Final report AO-2015-005: Unplanned interruption to national air traffic control services, 23 June 2015

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

Aviation inquiry AO-2015-005
Unplanned interruption to national air traffic control services, 23 June 2015

Approved for publication: September 2017

Transport Accident Investigation Commission

About the Transport Accident Investigation Commission

The Transport Accident Investigation Commission (the Commission) is a standing commission of inquiry and 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 and the public, both domestically and internationally, of the lessons that can be learnt from transport accidents and incidents.

Commissioners

Chief Commissioner	Jane Meares
Deputy Chief Commissioner	Peter McKenzie, QC
Commissioner	Stephen Davies Howard
Commissioner	Richard Marchant
Commissioner	Paula Rose, QSO

Key Commission personnel

Chief Executive	Lois Hutchinson
Chief Investigator of Accidents	Captain Tim Burfoot
Investigator in Charge	Barry Stephenson
General Counsel	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

This report remains the intellectual property of the Transport Accident Investigation Commission.

This report may be reprinted in whole or in part without charge, provided that acknowledgement is made to the Transport Accident Investigation Commission.

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 1982 have been referenced as footnotes only. Other documents referred to during the Commission's inquiry that are publicly available are cited.

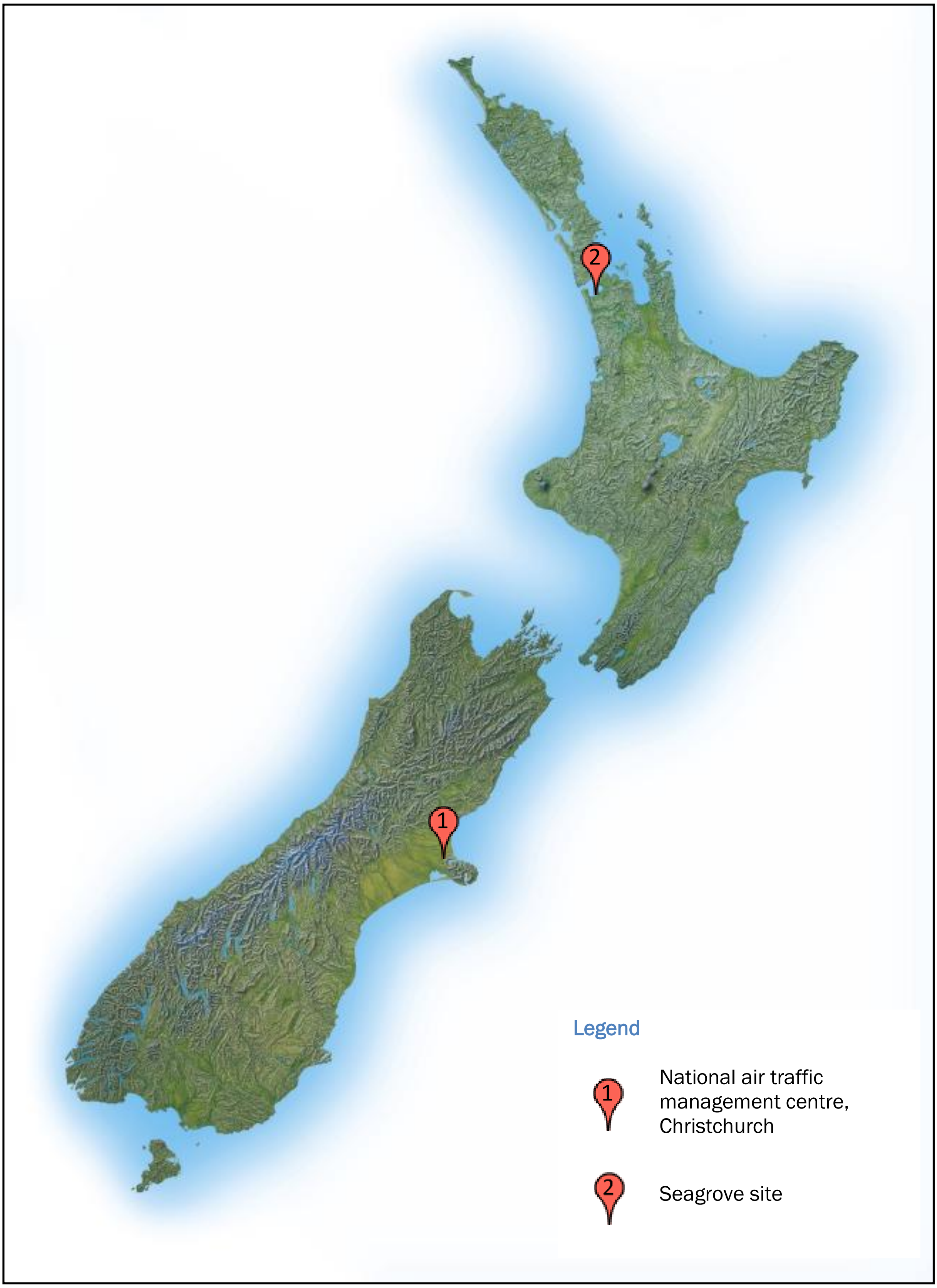
Photographs, diagrams and pictures

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

Verbal probability expressions

The expressions listed in the following table are used in this report to describe the degree of probability (or likelihood) that an event happened or a condition existed in support of a hypothesis.

Terminology (adopted from the Intergovernmental Panel on Climate Change)	Likelihood of the occurrence/outcome	Equivalent terms
Virtually certain	> 99% probability of occurrence	Almost certain
Very likely	> 90% probability	Highly likely, very probable
Likely	> 66% probability	Probable
About as likely as not	33% to 66% probability	More or less likely
Unlikely	< 33% probability	Improbable
Very unlikely	< 10% probability	Highly unlikely
Exceptionally unlikely	< 1% probability	



Source: mapsof.net

Location of major sites

Contents

Figures

Abbreviations

Airways	Airways Corporation of New Zealand Ltd
ATC	air traffic control
ATN	aeronautical telecommunications network
CAA	Civil Aviation Authority of New Zealand
CAR	Civil Aviation Rules
Commission	Transport Accident Investigation Commission
control centre	national air traffic management centre, Christchurch
controller	air traffic controller
DDC	detailed design certificate
ICAO	International Civil Aviation Organization
IPMux	internet protocol multiplexor
OCS	Oceanic Control Service
telco	telecommunications company
VoIP	voice over internet protocol
VLAN	virtual local area network

Glossary

broadcast storm	an extreme amount of broadcast traffic that consumes sufficient network resources so as to render the network unable to transport normal traffic
bypass mode	a display mode for air traffic controller workstations. It uses raw radar data directly from a local radar surveillance unit rather than processed radar data from the control centre
firmware	software that has been saved onto a non-volatile memory chip fitted to a hardware device. The firmware controls how that hardware device operates
multiplexor	a network device that connects multiple inputs to a single data stream output
packet	a collection of digital data transmitted as a unit. It consists of a payload (the information) enclosed within a wrapper
protocol	a set of rules that governs some activity
radar target	processed raw radar data after it has been correlated with an aircraft's transponder code, and the most accurate track, current position and height have been selected from multiple radar sources. This is the normal radar target displayed at an air traffic controller's workstation
raw radar data	raw radar target and track data directly from a selected radar head in the field that has not been processed with other information

Data summary

System particulars

Purpose:	national air traffic management centre
Subsystem:	digital data network
Physical location:	Andy Herd Building, Airways' national air traffic management centre, Christchurch
Operator:	Airways Corporation of New Zealand Ltd

Date and time	23 June 2015 at 1441[1]
Location	New Zealand domestic air space
Consequences	no physical damage, but nearly all air traffic control communication and surveillance services within the New Zealand domestic controlled airspace were disrupted for approximately four minutes

[1] Times in this report are New Zealand Standard Time (Co-ordinated Universal Time + 12 hours) and expressed in the 24-hour format.

1. Executive summary

1.1. On the afternoon of 23 June 2015, the domestic air traffic control services for New Zealand were suddenly and unexpectedly interrupted for about four minutes. During this outage, air traffic sector controllers in the national air traffic management centre at Christchurch lost radar and radio contact with the aircraft under their control.

1.2. Although the sector controllers had alternative radio frequencies and standby radios to contact aircraft, not all of these systems worked as expected.

1.3. The telephone system was also disrupted by the outage, which prevented normal communication between the sector controllers and the airport control towers around New Zealand.

1.4. The radar, radio and telephone services of the national air traffic control system were integrated in a digital data network. The interruption of services occurred when activities during an upgrade program to migrate remaining services on another part of the digital data network inadvertently caused a ‘broadcast storm’. The storm prevented normal digital data traffic from reaching the control centre and thereby interrupted radar surveillance and communication systems.

