Report R0-2012-102:
Train control power failure, 26 April 2012

The Transport Accident Investigation Commission is an independent Crown entity established to determine the circumstances and causes of accidents and incidents with a view to avoiding similar occurrences in the future. Accordingly it is inappropriate that reports should be used to assign fault or blame or determine liability, since neither the investigation nor the reporting process has been undertaken for that purpose.

The Commission may make recommendations to improve transport safety. The cost of implementing any recommendation must always be balanced against its benefits. Such analysis is a matter for the regulator and the industry.

Final Report

Rail inquiry RO-2012-102
Train control power failure, 26 April 2012

Approved for publication: October 2014

Transport Accident Investigation Commission

About the Transport Accident Investigation Commission

The Transport Accident Investigation Commission (Commission) is an independent Crown entity responsible for inquiring into maritime, aviation and rail accidents and incidents for New Zealand, and co-ordinating and co-operating with other accident investigation organisations overseas. The principal purpose of its inquiries is to determine the circumstances and causes of occurrences with a view to avoiding similar occurrences in the future. Its purpose is not to ascribe blame to any person or agency or to pursue (or to assist an agency to pursue) criminal, civil or regulatory action against a person or agency. The Commission carries out its purpose by informing members of the transport sector, both domestically and internationally, of the lessons that can be learnt from transport accidents and incidents.

Commissioners

Chief Commissioner	John Marshall, QC
Deputy Chief Commissioner	Helen Cull, QC

Key Commission personnel

Chief Executive	Lois Hutchinson
Chief Investigator of Accidents	Captain Tim Burfoot
Investigator in Charge	Barry Stephenson
General Manager Legal & Business Services	Cathryn Bridge

Email	inquiries@taic.org.nz
Web	www.taic.org.nz
Telephone	+ 64 4 473 3112 (24 hrs) or 0800 188 926
Fax	+ 64 4 499 1510
Address:	Level 16, 80 The Terrace, PO Box 10 323, Wellington 6143, New Zealand

Important notes

Nature of the final report

This final report has not been prepared for the purpose of supporting any criminal, civil or regulatory action against any person or agency. The Transport Accident Investigation Commission Act 1990 makes this final report inadmissible as evidence in any proceedings with the exception of a Coroner's inquest.

