Office of the Chief Investigator
Transport Safety

Rail Safety Investigation
Report No 2009/07

Derailment

Pacific National Train 9564

ABB Siding, Dandenong

1 June 2009

TABLE OF CONTENTS

THE CHIEF INVESTIGATOR

The Chief Investigator, Transport Safety is a statutory position under Part 7 of the *Transport Integration Act 2010*. The objective of the position is to seek to improve transport safety by providing for the independent no-blame investigation of transport safety matters consistent with the vision statement and the transport system objectives.

The primary focus of an investigation is to determine what factors caused the incident, rather than apportion blame for the incident, and to identify issues that may require review, monitoring or further consideration. In conducting investigations, the Chief Investigator will apply the principles of 'just culture' and use a methodology based on systemic investigation models.

The Chief Investigator is required to report the results of an investigation to the Minister for Public Transport or the Minister for Ports. However, before submitting the results of an investigation to the Minister, the Chief Investigator must consult in accordance with section 85A of the *Transport (Compliance and Miscellaneous) Act 1983*.

The Chief Investigator is not subject to the direction or control of the Minister in performing or exercising his or her functions or powers, but the Minister may direct the Chief Investigator to investigate a transport safety matter.

EXECUTIVE SUMMARY

On 1 June 2009 a Pacific National freight train was derailed as it was departing a siding between Dandenong and Cranbourne. The derailment was a consequence of a set of points moving beneath the train in response to the signalling control system requesting a route to enable the passage of a suburban passenger train from Lynbrook Loop to Dandenong.

The signalling system between Dandenong and Cranbourne had recently undergone an upgrade which included the introduction of Computer Based Interlocking. The investigation identified deficiencies within the signalling design, data reviewing, system testing and configuration verification procedures. The deficiencies in these processes resulted in a signalling data input programming error going undetected. The error remained latent in the signalling system from 17 May 2009 until the incident.

Post incident analysis of the computer program data identified the error, which was rectified, tested by the contractor and verified by the Network manager prior to the resumption of services.

As a consequence of this event the contractor responsible has implemented a plan to restructure their procedures for signalling system design, Computer Based Interlocking programming configuration, testing and verification. The investigation recommends that the contractor review their standards for the design, construct and commissioning of signalling systems.

Since the incident the infrastructure manager has changed and the investigation has recommended that the new infrastructure manager review their signalling contractor management processes and their standards for the design, construct and commissioning of signalling systems.

1. CIRCUMSTANCES

1.1 Infrastructure

1.1.1 Introduction

The rail line between Dandenong and Cranbourne is a single bi-directional electrified line forming part of the Melbourne suburban system. The sections are: Dandenong to Lynbrook Loop and Lynbrook Loop to Cranbourne. The Dandenong to Lynbrook Loop section has intermediate locations at the Through/ABB Siding and Lyndhurst Siding (see Figure 1). Route and signal settings are controlled and monitored by a signaller stationed at Dandenong.

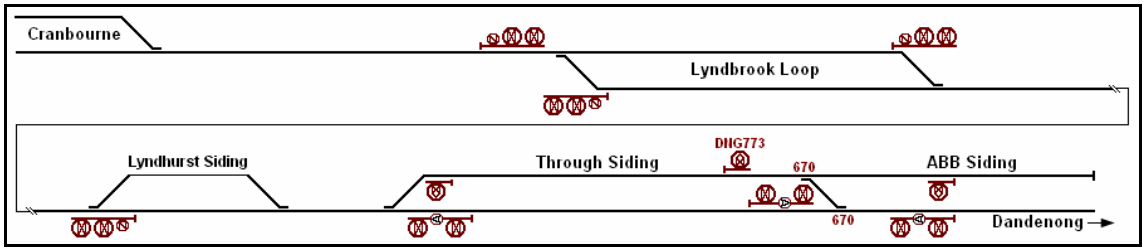

Figure 1 – Schematic of line Dandenong – Cranbourne

1.1.2 Lynbrook Loop

Lynbrook crossing loop consists of two uni-directional tracks and facilitates the crossing of trains. It has the flexibility to be operated in either automatic mode[1] or non-automatic mode. The normal operation is for trains to be routed via the left-hand track in the direction of travel.