1.5. The Transport Accident Investigation Commission (the Commission) found that the broadcast storm was initiated by a software code error in a device. The broadcast storm subsided and the systems returned to normal when the device was removed. The national air traffic services were brought back to full service in a controlled manner over the next few hours.

1.6. The Commission found that Civil Aviation Rules Part 171, which defines how an aeronautical telecommunications network is to be managed, was not contemporary for the digital network technology used by Airways Corporation of New Zealand Ltd (Airways).

1.7. The Commission identified the following safety issues:

- Airways’ digital data network did not have the resilience necessary to support an air traffic control service
- the Civil Aviation Authority of New Zealand did not have the appropriate capability to determine independently if the Airways’ aeronautical telecommunications network would perform as the rules required.

1.8. Airways engaged an external specialist organisation to critically review the architecture of its digital data network and how it was managed. Airways has since implemented many of the recommendations made by the external reviewer.

1.9. The Commission made the following recommendation:

- that the Secretary for Transport update and restructure Civil Aviation Rules Part 171.

1.10. The key lessons arising from this inquiry are:

- the incident was a reminder that effective risk management is a continuous process that applies to all aspects of an organisation’s activities. From major projects to minor tasks, consideration must be given to the context of the activity within the organisation’s purpose
- it is important that well-defined processes that are critical to the efficient and safe operation of a system are followed.

2. Conduct of the inquiry

2.1. The Transport Accident Investigation Commission (the Commission) became aware of the national outage of air traffic control (ATC) services through the news media on 23 June 2015. After obtaining more information about the circumstances from the Civil Aviation Authority of New Zealand (CAA) and Airways Corporation of New Zealand Ltd (Airways), the Commission opened an inquiry on 24 June 2015 under section 13(1) of the Transport Accident Investigation Commission Act 1990.

2.2. Three investigators visited the national air traffic management centre (control centre) in Christchurch on 26 June 2015 to gather evidence and conduct interviews. They returned the following week to conduct further interviews with Airways' operational staff.

2.3. On 6 July 2015, two investigators visited the Wellington ATC tower to interview air traffic controllers (controllers) who had been on duty at the time of the outage.

2.4. The Commission contacted five airline operators and talked to 13 pilots to find out how the outage had affected their operations.

2.5. The Commission engaged Liverton Technology Group Limited to provide specialist advice on digital network engineering.

2.6. On 10 March 2016, two investigators conducted follow-up interviews at the control centre.

2.7. Two Commission investigators met with the CAA twice during March 2017 to present findings, consider potential safety recommendations and discuss action the CAA had taken since the outage.

2.8. On 21 April 2017, the investigator in charge met with Airways to present the findings and potential safety recommendations and to discuss action that Airways had taken since the outage.

2.9. On 27 July 2017, the Commission approved a draft final report for distribution to interested persons for comment. The Commission has considered the submissions received and any changes as a result of those submissions have been included in this report.

2.10. On 27 September 2017, the Commission approved this final report for publication.

3. Factual information

3.1. Narrative

Introduction

3.1.1. On the afternoon of 23 June 2015, the domestic ATC services for New Zealand were interrupted suddenly and unexpectedly for about four minutes. During this outage, controllers in the control centre lost radar and radio contact with the aircraft under their control, and communications with airport control towers around New Zealand.

3.1.2. This interruption to services occurred when maintenance activities by a network engineer on another part of the digital data network at the control centre inadvertently caused a broadcast storm.[2]

The control centre

3.1.3. Nearly all of New Zealand's domestic controlled airspace is managed from the control centre located in Christchurch. Workstations dedicated to each of 10 control sectors allow controllers to see, communicate and manage the air traffic movements within their control sectors, and to see aircraft in the adjacent sectors.

3.1.4. A separate control centre in Auckland manages the oceanic controlled airspace beyond the domestic airspace.

3.1.5. Surveillance information is displayed at the control centre workstations on large screens. This information includes radar targets,[3] flight planning data blocks, track vectors and navigational charts. Each controller has a multifunction desk phone system[4] that allows them to communicate via radio or telephone. If this fails, they have a separate standby radio handset and a back-up cell phone.

3.1.6. Raw radar data[5] from surveillance radar sites around the country is received and processed in the control centre's surveillance radar data-processing facility before being displayed as radar targets at the control workstations. Processing the raw radar data adds information that is relevant and specific to each sector controller. This includes filtering out radar targets that are outside the control sector and adding a track, speed vector and data block with flight planning information to each radar target. The radar target symbol and its colour are also changed to provide further information to the controller.

3.1.7. The infrastructure supporting this air navigation service includes a network of communication, navigation and surveillance facilities around the country, a central data-processing system and the user interface software system that enables the controllers to achieve a safe, efficient and orderly movement of air traffic.

3.1.8. All parts of this air navigation system (the system) are connected through a number of digital data networks.

The outage

3.1.9. At 1441 on Tuesday 23 June 2015, most controllers in the control centre experienced a progressive loss of radar target (aircraft) positional accuracy on their display screens. Within a very short period the radar targets turned from green to orange to indicate that only

[2] A broadcast storm is an extreme amount of broadcast traffic that consumes sufficient network resources so as to render the network unable to transport normal traffic.

[3] A radar target is processed raw radar data after it has been correlated with an aircraft's transponder code and the most accurate track, current position and height have been selected from multiple radar sources. This is the normal radar target displayed at a controller's workstation.

[4] The multifunction desk phone system is a voice over internet protocol (VoIP) phone system. It operates through a voice switch that uses the digital data network to make trunk calls.

[5] Raw radar data is raw radar target and track data directly from a selected radar head in the field that has not been processed with other information.

interpolated positions and tracks were being displayed. An interpolated position is an automatically plotted back-up position of an aircraft based on its filed flight plan. Interpolated radar targets are displayed whenever a radar target position has not been updated with raw radar data within a pre-set time period.

3.1.10. The one exception was the Southern Sector covering the Dunedin-Invercargill-Queenstown area. Target information in this sector continued to be displayed normally.

3.1.11. Controllers primarily monitor aircraft compliance with the approved (cleared) flight plans, so they do not need to talk to the pilots often. However, gradually some controllers became aware that they could not communicate by radio with aircraft in their sectors. When this happened, they initially switched to their alternative radio frequencies, which did not work for all controllers who tried them.

3.1.12. The duty manager in the control centre instructed all controllers to stop all aircraft taking off and to land all aircraft in the controlled airspace in accordance with their existing flight plans. He also instructed controllers to increase the minimum vertical and horizontal separation between airborne aircraft.

3.1.13. While controllers were attempting to re-establish radio and telephone communications to put these instructions into effect, the radar targets and voice communications started to come back online. The system outage, including a period of degraded service, lasted four minutes before full functionality was restored.

3.1.14. The control centre management did not know what had caused the outage or if it was likely to reoccur. While the engineering staff investigated the cause, the control centre management decided to remain vigilant for signs of a further outage. No new flight plans were accepted until the Airways Executive Crisis Management Group was satisfied that the network was stable and would remain operational. Normal ATC services were resumed in stages from 1630.

The impact upon aircraft

3.1.15. The weather across the country was generally fine.

3.1.16. There were 42 aircraft flying under ATC within New Zealand's airspace at the time of the outage. Three aircraft were delayed in landing due to their being required to hold en route before they could enter the next sector.

3.1.17. The outage caused 49 scheduled departures to be delayed and 19 flights to be cancelled.

The impact upon airport control towers

3.1.18. The controllers at the four international airports retained communications with aircraft and continued operating with only a minor reduction with the performance of their flight planning systems. They could not contact the sector controllers in Christchurch by phone, but the back-up cell phone system was operational.

3.1.19. The 13 control towers at regional airports retained communications with local aircraft, but lost their surveillance and flight planning systems. They also lost telephone communication with the sector controllers, but could use the back-up cell phones. They had another system that enabled local aircraft movements to be controlled visually with signal lights if required.

3.1.20. The Oceanic Control Service (OCS) in Auckland, which manages air traffic outside the domestic air space, had a partial loss of services but continued to operate with back-up systems. One connection to the aeronautical fixed telecommunications network failed, but the other remained in operation. The surveillance display changed automatically to bypass mode[6] and continued to operate.

Airways' response

3.1.21. The control centre management formed two response groups at 1445: one focused on fixing the problem; and the other on its response to the public and Airways' customers. The Executive Crisis Management Group first met at 1515 and took charge of the public response.

3.1.22. A senior controller was allocated the role of operations crisis manager. He set up a teleconference with local air traffic managers, technical co-ordinators and other selected managers from around the country. He also co-ordinated the immediate technical response to find out what had happened, so that the system could be returned to a fully operational status.