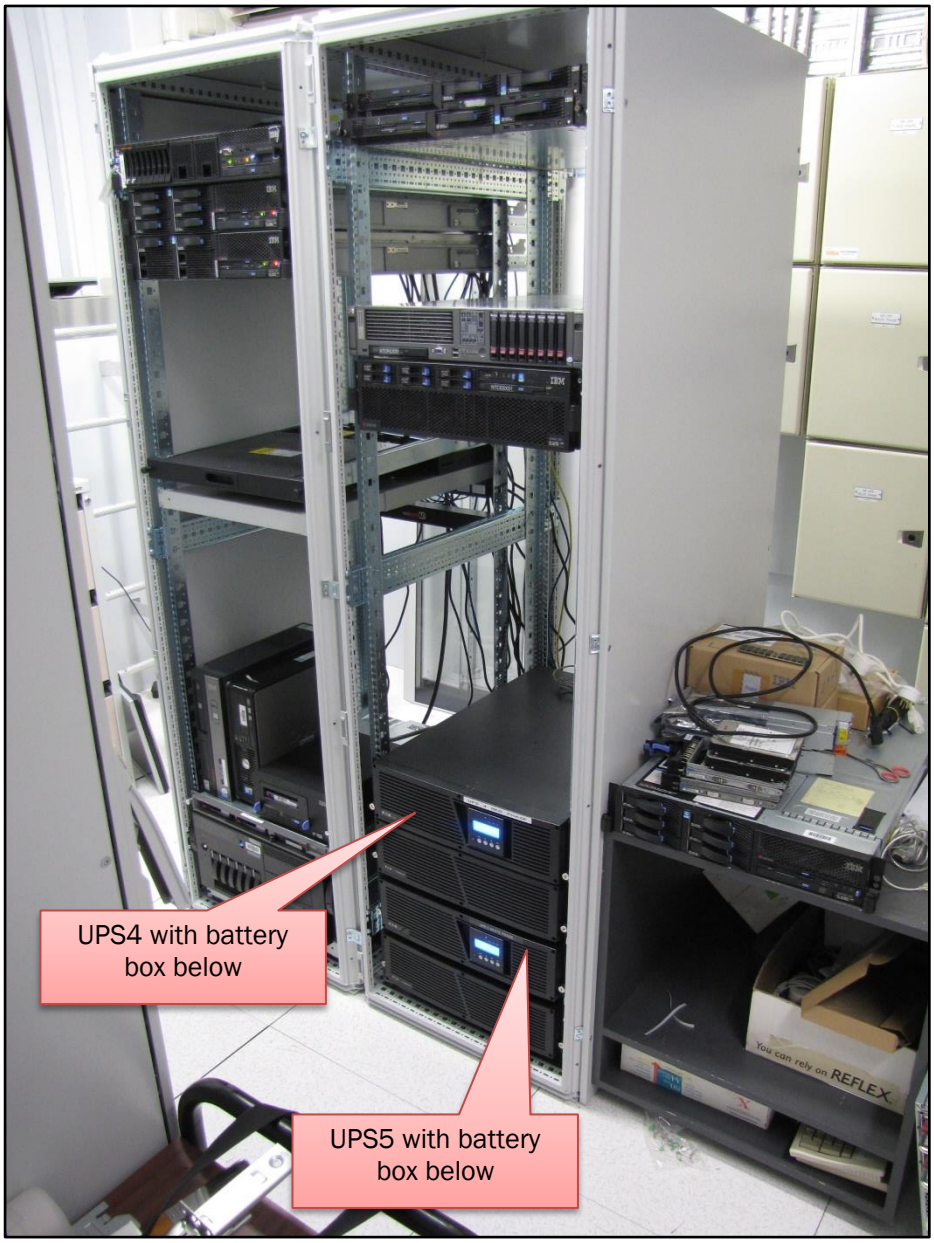
Ownership of report

Citations and referencing

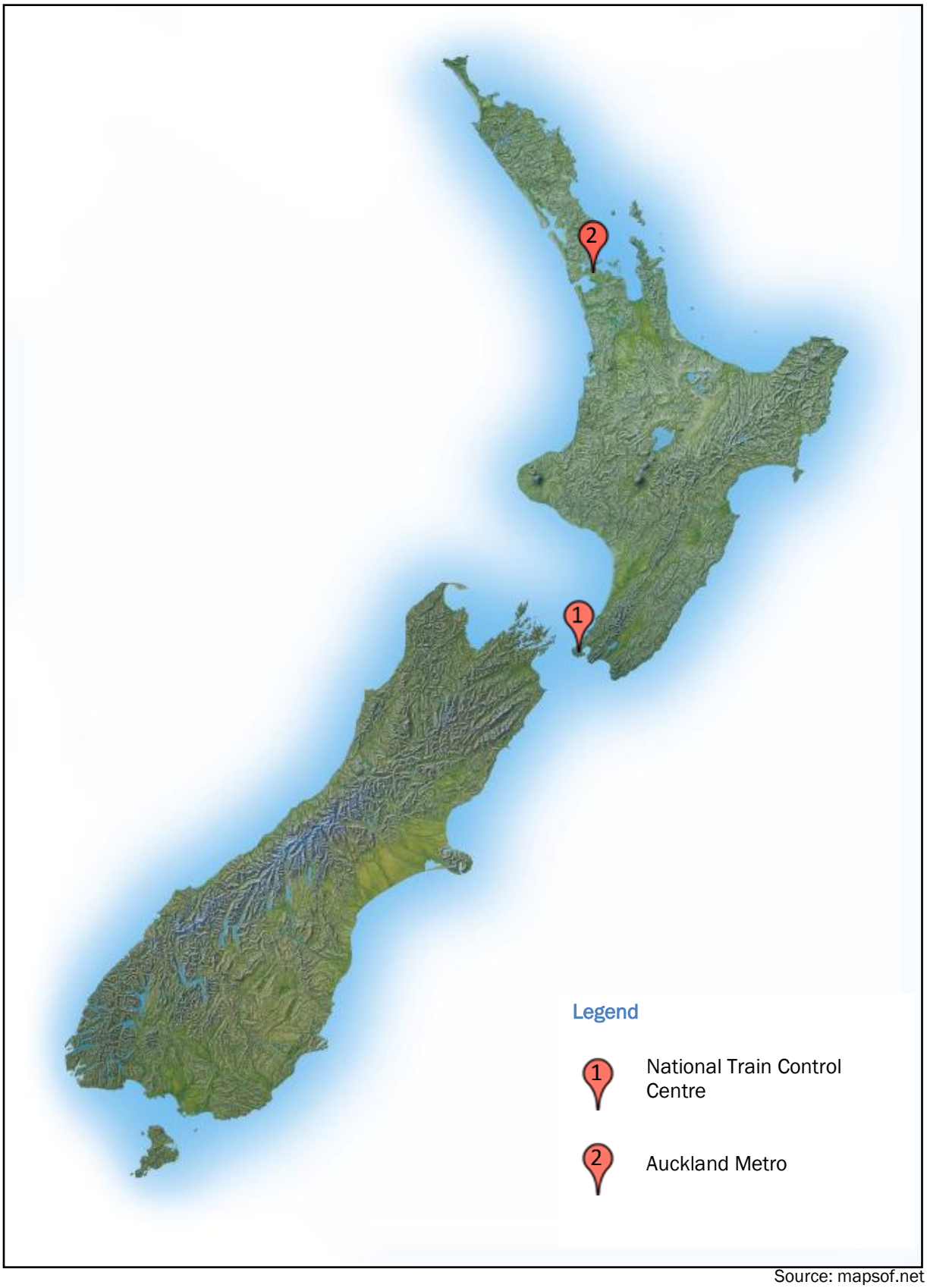
Information derived from interviews during the Commission's inquiry into the occurrence is not cited in this final report. Documents that would normally be accessible to industry participants only and not discoverable under the Official Information Act 1980 have been referenced as footnotes only. Other documents referred to during the Commission's inquiry that are publicly available are cited.

Photographs, diagrams, pictures

Unless otherwise specified, photographs, diagrams and pictures included in this final report are provided by, and owned by, the Commission.



UPS4 and UPS5



Source: mapsof.net

Location of accident(s)

Contents

Abbreviations ii
Glossary ii
Data summary iii
1. Executive summary 1
2. Conduct of the inquiry 2
3. Factual information 3
3.1. Narrative 3
The occurrence 3
3.2. The train control system 4
3.3. Background history 4
3.4. Veolia service delivery operations 5
4. Analysis 6
4.1. Introduction 6
4.2. The power failure 6
4.3. Design of the electrical systems 9
4.4. Risk management 11
4.5. Management and maintenance of the emergency power supply system 12
5. Findings 14
6. Safety actions 15
General 15
Safety actions addressing safety issues identified during an inquiry 15
Safety actions addressing other safety issues 15
7. Recommendations 16
General 16
Recommendations 16
8. Key lessons 17
9. Works cited 18
Appendix 1: Electrical concepts 19
Appendix 2: Timeline 21
Appendix 3: Examples of circuit breaker trip curves 22

Figures

Figure 1 Photograph showing typical train controller workstation at train control 4
Figure 2 Single line power schematic of train control..... 7

Abbreviations

GPS	global positioning system
UPS	uninterruptable power supply

Glossary

amp (ampere)	a unit measurement of electrical current
multi-box	an electrical portable outlet device, commonly known as a “powerboard”, “multi-plug” or “multi-box”. A multi-box contains several distribution socket outlets for connecting multiple electrical appliances to one wall outlet
Veolia	the contracted metropolitan rail passenger service train operator for the Auckland metropolitan rail network. The operator has since changed the company name to Transdev but it was known as Veolia at the time of this incident

Data summary

Vehicle particulars

Train type and number:	N/A
Classification:	Infrastructure
Year of manufacture:	N/A
Operator:	KiwiRail
Date and time	26 April 2012, 1603[1]
Location	National Train Control Centre, Wellington
Persons involved	Auckland train control operators (located in the Wellington National Train Control Centre), passengers and crew on Auckland metro trains, Veolia operations (located at Britomart Station, Auckland)
Injuries	nil
Damage	nil

[1] All times stated in this report are in 24-hour format New Zealand Standard Time (co-ordinated universal time + 12).

1. Executive summary

1.1. At about 1600 on 26 April 2012, the four train control workstations in the Auckland control room located in the Wellington National Train Control Centre (train control) suddenly lost power and shut down. As a consequence, all of the signals in the Auckland metropolitan area automatically reverted to red ("Stop") and all rail movements in Auckland progressively stopped.

1.2. Train controllers were unable to communicate with the stranded trains and could not issue control instructions. Veolia[2] was advised of the power outage and immediately activated its emergency plan. Veolia sent messages to all its on-board train managers, explaining the situation. All passengers were retained on board trains that were prevented from reaching their next stations.

1.3. The power outage lasted for about one hour and scheduled passenger services were affected for the rest of the evening. There were 27 train services travelling within the Auckland metro area at the time, with an estimated passenger load of between 1000 and 2000.

1.4. The power outage occurred when an electrical fault caused an electrical circuit breaker that was feeding power to all four Auckland workstations to trip. The electrical fault should have first tripped a different circuit breaker, which would have resulted in only one of the four workstations being lost.

1.5. The control of all signals for the Auckland metropolitan area had been centralised into Wellington train control since 1997. The last phase of centralisation was the provision of the four new workstations that subsequently lost power in this incident. All train control functions for the Auckland metropolitan area had been managed from these four workstations since late 2010, about 16 months before the incident.

1.6. The Commission identified the following safety issues:

- the project team responsible for the Auckland train control centralisation project lacked the appropriate expertise for designing and installing the emergency power supply system
- the management and maintenance of the emergency power supply system for train control were not sufficient to ensure the integrity of what had been designated an "essential service"
- KiwiRail's Risk Management Policy for "continuity of core services" did not give proper consideration to the safety of passengers and crew when a core service such as train control failed, causing the widespread stoppage of an entire metropolitan passenger rail system.

1.7. KiwiRail took the necessary safety action to improve the management and maintenance of the power supply system for train control.

1.8. The Commission made one recommendation to the Chief Executive of KiwiRail to review its risk assessment matrix to improve the focus on safety risk.

1.9. The key lessons learnt from the inquiry into this occurrence were:

- projects involving essential core services must be appropriately scoped and resourced to ensure that the service integrity is not disrupted at any time
- essential core services must be subjected to a rigorous safety risk assessment process that ensures that the risks to people and infrastructure are appropriately managed and tested
- power distribution systems for essential core services must be properly managed and serviced to ensure that the integrity of the service is maintained.

[2] Since this incident Veolia has changed its company name to Transdev, but Veolia is used in this report.

2. Conduct of the inquiry

2.1. The Commission was made aware of this incident on 26 April 2012 when news media reported that a power failure had stopped all Auckland metro trains.

2.2. The Commission opened an inquiry the following day under section 13(1)(b) of the Transport Accident Investigation Commission Act 1990, to determine the causes and circumstances of the incident, and appointed an investigator in charge of the investigation.

2.3. Requests for information were sent to KiwiRail on 27 April 2012. During the following week meetings were held with KiwiRail staff in Wellington to determine the circumstances of the power failure at the national train control centre (train control) in Wellington.

2.4. Further investigations and interviews were conducted in Auckland about three weeks later. At the Commission's request the Auckland metropolitan train operator, Veolia, distributed a questionnaire to its train drivers who had been on duty at the time of the incident, for the purpose of determining the risk that train stoppages posed to rail safety.

2.5. Drawings and documents pertaining to the project for the centralisation of the Auckland signal boxes into Wellington train control were obtained and examined.

2.6. On 27 August 2014 the Commission approved a draft final report to be circulated to "interested persons" for comment. The period for comment was extended to 7 October 2014 at the request of a respondent. Two parties responded and KiwiRail offered to present to the Commissioners on their response.

