

ATTACHMENT 5: RAILCORP SECURITY REQUIREMENTS

The RailCorp Security Requirements comprise the following five (5) documents:

- Security Components Functional Specifications and Standards for Train Services Rollingstock – Security Components for Maintenance Centres – V1.2, 31 August 2005
- Part A: Fencing Functional Specification for RailCorp Maintenance Centres and Stabling Locations – V1.3.1, 10 July 2006
- Part B: Exterior Lighting Functional Standard for RailCorp Maintenance Centres and Stabling Locations – V1.1, 31 August 2005
- Part C: CCTV Functional Standard for RailCorp Maintenance Centres and Stabling Locations – V1.2, 7 June 2006
- Part D: Access Control Functional Specification for RailCorp Maintenance Centres and Stabling Locations – V1.2, 16 August 2005



Security in Confidence

Security Components Functional Specifications and Standards

For

**Train Services – Rollingstock
Division**

Maintenance Centres



RailCorp

Uncontrolled when printed

31 August, 2005. V1.2

A handwritten signature in the bottom right corner of the page.

Security in Confidence

Security Components for Maintenance Centres

Document Control

The current status of this document is shown below.

Title	Security Components for Maintenance Centres.	
Long title	Security Components Functional Specifications and Standards for Train Services – Rollingstock Division Maintenance Centres.	
Version	Version 1.2	Approved
Label	Security in Confidence	
Effective date	31 August, 2005	
Controlled by	RailCorp Security Division	
Endorsed By	Paul Passmore – A/General Manager Security Division	

Security in Confidence

Security Components for Maintenance Centres

Table of Contents

Document Control.....	ii
Table of Contents.....	iii
Revision History.....	iii
Disclaimer.....	iii
1. Introduction.....	1
1.1 Purpose.....	1
1.2 Document Conventions.....	2
1.3 References.....	2
2. Overall Description.....	2
2.1 Security Performance Outcomes.....	2
2.2 Security Components.....	4
2.3 Maintenance Centre Categorisation.....	4
2.4 Operating Environment.....	5
3. Extraordinary Items.....	7
3.1 Design and Implementation Constraints.....	7
4. Other Non-functional Requirements.....	7
4.1 Safety Requirements.....	7
4.2 Security Requirements.....	7
5. Other Requirements.....	7
Appendix A: Issues List.....	8

Revision History

Name	Date	Reason For Changes	Version
D. Wolff	11/08/05	Replace 'VMD' and references, to, 'Electronic Intruder Detection', plus periodic amendments.	V1.1
D. Wolff	31/08/05	Re-format.	V1.2

Disclaimer

RailCorp has used its best endeavours to ensure that the content, layout and text of this document is accurate, complete and suitable for its stated purpose.



Security in Confidence

Security Components for Maintenance Centres

1. Introduction

1.1 Purpose

The purpose of the series of documents is to nominate the required security components that a Train Services Rollingstock Division Maintenance Facility should have as a minimum security standard.

These requirements are to apply to:

- All new facility constructions.
- Upgrades to existing facilities.

These facilities are locations that are owned and / or managed by Train Services Rollingstock Division and provide RailCorp with the following:

- A location for stabling of trains not in service.
- A location where train presentation activities can occur.
- A location where storage of valuable assets or refuelling may be carried out.
- A location where major and minor maintenance of trains can be carried out.

These standards are to apply to any locations where one or more of these activities occurs as part of regular RailCorp activities.

These standards are to be applied as a minimum. Individual sites specific requirements above these standards will need to be reviewed and addressed on a case by case basis.

Exemptions to components of these standards may be submitted to Security Division for consideration after being subject to a formal evaluation.

Security in Confidence

Security Components for Maintenance Centres

1.2 Document Conventions

EID. Electronic Intruder Detection. This is technology that can detect an intruder by way of electronic sensors providing input into hardware and software based systems that then notify or alarm of an intruder at a particular location, point or input. This type of system may have a number of different types of proven technologies interfaced to provide a specified performance outcome. This could include VMD or other forms of detection.

VMD. Video Motion Detection. This is technology that is interfaced with a CCTV system that can alarm by exception to an object moving within the field of view of a CCTV camera. This technology is sometimes referred to as *Object Video Detection*.

1.3 References

1. *Stabling Yards (Maintenance Centres) Security – Value / Risk Management Report. November 2004.*
2. *The Australian Government National Security web site www.nationalsecurity.gov.au*
3. *RailCorp Safety division*
<http://intranet.railcorp.nsw.gov.au/Safety/Safety%20Reform%20Agenda/index.htm>
4. *RailCorp Train Services Group*
<http://intranet.railcorp.nsw.gov.au/Operating%20Groups/Train%20Services/Divisions/index.htm>

2. Overall Description

2.1 Security Performance Outcomes

2.1.1 The facilities shall have a security fence surrounding, where ever possible, 100% of the site. This fence shall provide an effective security and safety barrier for the facility.



Security in Confidence

Security Components for Maintenance Centres

2.1.2 All new facilities shall, where ever possible, provide sufficient clearance for the installation of a second fence within the perimeter of the primary fence, providing a sterile security zone. This space shall not be less than 3 meters in width. This fence is to be of a like standard to the Fencing Functional Specification outlined in Part A.

2.1.3 The facilities shall have high intensity security lighting. This lighting shall illuminate the perimeter and the key egress locations along this perimeter to a minimum prescribed lux level.

2.1.4 The facilities shall have a CCTV security system integrated with the existing RailCorp system. This CCTV system is to primarily provide security surveillance along the perimeter of the site as well as key egress locations and be able to be utilised by on site security personnel.

2.1.5 The facilities shall have an integrated electronic access control system. This system shall use an identified common control medium. This access control shall, where ever possible, eliminate a keyed locking interface.

2.1.6 The open train entry of the facilities shall have either :

- Train gates integrated with track signalling infrastructure [See Part A paragraph 3.10] or,
- EID (Electronic Intruder Detection) and an effective alarm and response capability, which shall include a physical human security element.

2.1.7 The installation of the security components shall, where ever possible, avoid construction adjacent structures that will reduce the performance outcomes of the security upgrade.

Security in Confidence

Security Components for Maintenance Centres

2.1.8 All exposed fixtures and fittings of the security components shall be of a vandal resistant design and shall not reduce the vandal resistance of any other security component. These shall include but be limited to fasteners, brackets and conduits.

2.1.9 All exposed fixtures and fittings of the security components shall have a corrosion resistance of not less than the agreed life cycle of the individual security component, and its installation shall not reduce the corrosion resistance of any other security component.

2.1.10 All components shall be designed, constructed and installed to meet or exceed all applicable Australian Standards.

2.2 Security Components

2.2.1 See Part A: Fencing Functional Standard.

2.2.2 See Part B: Exterior Lighting Functional Standard.

2.2.3 See Part C: CCTV Functional Standard.

2.2.4 See Part D: Perimeter Access Control Functional Standard.

2.3 Maintenance Centre Categorisation

These standards are to be a minimum for all categories of Train Services Rollingstock Division locations. Individual locations may have further specific security requirements.



Security in Confidence

Security Components for Maintenance Centres

2.4 Operating Environment

Rollingstock Division is part of Train Services Group, RailCorp. Their facilities are located throughout the Sydney metropolitan area and provide:

- Maintenance of the electric and diesel passenger fleet to ensure safe and reliable operations.
- Management of engineering standards and maintenance planning for the electric and diesel passenger fleet.
- Provision of engineering and maintenance support for Rollingstock capital works program.
- Develop and deliver projects making up the Rollingstock capital works program.

Rollingstock Division has a number of smaller sites in regional areas for refuelling purposes. They also provide stabling facilities for the fleet in these locations that allows for Cleaning and Train Preparations to take place.

The major PFM sites cover an extensive area, largely covered by rail traffic roads, Maintenance Storage Buildings, Brake Inspection Roads, Inspection facilities and Administration Buildings. Most of the sites being relative flat with concrete sections bounding the inspection buildings and 'Ballast' covering the majority of open track corridors within the maintenance facility. The site infrastructure provides for access pathways for both pedestrian and road vehicles around and within the facility.

The facility has a large number of roads (rail tracks) leading into the various workshops. These roads converge into an open neck at one end of the facility of usually 3 or 4 roads. Of a night the trains will be stored, or stabled, in the maintenance centres, this could number up to 200 railcars. There is significant electrical overhead wiring for train running within the facilities. These over heads are carrying 1500 volts for train operation. There is train running operations (Shunting) within the yards at most times of the day and night. There is a primary road vehicle entrance that is manned by a contract security service.

Security in Confidence

Security Components for Maintenance Centres

The facilities have car parking for staff and visitors. The facilities can have up to 200 staff on site at any one time. The facilities have staff on site 24 hours a day seven days a week including public holidays. There is a contracted security guards presence on site 24 hours a day seven days a week including public holidays.