3.1.23. Within three days of the outage Airways had technical representatives from its overseas equipment suppliers on-site and working with its own engineers to identify the cause of the outage. It had simulated the network structure in a laboratory and had confirmed its suspected cause by replicating the outage.

3.2. Background

New Zealand's air navigation services

3.2.1. The Minister of Transport makes rules under the Civil Aviation Act 1990 that define the required air navigation and management services. The CAA is the issuing authority for an operator certificate to provide air navigation services. At the time of the outage Airways was the only certificated provider of these services in New Zealand. The CAA checks Airways' compliance with its operating certificate and the requirements of the Civil Aviation Rules (CAR). The current rules separate air navigation services into two parts: air traffic management under CAR Part 172; and the aeronautical telecommunications network (ATN) under CAR Part 171.

3.2.2. New Zealand's domestic airspace is controlled by Airways at its control centre in Christchurch. In an emergency, control can be handed over to the Main Contingency control centre in Auckland.

3.2.3. Airways also provides aerodrome control services at the four international airports and at 13 regional airports around the country. Tower controllers manage aircraft within the airports' control zones, including aircraft manoeuvring on the ground and those taking off and landing.

3.2.4. A separate OCS control centre is located in Auckland to manage the large area of oceanic air space for which New Zealand is responsible. The OCS can also be managed from a dedicated workstation in the control centre in Christchurch.

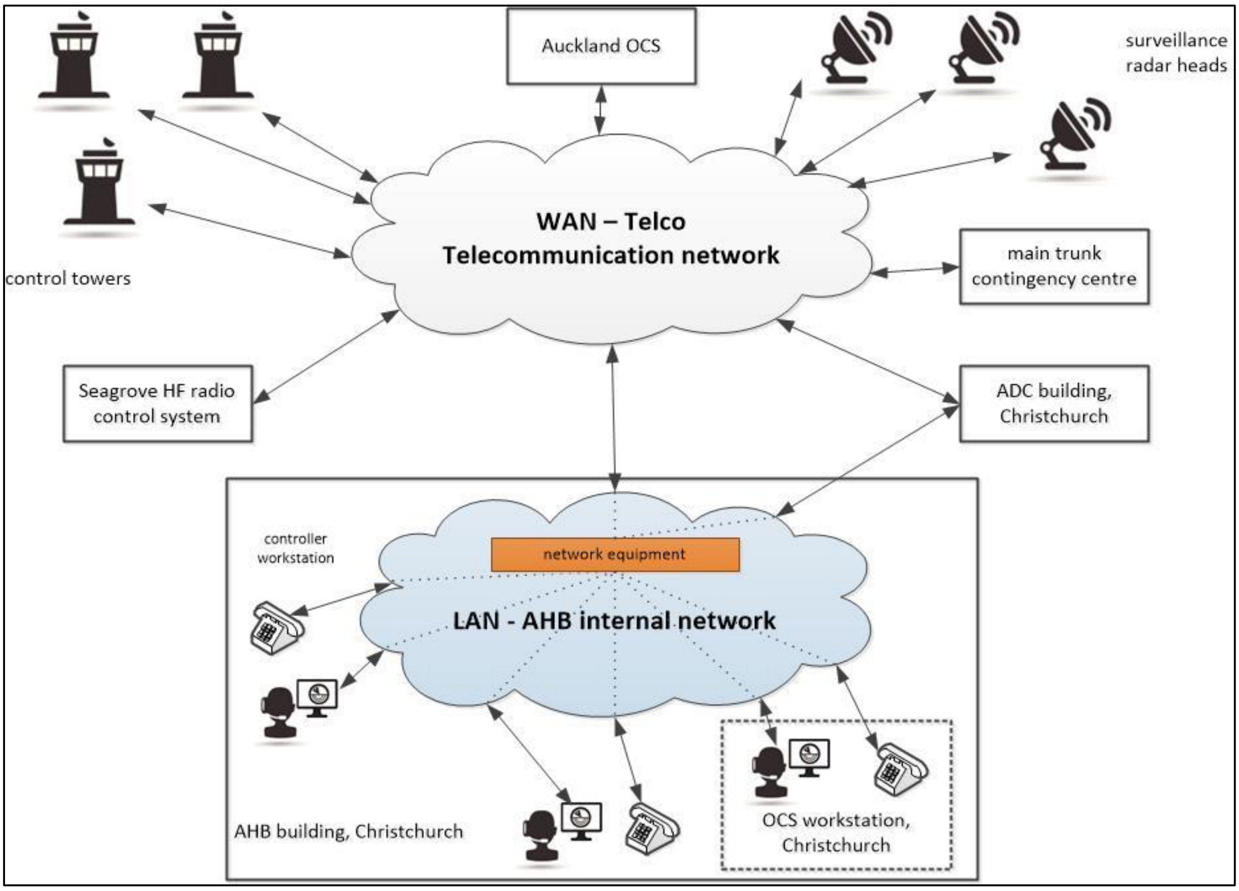
Aeronautical telecommunications network

3.2.5. The ATN includes all of New Zealand's air navigation services and the communication links to the control centre. The ATC part of the ATN includes navigational aids, radio transmitters, radio receivers, radar heads, airport facilities, back-up control centres and control towers (see Figure 1). Airways provides the physical infrastructure at each Airways site. The communication links between sites are generally duplicated and are Airways systems, or provided by one or both of the external telecommunication companies (telcos) with which Airways has agreements.

3.2.6. The ATN is managed by duty technical co-ordinator(s) located at a workstation next to the duty manager of the control centre. The technical co-ordinators are responsible for monitoring the ATN and related Airways' technical systems to ensure that they are operating correctly. The

[6] Bypass mode is a display mode for controllers' workstations. It uses raw radar data directly from a local radar surveillance unit rather than radar targets from the control centre.

technical co-ordinator is the first point of contact for controllers needing to resolve technical problems.



Auckland OCS
surveillance radar heads
control towers
WAN – Telco
Telecommunication network
main trunk contingency centre
Seagrove HF radio control system
ADC building, Christchurch
controller workstation
network equipment
LAN - AHB internal network
AHB building, Christchurch
OCS workstation, Christchurch

Figure 1
The aeronautical telecommunications network (part of)[7]

Digital data network

3.2.7. Since the mid-1990s, digital systems have been used to provide the telecommunications infrastructure for the ATN. This section is a brief description of how a digital data network works.

3.2.8. All information to be transmitted across a digital data network has to be converted to an appropriate digital format, after which it is treated much like a letter in a postal system. Input signals (such as speech for radio or telephone, radar data and control switch selections) are digitised, then transported through the network in data packets[8] to their intended destinations. Each packet includes the address details for its source and each destination. At the destination, the data packets are assembled in the correct order and may be converted back to their original (input) format or used as they are.

3.2.9. If the amount of information to be transmitted is greater than the capacity of one packet, multiple packets are grouped and linked to match the amount of information. The communication is often two-way, so a link between the two communicating devices (called a session) is established first. Once the session is established, the packets can flow between the two devices until the transfer is complete and the session ended. For example, a session would be established for the duration of a telephone call or a radio conversation.

[7] WAN = wide area network; HF = high frequency; ADC = Airways Development Centre (an Airways building); LAN - local area network; AHB =Andy Herd Building; and OCS = Oceanic Control Service.
[8] A packet is a collection of digital data transmitted as a unit. It consists of a payload (the information) enclosed within a wrapper.

3.2.10. Once a packet enters the network it can take a range of paths to its destination. Network equipment (such as a router) reads the address details within the packet and directs it to the next connected device until the packet reaches its destination.

3.2.11. If a route is blocked due to equipment failure, or the data transmission speed through a device is constrained for some reason, the router may send the packet by an alternative route. Some route information is configurable by the user and a router may also run specific programs to add selected network operational features to that device. These options and features are brought into play by the network operator's choice of configuration settings for each device.

3.2.12. Firewalls are placed within the network to monitor all packets that pass through that section. The firewalls check specific details within packets at the start of each session and apply a set of security rules to determine if the packets can pass or will be rejected.

IPMux project

3.2.13. About 18 months before this outage, one of the telcos advised Airways that it was planning to upgrade the network it provided to them for communication links. Once the upgrade was completed, Airways' equipment would no longer be compatible and the telco's current network would be dismantled. Airways was given a deadline to upgrade its own network equipment if it wanted to continue using the telco's (upgraded) network cloud.

3.2.14. Airways started the internet protocol multiplexor (IPMux) project in response. The project included the supply, test and installation of all the necessary equipment. Most of the new network equipment had been installed and services migrated across by June 2015. The system outage occurred while engineers were preparing to migrate one of the remaining services.

4. Analysis

4.1. Introduction

4.1.1. This incident could have presented a significant risk to the safety of air transport if the network had not recovered after a few minutes. Fortunately the outage occurred in daytime, while the weather across the country was good and before the evening peak traffic period. These factors minimised the potential consequences.