In automatic mode, train movements are routed and signalled to effect a cross of opposing trains and then to continue to either Dandenong or Cranbourne as the case may be, without any interaction from the signaller. All other applicable points and signals in the single line section are also set and cleared by the system. When the automatic mode is de-selected the signaller operates the points and signals as required.

1.1.3 Through Siding / ABB (Bombardier) complex

Access to the ABB complex is via the Through Siding which is a double ended siding. The Melbourne (Up) end is fitted with a crossover connecting with the ABB Siding whereas the Cranbourne (Down) end is fitted with a single turnout connecting the siding to the mainline. However, at the time of the incident this connection was not in use. The route setting and clearing of signals for train movements into and out of the siding must be set by the signaller. In automatic mode the signals on the mainline at this location are operated by the passage of trains.

1.1.4 Lyndhurst Siding

Lyndhurst Siding is a double-ended siding servicing a cement distribution facility. Train movements into and out of this siding are not controlled by signals. The siding

[1] Automatic mode is when the interlocking system automatically operates the points and signals for the passage of trains.

connects to the mainline using a ground frame lever and a remotely controlled electrical release to allow manual operation of the points.

1.2 The Incident

Prior to the incident, the Through Siding, Lynbrook Loop, and Cranbourne Station were operating in automatic mode.

Pacific National train 9564 was scheduled to run a freight service from ABB Siding near Dandenong to the Dynon terminal, Melbourne. To facilitate movement from the siding to the mainline, the signaller at Dandenong de-selected the 'Auto' mode for the Through Siding and set the crossover consisting of points 670D and 670U (points 670, see Figure 2) to 'reverse' and placed signal DNG773 to 'proceed'. Lynbrook Loop was left in 'Auto' mode, in accordance with the design and operating parameters of the system.

At 1411 train 9564 commenced its departure towards Melbourne from the Through Siding. Around the same time a Down suburban train arrived into Lynbrook Loop and cleared the Up end points. The system then automatically requested the route from Lynbrook Loop to Dandenong for an Up suburban train which was arriving at the loop from Cranbourne and proceeding to Dandenong

This was the first occasion since the Computer Based Interlocking (CBI)[2] upgrade (see section 2.3) of the signalling system that this combination of train operations and system conditions had occurred.

The automatic route request by the system was the 'trigger' event that resulted in points 670 moving from 'reverse' to 'normal' as the ninth vehicle of train 9564 travelled over them. The lead bogie of the ninth vehicle (VHQF-204C) was travelling through the points towards the mainline while the rear bogie travelled towards the ABB siding causing the bogie to derail about six metres beyond the points. The derailment resulted in damage to an Explorer passenger car, 670 points and destroyed dwarf signal DNG772.

