operations should be incremental, such as backing up only changed information since the last backup operation occurred. The backed-up information shall be stored at a physically different, safe and secure location.

If the restore functionality is not available in the TMS, then an approved and tested restore process shall be provided and supported with evidence-based analysis, including the impact on RAM requirements.

17.4 Security

The TMS shall be able to provide security against physical, personnel and cyber threats. A risk-based analysis shall be performed to prevent, detect and respond to any vulnerabilities and threats to the TMS, as required by TS 04992.

Other security provisions applicable to a TMS operating within the TfNSW environment are contained in relevant NSW legislation and NSW Government directives.

17.4.1 Cyber security

The TMS shall comply with all requirements detailed in CLC/TS 50701, which is based on IEC 62443 (all parts) and IEC 62425.

The TMS shall also comply with the following cyber security standards:

- TS 04990
- TS 04991
- TS 04993
- TS 00031.1
- TS 06305.

  Note: Requirements in TS 05377 complement the above list of standards at the protocol level, including the use of conduits specified in TS 04990.

18 Supporting tools requirements

The TMS can provide a number of supporting tools to fulfil its RAM requirements, however, this document sets out requirements only for maintenance and offline configuration tools.

The TMS shall handle a number of tools concurrently, as specified in Sections 18.1 and 18.2, without impacting the performance and functions of the TMS.

The tools shall be configured to run on different electronic devices such as tablets, laptops and personal computers, with a single screen or multiple screens. The tools shall be capable of running securely and safely at local and remote sites as specified in Section 17.4.

The number of local and supporting tools that can run concurrently shall be determined by the HFI assessment. The TMS shall support the outcome without any impact on its performance.

18.1 Maintenance tool requirements

The maintenance tool shall provide general and detailed views of the status of TMS components. This will enable it to monitor their status in real time and identify and locate issues as quickly and accurately as possible when an incident occurs.

HFI and security assessments shall be carried out to identify the TMS components to be presented to the maintainers.

These include as a minimum:

- servers, workstations and their components
- supporting equipment such as routers, switches and power supplies
- telecommunication infrastructure
- condition monitoring
- communication status between interfaces and, if applicable, between applications or equipment
- software components.

18.1.1 Tool functions

Information provided by the tool shall be able to identify and locate issues within the system with high accuracy. A graphical presentation method shall be the primary choice.

All status changes shall be presented on the tool after the event occurs in less than 10 seconds, 99% of the time over a period of the rolling year.

The HFI assessment shall determine the following aspects of the maintenance tool, as a minimum:

- the number of layers presented in the system, such as overview, communication, interfaces and subsystems
- navigation between layers
- details to be provided, including shapes, texts, colours, locations and positions
- statistical information, such as communication statistics, running time and resource usage
- the current status of components, including RAM figures and diagnostic and self-test results
- assistance for maintainers to perform their preventative maintenance works such as reminders of regular activities
- assistance for maintainers to perform predictive maintenance work by identifying potential failures based on the performance of the assets
- static configuration details of components such as version numbers, models and maintenance requirements
- dynamic configuration details such as active timetables and active users
- alarms that provide:

  - navigation between an alarm and a component, with the alarm having a list that goes directly to the layer containing the component source of the alarm
  - a list of alarms for selected system components including the TMS and equipment alarms, listed when that component is selected
- logs related to the selected system components including the TMS and equipment logs
- produce, save and print reports related to issues

The maintenance tool shall also provide the functionality to configure the system for maintenance and incident management purposes. Depending on the safety assessment outcome, it shall deliver the following functions as a minimum:

- selection of any side of redundant system as the active side, temporarily or permanently
- activation of the disaster recovery site
- resetting statistical information
- selection of a redundant communication path between applications as the active path, temporarily or permanently
- performing diagnostic or self-test functions remotely on components or systems
- remote access to the condition monitoring systems
- synchronisation of redundant sides at the main site and the disaster recovery site
- time synchronisation or other time-related operations.

The maintenance tool shall prevent multiple users from performing the same function on the same asset at the same time.

For a comprehensive maintenance tool, the following functions should also be available:

- TMS configuration updating, particularly for site configuration data, as detailed in Section 17.2
- TMS configuration checking functionality, outlined in Section 17.2
- back up functionality as detailed in Section 17.3.

18.2 Offline configuration tool requirements

The TMS is likely to be configured a number of times during its lifetime due to expansion or modification of the rail infrastructure. The TMS should provide an offline tool to perform the data configuration task efficiently, checking the integrity of the data to prevent errors. Personnel who require no specific knowledge of the TMS configuration without compromising quality should perform this task.

The TMS shall provide a tool capable of creating, viewing and modifying the following items offline as a minimum:

- site specific configuration
- simulation configuration
- TMS SOE configuration and patches
- security patches
- user management configuration.

Graphical presentation shall be used for configuration data presentation and entry instead of tabulation method. The use of tabulation shall be supported with evidence-based analysis.

The configuration data shall have enough metadata to identify its version and status when they are not in version control, for example, after the configuration is deployed to a site.

To encourage innovation, this document does not provide site specific infrastructure information the offline tool will use to create the TMS data configuration.

The configuration tool shall not run on the active TMS, and will not modify any configuration on the active TMS.

18.2.1 Tool functions

The offline configuration tool shall have the following functions as a minimum:

- creating and viewing:
    - business rules
    - individual display objects or items, including shape, colour, text and behaviour
    - complete display, design or modification capabilities such as maps and maintenance display
    - information entry interfaces and business rules
    - default information
    - layers, zooming
    - relationship between objects and items
    - user configuration including types and privileges
    - interface characteristics including communication protocols and failure definitions
- using previously verified or deployed configuration datasets, which can be in different formats such as spreadsheets or databases

- extracting or extrapolating configuration data required for TMS from previously provided configuration datasets, for example, conflict detection data from the topology configuration
- updating the complete configuration dataset according to new or updated data
- verifying configuration data for:
    - its integrity, based on set, approved and tested rules
    - compliance to set business rules
    - allowed boundaries, values and types
    - consistency, removing any contradictions with other relevant data within the configuration dataset
    - correctness.

18.2.2 HFI assessment

The following aspects, as a minimum, shall be analysed during the HFI assessment of the offline configuration tool:

- making data entry and production processes as automatic as possible
- when manual entry is required:
    - using graphical presentation when possible to select objects
    - providing context-based predictive inputs to the user for selection if alphanumeric data is required
    - verifying immediately for correctness and integrity within the configuration dataset.

18.2.3 Version control

The offline configuration tool shall handle version control mechanisms, including managing multiple versions of the configuration dataset for updating at the same time. If this function is not available as part of the configuration tool, then the tool shall be able to interface with another tool to manage the version control.

The version control shall have the following functions as a minimum:

- create and extract baselines
- create a branch from any baseline and maintain independently from other branches, including the main branch
- merge branches to the main branch
- find and list differences between different versions under development, including differences with the current configuration.

19 User management requirements

The TMS can be a large system accessed by different users performing tasks at varying levels of responsibilities and accountabilities.

The user management system provides the structure for users at different levels based on competencies, responsibilities and accountabilities. It also supports the overall system level security arrangement and prevents unauthorised access.

The signaller can control the signals and trains in two different configurations, such as area of control and line control. Area of control is based on interlocking boundaries and includes all lines within the controlled area. Line control is based on controlling a line from beginning to end. Two lines running in parallel can be controlled by two different signallers.

The TMS should be able to handle both types of operation at the same time or switch between them, depending on the operational requirements.

Only users with sufficient permissions shall be able to perform TMS functionalities remotely.

User management shall be part of the security assessment covered in Section 17.4.

Although a username and password mechanism is a requirement of this document, other forms of user identification may be considered with supporting evidence-based analysis, explained in Section 7.

The login process shall not have any limitation for unsuccessful failure attempts. However, a mechanism shall be present to alert to any potential security issue. All user management transactions shall be logged, including unsuccessful attempts.

If the user has not used the workstation or equipment for more than a set period of time, determined by TfNSW's security policy, then it shall automatically lock. This policy may not apply to systems that need to be continuously on, such as a signaller's workstation. A HFI assessment and a security assessment shall decide whether a workstation should lock automatically or not.

When the user logs in again, the display shall be presented without losing its integrity or changing presentation parameters.

19.1 User domains

The following two types of user domains shall be available. They shall be independent of each other:

- operational users, for example, for signalling and train management or supporting functions such as maintenance purposes
- system users for TMS configuration management or login to TMS equipment, for example, servers and workstations for infrastructure maintenance or configuration purposes

Operational users shall perform operations according to the allocated privileges detailed in Section 19.1.1.

The TMS shall provide integrity for the allocation of privileges and allocated privileges. User management information, including usernames and passwords, shall be protected and accessed as specified in IEC 62443 (all parts).

Based on the HFI assessment findings, each user domain shall have different user profiles with varying privilege and operation levels based on their competency, responsibility and accountability.

The number of user types and users created shall be unlimited.

System users shall not be able to access or perform any TMS operations. Operational users shall not be able to access or perform any TMS system functions.

19.1.1 Operational users

The complete log-in or log-out process shall not exceed 30 seconds, 99% of the time over a period of a rolling year.

Each user shall have an allocated storage space within the system's storage structure. This allocated space shall not be accessible by other users, for example, through reporting functionalities. The default configuration shall be set to 'no access to removable storage devices'. However, based on the security assessments, the TMS shall allow access to removable storage devices when required.

Each user shall be able to create and modify a profile for the following configurations as a minimum:

- display configuration
- coverage and control configurations, such as default and latest
- default storage location
- report configurations
- other personnel preferences.

All users shall have access to the following common functionalities:

- view selected display
- report without content modification privilege, such as modification of attached notes.

However, if the user has a higher level of privileges for a function, the lower level privileges for the function shall be overridden.

19.1.1.1 Generic user profiles

The following generic user profiles shall be created for the TMS, as a minimum:

- signaller
  - control the signalling assets
  - manage controlled area or line
  - manage rail traffic and train movement
  - manage restrictions and worksite protections
  - manage alarms allocated for signallers
  - perform axle counter reset operation
  - undertake incident management
  - set test mode as detailed in Section 16.2.6, which requires additional protection such as a password
- maintainer
  - view some part or overall system
  - manage alarms allocated for maintainers
  - perform maintenance activities
  - undertake condition monitoring
  - undertake performance monitoring
  - manage maintenance tools
- supervisor
  - user management
  - undertake condition monitoring
  - undertake performance monitoring
  - provide reporting with modification privileges
- infrastructure manager
  - manage restrictions and worksite protections
  - undertake performance monitoring
  - manage maintenance tools
  - provide reporting with modification privileges
- training supervisor

- undertake simulations
- perform scenario creation and testing

- configuration manager
  - manage configuration tool
  - manage simulator
  - perform scenario creation and testing.

A ‘guest’ user profile shall be created. This user profile shall only have the common functionalities outlined above.

19.1.2 System users

System users shall be able to access the TMS equipment or infrastructure for the following purposes, as a minimum:

- upgrades or modifications to software, firmware and configuration
- performing system level maintenance.

Access to the TMS component shall be enabled after successful login and password processes. Various levels of access privileges shall be available and assigned to system users according to their competencies and responsibilities.

19.2 Controllable object coverage

A user-controlled object can be modified due to incident management or work conditions, such as broader coverage for off-peak operations. The object can be an area, a line or an asset, or a combination of all.

Each controllable asset shall be controlled by only one signaller. All controllable assets shall be under control all the time. The TMS shall provide dynamic configuration of a controlled object without modifying the TMS configuration.

19.2.1 Handover process for controlled objects

When the control of an object is shifted from one user to another, a process shall be followed to handover the requested area. This handover process shall be determined by the outcomes of a HFI assessment, and observe the following requirements:

- The transfer shall not be performed if the user of the requested object declines the requests in a predetermined period.
- If the request is accepted by the original user or the predetermined time period has expired, then the transfer shall be initiated.

- After the request is granted, the user requesting the transfer shall acknowledge the handover report as detailed in Section 19.3. If this process is not completed within three minutes, the transfer operation shall be aborted and control returned to the original user.

19.2.2 Scenarios for controlled objects

The TMS shall handle the following types of scenarios for controlled objects, as a minimum:

- The requested object is not controlled – the handover report shall be presented immediately for the requested object. The user shall be able to control the object as soon as the handover report is acknowledged.
- Part of the requested object is controlled by another user and the rest of the object is not controlled – the handover process for the controlled object shall be initiated. The uncontrolled objects shall be allocated to the requested user immediately, as detailed in Section 19.2.1.
- Part of the requested object is controlled by more than one user and the rest of the object is not controlled – the handover process shall be initiated for each controlled object at the same time. One handover report is preferred for all controlled objects. The uncontrolled object shall be allocated to the requested user immediately, in line with Section 19.2.1.

19.2.2.1 User controls

The TMS shall detect whether all controllable objects are allocated to one of the current users. When the TMS detects an object is not controlled by a signaller, or is controlled by more than one signaller, it shall be reported to all other users to resolve so that only one user controls a controllable object.

If a signaller has logged off successfully earlier, the TMS shall provide an option to the signaller to use the last used configuration, as a minimum, after they log on to a workstation successfully. If there is no such configuration, then the default configuration shall be provided.

Signallers who have already logged on to a workstation successfully, shall be able to log on to another workstation if the original workstation malfunctions. When this happens, the following actions shall be taken:

- The new workstation shall be logged in and the display shall be presented exactly as the last screen configuration of the original workstation.
- If the original workstation is not functioning, then the new screen configuration shall be the same as the last screen configuration before the workstation became non-functional.
- All incomplete information entry process, commands or controls shall be discarded.
- The original workstation shall be logged off automatically when the login process on the other workstation is successful.

The acknowledgement process shall only be required if the requested object is different from the original login profile. If any workstation is logged on by a signaller, another signaller shall not be able to log into that same workstation until the original user logs out.

19.3 Handover report

When the signaller obtains control of an area, a line or an object, a report shall be generated automatically for that area, line or object in control.

The report shall contain the following information, as a minimum:

- current alarms
- current safety functions, such as restrictions and worksite protections
- outstanding axle counter reset operations
- trains within the requested control area or line
- any notes created in logs by the previous signaller for the requested area, line or objects.

The report shall also contain other information such as time, signaller details or workstation selection essential for future analysis. The operator shall acknowledge the report so as to obtain control of the selected area or line or object. This report shall be logged in its entirety for future use.

19.4 Remote access

The TMS shall provide the requested information remotely to the user according to the user credentials, as long as all the requirements in Section 17.4 are met.

The human interface at the remote site shall be identical to the local human interface as detailed in Section 20. If there is a deviation, a HFI assessment shall be carried out to identify and mitigate the deviations.

The HFI assessment shall identify which user configuration will have remote access capabilities. However, the following users shall also have the minimum remote access capabilities:

- maintainers
- supervisors
- infrastructure managers.

20 Human interface

The human interface requirements in this document are general and should undergo the HFI process.

This document covers some of the input and performance requirements that need to be addressed during the HFI process.

HFI should cover all types of workstations including overview, remote, offline or web-based workstations.

If the requirements in this section cannot be fully implemented, or met temporarily with staged signalling commissioning, they can be implemented on completion of the project or work. Rather than apply for a concession as detailed in TS 00003, the asset steward delivery or designated TAO shall perform the following, before completing the design phase set out in TS 01471 and TS 00096:

- Site and application-specific hazard analysis, based on the proposed planning and staging requirements, to identify new hazards and controls and ensure existing hazards and controls are intact.
- Identification of the best possible means of meeting this document's requirements based on the whole asset life cycle and cost analysis.
- Stakeholder identification, consultation and agreement involving the maintenance and operation branches of the RIM.
- Production of artefacts for all of the above activities.

  Note: The above process is also applicable for changes which may not be presented on the workstations.

20.1 Zoom and pan requirements

The zoom and pan function is used where the display cannot provide enough details. This function helps to view the selected area in a detailed manner so the user can handle the issue more effectively and efficiently. At the same time, the user may lose situational awareness for the area they should be controlling.

The HFI analysis and the associated risk assessment shall be done for the zoom and pan function to address the following cases, as a minimum:

- identify and mitigate risks arising from a loss of situational awareness, such as:
  - when the zoom and pan functions are initiated successfully
  - when the zoom and pan functions are used for a period of time
  - when the operator is unaware that zoom or pan functions, or both, are active

- zoom and pan functions are not available when required
- zoom and pan functions cannot be terminated.

