NATS System Failure 12 December 2014 – Interim Report

1. Introduction

1.1 Following a failure of some United Kingdom air traffic control (ATC) services on 12 December 2014 (the Incident), the Civil Aviation Authority (CAA) and NATS (formerly National Air Traffic Services) announced the establishment of an independent enquiry into the cause of the failure, the recovery and other relevant factors. After the appointment of the Panel members, the Enquiry formally started on 13 January 2015.

1.2 Terms of Reference (TORs) for the Enquiry, which include a list of Panel members, are at Annex A and were published on the CAA website on 16 January 2015. The TORs call for an Interim Report by 31 January 2015 and state that this should be focused on the NATS internal investigation[1] of the 12 December Incident. The Final Report, due no later than 14 May 2015, will address the remaining and generally wider issues specified in the TORs and will include the Panel's views on the root causes lying behind the Incident.

1.3 The Incident started with the failure at 1444 GMT (this and all subsequent times are reported in the 24 hour format at GMT) of a computer system used to provide data to Air Traffic Controllers to assist in their decision-making when managing the traffic flying at high level over England and Wales. This traffic includes aircraft that have departed or are planned to arrive at major London airports (Heathrow, Gatwick, Stansted, Luton and City) as well as aircraft transiting UK airspace. The Controllers put their pre-agreed operating procedures into action for the particular computer system failure; these include adopting manual methods for decision-making to ensure aircraft continue to maintain safe separation and restricting air traffic entering their area of responsibility.

1.4 At 1455 all departures were stopped from London Airports and at 1500 all departures were stopped from European airports that were planned to route through affected UK airspace. The engineering experts were able to determine the nature of the failure and agree a safe recovery procedure so that the computer system was restored to the Controllers at 1549, but without its normal level of redundancy (back-up). By 1900, the Engineering staff believed they understood the cause of failure and full redundancy of the computer systems was restored at 2010. Traffic restrictions were gradually lifted from 1555 as confidence increased, and the final restriction was lifted at 2030. The disruption caused by the restrictions affected airlines, airports and passengers into the following day.

2. Background

2.1 Air Traffic Management in the UK is carried out in two adjoining regions, The Scottish Flight Information Region (FIR) and the London FIR. The London FIR is divided into:

(1) London Area Control (LAC), which handles civil aircraft over England and Wales in flight at high level.

(2) London Terminal Control (LTC) which is a smaller area, including the five main London airports, and covers aircraft generally flying below 21,500 feet, with the precise height demarcation with LAC depending on the location.

2.2 These areas are shown diagrammatically at Annex B. Aircraft passing through UK airspace (principally between Europe and North America) transit LAC en route; aircraft destined for the London Airports transfer from LAC to LTC as they descend and vice-versa for departing aircraft.

2.3 The Incident on 12 December abruptly affected ATC throughout London Area Control at 1444. Air traffic services for both LAC and LTC are operated by NATS and, together with military aircraft services for the UK, are provided from separate control rooms within the same building at Swanwick, some 5 miles South-East of Southampton Airport.

3. The LAC Operation

3.1 LAC is divided into a maximum of 32 sectors that can be combined ("bandboxed") at times of light traffic or separated or sub-divided ("split") when the traffic is heavier. The number of staff varies through the day, week and season but broadly depends on the number of aircraft expected to be flying in or through the London FIR. There are five "watches" of Controllers to manage the Operations Room on a continuous basis.

[1] SP301 Major Incident Investigation: Preliminary Report Version 2.0 January 2015.

3.2 Each Controller can operate for up to 90 minutes without a break and controllers are rostered throughout the day to meet this requirement. When staff are not required at a workstation because of lighter traffic conditions, they are encouraged to leave the Operations Room, partly so as not to distract those engaged in operational duties. At the time of the Incident there were 26 Controllers in the LAC operations room with some further 42 (LAC) Controllers on duty elsewhere at the Swanwick site. At the time of the Incident there were also 6 operational engineering staff in Systems Control (which oversees the status of the technical systems supporting the Swanwick site) adjacent to the Operations Room. 244 aircraft were expected to be under control of LAC during the hour following the incident.

3.3 Controllers normally work in pairs: a Tactical Controller who communicates with the aircraft under control and a Planning Controller who manages the flow of traffic into and out of their area of responsibility through liaison with adjoining NATS or other national ATC areas. An Air Traffic Services Assistant provides support to the controllers when required. The primary safety objective of these arrangements is to ensure a height separation of at least 1000’ between aircraft or, where aircraft are within this limit, to maintain a lateral separation of at least 5 miles.