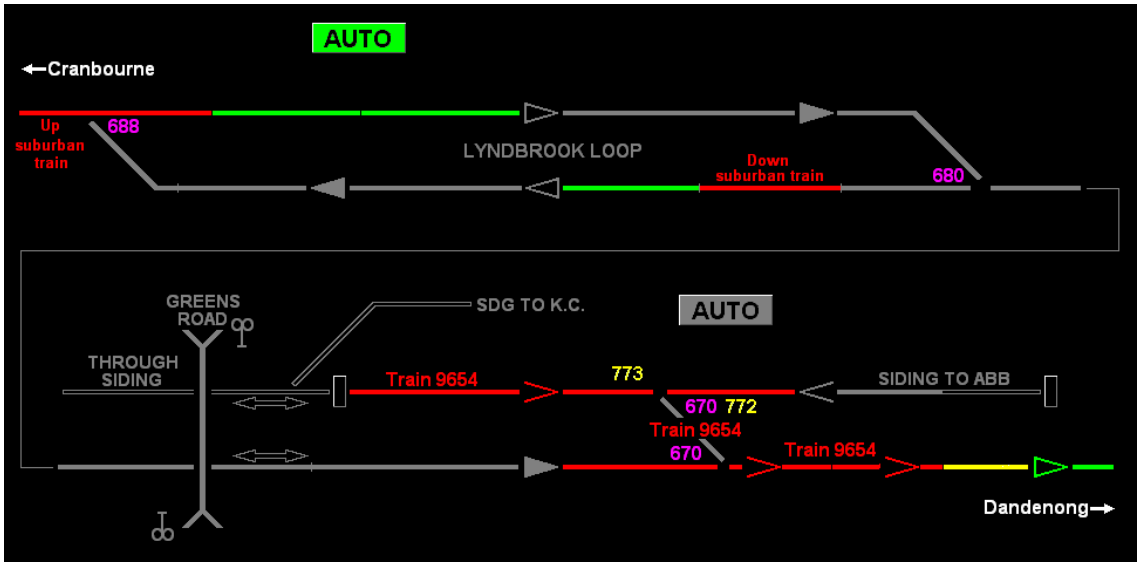

Figure 2 – Train locations and System conditions at Lynbrook Loop and the Through Siding at time of derailment.

[2] A complete railway signalling interlocking, inclusive of all features in which interlocking logic and equipment control are performed by digital microprocessors.

2. FACTUAL INFORMATION

2.1 The train

Train 9564 consisted of two locomotives (one at each end) and 14 vehicles, three of which were NSW Explorer rail cars for transit to NSW via the Dynon terminal after refurbishment.

2.2 Personnel

2.2.1 The signaller

The signaller was current in safeworking and medical requirements for his duties and had been operating the signalling system at Dandenong since 1989. The signaller said that on receiving a request from the driver of train 9564 to depart the Through Siding, he monitored the passage of a Cranbourne-bound suburban train on the Visual Display Unit (VDU). Once this train had cleared the Through Siding he deselected the 'Auto' mode and operated the points and signals to facilitate the departure of 9564. As 9564 departed the signaller was alerted to an abnormal situation when the fault alarm display indicated that 670 points were 'out of correspondence'[3] and that dwarf signal DNG772 was not displaying any indications. After communicating with the driver of 9564 it was identified that the train had derailed at the points.

2.2.2 The train crew

The Pacific National train crew operating 9564 were current in route knowledge, safeworking and medical requirements to operate this service. They reported that the departure from the Through Siding was normal until about half the train was on the mainline when they observed an unintentional reduction in brake pipe air pressure and the application of the train brake. When 9564 was stationary, an inspection identified that vehicle VHQF-204C was derailed with the leading bogie on the mainline and the rear bogie on the Through Siding.

2.3 Signalling System

During 2008-2009 the track configuration at Cranbourne was altered by the addition of several sidings to accommodate the stabling of suburban trains. The new configuration was controlled by CBI. Originally it was planned to incorporate a signal control system upgrade in conjunction with the introduction of these sidings. However, the train operators' project priority altered and the signalling control system upgrade component for the line was deferred.

In May 2009, the signalling control system was upgraded from a 'Unit Lever' panel to an 'Entry/Exit' VDU control system. The upgrade involved modifications to the interlocking command codes.

The status of field equipment on the Dandenong-Cranbourne line is monitored and transmitted to a central control centre – in this instance Dandenong. At the control centre the status of the field equipment, together with any commands received from the signaller, are processed and then transmitted to processing equipment at the field locations. Local commands are then transmitted to the field equipment – points and signals. The interlocking conditions and false release commands are managed by software commands incorporated within the computer program coding logic.

[3] Out of correspondence – is a situation when points are not fully set and locked.

2.4 Infrastructure maintenance

2.4.1 United Group Limited

United Group Limited (UGL) is a multi-service business offering construction, engineering, operational and maintenance services to the rail transport industry. The company was the design, construct and commissioning contractor for the Dandenong - Cranbourne signalling upgrade. To carry out the upgrade they utilised the SIGVIEW[4] software package.

The signalling Testing and Commissioning Plan for the Dandenong–Cranbourne upgrade indicated that the testing for this work was to be conducted in accordance with the *PTC Railway Signalling Testing and Commissioning Manual*, dated December 1992, and that the upgrade to CBI would be conducted in accordance with the provisions of the PTC Specifications in document ENG-SE-SPE-0009.