20.2 Workstation requirements

The following requirements are applicable to all types of workstations, unless indicated otherwise:

- All aspects of the state of the system necessary for the operators' safe and effective train management shall be explicitly, clearly and unambiguously shown.
- The system shall not introduce potential error or confusion.
- The human interfaces shall not draw the operator's attention away from other operating tasks unless necessary for the system to perform its operational and safety supervision functions.
- The characteristics of the visual and auditory alerts provided by the human interfaces shall be optimised, so they are clearly detected in the majority of operating conditions forecast to occur.
- If the user is managing safe and reliable signalling and train operations, they shall not be able to:
    - minimise applications used for signal and train management purposes
    - start any application not required for signal and train management purposes that can impact system performance, such as office tools or games
    - place other applications on top of the application used for signal and train management purposes
    - modify any configuration on the workstation that can impact the user's situational awareness, including audible and visual adjustments
    - access the operating system or any of its functions not required
    - shut down the application.
- The user shall have the following capabilities without the help of maintenance support:
    - replace the pointing device (such as a mouse) or text-entry devices (such as a keyboard) in less than 2 minutes, 95% of the time over a period of the rolling year
    - change to a redundant workstation without maintenance support, if the system has such a capability
    - transfer and use the spare workstation if required, including enabling systems such as voice communications.

- Access to portable storage devices such as USB and disks shall be prevented, if the requirements in Section 17.4.1 cannot be fulfilled.
- The workstation shall be capable of starting the required signal and train management applications automatically, when the workstation restarts after a crash or power failure.
- The current date and time shall be continuously displayed to the signaller with a resolution of one second, and updated every second.

The layout of workstations used within the TfNSW environment is provided in Appendix D.

20.3 Display requirements

The following requirements shall be applicable to all types of displays, unless indicated otherwise:

- The indication status shall display the actual state provided by the signalling safety system equipment, explicitly, clearly and unambiguously.
- The validity and integrity of the displayed objects shall be clearly presented to the user.
- Names and naming conventions shall be compatible with other signalling standards and those used within TfNSW systems, to ensure uniformity and consistency.
- Different type of assets used for the same purpose, such as track circuit and axle counter, shall be displayed and controlled in a unified manner.
- The TMS shall be able to use different sized workstations at the same time, for signalling operations, overview, and so on.
- The TMS shall be able to use different types of display technologies at the same time, such as LED, touch screen and projections.
- The TMS shall be able to manage workstations with different functionalities at the same time, such as signalling operations, maintenance, overview and management.
- The human interface shall comply with all relevant standards, including the following as a minimum:
    - AS/NZS 1680.2.2
    - AS/NZS 2107
    - AS 2700
    - ISO 9241-210
    - ISO 11064 (all parts).

- The following principles, as a minimum, shall be applied during the HFI assessment:
    - The complete area of control shall be displayed in sufficient detail for the user to be aware of what is happening in their area without the need to manipulate the system in any manner.
    - The display shall also cover the approaches to the user's area of control.
    - Approaching train track occupancy indications adjacent to the area of control for each line shall be provided, as a minimum, to include all tracks involved in the conditions of the approach locking of the first controlled signal.
    - In a departing direction, the track circuit indications shall be provided, as a minimum, for all tracks up to and including the overlap track of the last controlled signal.
- Events that require a response or action by the signaller shall be brought to the signaller's attention visually and aurally.
- The display shall be of sufficient detail so that the signaller can, with the aid of their knowledge of signalling, determine the following:
    - the exact location of trains
    - clearance points for signals
    - type and form of each signal available
    - all information that affects a route's availability if that particular route is required to be available
    - sufficient details about any failure or fault (intermittent or permanent) that has occurred so that maintenance staff can effectively respond to the situation
    - names of assets
    - names of physical locations
    - geographical relationship of rail lines
    - purpose of the locations for train running.
- Sufficient information shall be provided on trains approaching the signaller's area of control for the signaller to efficiently manage trains.
- Sufficient information shall be provided on trains departing the signallers' area of control so the signaller can be aware of when the next train will be able to depart, and when a train has completely departed their area of control.

  Note: This should include some overlap into the adjacent area of control.
- No indication, display item or event shall obstruct or mask any other indication or event, leading to a loss of situational awareness.

- Details on the screen shall be configurable by the user. For example, names of assets shall be turned on or off in some parts or all parts of the screens.
- ‘Find asset’ functionality shall be provided within different contexts, such as controlled area only, or selected area, or whole system.
- If the user needs to access more than one type of TMS, the negative transfers between different systems shall be eliminated or minimised. The following, as a minimum, shall be part of a HFI assessment with inputs and agreement of end users:
    - workstation layout
    - ways to select visual items – pointing device or touch
    - accuracy or precision required to select visual items
    - density of visual items
    - fonts and text selection
    - display dimensions of visual items, including their dynamic states
    - consistency of visual items within the system and across each TMS
    - information to be presented for each visual item type to user when it is requested
    - when and how visual item information will be presented, such as hovering over or selecting
    - consistency of controls within the system and across each TMS
- The following requirements apply to the layout of the screen:
    - Tracks shall be laid out horizontally, by default.
    - Sydney Central Station shall be on the left-hand side. The direction away from Central Station shall be on the right-hand side.
    - If multiple screens are used, then tracks shall be drawn left to right across screens, before moving down to a second line on the screen.
    - The track plan on the screen shall be presented as close as possible to the signalling plan.
    - All display items shall be of a similar scale.
    - The display shall not be required to have one geographical scale. However, the screen shall not affect the operator's performances.
    - The display shall be structured in a way that minimises information usually displayed, so that the display does not have a cluttered appearance.

Information on some of the visual items used within TfNSW is provided in Appendix A. Appendix C provides human factors examples used within TfNSW.

20.4 Control and command requirements

The following requirements shall apply to all types of controls and commands, unless indicated otherwise:

- Controls and commands shall always be available if the operator has control of all related objects.
- Each controllable object shall be controlled by only one operator.
- Controls used to return the asset to their safest state shall not be prone to accidental operation. However, they shall be fast and easy to use in both emergency and failure situations. These controls shall operate irrespective of the indicated state of the asset.
- Safety-related controls and commands shall include a confirmation process.
- The HFI analysis shall be done to address the following, as a minimum, for each control and command:
    - The operator's use of hand or arm actions to complete the controls and commands shall be kept to a minimum.
    - The time period to complete the controls and commands shall be kept to a minimum, including limiting text entries.
    - Each control or command shall be initiated in at least two different ways, such as from object or from menu item.
    - If any control or command is initiated while another command or control is underway, then the incomplete command or control shall be aborted by default. All exceptions shall be identified and risk analysis completed.
    - If a command is not valid, it shall be rejected and presented as invalid by default. All exceptions shall be identified and risk analysis completed.
    - The process to initiate and complete commands shall be in line with accepted industry practice.
    - Consistency of controls and commands within the system and across each TMS shall be maintained.
    - By default, the command or control shall not be stored. All exceptions shall be identified and risk analysis completed.
    - Context-sensitive default command and control for each command and control shall be present. For example, if a point is in the reverse position and locked, then the default command can be 'set point free'.

- The responsiveness of the system to the user shall prevent the natural actions of the user being impeded by the system, such as waiting for a response or blocking safety-related controls.
- Controls and the use of controls shall not impede the user's situational awareness.
- If a response to commands or control takes longer than five seconds, then a feedback mechanism shall be put in place.

Information on some of the controls used within TfNSW is provided in Appendix B.

20.5 Form entry requirements

The TMS shall provide an interface to enter text-based information to forms for the following purposes:

- restrictions
- worksite protections.

The layouts, source of information, information entry mechanisms and other characteristics shall be identified as part of the HFI assessment.

The following general requirements, as a minimum, apply to all form entries:

- Information entry tools shall be presented initially at the empty or less functional areas of the workstation.
- The initial size of the information entry tool shall be minimal so as not to cover any used areas on the workstation.
- The user shall be able to modify the location and size of the report.
- Information entry tools shall be able to be pinned after a one-step acknowledgement process. The entry form shall stay on the location until it is closed or minimised.
- If the information entry tool is not pinned, it shall be minimised automatically if not used within the configurable period of time, by default 30 seconds with a 10 second visible warning countdown. The signaller shall be able to extend for another 30 seconds by stopping the warning.
- A mechanism shall be used to retrieve the minimised entry tools. The mechanism shall not affect the signaller's situational awareness.

20.5.1 Automated functions

The TMS shall eliminate manual information entry as much as possible by using appropriate techniques. These include automatic filling if information is already known, drop-down menus, context-sensitive typing or selection, or automatic filling of some information when a particular option is selected.

The TMS shall allow pre-filling of the form for pre-planned operations.

The TMS shall perform the following functions automatically, preferably when any information is entered:

- checking consistency, applicability and integrity
- checking for conflict within the system.

21 Logging requirements

The TMS shall store and then extract enough details and coverage of events to fulfil the following functionalities as a minimum:

- investigations, which can be used for legal purposes
- fault analysis
- replay
- training
- verification of RAM targets.

21.1 Types of events

The TMS shall be able to log the following kinds of events, as a minimum, within 10 seconds, 95% of the time over the rolling year:

- signalling assets
- train-related
- alarms-related
- safety operation
- digital forms
- human interface-related, such as commands, controls, login, logout, transfer
- interface-related
- operational
- handover
- system
- clock adjustments.

21.2 Logging of events

Events shall be logged. Details for each event shall provide enough information to perform an investigation, or to replay and perform fault analysis functions, without requiring additional information or resources. Unusual events leading to a failure shall be captured and logged accurately.

The logging information for each event shall include the following, as a minimum:

- timestamp complying with the AS ISO 8601 format expressed as YYYY-MM-DDTHH:mm:ss.sss(Z | ([+ | -] HH:mm). It shall specify time zone offset as either UTC (represented as Z), or the offset from UTC expressed in hours and minutes, indicating positive or negative offset from UTC
- time, precision to one millisecond, accuracy within one millisecond
- source
- event type, as listed in Section 21.1
- event description
- parameters
- notes, as detailed in Section 21.3.

The order of events shall be captured within the logs.

21.2.1 Integrity of logging system

The logging system shall maintain its integrity under the following conditions as a minimum:

- any external manipulation of the logging system, such as manual manipulation and external threats
- adjustment of time and date, such as daylight saving
- accessing the same logs for reading and writing at the same time
- handling a burst of logging due to disruptions.

If the logging system cannot log events due to disruptions, then the logging system shall mark disruptions within their records. If there is a redundant log system and missed events are available at the redundant side, logs shall be merged to have complete records. If the completeness of event logs cannot be guaranteed for the given period of time, the user shall be informed of the lack of integrity when they need to access records.

21.2.2 Capabilities of logging system

The logging system shall have the capability to:

- handle and store at least 500 events per second in the steady state without any impact on TMS performances
- handle and store 5000 events per second for 300 seconds as a burst without affecting TMS performances
- handle multiple events sources
- store and extract events at the same time without any impact on TMS performances.

21.2.3 Storage and accessibility of information

The logging systems shall keep all logged events safely and securely for seven years, including those stored in external systems for long-term storage. If the long-term storage needs to be located at another site, or a remote site, then access to the site shall be automatic. The integrity between original logs and stored logs at the long-term storage shall be maintained.

> Note: *State Records Retention and Disposal Authority FA403* sets out provisions for managing records relevant to transport network operations.

Stored events shall be accessible within the following times:

- less than five seconds, 95% of the time over the rolling year for events logged for a minimum of 300 days
- less than 12 hours, 95% of the time over the rolling year for events stored at long-term storage.

The logging system shall optimise the stored information in order to reduce the amount of information to be stored or transferred, without compromising the integrity and performance requirements. Logging shall be configurable so that information that is not usable can be limited or stopped.

Commercial off-the-shelf reporting or logging products shall be able to interface with the logging system without any software and interface modifications or intellectual property agreements.

If the remote locations or cloud storage are used for the log storage, these components or zones shall be considered as ‘industrial automation and control systems’, as detailed in Section 6.3.

21.3 Notes

The logging system shall add or attach multiple notes to each log entry using the reporting functionality without losing the integrity by ensuring:

- existing entries including the previous notes shall not be altered
- if the log entry is already stored in the long-term storage it shall be updated
- if the same log entry is accessed by more than one user, only one user shall be able to manipulate the log entry
- when the log entry is updated, the updated log entry shall be made available to all users.

22 Reporting requirements

Reports shall be available to users at their workstations as an integral part of the TMS. Reports shall be used either as a standalone or integrated product for maintenance purposes at remote locations. The number of reports that run concurrently shall not be limited, unless it impacts the performance of the TMS.

Some guidelines on the reporting functions required in this document are provided in Appendix I.3.

To maintain the operator's operational awareness, the following report characteristics, as a minimum, shall be considered during the HFI assessment:

- The report shall either be presented initially in the empty or less functional areas of the workstation.
- The initial report size shall be minimal or hidden, so as not to cover any used areas on the workstation.
- The user shall be able to modify the location and size of the report.
- The report shall be able to be pinned after a one-step acknowledgement process. The report shall stay on the location until it is closed or minimised.
- If the report is not pinned, it shall be minimised automatically if not used within the configurable period of time, by default 30 seconds with a 10 second visible warning countdown. The signaller shall be able to extend this period by another 30 seconds by stopping the warning.
- A mechanism shall be provided to retrieve the minimised report. This shall not affect the signaller's situational awareness.

22.1 User interface

The reporting system shall provide a user interface for each report type so the user can design a query without knowing the details of logged information. This interface shall be determined by the outcomes of a HFI assessment. The following two distinct components of the selection process shall be available:

- Presentation – the user shall be able to select or modify parameters that affect the report presentation, for example, fonts, colours and column sizes.
- Content – the user shall be able to set up a query in order to extract information for the logged files. The following query variables shall be provided as a minimum:
    - time period – start date and time and end date and time
    - time span – start date and time and period to be covered in hours
    - columns for items such as asset name, asset status and note. The default shall be all columns applicable to a selected report, which can be different for each report type
    - ordering within columns, such as ascending or descending order on asset names. The default shall be descending time order with the user able to select more than one column for ordering the information
    - name of objects to be shown in rows, such as specific asset names or events. The default shall be all objects within the log applicable to the selected time period or time span.

22.2 Templates and format

The TMS shall provide at least one template for each report type. The templates shall be available to all users for selection.

Each user shall be able to create and save as many templates as they like for each type of report within their allocated storage area. The templates shall be accessible from any workstation. The user shall be able to set one template from the previously saved templates as the default template for each report type. When the report type is selected, the report shall be opened with the default template.

Reports shall be presented in a tabular format with the column header always visible. The user shall be able to tailor the presentation format, similar to other presentation products such as spreadsheets.

22.3 Dynamic reports

The reporting system shall present the following events in real time, and update them as any changes occur:

- current alarms
- current restrictions
- current worksite protections
- outstanding axle counter reset operations
- current trains.

Due to the dynamic nature of these reports, no time or period selection shall be set. However control boundaries shall be selected as follows:

- area of control or line allocated to the user – as the default selection
- areas or lines selected by the user.

If other presentation options are available to the user, a mechanism to prevent losing the user's situational awareness shall be provided.

22.4 Historical reports

The reporting system shall be able to present the following events from the logs as historical reports, as a minimum:

- alarms
- trains
- asset status
- restrictions
- worksite protections
- human interface controls and commands
- user management events
- interface events
- operational events
- handover reports
- system events.

22.4.1 Failure requirements

The following additional information or warnings, as a minimum, shall be presented to the user, subject to the outcomes of the HFI assessment:

- retrieving records from the logging system takes longer than five seconds, for the part of the report the user is currently looking at
- retrieving complete records takes longer than 30 seconds
- the integrity of the record has a problem
- the requested records are not available online but are available in the long-term storage system.

22.4.2 Report functions

Reports shall have the following functions:

- previewing the report according to set parameters, such as page setup, fonts, colours and so on
- printing the report exactly as shown in the preview
- saving the report to a user-selected location, including the user's allocated storage area, with user-selected report name
- opening saved reports, including its selected parameters.

22.4.3 Printing of report

The reporting system shall be capable of printing the full report or part of it. Printing parameters shall be available for modification in line with accepted industry practice. The following information, as a minimum, shall be added automatically to the heading of the printed report, and printed once:

- user name
- date and time the report is generated
- date and time the report is printed
- report selection criteria.

The print preview functionality shall also be available in keeping with industry practice.

22.4.4 Saving of report

The user shall be able to save the report into the storage systems for which the user has access privileges. The saving process shall provide the following functionalities as a minimum:

- navigating and selecting a directory within the allocated storage space
- creating directories
- providing a default name as an outcome of the HFI assessment, if the report has no name already
- modifying file name
- overriding existing file
- saving in comma separated value (CSV) format.