The Maintenance Facility Environment provides for a variety of security, Operational needs and OH&S requirements, including:

- Car Parking for staff and visitors.
- 24 hour operation, 365 days per year.
- Housing and storage of major plant and equipment.
- Storage facilities for inventory.
- Fuel Storage Tanks and Environmental Treatment plants.
- Perimeter Fencing with access points.
- Lighting throughout the site.
- And in some locations CCTV camera's.
- Onsite 24hr security guards.

The security threats to the sites include graffiti vandalism and trespass. The current RailCorp security alert level is Medium (as at 01/03/2005). The level of national counter-terrorism alert is Medium (as at 01/03/2005). Medium is defined by the National Security web site (www.nationalsecurity.gov.au) as: "There is a medium risk of a terrorist attack in Australia".

RailCorp is committed as part of its Provisional Accreditation under the Rail Safety Act, to develop and implement an extensive Safety Reform Agenda. This Agenda covers all areas of operation across the Corporation and requires the full understanding and commitment of managers, supervisors and employees at all levels.

Through the effective implementation of this Agenda, RailCorp will develop the basis for a sustainable safety culture, which is required, if the Corporation is to deliver its objective of safe, clean, secure and reliable passenger rail transport.



Security in Confidence

Security Components for Maintenance Centres

It is anticipated that the security components shall assist Rollingstock Division in meeting its current and future security and safety requirements.

3. Extraordinary Items

3.1 Design and Implementation Constraints

Concessions to a component of these security measures may be required under limited circumstances. These shall be submitted to Security Division for review and on a case by case basis. Validation by Security Division will be subject to an alternative submission meeting the specified performance outcomes for the security component.

4. Other Non-functional Requirements

4.1 Safety Requirements

The installation shall be designed, installed and commissioned in accordance with, or where ever possible exceed, all applicable RailCorp and Australian safety standards.

4.2 Security Requirements

The installation shall be designed, installed and commissioned to allow the user group to functionally comply with their business units individual RailCorp Security Alert Procedures.

5. Other Requirements

5.1.1 Locations that have effluent storage and treatment facilities shall have, where possible, a security and safety fence surrounding the specific facility that meets the performance outcomes set out in Part A Fencing Functional Standard.

Security in Confidence

Security Components for Maintenance Centres

5.1.2 Locations that have diesel fuel storage facilities shall have, where possible, a security and safety fence surrounding the specific facility that meets the performance outcomes set out in Part A Fencing Functional Standard.

5.1.3 Locations that have other users based within the perimeter of the facility shall have, where possible, a physical barrier defining the boundary between the two groups. Ideally this barrier shall be consistent with the performance outcomes set out in Part A Fencing Functional Standard.

Appendix A: Issues List

All concerns and issues are to be listed and addressed and where required listed in the revision history and a new version issued.



12



Part A:

Fencing Functional Standard for RailCorp Maintenance Centres and Stabling Locations



RailCorp

A handwritten signature in the bottom right corner of the page.

Security in Confidence

Fencing Functional Standard

Document Control

The current status of this document is shown below.

Title	CCTV Functional Standard	
Long title	Part A: Fencing Functional Standard for RailCorp Maintenance Centres and Stabling Locations.	
Version	Version 1.3.1	Approved
Label	Security in Confidence	
Effective date	10 July, 2006	
Controlled by	RailCorp Security Division	
Endorsed By		

Security in Confidence

Fencing Functional Standard

Table of Contents

Document Control ii
Table of Contents iii
Revision History iv
Disclaimer iv
1. Introduction 1
 1.1 Purpose 1
 1.2 Document Conventions 1
 1.3 References 2
2. Overall Description 2
3. Perimeter Fence 2
 3.1 Fence mesh 3
 3.2 Vertical Fence Posts 4
 3.3 Horizontal Fence Rails 4
 3.4 Topping 5
 3.5 Under Fence Treatment 5
 3.6 Pedestrian Gates (Perimeter) 6
 3.7 Pedestrian Gates (Primary Staff Entry) 7
 3.8 Pedestrian Turnstiles (Primary Staff Entry) 8
 3.9 Vehicle Gates (Perimeter) 9
 3.10 Vehicle Gates (Primary Road Vehicle Entry Point) 10
 3.11 Train Gates 11
4. External Interface Requirements 12
 4.1 Electronic Access Control 12
 4.2 Hardware Interfaces 12
 4.3 Software Interfaces 12
 4.4 Communications Interfaces 13
5. Other Non-functional Requirements 13
 5.1 Performance Requirements 13
 5.2 Safety Requirements 13
 5.3 Security Requirements 13
6. Extraordinary Items 14
 6.1 Design and Implementation Constraints 14
7. Standards 15
Appendix A: Issues List 15

Security in Confidence

Fencing Functional Standard

Revision History

Name	Date	Reason For Changes	Version
D. Wolff	11/08/05	Replace 'VMD' and references, to, 'Electronic Intruder Detection', plus periodic amendments.	V1.1
D. Wolff	10/04/06	Review of fence fabric aperture dimensions. Review of post types. Review of footing dimensions.	V1.2
D. Wolff	07/07/06	Review of fence construction. Addition of horizontal fence rail performance criteria.	V1.3
D. Wolff	10/07/06	Periodic review.	V1.3.1

Disclaimer

RailCorp has used its best endeavours to ensure that the content, layout and text of this document is accurate, complete and suitable for its stated purpose.

Security in Confidence

Fencing Functional Standard

1. Introduction

1.1 Purpose

The purpose of the fence is to provide RailCorp Train Services Group and Station Operations train stabling and storage locations with the following:

- A defined and known perimeter.
- An effective physical security and safety barrier that is difficult to breach without the use of tools.

1.2 Document Conventions

The term '*Posts*' can also refer to a similar vertical support component of a fence.

The term '*resistance to scaling*' refers to a component or series of components not providing handholds, footholds or steps for an individual to use the fence as a ladder to gain illegitimate entry into the perimeter.

The term '*Plinth*' refers to a built up concrete fixture beneath a fence that restricts, or ideally eliminates, the ability to burrow under the fence. Also the '*Plinth*' shall restrict, or ideally eliminate, the ability for erosion to occur immediately beneath the fence and provide a space for a person to gain illegitimate entry into the perimeter.

The '*Shunters Hut*' is the small office type building located at or near the neck of the facility. This is where shunting operations can be controlled.

'*On time running*' is a performance measure used by RailCorp for train services running to the scheduled timetables.

'*Life cycle*' of the fence shall be nominally 25 years.



Security in Confidence

Fencing Functional Standard

1.3 References

1. *Australian Standard. AS 1725 – 2003 titled. "Chain – link fabric security fences and gates."*
2. *Australian Standard AS/NZS 3014 – 2003 titled. "Electrical Installations – Electric Fences."*
3. *Australian Standard AS/NZS 3016 – 2002 titled. "Electrical Installations – Electric Security Fences."*
4. *Specification for High Security Cantilever Gates. Griffen Pty. Ltd.*

2. Overall Description

The perimeter fence is to provide a number of functions to RailCorp Passenger Fleet Maintenance Division:

- Define a boundary.
- Be an effective safety barrier from train movements.
- Be an effective deterrent to potential intruders.
- Be an effective defence against potential intruders.
- Provide an effective delay to potential intruders.

3. Perimeter Fence

The perimeter shall be 100% of the boundary of the facility and have gates and shall conform to standards guidelines set by RailCorp Infrastructure Division with respect to the following:

- Structures around train running lines.
- Structures around Over Head Wiring.
- ESC510 – Perway fencing – High Security Fence

The perimeter fence shall have a nominal life cycle of 25 years. The fence shall maintain the performance criteria outlined in this document for this nominated life cycle.

The perimeter fence shall, where possible, be built not less than 3 meters away from a structure or object that may provide a 'natural ladder' that could allow a breach of the perimeter.

Security in Confidence

Fencing Functional Standard

3.1 Fence mesh

3.1.1 The fence panel mesh shall be of a design that is highly resistant to scaling.

3.1.2 The fence panel mesh shall be of a design that significantly increases the effort required to damage or breach the perimeter through the mesh.

3.1.3 The panels shall be treated to resist corrosion, and in addition shall have a finish that displays opacity sufficient for security surveillance, preferably black powder coat or similar.

3.1.4 The design shall facilitate or minimise the time / cost required to repair, remove, install, refit new fence mesh panels in situ.

3.1.5 Fence panels shall be of a 'Welded mesh' type product.

3.1.6 The wire mesh of these panels shall be not less than 4mm in diameter.

3.1.7 The aperture in the mesh pattern of these panels shall have dimensions of not more than 75mm in the horizontal plane by 13mm in the vertical plane.

3.1.8 The panels should be not less than 2.4 metres in height.

3.1.9 The panels should be attached to steel box section posts, I-Beam, UC Beam, or Uneven U-section (or vertical supports of similar engineering strength) with not less than eight (8) fittings per panel. All exposed fasteners including screws, nuts and bolts shall be of a tamper proof, security fastener design.



Security in Confidence

Fencing Functional Standard

3.1.10 The method of attachment of the mesh should be able to maintain the performance criteria of the fence for the life cycle of the fence, including corrosion resistance.

3.2 Vertical Fence Posts

3.2.1 The posts (or similar vertical support components) shall be treated to resist corrosion, and in addition shall have a finish that displays opacity sufficient for security surveillance, preferably black powder coat or similar.