4.1.2. The outage exposed a vulnerability in the digital data network, which Airways had previously believed was reliable and resilient to disturbances. The vulnerability was the existence of a single point of failure that could disable all New Zealand's domestic ATC services, including back-up radio communication systems, and adversely affect ATC services in this country's oceanic control area.

4.1.3. The controllers had trained for scenarios in which they lost radio communications or surveillance systems, but not both simultaneously. Airways had considered that concurrent failures were unlikely. The duty manager and controllers adapted standard procedures with which they were familiar and managed the outage safely and effectively. Airways promptly identified the reasons for the outage and made changes to its organisation, the network architecture and its operational procedures to prevent a reoccurrence.

4.1.4. Two safety issues were identified during this inquiry:

- Airways' digital data network did not have the resilience necessary to support an ATC service
- the CAA lacked the capability to determine independently if the Airways ATN would perform as the rules required.

4.1.5. The following analysis explains what happened, discusses these safety issues and recommends actions to prevent a reoccurrence.

4.2. What happened

Informal work on the network

4.2.1. A formal work plan had been set up to transfer one of the few existing services to the new network. This service comprised the air-ground radio communication links between the back-up OCS workstation located in the Christchurch control centre and the high-frequency radio control system located at Seagrove, Auckland.

4.2.2. The project engineers decided that it would be more efficient to conduct a pre-test to ensure that the Christchurch workstation could communicate through the new network to the radio control system in Auckland before the migration work was started. This would be a simple computer-to-computer communication link test through the network and not require any physical changes (see Figure 2). The engineers did not intend to operate the high-frequency radios.

4.2.3. The engineers considered the pre-test to be a minor task that did not require the approval of a formal plan. They considered it to be low risk because it was for a service related to a fourth level of back-up to the OCS. The main operations for OCS were based in Auckland and this work would not affect them. The engineers therefore considered that they needed just the approval of the technical co-ordinator on the day to proceed with the pre-test, and this was obtained.

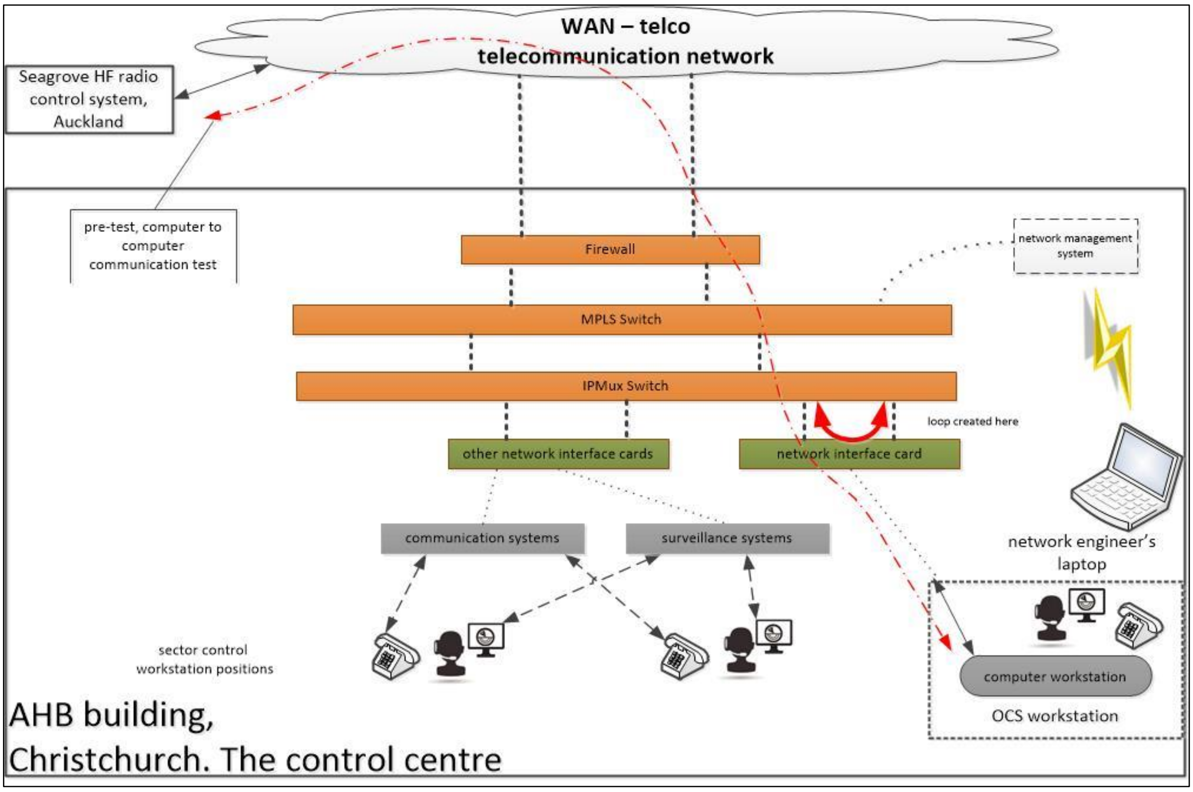

WAN – telco
telecommunication network
Seagrove HF radio control system, Auckland
pre-test, computer to computer communication test
Firewall
network management system
MPLS Switch
IPMux Switch
loop created here
other network interface cards
network interface card
communication systems
surveillance systems
network engineer's laptop
sector control workstation positions
computer workstation
OCS workstation
AHB building, Christchurch. The control centre

Figure 2
Where the broadcast storm started[9]

4.2.4. The network test traffic between the two computers would be transported on the same virtual local area network (VLAN)[10] that carried all services that were essential for the operation of the control centre, but this commonality was not considered at the time to be a risk for the pre-test.

4.2.5. The pre-test was conducted on 16 June 2015, with a radio engineer operating the Christchurch OCS contingency workstation adjacent to the control centre. The radio engineer was unable to get the two computer devices to communicate, so another pre-test was scheduled for 23 June 2015 with a network engineer present to assist.

Further informal work led to outage

4.2.6. On 23 June 2015, the two engineers received approval from the technical co-ordinator to conduct the second pre-test. After it failed again, the network engineer connected his laptop to the network management system and confirmed that the remote and local computer network interface cards were connected and configured correctly (see Figure 2). He found that the operating software (firmware[11]) in the local network interface card between the OCS contingency workstation and the digital network was the factory default version and had to be upgraded.

4.2.7. At the time it was normal procedure for Airways' network engineers to upgrade firmware in network equipment remotely and while the equipment was in an operational mode. The facilities to enable remote network management were standard provisions in the network management software and network equipment. The network team manager explained that remote network maintenance was preferable to sending members of his team to distant sites when he had limited resources.

[9] MPLS = label system.
[10] A VLAN extends across multiple networks to connect equipment as if they are on the same local area network.
[11] Firmware is software that has been saved onto a non-volatile memory chip fitted to a hardware device. The firmware controls how that hardware device operates.

4.2.8. The network engineer proceeded with the firmware upgrade without hesitation. He remotely downloaded the new firmware to the network interface card, then rebooted it to commence the installation process. After a delay that he considered was too long, the network interface card had not come back online, so he went to the equipment room to remove the card from the mounting rack (see Figure 3).

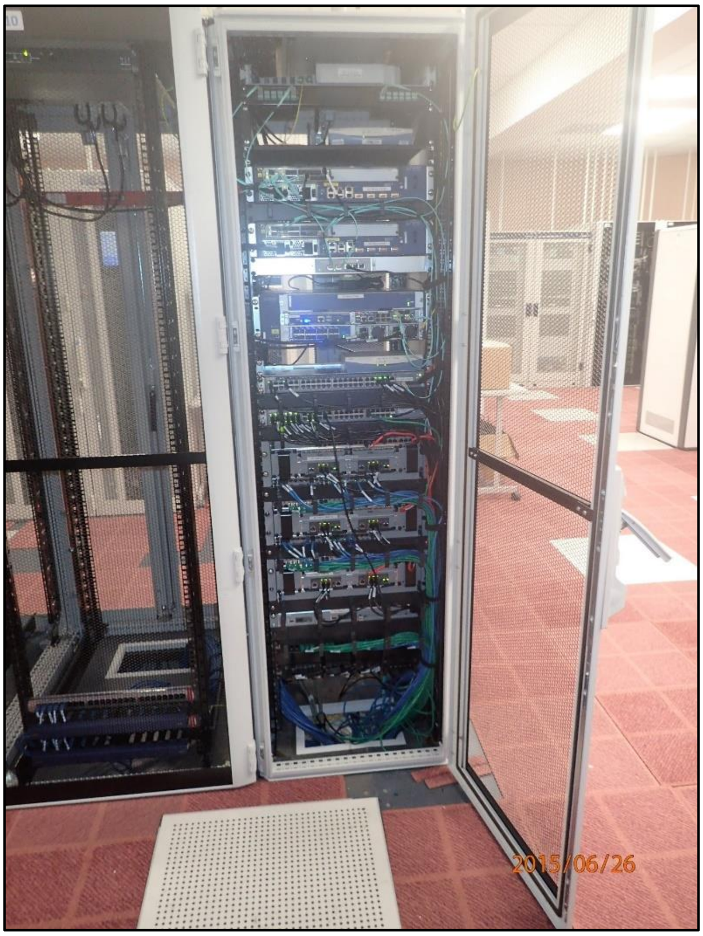


Figure 3
Digital data network cabinet

4.2.9. In doing so he walked through the ATC room and past the technical co-ordinators to the equipment room. He partially extracted the network interface card to disconnect it from the power supply, then left it in the mounting rack while he went to get an antistatic bag to take the card back to the workshop. He was diverted from that task to assist with a major problem that had developed in the control centre. This was the outage.