The reporting system shall be able to open any saved reports within the storage systems, allocated and specific to the logged-on user. The saved report shall not access the logging system for any purpose. That is, the saved report's content shall be static. However, the user shall be able to modify the filtering parameters to select the records to be presented among static records.

22.4.5 Adding notes

Each historical report shall have the capability to add a note to any entry. The entry shall have the following components, as a minimum:

- date and time shall be inserted automatically and not be editable
- user name shall be inserted automatically according to the user currently logged on and not be editable
- free text up to 2000 characters.

The user shall be allowed to save or abort the note after a confirmation. The TMS shall not allow modifications to any saved information, including notes and log details.

23 Printing requirements

The TMS shall provide complete printing functionalities in line with industry practice.

The TMS shall provide printing facilities for the following functions, as a minimum:

- reports, including logs and dynamic reports
- digital forms.

TMS shall connect to more than one printer. The user shall be able to select any available printer within the TMS infrastructure. Printers shall be configured so that at least one printer is available in the following situations:

- during disaster recovery
- when the redundant side is not available.

All connected printers shall be accessible by all users within the TMS infrastructure. The selection of the printer and its parameters shall follow relevant industry practices. Connection to printers shall comply with TS 05377.

The TMS shall also have the capability to print in PDF.

24 Replay requirements

The TMS shall provide replay functionality to support investigations, training and learning activities. Information used for this function shall be based on the logged information.

Replay functionality shall be set up with a user who has adequate privileges to perform this operation. The user shall be able to choose the following:

- start date and time
- end date and time
- area of control or line or object, such as train to be replayed.

When a replay starts, the time and date shown on the replay workstation shall be the time and date when the event was timestamped during the logging operation described in Section 21. The user shall be able to set the replay workstation's date and time to anytime between the start date and time and end date and time selected earlier for replay purposes.

The replay shall be continuous even if it covers more than one day. If the required log entries are in long-term storage and not available for immediate access, then the TMS shall be able to use the extracted information as historical reports, covered in Section 22.4.

If the integrity of the logged information is compromised, as detailed in Section 21.2.1, then the user shall be informed.

24.1 Replay functions

The replay function shall have the capability to 'play', 'stop' and 'pause'. Desirable functions would include 'play next event', 'play previous event', and 'play next event' for specified asset.

The user shall be able to perform the following functions:

- start the replay anywhere within the start time and end time with immediate effect
- save bookmark at a specific time and retrieve saved bookmarks

- modify the replay speed any time with immediate effect. Selectable speeds shall be 0.25, 0.5, one, two, four and eight times of actual time.

If the replay operation is running on a workstation that is connected to the active system used for the signalling and train operations, the performance or functionality shall not impact the TMS. This shall be identified and assessed during the system safety assessment. Workstations used for the replay operation shall indicate that they are not operational workstations.

24.2 Presentation of events

The replay shall present the following logged events as a minimum:

- signalling asset status
- train and related information
- alarms
- operator commands
- system events
- timetable information
- time and date.

The replay shall be shown on the workstation using the track plan. This shall be identical to the signalling and train operations used for the selected area or line. Events shall be presented identically to the actual system. If there is any difference, then an analysis to identify potential risks and mitigations shall be carried out.

The TMS shall indicate workstations used for replays so the operator does not confuse between replay and controlling workstations.

The TMS shall be able to export the replay data in a standardised video format such as MP4 or executable, so that the replay operation can be performed without requiring any additional tools or programs.

25 Simulation requirements

The TMS shall provide simulation functionality for training, investigation, configuration, development, testing and integration purposes. The simulator is also an important tool to support the whole life cycle of the TMS.

The simulator system shall be a replica of the commissioned TMS so as to support the TMS assurance requirements. Some interfaces such as field systems shall be simulated to make the simulator a practical tool.

The simulator shall have identical infrastructure and interfaces to the commissioned TMS. The simulator shall be developed and configured to the same level of integrity as the operational TMS.

The simulator shall perform all functions identically to the commissioned TMS. The simulator system shall simulate all interfaces as accurately as possible, including behaviour and timing aspects of the systems it is simulating. All deviations from the operational TMS used for signalling and train operations shall be analysed to determine their impact on the simulator usage, such as testing and configuration development.

External and field systems shall be simulated at the interface level, so the simulator system can be used with simulated or actual external or field systems, as shown in Figure 1. If the supporting systems illustrated in Figure 1 are not provided as a part of the simulation system, then they shall also be simulated at interface level.

The simulator shall simulate alarms identical to the commissioned TMS.

The simulator shall cover the same areas of controls and lines as the operational TMS. Workstations used for simulation purposes shall indicate they are not operational workstations.

25.1 Training requirements

The simulator system shall have the capability to train and assess users. The following two distinct simulator workstations shall be available for training purposes:

- The trainee simulator workstation shall fully replicate the operational configuration in use in the traffic management centre including enabling systems such as voice communications.
- The trainer simulator workstation shall be able to simultaneously manage the simulator scenarios for the entire TMS for multiple trainee simulator workstations. The trainer simulator workstations shall allow multiple trainers to run training scenarios as a team. The trainer simulator workstation shall have the communication facilities to replicate the voice communications for all operational events according to the RIM Network Rules and Procedures.

25.2 Train movement simulation

The movement of trains shall be based on the acceleration and braking performance curves of passenger trains, line speeds and local speed restrictions. And on dwelling times at stations typical of the time of day and train driver response to signals.

The trainer simulator workstation shall have the means to automatically simulate timetabled trains and manipulate trains and the timetable for the following purposes:

- training scenarios inclusive of the certification of operators to use the TMS
- confidence testing in the operation of the TMS

- gauging of human responses to varying workloads and failure conditions.

The simulator shall have the capacity for the automatic entry of trains into the system, or for starting at any location within the system, according to a timetable used in the operational system. The simulator shall be able to edit and save a timetable for the purpose of creating a timetable for use by the simulator.

The simulator shall create trains at any location without timetable information with a default train profile.

The train running speed shall be adjustable by 0.5, one, two, four and eight times of the actual train running speed, as a minimum.

25.3 Signalling simulation

Signalling assets shall be simulated as close as possible to actual asset behaviours, including timing. Field system simulation shall be based on the commissioned signalling data, such as signalling plans and control tables.

Any deviation or approximation from the signalling asset shall be analysed to determine impacts on the simulator usage, especially the impact on the safety, verification and validation integrity.

25.4 Simulation scenarios

The simulator shall be able to build and save scenarios for the following purposes, as a minimum:

- training the operator for:
  - normal train running
  - railway perturbation and events, such as asset failures and train running issues
  - timetables, including special train notices
  - train variances from schedule
  - unauthorised train movements such as SPAD or train reversing without authority
- testing at various levels, including unit, factory acceptance, integration, regression or stress testing
- testing automation
- benchmarking
- demonstrating and presenting situations.

25.4.1 Creating scenarios

The simulator shall be able to place trains in the control area and place the signalling infrastructure into a predetermined state to start training or testing a scenario.

The start time of the simulator scenario shall be through either:

- setting the system time
- setting the scenario time as not being absolute and being relative to the current system time.

The trainer shall have the ability to control the movement of trains, the signalling infrastructure and all input and output that the control centre displays or controls. The trainer shall be able to set preconfigured times when the controls are to be activated.

The simulator shall record the responsiveness of the operator and produce on-time running profiles for the duration of the scenarios, for the purposes of operator assessment, workload modelling and timetable validation.

25.5 Development and testing

The simulator shall be used for testing and development purposes to support the whole life cycle of the TMS.

The outcomes of simulations shall be able to demonstrate integrity so they can be used as supporting evidence for assurance purposes. An evidence-based supporting analysis shall be carried out to prove that the simulator has such integrity.

The simulator shall allow testing of the following configuration items in any combination:

- hardware
- SOE and firmware
- software and its configurations
- site configurations.

The simulator shall be able to perform the following testing activities, as a minimum:

- fault finding and fault repeating
- acceptance testing
- regression testing
- integration testing
- timetable testing
- performance and stress testing

- verification and validation testing
- integrity and assurance testing.

The presence or use of a simulator in testing shall not invalidate the test results. An analysis shall be carried out to determine the impact the simulator has on the integrity of any test performed in the test environment.

26 Alarms requirements

Alarms are an integral part of any management system to inform the user of any unexpected or unusual events. Alarms should be provided in real time with integrity and accuracy. Otherwise, they can have negative effects on safe and reliable signalling and train operations.

The TMS shall have a mechanism to generate and clear alarms and present them accurately and reliably. To ensure an effective and efficient alarm system, the HFI assessment should include alarm requirements in its scope. Alarms and alarm handling shall be based on the outcomes of the HFI assessment. This analysis shall be based on EEMUA Publication 191.

The analysis shall include the following aspects of the alarm, as a minimum:

- Visual and auditory alerts shall be optimised so they are clearly detectable in the majority of operating conditions reasonably expected to occur.
- Alarms shall not be generated unnecessarily in the following conditions:
    - during system startup and shutdown
    - in a changeover period
    - without establishing complete integrity
    - during scheduled work, such as project work or maintenance.
- If an identical alarm, including asset and its state, is already within the system, a new alarm shall not be generated.
- If an alarm is generated due to an alarm condition being detected at the source, the alarm shall not be cleared until the status of the source is changed, so the alarm condition is no longer valid. Acknowledgement by the user shall not clear the alarm.
- If an alarm cannot be cleared by changing the alarm’s source condition, then the alarm shall be cleared by user acknowledgement.
- Alarms shall be kept within the system as active alarms until they are cleared and acknowledged.
- The TMS shall be able to keep acknowledged and cleared alarms within the system for up to seven days with the user able to access them using the mechanism.
- Different severity levels shall be set within the alarm system.

- The associated audible annunciation shall be provided for different alarm severities and types.
- A mechanism shall be provided to distribute alarms according to their relevance, such as maintenance or area of controls. The TMS shall be able to distribute an alarm to different users. However, only one user with adequate privileges shall be able to clear and acknowledge the alarm.
- If the generated alarm cannot be presented to any user, then the alarm shall be presented to the most relevant user available within the system. This shall be determined by the outcomes of the HFI assessment.
- Alarms shall be presented to the user in a form determined by the HFI assessment. Alarms shall be presented according to the parameters selected by the user. These parameters shall include the following, as a minimum:
    - time
    - severity
    - state
    - asset.
- If the system has an alarm-filtering mechanism and it is activated, then the user shall be informed, to prevent them from losing situational awareness.
- If the user is dealing with an alarm, then the user shall be able to temporarily stop the dynamic nature of the alarm presentation. For example, if the order of alarms is changing due to new alarms. When this option is selected, the user shall be informed, to prevent them from losing situational awareness.
- A mechanism shall be established to show the relationship between the alarm and the asset on the workstations related to the alarm. For example, when the alarm is selected, the source object can be shown on the display. Or, when the display object is selected, all alarms for the selected object can be presented.
- A mechanism shall be provided to stop or minimise nuisance alarms.
- Audible annunciation shall not be able to be turned off or silenced permanently.
- The TMS shall provide a functionality to mute currently sounding alarms without acknowledging alarms, to maintain the user’s operational awareness. When a new alarm is generated, or the state changes, the audible annunciation shall be activated automatically.

While some alarms are identified in this document, a complete list of alarms shall be identified during the HFI assessment based on the operational requirements.

27 Timetable requirements

Timetables are a schedule of train running times and contain trip information and other information relevant to train management. To aid the user with train operations, the TMS should be able to interpret timetable content and present it to the user correctly and accurately.

Timetables can change on any day of operations in response to incidents. An operator shall be able to reschedule the times using incident management tools such as timetable manipulation, simulation and deployment.

Timetable information can be generated outside of the TMS, which is the current configuration used by TfNSW. However, timetable creation, testing, modification, distribution and related functions should be part of the TMS.

The TMS shall have the capability to receive and store timetable information from external systems, in line with TS 05261. The information can be modified if it is unable to support TMS requirements. The TMS shall be capable of converting the timetable information from external systems for internal use.

The TMS shall be capable of sourcing train running information for the day of operations from one or more stored timetables, which become active timetables.

27.1 Timetable content

Timetables shall contain the following information, as a minimum:

- unique timetable name
- version
- usage, such as standard usage or specific to a date or day
- train information such as:
    - unique trip name
    - travel locations including arrival and departure times and operation. These locations shall be recorded with accuracy and precision to enable effective train management.
    - stopping patterns
    - dwell times
    - trains it forms
    - rolling stock information, if available
    - crew information, if available.

27.2 Timetable functions

The TMS shall provide the following capabilities related to timetables, as a minimum:

- An integrity check shall be done when the timetable is received or modified. If an issue occurs that affects the safety and reliability of train operations, then the user shall be informed. If requested, the received timetable shall be deleted.
- If the timetable information exchanged between an external system and the TMS is not compatible with the components of the TMS, then the TMS shall be able to translate the timetable information without losing the integrity and accuracy of the original timetable.
- Before any timetable is loaded as the active timetable, the original timetable shall be backed up in a safe and accessible location.
- The system shall have the ability to receive the same timetable more than once under the following conditions:
    - If the received timetable and the existing timetable have the same version number then:
        - For an active timetable, the existing timetable with the same name and version number shall be purged, excluding any running trains. The active timetable shall be loaded
        - For a timetable that is not currently active, the existing timetable with the same name and version number shall be purged. The received timetable shall be stored.
    - In all other conditions, the received timetable shall be stored as a different timetable.
- The TMS shall be able to present all timetables within the system to the user, including backed up timetables. This shall allow it to perform the following functions, as a minimum, to create an active timetable:
    - Load – loads or reloads selected timetables without removing active timetables. The trips shall override if the active timetable has the same trips, as long as they are not running.
    - Replace – removes selected active timetables and loads the selected timetables.
    - Delete – deletes the selected active or received timetables from the system but does not delete inactive timetables.
- When all trains within the timetable complete their run or are deleted, then the timetable shall be deleted automatically. If a train within the timetable has not been run in the previous two days, then the timetable shall be automatically deleted.
- When the active timetable is deleted, then the associated backed up timetable shall also be purged automatically.

- When any timetable operation is initiated, the train integrity shall be analysed according to the set business rules. These rules shall be determined according to the hazard analysis outcomes. The user shall be informed if a problem is detected.
- Timetable operations shall not affect the TMS functional or non-functional performance, or user operations such as delays or unresponsiveness.

27.3 Timetable presentation

The TMS shall provide the functionality to view the timetable in a tabular or graphic form. The HFI assessment shall determine the following:

- the timetable to be presented, such as an active, received or stored timetable
- the content of the timetable information to be presented
- the way information is presented, including order, colour and details.

The user shall be able to search a selected pattern within the presented timetable.

The user shall be able to print all or part of the presented timetable.

The timetable shall be presented to the user, according to their selected control area, as the default configuration. However, the user shall be able to select other areas without losing situational awareness.

27.4 Train performance

A list of reporting points, which are travel locations as detailed in Section 27.1, shall be defined and agreed upon for timetable comparison. When trains arrive at the reporting point, the actual time shall be recorded with a comparison to the timetabled time for the reporting point. This can be valid for departing from a reporting point when specified. Arrival time is defined as the detection of the train head at the location. Departure time is defined as the first detection of the train head beyond the location.

Train performance shall be presented to the user in the following two ways:

- as part of the train description, such as colours, or measurement of delays in minutes
- in a report, which lists trains in a selected order such as by:
    - magnitude or type of deviation from the timetable, or both
    - a location or line or area
    - different operations, for example, cancel, skipped or truncated.

Reports shall include the following content as a minimum:

- the train description
- deviation characteristics such as early or late, and magnitude in minutes

- the time of scheduled arrival (or departure), if a reporting point is selected.

On-time running information shall be calculated and presented according to selected parameters, such as timeframe, location, line or area.

28 Train management

Train management functions are based on train running order, and this can be implemented in different ways, for example:

- when the train order is modified, the timetable is updated and the current timetable reflects the current train running order
- when the train order is modified, the local queues based on a timetable are updated, however the original timetable is not modified.

A user with adequate privileges shall be able to modify the train running order based on the train management requirements, including incident management principles.

The TMS shall have an ARS which allocates required resources as they become available, according to the train running order. ARS assumes that all safety and conflict issues have already been resolved.

28.1 Automatic route setting

The ARS shall set routes for trains according to their running order when all of the following conditions are fulfilled, as a minimum:

- a train is at the required location, for safe and optimum train operation
- infrastructure resources are available
- there are no restrictions affecting the route
- the signaller allows the automatic route setting operation
- all assets affecting train movements are under the user's control
- other conditions identified during the system safety assessment are met.

