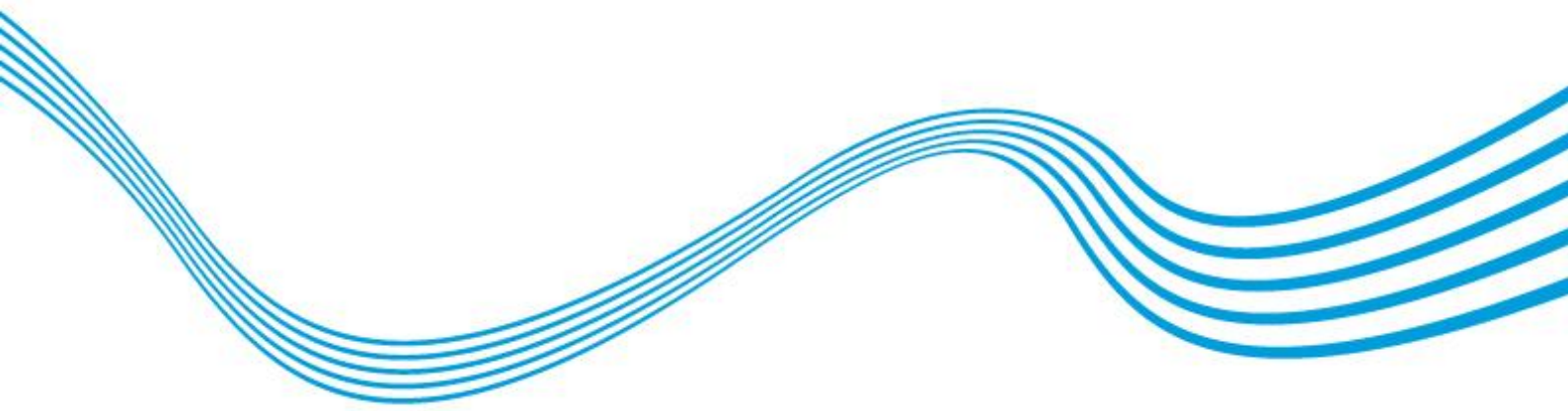
NATS

Air Traffic Control Disruption 7th December 2013

A Report to the Civil Aviation Authority

Version: **Final** – 3 July 2014



Air Traffic Control Disruption on 7th December 2013

Contents

Appendices:

A. Post Event Consultation with Customers and Stakeholders

B. Wider Communications – on the day and post-event

C. ATICCC Coordination with Customers

D. Independent Assessment of the Engineering Response

E. Evidence of Historic System Resilience Levels

London Area Control Operations Room, Swanwick Centre

1 Executive Summary

1. NATS manages air traffic flying in Britain's airspace to ensure the safety of aircraft. It owns and operates critical parts of the UK's national transport infrastructure, including its two air traffic control (ATC) centres at Swanwick and Prestwick. It employs c.4,500 people and handles c.2.2 million flights each year. The company is a commercial enterprise, operating under a Licence from the industry regulator – the Civil Aviation Authority (CAA) – and charging airlines fees for providing its services.

2. ATC operations and technology are generally extremely robust. For example, throughout the unprecedented weather and storms in 2013, NATS' technical and operational contingency measures helped ensure that airports and airlines could continue to operate safely in extremely demanding circumstances.

3. However, a technical failure at the Swanwick ATC Centre early on Saturday 7th December 2013 caused significant disruption to air travel throughout that day. While NATS' contingency arrangements enabled over 90% of flights to operate that Saturday, some 300 flights were cancelled, hundreds more delayed and thousands of passengers left frustrated at airports.

4. NATS recognises that it suffered a significant failure and regrets the considerable impact it had on air travel. Having issued an unreserved apology to all affected, NATS launched immediate investigations into why this system failure resulted in such disruption. These investigations have identified a range of improvements against a background of high levels of resilience in NATS' operations and systems.

5. This Report presents the findings of those investigations.

What happened on Saturday 7th December 2013

6. ATC systems are recognised as being highly complex, integrating many diverse technologies, components and data to enable controllers to safely manage high volumes of aircraft in the UK's densely packed airspace. Accordingly, NATS' systems and procedures are designed to specifically minimise the probability and impact of any technical failure. While elements of ATC systems do fail, they are designed with redundancy and NATS' tried and tested processes normally make such failures virtually invisible to air travel. In situations where there is an impact, the fall back approach is to preserve safety above all else, sacrificing capacity if necessary. This is standard practice across ATC services worldwide.

7. On the night of 6/7 December 2013, NATS' engineers were carrying out an update of the Voice Communication System (VCS) at Swanwick Area Control (AC) as part of a series of overnight activities on some 20 systems at the Centre.

8. During the VCS update process, the Technical Monitoring and Control System (TMCS) servers (main, standby and back-up) failed. TMCS is used to configure the VCS, in particular the touch-screen panels at every workstation which enable controllers to access all the ground communication channels. This failure meant that that Swanwick AC – which is NATS' largest operation controlling flights operating in upper airspace over England and Wales (generally above 25,000 feet) – was unable to change from its night time configuration of just 5 airspace sectors to its normal day time 20-25 sector operation. While air-ground communication was unaffected, the additional 15-20 sectors needed to handle daytime traffic had no access to the extra ground communication channels necessary to support high intensity daytime operations.

9. By 0315, it was clear that normal engineering processes could not recover TMCS before the early morning traffic flows materialised and, therefore, the engineering manager triggered escalation and full crisis management processes were activated. While Swanwick's senior management, engineering and operations teams tested potential system recovery and work-around options, traffic managers at 0445 began re-routing flights to avoid AC airspace and Eurocontrol was alerted with flow restrictions applied to critical AC sectors from 0530.

10. The crisis was escalated through the NATS management chain, including the NATS Board, with activation of the Air Traffic Incident Coordination and Communication Cell (ATICCC) at 0545. This stakeholder communications cell co-ordinates with the government (DfT), CAA, airlines, airports, neighbouring air navigation service providers (ANSPs) and Eurocontrol. This communication vehicle was used almost hourly from 0725 onwards to inform those stakeholders of the latest progress, including phone conferences, e-mail, text and website updates. In addition,

NATS' communications teams used a range of media to keep stakeholders and the travelling public updated on the situation, including live TV news broadcasts with Swanwick's Operations Director.

11. The failure of TMCS servers and associated normal recovery processes presented a huge challenge for engineers, making fault diagnosis and recovery extremely complex and time consuming. A rapid response by the VCS manufacturer's team (Frequentis in Vienna) enabled the problem and recovery solution to be fully confirmed by midday. Then, what would normally take more than a day to complete took just 6 hours, with NATS' engineers completely re-building, testing and safely re-booting re-built TMCS servers. Safety processes demanded that this was done in a highly rigorous and carefully planned manner which ultimately dictated the speed of recovery. Over 100 additional engineers and specialists supported the effort to restore the system. At 1300, engineers predicted that 'systems normal' could be achieved by 1830 which proved accurate. 'Operations normal' – the point at which all air traffic restrictions were lifted across the UK – was completed by 1930.

12. Despite the huge constraint on UK ATC operations throughout the day, by using Swanwick Terminal Control, Prestwick and Military ATC airspace and resources together with help from adjacent ANSPs, over 90% of flights were able to operate albeit with some significant delays averaging more than 30 minutes per flight. NATS' traffic managers helped airlines plan re-routes and flights at lower levels to offload aircraft from affected sectors, as well as constantly adjusting flow rates with Eurocontrol to minimise delay as far as possible. Throughout, safety was not compromised.

Industry reaction

13. In the immediate aftermath, reaction to how NATS managed the crisis was mixed. Many airlines and airports were pragmatic about a system failure that was difficult to prepare for or predict. They recognised the extraordinary challenges that NATS had faced and felt that it had handled a difficult situation well. In particular, they appreciated the regular ATICCC communications and the help of traffic managers to keep flights moving, stating that all this was well in excess of what other ANSPs do under similar circumstances. Others felt that changes were vital to assure airlines and airports that there would not be a recurrence of such technical failures with consequent disruption.

14. Regarding resilience and contingency, the industry accepts that there will be technical failures and the key learning is a) just how dependent the UK is on an air traffic service that maintains 100% throughput 100% of the time, and b) when a failure does occur then there is a need for a coordinated industry and government wide plan to minimise disruption.

15. NATS subsequently held discussions with many airlines and airports on lessons learnt and improvement actions. Feedback on ATICCC communications and traffic management support has been very positive and there has been unanimous support for better ways of managing disruption on this scale, to be developed jointly by NATS and the industry including:

> Pre-planned traffic scenarios to help airlines react to non-standard routeing;

> Regular industry crisis exercises to establish the capability of entire UK air transport industry to maximise total network capacity when faced with significant disruption.

The investigations

16. Two special investigations into this disruption event have been undertaken:

> An immediate and comprehensive internal investigation into the engineering, operational, communications and contingency aspects of the event, and into NATS' resilience in general, including reviewing lessons learnt and mitigation action to prevent a repeat of the incident;

> A NATS Board instigated review, by its Technical Review Committee (TRC) and independent advisors, of the key issues and decision-making in order to provide independent assurance to the Board that NATS (in its reports to the Board) had fully addressed the underlying issues revealed by the events.

17. The CAA agreed that, given the scope of these investigations, further independent review would not be beneficial.

What NATS is changing as a result of lessons learnt and investigations

18. Key themes for further improvements have emerged:

> *Reduce the risk of similar failures* – immediate changes were made to TMCS to prevent a recurrence of this particular failure. A subsequent full review of resilience of systems to major failure concluded that effective barriers to reduce the likelihood and impact of failures were in place, and that restoration times that could be achieved following major failure were understood. NATS' capital investment programme's emphasis on replacing legacy architecture at the earliest opportunity would improve resilience to failure as investment plans proceed over the next few years.

> *Improve the engineering response to major failures* – enhancing existing escalation processes and identifying fall back methods of operation that could reduce the service impact and expedite recovery.

> *Improve operational responses to disruption* – longer-term proposals to enable other operations rooms to control aircraft in adjacent affected airspace, for example allowing Terminal Control or Prestwick to operate in adjacent AC airspace sectors (or vice versa) to provide continued safe passage of aircraft in airspace that would otherwise be unavailable.

> *Review crisis management and resilience* – with customers and Regulator the industry's ability to respond, identifying any changes to NATS' crisis management capabilities, resilience of systems and procedures, or service continuity plans to meet industry expectations for highest resilience of service.

> *Communicate better with customers, stakeholders and the wider world during a crisis* – improving in three main areas – further increasing the speed of response, increasing the use of social media, and engaging even more with non-media stakeholders.

The Conclusions

19. NATS' contingency plans for a major failure at its Swanwick ATC Centre, and their execution, worked to the extent that over 90% of flights operated on 7th December 2013 albeit with significant delay. However, more could be done across NATS and the industry – as outlined in this Report – to minimise the effect of severe disruption in rare cases such as this.

20. The cause of the TMCS failure was corrupted computer disks on three separate servers, which could not be recovered quickly using standard practices that have been effective in the past. Consequently, fault escalation processes were initiated to diagnose, resolve and recover the system. NATS and Frequentis deployed significant additional engineering resources to isolate a complex fault, identify corrective action and recover the system in a safe and robust manner. It is difficult to know in advance which approach will deliver a result in the earliest timeframe, but a new framework is being proposed to ensure alternative approaches for recovery are assessed and choices are made in a clear and transparent manner.

21. Crisis management was instigated quickly and effectively to ensure that NATS could respond directly to the incident, manage the operation and air traffic in the light of the failure, while also managing stakeholder interactions including customer and media communications.

22. NATS effectively applied processes and procedures to ensure safety of the operation whilst maintaining as much capacity as possible. The decision to keep the Swanwick AC operation running in 'night-time mode' was in the best interests of customers as it maintained as much capacity as possible while resolution and recovery took place. In this instance, a more draconian short-term shut-down of the Swanwick AC operation would not have recovered the situation more quickly, and would certainly have been significantly more disruptive to the airlines, airports and the travelling public.

23. There was highly effective cross-industry co-operation in managing the disruption. The co-operation via ATICCC and with Eurocontrol, combined with best use of Prestwick, Terminal Control and Military airspace and resources, provided alternative routings to offload flights from affected airspace and enabled maximum use of available capacity. Industry proposals for pre-planned traffic scenarios and capabilities will help all parties in future to better react at short notice. ATICCC processes are being improved to ensure customers are aware as quickly as possible of the causes, implications and options open to them, recognising that in communicating earlier the status / impacts of an event might not be as definitive.

24. NATS engaged pro-actively with a wide range of media, political and other stakeholders throughout the incident to ensure that a clear picture of what was happening was available. These

communications were coordinated with ATICCC customer communications to ensure consistency. While helping to influence the news agenda and reaction in difficult circumstances, simplifying the message for ease of public understanding ran counter to explaining why the problem was complex and difficult to fix. Despite the level of proactive communications undertaken with stakeholders, more could still be done – particularly using social media – during the incident and through post incident briefings. Care will need to be taken to ensure that there is appropriate separation between NATS' interaction with the public and airline/airport interactions with their customers during events of this nature.