3.2.2 The fence posts shall be of a design that is highly resistant to scaling.

3.2.3 The posts shall be of a box section of not less than 100mm by 100mm, or I-Beam, UC Beam, or Uneven U-section of similar engineering strength and function.

3.2.4 All posts shall be supported in a concrete footing not less than 450mm in diameter. The post depth shall be and not less than 900mm deep into the ground and surrounded by this concrete footing.

3.2.5 In differing ground conditions, the post depths shall be of a suitable depth to provide the required support and performance for the life cycle of the fence.

3.3 Horizontal Fence Rails

3.3.1 The fence shall be installed with a top and a bottom rail. This rail should provide added strength and support to the fence and shall be attached to the vertical fence posts and the fence mesh.

Security in Confidence

Fencing Functional Standard

3.3.2 The rails shall be treated to resist corrosion, and in addition shall have a finish that displays opacity sufficient for security surveillance, preferably black powder coat or similar.

3.3.3 The method of attachment of the top and bottom rail should be able to maintain the performance criteria of the fence for the life cycle of the fence, including corrosion resistance.

3.4 Topping

3.4.1 The fence structure shall be topped with stainless steel concertina short barb tape of not less than 550mm in height.

3.4.2 The topping shall be highly resistant to corrosion and be of a corrosion resistance equal to the fence and suitable for the life cycle of the fence.

3.4.3 The topping shall be attached with fasteners that are of a tamper proof, security fastener design.

3.4.4 The fence topping shall be of a design that significantly increases the effort required to damage or breach the perimeter through the topping.

3.5 Under Fence Treatment

3.5.1 The fence shall have a concrete 'plinth' along the length of the perimeter fence.

3.5.2 The 'plinth' shall not be greater than 60mm below the fence mesh structure, and ideally butt against the lower edge of the fence.

Security in Confidence

Fencing Functional Standard

3.5.3 The 'plinth' shall extend not less than 200mm either side of the perimeter fence centre line.

3.5.4 The footing depth shall be of sufficient depth as to strongly resist erosion for the life cycle of the fence and shall be not less than 200mm deep.

3.5.5 The fence 'plinth' shall be of a design that significantly increases the effort required to damage, breach, or burrow under the fence through the 'plinth'.

3.6 Pedestrian Gates (Perimeter)

3.6.1 The construction of the gates shall meet the requirement of the perimeter fence set out in the document. [See sections 3.1-3.3]

3.6.2 The gates shall be of a design that allows their functional integration with the proposed electronic access control system. [See Part D]

3.6.3 The gate, and gate support posts and structure, shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.6.4 If the gates are manual operated and hinged, all perimeter pedestrian gates leaf hinge points shall have greasable bearings in at least two (2) locations and shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.6.5 If the gates are manual operated and hinged, all perimeter pedestrian gates shall have an automatic close device fitted that is designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

Security in Confidence

Fencing Functional Standard

3.6.6 If the gate is a power driven electronically actuated sliding gate, it shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.6.7 A 'plinth' type construction shall be installed beneath the gate. [See section 3.4] and this component shall be installed so to not present a trip hazard to breach any standards or regulations.

3.7 Pedestrian Gates (Primary Staff Entry)

3.7.1 The construction of the gates shall meet the requirement of the perimeter fence set out in the document. [See sections 3.1-3.3]

3.7.2 The gates shall be of a design that allows their functional integration with the proposed electronic access control system. [See Part D]

3.7.3 The gate, and gate support posts and structure, shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.7.4 If the gates are manually operated and hinged, all pedestrian gate leaf hinge points shall have greasable bearings in at least two (2) locations and be of a suitable design fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.7.5 If the gates are manual operated and hinged, all perimeter pedestrian gates shall have an automatic close device fitted that is designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.



Security in Confidence

Fencing Functional Standard

3.7.6 If the gates are power driven electronically actuated sliding gates, it shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.7.7 A 'plinth' type construction shall be installed beneath the gate. [See section 3.4] and this component shall be installed so to not present a trip hazard to breach any standards or regulations.

3.8 Pedestrian Turnstiles (Primary Staff Entry)

3.8.1 Shall maintain the construction integrity of the fence.

3.8.2 Shall only allow one person at a time pass through the turnstile.

3.8.3 Shall be full height and allow safe egress of a person with a 'RailCorp' backpack to pass through safely.

3.8.4 The turnstiles shall be of a design that allows their functional integration with the proposed electronic access control system. [See Part D]

3.8.5 The pedestrian turnstile, and pedestrian turnstile support posts and structure, shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.8.6 A 'plinth' type construction shall be installed beneath the gate. [See section 3.4] and this component shall be installed so to not present a trip hazard to breach any standards or regulations.

Security in Confidence

Fencing Functional Standard

3.8.7 Where a pedestrian turnstile is installed, an emergency egress gate shall be placed as close as practicable to the turnstile. This emergency gate shall have controls that restrict its use to emergency conditions only. Further, the construction of the emergency gate shall meet the requirement of the perimeter fence set out in the document. [See sections 3.1-3.3]

3.9 Vehicle Gates (Perimeter)

3.9.1 The construction of the gates shall meet the requirement of the perimeter fence set out in the document. [See sections 3.1-3.3]

3.9.2 The gates shall be of a design that allows their functional integration with the proposed electronic access control system. [See Part D]

3.9.3 The gate, and gate support posts and structure, shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.9.4 The topping of the vehicle gates should be consistent with the perimeter fence [Section 3.3], however, a flat loop type topping can be used if a sliding gate is installed.

3.9.5 If the gates are manually operated and hinged, all vehicle gate leaf hinge points shall have greasable bearings in at least two (2) locations per leaf and be of a suitable design fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.9.6 If the gates are power driven electronically actuated sliding gates, they shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

Security in Confidence

Fencing Functional Standard

3.9.7 A 'plinth' type construction shall be installed beneath the gate. [See section 3.4] and this component shall be installed so to not present a trip hazard to breach any standards or regulations.

3.10 Vehicle Gates (Primary Road Vehicle Entry Point)

3.10.1 The construction of the gates shall meet the requirement of the perimeter fence set out in the document. [See sections 3.1-3.3]

3.10.2 The gates shall be of a design that allows their functional integration with the proposed electronic access control system. [See Part D]

3.10.3 The gate, and gate support posts and structure, shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.10.4 The topping of the vehicle gates should be consistent with the perimeter fence [Section 3.3], however, a flat loop type topping can be used if a sliding gate is installed.

3.10.5 If the gates are power driven electronically actuated hinged gates, all vehicle gate leaf hinge points shall have greasable bearings in at least two (2) locations per leaf and be of a suitable design fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.10.6 If the gates are power driven electronically actuated sliding gates, they shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

Security in Confidence

Fencing Functional Standard

3.10.7 A 'plinth' type construction shall be installed beneath the gate. [See section 3.4] and this component shall be installed so to not present a trip hazard to breach any standards or regulations.

3.11 Train Gates

If train entry / exit locations are to be gated for an identified facility the following should apply:

3.11.1 The gates shall be integrated with train signalling infrastructure.

3.11.2 Manual electronic over-ride should be located within the 'Shunters Hut'.

3.11.3 Manual mechanical over-ride should be located at the gated point and this mechanical operation should be able to be operated by one person within occupational health & safety guidelines.

3.11.4 The construction of the gates shall meet the requirements of the perimeter fence set out in the document. [See sections 3.1-3.3]

3.11.5 Should have mechanisms that upon initial failure the gate 'opens' to ensure no impact on 'on-time running' of trains into or out of the Maintenance Centre.

3.11.6 The gate, and gate support posts and structure, shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.11.7 The topping of the train gates should be consistent with the perimeter fence [Section 3.3], however, a flat loop type topping can be used if a sliding gate is installed.



Security in Confidence

Fencing Functional Standard

3.11.8 If the gates are power driven electronically actuated hinged gates, all train gate leaf hinge points shall have greasable bearings in at least two (2) locations per leaf and be of a suitable design fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.11.9 If the gates are power driven electronically actuated sliding gates, they shall be fit for purpose, in so far as to be designed, constructed and installed suitably for a 'high use' location for the life cycle of the fence.

3.11.10 A 'plinth' type construction shall be installed beneath the gate. [See section 3.4] and this component shall be installed so to not present a trip hazard to breach any standards or regulations.

4. External Interface Requirements

4.1 Electronic Access Control

4.1.1 Pedestrian access control - See Part D.

4.1.2 Vehicle access control - See Part D.

4.2 Hardware Interfaces

4.2.1 See Part D.

4.3 Software Interfaces

4.3.1 See Part D.

Security in Confidence

Fencing Functional Standard

4.4 Communications Interfaces

4.4.1 See Part D.

5. Other Non-functional Requirements

5.1 Performance Requirements

5.1.1 The fence shall have provision for retro-fitting of electric fencing. The ability to retro-fit this type of product shall not degrade the corrosion resistance of the fence nor shall it affect the performance of the fence or any of its components.