The signaller shall have the capacity to enable or disable the ARS for a selected area at any time. They shall also be able to override requests issued by the ARS.

The ARS status shall be presented to the signaller, based on the HFI outcomes.

When any of the following conditions are detected, the ARS shall be automatically disabled to maintain the safety of the train management:

- train safety cannot be assured
- restrictions or worksite protections are detected

- integrity is compromised
- manual asset operation is used within the enabled area or for the train, if the operation is contradicting the ARS operation
- other conditions are identified during system safety and HFI assessments.

ARS shall not issue any controls or commands that can compromise safety.

28.2 Train identities

The TMS shall indicate the train positions accurately and precisely regardless of its configuration or type.

If the TMS detects a train which has no associated information, it shall automatically generate a unique train description. The signaller shall be informed. If a new trip is assigned to a train, then the TMS shall link the train fitment and train type information from the data provided by other systems.

Train descriptions shall track the movement of the train based on the track section occupancy, points detection and routes set. The train's travel direction shall be shown on the display. Deviations from the scheduled running time shall also be presented.

Train descriptions shall be displayed as close as possible to the front of the leading track circuit occupancy of the train, and avoid overwriting other information on the display.

In country areas, trains leaving the system at a normal exit point shall have the train description automatically deleted from the system. In metropolitan areas, leave the description at the exit point and overwrite the previously exited train description.

A hold facility shall be provided for shunting manoeuvres, especially where the sidings, loops or yards are not track circuited. When held, the description shall not move until it is released.

28.3 Train operations

The TMS shall be able to allocate train descriptions according to the current timetable, prior to a train entering the controlled area or line. The TMS shall allocate the next train description on the timetable and any information received from the adjacent TMS. The TMS shall then request the signaller acknowledges this allocation, or rejects it, and provides an alternative description if inconsistencies or uncertainties are detected in the timetable information. The user shall be able to set this operation to automatic mode, to acknowledge trains automatically.

Train descriptions shall be able to be changed according to locations specified in the current timetable. The TMS shall automatically change these train descriptions when they arrive at the location defined as the change point.

The TMS shall be able to perform the following:

- handle merging and splitting trains at any location
- hold one or more train at the specific location
- reverse the direction of traffic of a route already started, if all trains within the route are proven to be at a standstill
- handle rail traffic on the same track, if the rail infrastructure and signalling operations allow bi-directional operation
- manipulate the stopping pattern of the selected trains and distribute this modification to other controls and systems.

Modifications to a running trip, or a trip run by different users simultaneously, shall be prevented. Any conflict shall be presented to the users.

The signaller shall be able to allocate the description of a train moving through their area of control, or change it, using one of the following methods:

- queues
- train graphs
- a combination of queues and train graphs, though not at the same time.

28.3.1 Route operations

The TMS shall allow the following route operations based on the outcome of the system safety assessment:

- inverting the direction of traffic of a route, if all trains within are proven to be at standstill
- setting a sequence of routes to allow a train to turn back.

28.3.2 Train alarms

The following train alarms shall be provided, as a minimum:

- a train passes beyond its allowed movement authority, such as SPAD
- a train is moving in a direction opposite to its movement authority
- safe train separation is compromised
- a train disappears or appears at a location which is not planned or scheduled
- a train is at the wrong location according to its characteristics.

28.3.3 Queue operations

The signaller shall be able to set train management functions in automatic or manual mode. If automatic mode is selected, the TMS shall assign train descriptions according to current timetable information and information provided at the boundaries with other systems. If manual mode is selected, the signaller shall be able to signal (or not) for the train to run.

The signaller shall be able to manage running trips using the following functionalities, as a minimum:

- duplicate – allows for two running trips to run simultaneously at different parts of what was originally a single running trip
- change – terminates a running trip at its current location and starts a new trip from that same location
- clear – removes the selected trip from its current location and from all locations in its timetable plan, and terminates the trip at its current location
- revise – swaps a running trip with either a trip to run or with another running trip.

The signaller shall be able to manage trips using the following functionalities as a minimum:

- reorder – changes the order of trips to run
- cancel – deletes a trip so it does not run at all, or ends earlier than planned
- restore – undoes a previously cancelled trip and puts it in the original run order
- next – makes the selected trip the next trip to run
- move – moves one or more trips to a different position
- insert – adds a new trip to the selected run order, either a copy of another trip or a new non-timetabled trip.

When the trip orders are modified, the scheduled running time of all affected trips shall be recalculated without losing the original information. The following requirements apply:

- trips shall not be started to run earlier than planned
- trips shall not be started to run at the same time or earlier than the previous trip
- safe separation between trips shall be maintained.

The following information shall be distributed to external systems for further processing, in line with TS 05261:

- any running trip attribute changes, such as location or timing
- any trip order changes.

28.3.4 ETCS boundary operation

The TMS and ETCS L2 interfaces are detailed in Section 16.3.1. Where the ETCS L2 and line side systems have different train numbering conventions, the TMS shall automatically translate between them when passing rail traffic into and out of the boundary.

The TMS shall support and automate, as much as possible, any operational processes required when authorising an unfitted train from a line side signalled area into an ETCS area.

28.3.5 Train graph

If the TMS provides a train graphic interface, then the interface requirements shall be based on the outcomes of the HFI assessment. The following shall be considered as a minimum:

- All operations listed in Section 28.3.3 shall be available for the interface.
- The interface shall be designed so the user does not lose situational awareness.
- The interface shall be able to handle multiple trains on multiple lines without causing confusion or misunderstanding under stress conditions.
- The interface shall be able to display the following information for each train at the same time:
    - scheduled train running
    - actual train running
    - proposed train running, if incident management is requested
- If the interface has zooming and panning functionality, the requirements detailed in Section 20.1 shall be met.
- The interface shall also display the following information, as a minimum:
    - restrictions and worksite protections
    - user’s control area or line
    - area where ARS is activated.

Appendix A Indication examples used within TfNSW

A.1 Overview

This appendix provides indication examples used within TfNSW. The information provided in this appendix should be used as a guideline.

A.2 Tracks and routes

The railway lines should be displayed with the lines subdivided into track circuits, according to the signalling track plan. The separation of track circuits should be shown by gaps in the line of width greater than 0.5 mm and less than 1 mm.

Tracks should normally be drawn horizontally, though may have any rotation to suit the geographical layout.

All track circuits should be brought back to the control centre as individual indications.

Track circuit indications on the display should only be grouped when the individual track circuit indications are logged and the display principles are not compromised, particularly for determining signal and points clearance points (see Table 1).

Table 1 – Track circuit indications

Track condition	Track colour
Quiescent state – unoccupied, no route set	White or line colour where specified
Occupied	Red
Route set up or in the process of being set up	Green
Route over points where points are not detected in required lie for the route	Green – flashing
Indication failure	Grey
Blocked for route setting, and track unoccupied	Blue
Blocked for route setting, and track occupied	Purple

A.2.1 Route indication

Tracks in the route between the commence and finish signals should be coloured green to indicate that the route over the tracks is set or in the process of being set. Overlaps should not be indicated.

The green route lines should remain ahead of a train travelling through a route while the route is set or while there is a train in the route. If the train does not complete the route and leaves the route, then the green route lines should return to quiescent state. If the train does not complete

the route and remains on a track circuit with time release, then the green route line to the end of the route should be removed, returning the track indication to the quiescent state when the time release occurs.

Track indications to the rear of the train travelling through a route should return to green if the route is still set. Otherwise, the track indications should return to their quiescent state.

Where there are intermediate automatic signals, the green route line should propagate to the next controlled signal or the boundary of the area of control.

Where there are overset shunt signals, the route line should be based on the main route set.

A.2.2 Track circuit occupation indications

Colouring the track indication red should indicate the track occupancy.

A.2.3 Track circuit unoccupied indications

Colouring the entire track white should indicate the track circuit is unoccupied with no route set over it.

A.2.4 Tracks over points

Track indications over points are made up of at least five pieces as illustrated in Figure 2. These are:

- common leg
- reverse detection leg
- normal detection leg
- points pivot normal
- points pivot reverse.

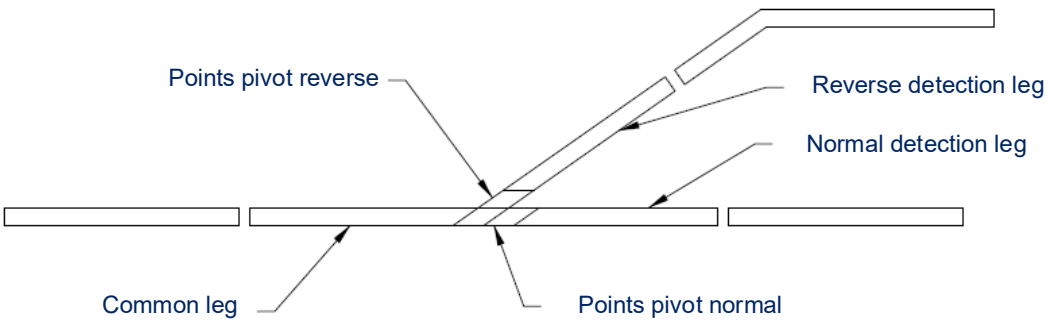

Figure 2 – Track pieces that make up a set of points

Route line indications over points should only be displayed on the common leg, the required detected leg and points pivot.

Where points for a route are not in the required position when the route is set, the required detection leg of the track should flash green until the points are detected in the required position, then it should become steady green.

Track occupancy indications over points should normally only be displayed on the common leg, the detected leg and points pivot.

If a track over points becomes occupied with a route set and no points detection, then the common leg, the called leg and pivot should flash.

If a track over points is occupied without a route set, then all three legs including the indicated pivot should show occupied – unless the system provides a warning to the signaller if a track becomes occupied out of sequence.

A.2.5 Track circuits with abnormal indications

Cut tracks, coded tracks, some intermediate receiver track circuits and axle counters indicated as track circuits can give abnormal track indications. This can cause these track indications to appear in the wrong sequence.

The system should cope with these types of abnormal indications and provide a consistent, meaningful display.

A.2.6 Non-track circuited track

Non-track circuited track should include those tracks for which there are no indications provided.

Non-track circuited track should be displayed in a darker shade of the colour used to display a quiescent state track indication.

Non-track circuited track should be provided on the display in sufficient detail for the signaller to determine the purpose of train movements into and out of a non-track circuited track, and possible alternative train movements.

Non-track circuited track may show occupied if it is part of the system's operation, together with train identification – and if the occupation indication can be removed by the signaller.

A.3 Signal repeaters

Signal repeaters should be provided for all controlled signals. All signals on the same pole should be combined into a single repeater, except where there is a shunt aspect – which should have its own repeater.

The signal repeaters should be drawn on the correct side of the track and in the correct geographical relationship with other display elements. The repeater should be drawn with the

base perpendicular and the stem parallel to the track it applies to. Each signal should be labelled with the same name that appears on the signal nameplate. When identified in reports and lists, the name should be the interlocking name followed by the signal name.

Automatic signals, except for those with emergency replacement, will not be indicated normally.

Automatic signals with emergency replacement should have an indication based on the signal being clear or at stop. The letter ‘E’, coloured red, is displayed at the base of the signal repeater when the signal has emergency replacement in force. The letter ‘E’ should be coloured grey when the signal does not have emergency replacement in force.

Automatic signals without emergency replacement that are indicated, or signals that can be identified as auto re-clearing, should have the letter ‘A’ displayed at the base of the signal repeater. The letter ‘A’ should be coloured green when the signal is in auto re-clearing mode. The letter ‘A’ should be coloured grey when the signal is not in auto re-clearing mode.

Subsidiary shunt signals should be provided with a separate yellow indicator on the main signal repeater to indicate that the shunt route has been selected.

Examples of signal repeater representation are given in Figure 3.

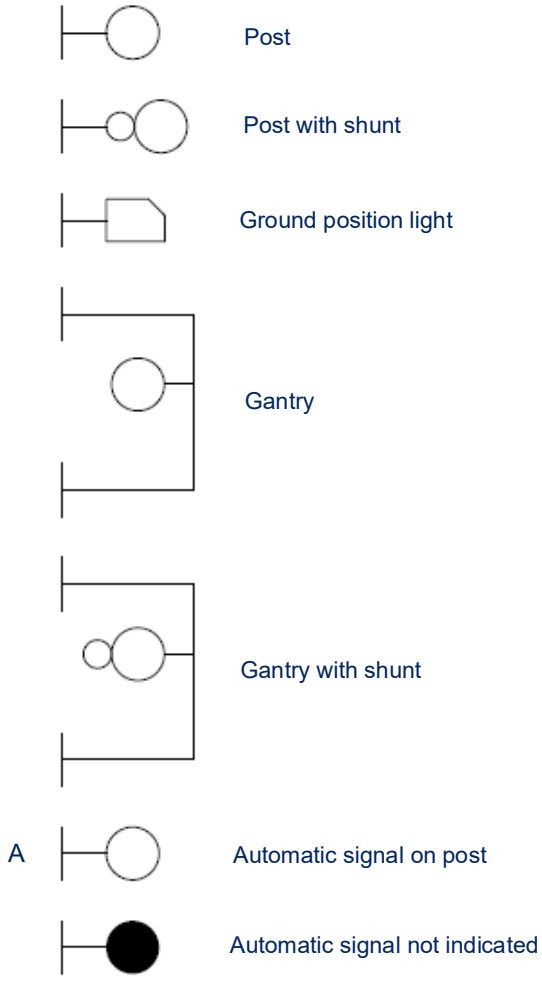

Figure 3 – Signal repeater representation

A.3.1 Colours

The base and stem or gantry for signals should normally be coloured grey.

The indication colour of the repeater should reflect the true status of the signal in the field as defined in Table 2.

Table 2 – Signal repeater colours

Colour	Meaning
Red	Signal is at stop
Red – flashing	The signal is at ‘stop’ but still subject to approach locking conditions
Green	A proceed indication is displayed in the signal
Green – flashing	Signal will clear when control conditions have been satisfied
Yellow	Shunt or subsidiary aspect clear
Grey	Failed or not indicated
Blue	Blocked and the signal is at stop
Orange	Blocked and the signal is not at stop

A signal is considered failed if it has no field indications, or if it has conflicting or unstable indications.

Automatic signals that are not indicated should be coloured grey.

A.4 Points and releases

Points and releases should be drawn for normal, reverse and failed conditions as shown in Figure 4.

Points normal detection should indicate the normal points pivot in the track colour. Points reverse detection should indicate the reverse points pivot in the track colour.

Points that are not detected normal or reverse are considered to be ‘in transit’. The ‘in transit’ condition should be indicated by the points detection leg and points pivot of the requested lie flashing.

The requested lie is:

- the same as the points call when the points call is normal or reverse
- the opposite lie to the previously detected or called lie when the points are not interlocked
- the existing lie when the points are interlocked.

If the points are detected both normal and reverse, they should be indicated as failed.

The points free indication should be given using one of the following methods:

- colouring the points number – red for locked, green for free, with the points number always displayed
- colouring the points pivot piece in the track – indicating either a free quiescent track, or track occupied, or route line for locked
- colouring a separate points free indication – red for locked, background colour for free.

The points control indications are detailed in Appendix B.6.

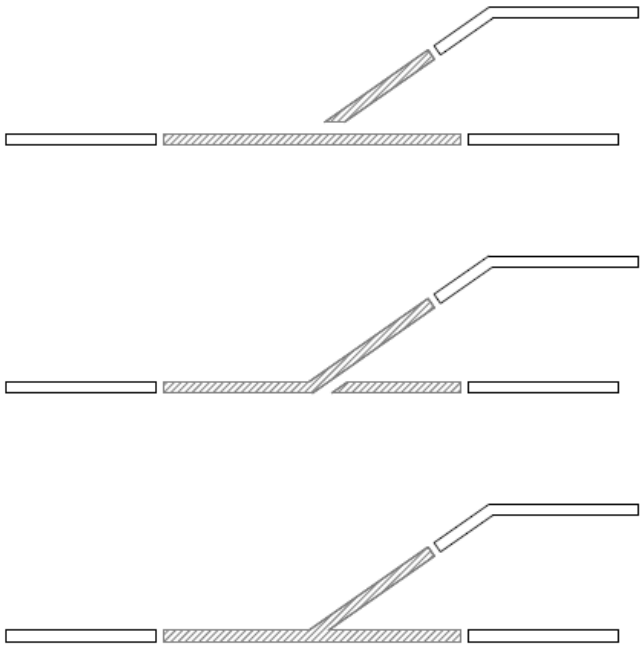

Figure 4 – Points and release representation

A.4.1 Releases and ground frames

The lie of switches controlled by ground frames should be drawn and indicated in a similar manner as points.