2.7. A revised draft report was provided to KiwiRail for preliminary review and comment and to consider if they still wished to speak to their submission. The final report was approved by the Commission on 28 October 2014 subject to minor changes.

2.8. On 29 October 2014, the Commission wrote to the Chief Executive Officer of KiwiRail describing the final wording of the safety recommendation and seeking KiwiRail's intentions to address the safety recommendation.

2.9. The final report was approved for publication on 29 October 2014.

3. Factual information

3.1. Narrative

The occurrence

3.1.1. On Thursday 26 April 2012, train movements in the Auckland area were being controlled by four train controllers from train control in Wellington. Each controller was operating several zones within the Auckland area from their own workstation.

3.1.2. At 1603, in train control, an electrical short circuit fault developed in a domestic multi-box[3] (or in a device that was connected to the multi-box). The electrical short circuit fault should have caused the closest circuit breaker to trip, which should only have caused a power loss to the workstation that used that multi-box. Instead, a circuit breaker further up the line tripped first, which resulted in a power failure to all four workstations that were controlling the Auckland area[4].

3.1.3. The train controllers at the four affected workstations could not see the status of signals or the positions of trains running in their respective control zones. They were consequently unable to control rail movements. The power failure also prevented their communicating with the train drivers by radio. The train controllers could only use paper timetable diagrams and telephones to check train positions, and global positioning system (GPS) displays on adjacent train control workstations. The train controllers did not have a list of the train drivers' mobile phone numbers at hand. Consequently, they could only establish communication with a driver if that driver had initiated the first call to train control.

3.1.4. The electronic system that controlled the rail network in Auckland recognised that it was no longer connected to a train control operator workstation. It then did what it was designed to do: it defaulted into "safe mode", in which all controlled signals reverted to display "Stop" (red) and rail routes remained in the positions in which they had last been set. Vehicle and pedestrian crossing systems remained fully operational because they were locally controlled and did not require input from the train controllers.

3.1.5. At the time of the power failure there were 27 train services travelling within the Auckland metro area with an estimated load of between 1000 and 2000 passengers. Some trains were near, or could reach, their next stations without having to pass red signals, but others were stopped at red signals in places where passengers could not safely disembark. The network was just entering the afternoon peak travel period. All rail movements in Auckland were progressively stopped.

3.1.6. Veolia operated the rail passenger services throughout Auckland. KiwiRail provided and operated train control services for the controlled rail network throughout New Zealand. The network control manager in train control promptly advised Veolia's service delivery manager in Auckland of the power failure.

3.1.7. The service delivery manager implemented the Veolia emergency plan. Messages were sent to all train managers on their trains, explaining that the power had failed at train control and that all signals had reverted to "Stop". Train managers were expected to inform their drivers of the situation and have them stop at the next stations that they could reach, then remain there for further instructions. If a train were already at a station, the train manager was requested to hold it there. Veolia warned the public about potential delays to scheduled rail services using passenger information displays and public address announcements at all stations. These messages recommended that passengers make alternative travel arrangements.

---

[3] A multi-box contains several distribution socket outlets for connecting multiple electrical appliances to one wall outlet.

[4] Mains power was still available within the train control building. Trains on the rest of the network could still be controlled by their respective train controllers.

3.1.8. KiwiRail called its maintenance support contractor to fix the fault and restore power. Restricted services were restored about one hour later. Full train control operations were back on line soon after that. Scheduled passenger services were affected for the rest of the evening.

3.2. The train control system

3.2.1. The train control system is a duplicated "distributed[5] system". Devices installed around the rail network control the status of signals, rail points and track monitoring equipment. These devices are connected to central control processors in Auckland, which are in turn connected to the train control computer workstations in Wellington train control through a "wide area network". A train control program[6] installed on the workstation computers presents the rail network as an active mimic to the train controllers. The mimic displays the status of the signals, rail points and track monitoring equipment, as well as the positions of trains within sections of track. Train controllers use the mimic diagram to set the routes for trains and to change the status of signals. Their commands are relayed to the devices in the field through the central control processors in Auckland, which then provide information back to the workstation mimic about the status of equipment in the field.

3.2.2. In Wellington train control the Auckland rail area is partitioned into 10 control zones, which are normally controlled by four train controllers from four separate workstations. These four workstations are located together in a room known as the "Auckland control room". A train controller can take control of any number of the 10 zones at once. However, each zone can only be controlled by one workstation at a time.

3.2.3. Each train controller workstation has multiple computers and monitors and associated radio and telephone communication systems (see Figure 1).

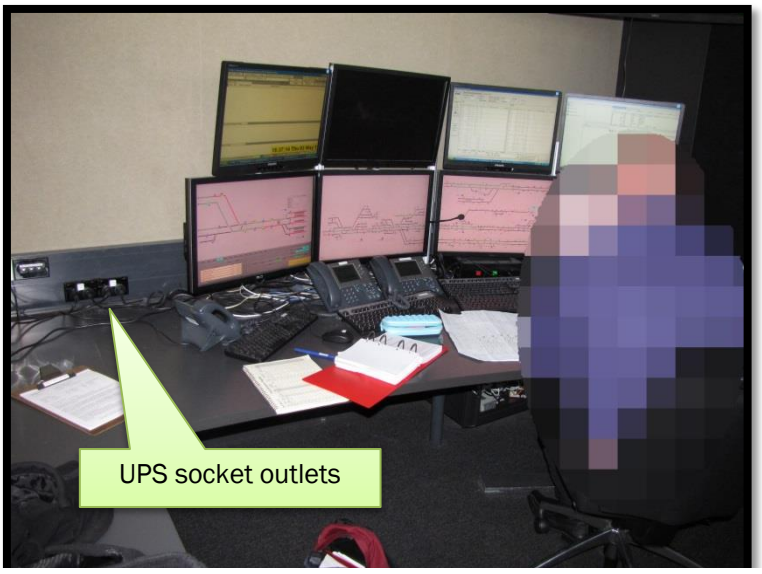


Figure 1
Photograph showing typical train controller workstation at train control

3.3. Background history

3.3.1. This power failure occurred in an area of train control that KiwiRail had recently built to house the train control facilities for the Auckland metro rail network.

[5] A control system that consists of multiple control processors that talk to each other, rather than one central processor.
[6] Rail 9000.

3.3.2. From 1997 until late 2009, the Auckland metro rail network was controlled by a single Wellington-based train controller with the aid of signallers who operated several signal boxes sited around Auckland. A government-funded rail electrification and upgrade project in Auckland had been underway during 2009 to replace the existing diesel locomotives with new electric multiple units.

3.3.3. The project scope included many associated rail upgrades for the Auckland area. As the existing signalling would not be compatible with the changes brought about with the electrification of the rail network, the project scope included a new train control system for the Auckland area and other associated rail upgrades. The signal boxes were to become redundant and be replaced by train control workstations. The signalling contract made provision for control workstations to be in both Auckland and Wellington; however, KiwiRail decided to operate the entire Auckland train control operation from Wellington train control. The KiwiRail Board approved the "train control centralisation project" in December 2009, and a separate project team was set up in Wellington to manage a new sub-project for expanding Wellington train control to accommodate the four new workstations.

3.3.4. A design contract was let and construction works to expand Wellington train control were completed at the end of September 2010. The Auckland signal boxes were gradually decommissioned and Auckland-based train control staff relocated to Wellington during 2011. The new facilities had been fully operational for 10 months when the power supply failed.

3.4. Veolia service delivery operations

3.4.1. Veolia had a separate control room in Britomart Station to manage its passenger operations in Auckland. Several of its monitor screens repeated the Wellington train controllers' views of train movements. These screens reverted to blank red screens when the power failed in Wellington. Veolia also had a real-time train position display system, called RAPID, which helped Veolia operators to establish where trains had been stranded. The Veolia operators were able to use this system to assist the Wellington train controllers to co-ordinate train movements during the power outage. This system used GPS signals from the trains overlaid on an electronic map display of the Auckland area. It was independent of a similar KiwiRail system that covered the entire rail network.