5.1.2 The fence shall have provision for retro-fitting of electronic intruder detection technology. The ability to retro-fit this type of product shall not degrade the corrosion resistance of the fence nor shall it affect the performance of the fence or any of its components.

5.1.3 The installation shall be designed, installed and commissioned in accordance with, or where ever possible exceed, all applicable Australian technical standards.

5.2 Safety Requirements

The installation shall be designed, installed and commissioned in accordance with, or where ever possible exceed, all applicable Australian safety standards.

5.3 Security Requirements

The installation shall be designed, installed and commissioned to allow the user group to functionally comply with their business units individual Security Alert Procedures.



Security in Confidence

Fencing Functional Standard

6. Extraordinary Items

6.1 Design and Implementation Constraints

6.1.1 Alternatives to 'Welded Mesh' for the perimeter fence may be required under limited circumstances. These shall be submitted to Security Division for review on a case by case basis. As a minimum standard, the alternative fence type must meet the performance criteria set out in paragraphs 3.1.1 – 3.1.5.

6.1.2 Alternate pedestrian gate constructions may be required under limited circumstances. These shall be submitted to Security Division for review on a case by case basis. As a minimum standard, the alternative pedestrian gate type must meet the performance criteria set out in paragraphs 3.5.2 – 3.5.6.

6.1.3 Alternate vehicle gate constructions may be required under limited circumstances. These shall be submitted to Security Division for review on a case by case basis. As a minimum standard, the alternative vehicle gate type must meet the performance criteria set out in paragraphs 3.8.2 – 3.8.7.

Security in Confidence

Fencing Functional Standard

7. Standards

All constructions shall meet all applicable RailCorp / Rail Infrastructure Corporation standards, guidelines and policies. Of these documents, particular interest should be drawn to the following:

Rail Infrastructure Corporation

Transit Space Policy. Ref C 2101.

Transit Space Standards. Ref C 2103.

Application of Kinematic Envelope. Ref C2105.

Base Operating Standards for Clearances. Ref C 2107.

Metallic Lineside Fencing in Electrified Areas. Ref C 4501.

Low Voltage Installation Earthing. Ref EP 12 10 00 21 SP.

Buildings and Structures Under Overhead Lines. Ref EP 12 10 00 22 SP.

RailCorp:

Safety Standard – Construction Work. Ref A10-08-N112.

Appendix A: Issues List

All concerns and issues are to be listed and addressed and where required listed in the revision history and a new version issued.

Part B:

Exterior Lighting Functional Standard for RailCorp Maintenance Centres and Stabling Locations



RailCorp

A handwritten signature in black ink, appearing to be "Jm", is located in the bottom right corner of the page.

Security in Confidence

Exterior Lighting Functional Standard

Document Control

The current status of this document is shown below.

Title	Exterior Lighting Functional Standard	
Long title	Part B: Exterior Lighting Functional Standard for RailCorp Maintenance Centres and Stabling Locations.	
Version	Version 1.1	Approved
Label	Security in Confidence	
Effective date	31 August, 2005	
Controlled by	RailCorp Security Division	
Endorsed By	Paul Passmore – A/General Manager Security Division	

Security in Confidence

Exterior Lighting Functional Standard

Table of Contents

Document Control ii
Revision History iii
Disclaimer iii
1. Introduction 1
 1.1 Purpose 1
 1.2 References 1
2. Overall Description 1
3. System Features 2
 3.1 Lighting Array 2
 3.2 Levels of Light 3
 3.3 Lighting Poles 3
 3.4 Cabling and Conduit 4
4. External Interface Requirements 4
 4.1 User Interfaces 4
5. Other Non-functional Requirements 5
 5.1 Performance Requirements 5
 5.2 Safety Requirements 5
 5.3 Security Requirements 5
6. Standards 5
Appendix A: Issues List 6

Revision History

Name	Date	Reason For Changes	Version
D. Wolff	31/08/05	Periodic amendments.	V1.1

Disclaimer

RailCorp has used its best endeavours to ensure that the content, layout and text of this document is accurate, complete and suitable for its stated purpose.



Security in Confidence

Exterior Lighting Functional Standard

1. Introduction

1.1 Purpose

The purpose of the lighting is provide adequate illumination of the site to allow effective surveillance by:

- Contract Security Personnel.
- CCTV systems.
- Facility staff.

1.2 References

1. *Australian Standard. AS / NZS 1158.6 : 2004. Lighting for roads and public spaces. Part 6: Luminaries.*

2. Overall Description

The lighting array for the maintenance facilities is to provide high intensity security lighting that should enhance the security outcomes for the site.

The lighting should enhance the opportunity for natural surveillance and also enhance the functional performance of the CCTV system.

The system should provide this performance under all weather conditions typical for the geographical location of the facility.

It is anticipated that the lighting array shall have a life cycle of not less than 25 years.

The installation shall meet, or exceed, all applicable Australian Standards.

Security in Confidence

Exterior Lighting Functional Standard

3. System Features

The lighting array should comprise of both high level pole mounted flood type lighting and low level lighting illuminating the perimeter fence line.

The lighting will be connected to the power available within the site and should interface with existing infrastructure.

3.1 Lighting Array

3.1.1 High level lighting to provide lighting between the standing train sets at a light level suitable for CCTV performance.

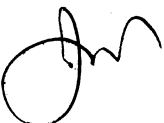
3.1.2 Low level lighting along the entire length of the perimeter fence. This lighting should illuminate not less than 5 metres either side of the fence. This lighting should not impact on any of the performance criteria of the perimeter fence.

3.1.3 The colour of the light must allow accurate colour rendering suitable for CCTV surveillance, and assist in the compliance with the requirements of the Evidence Act (NSW) 1995.

3.1.4 All components of the lighting array shall be highly resistant to vandalism.

3.1.5 All luminary components and their housings shall have a durable corrosion resist finish that shall resist corrosion and weathering from the elements for the life cycle of the lighting array.

3.1.6 The lighting array shall be designed to be energy efficient whilst meeting all other performance criteria.



Security in Confidence

Exterior Lighting Functional Standard

3.1.7 The life cycle for the luminaries shall meet AS/NZS 1158.62004 of 20 years, or ideally exceed, the minimum standard for the type of luminaries selected and provide a life cycle of 25 years.

3.1.8 All fitting used in the lighting array shall be of a design fit for purpose and installed accordingly.

3.1.9 All fitting used in the lighting array shall be effectively sealed to strongly resist the ingress of dust, insects and water.

3.2 Levels of Light

3.2.1 Perimeter fence shall be illuminated to a minimum of **50 lux**.

3.2.2 Carparks shall be illuminated to a minimum of **50 lux**.

3.2.3 Primary pathways shall be illuminated to a minimum of **150 lux**.

3.2.4 Primary pedestrian entry locations shall be illuminated to a minimum of **150 lux**.

3.2.5 Primary road vehicle entry locations shall be illuminated to a minimum of **150 lux**.

3.3 Lighting Poles

3.3.1 All poles shall meet local area wind loadings.

3.3.2 All poles shall meet local government ordinances.

Security in Confidence

Exterior Lighting Functional Standard

3.3.3 All poles shall be designed and installed so to allow efficient maintenance of the lighting array with minimal impact on regular operations within the maintenance facility.

3.3.4 All lighting poles shall have a durable corrosion resist finish that shall resist corrosion and weathering from the elements for the life cycle of the lighting array.

3.4 Cabling and Conduit

3.4.1 All cabling and conduit shall meet or exceed Australian Standards.

3.4.2 All cabling shall be enclosed in a type of conduit, and, where this is above ground the conduit shall be of a highly vandal resistant design affixed with tamper resistant security type fasteners.

3.4.3 All conduits shall be highly resistant to corrosion and be of a corrosion resistance equal to the lighting array and suitable for the life cycle of the lighting array.

4. External Interface Requirements

4.1 User Interfaces

4.1.1 The lighting shall have the ability to be switched automatically by either turning on and off at prescribed light levels or by prescribed times. This is to be determined on a site specific basis by consultation with end users.

4.1.2 The lighting shall have the ability to be switched on or off manually, on site, by non-trade qualified persons, when required.



Security in Confidence

Exterior Lighting Functional Standard

5. Other Non-functional Requirements

5.1 Performance Requirements

The installation shall be designed, installed and commissioned in accordance with, or where ever possible exceed, all applicable Australian technical standards.

5.2 Safety Requirements

The installation shall be designed, installed and commissioned in accordance with, or where ever possible exceed, all applicable RailCorp and Australian safety standards.

5.3 Security Requirements

The installation shall be designed, installed and commissioned to allow the user group to functionally comply with their business units individual RailCorp Security Alert Procedures.

6. Standards

All constructions shall meet all applicable RailCorp / Rail Infrastructure Corporation standards, guidelines and policies. Of these documents, particular interest should be drawn to the following:

Rail Infrastructure Corporation:

Transit Space Policy. Ref C 2101.

Transit Space Standards. Ref C 2103.

Application of Kinematic Envelope. Ref C2105.

Base Operating Standards for Clearances. Ref C 2107.