Releases should have a label giving the name of the associated ground frame drawn next to the display indication to identify that it is a release or ground frame and not a set of motorised points.

Control and block indications are detailed in Appendix B.9 on release or ground frame controls.

If the release does not have reverse detection, then the reverse detection will be composed of no normal control, no normal lock indication and no normal detection.

A.5 Blocking

When a block has been applied to equipment, the equipment should normally be coloured blue. How the blocking is indicated for each equipment type is detailed in the respective equipment sections in this appendix.

Vital blocks should be distinguished from non-vital blocks.

Vital blocks should be indicated by text naming the block. The colour of the text should change from grey to blue when the indication is received from the interlocking that the block is applied.

A.6 Alarms

Alarm indications should be provided for detectable equipment failures that require immediate attention from maintenance staff to prevent or minimise train delays.

The alarm display element should be in red colour when it is in the alarm state. The alarm display element should not be visible when it is not in the alarm state.

Typically alarms will be provided for the following:

- grouped signal lamp failure
- power supply failure for each AC, DC power supply point
- telemetry failure for each field station
- inability to deliver a control to a field station
- level crossing equipment failure
- location equipment failure
- fire alarm.

A.6.1 Alarm state

When an alarm indication changes to the alarm state, the signaller should be informed in one of the two following ways:

- Flashing the particular alarm display element in its alarmed state with a continuous audible warning until the signaller acknowledges the alarm indication. The alarm display element then displays steady in its alarmed state and the audible warning is silenced.
- The alarm display element displays steady in its alarmed state, a one second audible warning is sounded and an alarm acknowledgement ‘dialogue box’ or ‘window’ is presented to the signaller. The ‘dialogue box’ or ‘window’ should not obscure the signalling display or prevent the signaller from controlling the signalling.

The second method should be able to handle extreme cases of repeated alarm occurrence without requiring acknowledgement.

Alarms should have a hierarchy so that the failure of one piece of equipment does not cause false alarms in equipment it controls or affects.

An ‘acknowledge all alarms’ command should be provided if the second method is used.

A.6.2 Non-alarmed state

When an alarm indication changes to the non-alarmed state, the signaller should be informed with both:

- an audible warning of one second duration
- the particular alarm display element becoming invisible.

A.7 Warnings

Warning indications should be provided for detectable equipment failures requiring attention from maintenance staff to prevent a failure that can cause train delays.

The warning display element should be yellow in colour when it is in the warning state. The warning display element should not be visible when it is not in the warning state.

Typically warnings should be provided for the following:

- grouped signal lamp, primary filament failure
- power supply equipment warning for each AC and DC power supply point
- an LED warning for each AC and DC power supply point
- telemetry equipment warning for each field station
- level crossing equipment warning
- location equipment warning
- point transit warning when any point machine has been in transit for more than 15 seconds
- track occupancy out of sequence
- track clearance out of sequence
- train past signal at stop
- train ready to depart.

A.7.1 Warning state

If an indication changes to the warning state, then the signaller should be informed in one of the following ways:

- Flashing the particular warning display element in its warning state with a continuous audible warning until the signaller acknowledges the warning indication. The warning display element then displays steady in its warning state and the audible warning is silenced.
- The alarm display element displays steady in its warning state, a one second audible warning is sounded, and a warning acknowledgement ‘dialogue box’ or ‘window’ is presented to the signaller. The ‘dialogue box’ or ‘window’ should not obscure the signalling display or prevent the signaller from controlling the signalling.

The second method should be able to handle extreme cases of repeated warning occurrence without requiring acknowledgement.

An acknowledgement of all unacknowledged warnings command should be provided if the second method is used.

A.7.2 Non-warning state

When a warning indication changes to the non-warning state, the signaller should be informed with both:

- an audible warning of 0.5 second’s duration
- a particular warning display element becoming invisible.

A.8 Healthy indications

Healthy indications are not normally used for workstations.

However, a corresponding healthy indication should be provided in the following instances:

- if the display system fails and particular alarm or warning indications are not displayed
- when alarm and warning indications are in the alarm or warning state without a complete failure of the operator interface system.

The healthy display element should be grey or green in colour when the corresponding alarm and warning indications are not in the alarm or warning state.

The healthy display element should not be visible when either of the corresponding alarm and warning indications is in the alarm or warning state.

A.9 Authority to control interlocking

An interlocking may be controlled from an ELCP or an RCP. Either of these control panels may conform to this signalling operator interface. The control panel that is controlling the interlocking has all of the voice communications to the controlled area.

A.9.1 Emergency local control panel

The ELCP is provided with a control key switch that has a local control position, a remote control position and an optional closing position if appropriate.

The switch status indications should be displayed by one of the following methods:

- text local, remote and closing adjacent to a yellow display element that is displayed when the interlocking is in that mode of control
- text local, remote or closing appearing in yellow colour adjacent to the interlocking name when that mode of control is in use.

If more than one operator interface exists or may exist, then the operator interface with the authority to control the interlocking will normally display the interlocking name in green colour. Operator interfaces that do not have authority to control the interlocking should display the interlocking name in a colour that distinctively identifies it is operational, but not controllable, from the operator interface.

A.9.2 Remote control panel

The RCP should display the position of the control switch at the ELCP.

If the ELCP control switch is in the local control position, then a local control indication should be displayed near the name of the interlocking. Normally, this indication will be designated by the text ‘local control’ in steady yellow text appearing near the interlocking name. When the interlocking is in ‘local control’, it should prevent control of the interlocking from the RCP.

If the ELCP control switch is in the remote control position, then neither the local control indication nor the closing control indication should be displayed near the name of the interlocking and the RCP is not prevented from controlling the interlocking.

If the ELCP control switch is in the closing control position then a closing control indication should be displayed near the name of the interlocking. Normally, this indication will be in text ‘closed’ in steady yellow text appearing near the interlocking name. When the interlocking is in ‘closing control’, it should prevent control of the interlocking from the RCP.

A.10 Test mode

When the operator interface is in the test mode, as detailed in Appendix B.9.2, then the operator should be indicated that this mode of operation is in effect using the words ‘test mode’.

A.11 Axle counter

Axle counters should be displayed as for track circuits.

Alarms and warnings should be provided for any alarm or warning generated by the axle counter equipment.

A.12 Miscellaneous indications

Indications not explicitly covered should operate as shown in Table 3.

Table 3 – Miscellaneous indications

State	Indication
Normal state	Name of indication in grey text on display
Not normal state	Name of indication in yellow text on display

A.13 Bidirectional or single line working

Bidirectional lines or single lines between interlockings should be provided with an indication of the direction of travel of trains in the section.

The direction indication should be provided for the following:

- as part of the train description
- as part of the track occupancy indication
- as a separated direction indication.

Separate direction indications should be illuminated and coloured red for trains approaching and green for trains departing if only one interlocking is in the signaller’s area of control. Otherwise, the separate direction indications should be illuminated in blue for ‘up’ trains and yellow for ‘down’ trains.

A.14 Time release indications

For track circuits that are provided with time release facilities for the release of route holding, a red display element should be provided below or adjacent to the track it applies to, to indicate the timing release is in effect. The display element should not be visible when the timing release is not in effect.

A.15 Dual controlled signals

Dual controlled signals can be used at the interface to an adjacent signaller's area of control.

Control is given to clear a signal into the area of control by selecting the signal repeater as commence and the home signal as finish. This is indicated by flashing the dual control signal repeater in green.

A dual control signal out of the section of control is available to be set when control has been granted from the adjacent section. This is indicated by a steady yellow control repeater above the signal. The signal can then be cleared by selecting the signal as commence and then selecting the appropriate finish point.

A.16 Maintenance call light

If maintenance call facilities are provided, then the text 'maintenance call' in yellow colour should be displayed adjacent to the particular location name when the maintenance call is active. Normally, the text 'maintenance call' is in grey colour.

A.17 Maintenance releases

Where there are maintenance releases for maintenance in bidirectional areas, they should usually be indicated as shown in Table 4.

Table 4 – Maintenance release indications

Indication	Colour
Normal	Name of release in grey text
Release given but not taken or returned	Name of release in yellow flashing text
Reverse	Name of release in yellow text

A.18 Master shunt

For each interlocking that has the master shunt facility, the master shunt should be indicated as shown in Table 5.

Table 5 – Master shunt indications

Indication	Colour
Normal state	The text 'master shunt' is displayed near the interlocking name in white colour or grey colour
Active state	The text 'master shunt' is displayed near the interlocking name in yellow colour

A.19 Derail

Derails should be drawn as a solid equilateral triangle with one side on the track and the opposite point pointing in the direction that a train is intended to derail in.

A.20 Audible warnings

A.20.1 Train arrived indication

An audible warning occurs whenever an alarm or warning indication changes to the alarm or warning state.

An audible warning should be provided to indicate the approach of a train to the controlled area. A different tone should be used for each direction, the up direction being a higher tone than the down direction. The signaller should be able to enable or disable the ‘train arrived’ indication.

A.20.1.1 Performance

Audible indications should be at least 10 dB above ambient noise level in the area where the signaller is located.

The audible warning should be at least 0.5 seconds for a warning and at least one second for an alarm.

If the associated visual indication is insufficient to ensure the signaller is aware of the alarm or warning, then the audible warning should be continuous until the alarm or warning is acknowledged.

Appendix B Control examples used within TfNSW

B.1 Overview

This appendix provides control examples used within TfNSW. This information should be used as a guideline.

B.2 Route setting

B.2.1 Entrance – Exit control system

All controlled signals should be identifiable as commence signals.

A route is set and the signal leading over it is cleared by the signaller identifying the commence signal and then identifying the finish signal in sequence. The finish signal is generally at the next signal applying to the direction of traffic being dealt with.

If the route leads out of the signaller's area of control, the finish signal can be an automatic signal or a controlled signal that is only valid as a finish signal for the signaller.

If the route leads into a siding or terminal road, the finish signal can be a notice board or a dummy non-indicated signal that is only valid as a finish signal for the signaller.

Once the commence and finish signal have been identified and registered by the system, the route request is sent to the signalling safety system, which will respond with corresponding indications as a result of the request.

If a conflicting route is set, or points within the route are locked in the incorrect position for the route being called, then the interlocking will reject the route. The signaller should identify the route again when the conflicts no longer exist.

To clear the next route on the line, the last signal identified, which represented the finish of the previous route, is again identified and this time it acts as a 'commence' for the next route. The next signal along the track in the same direction is then identified to set the route.

B.2.2 Identification of signals

B.2.2.1 Ability to identify signals without selecting signals

For video display unit systems, a signal can be identified by pointing to the signal or track before the signal with a pointing device such as a mouse and pressing the left mouse button.

For panels with push button controls, signals should be identified by pressing the button associated with that signal.

Where a commence signal leads to a finish signal that is not able to be controlled by the signaller, then the finish signal should be identifiable as a finish signal only.

Where a commence signal does not lead to a finish signal, then a finish point that is not a signal should be identifiable.

B.2.2.2 Control feedback

The system should provide feedback to the signaller that a particular signal has been identified as a commencement signal.

The commence signal control should flash. A display element labelled ‘machine in use’ should flash green on the display in the following situations:

- if the controls are not positioned on the display with the object they control but are located separately
- a commence signal has been identified but not the finish signal.

On identification of the finish signal, the commence signal should cease to indicate that it has been identified as the commence signal.

B.2.2.3 Identification of a main or shunt signal

Where a subsidiary calling-on or shunt signal is provided on the post of a running signal, a separate indication should be provided. Where relevant, a control point for both types of route should be available.

When a track is selected before the signal, the main route should be selected rather than the shunt route.

Only the main signal should be identifiable as a finish.

To identify a main route, the main signal repeater or control point is identified.

To identify a shunt or subsidiary route, the shunt or subsidiary signal repeater or control point is identified.

B.2.2.4 Preset shunts and overset shunts

The actions of setting and cancelling main and overset shunt signals should affect each other as defined in the control tables.

To clear the preset and overset shunt signals for movements originating at the shunt signal, the shunt signal is identified as the commence signal and a finish point is selected in the normal manner.

B.2.3 Master shunt override

If the master shunt override facility is provided for an interlocking, then a ‘master shunt’ control point is provided near the interlocking name. The master shunt control point is identified after identifying the commence shunt and before identifying the finish signal.

The master shunt control point will indicate that it has become active when it is identified and will return to its normal state when the finish signal has been identified.

B.3 Cancelling signals

When a signal is cancelled, the control is issued to the interlocking to put the signal to stop.

If the route needs to be cancelled before the passage of a train or before the establishment of the route, then the commence signal for the route is cancelled.

Signals should be cancelled in one of the following ways:

- pointing to the signal and issuing a cancel command
- entering cancel mode and identifying the signal
- pulling the signal button on a panel.

If a signal is in automatic re-clear mode or any other mode when it is cancelled, then the signal should be removed from the particular mode and put to stop.

B.4 Automatic re-clear

An automatic re-clear function may be provided to enable a group of controlled signals (one or more) to act as automatic signals. When a signal is selected to operate in the automatic mode the signals will continue to re-clear, subject to the conditions of the interlocking or track occupancy following the passage of each and every train to pass the signals. Removal of automatic re-clear mode returns all the applicable signals back to a fully controlled mode of operation.

Automatic re-clear is normally provided for the through lines of each interlocking where there are multiple lines through the interlocking.

Signals should not be able to be placed into automatic re-clear mode unless all the applicable signal routes have been previously set in the normal manner.

Removing a group of signals from automatic re-clear mode should not affect the routes set from the signals.

Groups of signals are placed into an automatic re-clear mode after they have been set by applying the ‘automatic re-clear’ command to one of the signals in the group of signals or by identifying the particular automatic re-clear control point on the display or control panel.

Signals or groups of signals are removed from automatic re-clear mode by applying the ‘remove automatic re-clear’ command to one of the signals in the group of signals. They can also be removed by identifying the particular automatic re-clear control point on the display or control panel for cancel. When any of the signals in the automatic group is cancelled, only the signal in the auto group should be removed from automatic re-clearing mode.

B.5 Emergency replacement

Certain automatic signals can be forced to remain at stop. This facility is called emergency replacement. Signals with the emergency replacement facility are normally at the end of a station platform on a line that is proceeding into a tunnel or over a bridge or viaduct.

The method of placing a signal into emergency replacement should be the same as that of cancelling a controlled signal.

Emergency replacement is removed by identifying a signal as ‘commence’ and the next signal as ‘finish’, similar to setting a route from a controlled signal.

B.6 Points

Controls should be provided to operate points without the necessity to set a route. This type of operation is required for maintenance purposes and under failure conditions or where it is required to hold a set of points in a particular position during route setting.

Each set of points has three controls: ‘normal’, ‘reverse’, and ‘centre’. The ‘normal’ control requests the interlocking to move the points normal and lock the points in the normal position. The ‘reverse’ control requests the interlocking to move the points reverse and lock the points in the reverse position. The ‘centre’ control allows the interlocking to move the points, based on the interlocking conditions. The points controls are sometimes referred to as ‘points calls’ as they only request the signalling safety system to move the points.

When route setting is being used, the points control is placed in the centre position. If individual operation of the points is required, then the control is placed in the normal state to set the points normal and in the reverse state to set the points reverse.

The points operation is such that before the position of the points can be changed from normal to reverse, the point call should be set to the centre call until the points become free and then the points call can be set to the desired call. This pause in the centre call is necessary to allow the point locking to be removed. The centre call, intermediate step is also used to prevent the storage of points controls in the interlocking moving the points.

One of the following three methods for controlling points should be used:

- Select the common leg and the required leg to move the points to the required lie. Select the points number to turn on or turn off the points centre control.

- Select the points command and required leg to move the points. Select the points number to turn on or turn off the points centre control.
- Select the normal, centre or reverse control point for the set of points.

The state of points controls should be indicated on the display.

The method of indicating the state of points controls should not mask or change the field indications of the points as to the current position of the points.

The indications for the points control should either be N for normal, R for reverse, or C for centre adjacent to the points. Or by changing the display to normal, reverse and centre control points for the points.

Additional controls for blocking of points should be provided. See Appendix B.8 for details on these controls.

B.7 Releases

B.7.1 Ground frame

Ground frame releases should be provided to allow an electrical release to be given to the line side releasing switches, enabling the Annett's key to be removed once personnel in the field have accepted the release.