4.2.10. The outage had started when the engineer rebooted the network interface card, and the disruption began to subside when he disconnected the card from the power supply. He had no idea at the time that his actions had both initiated and stopped the outage. The reboot had created a 'broadcast storm' within the network, and specifically within the VLAN that carried all services to the ATC workstations. The storm had prevented legitimate data packets transported within the VLAN from reaching their intended destinations.

What is a broadcast storm?

4.2.11. An example of a 'broadcast message' is the message packet initiated by a digital network switch to find out what devices it is connected to. In this case the switch broadcasts an 'address request' message to all connected devices to request their address details, then uses the responses to update its switching table. The switch reads the destination address details of all incoming data packets, checks its switching table and forwards the data packets to their correct destinations.

4.2.12. A broadcast storm can be created under certain conditions if a network switch gets a confused response about which devices are connected to its ports, which can then corrupt the switching table. For example, if two ports on a switch are unintentionally looped together through external cables or connections, the switch will send broadcast messages to both ports and they will be received by the same switch through the port at the other end of the loop. Each incoming broadcast message from the loop is re-broadcast to all other ports. This sequence keeps repeating and will rapidly generate a storm of 'address request' messages unless some action is taken to quell them.

4.2.13. The network switching equipment must still manage the address request messages, but the volume of such messages in a storm can overload a switch. An overload prevents the switch passing genuine packets to the appropriate ports and on to their respective destinations. Once genuine packets are hindered, dropped or blocked from passing through the network, user services are affected.

4.2.14. Broadcast storms are a known phenomenon within data networks. Commercial network equipment usually has standard configuration settings and software protocols,[12] such as 'loop detection', 'storm control' and 'Spanning Tree Protocol', to detect the conditions that could initiate a broadcast storm and prevent one building.

What started the broadcast storm?

4.2.15. The firmware in the network interface card had a dormant code error that had escaped the manufacturer's quality assurance tests. It was found later to have an effect only when the firmware was upgraded from the factory default version to the version current at the time of the pre-test. Airways' engineers were not aware that the code error existed either, because they had not made this particular firmware version upgrade. The network interface card was connected to the switch by two separate ports to provide redundancy if one path failed. When the engineer rebooted the network interface card to install the upgraded firmware, the code error took effect. It unintentionally bridged the two ports on the network interface card, which formed a loop in the switch and thereby created the conditions for a broadcast storm.

4.2.16. The switch (called the IPMux switch) to which this interface card was connected had the capability to protect itself against loops and broadcast storms, but this had been disabled in the configuration settings for other reasons (see paragraph 4.3.19). Consequently, a broadcast storm built rapidly and escalated out of control.

How did the broadcast storm cause the outage?

4.2.17. Airways' network was arranged so that all operational telephones, radio, surveillance and runway information services were connected to one common VLAN across the country (called the IPMux VLAN). Other VLANs were also used for related ATC services.

4.2.18. The storm was initiated and contained within the IPMux VLAN, but moved through the adjacent, upstream network switch to the firewalls. Both switches were very high-performance types and had ample processing capacity to handle the broadcast messages and their normal packet traffic, but the firewalls were affected. The firewalls were not able to process both the storm of broadcast messages and apply the security rules to the normal data traffic. The firewalls dropped connections from the normal data traffic in order to respond to the broadcast messages.

4.2.19. The dropped data traffic was the radio and telephone conversations that controllers were conducting and the incoming raw radar data for the ATC data-processing system.

4.2.20. The controllers' digital desk phone system for radio and telephone conversations used the digital data network to make external connections to control towers and radio equipment around the country. As the broadcast storm built, new telephone calls and radio communications to and from the control centre could not be connected to Airways' network.

[12] A protocol is a set of rules that governs some activity.

4.2.21. The controllers' alternative radio frequencies were accessed through the same digital desk phone system and were dependent on the network, so they became unusable. Some of the standby radio systems were connected to the digital telephone exchange and some were hard-wired to an adjacent building. All those connected to the digital telephone exchange were disabled by the blockage at the firewalls.

4.2.22. At the same time, the processed surveillance and flight planning information displayed at controllers' workstations started to degrade as raw data from sources outside the control centre was blocked from updating the ATC data-processing system.

4.2.23. The surveillance data from the southern area of the South Island was not affected by the broadcast storm and was displayed as normal. This data traffic travelled through the same physical firewalls, but the data packets were logically[13] associated with another VLAN (independent of the IPMux VLAN), so were isolated from the broadcast storm.

Effect on airport control towers

4.2.24. All airport towers received their processed radar targets and flight planning information from the data-processing centre at Christchurch, so they suffered the same degradation of processed data as the controllers in the control centre.

4.2.25. International control towers had a local radar data-processing capability that was synchronised with the Christchurch system. However, they also had links to alternative raw radar data directly from their local surveillance radar heads, so they were able to continue to operate with reduced capability in bypass mode. The telephone and radio worked normally for local calls and airport radio frequencies.

4.2.26. Regional towers did not have local data-processing capabilities, so those controllers lost all processed data from their workstation displays. The telephones and radios worked normally for local calls and local radio equipment, but radios that were physically remote and connected through the network would not have worked.

4.2.27. All airport tower controllers were unable to contact the sector controllers in Christchurch using Airways' phone system, but could by cell phone.

Findings

1. The loss of ATC services occurred when a broadcast storm in the Airways digital data network blocked normal communications and raw radar data traffic to and from the control centre.
2. A dormant programming code error in the firmware of a network interface card created a bridge between its two ports during a firmware reboot. Both ports were connected to a network switch at the time, which created a loop and initiated the broadcast storm.
3. The IPMux network switch had the capability to detect and prevent broadcast storms escalating, but Airways had temporarily disabled these mitigation protocols when it configured the switch due to an unexpected side effect. Airways had not made alternative arrangements to protect against broadcast storm events.

[13] This means that the digital code in the data packets separated them from packets in other VLANs.

4.3. Airways' network resilience

Safety issue – Airways' digital data network did not have the resilience necessary to support an ATC service.

4.3.1. Resilience is the ability of a system to recover quickly and provide at least a basic service if some part of it fails or is disabled. In terms of the ATN, resilience is the product of good design with built-in redundancy, sound maintenance processes, and testing to ensure that the overall system remains resilient. This section explains why Airways' ATN lacked sufficient resilience for its intended purpose.

Compliance documentation

4.3.2. The Airways Engineering and Maintenance Group's exposition defined how the group would meet its obligations under CAR Part 171. The exposition linked to the Engineering and Maintenance Group's Information Framework for details of the policy and processes.

4.3.3. The standard Airways design and development process started with a concept design, then progressed through preliminary design to the detailed design phase. Each phase required an approval process to start, and a check and approval process to end. The design certificates for the preliminary and detailed design phases defined the information required for each phase and provided a record of the completed design. The completed design package had to be in a final, approved state and certified to that effect on the design certificate before installation could commence.

4.3.4. The new portion of the digital data network contained within the IPMux project was designed and built by the network team from the Airways Engineering and Maintenance Group.

4.3.5. A contract of service between the Engineering and Maintenance Group and the Service Delivery Group was defined in an Airways document called the Letter of Agreement. The letter included the process for seeking approval to carry out any work on the network and the equipment that was regarded as critical to service delivery.

Network design control

4.3.6. When the Airways IPMux Project Charter was authorised on 1 July 2013, the next step was the detailed design phase. The detailed design certificate (DDC) should have been up to date and approved before installation work started, but the most recent version (obtained five months after the outage) was dated 5 August 2014. It was an old draft version with obvious differences from the system that was installed.