25. Regarding the broader issue of whether NATS' resilience plans are sufficiently robust and effective, NATS' approach is to build sufficient resilience into its systems and operation to ensure that it can cope with a failure without impacting the service to airspace users. In common with standard practice in ATM systems worldwide, such resilience is enabled by reducing the likelihood of system failures to a very low level combined with minimising the impact of any failure on the ATC service. This approach and the associated resilience targets are reviewed periodically at Board level (by the TRC) along with specific resilience risks and their mitigation progress.

26. A cross-industry review of crisis management and resilience should determine whether NATS' target levels of resilience are appropriate in light of this event and – if not – what additional mechanisms are necessary. NATS' view is that current investment plans provide the best balance of cost versus risk. Irrespective of the level of investment in additional resilience, it is unrealistic to assume that a highly complex non-stop 24/7 operation can operate at 100% capacity without occasional constraints on service capacity. Therefore, rather than immediately invest in additional technology which would add complexity and could be counter-productive by creating more risk, in NATS' view a better approach is the one being taken to develop a systematic and simple pre-planned industry response to minimise the effect of severe disruption in rare cases such as this. In the longer-term, NATS' capital investment plan includes new technologies to further enhance technical resilience.

The scope of this Report

27. This Report now presents the findings of the investigations in detail:

> Chapter 2 provides context of NATS' approach to minimising the potential for disruption in its operations and systems;

> Chapter 3 summarises the events of 7th December 2013 and how it affected airlines, airports and their customers;

> Chapter 4 explains how the subsequent investigation process has been carried out;

> Chapter 5 assesses the adequacy of NATS' response to events on 7th December 2013 and the extent to which the steps taken managed and minimised the impact on air travel;

> Chapter 6 considers whether NATS' contingency and resilience plans, and their execution, are sufficiently robust and effective;

> Chapter 7 sets out the changes NATS is making as a result of investigations, lessons learnt and the investigations.

28. Additionally, the CAA asked NATS to address a number of specific questions in this Report which are signposted in the narrative – the first is below.

CAA Question: How will the Comprehensive Report provide assurance that all aspects of this event and the follow-up have been adequately addressed?

29. This Report – which has been reviewed and approved by the NATS Board – provides a full analysis of the events of 7th December 2013 on the day, in the immediate follow-up and subsequently as lessons have been identified. It draws together all of the threads of investigative activity undertaken, including internal reviews and actions and the process, and outcome of, the independent TRC review commissioned by the NATS Board. It also reflects the follow-up discussions held with key stakeholders, notably airline and airport customers, on NATS' response and on joint actions to improve responses to similar events. At each stage, the Report shows traceability from the issues identified to the mitigations and improvement actions put in place.

30. Overall, the Report demonstrates NATS' view that it has undertaken thorough and wide-ranging assessments of the event, taken account of internal analysis and external views, learned lessons and acted fully in response to the findings identified.

2 Context

1. The UK has some of the busiest and most densely used airspace and runways in the world. The whole air travel industry relies on NATS to ensure that the daily choreography of flights in Britain's skies is always safe and managed efficiently so that airlines, airports and passengers can run to schedule. The consequence of such high intensity airspace and runway operations is that any disruption to normal operations – weather, airport / runway closures, ATC problems – has an immediate and marked impact on air travel.

2. NATS has a strong track record in successfully managing the unexpected to minimise disruption. For example, during 2013 the challenging weather conditions and airport disruption tested NATS' resilience and contingency arrangements, and in each instance capabilities and resources were deployed to keep airports and airspace safely operating no matter what the circumstances.

3. It also has a good record in ensuring ATC problems do not cause disruption. Current ATC technology and systems are highly complex and extremely reliable, being constantly updated to meet the industry's demand for ever increasing efficiency in using airspace and runways. But ATC systems do fail and NATS has 'defence in depth' to reduce both the likelihood of a failure and its effect on the ATC service. These defences have been effective in the past with less than a handful of 'significant engineering events' each year, all of which are virtually invisible to air travel.

4. Swanwick is one of the largest and busiest ATC Centres in the world in terms of flights managed, so on the rare occasion where 'defence in depth' is not effective and things go wrong a degree of disruption is inevitable as fall back procedures are deployed to ensure skies remain safe. Here, NATS' record is extremely good. Across its whole ATC centre operations there have only been 21 occasions in the last 5 years where engineering events have caused air traffic flow management (ATFM) delays to be imposed on flights to ensure safety, most causing minimal delay (largely unnoticeable by the travelling public) and none resulting in a safety incident. The delays / cancellations caused by 7 December were of an order of magnitude higher than any other single NATS engineering event in the last 10 years.

5. NATS does have a contingency back-up facility for Swanwick for a major and prolonged disruption, but it is not a 'hot standby' and takes around 48 hours to bring into operation. Other ATC Centres can't simply step-in currently as they don't have access to procedures or radar / radio coverage and are not approved to operate in the airspace, although planned investments in our two centres will increase the level of flexibility we have to move airspace between them over the next few years. Contingency planning therefore focuses on recovering normal operations at Swanwick as quickly as possible, together with managing traffic flows at a European network level to optimise work-arounds and resources to help keep disruption to air travel to an absolute minimum.

6. But ATC systems continue to evolve and the next-generation technology being developed under the umbrella of the 'Single European Sky' project will change the way ATC responds to technical problems. Virtual control towers are already available to take over control in the event of ATC problems at airports. At the end of the decade, NATS' significant investment in proven next-generation technology will enable it to move to a 'one airspace, one operation' across its ATC Centres at Swanwick and Prestwick, such that 'any airspace can be controlled from anywhere'. This will open-up a whole range of new possibilities in dealing with events like 7th December 2013.

3 The Events of 7th December 2013 and their Impact

3.1 OVERVIEW OF THE FAILURE AND WHY IT CAUSED DISRUPTION

1. The failure occurred in the Voice Communication System (VCS) which provides controllers with integrated voice communications for radio, telephone and intercom in one system. VCS has three main elements:

> A digital telephone exchange system (known as a 'voice switch') which provides all the channels for controller-to-controller and controller-to-aircraft communication;

> Operator touch-screen panels at every workstation which enable controllers to access all the communication channels associated with their task and to amend individual workstation configuration, for example when combining airspace sectors ('band-boxing') for night time operations;

> A Technical Monitoring and Control System (TMCS) which is a computer system for monitoring VCS and managing system changes – essentially a 'control computer' connected to all the other system components but with no connections to the 'outside world'.

2. The VCS in Swanwick Area Control (AC) is an established system supplied by Frequentis, with the TMCS already due for upgrade during 2014. The Swanwick AC VCS is separate from those in Swanwick Terminal Control and Prestwick operations rooms which are completely independent systems from another supplier and were unaffected.

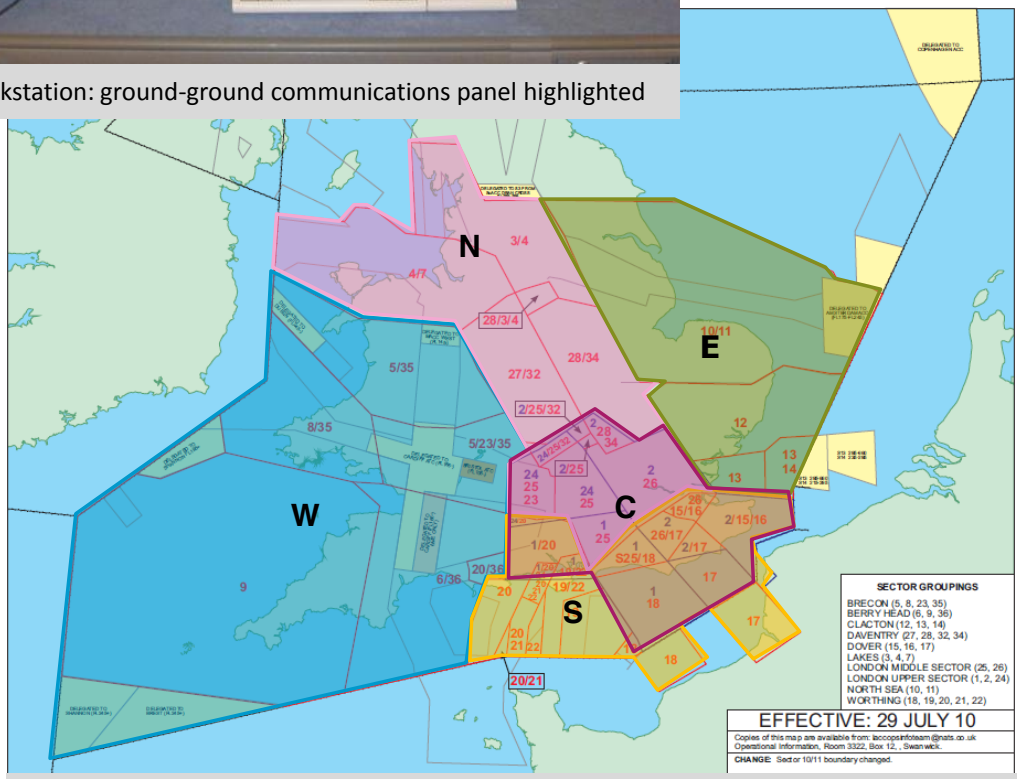
3. It was the TMCS system which failed on the 7th December 2013. TMCS is fully duplicated using a Master and Hot Standby (i.e. ready to take over immediately) arrangement. Both the TMCS servers failed during an overnight installation of data changes ('adaptations') while Swanwick AC was in night-time operational mode with just 5 band-boxed sectors controlling all upper airspace above England and Wales.

4. The failure early on the 7th December 2013 left the voice switches fully serviceable but rendering the controller panels unable to reconfigure for the daytime operation. The panels, however, retained their operating functionality, which allowed controllers to talk to other controllers and to use radio communication with aircraft, but restricted to night-time configuration. While air-ground communication was unaffected, the additional 15-20 sectors needed to handle daytime traffic had no access to the extra ground communication channels necessary to support high intensity daytime operations.

5. Swanwick AC is by far NATS' biggest operation, with most flights arriving and departing UK airports entering its airspace as well as trans-Atlantic overflights. Capacity is determined by the numbers of airspace sectors it can operate to match traffic demand on an hour-by-hour basis. The 'frozen night-time configuration' meant that NATS' biggest operation would have to operate with just c.20% of its normal daytime sectors until the TMCS failure was resolved.

6. This capacity shortage manifests itself in ATC flow restrictions being applied to affected airspace until normal operations resume. This translates into ground delays for flights at airports until a departure slot can be allocated by Eurocontrol who manage the European air traffic management network. With large numbers of flights in a queue for departure slots through Swanwick AC's airspace, the length of ground delays increases dramatically and can leave some airlines no option but to cancel flights.

Area Control workstation: ground-ground communications panel highlighted



Swanwick Area Control: Night-Time Five Sector Configuration

3.2 TIMELINE OF KEY EVENTS

	Incident Management and Customer / Stakeholder Engagement	Technical Resolution	Operational and Traffic Management
0030-0315		TMCS disc corruption failure recognised Attempts at standard recovery procedures fail	
0315	Engineering escalation commenced Swanwick senior management alerted to seriousness of failure		Sector configuration could not be changed until fault resolved Eurocontrol, Terminal Control, Prestwick and Shannon advised of potential need for help in re-routing flights
0400	Bronze command and control in place Decision to remain in known night-time configuration pending resolution	NATS system design authority and manufacturer consider recovery approaches	
0500		Begin developing and testing other sector splitting options	
0520	Swanwick Operations commence checklist for ATICCC activation		
0530			Flow regulations applied to key AC sectors
0545	ATICCC activated	Alternative sector splitting options not viable	
0550	Duty Press Officer (DPO) alerted		Terminal Control and Prestwick mobilised to handle re-routes
0625	ATICCC convened		Traffic management plan developed with Eurocontrol, Terminal Control, Prestwick and adjacent Centres
0700	Silver team present at Swanwick ATICCC activation notified by text, e-mail and website ATICCC update BA Silver Team		
0725	1st ATICCC conference call		
0730	DPO responds to media requests with prepared statement		Options for use of military airspace / resources
0800	Press office active BBC TV journalist briefed 1st media statement released	Engineering conference call including Frequentis to consider diagnosis, options, key actions and timescales Additional engineering resources called-in	
0830	Gold present at Swanwick Decision not to invoke Silver command and control		

	Incident Management and Customer / Stakeholder Engagement	Technical Resolution	Operational and Traffic Management
0900	On-going discussions with airline operations centres on re-routes and flight level capping	Initial forecast that restoration would take 4-6 hours once solution was available	
0915	2nd ATICCC conference call 2nd media statement released		
0930		Frequentis begin testing in Vienna	Western Radar work-arounds operational
1000			Method of flow regulation changed to better match demand to available capacity
1030		Frequentis confirm that April 2013 TMCS discs could be used as basis for recovery – copy sent electronically to Swanwick	
1040	Decision to change recovery strategy to Plan B server re-build solution		
1100	1st live TV news interviews		
1130	3rd ATICCC conference call	April disc image received, TMCS rebuild process to December 2013 standard begins	Flow regulations extended to 2000 hours
1200	Crisis management review with solution and defined timeline in place 2nd decision not to invoke Silver	Updated forecast that restoration would take 6 hours – i.e. to 1800	
1230	3rd media statement released	Server re-build testing begins at CTC	
1315	4th ATICCC conference call		
1430		Reconnection risks reviewed, additional back-up processes agreed	
1515	5th ATICCC conference call		
1600		Begin testing TMCS reconnection to VCS at Swanwick Each workstation panel updates in turn, unused workstations being switched-off to speed progress	Reload process causes issues in 2 of the 5 in use panels – flow rates reduced by c.15%
1715	6th ATICCC conference call		
1840		Panel re-load completed, functionality checked	
1900			Sector splitting from night-time configuration begins
1920	4th (final) media statement		
1930	Final ATICCC conference call		Operations normal
2000			All flow restrictions removed
2040	Final broadcast interview Media enquiries continue from Sunday news outlets		

3.3 THE IMPACT ON AIR TRAVEL

7. NATS made immediate apologies – both on the day and in the aftermath – to customers and passengers affected by the disruption resulting from the system failure.

