NATS Major Incident Investigation Final Report

Flight Plan Reception Suite Automated (FPRSA-R) Sub-system Incident 28th August 2023

Prepared by:
NATS

Table of contents

1. Introduction from the Lead Investigator 4

2. Executive Summary 6

3. Timelines 10

3.1. Brief history of the FPRSA-R system 10

3.2. Timeline – what happened on the day 11

4. Outputs and themes 20

4.1. NATS primary purpose of ensuring safety 20

4.2. Technical issue that led to the system event 21

4.2.1. Technical aspects (six attributes) 21

4.2.2. Design and implementation of the system 23

4.3. The response across the organisation to return the operation to normal 25

4.3.1. Response 25

4.3.2. Four hours flight plan data storage 26

4.3.3. Technical resolution 28

4.3.4. Flow management 30

4.3.5. Staffing 32

4.3.6. Escalations 34

4.3.7. Command-and-control 36

4.3.8. Communications 37

4.3.9. Wider observations 39

4.3.10. Actions to date, rectifications complete, and improvements underway 42

5. Recommendations 45

5.1. Recommendations 45

5.1.1. Major Findings 45

5.1.2. Minor Findings 46

5.1.3. Observations 48

5.1.4. Opportunities for Improvement 51

5.1.5. Positive Outputs 53

6. Glossary of Terms 56

Appendix A – Initiating Instruction SAF 013 – System Failure – 28th August 59

Appendix B – Preliminary Report 61

1. Introduction 63

2. Scope of this report 64

3. Overview of NATS' Air Traffic Control System 65

a. Overview of Air Traffic Control System 65

b. Overview of Flight Plan Processing 66

4. Description of the issue 68

a. Sequence of events leading to the failure 68

5. Technical Recovery 71

a. Actions taken to diagnose and mitigate the failure 71

b. Response by Technical Services team 71

6. Operational Recovery 73

a. Air Traffic Control Team Actions 73

b. Application of Business Resilience Processes 73

7. Impact on the NATS Operation 75

a. Safety impact 75

b. Service Delivery impact 75

8. Steps Taken to Prevent Recurrence 77

a. Actions taken or underway to prevent the interruption recurring 77

9. Areas for Further Investigation 78

10. Appendices 79

1. Introduction from the Lead Investigator

This is the Final Report of the Major Incident Investigation into the events of the 28th August 2023, a bank holiday Monday. This investigation was initiated by the NATS Chief Executive Officer (CEO) Martin Rolfe and has been managed in accordance with the NATS SAF 013 process. This Final Report follows on from the Preliminary Report into this incident, which was published on 4th September 2023, and includes commentary and feedback addressing points of clarification raised to date by the CAA Independent Panel appointed to review the 28th August events.

The scope of this investigation is as per the Initiating Instruction issued by the NATS CEO on 31st August 2023, available at Appendix A to this report. Further detail was added to the scope from Section 9 of the Preliminary Report. The full Preliminary Report is available at Appendix B to this report.

This report is being issued to the NATS CEO and Safety Director in accordance with the initiating instruction. Further dissemination is at the discretion of the NATS CEO.

The events of the 28th August demonstrate the complexity of the air traffic management network which, as a rule, operates safely and efficiently throughout the year. Technical and operational issues are overcome on a daily basis without impacting the network. It is a tribute to the network's highly skilled staff that their work goes unnoticed by the travelling public – because that means the system is working smoothly.

Yet unforeseen circumstances of a highly technical nature inevitably occur, requiring a reduction of flight capacity for the skies to remain safe. As set out in the Transport Act 2000, safety is the primary objective of NATS under its Licence from the Government and as regulated by the Civil Aviation Authority. NATS complied with that requirement on 28th August, because there were no safety incidents.

NATS has been set up to take a demonstrably safe approach when difficult problems emerge. The reduction in capacity on 28th August is, however, a stark reminder of the importance of underlying air traffic infrastructure to the operations of wider stakeholders such as airlines and airports. When unexpected incidents affect that infrastructure, as on the 28th August, these aviation stakeholders are presented with difficult decisions about how best to protect their respective operations and meet the needs of their own customers – the travelling public. Equally, effective communication between stakeholders during such incidents is critical to continue delivering a safe and effective operation.

Unfortunately, even a small reduction in flight capacity can lead to a disproportionate increase in delays across aviation. NATS is constantly developing its systems and processes so that UK skies remain accessible without ever compromising safety. However, on the 28th August, the delays adversely impacted many of the stakeholders and customers described above.

This report seeks to provide recommendations that will mitigate or avoid similar disruption during future events. It provides a brief history of the relevant technology NATS employs and outlines the events of 28th August. The report then turns to a range of themes to identify shortcomings, successes and lessons to be learned. The themes range from data storage times to safety, customer communications to system supplier support.