Metallic Lineside Fencing in Electrified Areas. Ref C 4501.

Low Voltage Installation Earthing. Ref EP 12 10 00 21 SP.

Buildings and Structures Under Overhead Lines. Ref EP 12 10 00 22 SP.

RailCorp:

Safety Standard – Construction Work. Ref A10-08-N112.

Security in Confidence

Exterior Lighting Functional Standard

Appendix A: Issues List

All concerns and issues are to be listed and addressed and where required listed in the revision history and a new version issued.

A handwritten signature in black ink, consisting of a stylized 'J' followed by a cursive 'm'.

Security in Confidence

Part C:

CCTV Functional Standard for RailCorp Maintenance Centres and Stabling Locations



RailCorp

Uncontrolled when printed

7 June, 2006. V1.2

A handwritten signature in the bottom right corner of the page.

Security in Confidence

CCTV Functional Standard

Document Control

The current status of this document is shown below.

Title	CCTV Functional Standard	
Long title	Part C: CCTV Functional Standard for RailCorp Maintenance Centres and Stabling Locations.	
Version	Version 1.2	Approved
Label	Security in Confidence	
Effective date	7 June, 2006	
Controlled by	RailCorp Security Division	
Endorsed By	Paul Passmore – General Manager Security Division	

Security in Confidence

CCTV Functional Standard

Table of Contents

Document Control	ii
Table of Contents	iii
Revision History	iii
Disclaimer	iv
1. Introduction	1
1.1 Purpose.....	1
1.2 Document Conventions.....	1
1.3 References.....	1
2. Overall Description	2
3. CCTV System Features	2
3.1 Cameras.....	3
3.2 Housings	3
3.3 Cabling and Conduit.....	3
3.4 Coverage of Facilities.....	4
3.5 Future Provisions	4
4. External Interface Requirements	5
4.1 User Interfaces.....	5
4.2 Hardware Interfaces.....	5
4.3 Software Interfaces	5
4.4 Communications Interfaces.....	6
5. Other Non-functional Requirements	6
5.1 Performance Requirements	6
5.2 Security Requirements.....	6
6. Standards	7
Appendix A: Issues List	7

Revision History

Name	Date	Reason For Changes	Version
D. Wolff	31/08/05	Periodic amendments.	V1.1
D. Wolff	15/05/06	Periodic amendments.	V1.1.1
D. Wolff	07/06/06	Periodic amendments – Revision of CCTV coverage performance requirements.	V1.2

Security in Confidence

CCTV Functional Standard

Disclaimer

RailCorp has used its best endeavours to ensure that the content, layout and text of this document is accurate, complete and suitable for its stated purpose.

Security in Confidence

CCTV Functional Standard

1. Introduction

1.1 Purpose

The purpose is to provide Passenger Fleet Maintenance locations with an effective security closed circuit television system (CCTV) that:

- Can provide all weather, day night capability.
- Has an interface into both local and off-site monitoring.
- Has off-site digital recording and in excess of 14 days of storage of the recorded data.
- Has coverage of the perimeter and key egress locations.
- Has an interface with the local electronic access control system.
- Has provision for the addition of other technologies like Video Motion Detection (VMD).

1.2 Document Conventions

CCTV. Closed Circuit Television. Now more broadly a functional electronic surveillance system using video images combined with digital processing and storage.

VMD. Video Motion Detection. Technology that interfaces with CCTV to detect the changes in the field of view of an image that in turn can alarm or notify a user through a number of methods.

1.3 References

1. *RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation. Part C.*
2. *SANDIA REPORT. Evaluation of Commercially Available Exterior Digital VMD's.*
3. *A National approach to CCTV. National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism (2006) Consultative Draft version 17a.*
4. *Australian Standard AS 4806.2 – Closed Circuit Television (CCTV) – Application Guidelines.*



Security in Confidence

CCTV Functional Standard

2. Overall Description

The CCTV system is to provide the Maintenance Centres with a comprehensive CCTV coverage of its perimeter fence line and the key entry / exit locations along this perimeter.

The system is to provide this coverage under all light and weather conditions.

The system shall interface with the existing RailCorp CityRail stations CCTV system. It shall also provide a local interface for local management and response. The system shall have the ability to interface with the local access control system.

The system shall have provision for expansion. This expansion could include the addition of extra cameras providing enhanced coverage, and, future technologies that could include Video Motion Detection.

Video Motion Detection could be required in the first initial installation dependant on site specific requirements. VMD shall interface with the CCTV and provide an alarm only on the detection of a person, and not alarm when an approved track vehicle enters the camera field of vision.

The system shall meet or exceed the requirements of the RailCorp contract titled 'RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation.' Of particular note, the performance specifications set out in Part C of this document.

The installation shall meet, or exceed, all applicable Australian Standards.

3. CCTV System Features

The system is to provide surveillance of the perimeter of the identified passenger fleet maintenance locations.

Security in Confidence

CCTV Functional Standard

3.1 Cameras

3.1.1 The camera and lens combination shall meet all performance requirements of CCTV contract RFP No. 2004/1503.

3.1.2 The cameras shall operate 24 hours a day, 7 days per week under light conditions ranging from sunlight to maintenance centre lighting.

3.2 Housings

3.2.1 The camera and lens housings shall meet all performance requirements of CCTV contract RFP No. 2004/1503.

3.2.2 Housings shall be placed at a height to minimise vandalism and unauthorised adjustment or tampering.

3.3 Cabling and Conduit

3.3.1 All cabling and conduit shall meet or exceed Australian Standards.

3.3.2 All cabling shall be enclosed in a type of conduit, and, where this is above ground the conduit shall be of a highly vandal resistant design affixed with tamper resistant security type fasteners.

3.3.3 All conduits shall be highly resistant to corrosion and be of a corrosion resistance equal to the lighting array and suitable for the life cycle of the lighting array.



Security in Confidence

CCTV Functional Standard

3.4 Coverage of Facilities

3.4.1 Each pedestrian egress point must have 100% coverage and must meet the Identification image requirements of the Australian Standard AS 4806.2 – Closed Circuit Television (CCTV) – Application Guidelines.

3.4.2 Each vehicle egress point must have 100% coverage and must be able to identify the number plate of a stopped vehicle in the field of view and also meet the identification image requirements of the Australian Standard AS 4806.2 – Closed Circuit Television (CCTV) – Application Guidelines.

3.4.3 Not less than 95% of the perimeter of maintenance centres shall be covered and shall meet the Intruder Detection image requirements of the Australian Standard AS 4806.2 – Closed Circuit Television (CCTV) – Application Guidelines.

3.4.4 Not less than 95% of the perimeter of stabling yards shall be covered and shall meet the Crowd Control image requirements of the Australian Standard AS 4806.2 – Closed Circuit Television (CCTV) – Application Guidelines.

3.4.5 There shall be CCTV coverage between the standing sets stabled within the maintenance centre and stabling yard and shall meet the Crowd Control image requirements of Australian Standard AS 4806.2 – Closed Circuit Television (CCTV) – Application Guidelines.

3.5 Future Provisions

3.5.1 The system shall have provision for the addition of Video motion Detection (VMD) technology to be added to the system. This shall not impact or degrade the performance of the CCTV system.

Security in Confidence

CCTV Functional Standard

3.5.2 The system shall have provision for the VMD to provide an alarm output to a number of locations to be determined by the users requirements.

3.5.3 The system shall have the provision for additional cameras to be added to the system.

4. External Interface Requirements

4.1 User Interfaces

4.1.1 The main entry point security guard station shall have facility to view the CCTV system and select cameras to be viewed. This interface shall comply with the user requirements and performance criteria detailed in CCTV contract RFP No. 2004/1503.

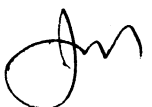
4.1.2 The installation shall be designed, installed and commissioned to allow full functionality with the specifications of RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation. Part C.

4.2 Hardware Interfaces

The installation shall be designed, installed and commissioned to allow full functionality with the specifications of RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation. Part C.

4.3 Software Interfaces

The installation shall be designed, installed and commissioned to allow full functionality with the specifications of RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation. Part C.



Security in Confidence

CCTV Functional Standard

4.4 Communications Interfaces

4.4.1 The installation shall be designed, installed and commissioned to allow full functionality with the specifications of RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation. Part C.

4.4.2 The installation shall be designed, installed and commissioned to allow full functionality with the access control system outlined in 'Perimeter Access Control Functional Specification - Part D'.

5. Other Non-functional Requirements

5.1 Performance Requirements

5.1.1 The installation shall be designed, installed, commissioned and maintained in accordance with, or where ever possible exceed, all applicable Australian technical standards.

5.1.2 The installation shall be designed, installed, commissioned and maintained in accordance with the specifications of RFP No. 2004 / 1503. CCTV and Help Point System – Upgrade and Operation Safety Requirements.

5.1.3 The installation shall be designed, installed and commissioned in accordance with, or where ever possible exceed, all applicable RailCorp and Australian safety standards.

5.2 Security Requirements

The installation shall be designed, installed and commissioned to allow the user group to functionally comply with their business units individual RailCorp Security Alert Procedures.