8. The impact on customers on Saturday 7th December was significant, with around 300 flights being cancelled and 1,472 flights delayed with total delays amounting to 126,080 minutes:

> NATS handled 3,764 flights in total that day, which is c.9% lower than the previous Saturday (30 November 2013) and the comparable date in 2012 (8 December 2012);

> 39% of all flights that operated throughout the day were delayed (i.e. 61% suffered no delay at all or less than 15 minutes);

> Average delay per flight was 33 minutes, those that were delayed having an average delay of 86 minutes;

9. This level of disruption had a significant impact on many airports within the UK, notably within the London TMA, where Heathrow and Gatwick were only able to operate around 80% of their flights during peak hours.

Key Figures

> Heathrow – 432 flights delayed (270 departures, 162 arrivals)[1], 231 cancellations (118 departures; 113 arrivals), plus some cancellations on Sunday 8th December 2013 due to aircraft/crews being out of position.

> Gatwick – 86 flights delayed, 14 cancellations

> British Airways –150 flights cancelled, total delay into/out of Heathrow c.17,000 minutes

> Worst delay – 315 minutes (Iberia: Heathrow – Madrid)

> Airport arrival and departure rates:
(measured between 1200-1500, in comparison with Saturday 30 November 2013)

Airport	Arrivals	Departures
Heathrow	85%	76%
Gatwick	80%	83%

> Impact of en-route sector flow regulations on London's airports:
(measured between 1100-2000, based on Dover sector which was one of the most penalising regulations that affected these airports)

Dover Sector	Heathrow	Gatwick	Stansted	Luton
Flights regulated	98%	100%	95%	80%
Average delay per flight (mins)	39	63	68	63
Longest delay (mins)	106	116	109	92

[1] Primary air traffic flow management (ATFM) delay only. Long haul arrivals into Heathrow are not subject to flow regulation.

4 The Investigation Process

1. Recognising the level of disruption, immediately on Sunday 8th December 2013 NATS CEO launched an internal major incident inquiry and the NATS Chairman instigated a Board-level investigation through its Technical Review Committee (TRC).

2. The purpose of the internal major incident inquiry was to report to the Board – initially to an extraordinary Board meeting on 17th December 2013 and to the January 2014 meeting – on the facts surrounding the failure, its cause and impact, how the event was managed at every level, and to make recommendations on preventative and improvement measures.

3. The purpose of the TRC investigation was to provide the Board with the necessary assurance that NATS (in its reports to the Board) had fully addressed the underlying issues and any internal weaknesses revealed by the failure. In this respect, the TRC examined – during February and March 2014 – two aspects in making its recommendations:

- The specifics of the failure, its management and impact;
- The broader management of system risks and resilience.

4. The NATS Board as a whole considered the areas of communication, customer relations, and political impact.

5. These formal investigations have been supplemented by an extensive round of discussions, at both executive and operational levels with airlines and airports and in customer forums, to gain feedback on the way that the event was handled by NATS, on key lessons learnt and the actions considered necessary to maintain the highest service resilience. These discussions took place in the period from December 2013 to June 2014 and are detailed in Appendix A.

6. NATS executives have also had briefings and meetings with the DfT and CAA (see questions below).

7. Recognising the infrequency of failure situations in this industry and the opportunity to learn as much as possible from the event, the NATS CEO has commissioned an additional review of NATS' broader crisis management capability and resilience to ensure that, in light of these investigations and findings, all aspects of the business are better able to deal with the impact of unusual events. This process will include a cross-industry review of the wider industry response.

Post Event Meetings

Airlines:	**Airports:**
BA	Heathrow
easyJet	Glasgow
Ryanair	Southampton
Flybe	**Customer Groups:**
Monarch	Future Airspace Strategy (FAS) Deployment Steering Group
Aer Lingus	FAS Industry Implementation Group (FASIIG)
CityJet	Operational Partnership Agreement (OPA)
American	Lead Operator Group
Delta	
United	

CAA Questions

Who determined what was appropriate in terms of independent oversight / governance of the process?	The NATS Board directed the arrangements for the investigations and provided independent oversight through its non-executive structure. The scope of the internal major incident inquiry was set by NATS CEO in discussion with the Chairman, with the process and reporting overseen by MD Operations. The TRC investigation was overseen by an independent non-executive member of the Board who chairs the committee. The Board has reviewed and discussed all reports in Board meetings.
Did NATS' reporting and investigation mechanisms identify the major issues and address them appropriately?	The internal major incident inquiry examined in detail the root causes of the event, the escalation and rectification processes, the traffic management approach and communications response. It highlighted what worked, uncovered the key lessons and recommended important improvements. The TRC's investigation concluded that the underlying issues and weaknesses were being addressed effectively by NATS, but making additional recommendations on further improvement measures. All actions are being reported and tracked to completion using recognised 'corrective action' business processes, with regular reports at NATS Executive and Board level.

How was the TRC process initiated?	The Board Chairman and TRC Chairman agreed that, given the seriousness of the incident, the TRC should provide follow-up assurance to the Board, which was also agreed by the extraordinary Board meeting.
Who shaped and influenced the TORs?	Draft TORs were prepared by TRC members and technical advisers, discussed with the CAA and approved by the Board.
How did the NATS Board assess the TRC review?	The Board accepted the technical content and recommendations of the TRC review and approved the report which was forwarded to the CAA.
How will progress be reported to customers / regulator on the outcome of the TRC review?	The recommendations and outcome of the TRC review were provided to the CAA and shared with customers via the Operational Partnership Agreement (OPA) and via face to face briefings. The findings of all the investigations are summarised in the next chapters of this Report together with actions taken in response to recommendations. The expectation is that the CAA will publish this Report so that the whole air transport industry and air travellers are made aware of the outcome of the investigation process.
How are customer views being taken into account in the post-event review process?	All customer feedback from the OPA and face to face meetings has been taken into account. The most in-depth review with airline and airport customers has been via an OPA Hotspot project specifically established post-event to develop enhanced recovery procedures. In addition to the direct feedback, NATS annual customer survey took place across the period and has provided some insight into customer perceptions of management of the event.
Since the event how have relationships with the DfT, the Transport Select Committee, the CAA, customers and consumers been managed?	**DfT** - Richard Deakin (CEO) and Martin Rolfe (MD Operations) provided personal briefings, including Patrick McLoughlin (Secretary of State for Transport), Simon Burns (Aviation Minister) and Tricia Hayes (Director of Aviation). Additional briefings and support were provided to help in answering parliamentary questions. **MPs** – written briefings were provided to MPs with specific interest. **Transport Select Committee** – a report was provided in January 2014 (reproduced in Appendix B). Louise Ellman (Chair) visited Swanwick in May 2014 and was given an additional briefing. **CAA** – several meetings at Group Director and senior management levels. **Customers** – via the extensive round of discussions with airlines and airports and in customer forums (see para 5 above). Richard Deakin and Martin Rolfe wrote to the CEOs and Ops Directors of Airlines and Airports offering a face to face meeting to discuss the way that the systems failure was handled, actions taken to resolve the issue and maintain service and lessons learnt. NATS also requested that airline and airport customers provide feedback on areas that could be improved. There was discussion and correspondence with some airlines and airports on the variation in impact on operations (depending on location / route), and on NATS compensating them for the disruption caused. **Consumers** – communication with passengers that had been affected was provided via briefings to journalists and media outlets who were commenting on passenger criticisms. A post event statement by NATS CEO was posted on NATS website on 9 December 2013.

5 Adequacy of NATS' Response

Did NATS do a good job in minimising disruption faced with unusual circumstances?

5.1 SPEED AND SCALE OF REACTION TO A DEVELOPING CRISIS

5.1.1 Decision-making and escalation

Initial Engineering Escalation

CAA Questions:
How well did NATS' engineering staff follow their own escalation procedures on the day?
Was the decision to escalate made early enough?

1. NATS' engineering escalation procedures are based on a managed series of steps to engage more senior levels in resolving a problem or failure. This ensures that there is a proportionate response to failures and prevents the daily escalation of 'normal failure events' which do not require management attention to resolve or impact ATC service delivery.

2. In this incident the escalation process started within 30 minutes of the failure occurring. When the fault was first recognised at 0030, engineers made several attempts to recover the failed units following normal restoration procedures which had been successful in the past. This included structured fault finding and testing in the equipment rooms and engineering systems control, as well as 1st step escalation by contacting a specialist NATS engineer who was on-call for telephone support. This thorough approach is normally effective in resolving issues, however by 0315 it was clear to the on-site engineers that they could not resolve the issue using the normal recovery procedures ahead of daytime traffic starting, and therefore the Engineering Service Manager (ESM) initiated the next stages of escalation.

3. Escalation procedures were followed which triggered three lines of action:

> *Technical* – a discussion with key experts (at 0400) to consider options for recovering the system, a series of tests (up to 0530) to see whether sector splitting could be achieved by other means, and a cascade call-out of Engineering management and resources (0400-0800).

> *Operational* – the ESM had earlier alerted the Operations Supervisor (OS) who had taken precautionary measures to alert other NATS operations and Eurocontrol. Upon escalation, Eurocontrol and adjacent Centres (Terminal Control and Prestwick) were mobilised and Senior Operations Management contacted. As the seriousness of the impact on traffic became apparent (0530), ATICCC activation checklists commenced.

> *Incident management* – the technical and operational escalation resulted in Bronze command and control being in place from 0400. The timeline for escalation took place in a systematic manner, progressively notifying more senior levels of management as the potential impact of the event became clear, with Gold management involved at an early stage by telephone and on site by 0830.

4. Overall, escalation was started sufficiently early to allow operational contingency plans to be put in place in advance of normal daytime traffic (ATICCC, Eurocontrol, Terminal Control and Prestwick) and to ensure crisis command and control was established and effective. It also rapidly mobilised key engineering experts and resources (0400) to focus on a different recovery approach at the earliest opportunity.

Decision Making

CAA Question: Who was ultimately exercising oversight of the NATS' decision making on 7 December and how was this executed?

5. NATS' crisis management is organised on the Gold/Silver/Bronze model of command of control which is commonplace in the UK. This is supplemented by ATICCC which performs a

communication function between NATS and its customers during a disruptive event, as well as coordinating communications with other key stakeholders to ensure consistency.

6. The first decision-makers at Bronze level (engineering and operational managers) were in place by 0400 and also activated ATICCC. Given the seriousness of the impact on daytime traffic, Silver and Gold level managers were alerted and fully engaged, with Silver in place at Swanwick by 0700 and Gold by 0830.

NATS Crisis Command and Control Model

Level	Composition and Function
GOLD	Executive level crisis management team responsible for strategic matters, communication and sustaining the business
SILVER	Site senior management team responsible for managing the incident on the affected site
BRONZE	Working level management teams responsible for dealing with specific activities, normally at the scene of the disruptive event

7. The full crisis management organisation on 7 December 2013 is shown in the diagram below.

8. Ultimately, Richard Deakin as CEO provided oversight. Martin Rolfe, as MD Operations led Gold and was accountable for directing NATS' response supported by his regular management team through Silver and Bronze levels. The Gold/Silver/Bronze levels of management worked closely together throughout the day with the centre of activity focused at Swanwick, primarily within the ATICCC facility. The press office was based at CTC, as was the engineering support team.