3.4.2. Veolia also had: a selection of Auckland Transport's closed-circuit television cameras displayed on overhead monitors to help manage passenger movements at some Auckland metro stations; message controllers for passenger information displays; public address and intercom systems at all station platforms; and radio and telephone communication systems for its staff operations. Veolia was not able to communicate with train drivers over the radio.

4. Analysis

4.1. Introduction

4.1.1. As a result of a circuit breaker tripping in Wellington train control, train control services for the entire Auckland metro rail network were disabled. The electrical distribution system for train control was supposed to have been designed to prevent a single point failure from affecting the complete system.

4.1.2. There was no risk of trains colliding or proceeding down wrong routes when the train control workstations lost power because the system defaulted to safe mode, as it was designed to do. The train routes remained as they had been set before the power failure occurred and the signals automatically reverted to red ("Stop"), eventually stopping all trains on the network.

4.1.3. Members of the general public using controlled pedestrian and road crossings at the time of the power failure were not at risk. These systems detected the presence of trains near to the crossings and operated automatically without input from the train controllers.

4.1.4. In this case the train control systems were reinstated within one hour and the situation was well controlled by the train operator. There are, however, consequential risks with containing passengers on immobile trains for any length of time, particularly when the trains are at locations where they cannot be safely disembarked.

4.1.5. The following analysis discusses why the power failure occurred and why that resulted in a total loss of train control function for the Auckland area. The analysis also discusses the following safety issues:

- the project team responsible for the Auckland train control centralisation project lacked the appropriate expertise for designing and installing the emergency power supply system
- the management and maintenance of the emergency power supply system for train control were not sufficient to ensure the integrity of what had been designated an "essential service"
- KiwiRail's Risk Management Policy for "continuity of core services" did not give proper consideration to the safety of passengers and crew when a core service such as train control failed, causing the widespread stoppage of an entire metropolitan passenger rail system.

4.2. The power failure

4.2.1. Figure 2 is a simplified schematic of the emergency power distribution system for Wellington train control. The train control workstations were considered by KiwiRail to be "essential services". For this reason a generator was provided as an automatic back-up if the external mains power to the entire building were lost. However, in this case there was no loss of external mains power to the building. Instead, the loss of power affected only the Auckland control room within the building, so the back-up generator was not required and did not start.

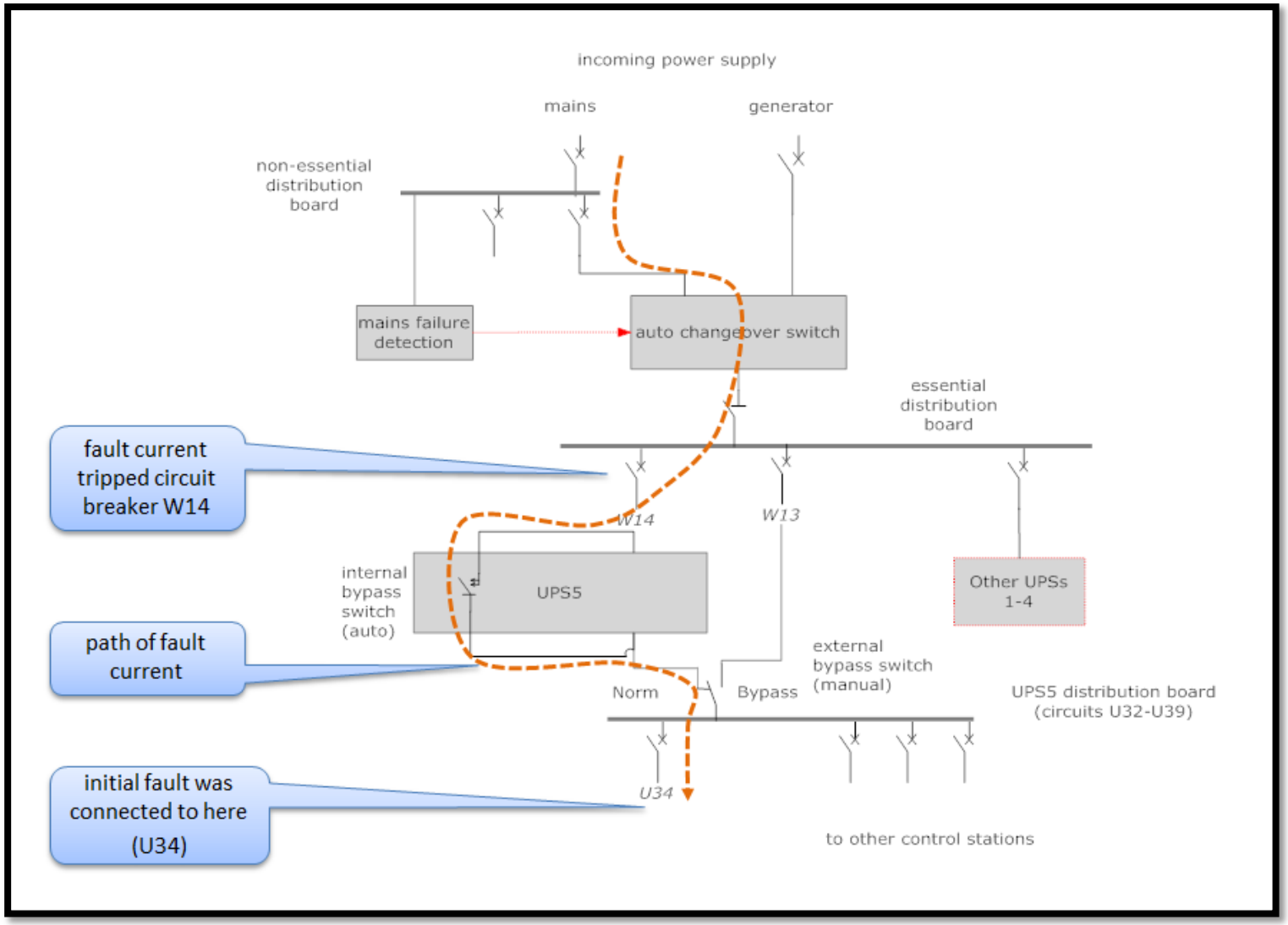


Figure 2
Single line power schematic of train control

4.2.2. Five uninterruptable power supply (UPS) devices were installed in the emergency power distribution system to ensure a constant power supply to the train control workstations. If the mains power supply failed, or was interrupted for any reason, a battery within each UPS continued to supply power to the wall socket into which the various computers and screens making up the workstation were plugged.

4.2.3. UPS number five (UPS5) supplied power to all UPS power sockets in the Auckland control room. The various computers and monitor screens making up each of the four Auckland workstations were plugged into UPS power socket outlets, and where more connections were required multi-boxes were used. Groups of power socket outlets were protected by circuit breakers.

4.2.4. When the fault developed in one of the multi-boxes, or in a device that was plugged into the multi-box, this should have tripped the closest protection device to that fault (circuit breaker U34). Had this occurred, only one of the four Auckland workstations would have been lost. Instead, the next protection device up the line (circuit breaker W14) tripped first, which caused a loss of power to all four Auckland workstations.

4.2.5. Normally, faults downstream of UPS5 would have been isolated from the UPS by a downstream circuit breaker tripping, but in this case UPS5 tried to feed the fault. However, the static inverter[7] in UPS5 was electronically "current limited", and as the fault current continued to flow through the static inverter it heated towards its maximum operating temperature. When the static inverter temperature reached its limit, UPS5 registered a "thermal overload" alarm in the memory and protected itself by switching over to "internal bypass" mode. This had the effect of the fault current passing through both the W14 and U34 circuit breakers in series.

4.2.6. The situation where a fault current flows through two circuit breakers is normal, but an electrical designer's task is to anticipate potential fault situations and select protection trip characteristic curves[8] that ensure a proper discrimination between the two circuit breakers. That is, the circuit breaker closest to the fault would trip first to isolate the fault current and allow the rest of the connected distribution to remain operational (see Appendix 3 for examples of C- and D-type trip curves).