3.4 Each pair of Controllers is assigned to a particular sector or combination of (bandboxed) sectors. They are supervised in groups of 5-8 sectors by Local Area Supervisors. An Airspace Capacity Manager is focused on the overall flow of traffic in the LAC and supports the Local Area Supervisors in managing the bandboxing or splitting of sectors. The Operations Room as a whole comes under the charge of the Operations Supervisor. Both the Operations Supervisor and the Airspace Capacity Manager have designated Assistants.

3.5 NATS operates a network of radar stations that provide the position and height of all aircraft flying in the LAC. A data fusion system determines the best estimated position when an aircraft is detected by more than one radar so that the aircraft appears only once on the workstation screen; a label adjacent to the aircraft icon gives its height and can give the heading and other related information.

3.6 The Controller can call up all other necessary data associated with a particular aircraft, derived from its flight plan information. The flight information derives from a flight data processing system, also operated by NATS and known as NAS (or National Airspace System), and this is routed to a System Flight Server (SFS) that delivers the right information to each workstation. Annex C contains a schematic of this data routing.

3.7 When a Controller signs on to a workstation in its initial powered state, it changes from “Base Mode” to “Prepare Mode” and recording to archive starts of all information available to the workstation; but the workstation cannot be used to control air traffic. The Controller then selects his designated sector thereby notifying the System Flight Server of the aircraft data required by the workstation; the workstation moves into “Elected Mode” and displays a copy of the data being used at that time to control the selected sector. If the Controller then selects “Open Sectors”, a workstation goes into “Controlling Mode” and becomes fully operational while the workstation previously controlling that sector moves into the Elected State; this transfer of responsibility is managed by the Local Area Supervisor (see paragraph 3.4).

3.8 There is a further mode called “Watching Mode” which allows a workstation to display a full copy of the data from another workstation. “Watching Mode” is entered by selecting sectors on a workstation that is not signed on (whereas a signed on workstation would move into “Elected Mode”). Normally all the workstations in the LAC Operations room are “Signed On” – even when unattended – so that they are readily available for use, e.g. when splitting previously bandboxed sectors in anticipation of a traffic increase. The “Soft” “Sign Off” button on a Controller’s workstation screen is, however, immediately adjacent to the “Select Sectors” button; not infrequently – NATS data suggests that this occurs a few times in a week – the Sign Off button is pressed by mistake. If a Controller then presses the Select Sectors button the station will enter Watching Mode – but until 12 December 2014 this did not lead to service disruption.

3.9 All of the operational roles that can be performed within the LAC (for example the Tactical Controller for Sector 16) have a unique identifier known as an Atomic Function. Atomic Functions are therefore allocated to each of the various roles managing each specific civil sector (or bandboxed sectors) in the LAC, as well as to the military ATC control and supervisory services throughout the UK (paragraph 2.3). The Atomic Function identifiers are the unique label that ensures that the SFS (paragraph 3.6) supplies the appropriate information and communication capabilities to each workstation. The integrity and accuracy of this data distribution is therefore a fundamental requirement of the overall system of control.

3.10 Whenever the role of a workstation is changed anywhere in the operations room (e.g. when two sectors are bandboxed), the list of newly current Atomic Functions is recompiled and is then used to create a new look-up table in order to distribute the correct information and capabilities to each Atomic Function. The system is capable of providing a look-up table for up to, but no more than, 193 Atomic Functions, and would be unable to assure the integrity of the distributed information and capabilities to any greater number. This limit of 193 has never been closely approached in practice.

4. The Incident

4.1 The failure occurred in the System Flight Server (SFS) at Swanwick Area Control. The SFS has two channels so that one channel will normally continue to operate and provide service, if the other fails. The disruption on 12 December 2014 arose because (for the first time in the history of the SFS) both channels failed at the same time.

4.2 The importance of the unique identifying labels for each Atomic Function was explained at paragraph 3.9. When a workstation requests to enter Watching Mode, SFS must check that the command is valid which involves creating a list of active Atomic Functions. However, when this check is performed on entering Watching Mode, the maximum system capacity had been programmed as 151 Atomic Functions (rather than the correct capacity of 193). The total number of Atomic Functions in use at the time of the Incident was 153, a figure that was reached because of a November 2014 system change to allow the amalgamation of further military controller functions with the NATS system and which was put into operation on 11 December. Hence when trying to validate the request to enter Watching Mode, the primary SFS believed that it had more active Atomic Functions than the maximum capacity, a situation that should not be allowed to occur. When an error of this kind occurs SFS is programmed to shut down in order to prevent the risk of supplying corrupt data to controller workstations. When responsibility transferred to the secondary SFS the command to enter Watching Mode was replayed triggering the same error.