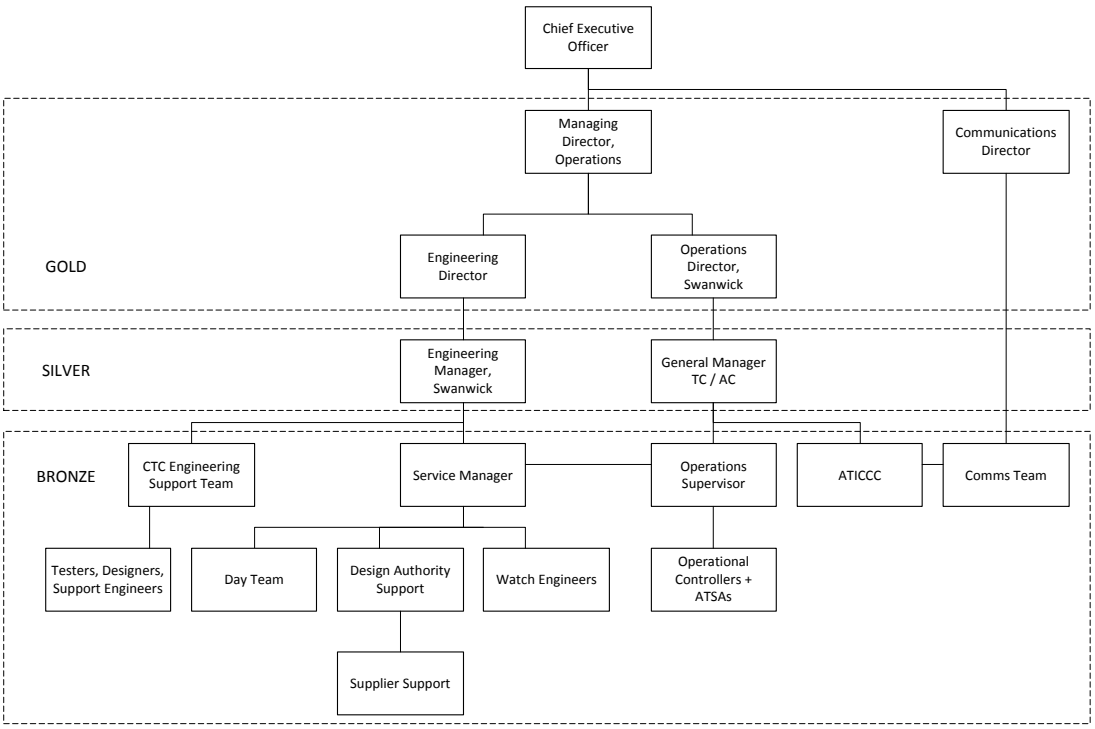
ATICCC's Role

- Assess the implications of the incident and establish mitigating actions
- Set the strategy for allocating available capacity and ensuring it is effectively utilised
- Confirm actions for a co-ordinated and planned recovery
- Communicate key information on the incident, mitigating actions and recovery
- Liaise with Government and the CAA
- Co-ordinate the media response

9. While operating effectively at Gold/Silver/Bronze levels, Gold and Silver teams were not formally invoked. An initial decision was taken at around 0830 not to formally invoke Silver as all the necessary personnel were in place, with an option to call it later if required. When the situation was reviewed at 1200, a solution with a defined timeline was in place and activation of Silver was not considered necessary.

10. All this demonstrates that an appropriate crisis management structure was in place to manage the events with an appropriate level of responsibility for key decisions.

Crisis Management Organisation on 7 December 2013



CAA Question: How is the relationship between the NATS' Board and the Executive structured to deal with a crisis scenario and with the necessary follow-up action effectively and efficiently?

11. The relationship between the NATS Board and the NATS Executive is governed by the shareholders agreement put in place at PPP in 2001. The agreement delegates management and control of the business of the company to the Executive, with the Board having overall responsibility for oversight and assurance in respect of the operation of the business.

12. In the event of a crisis, the Executive's policy is to promptly inform the Board of the circumstances, including mitigation activities underway and stakeholder communications. This provides the Board (generally through the Chairman) with the opportunity to discuss lines of action and specific issues with the Executive (CEO or Gold Lead) to gain assurance that sufficient and appropriate action is in hand.

13. In terms of follow-up, the Board may request immediate reports and special Board meetings – as was the case after 7th December 2013 – to facilitate prompt consideration of the issues arising from the event and to decide whether any additional assurance is required. Such assurance will normally be overseen by the Chair of a relevant Committee of the Board, in this instance by the Technical Review Committee (TRC). The Board has the full power to insist actions arising out of its assurance activities be implemented effectively and efficiently by the Executive.

5.1.2 Availability of contingency plans

CAA Question: Did NATS have an effective crisis management plan in place?

14. NATS has a hierarchy of crisis management and contingency plans that were deployed to respond to this incident.

Business Continuity Plan

15. NATS has a long-standing crisis management plan documented within The NATS' Business Continuity Plan ("BCP"). The BCP is designed to assist the management of NATS' responses during a period of crisis, to recover critical services and to return NATS to as near a normal business situation as possible. Compliant with UK standards and best practice, the BCP is consistent with the 5-step cycle – Detect, Assess, Plan, Act and Review. Parts 1 to 5 of the BCP are generic and apply across all NATS; Part 6 is site specific and owned by the relevant Unit Manager (see below).

16. The BCP is based on a wide-ranging evaluation of the criticality of areas of NATS' business and the options available to cater for a multitude of events that could cause partial or total disruption. The Plan explains how NATS should respond to different types of disruption, providing options for dealing with various scenarios and establishing priorities for critical activities. It is designed to provide guidance but will not obviate the need for 'tactical planning' on the day as the specific circumstances and consequences of an event unfold.

17. Execution of the BCP on 7th December 2013 was through the Gold/Silver/Bronze command and control, although Gold and Silver teams were not formally invoked. While operation of the principles of the BCP was effective, there are specifics associated with formal invocation of Silver and Gold that could have yielded additional clarity and benefit. While no specific issues have been identified, NATS would now plan to formally invoke Gold / Silver teams for future similar events in order to ensure that the expertise and experience of the teams is underpinned by the structure and clarity of the formal business continuity processes.

Unit Business Continuity Plans

18. Swanwick has a Unit Business Continuity Plan (Part 6) which is designed to ensure continued operations in response to sudden changes in their operating environment. The Plan ensures that traffic levels can be managed safely in the event of non-standard conditions, being continually reviewed to ensure appropriate levels of response to various scenarios. Critical system failures are one of the disruptive scenarios covered.

19. Scenarios from the Unit BCP are exercised regularly as part of annual Training in Unusual Circumstances and Emergencies (TRUCE) for operational staff. Additionally, due to the number of

units in NATS, there is the opportunity to apply lessons learnt from both real and exercised scenarios elsewhere to enhance the Unit's BCP and response capability. Beneath the Unit BCP sits a range of operational procedures in Swanwick's Manual of Air Traffic Services (MATS) Part 2 and in Engineering Instructions which detail actions in response to critical system failures.

20. The Swanwick Unit BCP and its execution are therefore considered to be robust, credible and tested.

5.1.3 Alerting airlines, airports, Eurocontrol and key stakeholders

21. Early planning took place on the potential requirement for traffic flow regulations. The Operations Supervisor (OS) alerted Eurocontrol early in the escalation process as incoming trans-Atlantic flights and other long-haul traffic flows could exceed the available capacity in night mode. At 0445 engineering confirmed that the operation would need to remain in night time configuration while the problem was resolved. Therefore, flow regulations were applied at 0500 to control the demand in some pinch-point sectors, and Eurocontrol advised airlines to re-route to avoid Swanwick AC airspace.

22. The decision to convene ATICCC was taken at 0547. Texts and e-mails notifying airlines and airports that ATICCC was in operation were sent out at 0630, with a brief notice on the ATICCC Customer website at 0700 giving the reasons for the activation. The first Customer ATICCC conference call was held at 0725 which explained the problem and re-route options so that airlines could make adjustments to their plans.

23. Airlines and airports were already aware of mounting delays to flights due to problems at Swanwick, prompting British Airways' Silver, for example, to request a specific briefing from NATS as early as 0700. Therefore, the processes for convening and activating ATICCC, and for communicating with airlines and airports ahead of ATICCC coming on stream, are being improved to ensure customers being affected by the problem (by traffic flow restrictions) have much faster information on the cause, implications and options open to them. In communicating earlier, it should be recognised that the status / impacts of an event might not be as definitive. Additionally, some customers were affected by slow delivery of e-mail notifications largely due to their internal e-mail virus scanning processes. Electronic alerting is being addressed by the joint NATS/customer OPA.

24. The ATICCC communication and dialogue with Eurocontrol continued at regular intervals throughout the day (explained later). This was supplemented by extensive bi-lateral telephone calls and e-mails during the morning of 7th December between NATS executives (Gold level and Customer Affairs) and airlines' and airports' executives.

CAA Question: What interface was there from a NATS' perspective with other, non-customer, key stakeholders on the day – DfT, CAA, the Network Manager?

25. NATS executives (Gold level) provided briefings to the NATS Board, Mary Creagh MP (Shadow Transport Secretary), Tricia Hayes (Director of Aviation DfT) and the CAA. Additionally, briefings were provided to press offices at DfT, CAA and trade bodies. The dialogue with DfT and CAA continued throughout the day.

26. The DfT, CAA and Eurocontrol's Network Manager (DNM) are included within the ATICCC communications, with DNM joining both the internal (ATC) and external (customer-wide) ATICCC conferences.

5.1.4 Communicating with the wider world

27. Bronze notified the Duty Press Officer (DPO) at 0555, who in turn notified other senior members of the communications team in line with company crisis communications plan. A senior member of the communications team deployed to ATICCC. The DPO started receiving media calls from around 0730 while other communications managers activated the Press Office.

28. An initial line to take was agreed between the CEO, MD Operations and Director Communications which was passed onto NATS' Head of Media Relations directing the Press Office response to media questions. Early "flash" reporting on the BBC accurately reflected this line and thus established the correct direction for the media story.

29. NATS issued four media statements during Saturday 7 December, each including an unreserved apology. NATS' first statement was cleared by ATICCC at 0755, passed to the Duty Press Officer for distribution at 0802 and tweeted/posted on the website at 0810. Initially, NATS' focus was to explain in simple terms why fewer aircraft were able to fly – i.e. the inability, due to the technical failure, to transition from the lower capacity night-time operation to the higher capacity day-time operation. Statement 2 (0940) gave more information about the nature of the problem and statement 3 (1220) included information on how long the problem would take to fix. A final 4th media statement was issued at 1920 confirming 'operations normal'. The statements are detailed in Appendix B.

30. The story led TV news with breaking reports occurring throughout the morning. A decision was taken by the CEO, MD Operations and Director Communications at 1015 that, even though the precise problem and fix had not yet been identified, the level of disruption and media coverage was such that NATS had to be publicly seen to be explaining and taking accountability for what had happened. Juliet Kennedy (Swanwick Operations Director) was interviewed on BBC News at 1100, although this could have occurred much sooner had the TV crew gone to the right location.

31. In line with best practice, Twitter messages were posted in tandem with statements during the course of the morning. However, with hindsight, greater use could have been made of social media (Twitter) to keep passengers and observers updated later in the day in the gap between media statements. Care has to be taken to ensure that there is appropriate separation between NATS' interaction with the public and airline/airport interactions with their customers during events of this nature (which are based on each airline's/airport's particular operational situation).

32. Overall, crisis communications were handled competently and thoroughly. NATS engaged actively with the media throughout the incident, ensuring it was highly visible and clearly taking accountability as well as being seen in public to react rapidly and responsibly to correct the failure and restore full operations. A fully staffed press office was operational for 10 hours with specialist support from key communications staff, providing some 80 telephone briefings for journalists. Media statements contained key messages on safety, causes of the problem and NATS response as well as critically, an apology to people affected. Juliet Kennedy gave 5 live media interview updates to rolling news broadcasts which assured a substantial response from NATS in order to respond to media and public interest in the event.

33. While effective communications messages were delivered, lessons have been learned in terms of messaging and the impact on multiple audiences. For example, use of terms such as "night time and day time operations" or "internal telephone system" sought to make the issues easily understandable to non-technical audiences but had the effect of over-simplifying the nature of the problem, which attracted criticism from certain quarters. Equally, messaging about the number of flights flown, while factually accurate and clearly designed to highlight NATS' response, may not have aligned with passengers' or airlines' experiences at affected at airports.

34. Follow-up actions resulting from communications lessons learnt include:

> Developing broader stakeholder communications during a crisis response, rather than becoming too focused on the media alone;

> Greater use of social media platforms to support rapid briefing of non-media stakeholders;

> Holding media conference calls immediately following ATICCC customer calls to ensure a regular and rapid update to the media to ensure a consistent and transparent approach;

> Relocating the Crisis Press Office to improve liaison with ATICCC and facilitate media update calls from appointed spokespeople.

CAA Question: What scrutiny was exercised, and by whom, over the communication messages issued on 7 December?

35. NATS CEO, MD Operations and Director Communications elected to pursue a policy of proactive engagement with external stakeholders to seek to control the communications agenda through the release of timely, accurate and factual information, while clearly acknowledging the impact and NATS' accountability for the incident.

36. Planning and creating key messages centred on the following priorities:

> Providing timely and accurate information, striking the right balance between communicating early and communicating facts;

- Being clear that safety was not compromised;
- Apologising for any inconvenience to customers and their passengers;
- Being clear that NATS was putting all available resources into resolving the problem; and
- Being factual about the levels of traffic being handled.