The release should be given and taken back in a similar manner to controlling a set of points. The release should be given by identifying the reverse leg of the switch that the ground frame operates. The release should be taken back once the ground frame has been returned to its normal state, and the Annett's key returned, by identifying the normal leg of the switch.

When the release has a normal call, the releasing switch number should have an 'N' suffix.

When the release has a reverse call, the releasing switch number should have an 'R' suffix.

B.7.2 Maintenance

Maintenance releases are provided for double line bidirectional sections. When the maintenance release is given, it disables the bidirectional operation.

Maintenance releases are displayed and labelled as control points. When they are identified, they either give a release or normalise the release as appropriate.

B.8 Blocking

The blocking facilities are used in conjunction with the TAO's relevant safeworking units and provide protection to people or equipment, or both.

The application and removal of some blocks is associated with completing particular safeworking forms.

Both the application of blocks and the removal of blocks should be at least a two-step process.

Non-vital blocking should be available to prevent the clearing of routes, moving points or allowing trains into sections. Non-vital blocks can be identified for placement and removal by the signaller. This will act as a reminder to the signaller of existing special conditions, such as maintenance activity or unsafe conditions that the interlocking is unable to detect.

Vital blocking is provided as part of some signalling safety systems.

If the signaller attempts to perform a function that is blocked, then the system should notify the signaller that the function is not available and give the reason.

All blocks should be stored in non-volatile memory so that in the event of a system restart, the blocks remain in effect.

As a minimum, the system should record when each block is placed and by whom, and when removed and by whom. This record should be kept as historical information.

The signaller should be able to bring up a list of all of the blocks currently applied to their area of control.

> Note: The concept of ‘vital’ is replaced with the ‘safety function’ as detailed in IEC 62278.

B.8.1 Safeworking forms

The safeworking procedures require that specific safeworking forms are filled out when blocks are used.

Signalling operator interfaces should provide the forms and manage the record keeping of the forms in a database. However, the process should not be more onerous than any existing paper forms. This process should include the following:

- being able to set routes and so on while filling out the form
- being able to view old forms
- changing to a new form format.

Any forms that the procedures require should be duplicated by the TMS. The TMS should automate the entry of details on these forms.

A unique sequential number should be given to the form for each particular block applied.

The TMS should record the date and time and the login name of the signaller that is applying an action, which results in changes to the blocking arrangements on the safeworking forms.

When a signaller applies a block, the effect of the block should apply immediately. The TMS should then require the signaller to enter the details to appear on the safeworking form.

A signaller should be able to add to the form, while the block has been placed, details such as extensions of time or change of staff information.

When a signaller removes a block, the block should remain in effect until the signaller has entered the required information in the safeworking form.

The details entered on the safeworking form should not be able to be changed once the signaller has completed the removal of the block.

Safeworking forms should be kept as historical information.

B.8.2 Vital blocking

Vital blocking is implemented in the signalling safety system. The TMS allows the signaller to apply these types of blocks and indicates to the signaller the state of these blocks.

Vital blocks normally apply to a section of single line and are displayed by the name of the block appearing alongside the track where the block is applied. Vital blocks are applied by the signaller identifying the name of the block.

B.8.3 Non-vital blocking

Non-vital blocking is implemented by the TMS and requires an independent validation review on its integrity.

Non-vital blocking should be able to be applied to each signalling control available on the signalling operator interface.

B.8.3.1 Signal blocks

Signal blocks should be applied by selecting the blocking mode and then identifying the signal that the block should apply to. This should have the effect of not allowing routes to be commenced from the blocked signal. Routes should not be able to be stored from or through a blocked signal. Routes should be able to finish at the signal while it is blocked.

A signal block should not be able to be applied while the signal is clear or has been requested to clear or there is a route in storage that would be applied over the block.

If a signal is blocked, then this should be indicated by colouring the signal repeater blue.

If the signal clears while blocked, then an alarm should be generated.

B.8.3.2 Track blocks

Track blocks should be applied by selecting the block mode and then identifying the track circuit the block should apply to. This should have the effect of not allowing routes to be called where the clearing of the route would allow a train to proceed over the blocked track circuit. Routes over the affected track should not be able to be stored.

A track block should not be able to be applied while a route has been set over the track circuit being blocked, or while there is a route in storage that would be set over the blocked track circuit.

Track blocks should apply to the entire track that is indicated by the same track circuit. That is, a track block applied to a points track should block routes over both lies of the points.

Track blocks should be indicated to the signaller by colouring the track circuit repeater in blue.

Track blocks should not mask track occupation. Tracks should be coloured purple when blocked or occupied.

B.8.3.3 Points and ground frame blocks

Points should be able to be blocked in a particular lie. Blocking a set of points should prevent the TMS from calling the points to the other lie, or requesting any routes that would call the points to the other lie. Points blocks should be applied after calling the points to the lie in which they are to be blocked, by selecting the blocking mode then identifying the opposite lie of the points.

The points controls should either be in ‘normal’ or ‘reverse’ before a points block is accepted. Points should not be able to be blocked with a ‘centre’ points call.

Points blocks should be identified by colouring the tracks of the other lie of the points blue. For double-ended sets of points, both ends of the points should be blocked when one end of the point is blocked, with the block displayed on both ends.

Ground frames are blocked in the same manner as points.

B.8.3.4 Removal of blocks

Blocks should be removed by selecting the remove mode then identifying the piece that is indicated as blocked, or by displaying the list of blocks and identifying a block in the list for removal.

B.9 Authority to control an interlocking

An interlocking can be controlled from an ELCP or an RCP. Either of these control panels may conform to this signalling operator interface. The control panel that is controlling the interlocking has all of the voice communications to the controlled area.

If the signaller's interface is for an ELCP, then the signalling operator interface should provide for local, remote and closing controls.

If more than one operator interface at either site can control the interlocking, then facilities to manage the control of interlockings between operator interfaces are required. These facilities should include the following:

- ensuring that normally only one operator interface is controlling a particular interlocking
- requesting, granting, and releasing of authority to control an interlocking
- taking authority to control an interlocking if the controlling operator interface has failed
- temporary shared authority to control an interlocking to allow for maintenance work.

B.9.1 Emergency local control panel control switch

The ELCP is provided with a control key switch that has a local control position, a remote control position and optionally a closing position, if appropriate.

If the control switch is in the local control position, then the ELCP has full control of the interlocking and the RCP is prevented from controlling the interlocking. In the local control switch position, the voice communications for the controlled area are directed to the ELCP.

If the control switch is in the remote control position, then the RCP has full control of the interlocking and the ELCP is prevented from controlling the interlocking. In the remote control switch position, the voice communications for the controlled area are directed to the RCP.

If the control switch is in the closing position, then the RCP is prevented from controlling the interlocking and the ELCP is prevented from controlling the interlocking. In the closing control switch position, the voice communications for the controlled area are directed to the nearest attended control panel.

B.9.2 Test mode

A test mode facility should be provided to allow direct control of the signalling safety system. This is only required on the ELCP to allow the signalling safety system to be tested.

The test mode should allow all controls to be passed to the signalling safety system, without any integrity or availability checking, so the signalling safety system can be tested.

If the signalling operator interface is in test mode, it should display 'test mode' as a warning as described in Appendix A.10.

Entry to test mode should be protected against unauthorised use. The protection mechanism should be able to prevent a person who has observed the entry to test mode from gaining test mode authority.

B.10 Acknowledgements

Alarm and warning acknowledgements should be provided as required.

B.11 Notations

The signaller should have a facility for placing text notes on the display. The text should be able to be placed anywhere on the geographical display, to locate the text when required.

Notations have a title and detail text. The title is normally all that appears on the display.

By identifying the notation title, the system displays a text window displaying the existing detail text and the signaller can enter more text.

The signaller should have the facility to create, move, edit and delete notations. The notations should be stored in non-volatile memory on the system, so that if a system restarts, the notations will not be lost.

B.12 Reset equipment

Some equipment used as part of the signalling system may need to be reset under certain circumstances. The signalling operator interface should provide the means for these resets.

The resetting of devices should only be performed as part of a safeworking procedure. Any reset should be at least a two-step process.

Resets may be provided for axle counters and track sequence warnings.

B.13 Multiple route setting

When the majority of signals for the commonly used train paths cannot be put into automatic re-clearing mode, then multiple routes in sequence should be able to be set in one request. This should be achieved by identifying the commence signal as the start point for the multiple routes, and the finish point for the last route. Where more than one path exists between the commence signal and finish signal, the TMS should select the optimum path (these may be predefined but should follow the main lines as far as possible). The signaller may specify the path to take by identifying the intermediate point.

Appendix C Human factors example used within TfNSW

C.1 Overview

This appendix provides guidance on user requirements for signalling operator interfaces. The information is based on recommendations from numerous human factors workshops.

C.2 Visual display unit layout

All visual items displayed on the signalling operator interface that are part of the operator's regular tasks should fit within an area bounded by 2 x 65 degree arcs separated by a 300 mm channel centred on the signaller's centre ERP. Figure 5 illustrates an example of a 4 x 30 inch screen layout.

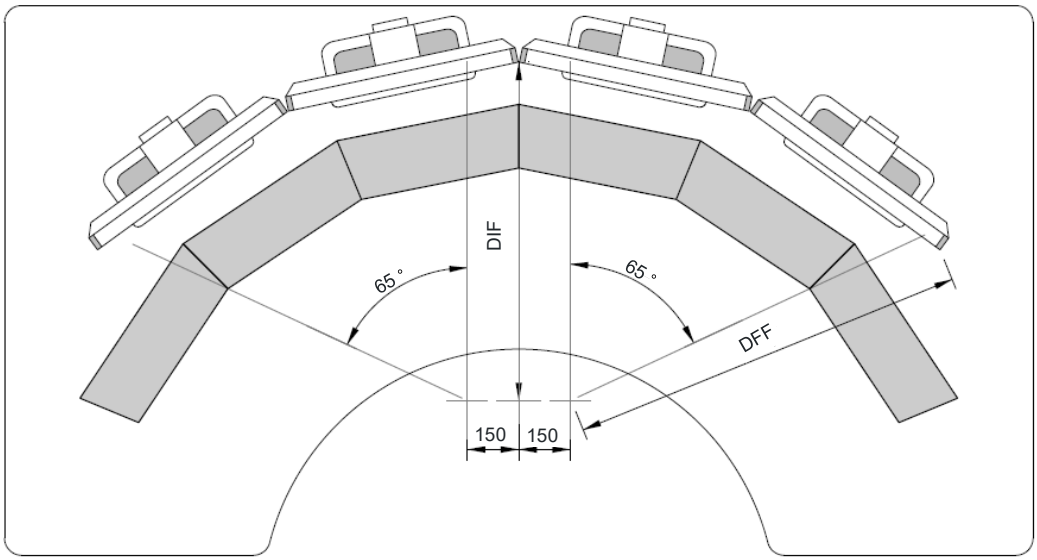

Figure 5 – 4 x 30 inch visual display unit layout

The operator has three ERPs, a centre ERP and two 150 mm on either side of the centre.

The distance directly in front of the signaller (shown as DIF in Figure 5) is the viewing distance from the primary visual display units directly in front of the signaller's centre ERP.

The distance further from the signaller (shown as DFF in Figure 5) is the furthest viewing distance from the primary visual display units to the signaller's furthest ERPs.

C.3 Font and text selection

The following factors should be considered for font and text of the visual displays:

- text should appear in title case or lower case to achieve better readability
- sans-serif fonts should be preferred to more decorative fonts
- height to width ratio of letters should be between 10:8 and 10:5
- spaces between words should be equal (that is, left or right aligned text should be used instead of justified text)
- fixed width fonts should be avoided.

Optimal stroke width is dependent on polarity and screen technology. As a broad guideline, displays with dark characters on light backgrounds should have a stroke width of about 14% to 20% of character height. Displays with light characters on dark backgrounds should have a stroke width of between 8% and 14% of character height.

When necessary, borders should be placed around text symbols to ensure that sufficient contrast is achieved.

C.4 Display measurement of visual items

The required sizes of the visual items are specified in arc minutes. An arc minute (or minute of degree of arc) is an angular unit of measure used to specify the height of an item at a given distance as shown in Figure 6. Given the arc minute (ArcMin) value of an object and the viewing distance (d) to that object, the required height (h) in millimetres can be calculated as follows:

h = d x Tan(ArcMin/60)

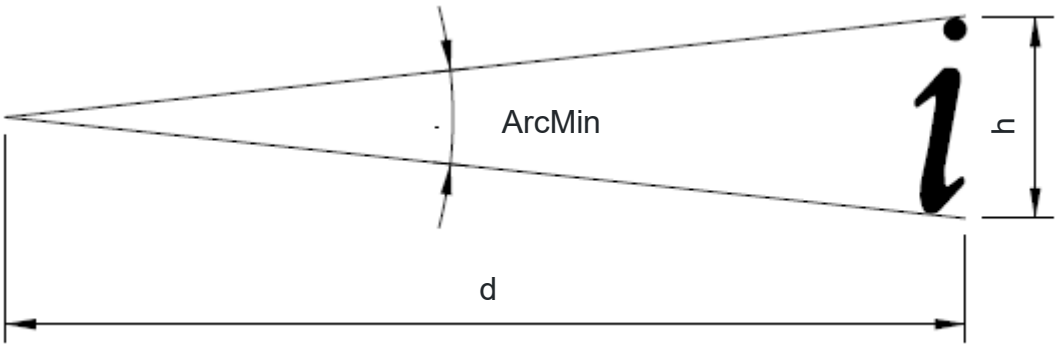

Figure 6 – Required height, viewing distance and ArcMin

C.5 Size of visual items

Based on the outcomes of the human factors workshops, the required size of visual items on the TMS should meet the arc minute (ArcMin) measurements in Table 6.

Table 6 – Signalling operator interface visual items size

Items	Distance to use	Requirement factors Dynamic state	Requirement factors Dynamic outline	Requirement factors Text	Requirement factors Primary	Requirement factors Contin. static	Requirement (ArcMin) Human factors	Requirement (ArcMin) Workshop (final)	mm## 30 inch screen
Menu item text	Furthest from signaller	X		X	X		15 tall	15 tall	5
Status bar text	Directly in front of signaller	X		X	X		15 tall	15 tall	4.5
Tool tip text	Furthest from signaller	X		X	X		15 tall	15 tall	5
Alarm text	Directly in front of signaller	X		X	X		15 tall	15 tall	4.5
Controlled signal symbol	Furthest from signaller	X			X		15 tall	15 tall	5
Automatic signal symbol	Furthest from signaller	X			X		15 tall	15 tall	5
Train description text	Furthest from signaller	X	X	X	X		15 tall	15 tall	5
Track symbol	Furthest from signaller	X			X	X	4.5 thick	7 thick +++	2.5
Block joint (track separation)	Furthest from signaller						1.5 wide	1.5 wide	0.5
Track label	Furthest from signaller			X			7.5 tall	6.75 tall +++	2.25
Signal label	Furthest from signaller			X			7.5 tall	8 tall	2.75
Points label	Furthest from signaller			X			7.5 tall	8 tall	2.75
Miscellaneous static text	Furthest from signaller			X			7.5 tall	8 tall	2.75

Items	Distance to use	Requirement factors Dynamic state	Requirement factors Dynamic outline	Requirement factors Text	Requirement factors Primary	Requirement factors Contin. static	Requirement (ArcMin) Human factors	Requirement (ArcMin) Workshop (final)	mm## 30 inch screen
Platform name	Furthest from signaller			X			7.5 tall	14 tall	4.75
Ars group	Furthest from signaller	X		X	X		15 tall	18.5 tall	6.25
Auto reclear	Furthest from signaller	X			X		15 tall	17 tall	5.75
Control status indicator (light)	Furthest from signaller	X					7.5 tall	13.5 tall	4.5
Control status indicator (text)	Furthest from signaller			X			7.5 tall	10.5 tall	3.5
Direction indicator	Furthest from signaller	X					7.5 tall	13.5 tall	4.5
Direction override	Furthest from signaller	X		X			15 tall	20 tall	6.75
Dual control indicator	Furthest from signaller	X					7.5 tall	11 tall	3.75
Dual control repeater	Furthest from signaller	X					7.5 tall	11 tall	3.75
Emergency replacement group	Furthest from signaller	X			X		15 tall	38 tall	12.75
Emergency shunt function	Furthest from signaller	X		X			15 tall	20 tall	6.75
Fixed red	Furthest from signaller				X		7.5 tall	9.75 tall	3.25
Flood detector (light)	Furthest from signaller	X					7.5 tall	13.5 tall	4.5
Flood detector (text)	Furthest from signaller			X			7.5 tall	11.25 tall	3.75
Half pilot staff	Furthest from signaller	X	X				15 tall	18.75 tall	6.25
High load detector	Furthest from signaller	X					7.5 tall	18 tall	6
Level crossing	Furthest from signaller	X			X		15 tall	37.5 tall	12.5
Local control panel	Furthest from signaller	X		X			15 tall	18.75 tall	6.25
Non stopping train function	Furthest from signaller	X		X			15 tall	22.5 tall	7.5

Items	Distance to use	Requirement factors Dynamic state	Requirement factors Dynamic outline	Requirement factors Text	Requirement factors Primary	Requirement factors Contin. static	Requirement (ArcMin) Human factors	Requirement (ArcMin) Workshop (final)	mm## 30 inch screen
Notice board/stop board	Furthest from signaller				X		7.5 tall	13.5 tall	4.5
Releasing switch	Furthest from signaller	X	X				15 tall	23 tall	7.75
Ring circuit	Furthest from signaller	X		X	X		15 tall	18.75 tall	6.25
RTU	Furthest from signaller	X		X			15 tall	18 tall	6
Track timer	Furthest from signaller	X					7.5 tall	8 tall	2.75
Train stop	Furthest from signaller	X	X				15 tall	16.5 tall	5.5
Ventilation lock	Furthest from signaller	X					7.5 tall	8 tall	2.75
Point selection area (width)	Furthest from signaller				X		27 tall	27 wide +++	9
Point selection area (height)	Furthest from signaller				X		18 tall	18 tall +++	6

C.6 Height of visual items

The required height of a visual item should be identified by evaluating the following factors in order:

- Every item should match or exceed the minimum visible level of detail at 1.5 arc minutes.
- A visual item categorised as having a continuous static outline should be at least 4.5 arc minutes tall. All other aspects can be ignored.
- A visual item that meets the criteria for only one of the following categories should be at least 7.5 arc minutes tall:
    - dynamic
    - state
    - dynamic outline
    - text and primary function.