Security in Confidence

CCTV Functional Standard

6. Standards

All constructions shall meet all applicable RailCorp / Rail Infrastructure Corporation standards, guidelines and policies. Of these documents, particular interest should be drawn to the following:

Rail Infrastructure Corporation:

Transit Space Policy. Ref C 2101.

Transit Space Standards. Ref C 2103.

Application of Kinematic Envelope. Ref C2105.

Base Operating Standards for Clearances. Ref C 2107.

Metallic Lineside Fencing in Electrified Areas. Ref C 4501.

Low Voltage Installation Earthing. Ref EP 12 10 00 21 SP.

Buildings and Structures Under Overhead Lines. Ref EP 12 10 00 22 SP.

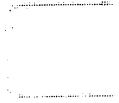
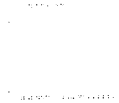
RailCorp:

Safety Standard – Construction Work. Ref A10-08-N112.

Appendix A: Issues List

All concerns and issues are to be listed and addressed and where required listed in the revision history and a new version issued.





RailCorp

Part D:

Access Control Functional Specification

Version 1.2 Endorsed DRAFT

Prepared by

Security Division - RailCorp

16/08/2005

Security-in-Confidence

Table of Contents

Table of Contents	ii
Revision History	iii
Disclaimer	iii
1. Introduction.....	1
1.1 Purpose.....	1
1.2 Document Conventions.....	1
1.3 Reference Material and Related Document	2
1.4 Overall Description	2
2. System Features	3
2.1 System Capabilities.....	3
2.2 Functional Capabilities	4
2.3 Design Considerations	7
3. External Interface Requirements.....	11
3.1 User Interface.....	11
4. Hardware Interface.....	14
4.1 Credential Readers	14
4.2 Electric/Electromechanical Locking Devices	15
4.3 Request to Exit.....	15
4.4 Emergency Breakglass Units	16
4.5 Associated Devices	16
4.6 Software Interface	16
4.7 Specific to an alarm detection system:.....	17
4.8 Communication Interface	18
5. Non-Functional Requirements.....	18
5.1 Performance Requirements	18
5.2 Safety Requirements.....	22
5.3 Security Requirements.....	22
6. Standards	24
Appendix A: Issues List.....	24

Revision History

Name	Date	Reason For Changes	Version
D. Wolff	05/04/05	Re-format of document to reflect current presentation standards, plus periodic amendments.	V1.1
D. Wolff	16/08/05	Re-format of document to reflect current presentation standards, plus periodic amendments.	V1.2

Disclaimer

RailCorp has used its best endeavours to ensure that the content, layout and text of this document is accurate, complete and suitable for its stated purpose.

1. Introduction

1.1 Purpose

The purpose of the perimeter access control is to:

1.1.1 Improve the working condition of RailCorp employees by maintaining a safe, secure and reliable working environment through ensuring only authorised users of worksites gain access.

1.1.2 Assist with administration and day to day operation of a working site.

1.1.3 Minimise the opportunity for unauthorised or accidental entry onto RailCorp grounds.

1.1.4 Minimise the risk of injury or death to trespassers onto RailCorp grounds.

1.1.5 Minimise the cost and disruption to rolling stock through reducing damage from criminal activity.

1.2 Document Conventions

1.2.1 Reference has been drawn from Australian Standards and other relevant documents previously written for similar functional access control systems.

1.2.2 Abbreviations used in this document are spelt out in words with the abbreviation following.

Security-in-Confidence

1.2.3 "The system" refers to the complete access control system including all functional and operational properties.

1.2.4 The "Contractor" refers to the company or person who has been awarded a contract with RailCorp for the completion of project works related to this document.

1.3 Reference Material and Related Document

- Australian Standard AS 2201 (all additions and subsequent updates)
- Australian Standard AS 3745 – 2002 Emergency Control Organisation and Procedures for Buildings, Structures and Workplaces
- Australian Standard AS 2052 – Metallic Conduit and Fittings
- Australian Standard AS 2053 – Non Metallic Conduit and Fittings
- Australian Standard AS 3000 – Australian Wiring Rules
- Building Code of Australia
- Inclosed Lands Protection Act 1901 No. 33 and its amendments
- Rail Corp Documents
- Part A: Fencing Functional Specification
- Part C: CCTV Functional Specification
- Information Technology and Telecommunications Division Policy No. __ Wireless LAN Policy
- IT & T Procedures No 024 – Software Standard
- Cabling near Overhead Cables and Tunnels

1.4 Overall Description

The use of access control devices includes the coordinated use of physical security measures such as existing building structures, security fencing and associated gates, mechanical and electromechanical locking systems, as well as the applied use of strategic



lighting, volumetric detection including electronic beams, closed circuit television systems and the ability to detect and respond appropriately to the notification of an intrusion.

The implementation of some of these measures is separately specified in the document reference list above in Part 1.3. Any proposal for access control shall review the entire existing infrastructure and propose any upgrade or additions necessary to meet the desired outcome performance.

2. System Features

2.1 System Capabilities

2.1.1 Be capable of deterring a concerted attack using tools and equipment as determined through a risk assessment of each individual site.

2.1.2 Detect any attempt and/or actual attack to perimeter intrusion equipment and /or actual intrusion into the protected zone.

2.1.3 Report by exception, the location of the incident clearly and if applicable, identify the offender.

2.1.4 Deny the ability for unauthorised access to identified high-risk zones within the protected area, as established through a risk assessment of the site.

2.1.5 Have the capability to assist but never impede upon the administration and day to day operation of the site.

2.2 Functional Capabilities

2.2.1 Record access and egress of all authorised users, and support any existing "Smart Card" application currently implemented, or proposed by RailCorp.

2.2.2 Operate in conjunction with barrier fencing and gates as well as other electronic surveillance measures.

2.2.3 Be compatible with, and fully integrated to other existing RailCorp security equipment including, where applicable, the use of "Smart Card" technology.

2.2.4 Report on exception activity that would normally be reportable by such equipment,

2.2.5 Identify the specific location of a reportable occurrence.

2.2.6 Be simple to operate and operate in accordance with the functional design and intended outcome.

2.2.7 Shall have provision for remote and local control of equipment as well as the capability to interface with wireless fixed and handheld devices.

2.2.8 Access control shall cover and be effective to 100% of the boundary of the facility and shall conform to standards and guidelines set out by RailCorp Infrastructure Division with respect to the following:

- Structures around train running lines
- Structures around overhead wiring



Security-in-Confidence

2.2.9 Smooth and rapid management of all vehicular traffic accessing or exiting a controlled area shall be considered essential.

2.2.10 The equipment must be self monitoring and capable of self-diagnostics and reporting. This includes but is not limited to alarm, fault, tamper, forced door, door held open, system box tamper, power supply conditions where relevant and system activity outside pre-designated time periods.

2.2.11 System shall be programmable for a user-adjustable time period for each access point for Door-Held-Open condition. The act of opening the door shall initiate the door timer, and also cause the immediate reset of the door lock.

2.2.12 The operating mode of access controlled doors shall indicate all possible states. (locked, unlocked, or controlled - Door strike shall monitor and report Door Open Too Long (DOTL), forced door and its open / close status).

2.2.13 The system shall provide for automatic lock/unlock of access controlled doors on a scheduled basis using time zones or during an emergency through the use of a "Hot Key" function.

2.2.14 The system shall have the ability to globally lock or unlock the entire system.

2.2.15 The system shall, in the event of an evacuation of the site, provide a record of all users within the controlled area. This feature shall provide the capability of tracking personnel movement in the event of an emergency. During the emergency, all personnel within a risk area are expected to evacuate and are required to badge at a reader outside the risk area. This shall produce real-time

Security-in-Confidence

monitoring, printed or on-screen, as to whom may be still in the affected area. This information can be used to direct search and rescue operations. One or more areas within a plant or facility can be designated as Muster Zones.

2.2.16 Where an elevator exists within the facility, the system shall have the ability to control elevators. History of elevator activity shall be maintained in electronic or printed form, including the card that accessed the elevator, and the floor that was accessed.

2.2.17 The system shall be capable of controlling the number of personnel/cardholders that are allowed within a controlled area, thereby allowing large facilities to manage specific areas more easily. For example, a controlled substance room can be monitored, and the system will be able to report and display in real time how many and which cardholders are within the area at any given time.

2.2.18 The system should have the capacity to interface with administrative systems for recording and managing all users within a controlled area.

2.2.19 The software package shall provide for global and local anti-passback, and also provide a facility for soft anti-passback (ie. allowing entry following an anti-passback violation but still report and log the violation). The system shall also be capable of providing timed anti-passback at individual readers, and the time shall be capable of being selected by the operator.

2.2.20 All access requests, both authorised and denied, shall be sent to the host for storage and annunciation, as required, recording the door/access point identity, cardholder number, time and whether access was attempted or gained.

Security-in-Confidence



Security-in-Confidence

2.2.21 The system shall have the capacity to interface with intelligent (Smart) card technology, as well as all existing RailCorp access control systems.

2.2.22 The system shall be capable of automatic backups to an alternative medium or alternative location at prearranged time spans.