4.2.7. The UPS manufacturer's installation manual recommended that the input circuit breaker (W14) have a 32-amp rating but with a D-type trip curve. It also recommended that the UPS output distribution circuit breakers (U34) have six-amp ratings with C-type trip curves. Instead, both circuit breakers were installed with C-type trip curves. W14 was rated at 32 amps but circuit breaker U34 had a 20-amp rating instead of the recommended six-amp rating. Without the appropriate discrimination between the two circuit breakers, after a period of less than one second from the initial fault occurring circuit breaker W14 tripped, causing the loss of power to all four Auckland workstations.

4.2.8. As UPS5 had already switched to "internal bypass" mode to protect itself from feeding the fault, it was unable to use stored energy from its batteries to maintain power to the workstations. Consequently power was lost to all four workstations controlling the Auckland rail network, bringing all trains on the Auckland network to a halt.

[7] UPS5 converted the direct current (DC) internal battery voltage to alternating current (AC) through an electronic static inverter and supplied this through a distribution board and circuit breaker U34 to the socket outlet.

[8] This is a diagram that graphs current against time for a particular circuit breaker and plots the points where that circuit breaker will trip.

Findings

1. Train control services in the Auckland metropolitan rail network were lost when an electrical fault at one of the four workstations that were being used to control trains in the Auckland area tripped a circuit breaker feeding power to all four workstations.
2. Weaknesses in the design and installation of the emergency power distribution system for train control resulted in an electrical fault that should have been detected and contained in one part of the electrical distribution system, causing a power outage to a much wider portion of the system.

4.3. Design of the electrical systems

Safety issue – The project team responsible for the Auckland train control centralisation project lacked the appropriate expertise for designing and installing the emergency power supply system.

4.3.1. Emergency power supply systems are commonly used in many electrical facilities that require a reliable, continuous supply of electricity. The technology used in them is mature and well known.

4.3.2. The electrical design of UPS distribution systems requires a different approach from that used for standard office fit-outs. Specific needs are considered, such as what would happen to train control workstations if a UPS failed or if it had to be taken out of the circuit for maintenance. The designer has to consider how to combine the UPS protection system with other protection devices.

4.3.3. The manager of the KiwiRail project management office initiated the train control centralisation project through the KiwiRail property department. They engaged a well proven and experienced architect to provide conceptual drawings. The manager then appointed an internal project manager from the project management office to run the project for KiwiRail.

4.3.4. The building architect (construction team project manager) for the train control centralisation project engaged an electrical design company on behalf of KiwiRail to design the electrical distribution for the new rooms that were to house the Auckland train control workstations. The scope of work asked for was for a standard office fit-out. Therefore, expanding the UPS capacity for Wellington train control was not included in the electrical design scope of works.

4.3.5. The KiwiRail Board had previously approved the project budget, which included an allowance to review the UPS capacity and distribution. This work was designated to be carried out during the design/construction phase. However, the architect engaged the electrical design company before the KiwiRail project manager had been appointed. The contractual electrical design scope of work did not include any work associated with the UPS devices.

4.3.6. Once the KiwiRail project manager had been appointed, he included in his strategic project plan[9] that expanding the UPS capability was part of the electrical designer's scope. This strategic project plan was an internal planning document that had no contractual significance. The KiwiRail project manager was unaware at this time that increasing UPS capacity had not been included in the electrical design scope of work.

4.3.7. During May 2010 the electrical design company eventually realised that decisions were required about the UPS capacity. It included additional UPS capacity as a design option in a "Developed Design Report" dated 11 May 2010, for a decision by KiwiRail. The Developed Design Report explained how existing train control workstations were protected by UPS and anticipated that there would be sufficient spare existing UPS capacity for the new workstations. However, if KiwiRail was unable to confirm that the UPS had sufficient capacity,

[9] Strategic project plan, NTCC [National Train Control Centre] Auckland signal box centralisation, version 1.0, 24/6/10.

the electrical design company offered two other options. They were to (a) design the new workstations without providing UPS power, and (b) upgrade the existing UPS to provide UPS-backed power outlets to all new workstations. The report also said that once KiwiRail had confirmed its requirement, the electrical design company would proceed with assessing the impacts on existing infrastructure. KiwiRail verbally confirmed on 3 June 2010 that the new workstations were to be connected to UPS power.

4.3.8. The electrical design company raised the question about the UPS design scope again during a design team meeting with the architect on 27 May 2010, but it was not pursued formally and the contract scope did not change. Instead KiwiRail purchased two new UPS units in late July 2010 that were identical to the ones that were already in use at train control. The electrical design company agreed to duplicate the existing UPS distribution drawings and describe the required modifications to the existing UPS distribution board to facilitate the installation of the new UPS units. The design documentation was issued for tender on 24 June 2010. The UPS coverage had been designed to match the office room layout as would be typical in a standard office fit-out design. UPS5 fed all the power socket outlets in the Auckland control room, and UPS4 fed the power sockets in another room that was to house traction control[10] and the rail network helpdesk operators.

4.3.9. The result was that all four of the Auckland train controller workstations were connected to the same UPS, creating a single point of failure for Auckland's train control, thus not achieving an appropriate level of redundancy for such an essential service.

4.3.10. Several key examples during the project works demonstrated that the UPS-specific design was not part of the electrical design scope:

- the electrical designer was not responsible for selecting the UPS devices, just for replicating existing UPS specifications and distribution drawings copied from the others on-site to enable the physical connection of the two new UPS devices
- the UPS installation manual cautioned about providing adequate circuit breaker discrimination for UPS distribution, and provided examples. KiwiRail did not provide the electrical designer with a copy of the UPS installation manual, so this advice was not reflected in the design drawings
- no allowance was made in the design drawings for UPS redundancy to ensure that if one UPS failed, part or all of KiwiRail's critical train-control services could still operate. The electrical design company was not briefed by KiwiRail about how it intended to operate the new workstations, nor did the design company seek this information. Two new UPS devices were installed for the train control centralisation project. Splitting the four workstations between the two new UPS devices would have provided an appropriate level of redundancy
- the electrical designer did not formally check that the new UPS devices had sufficient capacity for the loads that KiwiRail wanted to connect. Calculations made after the incident, based on information provided to the electrical design company at the start of its engagement, showed that the capacity of UPS5 would have been exceeded once the Auckland train control room was fully operational.

4.3.11. The design process for the portion of the signal upgrade works in Auckland was guided by a well proven international standard[11] for the design of safety-related systems. The standard was focused on the functional safety of electric, electronic and programmable electronic control systems that had safety implications, such as railway signalling systems. This involved defining potential hazards in a safety function then a desired safety integrity level of reliability that the safety function would be performed satisfactorily. For the Auckland design team, it included actions such as preliminary designs being reviewed by an independent design team, and extensive failure-mode analysis and proof-of-design testing.

[10] The monitoring and control of the electric train overhead power network.
[11] Functional safety requirements in accordance with International Electrotechnical Commission Standards IEC 61508.

4.3.12. The same or similar design assurance standards were not applied to the Wellington portion of the Auckland train control facility, even though it was part of the same system and provided the only human-operator interface for the railway signalling system. It became a commercial building refit project but should have been a mix of that plus a complex systems engineering project. The electrical design was reviewed by a KiwiRail engineer, but he said he was more familiar with line-type diagrams than the plan layout format used in the commercial electrical design specifications, and he did not see any associated UPS load calculations. The UPS support technician allocated to the project team left KiwiRail during the project design phase, but his replacement was not familiar with UPS systems and no alternative was arranged. The design team in Auckland responsible for the rest of the train control system was not involved in the Wellington project.

4.3.13. Soon after the power failure, KiwiRail engaged an independent electrical consultant to examine and review the existing train control power arrangements, and report[12]. That report confirmed the safety issues identified during this investigation, identified others and made 16 recommendations for improvement. A paragraph from the executive summary of the report stated:

> The report agrees that the original design concept of the power system for NTCC [the National Train Control Centre] was fit for purpose however the extension of this design for Auckland train control did not fully implement the control redundancy provisions of other sections of train control. There are design detail and implementation shortcomings in the entire National Train Control Centre power system that make it highly likely that if an electrical fault occurs the resultant power outage will be more wide spread through the train control suite than expected.