4.3 Against this background the Enquiry team agree with the analysis in the NATS Preliminary report, that the proximate cause of the failure on 12 December 2014 was a combination of:

- A latent defect in the SFS software that has probably been present since the software was written in the 1990s.
- A system change made in November 2014 to increase the number of available Atomic Functions.
- An incorrect (but valid from the computer system's viewpoint) action applied during the routine splitting of two air traffic control (ATC) sectors that put a workstation into a Watching Mode rather than an Elected Mode.

4.4 The latent defect was an incorrect check of the maximum number of Atomic Functions (the limit was wrong – 151 not 193), and the defect was exposed by the increase in the number of available Atomic Functions and by an increase in the number of Atomic Functions in use.

4.5 The Enquiry has already made some progress in understanding the deeper causes of the failure, and will investigate them further in order to establish the root causes. The issues that the Enquiry will investigate include key design decisions and principles:

- Why entry into Watching Mode was not generally prevented (or made less likely) even though it was agreed that the function was not to be used, and it was not infrequently triggered accidentally (see 3.8).
- Why, when the problem was detected in the software (the failed check), it was not handled where the failure occurred in the software and instead was dealt with by a general failure handling mechanism that took the conservative action of shutting down one SFS channel.
- Why the design philosophy was automatically to replay commands on SFS failure; whilst this is appropriate in some circumstances, on this occasion, repeating the command to enter Watching Mode led to the double failure of the SFS.

4.6 The Enquiry will also investigate the underlying causes of the defect and the reasons for the design choices, including considering the necessary balance between performance, availability and cost.

5. Recovery of the System Flight Server

5.1 In order to restart operations using the SFS two steps were required: restart of the SFS hardware and update of the flight data in the SFS to accurately reflect the current state of operations.

5.2 The engineering recovery was coordinated through the Engineering Technical Incident Cell (ETIC). Whilst some recovery actions are automatic, ETIC approached the necessary manual recovery actions with due care and deliberation; this is important, as the wrong decisions could have further downgraded the ATC performance.

5.3 The SFS servers restart automatically. ETIC asked for a further manual restart to increase their confidence in the state of the hardware. At the time ETIC did this, they were not fully aware of the proximate cause of the failure, hence this precautionary measure was taken.

5.4 ETIC decided that only one SFS (Server B) should be updated with flight data, as this gave more options should an error be made in the process of returning the system to service. The key decision was to update SFS with the information held in NAS. It is also possible to update NAS from the SFS; if this had been done under the prevailing circumstances, then there would have been serious degradation of ATC capability. ETIC uses a “Take Five” process where they carefully review all relevant information to reduce the chance of making and then implementing an erroneous decision. This process was used during the ETIC operation, including for confirming the decision to update SFS from NAS.

5.5 Following this process, SFS Server B was available to support ATC operations almost exactly an hour after the failure. Server A was not made available as a back-up until about five hours after the failure. This was done when ETIC believed that the risk of restoring redundancy (operating both servers) was low as the proximate cause of the failure was by then understood, and the system had been operating stably for over four hours.

5.6 ETIC was staffed by highly competent engineers, who had a very deep understanding of the systems and had a good attitude to the assessment and management of risk, e.g. as evidenced by the “Take Five” process. They also operated a consensual decision making process which helped to ensure that appropriate decisions were made. Whilst it would, in principle, have been possible to restart the systems sooner, a prudent approach was taken balancing expediency with control over risk.

6. The Operational Recovery

6.1 A set of operating procedures, with safety as their absolute priority, has been devised and approved by NATS to cover foreseeable events that disrupt normal operations. These procedures are included in the initial and continuation training of operational staff and are documented in loose-leaf binders, titled Fallback Check Lists that are available in the Operations Room at each workstation. Section 4 of the Check List addresses “Loss of System Flight Server” and requires the Controller to “take all action to reduce traffic and workload”, thereby allowing the Operations Room staff to focus on those aircraft already in flight that cannot be re-routed to avoid LAC. Accordingly, a number of measures were taken to restrict the flow of traffic:

(1) At 1455, and as a short term measure until formal traffic Regulations were in place, Prestwick Centre, London Terminal Control and London Area Control stopped departures from UK Airports.

(2) At 1500 a Zero Rate Regulation was applied stopping all flights from European Civil Aviation Conference (ECAC) states that would enter the London FIR except for departures from Heathrow, Gatwick and Manchester Airports. The duration of the Regulation was initially from 1500 to 1900 (but was eased before the planned expiry time).

(3) At 1530 Zero Rate Regulations were applied stopping all departures at each of Heathrow, Gatwick and Manchester Airports (and the short term measure at (1) was lifted for other UK Airports). The duration of the Regulations was initially from 1530 to 1930 (but they were eased before the planned expiry time).