4.3.7. The list of design standards in the DDC omitted some standards that were considered critical, and listed others that were critical but had not been complied with in the design. For example, ICAO (International Civil Aviation Organization)[14] Annex 10, Volume 3 described the basic requirements for an ATN to transport communications and digital data, but was not listed. European Organisation for Civil Aviation Electronics (EUROCAE)[15] standards ED-136 and ED-138, which described the operational and technical requirements for ATNs that transported digitised voice communications,[16] were listed but not met.

4.3.8. The minimum standard required by EUROCAE ED-138 is for data and voice services to be separated logically or physically to maintain their independence.[17] The requirement for separation was specified in Airways' DDC, but was not implemented in the IPMux network. An acceptable option would have been to transport voice and surveillance data on different VLANs. Airways had used VLANs to separate other ATC services in previous network iterations and carried the same grouping over to this new design for the IPMux project. Had the

[14] The ICAO is a UN specialised agency established by states in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).

[15] EUROCAE is a European forum focusing on electronic equipment for air transport, which deals exclusively with aviation standardisation for both airborne and ground systems and equipment.

[16] Commonly called VoIP.

[17] ED-138, Part 1, section 3.5.3.

surveillance and voice services been logically separated into separate VLANs, the outage may have been limited to just communications or surveillance, rather than both.

4.3.9. The DDC had not been updated to reflect the equipment changes made during the design process. The design team had decided to change the network switches to a type from a different manufacturer. The new equipment had different broadcast storm mitigation protocols that were found to have an unexpected side effect, so these protocols had been temporarily disabled. This unrecorded design change therefore had a significant consequence during the events leading to the outage.

4.3.10. The DDC proposed that device configuration settings be recorded in the different network management tools specific to each manufacturer's products, and in a design document for each major component of the new network. Configuration settings for network switches and routers are critical parts of a design that define how the network will operate. It was not clear how, or whether, these settings were designed and approved.

Network drawings

4.3.11. The standard for drawings and documentation required by a DDC for a completed design was defined in the Airways exposition. The exposition required design documents to be traceable and approved with a level of detail 'sufficient to allow the installation engineer to meet the customer requirements'. It went on to state that, 'The watermark shall state "Approved for Detailed Design Purposes, or Installation Purposes as applicable"'. Appendix A in the DDC was supposed to be a register of design documentation, but was blank.

4.3.12. The network design drawings obtained immediately after the outage had not been approved, nor did they show their revision status. The drawings focused on detailed aspects of the digital data network without the high-level system information that would have provided an end-to-end view of how each service would use the digital data network. Several drawings were generic and had been copied to use for other equipment, but the unique connection details did not match. Several drawings with the same number were obviously different and others did not match the equipment that had been installed.

4.3.13. The drawing set was incomplete and should not have been used to install the new network in the control centre. However, the physical installation was complete and had been in operational service for some time when the outage occurred.

Design review

4.3.14. A normal step during a design process is for an independent designer to review the design documents against the design objectives and check key points to ensure that the design can be built and that the documentation is complete.[18] A design review team was nominated in the DDC, but a review did not take place.

4.3.15. After the outage Airways arranged for an independent technical review of its entire ATN and the new network design. The extensive report made many observations and listed 26 recommendations in the subject areas of network design and configuration, network operations, network security and general processes and management. Key recommendations were to strengthen the governance, form an operations support centre and increase staff resources of the network team to match its importance to Airways' service delivery. This included establishing a new network management position that was closer to the General Manager System Operator.

[18] A typical design process that was in accordance with the ISO 9001 standard would include these processes and checks.

Risk management by the network team

4.3.16. The Airways network team had a risk management process for maintenance on the network,[19] but it was not used in every instance and nor was it effective. This section discusses the adequacy of the risk management processes for network maintenance activities.

4.3.17. The network engineering team considered it normal practice to update firmware on network equipment while the equipment was in service and without taking any special precautions. This activity should not have been permitted in a data centre where the risk of something going wrong could have safety implications. It was also contrary to the expectations of the contract for service between the Engineering and Maintenance Group and the ATC Service Delivery Group.

4.3.18. The Letter of Agreement listed 'network equipment' in the highest level of criticality for Airways' ability to manage aircraft safety. Under the terms of the agreement,[20] the network engineer should have sought formal approval to upgrade the firmware on the network interface card. However, as he had already commissioned about 100 of these network interface cards and upgraded their firmware at various times during the IPMux project without a problem, and he was about to undertake what the network team considered a 'normal practice' of upgrading equipment while it was in service, he did not seek formal approval.

4.3.19. When the new IPMux network switches were first installed and configured, the engineers had discovered a conflict between the broadcast storm mitigation software within the switches and another network service. The project manager's decision for dealing with this conflict and higher priority work was to temporarily disable the broadcast storm protocols in the IPMux switches until it could be resolved at a later date. The ramification was that all IPMux switches installed from that date would have been unable to suppress a broadcast storm.

4.3.20. If the disabling of the broadcast storm mitigation had been logged as a system risk, and the engineer had considered that risk when he was thinking about upgrading the network interface card's operating software, the outcome may have been different. Similarly, if the practice of upgrading equipment within an operational environment without taking any additional precautions had included some basic risk management steps, the broadcast storm would not have been created.

4.3.21. Any of the following actions would have minimised or eliminated the risk of a broadcast storm. The engineer could have removed the network interface card and upgraded it in the test lab then reinstalled it. Alternatively, he could have removed one of the network connections from the card and upgraded it in situ, or he could have replaced the card with a pre-tested unit. If he had sought approval from the Service Delivery Group, the decision may have been to postpone the pre-test to a time with minimal impacts on air traffic.

Risk management during historical network maintenance

4.3.22. Samples of the maintenance work planning processes in the six months leading up to the outage[21] were reviewed and found to lack adequate risk management. These contained generic and non-specific information that was copied from one plan to another with minimal change. The sampled plans did not have drawings associated with them. The plans did not consider the possibility of a problem or include 'back-out' actions if the work could not be completed in the approved timeframe.

4.3.23. In the six months before the outage in 2015 and for up to 12 months afterwards, Airways notified the CAA of several network incidents. This period coincided with the commissioning and migration of services to the new network. These incidents were reviewed as part of this inquiry in order to understand the work that was being performed and to identify any common

[19] Defined in the Engineering and Maintenance Group Information Framework.
[20] Section 9.2 of the Letter of Agreement.
[21] These were Network Engineering Notices.

themes. Eleven of the incidents that had some similarities to the outage were examined further in conjunction with Airways.

4.3.24. Two themes were apparent. First, the incidents had surprised the engineers involved because they had initially assessed the work as being non-intrusive to operations. Secondly, the network configuration did not seem to have had the diversity and self-repairing ability that engineers said it was designed to have. The incidents had been disruptive, but digital services had not always transferred automatically to a secondary path when the primary path failed. Both themes pointed to inadequate considerations of risk management during the design of the network and for the maintenance.

4.3.25. The examples of unexpected problems caused during maintenance indicate that the network team's risk management processes were not mature. The Commission previously investigated two incidents involving Airways' systems in 1997 and 2000 that had similar themes to the more recent events (see Appendix 1). International data on such events was not readily available, which could have indicated either that such incidents were not normally reported to, or investigated by, aviation authorities or that they were rare. Either way, the lessons have not been made available to the public.

Risk management for the IPMux project

4.3.26. The design and installation of the new network was managed by a dedicated project manager, but at least two major project risks could only be resolved with corporate input – equipment delivery delays and a lack of project staff resources. Both risks had been identified in the IPMux Project Charter when the project received corporate approval and both materialised with detrimental impacts on the project's delivery.

4.3.27. The telco had set a fixed deadline for Airways to upgrade its network equipment in order to maintain connectivity, and that drove the project timeline. When an international supplier delayed its equipment delivery, Airways' response was to reduce the planned equipment test program to meet the external deadline. During the installation phase the small team of engineers was working long hours and away from home for extended periods. The lack of team resources became a significant risk to the success of the project, and for Airways in terms of the health and safety of the network installation team.

4.3.28. A test laboratory had been proposed, where engineers could create a replica network and test new equipment interfaces, new software and configuration changes before placing them into a production environment. Funding for this laboratory was not approved by Airways' senior management until after the outage.

ATN vulnerabilities exposed by the outage

4.3.29. The outage presented a real situation to test the resilience of the ATN. It exposed a major weakness in that all air traffic services delivered from the control centre were subject to a single point of network failure along with other design vulnerabilities.

4.3.30. Airways had taken steps in its design of the ATN to avoid single points of failure. These included: equipment duplication and physical separation between items of equipment; diverse cable routes; back-up and uninterruptable power supplies; and telco independence. In spite of these efforts the network itself remained common to all services.

4.3.31. The standby radios were connected to the same digital telephone exchange as the main and alternative radio frequencies, and the primary telephones. When the broadcast storm occurred, the digital telephone exchange was unable to make connections through the network to locations outside the building, so the standby radios did not have the intended independence.