Finding

3. The project team responsible for the Auckland train control centralisation project did not apply the appropriate expertise to scoping, designing and installing the power management system.

4.4. Risk management

Safety issue – KiwiRail's Risk Management Policy for "continuity of core services" did not give proper consideration to the safety of passengers and crew when a core service such as train control failed, causing the widespread stoppage of an entire metropolitan passenger rail system.

4.4.1. KiwiRail's Risk Management Policy[13] required all business units within KiwiRail to apply the corporate Risk Management Policy and use the associated risk rating assessment matrix. It was used by the project management team for the train control centralisation project. The risk element in the matrix that was most appropriate for assessing train control was called "continuity of core services", but it was based on freight train operations only and did not feature passenger services. Risk assessments for that element were driven by the premise that train control could be out of action for several hours with minimal impact on KiwiRail businesses. The Chief Executive of KiwiRail reiterated this in a report to Auckland Transport about the resilience of a centralised train control after this power failure, saying that, "The safety impacts are very small [referring to disaster recovery after a failure of train control]; in the event of a failure the lights go red and trains stop" (KiwiRail, 2012).

4.4.2. Just prior to the power failure, KiwiRail had sought an external review[14] of the train control facility to assess its vulnerability. That review was referred to by KiwiRail in its report to Auckland Transport above. The external review noted, among other points, that there was a greater risk to the continuity of the Auckland train service while all of the Auckland train controllers were located in a single room, and it recommended that KiwiRail reconsider the

[12] KiwiRail National Train Control Centre – Power system review, J4035, May 2012.
[13] KiwiRail Risk Management Policy, effective from 30 August 2010.
[14] NTCC Risk Analysis Report, revision 1.0, 7 December 2011.

risk consequences for the element in its risk assessment matrix called "continuity of core services".

4.4.3. There did not appear anywhere in the KiwiRail Risk Management Policy a consideration of the risk to passengers and train crews of a long-term stoppage of metropolitan trains in the Wellington and Auckland areas, at peak-hour travel times when crowd control could become a safety issue. Instead it focused on a fixed period of outage involving a single passenger train.

4.4.4. For example, there is a risk that passengers will decide to leave a train forcefully and walk along the railway track to the nearest exit from the rail corridor. Passengers trespassing within the rail corridor are exposed to a high level of risk, not least the risk of trains beginning to move as the system begins to recover. Recent incidents in both Wellington[15] and Auckland[16] and one in Melbourne after the Flemington races (TMSI, 2008) have shown that self-initiated passenger evacuation is a real risk. Following this incident most affected train drivers responded to a questionnaire about the impacts that the power failure had had on their trains, and some reiterated this risk. The trains in Auckland did not have toilets so there was a natural limit to passive passenger containment and some passengers became aggressive towards train crew.

4.4.5. The passengers' safety was promptly managed by Veolia. Veolia had anticipated the possibility of trains being stranded. Veolia immediately activated its emergency plan and stepped up its response actions further when the delay reached 10 minutes, and again after the delay passed 30 minutes. Veolia communicated with the public and helped to subdue any potentially unsafe crowd action. However, had the power failure occurred during peak travel times and continued for longer, the Veolia response plan would have been at increasing risk of not being able to contain the situation.

4.4.6. A proper assessment of the safety risks of such an outage would arguably increase the rating of continuous train control services from "essential" to "safety-critical".

Finding

4. KiwiRail's Risk Management Policy for "continuity of core services" did not give proper consideration to the safety of passengers and crew when a core service such as train control failed, causing the widespread stoppage of an entire metropolitan passenger rail system.

4.5. Management and maintenance of the emergency power supply system

Safety issue - The management and maintenance of the emergency power supply system for train control were not sufficient to ensure the integrity of what had been designated an "essential service".

4.5.1. KiwiRail technicians responsible for the maintenance of the facility said that they were not familiar with the operation of the UPS. They had not been trained on the equipment and at no time during the 18 months in which the system had been operating had they carried out a regular test programme of the emergency power supply system to simulate a power supply failure. The as-built documentation required at the end of the construction phase of the train control centralisation project was not available on-site when the power failed. Later, when trouble-shooting the cause of the failure, electrical engineers were provided with hand-annotated diagrams to work with. No-one had regularly checked the UPS loading or alarm status on the UPS front panel displays. The alarm history showed that UPS5 had overloaded several times after it was commissioned, including at the time the power failed. The alarms recorded in the UPS5 event log showed that:

[15] The Wellington incidents occurred on 4 September 2009, 15 February 2010 and 17 February 2010.
[16] The Auckland incidents occurred on 9 September 2011, 26 April 2012 (this incident) and 14 November 2012.

- on 30 September 2010 the UPS inverter exceeded its safe operating limits
- on 20 December 2010 the UPS inverter exceeded its safe operating limits
- on 19 January 2012 the UPS inverter exceeded its safe operating limits
- on 26 April 2012 the UPS inverter shut down due to thermal overload (the power failure event)
- the UPS had recorded about six months out of about 18 months' total time in service where it had been operating above its "over-temperature" limit[17]
- the UPS ambient air temperature, measured where it passes through the UPS, was 26 degrees Celsius.

4.5.2. During each of these alarms the UPS would have switched to internal bypass, which meant that the connected loads would have been exposed to mains power fluctuations during that time. The total time that UPS5 had been operated in the internal bypass mode since the UPS was commissioned was 382 minutes (more than six hours).

4.5.3. It is good practice to monitor closely UPS units' health status remotely, particularly when they are supplying an essential service. Optional alarm modules for remote alarm monitoring are available for the UPS units installed, but this option was not included in the design scope. KiwiRail purchased and installed UPS remote alarm monitors as part of its safety actions following the power failure.

4.5.4. The multi-boxes purchased for connecting the workstation equipment to the UPS power sockets were not the type fitted with circuit breakers. These multi-boxes would have provided an additional safeguard against more important critical circuit breakers tripping further up the line. Also, there was little control on what equipment was connected to the UPS power sockets. An electrical audit carried out throughout the train control facility after the power failure[18] found several examples where non-essential equipment, such as printers, was plugged into UPS power sockets. Some non-essential closed-circuit television monitors had been connected to UPS5 and would have contributed to its overloaded state.

4.5.5. Solid-state power devices as used in these UPSs are prone to self-destruct from thermal runaway if the device operating temperature exceeds a safe limit. While the particular UPSs are rated to operate at up to 40 degrees Celsius, it is usual to maintain the room temperature for critical computer equipment rooms and datacentres at between 18 and 27 degrees Celsius[19]. Hot spots should be avoided by an appropriate direction of airflow through the equipment racks and monitoring temperatures at critical points. The train control equipment room temperature was set to 20 degrees Celsius. Combined with a likely less-than-optimum cooled air supply to the UPS, it possibly contributed to the high recorded UPS average input cooling air temperature of 26 degrees Celsius.

Finding

5. The management and maintenance of the emergency power supply system for train control were not sufficient to ensure the reliability of what had been designated an "essential service".

[17] Load was above 90% of its rated capacity.
[18] KiwiRail engaged an electrical consultant to investigate and report.
[19] American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE) and Telecommunications Industry Association (TIA) "TIA-942, Telecommunications Infrastructure Standard for Data Centres" recommendations.

5. Findings

5.1. Train control services in the Auckland metropolitan rail network were lost when an electrical fault at one of the four workstations that were being used to control trains in the Auckland area tripped a circuit breaker feeding power to all four workstations.

5.2. Weaknesses in the design and installation of the emergency power distribution system for train control resulted in an electrical fault that should have been detected and contained in one part of the electrical distribution system, causing a power outage to a much wider portion of the system.

5.3. The project team responsible for the Auckland train control centralisation project did not apply the appropriate expertise to scoping, designing and installing the power management system.

5.4. KiwiRail's Risk Management Policy for "continuity of core services" did not give proper consideration to the safety of passengers and crew when a core service such as train control failed, causing the widespread stoppage of an entire metropolitan passenger rail system.