6.2 Following an SFS failure, the Controllers continue to have an up to date radar picture and a communications capability with aircraft. They do not have the electronic support tools that assist them to predict, monitor and detect conflicts between aircraft; nor is there electronic assistance in coordinating the transfer of aircraft between sectors. Instead, the Controllers work with the limited data available and rely on their own expertise to operate manual procedures to avoid conflicts between aircraft. They use telephones to coordinate the acceptance of aircraft from adjacent sectors. The Controllers working at the time of the Incident were assisted by staff returning to the Operations Room from elsewhere on the Swanwick site.

6.3 Following the engineering recovery of the first SFS and its repopulation with data from the NAS, the air traffic Regulations were gradually lifted from 1555 so as to allow progressively increasing rates of departures and arrivals. The second SFS was restored to its normal back-up state at 2006 and the final Regulation was cancelled at 2030.

7. The NATS Major Incident Investigation

7.1 The NATS Preliminary Report presents the detailed timelines of the Incident data and the recovery as set out in Sections 4, 5 and 6 above. The Enquiry has not yet verified the narrative and its detailed timing by examination of the records at Swanwick, but has no reason to doubt the accuracy of the presented information. The same report states that the failure of the System Flight Server was caused by a combination of three factors, as set out in Section 4, which can be summarised as:

(1) A latent defect in the software.

(2) An increase in the number of available Atomic Functions that was enabled by a system change made in November 2014.

(3) The incorrect "Sign Off" of a workstation that unintentionally put it into Watching Mode.

7.2 The Report also states that safety was not compromised at any time and that this was the result of the application of pre-defined fallback procedures and traffic management plans.

8. Conclusions

8.1 The Proximate Cause. The Independent Enquiry Panel agrees with the three factors identified by the NATS report as being the immediate cause of the incident. The Panel does however believe that there are other relevant factors, such as the architectural choices made during the software design and the tolerance of inadvertent "Sign Offs", which it will investigate for its final report.

8.2 Safety. The Panel will wish to confirm that the response did indeed avoid any compromises to aircraft safety and will wish to gain a better understanding of how NATS assesses safety performance.

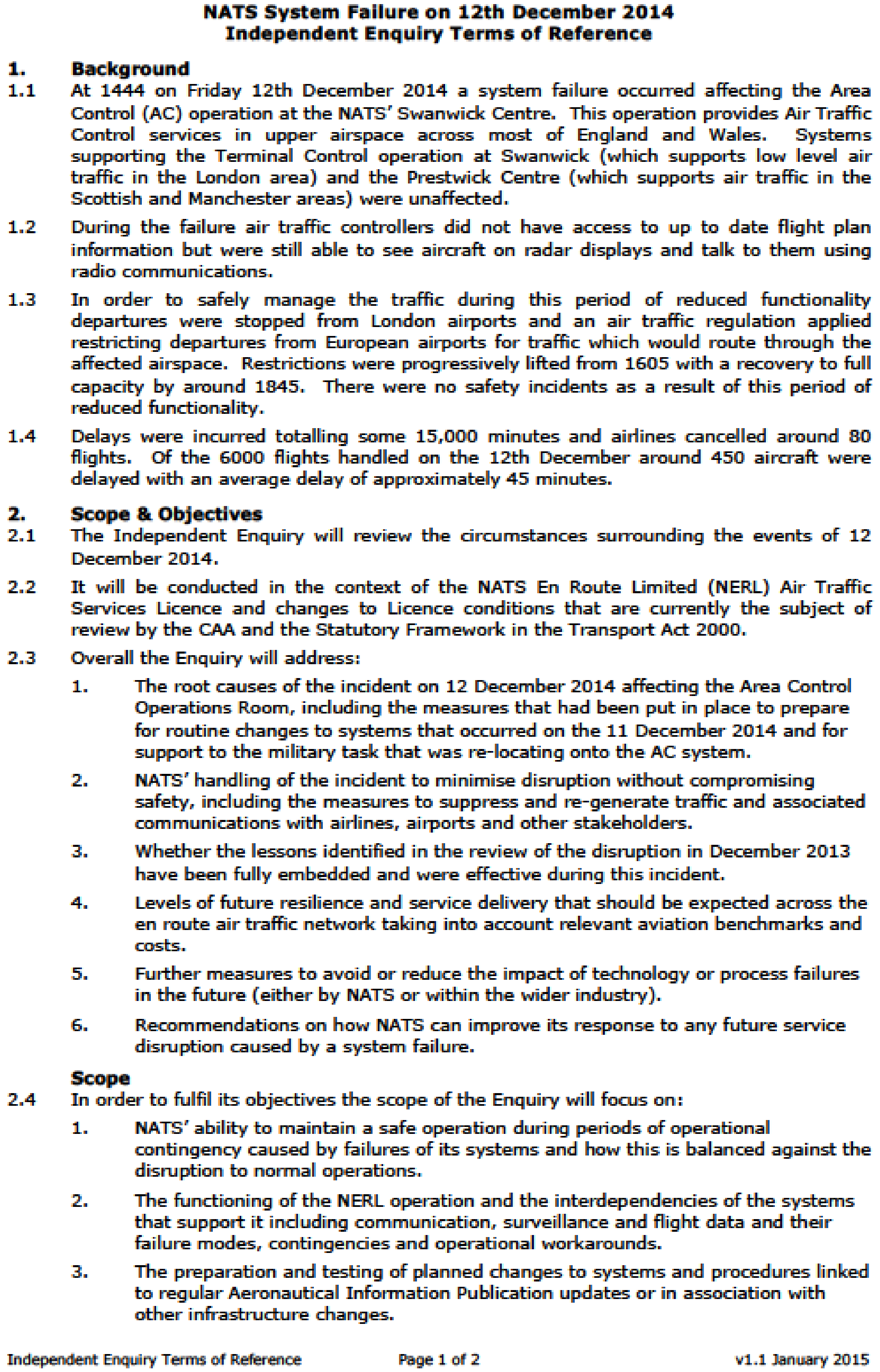
8.3 Recovery Procedures. Part of the contribution to the safe handling of the Incident arose from the application of a Zero Rate Regulation. In general the Panel strongly supports the application of agreed procedures in an emergency. It will however wish to investigate whether anything other than a Zero Rate Regulation would be an appropriate response and how best to ease the restrictions during the recovery to normal operations.