37. The communications team operated as part of ATICCC to prepare coordinated messaging. MD Operations, Director Communications and Swanwick Operations Director (Gold level) all had direct input to messaging being developed, with the CEO having oversight of these activities. All had access to external media to review how messaging was being re-played. In some cases where it was felt messaging had been misinterpreted, the communications team engaged reporters to adapt/correct media understanding.

38. The same senior grouping decided that Juliet Kennedy would act as initial lead spokesperson, with the option to escalate to MD Operations and ultimately CEO if unfolding events required. As Swanwick Operations Director, Juliet was considered a highly credible spokesperson with extensive air traffic operations experience (a qualified ATCO), who was recently media trained and as leader of the affected unit would convey greater meaning to audiences. She received support from executives and the communications team, both ahead of each interview and afterwards, to refine the key messages based on the evolving nature of the media questioning.

39. MD Operations and the CEO personally carried out one-to-one briefing of other key stakeholder executives outside the ATICCC process. Post event on 9 December, CEO NATS issued a statement – discussed and agreed with NATS Board Chairman – which provided a factual briefing on events and explained the basis of the NATS-led inquiries and follow-up.

5.2 MAXIMISING AVAILABLE CAPACITY TO MINIMISE DISRUPTION

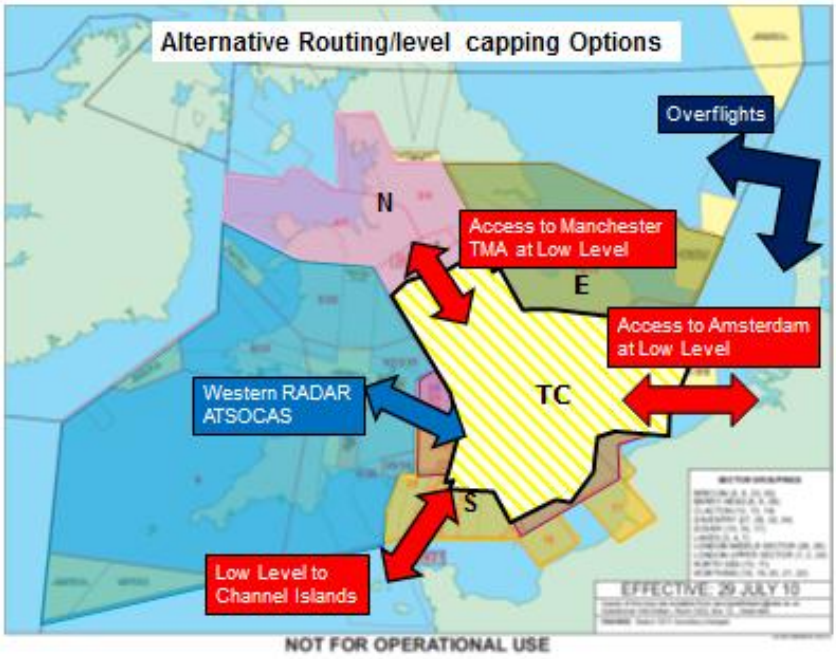
40. Throughout the day, whilst NATS engineering staff were working to resolve the problem, other staff at NATS were assisting the airlines and airports to minimise the impact of the disruption. This was achieved by re-routeing flights, much greater use of lower level routes (known as 'level capping'), a reduction in "danger area" activity in northern UK and the provision of some services in uncontrolled airspace. The Network Manager at Eurocontrol diverted some 500 transit flights around the affected airspace.

5.2.1 Operational work around measures to deliver extra capacity

41. NATS traffic managers (the Flow Management Position – FMP) enacted work around procedures in conjunction with Eurocontrol's Network Manager team (known as DNM). The work arounds (illustrated in the diagram) involved using Terminal Control (TC), Prestwick and Western Radar[2] to offload traffic from Swanwick AC's affected airspace:

- *Flights to/from the East* – transit to/from the London TC airspace directly by level capping from Amsterdam TMA
- *The North* – similar level capping by Manchester TMA (controlled at Prestwick)
- *The West* – employing the ATSOCAS service from Western Radar
- *The South* – via a bridge from Channel Islands airspace also provided by Western Radar
- *North Atlantic Overflights* – re-routed through Prestwick airspace.

[2] Western Radar is an independent NATS unit providing Air Traffic Services Outside of Controlled Airspace (ATSOCAS) to the west of the London TMA up to FL245.



5.2.2 Ensuring available capacity was used efficiently

42. Proactive network management by the Swanwick FMP with Eurocontrol DNM, together with the continuous dialogue with airlines and airports throughout the day, ensured the available capacity was used most efficiently:

> ATICCC regularly updated airlines on the re-route and level cap options open to them;

> Additional staff were deployed in the FMP to help airlines apply re-routes and level caps into London Terminal Control and Prestwick;

> Eurocontrol DNM supported airlines in applying re-routes and level caps to avoid Swanwick AC airspace, providing regular updates on their Network Operations Portal. They also coordinated potential capacity issues with Brussels and Amsterdam ACC caused by the level capping;

> Flow regulations were continually reviewed and adjusted in light of traffic demand and delay impacts;

> On-going and extensive dialogue took place between FMP and key customer touch-points to address specific needs – such as the Heathrow Operational Efficiency Cell, airline operations centres, airport control towers, etc. In many cases help was provided for individual flights experiencing substantial delay, for example DNM excluding flights from the regulations at NATS' request to free up capacity and reduce delay.

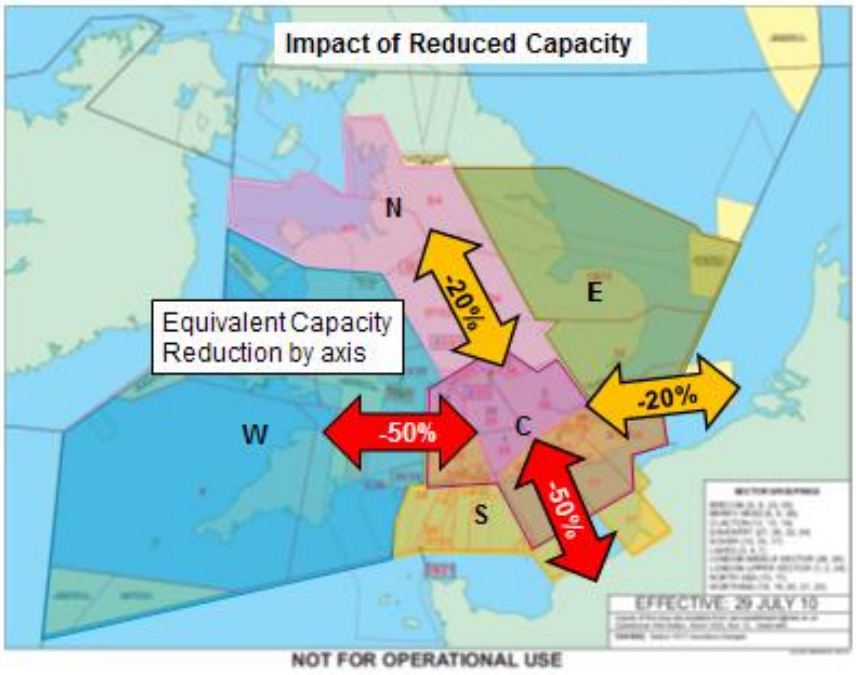
5.2.3 The outcome of these measures

CAA Question: Did the operational work-around measures deliver extra capacity?

43. The capacity generated by the work arounds and accompanying network management actions has been explained inversely to airlines, i.e. how they worked in minimising the capacity reduction compared to a normal Saturday in winter. As a broad measure, given that Swanwick AC only had 5 of its planned 20-25 sectors available, capacity reduction in the order of 75%-80% might have been the outcome in the absence of these mitigating actions.

44. Those flights that were in a position to use work arounds experienced a reduction in delay. However, the capacity reduction varied across the axes as illustrated in the diagram below. The South and West axes saw the highest level of demand and had limited options available to avoid the affected airspace, and therefore delay (capacity reduction) was greater. For North and East, there was less demand and flights had the option of level capping to remain in Terminal Control or Prestwick airspace until they were clear of the affected airspace, resulting in less delay (extra

capacity greatest). This diagram was shared with the OPA and at bi-lateral meetings with airlines and airports to explain why delays to flights and airports varied dependent on route.



45. However, a number of operators were offered alternative routing options but were unable to revise flight plans on the day (due to in some cases to weekend staffing or to the workload from the disruption itself) and did not take up these opportunities. In addition a number of operators were not approved to fly outside controlled airspace (CAS) or to accept a Military service outside CAS.

46. Overall, the mitigating actions resulted in a far smaller reduction in capacity than might have been expected given the failure had impacted NATS' largest operation. The effectiveness of work arounds and network management has been the subject of considerable discussion subsequently, both in the OPA (see Appendix A) and in one-to-one meetings with airlines and airports. This has resulted in unanimous support for further action to:

> Develop 'off the shelf' re-route scenarios via the Swanwick and Prestwick Operational Resilience Enhancement Plan (OREP) work;

> Evaluate within the OPA Hotspot project use of ATSOCAS services offered by UK Military and Western Radar, and the potential benefit that could be enabled by creating temporary CAS for a small number of specific routes;

> Publish these scenarios as they are developed via the UK Standard Routing Document (SRD) so that they are available as contingency scenarios for Airlines to use in disruption;

> Enhance the process for dissemination of active re-routes such that they can be 'broadcast' more directly via pre-formatted messages on AIM, DNM NOP Portal and NATS Customer Website/Info Portal;

> Improve DNM re-route verification processes to avoid the risk of re-route flight plans being rejected by the DNM Integrated Flight Planning System (IFPS) and causing extra delay.

5.3 HELPING AIRLINES AND AIRPORTS TO MANAGE THE DISRUPTION

CAA Questions:
How was customer engagement managed on 7 December?

47. Customers were engaged primarily via NATS' ATICCC which was the main vehicle for helping airlines and airports to respond optimally to the disruption to their flights and schedules. It was also the conduit for information that airlines and airports could use to keep their customers updated on the situation.

48. The ATICCC process included conference calls every 2 hours, NATS customer website updates and one-to-one discussions on specific issues. Also on-going dialogue took place with customers via the Heathrow Operational Efficiency Cell and NATS' traffic managers (FMP). Details are provided in Appendix C.

49. The operation of ATICCC was managed at Gold level by MD Operations and Swanwick Operations Director. The ATICCC conference calls and other specific assistance to airlines and airports (outlined above) were supplemented by extensive bi-lateral telephone calls and e-mails during the morning of 7th December between NATS executives (Gold level) and airlines' and airports' executives. Key points of discussion included:

- Timeline for fixing the problem;
- Likelihood of re-occurrence (near and long term);
- Risks for the following day operations (airlines and airports);
- Traffic balance (arrivals and departures) at the major UK airports;
- Re-routes and level caps;
- Management of flight plans.

50. Feedback from airlines and airports on the engagement process was generally very positive. In particular, they appreciated the regular ATICCC communications and the help of traffic managers to keep flights moving, stating that all this was well in excess of what other ANSPs do under similar circumstances. However, tactical communication was limited by the ability to contact airline operations centres during disruption, and there was feedback that one-to one-communication with some senior airline and airport managers could have been improved.

51. Feedback in NATS' annual airline customer survey – which was conducted during November and December 2013 – also provided an insight into customers' reaction to how well NATS managed the event. When comparing survey responses pre/post 7 December, post event scores for 'technical resilience' dropped whereas scores for all other aspects of 'managing unusual events' increased. (See Appendix A – Extract from 2013 Customer Survey).

CAA Questions: Who engaged with key customer stakeholders on 7 December and when?

52. The number of bi-lateral telephone calls and e-mails during the morning of 7th December between NATS executives (Gold level) and airlines' and airports' executives was extensive. Martin Rolfe (MD Operations and Gold lead) had personal calls with senior executives, for example:

- British Airways – Director of Operations and MD Operations;
- Heathrow Airport – Chief Operating Officer;
- CAA – Assistant Director Airspace Policy;
- And with his counterparts at many other airlines and airports.

5.4 TIME TAKEN TO FIX THE PROBLEM

53. The failure of the Technical Monitoring and Control System (TMCS) servers (main, standby and back-up) occurred during an update of the Voice Communication System (VCS) as part of a series of overnight activities on some 20 systems at the Centre.

54. Subsequent investigations revealed that the failure occurred during re-start procedures following installation of planned changes. The re-start failed due to corruption of 19 start-up files in the TMCS servers which control the VCS system. The fault corruption was replicated to the second standby server and subsequently a back-up spare.

55. The start-up files were corrupted at some point during November 2013, and were lying dormant until the next requirement for a re-start. Investigation by the manufacturer (Frequentis) discovered corruption in network system files, most likely due to an intermittent network connection fault. The TMCS system hardware has since been entirely replaced and the precise reason for the corruption may never be established.

56. The investigation into the subsequent sequence of events is summarised below. A summary of the findings of TRC's independent technical systems expert is at Appendix D which broadly concur with NATS' investigations.