5.5. The management and maintenance of the emergency power supply system for train control were not sufficient to ensure the reliability of what had been designated an "essential service".

6. Safety actions

General

6.1. The Commission classifies safety actions by two types:

(a) safety actions taken by the regulator or an operator to address safety issues identified by the Commission during an inquiry that would otherwise result in the Commission issuing a recommendation

(b) safety actions taken by the regulator or an operator to address other safety issues that would not normally result in the Commission issuing a recommendation.

Safety actions addressing safety issues identified during an inquiry

6.2. KiwiRail took immediate action to investigate and rectify the deficiencies described in this report. Some of the critical points that were corrected were:

- UPS circuit breaker discrimination has been improved for UPS4 and UPS5
- UPS output load diversity in the Auckland control room and the traction control room has been improved
- all UPS alarms are now remotely monitored
- as-built drawings and manuals have been provided and are held on site
- technician training on the UPS has been completed
- the emergency power supply system is regularly tested
- all train control power supply outlets have been audited to ensure loads are connected to the right type of supply
- management control processes are in place to manage new appliance loads in train control.

Safety actions addressing other safety issues

6.3. Nil.

7. Recommendations

General

7.1. The Commission may issue, or give notice of, recommendations to any person or organisation that it considers the most appropriate to address the identified safety issues, depending on whether these safety issues are applicable to a single operator only or to the wider transport sector. In this case, recommendations have been issued to KiwiRail.

7.2. In the interests of transport safety it is important that these recommendations are implemented without delay to help prevent similar accidents or incidents occurring in the future.

Recommendations

7.3. KiwiRail's Risk Management Policy for "continuity of core services" did not give proper consideration to the safety of passengers and crew when a core service such as train control failed, causing the widespread stoppage of an entire metropolitan passenger rail system.

On 29 October 2014 the Commission recommended that the Chief Executive of KiwiRail revise the risk rating assessment matrix in its Risk Management Policy to reflect the fact that train control is a safety-critical service, and to consider the safety of people in crowds when assessing and mitigating the risks. (022/14)

7.4. On 20 November 2014 KiwiRail replied:

> KiwiRail have considered the recommendation and respond as follows:
>
> - The KiwiRail risk matrix, which forms part of KiwiRail's risk management policy, applies across all business units and is designed to provide guidance when assessing many different types of risk for the business.
> - The risk matrix provides a consistent methodology that can be applied across different business units and types of risks.
> - When assessing a risk, the person or project team responsible must consider the context of the risk; the various consequences that may arise should a risk materialise, and the impacts of those consequences. As there may be multiple potential consequences, the consequence with the highest degree of impact should be used as the factor when determining the overall risk rating. Failure to do this may underestimate the level of risk exposure.
> - The Commission have identified that although the initial project team used the risk matrix in order to determine the risk rating, the risk was evaluated based on the impact of continuity of core services being compromised as opposed to potential safety impacts.
> - Rating the risk based only on the impact of continuity of core services resulted in the risk not receiving the required level of management attention. Had the risk been evaluated on the basis of potential adverse safety impacts, the risk would have been rated higher and therefore received the required degree of management attention.
> - It is KiwiRail's view that the risk matrix did not contribute to the failure to identify train control as a business critical risk. Rather, the consequences of the risk were not adequately identified resulting in the risk not being assessed against potential safety consequences on the matrix. This resulted in a risk rating lower than it should have been.
> - A Risk Management Manual was developed in July 2013 to provide guidance to KiwiRail business units in their assessment of risks and the application of the risk matrix. The Risk Management Manual highlights the need to assess all potential consequences and that the highest degree of impact should be used as the factor when determining the overall risk rating. The manual had not been released at the time this incident occurred. It is available to all staff on the KiwiRail intranet and risk assessment practices have improved significantly since this incident occurred.

8. Key lessons

8.1. Projects involving essential core services must be appropriately scoped and resourced to ensure that the service integrity is not disrupted at any time.

8.2. Essential core services must be subjected to a rigorous safety risk assessment process that ensures that the risks to people and infrastructure are appropriately managed and tested.

8.3. Power distribution systems for essential core services must be properly managed and serviced to ensure that the integrity is maintained.

9. Works cited

KiwiRail. (2012, 18 December). *https://at.govt.nz.* Retrieved May 2014, from Auckland Transport: https://at.govt.nz/about-us/our-role-organisation/meetings-minutes/board-reports-2012/ [Board meeting 18 December 2012, Agenda item 10(i)]

TMSI. (2008). *Infrastructure failure, Connex, Kensington/North Melbourne, 6 November 2008.* Melbourne, Australia: Chief Investigator, Transport and Marine Safety Investigations.

Appendix 1: Electrical concepts

The following general electrical concepts are provided for readers if they require further explanation.

Current flow

In simplistic terms, electrical current flows from a source (generator or transformer) through an arrangement of wiring or circuits (distribution) to where it is required by an appliance (connected to a socket outlet). Near the source the distribution system carries a large current, but this is split out at distribution boards into multiple smaller circuits that carry less current.

Fault current

The current that an appliance would normally draw in order to operate is stated on the appliance as the maximum load current. If an electrical fault occurred within an appliance, the load current might increase to above the stated maximum load. If this overload fault current flowed for about four hours at about 1.5 times the maximum rated current for the appliance, the appliance's internal protection device should trip and disconnect the mains supply to it.

Under certain serious fault conditions, such as a short circuit between supply and return conductors or supply and protective earth conductors, the fault current may rise rapidly and exceed the maximum load current by many times. This type of fault is called a short circuit fault and, being the worst possible scenario, is one factor that electrical designers use to determine ratings for electrical protective devices such as circuit breakers and fuses.

Protection devices

The prime purpose of protection in an electrical distribution system is to protect the integrity of the fixed wiring. The fixed wiring distribution in a building stops at the socket outlets where appliances can be connected. Electrical wiring is made to conduct a prescribed current safely, but if this rating is exceeded the wiring may overheat and damage the insulation or cause a fire.

Protection devices are installed throughout a distribution network at the origin of every cable or final circuit that leads from a distribution point. This ensures that if a fault occurs the cables will be protected and it will not prevent other parts continuing to operate normally. In electrical distribution systems the protection devices are generally fuses or circuit breakers that automatically trip when the current flowing through the circuits exceeds pre-set limits.

Most appliances approved for use in New Zealand have some sort of internal protection device to protect the distribution network if a fault develops within an appliance. The standard protection device ratings used in New Zealand for final fixed wiring circuits to socket outlets is either 16 amps (a measurement of the current flowing through the circuit) or 20 amps, but a standard three-pin socket outlet is only rated at 10 amps, so every connectable, portable appliance should not draw more than 10 amps. There are circumstances when the protection rating for a final circuit is reduced below 16 amps, but this is not usual due to the likelihood of false trips.

Portable electrical fittings such as multi-box socket outlets are designed to allow multiple appliances to be connected to one wall socket outlet. The maximum allowable current is set by the socket outlet at 10 amps. Many multi-boxes have internal 10-amp circuit breakers fitted, but some do not. In the latter case the user is expected to limit the connected appliance loads to less than 10 amps, or risk tripping a protection device further up the electrical system.