    The remaining elements should be at least 15 arc minutes tall.

C.7 Categorisation of visual items

The following factors should be used to categorise visual items:

- Dynamic state – the visual item displays a dynamic state. This may be in the form of changing colour, text or shape.
- Dynamic outline – the visual item displays its state by changing its outline or shape.
- Text – the major element of the visual item is text. A visual item can include text in its appearance yet be defined by its other elements such as an emergency replacement group symbol.
- Primary function – the visual item is used as part of the primary function of the operator such as primary task and safety task.
- Continuous static outline – the visual item is part of a continuous static outline, for example, track.

Appendix D Geographical display examples used within TfNSW

D.1 Overview

This appendix provides examples of geographical displays used with TfNSW. The information should be used only as a guideline. A HFI assessment should determine the actual controls and commands that will be used for the TMS.

D.2 General information on geographical display

The geographical display should show the complete geographical area for the signaller's area of control and approaches to the area of control.

The background colour for the display should be selected to provide the optimum colour contrast for the range of colours used by the dynamic and static display elements.

The display should have dynamic elements that change the way they are displayed depending on their signalling status and signaller commands.

The display should also have static elements that do not change their display. These dynamic elements should include the following:

- signals
- tracks
- points
- releasing switches
- vital and non-vital blocks
- time releases
- alarms
- warnings
- miscellaneous equipment
- static elements, including:
    - platforms
    - block joints
    - automatic signals
    - distant signals
    - notice boards and landmark signals

- tunnels
- major overpass, underpass, bridges and viaducts
- level crossings
- non-track circuited sidings
- freight loading and unloading facilities
- weighbridges.

The tracks should be laid out horizontally. In general, the direction to Sydney Central Station should be on the left-hand side and the direction away from Central Station on the right-hand side.

If the controlled area needs to be displayed on more than one screen, the lines should be drawn from left to right across screens before moving down to a second line on the screen.

Figure 7 shows the preferred sequence and Figure 8 shows the sequence that is not preferred.

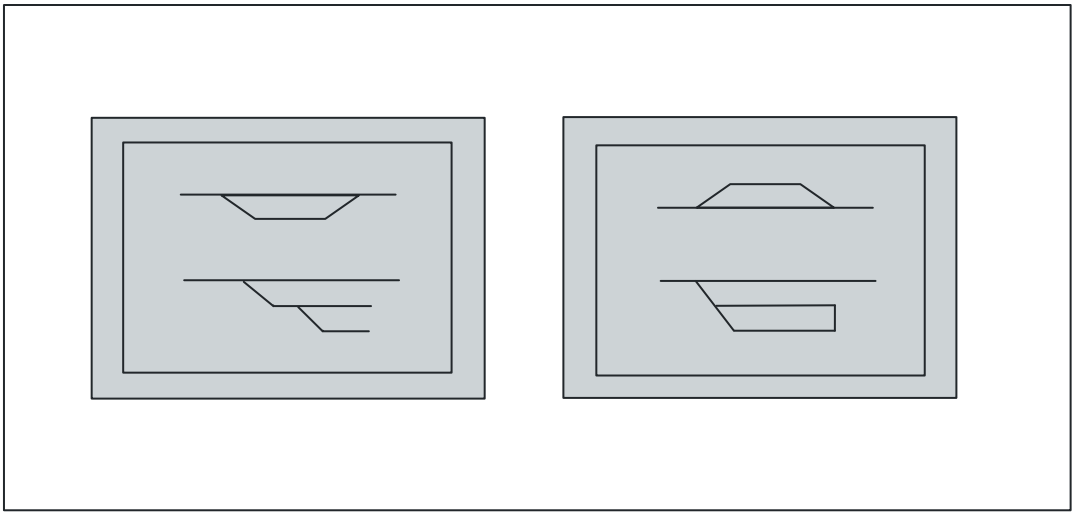

Figure 7 – Preferred sequence to draw tracks across screens for single control area

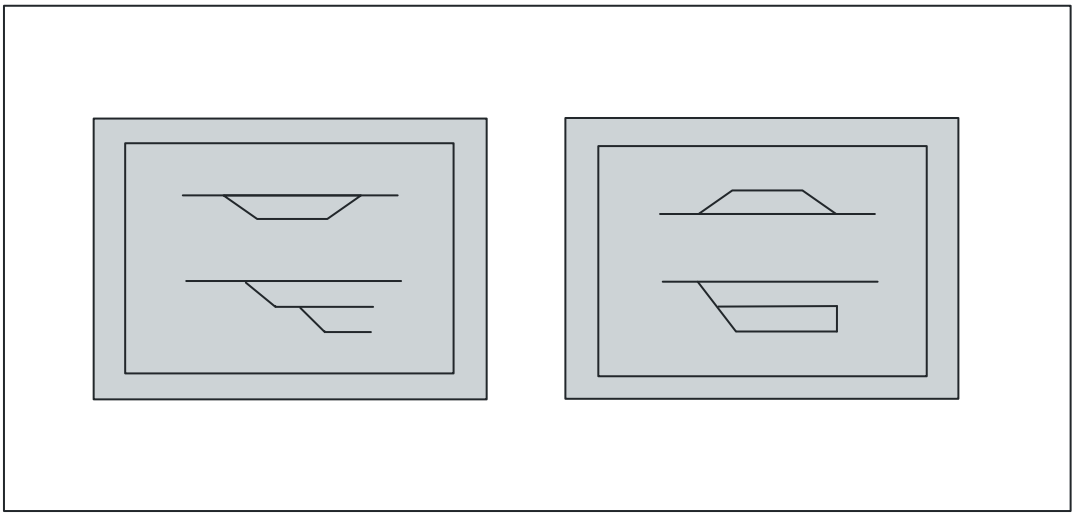

Figure 8 – Sequence not preferred to draw tracks across screens for single control area

Where the display is in a fixed position, the direction of the tracks as shown on the display should reflect the geographical direction of the tracks, particularly when the control centre is next to the railway line.

An alternative is for tracks to the north and west of Sydney to have the up direction towards the left, and tracks to the east and south of Sydney to have the up direction towards the right.

When multiple screens are used, they should be designed to be fitted adjacent to each other to produce a single continuous display. This is to reduce the gap between displays and ensure that they do not cause distorting electromagnetic interference to each other.

The display should show all individual track circuitry arrangements, signal names, point names, station names, alarms, warnings, track names, track circuit names, time release lights and any other miscellaneous indications. These names need not be continuously displayed or all displayed at the same time.

The display should be positioned so that it is fully visible to the signaller while they are performing other duties away from the display when a dedicated signaller is not employed.

D.3 Other types of displays

The TMS can be used by other users for different purposes. These displays present information in varying details, contents, coverage, and so on, for purposes including:

- overview workstation
- train graph
- maintenance
- timetable and crewing.

D.4 Limits of display area

The display should cover the approaches to the signaller's area of control.

Approaching train track occupancy indications adjacent to the area of control for each line should be provided, as a minimum, to include all tracks involved in the conditions of the approach locking of the first controlled signal.

In a departing direction, the track circuit indications should be provided, as a minimum, for all tracks up to and including the overlap track of the last controlled signal.

Appendix E Reliability, availability and maintainability

E.1 Overview

This appendix provides supporting information for failure and RAM concepts within the context of a TMS.

E.2 Failure

The main objective of the TMS is to manage signalling and train operations safely, reliably and efficiently every day of the year. If this objective cannot be met, it is assumed that the TMS is not fulfilling its requirements, and has a failure.

The TMS can be designed or configured such that failures in one section of the rail network do not have an impact on other sections of the rail network. However, a failure in part of the TMS can impact the safe, reliable and efficient signalling and train operations within other parts of the TMS. Therefore, a failure in any part of the TMS is assumed as a failure of the TMS as a whole.

Planned activities, with assessed and approved controls in place for safe and reliable signalling and train operations, should not be assumed as down time. Failures that activate disaster recovery site due to force majeure should not be assumed as a failure.

E.3 Availability

Any failure or unplanned maintenance activity that impacts on TMS functions for safe and reliable signal and train operations, contributes to determining the system availability.

If any train or signalling asset cannot be controlled or managed safely, reliably and efficiently within any area of control or line within the entire TMS due to any TMS failures, this period is assumed as an ‘unavailable’ period. The availability of the TMS is defined as an overall availability.

If differences between scheduled train behaviour and actual train behaviour are used for the TMS availability, then the differences that have occurred in the location and time period should be normalised in order to reduce or eliminate the randomness factor. For example, failure at a major junction may affect more trains at peak hours than a failure at the edge of the metropolitan rail area during the off-peak period.

E.4 Reliability

Similar to availability, any failure which impacts on the safe and reliable signalling and train operations, regardless of whether it concerns a small part of the TMS, or the whole, contributes to determining the system reliability. Reliability requirements are for the TMS as a whole.

E.5 Maintainability

Maintainability is determined by the extent to which a failed component or system is restored or repaired to a specified condition within a set maintenance period, according to prescribed procedures.

The maintainability requirements are for the whole TMS regardless of its configuration, such as redundancy configuration. Some configurations can fulfil the required availability and reliability requirements while having difficulty maintaining the subsystems.

The scope of the maintainability should be based on the impact of failures and potential exposure for multiple failures.

Appendix F Integrity

F.1 Overview

This appendix provides guidance on the basic integrity concept used in this document.

F.2 General integrity concept

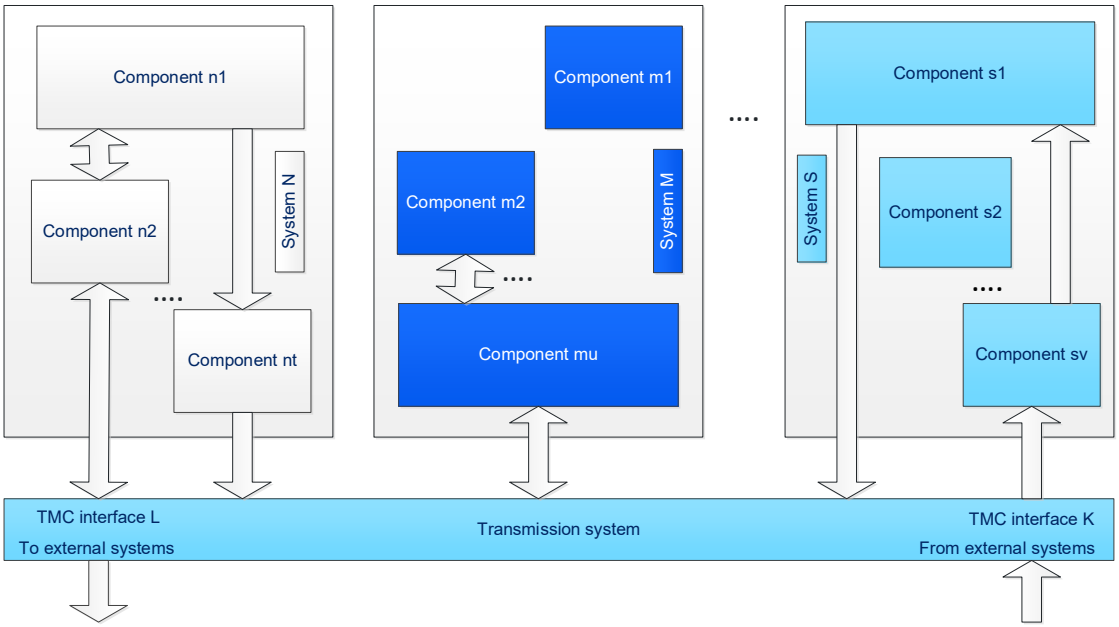

Figure 9 – Generic communication paths for information flow

The assumption is that raw information comes in the TMS via ‘TMS interface K’ and processed information goes out from ‘TMS interface L’ as shown in Figure 9. To ensure the information sent out has complete integrity, the TMS should monitor the following:

- integrity of the information coming in from ‘TMS interface K’
- integrity of each component on the information path including the transmission of information. For example, ‘comp sv’, ‘comp s1’, ‘comp mu’, ‘comp m2’ and so on, and their transmission integrity.

If any component has an integrity issue, all components after the failed component should lose their integrity and handle the situation as required, such as set all assets to their failed states. The failed component should have the capability to recover from its integrity lost state and establish its integrity. When this is done, the next component should be informed or be able to understand that the failed component has restored its integrity. This process should be followed for all components assuming that their integrity is also lost. For example, if the integrity of the component ‘m2’ is broken, the integrity of all components after that, such as ‘mu’, ‘n2’, ‘n1’ and ‘nt’, will also be broken.

Based on the system safety assessment and functions to be performed by the component, the following, as a minimum, should be performed by each component that is a part of the communication flow:

- detect integrity loss
- perform required process after the integrity loss to mitigate identified hazards
- inform other TMS components the component's current status along with other information required
- determine whether the integrity has been established
- if integrity is established, perform the required process to mitigate identified hazards
- when the component's integrity is established, inform other TMS components about the component's current status along with other information required.

The timing of receiving information according to the performance criteria is one of the major components of integrity concept. Delay or staleness of information determines the integrity of the component.

F.3 Generic threats

The following generic threats may be used to identify threats within the context of this document:

- Ineffectiveness – the function looks complete or effective; however, it actually does not perform its function under specific circumstances. For example, when a block is put on a track, the workstation can indicate that the track is blocked. The blocking operation that actually works on the routes can only stop the train running in one direction or in some routes.
- Effectiveness – the function looks complete and effective under all possible circumstances, such as when the track is blocked; all possible routes using that track are blocked, including the safety zone.

Appendix G Redundancy

G.1 Overview

This appendix provides guidance on the basic redundancy concept used in this document.

A number of technical solutions exist to support or improve the system's RAM requirements. Redundancy is one of the most widely used techniques for improving and supporting RAM requirements.

This appendix provides information on three different components of the TMS, as shown in Figure 1.

G.2 General information on redundancy

A TMS usually contains one software suite with more than one software package or executable and an associated configuration for a given rail network. As a result, an identical software and configuration runs on the redundant systems. If a problem exists within the software or configuration, both sides present the same outcomes, as the software failures are classified as systematic failures. That is, having a redundant system increases the system availability against random hardware failures, but does not improve the software and configuration availability. Systematic failures should be mitigated by the TAO using appropriate engineering techniques, processes, procedures and standards, such as those outlined in IEC 62279.

Consistency of the component's configuration within the system should be maintained, such as software and data versions. If a discrepancy exists, the TMS should be able to report the problem and not allow unsafe signalling and train operations.

Common cause failures should be taken into account, especially within the switching mechanisms.

A disaster recovery site should not be used for the redundant system because the site may be out of action for a long time owing to the nature of disaster. This would make the TMS vulnerable against failures.