The investigation was provided with documentation in respect to design checking, factory acceptance testing, control tables, points sequencing tables and CBI software versions. However, the investigation was not provided with UGL's documentation describing their testing and commissioning strategies.

In addition, the UGL supplied documentation did not provide evidence to support the identification of competencies and responsibilities of personnel involved in the design, checking or verification processes.

In respect to error checking, the design data errors identified during the checking process were corrected. However, the re-check was not conducted by the checker who identified the errors. There was no evidence to indicate that a briefing for the substitute checker was conducted and UGL could not provide documentation that any verification of the design re-check process was completed.

In discussions, UGL stated that they relied heavily on the local knowledge and experience of a select few employees and contractors but their skills and knowledge had not been documented.

2.4.2 MainCo

At the time of the incident MainCo was contracted by Connex Melbourne Limited (CML)[5] to undertake the maintenance of their rail infrastructure. MainCo held rail safety accreditation as a Rolling Stock Operator only and the MainCo procedures, processes and standards were part of the CML Safety Management System.

MainCo procedures did not require them to approve the design or validate software versions of a signalling system. These functions were the responsibility of the signalling design testers – in this case UGL. However, the procedures required MainCo to approve the Testing and Commissioning Plan, which was to be prepared by UGL. The investigation noted that the UGL Testing and Commissioning Plan did not show that it had been approved by MainCo.

The MainCo procedures required "the contractor shall ensure that their staff have had adequate training and experience to design and check critical and safety related work and shall produce a CV (*Curricula Vitae*) for all the design and checking engineers to be utilised on the project."

[4] SIGVIEW provides a means for signallers to remotely control and monitor the signalling equipment located trackside. The status of all signalling in the total area of control can be observed from a VDU panel.
[5] Connex was the Melbourne metropolitan train operator at the time of the incident.

In regard to field commissioning, MainCo was the agency responsible for issuing the Certificate of Signalling, which records that testing has been conducted in accordance with project documentation and the acceptance of the associated works into the network for operation. The Certificate of Signalling dated 7 May 2009 issued by MainCo certifying that the upgrade works between Dandenong and Cranbourne was operational was not signed by a testing witness, as required.

At 30 November 2009, MainCo's infrastructure maintenance functions were absorbed into Metro Trains Melbourne's company structure.

2.5 Checking and testing

2.5.1 Software version comparisons

Araxis Merge is a software program that compares software listings and highlights differences. The highlighted differences between the listings are referred to as the 'Data Differences List'. The Araxis Merge process is applied repeatedly during each development phase of the project to serve as a regular check of progress and draw attention to unintended changes or omissions.

Following this incident Data Differences Lists were run to compare the software version existing prior to 21 April 2009 to the version produced subsequent to the event on 2 June 2009. The comparison found that there was a missing backslash symbol [\] in the programming of the command code in respect to the interlocking requirements for 670 points in the 21 April 2009 version.

2.5.2 Mimic facilities

Both MainCo and UGL had mimic facilities, which were made available to review the event. The review enabled the investigation to identify the commands and sequence of events that led to 670 points running under train 9564.

CBI codes for the routing between Lynbrook Loop and Dandenong were analysed by UGL immediately after the incident. This analysis identified that there was a coding error that allowed the electrical locking of 670 points to release, which in turn permitted these points to move while occupied by a train travelling from the Through Siding to the mainline. However, when the missing backslash was inserted in the program code, the electrical locking of the points did not release when the points were occupied by a train.

2.5.3 Control tables

Control tables are a method of setting out the interlocking requirements for a signalling layout and are one of the fundamental inputs used by designers in the detailed design of the interlocking. As such, they constitute a functional specification by detailing the interlocking requirements for each signalled route under all foreseeable operating conditions.

Following the preparation of control tables to the satisfaction of rail operators, control tables then form the design basis for physical implementation. In addition, they are also used as a primary reference document during the functional testing of an interlocking. All of the requirements of a control table are proved to be operating correctly as part of the testing process.