8.4 Other Lines of Enquiry. The Panel has identified other lines of enquiry, including the operational communication of the situation to stakeholders, and these are all covered by the Terms of Reference. The intention is not to fall into the trap identified by the investigation into the Columbia Space Shuttle Disaster: "When causal chains are limited to technical flaws and individual failures, the ensuing responses aimed at preventing a similar event in the future are equally limited: they aim to fix the technical problem and replace or retrain the individual responsible."

8.5 People. In the first two weeks of its 4 month long investigation, the Independent Panel has held two in-depth meetings with NATS senior staff and has visited Swanwick for a day of familiarization. Overall, the depth of knowledge of the staff and their commitment to supporting the Enquiry has been highly impressive.

Robert Walmsley
Enquiry Panel Chairman
28 January 2015

Annex A. Enquiry Terms of Reference



NATS System Failure on 12th December 2014
Independent Enquiry Terms of Reference

1. Background

1.1 At 1444 on Friday 12th December 2014 a system failure occurred affecting the Area Control (AC) operation at the NATS' Swanwick Centre. This operation provides Air Traffic Control services in upper airspace across most of England and Wales. Systems supporting the Terminal Control operation at Swanwick (which supports low level air traffic in the London area) and the Prestwick Centre (which supports air traffic in the Scottish and Manchester areas) were unaffected.

1.2 During the failure air traffic controllers did not have access to up to date flight plan information but were still able to see aircraft on radar displays and talk to them using radio communications.

1.3 In order to safely manage the traffic during this period of reduced functionality departures were stopped from London airports and an air traffic regulation applied restricting departures from European airports for traffic which would route through the affected airspace. Restrictions were progressively lifted from 1605 with a recovery to full capacity by around 1845. There were no safety incidents as a result of this period of reduced functionality.

1.4 Delays were incurred totalling some 15,000 minutes and airlines cancelled around 80 flights. Of the 6000 flights handled on the 12th December around 450 aircraft were delayed with an average delay of approximately 45 minutes.

2. Scope & Objectives

2.1 The Independent Enquiry will review the circumstances surrounding the events of 12 December 2014.

2.2 It will be conducted in the context of the NATS En Route Limited (NERL) Air Traffic Services Licence and changes to Licence conditions that are currently the subject of review by the CAA and the Statutory Framework in the Transport Act 2000.