5.4.1 Could the failure have been anticipated?

57. The TRC investigation looked at the history of related problems with TMCS. System logs revealed that difficulties with previous re-starts in April and October 2013 had given engineers cause for concern. For example, in April 2013 there was a similar incident involving TMCS which on that occasion prevented controllers from combining sectors (band-boxing), a scenario which has no impact on capacity provided there are adequate numbers of controllers to continue to operate the unbandboxed sectors. Since then there had been a series of problems which were successfully resolved each time.

58. NATS had already ordered (in November 2013) an enhancement to TMCS from Frequentis to be available during 2014. In the interim, the engineering judgement was that – as these problems had not impacted the ATC service to customers – the residual risk was tolerable in the short term.

59. Given the previous experience with TMCS, the TRC's experts considered that NATS' engineering team could have been more prepared for resolving re-start problems. In particular, re-start problems had been experienced in October 2013 and other faults found before and after 7 December 2013, all of which with hindsight could have merited deeper investigation and response by NATS. However, the experts concluded that *"this particular failure was not realistically predictable"*. But they considered that it would be appropriate for NATS to review the level to which the residual risk of such problem conditions could be considered tolerable / acceptable. The key judgement, however, is that none of the residual risks result in an unsafe system or operation.

60. Engineering procedures for TMCS were immediately changed post event. A planned enhancement to the VCS and TMCS systems has also been deployed which allows band-boxing/splitting without the TMCS. These two changes provide far greater resilience to failure in the future.

5.4.2 Was the system restoration strategy optimal?

Initial Approach

61. Given past experience, it was entirely reasonable for NATS engineers to initially follow normal recovery processes that had been used successfully to recover from previous failures. Engineers made several attempts to recover the failed units using normal processes and procedures, re-booting TMCS several times (main, standby and back-up). This process also included 1st level escalation by telephoning for support from another day team expert.

62. When it became clear that normal engineering processes could not recover TMCS before the early morning traffic flows, escalation processes alerted the NATS Design Authority (DA) and the manufacturer to the problem.

63. At this point there were two competing pressures:

- Establish the quickest way to restore the failed system;
- Don't make the situation worse by taking quick action that has not been thought through.

64. The initial plan (Plan A) – developed in conjunction with the DA and Frequentis – focused on using all available experts to identify and correct the corrupt file and restore the disks as this represented the quickest way to restore the failed system, but options to restore a fresh disk were postulated as a Plan B.

65. In parallel, options for sector splitting were tested by the ATC team in order to understand the limits of what could be done in the night-time configuration. As a result of these tests, the risk to sectors still operating of attempting sector splits was considered too high, and therefore the Operations Supervisor (Bronze) elected to remain in night-time configuration, a decision endorsed by Silver and Gold, as it provided the only guaranteed way of maximising air traffic capacity without introducing uncertainty and change into an already complex situation.

Change in Strategy

66. By 1040 it was clear that the likelihood of Plan A being successful was diminishing as normal processes were not able to restore the service. Therefore, Plan B was adopted to create a new TMCS server, rebuilt from a secure back-up. It was decided to re-build the system from known good copies of the disks dating back to April 2013, which were received electronically from Frequentis at 1130.

67. The TRC's investigation felt that the decision to adopt Plan B could have been made 2 or 3 hours earlier had it been possible for testing of the April disks (by Frequentis) to start much sooner than 0930. That said, the TRC's experts noted that support from Frequentis was good in providing in-depth expertise and service out-of-hours from Vienna.

68. It was recognised that Plan B would necessarily be a lengthy process as there had since been many updates and changes which had to be installed on the April disk to bring it up to December 2013 configuration. This re-built server had to be tested before it could be connected to the operational system. Once connected, it had to complete a process of populating its database with the actual operations room configuration. Safety processes demanded that all this was done in a highly rigorous and carefully planned manner which ultimately dictated the speed of recovery.

69. By 1130 an outline plan for creating a new server had been agreed by the engineering management team. By 1200, a procedure was provided by the DA and a time-line established that would take 4-6 hours to execute. At the 1315 ATICCC conference call customers were advised that the failed system would be operational between 1730-1830.

70. From 1200 onwards the server creation and testing process was followed. Following a safety and service review with the engineering operations and management team, an additional step was inserted to backup the newly created server before it was reconnected to the main voice system. This was considered a reasonable step in case there was actually a fault elsewhere that was causing the servers to fail. This back-up added 30 minutes to the timeline and customers were updated on the 1515 ATICCC conference call.

71. At 1540 the replacement server had been completed and backed up, and was reconnected at 1605. Once the TMCS servers were reconnected to the voice switch, the synchronisation process progressed more slowly than envisaged (as live panels needed to download new configuration) and an additional step of powering off the unused workstation positions was implemented following advice from the DA and manufacturer to speed up the process.

72. However, at 1630 ATC reported an automatic reconfiguration of the current ground-ground communication panels. This was unexpected and led to the application of reduced flow (c.15%), but was quickly resolved. At 1840 the TMCS service was restored and following a short period of testing with engineering and supervisor positions, careful splitting of ATC sectors commenced.

73. Overall, once the decision to go for a full re-load using the April version was taken, Plan B was delivered successfully to the predicted timescales. This followed a period of uncertainty up to 1315 when customers had no reliable information about full restoration of service upon which to plan. At the time, it was difficult to know which approach would deliver a result in the earliest timeframe, and so the communication to customers had to strike a balance between providing certainty and avoiding setting false expectations. The communication principle used was to provide regular briefings but only release expected resolution times when there was an appropriate level of confidence to so – i.e. to get the balance right between communicating early and communicating facts.

What alternative approaches were ruled out?

CAA Questions:
Who made the decision not to shut down and re-boot the [VCS] system?
How was this decision made and communicated to customers?

74. Key decisions on recovery options were made at Gold level. In examining recovery options, the primary aim of NATS' Crisis Management was to ensure safety of the operation whilst maintaining as much capacity as possible. This meant applying prudence in potential changes to the operation while in fallback mode. The overriding need to keep the air-ground-air service operational whilst dealing with a major failure of the ground-ground service (caused by a system that is shared between the two) limited the technical options available for recovery.

75. However, given the potential duration of this failure, NATS was acutely aware that keeping as much capacity as possible could be counter-productive, as a short term more draconian reduction in traffic could provide an opportunity to recover to full service more quickly.

76. TMCS was re-booted several times during initial recovery attempts. Subsequently, shutting down and re-booting the entire Voice Communication System was one of the options considered by the Gold Team. However, it was discounted because: a) it would add significantly to the level of disruption; and b) it might still not solve the underlying problem of re-starting TMCS. The main VCS systems continued to provide air and ground voice communications throughout the event, only the ability to provide pre-configured controller panels to newly opened sectors was impaired. Restarting the entire VCS system would have taken c.2 hours during which time Swanwick AC capacity would be reduced by 90% (compared with the 20%-50% reduction achieved by the operational work arounds).

77. The option of Swanwick contingency at the CTC[3] was also ruled out as it would take time to establish and test, and would require both AC and TC to re-deploy disrupting the entire Swanwick operation for a considerable period. Other technical work-around options for splitting sectors were considered, but carried more risk than the server rebuild and were therefore held in reserve.

78. Communication with customers on recovery steps was via the ATICCC telephone conferences and one-to-one phone calls at Gold level. ATICCC focused solely on recovering the operation, while one-to-one conversations included discussion of options in general terms.

5.4.3 Were resources sufficient?

79. Over 100 additional engineers and specialists from NATS and the Frequentis supported the effort to restore the system. From the change in strategy, what might normally take more than a day to complete was delivered in just 6 hours. This was achieved through highly effective working in different teams (both inside and outside NATS) to complete 'Plan B' as expeditiously as possible, meeting the predicted time for when the ATC operation would be back on line.

80. In deploying so many resources, the engineering team's priorities were to preserve the safety of the current services and to avoid inadvertently making the situation worse. An established process called "TAKE 5" was used to ensure that risks were considered, understood and mitigated before taking actions that could have a service risk. TAKE 5 was used for several critical decisions during this process slightly adding to the timeline but significantly reducing risk.

81. The TRC investigation noted that *"Faced with what must have been a frustrating and unnerving situation it has to be said that the work was carried out in a highly professional manner, the correct processes were followed and there was excellent co-operation from all concerned including the suppliers of the system"*.

[3] A back-up facility for Swanwick for a catastrophic failure scenario which takes around 48 hours to bring into operation – see Chapter 2 Context.

5.5 ADEQUACY OF NATS' RESPONSE – CONCLUSIONS

Did NATS do a good job in minimising disruption faced with unusual circumstances?

Speed and scale of reaction to a developing crisis

82. Engineering escalation was started as soon as it was realised that normal fault isolation and correction would not be as quick as usual. This was sufficiently early to allow operational contingency plans to be put in place in advance of normal daytime traffic (ATICCC, Eurocontrol, Terminal Control and Prestwick) and to ensure crisis command and control was established and effective. It also rapidly mobilised key engineering experts and resources (0400) to focus on a different recovery approach at the earliest opportunity.

83. An appropriate crisis management structure was in place from 0400 (Bronze) to manage the events with an appropriate level of responsibility for key decisions. By 0830 all levels of management had been fully engaged. Credible business continuity plans and unit (Swanwick) contingency plans were in place and successfully executed.

84. ATICCC was activated at 0547 for crisis communication with customers, with the first customer conference call held at 0725. There was a time lag between customers being affected by the problem (by traffic flow restrictions) and being advised of the cause, implications and options open to them. Some customers were affected by slow delivery of e-mail notifications.

85. A key decision to keep the Swanwick AC operation running in 'night-time mode' was in the best interests of customers as it maintained as much capacity as possible while resolution and recovery took place. A more draconian short-term shut-down of the Swanwick AC operation – potentially causing more cancelled flights – would not have recovered the situation more quickly and, at the time, it was not certain this step would have worked.

86. Key stakeholders were alerted, with one-to-one discussions at Gold level to brief them on the circumstances and implications, and to provide assurance that sufficient and appropriate action was in hand.

87. Media questions were initially handled by the Duty Press Officer, with media statements at 0755 and 0940. A fully staffed press office engaged actively with the media, competently handling crisis communications throughout the day. There were clear messages on safety, cause of the problem and an apology to those affected, but over-simplification of some messaging attracted criticism. Live TV interviews took take place from 1100; an earlier broadcast would have provided an opportunity to respond more quickly and directly to customers and passengers. Greater use could have been made of social media (Twitter) later in the day in the gap between media statements.

Maximising available capacity to minimise disruption

88. The potential airspace capacity reduction due to the failure was mitigated by greater use of lower level routes, a reduction in danger area activity in northern UK and the provision of some services in uncontrolled airspace. Safety was not compromised at any time.

89. Proactive network management by the Swanwick FMP with Eurocontrol DNM, together with the continuous dialogue with airlines and airports throughout the day, ensured the available capacity was used efficiently.

90. A number of operators could not take-up alternative routing options due to flight planning constraints or limitations on operating outside controlled airspace. The Eurocontrol DNM diverted some 500 transit flights around the affected airspace.

Helping airlines and airports to manage the disruption

91. ATICCC helped airlines and airports to respond optimally to the disruption to their flights and schedules, also providing information that airlines and airports could use to keep their customers updated on the situation. Also on-going dialogue took place with customers via the Heathrow Operational Efficiency Cell and NATS' FMP. This was supplemented by extensive bi-lateral

telephone calls and e-mails between NATS executives (Gold level and Customer Affairs) and airlines' and airports' executives.

92. There is industry-wide consensus for pre-planned scenarios and capabilities to be developed to help all parties in future to better react to a crisis at short notice.

Time taken to fix the problem

93. NATS engineers initially followed normal recovery processes that had been used successfully to recover from previous TMCS failures. With hindsight, given the previous experience of TMCS failures, NATS' engineering team could have been more prepared for resolving re-start problems. The initial engineering response to failures could be improved by supplementing existing system recovery and escalation processes with additional solutions that provide alternative means to expedite recovery.

94. Escalation processes (at 0400) alerted the NATS Design Authority (DA) and the manufacturer to the problem. The initial plan (Plan A) focused on using all available experts to identify and correct the corrupt file and restore the disks as this represented the quickest way to restore the failed system.

95. Plan A was eventually abandoned at 1040 and Plan B adopted to create a new TMCS server, rebuilt from a secure back-up. If disk testing (of the secure backup) had been able to start much sooner, the decision to adopt Plan B could have been made 2 or 3 hours earlier.

96. By 1200, a procedure was provided by the Design Authority (DA) and a timeline established that would take 4-6 hours to execute. At the 1315 ATICCC conference call customers were advised that the failed system would be operational between 1730-1830. Communicating the recovery decisions and progress to customers had to strike a balance between providing certainty upon which they could plan and avoiding setting false expectations.

97. From the change in strategy, over 100 engineers and specialists worked to restore the system. This was done in a highly rigorous and carefully planned manner, meeting the predicted time for when the ATC operation would be back on line.

98. Key decisions on recovery options were made at Gold level. It is difficult to know in advance which approach will deliver a result in the earliest timeframe, but a new framework is being proposed to ensure alternatives approaches for recovery are assessed and choices are made in a clear and transparent manner.

6 Adequacy of NATS' Contingency and Resilience Plans

Are NATS' contingency and resilience plans, and their execution, robust and effective?