The control tables provided to the investigation addressed the local interlocking requirements of each location but did not address the 'whole of system' in its final configuration.

The investigation noted that UGL relied on the design reviewer having an intimate knowledge of the local network operating practices and acknowledged that it was

common practice for control tables to be synoptic of the system. International practice is for control tables to be extensive and detailed eliminating the reliance on the reviewer's local knowledge and experience.

2.6 Standards, Rules, Guidelines

2.6.1 Australian Standard 4292.4 – 2006

AS4292.4 provides guidelines for the Interface, Design, Construction and Implementation, Commissioning, Monitoring and Maintenance, and Modification for 'Signalling and Telecommunications Systems and Equipment'. It also provides a template to follow for the Life Cycle Phase Descriptions and Requirements (the project process). It is a recommended industry practice to follow the standard and to develop safety management systems incorporating the guidelines contained in the standard.

2.6.2 Signal Standard MSSP 0002 - Signalling Design and Documentation

This MainCo document was based on the PTC document ENG-SE-SPE-001 in an expanded version to reflect MainCo's involvement in the design checking and review process required for signalling system design. This documentation provides the detail of how AS 4292.4 is to be complied with. It also includes the stipulation that MainCo view the checking and review process as an audit process for their contractors.

MSSP 0002 advises that signal testing shall be conducted to ensure that the installation conforms to the interlocking requirements detailed in the control tables. To facilitate the testing, a simulator or test rig may be used to simulate the expected responses from external equipment.

2.6.3 PTC Specification ENG-SE-SPE-0009

This specification set out the requirements for design, supply, installation, standards, safety, validity, testing and commissioning, maintenance and quality assurance of CBI systems.

The specification states that the CBI system shall be protected against 'Wrong Side Failures'[6]. The system shall be specifically designed and proven intrinsically 'fail-safe' under all conditions, and shall have the documentation to prove this requirement.

2.6.4 Victorian Rail Industry Operators Group Standards (VRIOGS)

In December 2008, the Victorian Rail Industry Operators Group issued a number of standards with regard to rail signalling design and documentation and the testing and commissioning of railway signalling systems for the purpose of establishing uniform standards for the guidance of signalling system designers throughout the Victorian Rail Network.

The VRIOGS documents superseded the PTC documents and MSSP 0002 previously mentioned. However, the investigation noted that during the system and signalling upgrade, UGL and MainCo relied on PTC documents and MSSP 0002 and not VRIOGS. The investigation was informed that UGL and MainCo were aware of the development of the VRIOG standards however they were unaware that they had been issued in December 2008. At the time of the incident the VRIOG standards had not been adopted into the CML Safety Management System.

[6] A wrong side failure is any failure of computer based interlocking which endangers or has the potential to endanger the safe passage of trains; for example, release of points when they should be locked.

2.7 Post incident review

A post incident independent review commissioned by MainCo resulted in the following findings:

“Design review:

- No evidence of a design plan having been produced;
- No mention of data guidelines / code of practice used for the design of data;
- The change control of data documentation was not correctly handled;
- Inadequate reference details and management of the change control process;
- The work involved was underestimated;
- No evidence of design input sheets (cross disciplines);
- Engineering resources were strained, negatively influencing the Dandenong works.

Error checking:

- The errors identified in the data by the checker were corrected by the designer but the recheck was undertaken by a different checker;
- The experience of available data checking personnel was unclear;
- The templates used to record design errors were not clear enough;
- Only one level of data checking was employed for high volume complex alterations with no additional verification after check / rework / recheck process.

Testing processes:

- New but unchecked designs (control tables) were used as reference for the testing;
- Data differences lists (diff lists) not followed;
- Error report forms used during testing were not completed correctly;
- Extent of testing unclear / difficult to prove integrity due to
    - The process of documenting the scope of simulation was not adequate;
    - The management of the testing process was deficient;
    - Reference documents used during testing were inadequate;
    - Allocation of testing resources was insufficient.