Load diversity

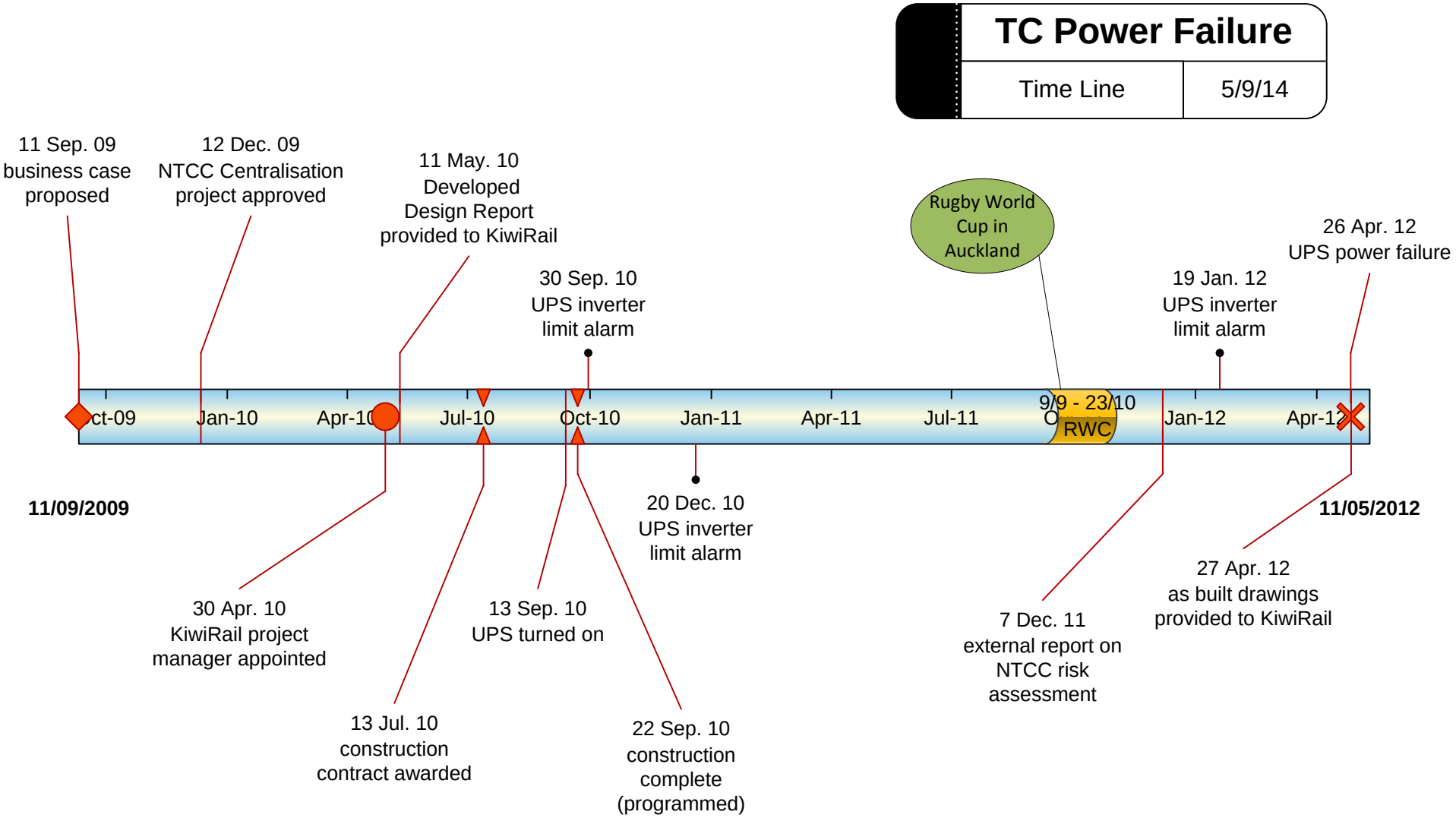
Load diversity in the sense of an electrical distribution network is where the selection of final circuits is arranged to ensure that one circuit breaker tripping will not remove power to 100% of similar services in an area. A common example is with lighting circuits. A typical design would ensure that if a lighting circuit protection device tripped, some lights would still be operational in the area because they are connected to a different circuit. If the lighting loss were 100%, the occupants might find it difficult to evacuate.

Discrimination

Discrimination in an electrical distribution network is about containing a fault in the immediate area of the fault by tripping the circuit breaker nearest to the fault. Generally a fault in commercial premises would occur beyond the extent of the fixed wiring installation, so the nearest protection device would be either the 16- or the 20-amp circuit breaker in the final distribution circuit. All the upstream protection devices would also detect the fault current as it flowed, but should not trip.

An electrical designer usually selects protection devices with trip curves that ensure that although multiple protection devices may "see" a fault current pass through them, only the one closest to the fault will trip. That is, the protection devices will discriminate on which one should trip first. If this does not occur, the fault current will escalate and may eventually trip a protection device further upstream towards the power source or cause damage to the installation. If the upstream protection device trips instead, a wider area is affected by the power loss.

Appendix 2: Timeline



Appendix 3: Examples of circuit breaker trip curves

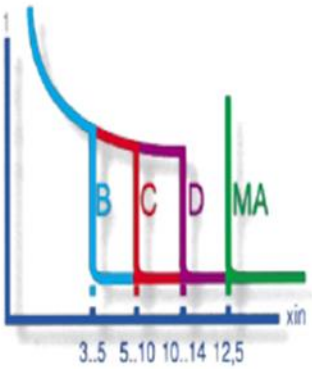
Protection

Merlin Gerin Multi 9 System
Miniature circuit breakers
Tripping curves
Markings & limitation capability

Trip Unit Variations

Circuit Protection

A choice of several curves
Whatever circuit has to be protected, a C60 or C120 circuit breaker provides the perfect solution with a suitable curve.



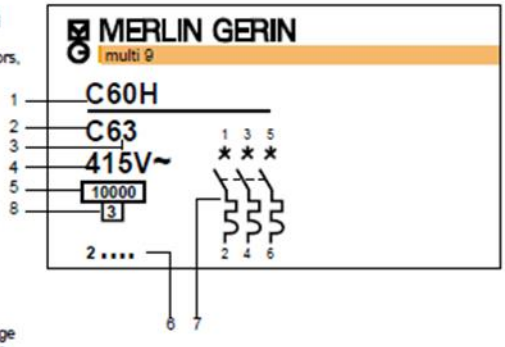
Curve B
tripping:
3 to 5 times the rated current (In);
protection of generators, persons, very long cables.

Curve C
tripping:
5 to 10 In;
protection of circuits, general applications.

Curve D
tripping:
10 to 14 In;
protection of high surge circuits, welders, transformers, motors.

Curve MA
(magnetic only)
tripping: 12 In;
protection of motor starters (+ thermal protection when combined with contactor).

Circuit Breaker Marking



1. Circuit Breaker Model Number
2. Tripping Curve
3. Circuit Breaker Current Rating
4. Operating Voltage
5. Rated Breaking Capacity
6. Circuit Breaker Part Number
7. Electrical Diagram - No. of Poles
8. I²t classification

Recent railway occurrence reports published by the Transport Accident Investigation Commission (most recent at top of list)

Interim Report RO-2014-103	Metropolitan passenger train, collision with stop block, Melling Station, Wellington, 27 May 2014
RO-2013-102	Passenger train travelled with doors open, Wingate - Taita, 28 March 2013
12-101	Load shift on Train 926D struck stationary, Train 845, Main South line, Rolleston, 6 April 2012
11-105	Freight Train 228 wrong-routed, into closed section of track Wiri Junction, South Auckland, 12 November 2011
RO-2013-108	Near collision between 2 metro passenger trains, Wellington, 9 September 2013
11-106	Hi-rail vehicle nearly struck by passenger train, Crown Road level crossing near Paerata, North Island Main Trunk, 28 November 2011
11-102	Track occupation irregularity, leading to near head-on collision, Staircase-Craigieburn, 13 April 2011
RO-2013-104	Urgent Recommendations: Derailment of metro passenger Train 8219, Wellington, 20 May 2013
11-103	Track workers nearly struck by passenger train, near Paekakariki, North Island Main Trunk, 25 August 2011
10-101	wrong route setting, high-speed transit through turnout, near miss and SPAD (signal passed at danger), Tamaki, 13 August 2010
11-104	Freight Train 261 collision with bus, Beach Road level crossing, Paekakariki, 31 October 2011
10-102	collision between 2 metro passenger trains, after one struck a landslide and derailed between Plimmerton and Pukerua Bay, North Island Main Trunk, 30 September 2010
07-102	(incorporating inquiry 07-111) freight train mainline derailments, various locations on the national network, from 6 March 2007 to 1 October 2009
11-101	Wrong line running irregularity, leading to a potential head-on collision, Papakura - Wiri, 14 January 2011

Price $14.00

ISSN 1178-4164 (Print)
ISSN 1179-9102 (Online)