1. The previous chapter of the Report examined NATS' *business* contingency and resilience plans, namely:

> Incident and crisis management via the NATS Business Continuity Plan (BCP);
> The ATICCC process and wider communication plans;
> Contingency plans, both operational (capacity re-generation) and technical (system restoration).

2. This chapter therefore focuses on NATS' *system* resilience:

> Whether NATS' overall approach to system resilience is sufficiently robust and effective;
> Whether the level of contingency this approach provides meets reasonable operational expectations of customers at reasonable cost?

6.1 NATS APPROACH TO SYSTEM RESILIENCE

6.1.1 How system resilience is provided

3. NATS' approach is to build sufficient resilience into its systems (and operations) to ensure that it can cope with a failure without impacting safety or the service to airspace users. The TRC's independent experts acknowledged that in complex environments with highly inter-dependent systems there will be failures, including incidents of hardware and software failures, and of data corruption. Many such failures will be difficult or impossible to predict, and hence carry residual risk.

4. In common with standard practice in ATM systems worldwide, NATS' objectives for resilience are:

> To provide adequately robust systems where the likelihood of failure is very low;
> To limit the impact of any failures on the ATC service to acceptable levels;
> To equip the organisation with high levels of recovery capability.

5. Against these objectives, the strategy for ensuring resilience against systems failure is a 'defence in depth' by applying proactive barriers to reduce the likelihood of a failure (or malicious attack) and reactive barriers to reduce the effect. NATS adopts a holistic approach to managing resilience risk, which is aimed at reducing both the likelihood and effect of failures.

Proactive Barriers	**Reactive Barriers**
Architectural mitigation – geographic separation and diversity	Automatic recovery
Systems self protection – links to other systems cut if errors occur	Graceful degradation – allowing a partial service
System design features – redundancy, hardware choice	Rapid fault diagnosis and recovery – by on-site or on-call engineers
Active in service monitoring and supervision by qualified engineers	Fallback systems & procedures – controllers trained in fallback modes
Predictive planned maintenance	
Implementing change in a controlled manner and avoiding demanding traffic scenarios	

6. In November 2011, the TRC examined NATS' approach to resilience, including the risks and choices on how resilience should be managed. This resulted in recommendations to increase the priority given to ensuring resilience in new systems, to reviewing resilience in current major systems and to measuring resilience in systems. The recommendations were all implemented and the Technical Advisors to the Board visited Swanwick in February 2012 to discuss the approach to managing resilience and review the results. The support of the TRC and their advisors has been valuable, providing useful challenge to ensure a robust approach.

7. Following the event on 7th December 2013, NATS is carrying out a further review of crisis management and resilience which will include a review of current resilience and contingency capabilities (see Chapter 4 also). Additionally, the TRC has tasked NATS with providing assurance on resilience of all existing and future operationally critical systems to a level that has been achieved by this investigation.

6.1.2 How effective is the current approach?

8. A good measure of the effectiveness of NATS' approaches to managing resilience and failure is the extent to which it achieves the objective 'to limit impact of any failures on the ATC service to acceptable levels'.

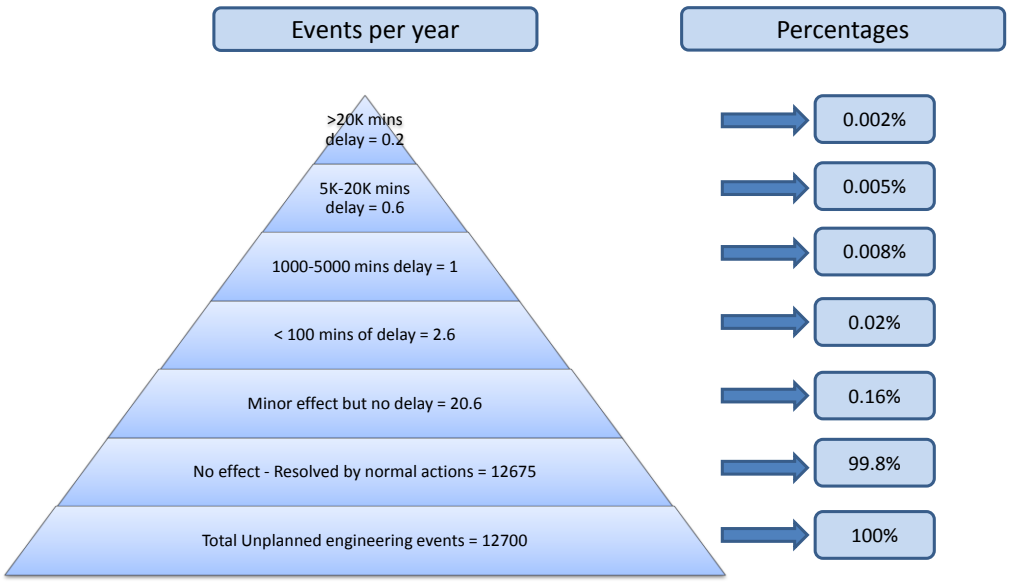
9. Each year NATS records on average around 12,700 unplanned engineering events. These span a wide variety of engineering activity that ranges from minor faults through to major incidents. NATS' processes for actively managing unplanned incidents, together with the nature of the system architecture and the other proactive resilience barriers put in place, result in almost all (99.8%) being resolved without any adverse impact on customers.

10. Around 25 of these unplanned engineering events each year are of such significance that they did, or could have, increased safety risk, caused delays or created some other adverse impact. In most cases, the reactive barriers were effective in mitigating and resolving the situation quickly such that the impact was avoided or kept to a low value. The diagram below shows the extremely low percentage of unplanned engineering events that actually cause delays to customers. Despite the unplanned events, NATS' safety record is exceptionally good.

11. The TMCS failure on 7th December 2013 fell into the 0.002% of unplanned engineering events that have a severe impact on customers. This is against a background where only a small number of significant system failure events (of similar magnitude to the 7th December failure) had occurred over a ten year period. None of such events had generated any increased level of safety risk, and the impact was restricted to operational disruption.

12. Further explanation is provided in Appendix E.

Impact of Unplanned Engineering Events – 5 Year Average



6.1.3 Who decides whether the level of resilience is appropriate?

13. NATS manages risks using a 'Risk Assessment and Management Plan' (RAMP) which is an industry-wide standard for monitoring and managing risks in an efficient, cost effective and consistent manner. Company level risks are recorded in a 'Blue RAMP' and lower level engineering risks are recorded in a 'Purple RAMP'.

14. Underpinning the RAMP is a Service Resilience Risk Framework to define what level of risk is acceptable to NATS' business and systems. The framework is based on the criticality of the risk (severity of impact) and the likelihood of the risk event occurring. The criticality/likelihood combination determines the extent to which the risk may be acceptable. In many instances, acceptability of risk is governed by the safety case process where the risk assessment and assurance required in approving a critical system is extremely demanding.

15. At a system-by-system level, the appropriate level of resilience is determined via engineering design and safety assurance processes – see 'risk sign-off' below.

16. At the overall system level, and against key customer requirements for predictability and continuity of service, NATS performance (including resilience) is incentivised via a range of delay metrics in its regulatory regime. A 'delay variability' metric (known as T3), which is designed to avoid instances of excessive delays caused by NATS such as by system outages, provides an industry-level measure of whether NATS' resilience is appropriate. To maintain balance, a headline average delay target (T1) ensures NATS focuses on overall delay performance, not just on the causes of delay spikes. T1 and T3 performance averaged over the last 5 years has been extremely good, and approximately five times better than the European average for service performance.

CAA Question: How are the limitations of [other] key supporting system/capabilities assessed and mitigated against?

17. The risks in NATS engineered system and mitigation plans are continuously reviewed and developed through the established Asset Management processes which are in line with the international standard ISO55000. Risks are identified and mitigation plans developed through a series of Asset Review Boards. The mitigating actions typically include procuring replacement assets, or interim engineering or ATC procedures to reduce the likelihood of an event occurring or to reduce its effect. General tactical mitigation actions are not included in the RAMP plan but include, for example, weekly reviews of incidents by NATS Design Authorities, asset health reviews and senior management reviews of planned service interruptions.

18. The company level risks (Blue RAMP) are regularly subject to senior management review including the NATS Board. Regular reports are made by the Executive to the Board (and TRC) on the primary areas of operational risk and on systems resilience, failure events and performance impact. Resilience is a standing agenda item at the TRC, with a report on risk status and current issues being presented to each meeting. At a company level, equipment issues are assessed as a general 'resilience risk' and this risk was reviewed by the NATS Board in November 2013. This includes reference to engineering delay performance as one output indicator as to whether the overall risk management process has been effective.

19. Following the November 2011 TRC review of resilience, on-going reviews of the resilience of key functional threads within NATS' systems architecture have been undertaken covering flight data processing, surveillance systems, voice communications, traffic management, ATC information systems and data networks. This has resulted in a clearer baseline of the resilience of the current systems, a more consistent approach to risk identification and mitigation, and ensured resilience requirements can be assigned at the outset of all new projects.

20. Following the TMCS failure on 7 December, a further review of all systems was completed to identify any that could fail in the same way and to ensure mitigation was effective. The review also considered restoration times for systems following catastrophic failure and the service levels that could be achieved. It concluded that effective barriers and mitigations to reduce the likelihood and impact of failures were in place, and that restoration times that could be achieved following major failure were understood.

21. Additionally, a new Asset Sustainment Board has been established to oversee the individual Asset Review Boards and provide additional assurance that the overall engineering risk is

tolerable. The Asset Sustainment Board is chaired by the Engineering General Manager with safety and service accountability.

CAA Question: Who within NATS signs off the risk tolerability/acceptability for major system components?

22. Risk tolerability/acceptability is part of NATS' formal and structured process for accepting new or modified systems into service, or asset management processes for in-service systems.

23. The delivery into service process requires evidence and assurance to be provided to demonstrate that the new system or change being introduced satisfies safety and operational requirements, has been fully tested, is fit for purpose in both normal and fallback/contingency operations, and has been accepted by the relevant authorities (e.g. the Safety & Airspace Regulation Group).

24. Regarding in-service systems, risks are reviewed via the Asset Management / RAMP process. The individual and collective risk is assessed by Senior Engineering Managers who decide on mitigation and corrective actions.

25. Who signs-off the risk tolerability/acceptability depends upon on criticality. For new systems, the Unit General Manager will generally sign-off residual risks at the 'operational handover' milestone, signalling that the system or change delivered has met all the requirements for being accepted into operational service. Senior Engineering Managers (within Asset Review Boards) sign-off the risk tolerability/acceptability of residual risks for in-service systems. However, if a significant safety risk remains in either case, additional sign-off processes must be agreed with the relevant Operations Director or MD Operations for the most significant risks.

CAA Question: As the risk presented by the VCS was only reviewed last November, are the mechanisms and procedures for review adequate?

26. The TMCS was a known resilience risk and was due to be replaced in early 2014 (and has now been replaced). A RAMP entry for the TMCS component of VCS was first raised in December 2012:

> "As a result of the AC VCS control and monitoring system (TMCS) becoming end of life, there is a risk that when the TMCS fails the restoration time will be significantly increased, which would lead to it being impossible to open or close sectors and therefore the need to impose up to 80% flow rates or having to keep all the sectors open during quiet periods leading to an additional 80 controllers being required."

27. The principal risk mitigation action was to procure an upgrade to the TMCS system, due from Frequentis in early 2014, that would permit the voice switches/panels to be reconfigured during a failure of TMCS.

28. The outcome of the November 2013 risk review was to support the mitigation action in place. The engineering judgement was that – as TMCS problems had not impacted the ATC service to customers – the residual risk was tolerable in the short term based on the historical failure rate, health reviews and close monitoring. The planned enhancement to the TMCS system has since been deployed.

29. As previously highlighted in section 5.4.1 (could the failure have been anticipated?), the risk review process appeared to focus too heavily on TMCS system change rather than the inherent vulnerability of the TMCS pending upgrade as evidenced by its history of problems. Therefore, the risk review could have also considered – as the system change had not yet been delivered – whether engineering and ATC procedures for dealing with a TMCS failure in the meantime were appropriate to the risk. Following the incident, the way risks are reviewed has been refined to include additional checks where a similar risk exists.

CAA Question: What is the role of the Systems Architect in this process?

30. NATS' Chief Architect is a strategic role that defines the overall future design of the air traffic system rather than be involved in the approval of each system change. The process for defining and validating the future architecture takes account of lessons learnt from the existing architecture. There are NATS Subject Matter Experts (SMEs known as System Design Authorities)

who have the safety accountability for the fitness for purpose of functional threads within the overall architecture. They monitor performance and risks relevant to the specific thread, in this case communications. However, overall resilience is a core responsibility of the Chief Architect role, providing assurance that the decisions and investments NATS makes maintain the necessary integrity and resilience of air traffic systems to meet current and future needs.

31. The Chief Architect operates at senior level with a high degree of authority and influence, autonomy and independence of thought. The role carries a clear duty, beyond any reporting lines, to bring to the attention of the Board (TRC) any conflicting judgements, or significant shortcomings of design or implementation which threaten the integrity or effectiveness of the systems in NATS. This is akin to the obligation and responsibility of the Safety Director.