Site testing and commissioning processes:

- References for testing and commissioning strategies not found;
- Site testing and commissioning activities did not test for interlocking data function faults;
- Testing and commissioning plan assumes satisfactory completion of all pre-testing and is not comprehensive;
- Site testing and commissioning processes for CBI’s are undertaken to verify the system is ‘set-to-work’ and each element corresponds correctly. These site tests do not involve a check for each element of data that has been changed and therefore would not detect the error under review.

Monitoring and supervision:

- Management of change considerations were overlooked;
- Engineering change considerations were overlooked;
- The mitigation of design risks and of testing risks identified in the MainCo Risk Register were overlooked.

Documentation regarding testing:

- The standards specified in the Scope of Works document did not adequately cover testing of CBI technologies;
- The Testing and Commissioning Plan did not show any mention of MainCo approval;
- The Certificate of Signalling used to bring the system into use was not signed by a Testing Witness.

Documentation regarding commissioning:

- Appropriate management and/or supervision functions regarding the MainCo Risk Assessment Register, Connex Change Management Process and MainCo Engineering Change Control seem not to have been applied."

3. ANALYSIS

3.1 The Incident

This particular combination of train movements and system status was the first such occurrence since the system was upgraded on 17 May 2009. The result was a 'wrong side' failure of the signalling system.

The call on 670 points while the freight train was travelling over those points was triggered by the normal operation of the signalling system, in automatic mode, in response to detecting an Up train at the Lynbrook Loop. The system was able to override the selection of the route due to an error in the CBI program, which had not been detected in pre-commissioning testing.

The investigation found that a data programming error caused the design to fail in two places by:

(1) locking other signal routes requiring the points in the opposite position, and

(2) allowing 670 points to move while a train was traversing them.

Railway operating integrity requires that this sort of incident is not possible and the very basis of signalling safety is such that there are no circumstances acceptable where points are 'free to move' whilst a train is passing over them.

3.2 Error checking

In their evidence, UGL stated that they relied on the local knowledge and experience of a select few employees and contractors in the error checking process. UGL appears to have assumed that the staff conducting checks of the upgraded signalling system would know what checks were required and no documented procedure was developed to guide staff.

It appears that the relevant employees overlooked the fact that the whole signalling system needed to be checked when each section was upgraded, and not just the section being upgraded. There was no documented procedure in place that would assist them in noticing this lapse.

With regard to identifying data design errors the investigation identified that before the commissioning of the upgrade on 17 May 2009 it was industry practice that checking of the data migration from 'Unit Lever' to 'Entry/ Exit' was conducted by only one checker.

Given the significant control system alterations being undertaken it would have been prudent for either UGL or MainCo to have included an additional verification check either by their own staff or by an independent expert.

Implementing additional verification processes would have improved the checking process and could possibly have found the missing backslash in the command data and rectified it before it reached the testers. In this instance, and in the absence of documented procedures, single person errors were allowed to go undetected.

3.3 Testing

In accordance with the Australian Standards, UGL was required to prepare a Testing and Commissioning Plan detailing its testing and commissioning strategy. However, the plan submitted to MainCo did not describe the strategy to be adopted and MainCo did not request UGL to submit a commissioning strategy.

An appropriate strategy in this instance would have included the testing and commissioning processes at each stage of the upgrade and details of how they were intended to be done. Had there been a testing and commissioning strategy, it is possible that those involved in developing the strategy would have noticed that a 'whole of system' test was not included in the plan.

Simulation testing is one of the most vital parts of the safety-critical processes in a CBI alteration and should be carefully managed. Those undertaking simulation testing duties need to have adequate knowledge of the type of technology and be able to understand the exact scope of testing required after the design alterations. Evidence of the competence of personnel conducting the proposed simulations was not presented to MainCo and was not asked for despite being required by MainCo's document MSSP 0002.

It is unclear whether the relevant testers had intimate technological knowledge of the requirements of CBI systems and background knowledge of the upgrades being undertaken. In order to understand the exact scope of testing required, the tester should study the data changes using the Data Differences Lists and carry out testing by reference to the control tables. In this incident, it was noted that the testing of the interlocking was conducted based on 'as in service' control tables at the individual locations and that the command codes introduced with the 17 May 2009 upgrade commissioning were not subjected to 'whole of system' design testing.