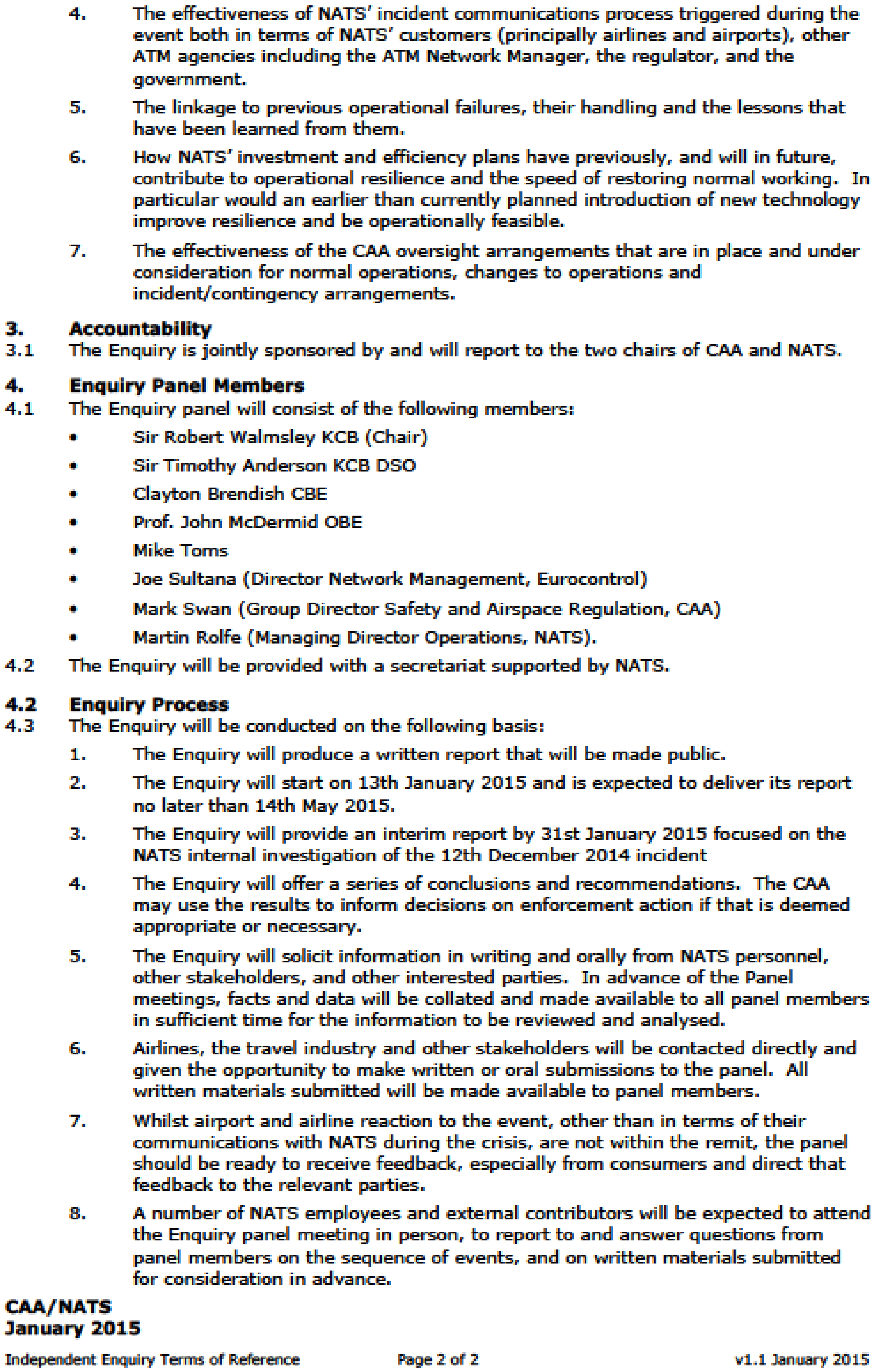
2.3 Overall the Enquiry will address:

1. The root causes of the incident on 12 December 2014 affecting the Area Control Operations Room, including the measures that had been put in place to prepare for routine changes to systems that occurred on the 11 December 2014 and for support to the military task that was re-locating onto the AC system.
2. NATS' handling of the incident to minimise disruption without compromising safety, including the measures to suppress and re-generate traffic and associated communications with airlines, airports and other stakeholders.
3. Whether the lessons identified in the review of the disruption in December 2013 have been fully embedded and were effective during this incident.
4. Levels of future resilience and service delivery that should be expected across the en route air traffic network taking into account relevant aviation benchmarks and costs.
5. Further measures to avoid or reduce the impact of technology or process failures in the future (either by NATS or within the wider industry).
6. Recommendations on how NATS can improve its response to any future service disruption caused by a system failure.

Scope

2.4 In order to fulfil its objectives the scope of the Enquiry will focus on:

1. NATS' ability to maintain a safe operation during periods of operational contingency caused by failures of its systems and how this is balanced against the disruption to normal operations.
2. The functioning of the NERL operation and the interdependencies of the systems that support it including communication, surveillance and flight data and their failure modes, contingencies and operational workarounds.
3. The preparation and testing of planned changes to systems and procedures linked to regular Aeronautical Information Publication updates or in association with other infrastructure changes.