2.2.23 The mechanical infrastructure must be such that any parts accessible without triggering an alarm must be tamper resistant using tamper resistant fasteners.

2.2.24 A general fire alarm connection is to be made between the base building fire panel and the access control system. This interface should not be terminated at either end, but clearly marked. The trip is not to release doors unless otherwise approved.

2.3 Design Considerations

This Section is intended to specify the general requirements for a fully automated and integrated access control system, including, but not limited to the following functions and capabilities:

2.3.1 The system shall be designed using open architecture and shall provide for automated access control at designated areas and doors. The installed system must be readily expandable via various communications methods including hardwire, wireless or other hybrid methods.

2.3.2 Recording, instantaneous display and retrieval of system activity for a minimum of 12 months including time stamping, activity, user group, user and resultant action from any activity.

Security-in-Confidence

- 2.3.3 Detection and reporting of alarm, trouble, forced door, door held open conditions detected by cameras, sensors, door strikes and/or other devices.
- 2.3.4 The completed system shall be readily interfaced with existing RailCorp equipment and infrastructure as well as being readily available "off the shelf" industry standard equipment and using industry standard protocols over an industry standard Ethernet local or wide area network (LAN/WAN).
- 2.3.5 Built systems must support standard file servers, printers, other hardware as well as interfacing readily with standard commercial databases.
- 2.3.6 All electronic equipment must be capable of resisting high voltage surges created through close lightning strikes. Lightning arresters shall be installed at each cable terminating to any vulnerable electronic device.
- 2.3.7 The equipment must be capable of full functionality during all weather conditions. This includes heavy fog and rain, thunderstorms, extreme temperatures, the range of visible light (spectrum) and if requested, outside the visible light spectrum.
- 2.3.8 Any computing devices shall be capable of efficiently managing all computerised functions with no perceivable delay to the operator of the system.
- 2.3.9 Networked intelligent controllers shall be capable of utilising both central processing and true distributed processing technology. Local processing shall be based on the full local storage of cardholders, access groups, time zones, input and output information in controller RAM.

Security-in-Confidence

2.3.10 The network must use standard secure industry protocols, encryption or some other tiered access and protection capabilities.

2.3.11 The proposed product must support all commercial card readers, door contact switches, request-to-exit devices, code pads, biometric devices and electric locks.

2.3.12 The system design shall consider egress in the event of a fire. The system shall be designed so that wherever possible, minimum numbers of doors are unlocked in the event of fire alarm activation. (Use of electric mortice locks, free handle access door furniture etc will reduce the need to unlock doors)

2.3.13 The contractor shall provide the latest product model and software version available from each manufacturer at the time of installation. No beta version or test software products will be accepted. All proposed and provided equipment and/or products shall be from the specified and approved manufacturers only, unless previously approved.

2.3.14 All installed access control gates and doors must be configured to ensure compliance with all emergency egress requirements as detailed in the Australian Building Code.

2.3.15 The use of wireless technology devices in lieu of hard-cabled devices will be considered.

2.3.16 Be configurable to accept a fire relay input to allow appropriate system action in case of a fire system emergency.

Security-in-Confidence

2.3.17 Emergency release or failsafe locking systems shall be installed on all critical exit routes or where there is no alternative exit route.

2.3.18 No proprietary or "exclusive vendor products" will be considered.

2.3.19 The equipment must have a minimum expected lifecycle of at least 10 years with an equipment and installation defect free full replacement warranty period of at least 18 months.

2.3.20 The system shall not readily date or become redundant. The expected life cycle must be provided with limited replacement guarantees based on a lineally diminishing time period ('N - 1' where 'N' is the expected life cycle).

2.3.21 All equipment will be new and comprise well-known brand items from reputable manufacturers and be supplied by established Australasian distributors with a substantial New South Wales parts holdings and New South Wales technical support.

2.3.22 Uniformity of type and manufacture of electronics, fittings and accessories shall be preserved throughout the whole installation.

2.3.23 Where applicable, any upgraded software released for any installed equipment within the warranty period shall be automatically supplied at no further expense to RailCorp. Outside of this warranty period, notification of all software upgrades must be communicated to RailCorp for their consideration of procurement.



2.3.24 The equipment must operate without significantly impeding normal staff and authorised visitor tasks throughout the site.

3. External Interface Requirements

3.1 User Interface

The proposed systems must be capable of:

3.1.1 Full graphic map/floor plan display (GUI) capability with selectable coloured alarm icons and indicators;

3.1.2 An audible alarm or voice activated notification.

3.1.3 An alarm descriptive text and operator instructions.

3.1.4 Allow an operator to lock and unlock doors and place them in a controlled mode, directly from the graphics display.

3.1.5 It shall provide for the acknowledgment of alarm conditions and the masking and unmasking of alarm points directly from the graphic display.

3.1.6 It shall provide facilities for graphically displaying the boundaries of individual security areas programmed into the system, and shall allow the operator to mask and unmask these security areas from the graphic display. This action shall automatically cause all alarm devices within these security areas to be masked or unmasked.

Security-in-Confidence

3.1.7 The system shall possess a visual indication of the status of the proximity and reader.

3.1.8 The system shall be programmable for tiered priority access.

3.1.9 System must be able to detect and exclude allocation of multiple cards to the same person.

3.1.10 System to be capable of manually disabling cards at any time without the requirement to delete the card as well as being able to subsequently re-enable the card at a later time.

3.1.11 Programming of cards shall be as flexible as possible to include multiple security levels, timed zones, limiting functionality (eg only arm or disarm).

3.1.12 The system shall provide the capability of setting a parameter of days whereby cards will be automatically disabled if they are not used at all for access for the preset number of days (ie. 30 days, 60 days, 90 days etc.). Any card can be subsequently re-enabled at any time.

3.1.13 Each cardholder shall be specified with access authority levels, number of security areas and groups of security areas, each security area comprised of one or more card reader controlled door.

3.1.14 Card records shall include the entry of activation and deactivation dates to provide or the automatic enabling and expiring of the card record.

Security-in-Confidence



Security-in-Confidence

3.1.15 The system shall provide for the designation of certain calendar days to be holidays, with special access privileges and system activity to be specified for those days.

3.1.16 All system controlled electric locks shall be capable of being unlocked via operator command at a workstation as well as by request-to-exit devices.

3.1.17 The software shall be capable of providing for the recall of system historical transactions for a period of 12 months.

3.1.18 Data searching parameters shall be provided as a menu driven feature. Searches shall include card activity, cardholder by card number and name, card reader activated, security area accessed, alarm point activated, alarm category, date and time period.

3.1.19 The software shall provide report creation capabilities which offers search, organise and sorting according to the operator instructions, and have the ability to print, spool, or display a full report at a printer or client workstation.

3.1.20 All operator commands and database entry functions shall be completely menu driven with plain English text and prompts, and the system shall provide on-screen Help information.

3.1.21 All access to the operator system functions shall require, at a minimum, the entry of a valid user identity and password. (A password must be used by the operator, manager, or administrator to access the system, access authority for each password is completely user-selectable by individual menu selection).

Security-in-Confidence

3.1.22 The system cannot be interfaced to other RailCorp information technology systems without the consent of RailCorp.

3.1.23 Training shall include the operation and appropriate end user programming functions of the intruder detection, access control and headend software systems.

3.1.24 Training material provided by the Security Contractor shall:

- Be presented by a competent workplace trainer who is able to communicate in non-technical terms.
- Cover all operational features of the system.
- Cover all end-user programmable features of the system.
- Include basic diagnostic processors to enable fault finding.
- Be presented in a structured format in a classroom environment.
- Include useful handout and reference material.
- Include practical instruction and assessment.
- Be provided to RailCorp for approval prior to delivery to staff or end users.

4. Hardware Interface

4.1 Credential Readers

4.1.1 The security access control system shall provide controlled entry, via access card readers, only for authorised personnel to secured areas based on cardholder information entered and stored in the system database.



Security-in-Confidence

4.1.2 Long range credential readers or other associated active "E-Tag" type devices may be requested in managing car parking or high frequency vehicular entrances.

4.1.3 The use of Smart Card shall support "multi-application" and be provided with appropriate encryption.

4.1.4 Smart Card data shall reside on both the card and the system database.

4.1.5 Smart Card memory will be sufficiently adequate to support current applications and enable upgrades with the system being able to support future applications.

4.2 Electric/Electromechanical Locking Devices

4.2.1 Electric locks shall be programmable for fail-safe or fail secure mode.

4.2.2 All mechanical operations shall be impervious to the ingress of moisture, dust or other contaminants.

4.3 Request to Exit

4.3.1 Request-to-Exit (REX) devices must be included on all doors.

4.3.2 Provide local audible alarm notification on all perimeter doors/gates that is activated on either "forced door" or "door held" alarms.

Security-in-Confidence

4.3.3 Shall be the most appropriate type of device and located in a suitable position so that it does not impede upon normal pedestrian or vehicular traffic.

4.4 Emergency Breakglass Units

4.4.1 Shall only be installed when required by local authorities.

4.4.2 If activated (glass broken), generate an alarm at the alarm monitoring station, irrespective of the alarm system's status.