The investigation found that simulation facilities were available to conduct a 'whole of system' test prior to commissioning. Had either UGL or MainCo considered this before, rather than after the incident, or had this requirement been included in the Testing and Commissioning Plan, the incident is unlikely to have occurred.

3.4 Actions by UGL

Initially the signalling control system upgrade was to incorporate the whole Dandenong-Cranbourne line. However the plan was amended and instead MainCo decided to upgrade the signalling system in separate stages. It appears that in doing so, the design plans developed by UGL only incorporated the checking and testing of the sections being upgraded and not the whole line. This fact was not noticed by MainCo.

The independent investigation commissioned by MainCo highlighted a number of lapses by UGL in its documentation and in its processes. The findings of the report indicate that there could have been a culture of laxity on the part of UGL in carrying out its contractual requirements in accordance with industry accepted practices.

3.5 Actions by MainCo

MainCo's procedures indicated that they would audit their contractor's processes related to design, use of suitably qualified personnel and supervision. It is evident that this did not occur and that the focus was on the installation and commissioning stages associated with the project rather than the design and off-site testing phases. Had audits been conducted in accordance with the criteria of MainCo standard MSSP 0002, it would have become apparent that UGL had not tested the 'whole of system' prior to the commissioning.

The independent investigation also indicated in its findings that there may also have been a culture of laxity in MainCo. It appears that MainCo did not:

- provide a comprehensive Scope of Works to UGL
- audit the documents submitted by UGL regarding design and testing, against the required standards, and

- supervise the testing of the system in accordance with the standards.

It is possible that had MainCo ensured the relevant standards were applied, the deficiencies in UGL's processes would have been highlighted and the shortcomings would have been detected and corrected prior to commissioning the system upgrade.

4. CONCLUSIONS

4.1 Findings

1. The signaller and the train crew were appropriately qualified and their actions did not contribute to the incident.

2. The detection of an Up train at the Lyndbrook Loop, when the signalling system at this location was operating in the automatic mode, was able to override the setting of 670 points at the Through Siding while they were occupied by a train.

3. There was a missing backslash symbol [\] in the programming of the command code in respect to Computer Based Interlocking requirements.

4. The error remained latent within the system since the commissioning of the upgrade on 17 May 2009.

5. The management systems employed within United Group Limited during design, data checking, configuration testing and at commissioning failed to identify the data error in the Computer Based Interlocking command codes associated with 670 points.

6. The management and supervision systems employed by MainCo failed to identify the lapses in United Group Limited's documentation and processes regarding design, testing and commissioning strategy.

7. Signalling system testing was conducted in accordance with the control tables, in so far as they were developed.

8. The signalling system upgrade was commissioned with an incomplete 'Certificate of Signalling'.

4.2 Contributing Factors

1. The design configuration control processes applied by United Group Limited did not detect the wrongly coded command code.

2. 'Whole of system' testing prior to and during commissioning of the upgraded system was not conducted.

3. The disposition of the signalling system at Lynbrook Loop and the Through Siding to facilitate the particular train movements.

5. SAFETY ACTIONS

5.1 Safety Actions taken since the event

United Group Limited has implemented a nine-stage process to address the procedural failures identified in their management systems.

5.2 Recommended Safety Actions

Issue 1

The management and supervision systems employed by MainCo failed to identify the lapses in United Group Limited's documentation and processes regarding design, testing and commissioning strategy.

RSA 2011003

That Metro Trains Melbourne reviews its systems and processes with respect to signalling contractor management.

Issue 2

MainCo and United Group Limited were unaware that the Victorian Rail Industry Operators Group had issued a number of Standards in December 2008 which replaced the PTC and MainCo Standards that were being used during the Dandenong-Cranbourne signalling system upgrade.

RSA 2011004

That United Rail Group aligns their systems and processes to the Victorian Rail Industry Operators Group Standards for Signalling System Design, Construct, Testing and Commissioning.

RSA 2011005

That Metro Trains Melbourne reviews their systems and processes to ensure alignment with the Victorian Rail Industry Operators Group Standards for Signalling System Design, Construct, Testing and Commissioning.