4. The effectiveness of NATS' incident communications process triggered during the event both in terms of NATS' customers (principally airlines and airports), other ATM agencies including the ATM Network Manager, the regulator, and the government.
5. The linkage to previous operational failures, their handling and the lessons that have been learned from them.
6. How NATS' investment and efficiency plans have previously, and will in future, contribute to operational resilience and the speed of restoring normal working. In particular would an earlier than currently planned introduction of new technology improve resilience and be operationally feasible.
7. The effectiveness of the CAA oversight arrangements that are in place and under consideration for normal operations, changes to operations and incident/contingency arrangements.

3. Accountability

3.1 The Enquiry is jointly sponsored by and will report to the two chairs of CAA and NATS.

4. Enquiry Panel Members

4.1 The Enquiry panel will consist of the following members:

- Sir Robert Walmsley KCB (Chair)
- Sir Timothy Anderson KCB DSO
- Clayton Brendish CBE
- Prof. John McDermid OBE
- Mike Toms
- Joe Sultana (Director Network Management, Eurocontrol)
- Mark Swan (Group Director Safety and Airspace Regulation, CAA)
- Martin Rolfe (Managing Director Operations, NATS).

4.2 The Enquiry will be provided with a secretariat supported by NATS.

4.2 Enquiry Process

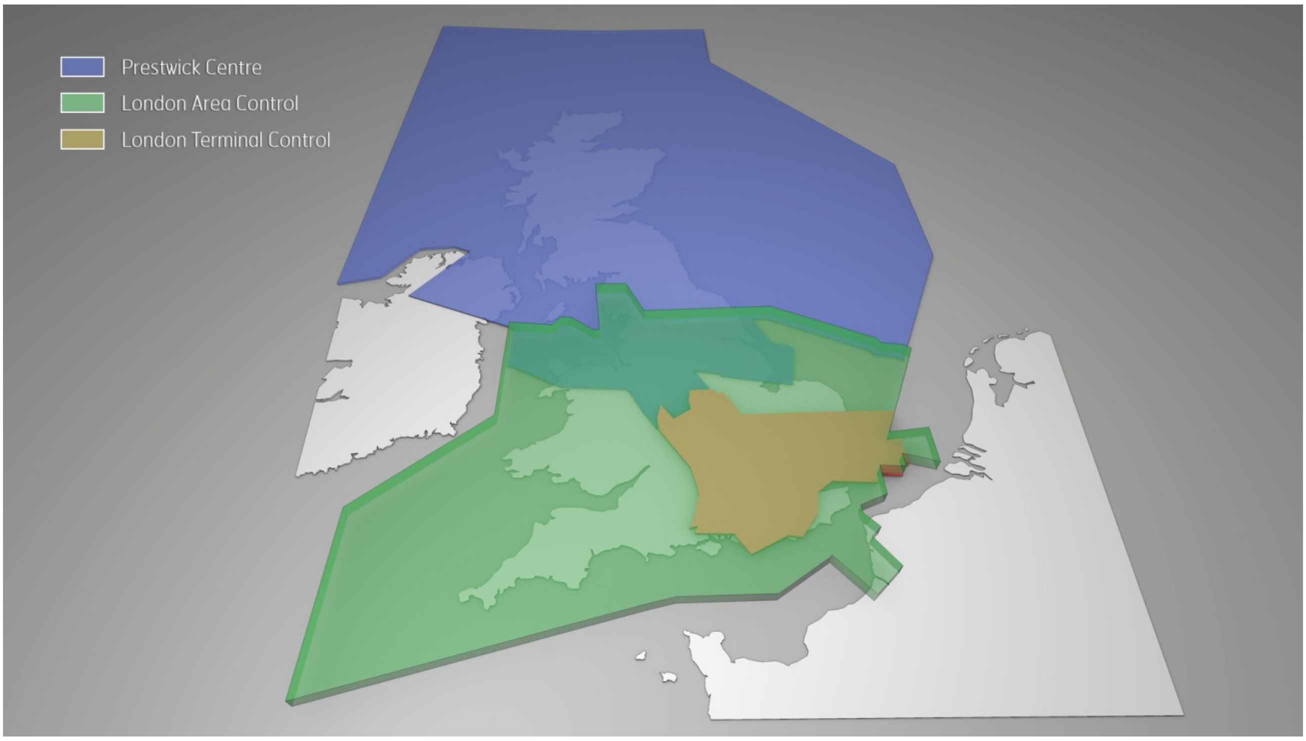
4.3 The Enquiry will be conducted on the following basis:

1. The Enquiry will produce a written report that will be made public.
2. The Enquiry will start on 13th January 2015 and is expected to deliver its report no later than 14th May 2015.
3. The Enquiry will provide an interim report by 31st January 2015 focused on the NATS internal investigation of the 12th December 2014 incident
4. The Enquiry will offer a series of conclusions and recommendations. The CAA may use the results to inform decisions on enforcement action if that is deemed appropriate or necessary.
5. The Enquiry will solicit information in writing and orally from NATS personnel, other stakeholders, and other interested parties. In advance of the Panel meetings, facts and data will be collated and made available to all panel members in sufficient time for the information to be reviewed and analysed.
6. Airlines, the travel industry and other stakeholders will be contacted directly and given the opportunity to make written or oral submissions to the panel. All written materials submitted will be made available to panel members.
7. Whilst airport and airline reaction to the event, other than in terms of their communications with NATS during the crisis, are not within the remit, the panel should be ready to receive feedback, especially from consumers and direct that feedback to the relevant parties.
8. A number of NATS employees and external contributors will be expected to attend the Enquiry panel meeting in person, to report to and answer questions from panel members on the sequence of events, and on written materials submitted for consideration in advance.

CAA/NATS
January 2015

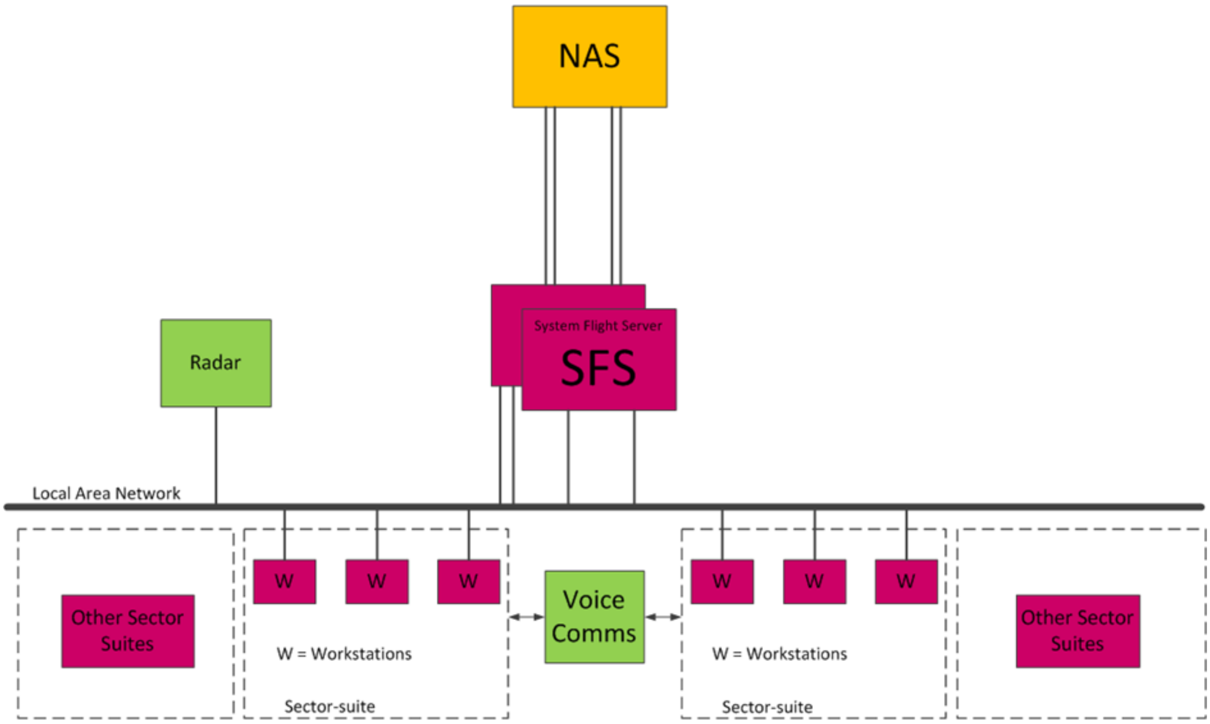
Annex B. UK Airspace

B.1 The chart below shows UK Airspace, specifically identifying that part which is controlled from the London Area Control operations room at the Swanwick Centre.



Annex C. UK Flight Data Flows

C.1 The chart below provides a simplified representation of the key data flows for UK Flight data in support of the London Area Control room.


NAS
Radar
System Flight Server
SFS
Local Area Network
Other Sector Suites
W
W
W
W = Workstations
Sector-suite
Voice Comms
W
W
W
W = Workstations
Sector-suite
Other Sector Suites