4.5 Associated Devices

4.5.1 All door contacts and request-to-exit devices must be connected in such a manner as to provide five-state supervised alarm monitoring. The input points used for door contact and request-to-exit devices shall be user-configurable.

4.5.2 All door contacts, reeds and strikes must be concealed or mechanically protected.

4.6 Software Interface

4.6.1 The system shall provide controls to operate closed circuit television (CCTV) cameras and monitors forming part of any CCTV system. The system shall provide the controls to define and run the following:

- Alarms, macros, and tours.
- Sequences from the monitors.
- Pan, tilt, zoom, focus, iris, wiper, washer and light controls for any given camera.

- Patterns, presets, and auxiliaries.

4.7 Specific to an alarm detection system:

4.7.1 Where an alarm system may already exist, the access control system shall have the capability to interface with this alarm system so that all detection, reporting, masking or other relevant control is achieved through one operating platform.

4.7.2 Where an alarm system is not installed but is recommended to further support the integrity of the access control system, a design proposal for the addition of an alarm detection system shall be presented as part of any project proposal.

4.7.3 Any new alarm system shall comprise both volumetric and perimeter detection devices that are immune to false alarming in the environment they have been designed to operate within. Consideration should be given to varying climatic conditions that may affect the performance of the alarm system during varying times of the year.

4.7.4 The system shall incorporate an integrated package that has the capability to manage visitor, gate, door control, intruder detection and CCTV.

4.7.5 The system shall have the capability to interface with PDA's or other similar handheld wireless devices. When interfaced, the PDA should be capable of viewing the operating system as well as limited control over the System.

4.7.6 The System shall be designed to interface with any existing fire detection system and shall be capable of:

- Appropriately controlling egress points to ensure the highest levels of safety is provided whilst maintaining the maximum possible level of security to the property.
- Providing secondary confirmation of a fire event, as well as being able to indicate the location and seriousness of the event.

4.8 Communication Interface

4.8.1 The system shall be capable of utilising any communications pathway available at the RailCorp site to communicate with remote locations, so that operators can download cardholder database information to remotely located card reader panels, and upload historical transaction information.

4.8.2 The system shall also be capable of receiving alarm transactions (active alarm, loss of primary power, door forced, etc.) from the remote location at any time.

4.8.3 The system shall be capable of various modes of communications including TCP/IP, PSTN, GPRS as a minimum.

5. Non-Functional Requirements

5.1 Performance Requirements

5.1.1 The access request response time from card presentation, database verification, to electric lock/unlock shall be no more than one second in normal operating mode on a fully loaded system. (Including biometrics or magnetic locks that have a longer operating time due to field collapse).

Security-in-Confidence

5.1.2 Have adequate battery backup of at least 6 hours in the event of a prolonged power supply outage.

5.1.3 Installation of all electrical outlets required for the proper operation of any equipment installed as part of the project scope will form part of the project. RailCorp's existing power outlets are not to be used to form part of the project scope unless approved prior to commencement of work in writing.

5.1.4 Other than consideration of performance, the location of all electronic devices shall consider the ease and impact of the surrounding building fabric for ease of cabling.

5.1.5 Where possible, cabling is to be concealed from view by running in ceiling spaces, concrete slabs, air space of stud walls or double brick walls or chased into rendered masonry walls unless otherwise specified.

5.1.6 Cabling and conduit shall be installed in a manner that will not necessitate penetration of damp courses or influence the entry of moisture into the building.

5.1.7 There shall be no exposed cable outside of any device unless it is installed in an approved cable tray. Where a cable tray is proposed to be used, prior written approval must be given. Existing cable trays may be used if mandatory separation of services can be achieved.

5.1.8 Where a conduit is installed to a device, the conduit shall be adequately secured to the device to resist removal and ingress of contaminants.

5.1.9 All cabling and conduit shall meet or exceed Australian Standards.

Security-in-Confidence

Security-in-Confidence

5.1.10 There shall be no exposed cabling. All external or underground cable shall be enclosed in a type of conduit, and, where this is above ground the conduit shall be of a highly vandal resistant design affixed with tamper resistant security type fasteners.

5.1.11 Where conduit is to be used, solid PVC or metal electrical conduit of a suitable diameter is to be indicated on the proposed installation plan. Flexible conduit will not be approved. Special consideration must be given to the type of material used within RailCorp tunnels or where flammability is of high concern.

5.1.12 All conduits shall be highly resistant to corrosion and be of a corrosion resistance equal to the equipment being installed as well as being meeting or exceeding the life cycle of this equipment.

5.1.13 Colour matched ducting may be used in highly sensitive areas where aesthetical appearance is paramount, and the area is deemed secure against cable tampering. Approval to install ducting must be given in advance by the Project Manager.

5.1.14 All cable size and specifications must adhere to all provisions of Section 17050 Wire Specifications.

5.1.15 Work and materials shall conform to the latest rules, regulation and codes of the appropriate government authorities. Nothing in these specifications shall be construed to permit work not conforming to the most stringent of applicable codes.

Security-in-Confidence

Security-in-Confidence

5.1.16 Full replacement or repair product warranty, or rectification of work at the discretion and direction of RailCorp for all products and installation shall be not less than 15 months.

5.1.17 During the warranty period the Contractor shall be required to replace or otherwise make good, at their expense, any part or parts that fail or may prove faulty in design, workmanship or material.

5.1.18 During the warranty period, the Contractor shall renew, repair, modify or adjust at their own expense any items of equipment, groups of items, or total systems that do not comply with the operating conditions and performance specified. This responsibility shall include the provision of labour and all incidental costs for the removal and replacement of defective parts or components.

5.1.19 During the warranty period the Contractor shall perform such works as instructed, in writing, within seven days, provided that such demands are compliant with the specification. Failures that impact on the security of a site shall be addressed with twenty-four hours. If the matter is not satisfactorily rectified, RailCorp reserves the right to engage others to finish such works or rectify faults with all costs incurred by such actions being the responsibility of the Contractor.

5.1.20 Items replaced during the warranty period shall be adjusted and tested to show that the system which it forms part of is giving satisfactory operation and that the performance of the replaced items meets or exceeds the requirements of the original contract specification.

5.1.21 The Security Contractor shall forward on to RailCorp all extensions of warranty on individual components or complete systems.

Security-in-Confidence

Security-in-Confidence

5.1.22 All work shall be undertaken in accordance with the requirements of the Building Code of Australia and any other standards that may be applicable, but not specifically mentioned.

5.1.23 The standards stated in this specification are current at this time; the Contractor shall comply with any revisions of the relevant standards by the appropriate authorities whilst executing this contract.

5.1.24 Work not covered by the requirements of Statutory Authorities or this document will comply with the appropriate publication of the Standards of Australia, Austel or other related certifying organisation.

5.2 Safety Requirements

All installed access control gates and doors must be configured to ensure compliance with all emergency egress requirements as detailed in the Building Code of Australia.

5.3 Security Requirements

5.3.1 Doors and doorframe must be capable of resisting reasonable force, and cannot be easily circumvented.

5.3.2 The door design shall consider if passback or tailgating cannot be tolerated and if necessary, design for this risk. (ie. Turnstile arrangement)

5.3.3 All mechanical locks and door hardware must be from a reputable Australian distributor.



Security-in-Confidence

5.3.4 Door keying systems must be in accordance with existing keying systems. Where a master keying system exists, the additional locks must be keyed to this master key system. A restricted master key broach is preferred where there is no existing master key system.

5.3.5 Access to door hinges must be restricted from both sides of the door when the door is closed. (Hinge pins must be concealed or installed on the inner side of hinged doors. Accessible hinge pins must be installed to resist removal).

5.3.6 All mechanical locks and door hardware shall resist reasonable force, and have protection against attack. (Strike plates to protect against the lock tongue being manipulated and all wiring through doors shall use power transfer hinge cabling routes).

5.3.7 The locking mechanism shall deadlock the door tongue to prevent forcing back when in the fully closed position.

5.3.8 If installing a new door, steel framing is preferred.

5.3.9 A fit for purpose automatic door closer that closes the door in all weather conditions shall be installed on all doors where an electric locking system has been fitted. (Consider 2 and 3 stage closers)

6. Standards

All constructions shall meet all applicable RailCorp / Rail Infrastructure Corporation standards, guidelines and policies. Of these documents, particular interest should be drawn to the following:

Rail Infrastructure Corporation

Transit Space Policy. Ref C 2101.

Transit Space Standards. Ref C 2103.

Application of Kinematic Envelope. Ref C2105.

Base Operating Standards for Clearances. Ref C 2107.

Metallic Lineside Fencing in Electrified Areas. Ref C 4501.

Low Voltage Installation Earthing. Ref EP 12 10 00 21 SP.

Buildings and Structures Under Overhead Lines. Ref EP 12 10 00 22 SP.

RailCorp:

Safety Standard – Construction Work. Ref A10-08-N112.

Appendix A: Issues List

All concerns and issues are to be listed and addressed and where required listed in the revision history and a new version issued.