4.3.32. Transporting voice communications for telephone and radio on the same logical VLAN as radar data meant that they shared a common potential point of failure. This was contrary to the best advice provided in EUROCAE's minimum specification, ED-138.

4.3.33. The earlier postponement of efforts to resolve the question of why the broadcast storm mitigation protocols of the IPMux switches did not work with other network services, and the decision to disable this feature temporarily left the network vulnerable to further loss of services.

4.3.34. An analysis of the configuration tables of the two switches directly involved in the outage revealed another deficiency that could have made the network less resilient. Some VLAN services passing in parallel between the two switches to the two firewalls would not have had an alternative route if the primary route had failed. In that event information would have been lost.

4.3.35. The two firewalls were also effectively placed in the centre of the internal network, rather than at the periphery. That was an inappropriate location for the network architecture, because it would likely have required the firewalls to make routing decisions for the data packets, as well as perform their prime function of making security decisions about through-traffic. This extra processing load for an already complex operating characteristic turned the firewalls into a single point of failure when they were faced with the broadcast storm from inside the network.

Training

4.3.36. The Engineering and Maintenance Group procedures required work requests to be reviewed and approved by technical co-ordinators. The technical co-ordinators on duty at the time of this outage, in common with other technical co-ordinators, did not have sufficient technical knowledge of the network structure and operation to assess properly the impact risk of network maintenance tasks on ATC.

4.3.37. The technical co-ordinators were familiar with aeronautical navigation systems, but less so with digital data networks. In general they had not been trained on the digital data network, so they lacked the knowledge and skills to make informed decisions about the risks to ATC services of proposed network maintenance. There was a lack of system drawings and explanatory documentation to show the technical co-ordinators how the ATC system used the network, so they had to rely on the advice of the network engineers.

4.3.38. Airways realised this weakness after the outage and implemented network familiarisation training for the technical co-ordinators and others who had an interest. Formal training modules have been put in place and now there is more contact and information sharing between the technical co-ordinators and the network engineers.

4.3.39. Airways also realised that network engineers lacked the skills to evaluate risk at a corporate level. Formal training in risk management has been conducted with the network engineering team.

The network team management

4.3.40. The network engineering team had been formed relatively recently, whereas the ATN (in various arrangements) had been managed by Airways for a long time and had established a track record of reliability.

4.3.41. The network engineering team's importance and responsibility had grown significantly as the ATN had become more dependent on digital data networking to connect Airways' infrastructure. Airways' organisational structure had not been altered to reflect the growing significance, which meant the team's management was several levels removed from the General Manager System Operator. This distance was likely as not a factor in the team being under-resourced for the IPMux project, and its inadequate approach to risk management.

4.3.42. Airways has made changes to improve the management and functioning of the network team to improve its performance (see section 6).

Findings

4. Airways' policy was not followed in the design process for the new digital data network. This resulted in design documentation that was not controlled or approved, and contained errors and omissions that made the documentation unfit for purpose.
5. The risk management process generally used by Airways' network engineers for planned network maintenance did not take proper account of the context of the work, or whether it was appropriate to be performed in the production environment, and therefore created some unexpected service disruptions to air navigation services.
6. The digital data network in the control centre had design vulnerabilities that had not been adequately considered or tested. This led to the outage being unexpected and having a greater effect on the ATC system than anticipated.
7. Airways had not trained the technical co-ordinators adequately to allow them to make informed decisions about the risks to service delivery of proposed maintenance on the digital data network.
8. The team responsible for the design, procurement, installation and commissioning of the new network did not have sufficient authority to manage significant project risks properly.

4.4. The CAA overview of the Airways network

Safety issue – The CAA did not have the appropriate capability to determine independently if the Airways ATN would perform as the rules required.

4.4.1. The CAA audited the provision of ATN services against CAR Part 171. The rules listed specific air navigation services such as non-directional beacons, distance measuring equipment and radio navigation aids. Further system and technical specifications were expected to comply with ICAO Annex 10, Volumes 1, 3 and 4, where appropriate. The rule defined the requirements in terms of the services required, documentation, manuals, operation, maintenance, management and quality assurance. Service providers such as Airways described in their expositions how these requirements would be met.

4.4.2. ICAO Annex 10 contained standards and recommended practices, but left options up to the respective states' civil aviation authorities. CAR Part 171 did not specify the options from ICAO Annex 10 that were appropriate for New Zealand.

4.4.3. CAR Part 171 was written in 1992 and had not been updated since to accommodate changes in the technology typically used by an ATN certificate holder in 2017. For example, the non-directional beacons listed were planned to be decommissioned in the near future and data networks were not mentioned. The digital data networks are an essential component of Airways' business, linking the ATN and ATC services, both of which incorporate increasingly advanced subsystems.

4.4.4. Although Part 171 was outdated, Airways had adopted new technology to modernise the ATC system, and had revised its exposition to reflect the changes. As Airways was the sole provider of both ATC and the ATN, it was able to define its technical requirements for the ATN in the Letter of Agreement between the two internal groups of Airways. The Letter of Agreement was outside the CAA's audit scope.

4.4.5. This arrangement led the CAA to stand back from auditing the wider network systems and processes that were not in CAR Part 171 and to concentrate on the traditional equipment and systems covered by the rule and ICAO Annex 10. However, by adopting this position the CAA allowed its internal technical knowledge and familiarity with Airways' systems to decline.

4.4.6. From the mid-1990s, digital data networks became more prevalent in the primary systems that underpinned Airways' ATN, but they were not listed in the Airways exposition. The CAA did not enquire into the design or maintenance of the digital data network systems or the ATC software systems, but did consider their overall performance as part of the complete ATN. At the time of the outage the CAA did not have the expertise necessary to conduct an effective audit of the technology or processes that Airways used to support the digital data network. The CAA Part 171 auditor in 2015 had no experience with digital data networks and retired shortly after the outage, leaving the position vacant.

4.4.7. At the time of the outage the digital data network was not listed in the exposition as one of the facilities that Airways provided, so it would not have been a focus for CAA audits either.

4.4.8. The future of New Zealand's controlled airspace has been set out in a plan called the New Southern Sky, which is led by the CAA in association with Airways and the Ministry of Transport. This is part of an international ICAO plan to update the global air navigation systems. A crucial part of this new plan is the digital data network that will support all the various aspects of the air navigation service.

4.4.9. As the performance of the New Southern Sky will have a high dependency on digital data networks, the CAA will need to maintain an active role to ensure that network performance and resilience are maintained at acceptable levels for the global system. This will include having the in-house technical capability and familiarity with all technology and software systems that Airways uses to provide the air navigation system, so that the CAA can understand how they work, how they are used and what performance to expect, and ensure that any potential vulnerabilities are managed.

Findings

9. CAR Part 171, which defines the requirements for an aeronautical telecommunications certificate holder, is not contemporary for regulating a modern aeronautical telecommunications system that uses technology such as digital data networks.
10. CAR Part 171 limited the CAA to an audit scope that reflected the technology environment of aeronautical telecommunications that were in place in 1992 when the Rule Part was developed.
11. The digital data network was a major part of the air navigation system provided by Airways, but the CAA did not have the capability in-house to audit or review the network's performance and management.

5. Findings

5.1 The loss of ATC services occurred when a broadcast storm in Airways' digital data network blocked normal communications and raw radar data traffic to and from the control centre.

5.2 A dormant programming code error in the firmware of a network interface card created a bridge between its two ports during a firmware reboot. Both ports were connected to a network switch at the time, which created a loop and initiated the broadcast storm.

5.3 The IPMux network switch had the capability to detect and prevent broadcast storms escalating, but Airways had temporarily disabled these mitigation protocols when it configured the switch due to an unexpected side effect. Airways had not made alternative arrangements to protect against broadcast storm events.

5.4 Airways' policy was not followed in the design process for the new digital data network. This resulted in design documentation that was not controlled or approved, and contained errors and omissions that made the documentation unfit for purpose.

5.5 The risk management process generally used by Airways' network engineers for planned network maintenance did not take proper account of the context of the work, or whether it was appropriate to be performed in the production environment, and therefore created some unexpected service disruptions to air navigation services.

5.6 The digital data network in the control centre had design vulnerabilities that had not been adequately considered or tested. This led to the outage being unexpected and having a greater effect on the ATC system than anticipated.

5.7 Airways had not trained the technical co-ordinators adequately to allow them to make informed decisions about the risks to service delivery of proposed maintenance on the digital data network.

5.8 The team responsible for the design, procurement, installation and commissioning of the new network did not have sufficient authority to manage significant project risks properly.

5.9 CAR Part 171, which defines the requirements for an ATN certificate holder, is not contemporary for regulating a modern aeronautical telecommunications system that uses technology such as digital data networks.