G.3 Servers

The following are some of the possible server redundancy configurations:

- Cold standby – this configuration has an identical secondary unit to back up the primary unit. The secondary unit typically does not monitor the system and is not synchronised with the primary unit, but is only present as a spare. It takes time to bring the standby unit into a known and safe state. This makes it more challenging to reconcile synchronisation issues.

- Hot standby – in this configuration the secondary unit runs in parallel with the primary unit and they are completely synchronised. However, the secondary unit does not produce any controls. Switching techniques between the two units include third-party units or agreement between two units.
- Dual modular redundancy – this configuration uses two functional equivalent units, so that any one of the units can produce controls. The voter unit decides the unit that delivers controls. Reaching the majority vote is a challenge within this configuration, however, there are various solutions industry uses.
- N modular redundancy – this configuration has multiple units running in parallel. All units are highly synchronised and receive the same input information at the same time. Their output values are then compared and a voter decides on the output values to be used.

If the selected availability calculation technique indicates that the non-redundant system configuration can fulfil RAM requirements, then this configuration should be assumed as ‘cold standby’ configuration – if there is a backup unit.

G.4 Workstations

Workstations also require redundancy capability. However, because of the nature of their operation, such as the login process and user privileges, automatic changeover functionality cannot be used for workstations. The following two types of redundancy can be used instead:

- Spare workstation – a spare workstation proportional to the total number of workstations should be available.
- Redundant workstation – this is similar to the ‘hot standby’ configuration; however, there is no automatic changeover. The user can initiate the changeover process when it is required. The user should then provide the required credentials to get control of the redundant workstation.

Workstations cannot operate signalling and train operations safely, reliably and efficiently without enabling systems such as voice communication systems. Thus, when a user gets control of any workstation, including spare workstations, all associated enabling systems should also be available.

G.5 Other systems

As shown in Figure 1, redundancy of supporting systems can be determined and justified according to their functionality or available technologies. For example, the logging servers use commercially available mirroring systems to achieve fault tolerance.

Appendix H Disaster recovery site configurations

H.1 Overview

This appendix provides examples of disaster recover site configurations.

A disaster recovery site is normally located at a geographically different location and can be configured in a number of different ways. This appendix analyses the three configurations used in the TfNSW environment. Other configurations may be available based on the capabilities of the TMS. Also, some common support functions can be located as a third site for common access, such as logging and common configuration repositories.

H.2 General information on discovery recovery sites

Field systems and other systems can interface with all sites without any configuration changes. For example, interlocking or telemetry systems should be able to connect to the main site and disaster recovery site at the same time.

After the disaster recovery site becomes active, the main site becomes the new disaster recovery site. All requirements applicable to the disaster recovery site should apply to the main site, to maintain the availability requirements.

The disaster recovery site can be operational for an extended period of time depending upon the damage at the main site.

Both sites normally synchronise their dynamic information automatically, including restrictions, train information and alarms. If this mechanism is not available for some reason, such as not being active, or not implemented in the first place, another mechanism should be present to ensure that the site can operate trains safely and accurately. These mechanisms include the following as a minimum:

- loading the latest electronically recorded dynamic information manually, such as shared file systems
- entering the dynamic information manually.

The site should become active after the assessment and acknowledgement of the site configuration for the safe and reliable train operation.

Note: For the different site configurations represented in the figures below, the following apply:

- the component’s redundancy is not shown
- network connections and its redundancy are not shown
- support systems are part of each site

- field and other systems are not shown
- field and other systems are able to connect all sites.

H.3 Four sites configuration

As shown in Figure 10 all main site components and workstations are duplicated. They are located at four different sites. This configuration can provide the best system availability.

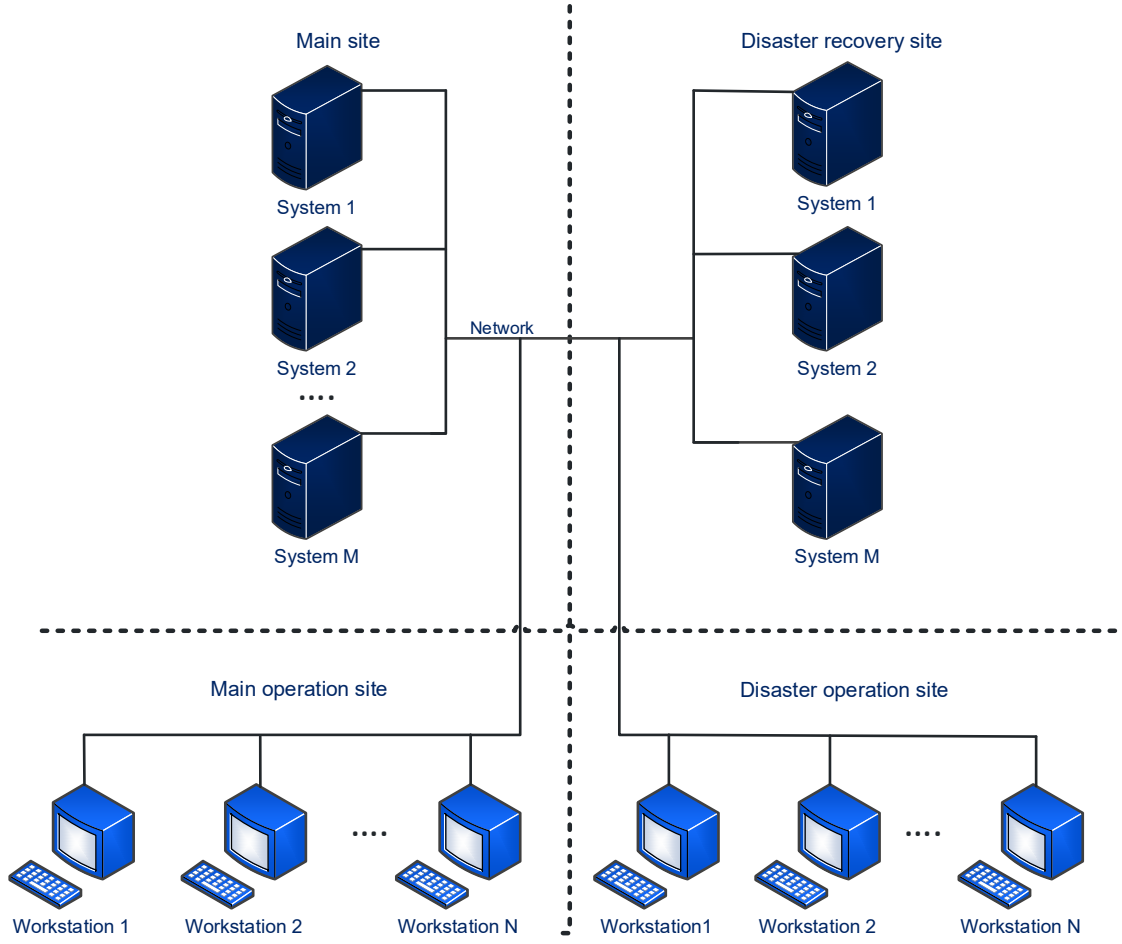

Figure 10 – Disaster recovery configuration model for four sites

H.4 Three sites configuration

As shown in Figure 11, all main site components are duplicated but workstations are not duplicated and they are located at different sites than servers. If there is a problem at the server sites, then the operation can continue without disruption or with very little or no disruption. If any disaster occurs at the operation site, then there will be no backup site and the disruption can continue until the operation site is restored.

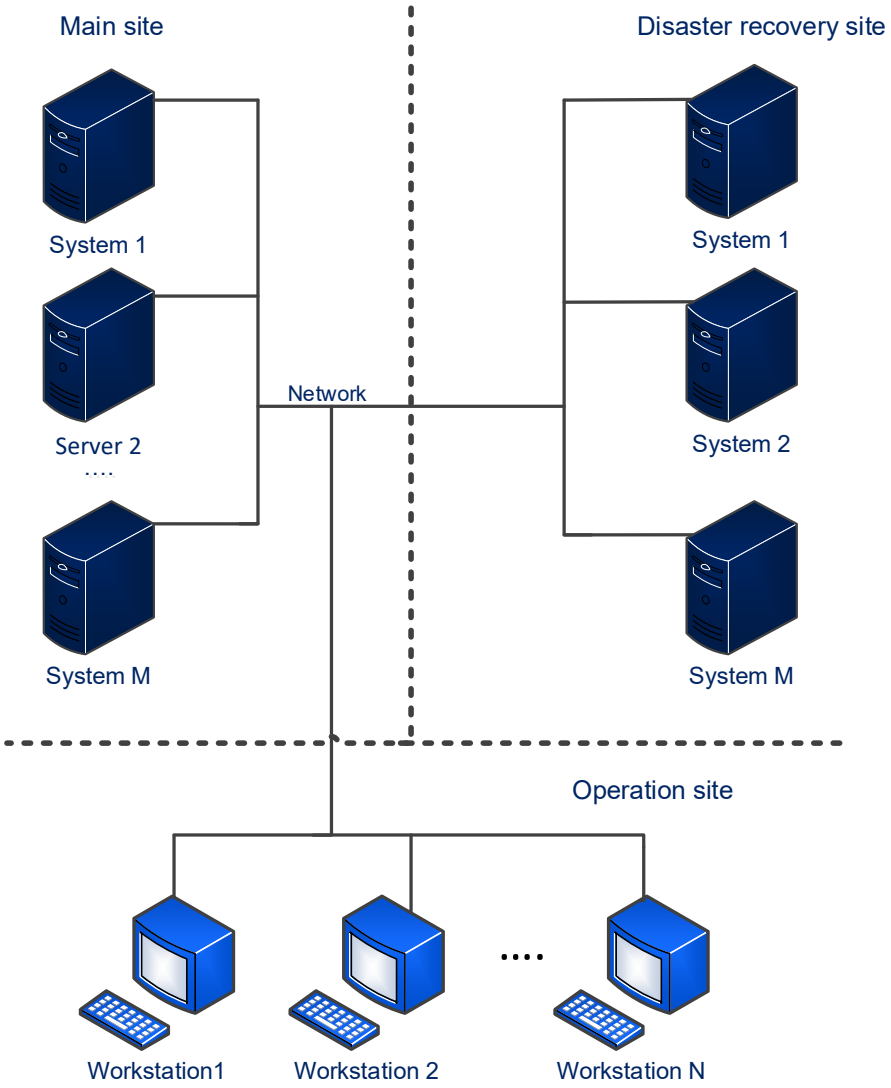

Figure 11 – Disaster recovery configuration model for three sites

H.5 Two sites configuration

As shown in Figure 12, all main site components and workstations are duplicated. In this configuration, workstations and servers are located at the same site. If any disaster occurs at one of the sites, then all workstations and servers at that site can become non-operational. However, there may be some impact on the operation since physical access to the disaster recovery site can take time.

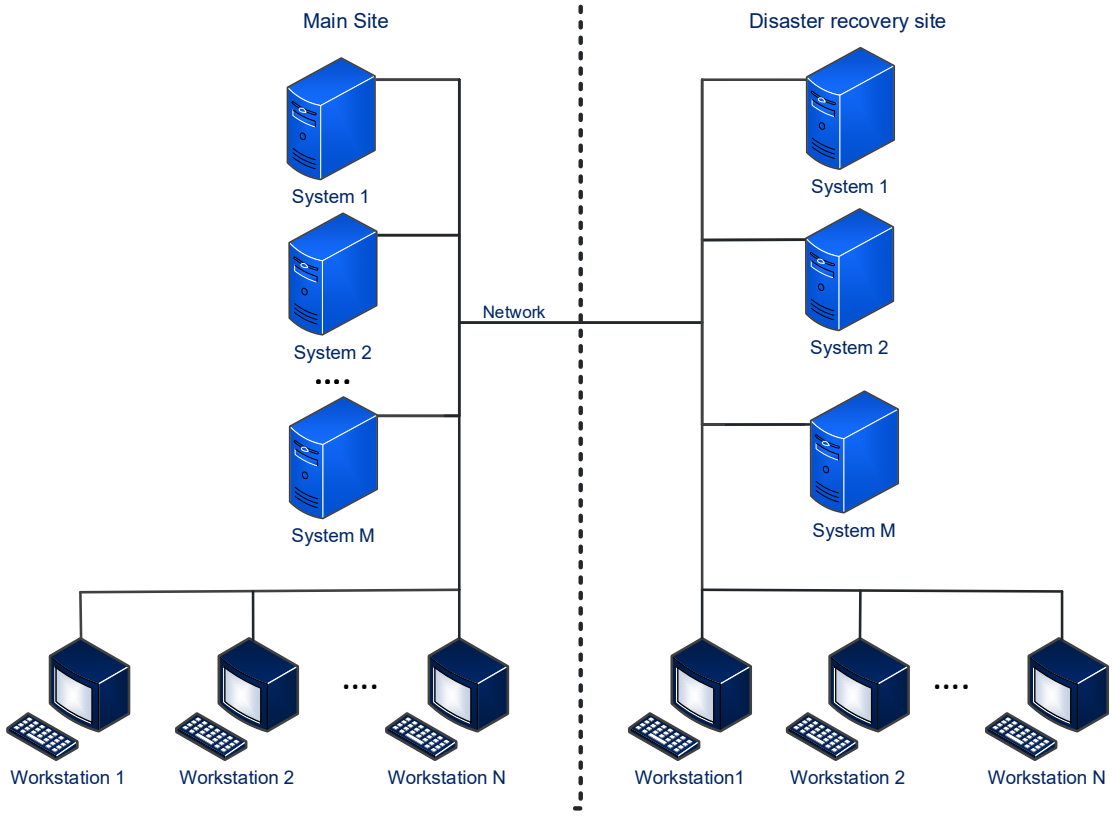

Figure 12 – Disaster recovery configuration model for two sites

Appendix I Logging and reporting

I.1 Overview

This appendix provides guidance on the basic logging and reporting concept used in this document.

I.2 Logging

The TMS uses real time information to manage signalling and train operations safely and reliably. These events are logged and they become historical information. They can be used for numerous purposes including:

- investigation
- fault analysis
- behavioural analysis
- information gathering
- learning
- teaching and training purposes.

Due to the physical size of logging over a long period of time, for example five years, it is expected that logs stored in a separate system for long-term storage may not be available online. In those instances, the time to access them can be quite lengthy. In most cases however, access requirements to historical logs are identified almost immediately after an incident or event. Therefore, the logging system should be capable of retaining the last 300 days of logs online for immediate access.

When the logs are transferred to long-term storage systems, the transfer should be done automatically without losing integrity.

Most events will be logged at the steady state, with logging activities increasing during disruptions such as starting or stopping components, or failures of internal or external systems. The logging system should have enough buffers for storing logs to compensate for any latency of permanent storage mediums like hard disks. Logging activities should not impact TMS performance and functionality.

The user should be able to add notes to records when log entries are presented in a report. Therefore, the logging system should be able to update the stored log entries without losing its integrity. The user should not be able to modify any existing log details including previously inserted notes. However, they should be able to add new notes to an existing log entry.

I.3 Reporting

The TMS should provide reporting functionality to the user, so they can manage signalling and train operations safely and reliably by accessing current and historical information.

The reporting system can be a commercial off-the-shelf product. The interfaces between reporting products and other systems, such as the logging system and the TMS, should not require any modifications to the reporting product's software or interfaces. This interface should be implemented by modifying the off-the-shelf product's configuration data.

The reporting system should be designed so that it can be part of the TMS, but also be run as a standalone system to provide a support and maintenance function tool. The number of report system clients should be unlimited without having an impact on TMS performances.

The following two types of reporting should be available:

- current information, such as trains in the system, or alarms
- historical information, extracted from logged events.

Report creation can be a two-step process. The first step is setting up the presentation and query parameters. These parameters can be saved as templates and be used by the user at a later time. The second step for historical reports is retrieving records from the logging system according to the set query.

A tabular format should be used for the report presentation. All parameters, such as column width, page layout, font, size and colour should be configurable, similar to a commercially available spreadsheet. Likewise, print, preview and save functions should be provided similar to a commercially available spreadsheet. For use of report outputs outside of the TMS environment, reports should be storable in commercially available formats such as a CSV.

The number of records provided by the logging system can be very large and take time to extract. The reporting system should be able to retrieve the records the user wants to view. For example, if the operator wants to view the last page of the record, the reporting system should not wait until all records are loaded.

Each user should have allocated secure storage space to fulfil the security requirements. Users should have complete freedom within the allocated storage space. Based on the security assessment outcomes, saved reports should be distributable outside the TMS through emails or portable storage devices such as a USB.