6.2 APPROPRIATE LEVELS OF CONTINGENCY

6.2.1 How NATS currently determines what contingency is appropriate

CAA Question: How does NATS interpret its Licence and SES obligation in relation to resilience and contingency?

32. Single European Sky (SES) regulations require ANSPs to have in place "contingency plans for all the air navigation services they provide in the case of events which result in significant degradation or interruption of their operations". The NATS En-Route plc (NERL) Licence requires it to "deliver Core Services to meet any reasonable level of overall demand on a continuing basis".

33. These requirements – SES 'contingency plans in case of degradation or interruption' and Licence 'deliver services on a continuing basis' – combine to ensure NATS considers contingency and resilience as part of its overall service delivery capability. This informs NATS' business and capital investment planning, resulting in a two-pronged approach.

- NATS' approach to resilience – which has already been discussed above.
- NATS' approach to contingency planning – which is now explained below.

Contingency Approach

34. At the strategic level, customers have consistently expressed their requirement (during consultation on NERL's Business Plans for regulatory control periods) for adequate levels of contingency to ensure continuity of service in the event of major failures or catastrophic loss. This has resulted in past consultations on appropriate levels of contingency, for example:

- Pre PPP (in the late 90s) on NATS' two-centre strategy and the appropriate level of contingency to be included in the investment;
- West Drayton closure strategy (in 2003) to replace the mutual capability between Swanwick and West Drayton with an 'operationally capable' training system;
- A reappraisal (in 2006) of operational contingency and capacity re-generation;
- The 'SLAM/ATSOCAS' project (in 2010) which included a 'sudden loss' capability to safely clear skies in the event of instantaneous loss of service from London Terminal Control.

35. Regarding contingency at the day-to-day operational ATC centre level, contingency arrangements are developed via NATS and Unit level Business Continuity Plans (see section 5.1.2 availability of contingency plans).

36. Each system, tool set, piece of equipment that is used in providing services have multiple levels of contingency and resilience requirements placed upon them. There are also processes and operational procedures in the event of any service interruption of equipment – often referred to as 'fall back procedures' which are approved by the CAA Safety and Airspace Regulation Group.

37. All this together demonstrates a robust and consultative approach to fulfilling SES and Licence requirements for contingency and resilience.

CAA Question: How are NATS' risk management mechanisms agreed with airlines and airports?

38. NATS' risk management and contingency procedures have been subject to review and discussion with the NATS/Customer Operational Partnership Agreement (OPA) and through NERL's Service and Investment Plan (SIP) process. As a result, plans have evolved over a number of years to include lessons learnt and joint industry actions stemming – for example – from ATICCC activations, system failure events, significant weather events, volcanic ash disruption and London Olympics airspace management. Similarly, airport ATC crisis management procedures are subject to regular and post event review with airport operators' crisis management teams.

6.2.2 Does contingency provided meet expectations at reasonable cost?

39. NATS maintains a significant level of contingency and resilience within its operation, for which a balance has to be struck between the level of residual risk and the cost / additional complexity of implementing further mitigations, either through system investment or extra staffing.

40. NATS considers that the current level of contingency and resilience strikes a reasonable balance between operational assurance and cost, and has been developed in consultation with customers. However, this is always a balance, which has to be judged against three influencing factors:

- A capital investment envelope which is fixed by the Regulator each 5-year control period based on proposals from NATS developed in consultation with customers;
- The substantial reduction in operating costs and manpower necessary to meet regulatory performance targets for cost efficiency;
- The level of service provided to customers, where delays have been at an extremely low level for several years, in particular delays caused by engineering events (see 6.1.2).

41. To put this in context, alongside the almost zero average delay on a daily and yearly basis, the events of the 7 December represent the only significant disruption event caused by NATS since the start of the regulatory performance regime (CP2) over 8 years ago. In this period NATS has safely and efficiently moved over 18 million aircraft and 2.2 billion passengers.

42. The sections below provide more detail on the planning and consultation approach NATS uses to ensure that the right balance can be retained.

CAA Question: How is resilience and contingency treated in NATS' planning of, and consultation on, capital expenditure?

Planning

43. NATS plans the evolution of resilience in its services via its portfolio of projects and programmes in the Long Term Investment Plan (LTIP).

44. In shaping the LTIP, NATS' Operations Strategy sets out broad objectives for investment, including for example "an ATM system with such resilience that it allows the operation to cope with a major ground system or data network failure, without impacting the service level to airspace users", and "a system of tools and procedures to ensure continuity and consistent service levels to our customers".

45. As specific investments are proposed, they must demonstrate the extent to which they meet strategic objectives. Specifically, two principles are applied to all investment proposals:

- Planned improvement: Service Resilience is included in Strategic Project Requirements (SPRs) and Architectural Design Envelopes (ADEs) for every investment.
- Prevent regression: ensure that other SPRs and ADEs do not degrade Service Resilience.

46. As highlighted in 6.2.1 above, some investment proposals are specifically for the provision of contingency to meet strategic resilience requirements, or include contingency (fall back) as part of a system or change project to meet specific 'reactive barrier' resilience requirements.

47. All this demonstrates that resilience and contingency is a fundamental part of LTIP planning.

Consultation

48. NATS is obliged in its Licence to consult airspace users regarding capital investment. This is done via consultation on business plans for each regulatory control period (every 5 years) and an annual progress review via the SIP process.

49. NATS' capital expenditure plans are subject to considerable scrutiny by customers and the Regulator, especially during consultation on NERL's business plans. This includes the extent to which plans contribute to customers' requirement for "adequate levels of contingency to ensure continuity of service".

50. Much of the debate focuses on the extent of so-called 'sustainment' capital expenditure (capex) which ensures a resilient ATM infrastructure and has historically been the dominant capital spend. This investment is directed at refreshing NATS' asset base to reduce the risk of failure as systems and buildings age, and to update / upgrade assets to keep the operation running efficiently on a day-to-day basis. Customers and the Regulator understand that, in arriving at an affordable capital investment plan, a smaller capex envelope than that proposed by NATS has the effect of increasing risk within NATS' asset base.

51. Other investment is directed at future capability. The recent RP2 process included, for example, consultation on future centre systems and how such investment improves resilience and contingency. NATS is focusing such investment on deploying new technology platforms to meet Single European Sky development goals in the next few years. This will enable retirement of legacy architecture at the earliest opportunity to improve resilience overall. Additionally, the new technology platform will create a single common operation across Swanwick and Prestwick ('two centres, one operation') which will enable far greater flexibility and capability in contingency provision. This approach essentially changes the emphasis of investment plans from asset sustainment and replacement to future capability, which has been supported by customers during the RP2 and SIP processes in 2013/14.

52. NATS' view is that current investment plans provide the best balance of cost versus risk. Irrespective of the level of investment in additional resilience, it is unrealistic to assume that a highly complex non-stop 24/7 operation can operate at 100% capacity without occasional constraints on service capacity. Therefore, rather than invest in additional technology, which would add complexity and therefore could be counter-productive by creating more risk, a better approach is the one being taken to develop a systematic pre-planned industry response to minimise the effect of severe disruption in rare cases such as this.

6.3 ADEQUACY OF NATS' CONTINGENCY AND RESILIENCE PLANS – CONCLUSIONS

Are NATS' contingency and resilience plans, and their execution, robust and effective?

NATS Approach to System Resilience

53. There are effective approaches to managing resilience and failure / fall back modes which ensured that the situation was understood and was dealt with safely and securely.

54. Industry standard Asset Management and RAMP processes ensure risk tolerability / acceptability is correctly identified, effectively mitigated and continuously reviewed.

55. TMCS was a known resilience risk but considered tolerable in the short-term, pending replacement, based on the historical failure rate, health reviews and close monitoring. Subsequently, the way risks are reviewed has been refined to include additional checks where a similar 'identified but system change pending' risk exists.

56. NATS fully reviewed the approach to resilience with the TRC (in 2011) and has regularly presented key resilience risks. Further review of the resilience of all existing and future operationally critical systems is now in progress following this event.

Appropriate Levels of Contingency

57. There is a robust and consultative approach to fulfilling SES and Licence requirements for contingency and resilience.

58. NATS maintains a significant level of contingency and resilience within its operation, for which a balance has to be struck between the level of residual risk and the cost / additional complexity of implementing further mitigations, either through system investment or extra staffing.

59. Contingency and resilience is a fundamental part of LTIP planning with all investment proposals demonstrating the extent to which they meet strategic resilience requirements, including contingency (fall back) measures where appropriate.

60. NATS' capital expenditure plans are scrutinised by customers and the Regulator during consultation on NERL's Business Plans and via the annual SIP process, including 'sustainment' capital expenditure which ensures a resilient ATM infrastructure.

61. New technology platforms to meet Single European Sky development goals will improve resilience and enable far greater flexibility and capability in contingency provision.

7 Changes Resulting from Investigations, Lessons and Consultation

Avoiding any recurrence, doing things better…

Crisis Management

Implementing the business continuity plan:

> More advantageous to formally invoke Gold / Silver teams for future similar events in order to ensure that the expertise and experience of the teams is underpinned by the structure and clarity of the formal business continuity processes;

ATICCC process:

> Faster process for activating ATICCC and for communicating with customers ahead of ATICCC conference calls to ensure customers are aware as quickly as possible of the causes, implications and options open to them;

> Faster and accurate delivery of e-mail notifications, including alternate solutions.

Decision-making:

> Framework to consider trade-offs between keeping as much capacity as possible versus a short term draconian reduction in traffic that may recover to full service more quickly;

> Decisions on recovery options made in a clear and transparent manner as soon as possible;

> Key decisions communicated to customers quickly to provide reliable information about restoration of service upon which they can plan, reducing uncertainty to airlines, airports and passengers.

Building on the strong teamwork shown on 7 December:

> New cross-NATS crisis management exercises and scenario training.

Contingency Plans

A simple cross-industry plan that is understood in advance:

> Industry proposals for pre-planned scenarios and capabilities to help all parties in future to better react at short notice;

> Pre-planned traffic scenarios to help airlines react to non-standard routeing;

> An industry crisis exercise to establish the capability of entire UK air transport industry to maximise total network capacity when faced with significant disruption.

Engineering

Improve the engineering response to failures and recovery processes:

> Enhance existing escalation processes and identify fall back methods of operation that could reduce the service impact and expedite recovery;

> A new framework to ensure alternative approaches for recovery are assessed and choices made in a clear and transparent manner.

ATC Operations and Network Management

Improve the operational responses to disruption:

> Operational Resilience Enhancement Plan (OREP) to progress options for enhancing service resilience and performance during contingency operations, including acceptably safe fallback methods of operation to reduce service impact;

> As part of OREP, enable other operations rooms to control aircraft in adjacent affected airspace, for example allowing Terminal Control or Prestwick to operate in adjacent AC airspace sectors (or vice versa).

Communications

Communicate better with customers, stakeholders and the wider world during a crisis:

> Collocate media response (press office) close to ATICCC to improve co-ordination;

> Enhance crisis communications with customers over and above the ATICCC process to ensure specific needs are understood;

> Develop a broader outreach to NATS' complex stakeholder network beyond customers that better recognises the number of different audiences in play during such incidents;

> Timing of media conference calls in relation to ATICCC customer calls to ensure a regular and rapid update to the media;

> Greater use of social media (Twitter), to keep passengers and observers updated.

Voice Communications System

Ensure the events of 7 December are not repeated:

> Immediate changes to TMCS and engineering procedures to prevent a recurrence of this particular failure;

> Deployment of a planned enhancement to the VCS and TMCS systems (completed in early 2014) which allows band-boxing/splitting without the TMCS to provide far greater resilience to failure;

> Alternative ground-ground communications contingency options to enable controllers to communicate between sectors / other agencies without VCS.

Resilience and Contingency

CAA Question: What will be different in future with regard to resilience and contingency as a consequence of the events of 7 December?

Improved crisis management and resilience capabilities:

> A wide-ranging review of crisis management and resilience covering the breadth of NATS' preparations for disruption to enable a better industry response to similar events.

Reduced risk of similar failures:

> A full review of resilience of systems to major failure to ensure effective barriers to reduce the likelihood and impact of failures are in place and that restoration times that could be achieved following major failure are understood;

> Provide assurance to the TRC on resilience of all existing and future operationally critical systems to a level that has been achieved by this investigation;

> Risk management review process refined to include additional checks where a similar 'identified but system change pending' risk exists;

> A new 'Asset Sustainment Board' to provide additional assurance that the overall engineering risk is tolerable.

Increased resilience levels:

> NATS' capital investment programme's emphasis on replacing legacy systems at the earliest opportunity to improve resilience to failure.

Final CAA Question: Have the changes that have been made since the 7 December highlighted any major flaws in the pre-existing NATS arrangements?

The changes being made have not highlighted any major flaws in NATS' arrangements. However, the changes listed above confirm that more can be done across NATS and the industry to further improve on the already high levels of resilience and to minimise the effect of severe disruption in cases such as this.