5.10 CAR Part 171 limited the CAA to an audit scope that reflected the technology environment of aeronautical telecommunications that were in place in 1992 when the Rule Part was developed.

5.11 The digital data network was a major part of the air navigation system provided by Airways, but the CAA did not have the capability in-house to audit or review the network's performance and management.

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. Airways resolved the problems it had with running broadcast storm protocols in its new network equipment and rolled out this change to the whole network.

6.3. The network maintenance procedures were reviewed and significantly revised to manage risks to service delivery from network maintenance works. This change included a strengthened process for Airways' Network Engineering Notice form and a risk assessment process through a Change Advisory Board.

6.4. Airways restructured the Engineering and Maintenance Group to create a new senior leadership team manager responsible for the enterprise architecture and networks. This appointment more aptly reflects the contribution that digital data networks make to the provision of Airways' air navigation services.

6.5. Airways developed training modules for the digital data network and ensured that the technical co-ordinators gained the required knowledge to manage the system safely.

6.6. The network engineering drawing standards and approval process were brought into line with the standard Airways expected from the rest of the organisation.

6.7. Airways engaged an external specialist organisation to critically review the architecture of its digital data network and how it managed it. Airways has already implemented many of the recommendations that this organisation made.

6.8. The CAA recognised the need to maintain organisational capabilities to allow it to appropriately identify and monitor risk that may be present within the aviation system as a result of ongoing and often rapid technological advances. It has addressed this risk by ongoing learning and development training for regulatory staff, revision of position descriptions and recruitment or secondment of new staff. The CAA engaged a replacement auditor for CAR Part 171 who is more familiar with digital data networks and in 2016, and updated the position description for the auditor role to include experience in air navigation and air traffic management technology.

Safety actions addressing other safety issues

6.9. Airways recognised that the network engineers lacked an appreciation of risk management from an organisational perspective. A training module has been developed to focus network engineers on how their work could affect the organisation's ability to meet its service delivery obligations. This training has been rolled out across the team.

6.10. Airways recognised that the network team was under-resourced to meet its organisational needs. New staff have been engaged and the team split into four groups to focus on network design, network support, security and the right architecture to support the future enterprise needs.

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 the Secretary for Transport and the CAA. 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

7.2. The current CAR Part 171 has become outdated owing to the natural growth and development of technology and software used to provide a modern air navigation service. In its current form the rule inhibits the CAA from ensuring that the air navigation service meets New Zealand's expectations and obligations to the ICAO.

On 28 September 2017, the Commission recommended that the Secretary for Transport update and restructure CAR Part 171 to include the wider scope of technology, software and navigation aids that are normal for a modern air navigation service and to make provision for the rule to cater for future changes in technology. **(028/17)**

7.2.1. On 20 October 2017 the Secretary for Transport replied:

> The Ministry recognises there have been considerable technology developments since the introduction of the CAR Part 171 in 1992. In light of this, I agree there is a need to review the rule.
>
> I am advised that the Civil Aviation Authroity (CAA) shares this position and are progressing with the rule consideration process. The Ministry will work closely with the CAA to progress the rule changes, and will keep the Transport Accident Investigation Commission (the Commission) informed of the progress of any changes to the rule, and any other work that relates to the Commission's recommendation.

8. Key lessons

8.1. The incident was a reminder that effective risk management is a continuous process that applies to all aspects of an organisation’s activities. From major projects to minor tasks, consideration must be given to the context of the activity within the organisation’s purpose.

8.2. It is important that well-defined processes that are critical to the efficient and safe operation of a system are followed.

9. Works cited

TAIC. (1997). *Air traffic control communications system failure, Christchurch area control centre.* Wellington, NZ: Transport Accident Investigation Commission.

TAIC. (2000). *Temporary loss of air traffic control communications system, Christchurch main trunk air traffic services centre.* Wellington, NZ: Transport Accident Investigation Commission.

Appendix 1: Other similar incidents

1. Commission investigations

1.1. In 1997, the Commission investigated a communications outage in the Wellington terminal area sector operated from the Christchurch air traffic management centre (TAIC, 1997). The terminal area sector lost main, alternative and standby radio frequencies for six minutes. It took another seven minutes to restore radio communications to the affected aircraft.

1.2. The outage occurred when an engineer upgraded the operating software in a network multiplexor[22] while it was in service and being used for air traffic management. When the multiplexor was rebooted to complete the upgrade, all digital services connected through it were disrupted rather than being rerouted through an alternative path.

1.3. The Commission found that if the technician had not disconnected the multiplexor, the outage would have spread to other network equipment. This suggested, but was not stated, that it was caused by a broadcast storm.

1.4. In 2000, the Commission investigated another outage in the Christchurch air traffic management centre when all sector workstations lost radio and telephone services for five minutes (TAIC, 2000).

1.5. The outage occurred when technicians were modifying the battery back-up to a voice switch,[23] but accidently tripped the power supply to it.

1.6. The investigation found that the drawings used by the technicians did not match the installed system and it led to their accidentally activating a trip relay.

2. United States telecommunications infrastructure outage, 19 November 2009

2.1. As the Federal Aviation Administration's flight data-processing telecommunications network was being migrated from a copper to a fibre backbone, a new router installed as part of the migration works failed. The failure required air traffic controllers to revert to manual flight data-processing procedures for five hours, causing delays for more than 800 flights.

2.2. The cause was identified as a router configuration error. When the new router started up, it expected a copper link between Los Angeles and Salt Lake City to be a high-capacity fibre optic link, so it directed all national data traffic through it. The equipment was not able to handle that capacity, so data either was corrupted or did not get to the destination. The router had sent alarm messages to the network monitoring system but that was switched off at the time. Additionally, all monitored alarms from the router's site location had been unintentionally suppressed when the intention was to suppress spurious alarms from a single faulty device at the site.

3. National air traffic system in United Kingdom, 12 December 2014

3.1. The national air traffic system's flight data processing was arranged with a central computer and remote terminals. The software had been set up to connect a maximum of 150 terminals, so when an extra one was connected without knowledge of this limit, the system shut down.

3.2. Air traffic controllers had to revert to manual procedures for all traffic in and out of London for six hours before the automatic flight data processing was re-established.

[22] A multiplexor is a network device that connects multiple inputs to a single data stream output.

[23] A voice switch provides a similar function to a business as a private telephone exchange.

Recent Aviation Occurrence Reports published by
the Transport Accident Investigation Commission
(most recent at top of list)

AO-2016-004	Guimbal Cabri G2, ZK-IIH, In-flight fire, near Rotorua Aerodrome, 15 April 2016
AO-2015-001	Pacific Aerospace Limited 750XL, ZK-SDT, Engine failure, Lake Taupō, 7 January 2015
AO-2013-010	Aérospatiale AS350B2 'Squirrel', ZK-IMJ, collision with parked helicopter, near Mount Tyndall, Otago, 28 October 2013
Addendum to final report AO-2015-002	Mast bump and in-flight break-up, Robinson R44, ZK-IPY, Lochy River, near Queenstown, 19 February 2015
Interim Report AO-2017-001	Collision with terrain, Eurocopter AS350-BA, ZK-HKW, Port Hills, Christchurch, 14 February 2017
AO-2013-011	Runway excursion, British Aerospace Jetstream 32, ZK-VAH, Auckland Airport, 2 November 2013
AO-2014-006	Robinson R44 II, ZK-HBQ, mast-bump and in-flight break-up, Kahurangi National Park, 7 October 2014
Interim Report AO-2016-007	Collision with terrain, Robinson R44, ZK-HTH, Glenbervie Forest, Northland, 31 October 2016
AO-2014-004	Piper PA32-300, ZK-DOJ, Collision with terrain, Near Poolburn Reservoir, Central Otago, 5 August 2014
AO-2015-002	Mast bump and in-flight break-up, Robinson R44, ZK-IPY, Lochy River, near Queenstown, 19 February 2015
AO-2013-008	Boeing 737-300, ZK-NGI, Loss of cabin pressure, near Raglan, Waikato, 30 August 2013
AO-2013-003	Robinson R66, ZK-IHU, Mast bump and in-flight break-up, Kaweka Range, 9 March 2013
AO-2014-002	Kawasaki BK117 B-2, ZK-HJC, Double engine power loss, Near Springston, Canterbury, 5 May 2014
AO-2013-006	Misaligned take-off at night, Airbus A340, CC-CQF, Auckland Airport, 18 May 2013
AO-2010-009	Addendum to Final Report: Walter Fletcher FU24, ZK-EUF, loss of control on take-off and impact with terrain, Fox Glacier aerodrome, South Westland, 4 September 2010

Price $15.00

ISSN 1179-9080 (Print)
ISSN 1179-9099 (Online)