Our executive summary includes an easy-to-read table of both the major findings and the positive outcomes from the day. These are supplemented further in the main body of the report with minor findings, observations and opportunities for improvement. Finally, we outline the fixes and improvements NATS has already made since the incident, as well as a summary of our recommendations for the future. Though some are repeated, the inclusion of all these elements is consistent with our primary focus upon safety, ensuring maximum clarity, transparency and learning for stakeholders.

We have also provided a comprehensive glossary of terms and acronyms at the end of this report.

The investigation has been run on the principles of a just culture, which encourages transparent investigation of incidents and thereby underpins the safety of the global aviation system. This is central to NATS' values. We were clear to all interviewees that this investigation focused on the incident, not on them as individuals. I want to thank all those interviewed for their openness and the level of detail they provided.

My thanks also to the diligent investigation team. Their work has not only led to findings directly related to this event, but additional observations that will improve NATS' resilience in the months and years ahead.

Guy Allison
Lead Investigator

2. Executive Summary

1. Safety is the primary objective of NATS as set out in its Licence from the Government and as regulated by the Civil Aviation Authority. However, even a small reduction in flight capacity to meet that primary duty can lead to a disproportionate increase in delays across the aviation sector. (Section 1)
2. The current system overseeing the automatic translation of flight plan messages became operational in 2018. This is known as FPRSA-R and is based at NATS' air traffic control centre in Swanwick, Hampshire. Until the incident of 28th August 2023, there were no delays caused by the use of this system in the operation. (Section 3.1)
3. On 28th August, FPRSA-R received a flight plan for a transatlantic flight. The set of data in the flight plan meant that there was a grouping of six distinct attributes which, taken in combination, created a unique exception that the system was unable to process. If any one of these attributes had not been present, the flight plan would have been processed normally. In the circumstance that occurred on the 28th August, the system acted as it should where it encounters such an exception, shutting down to make sure inaccurate information was not sent to an air traffic controller. From 08:32 automatic processing of flight plans ceased and manual input of flight plans became necessary to maintain safety. Manual data input can only achieve a significantly reduced rate compared to automatic processing, which ultimately led to traffic restrictions being required within UK airspace. The automated system was fully restored at 14:32. Between 15:24 and 18:03, air traffic regulations were gradually reduced and then removed. However, as explained in detail below, the wider impact of the incident lasted much longer for airline customers and their passengers. This was accentuated by the high demand in the aviation system surrounding the bank holiday. (Sections 3.2 and 4.2)
4. During the response on the 28th August, existing procedures were followed by NATS personnel. However, the investigation has identified areas where responses to future issues may be improved by having a wider range of alternative procedures available to staff. These areas are detailed within this report, along with relevant findings, all of which accept that technical and operational issues will inevitably occur in the future. Recommendations focus upon improving resilience through effective procedures that apply to a wider range of possible events, rather than purely focusing on further specific procedures that would only resolve a repeat of the 28th August event. (Sections 4.3 and 5)
5. Below is a table of major findings and positive outcomes from the day, with recommendations to improve NATS' systems and processes to increase resilience further. Further findings, observations and recommendations are available in sections 4 and 5.

Major Findings		**Recommendations**
Ma1	The circumstances under which this incident could occur and lead to the software exception noted are extremely rare, with a flight plan needing to include a combination of, as a minimum, six specific attributes. (Section 4.2.1)	A technical fix to prevent the occurrence of this software exception was implemented on the night of the 18th–19th September, within 21 days of this event.

Ma2	Requirements for the design of the system included NATS' understanding of a logical approach to processing flight plans. One specific part of that logic would have dealt with the issue that presented itself on the 28th August but inadvertently was not incorporated into the FPRSA-R software code by the manufacturer. The unique combination of flight plan attributes that led to this event would be extremely difficult to predict, however, and was therefore not part of the formal test programme. (Section 4.2.2)	No recommendation, beyond the need for ongoing, effective application of NATS' existing comprehensive design requirement development methodology which follows industry best practice. It is not possible to foresee and test for every possible scenario that may transpire due to complex interactions of multiple attributes. NATS has teams and procedures in place to mitigate against unexpected events.
Ma3	NATS operates a joint decision-making model through the pre-invocation, escalation and invocation phases. In this circumstance, a blend of joint decision making with a single individual providing overall incident oversight could have led to a quicker critical escalation path. (Section 4.3.2)	NATS should review the current command structure, its supporting technology and processes. This should analyse whether the current model is likely to lead to the best outcomes in the majority of incidents, or whether it can be optimised further with the addition of alternative options. The review should include, as a minimum: - Options for alternative models and examples of other effective command structures, including the use of a single incident manager model. Such options should include guidance about when the use of each option is most appropriate. - Training requirements to maximise operational oversight capabilities during incidents. - System and process requirements to support selected structures, including decision-making, escalation and creation of a common operating picture.
Ma4	A subset of unprocessed data remained in the system but was outside the established pause queue. This required further escalation to identify the root cause of the issue. (Section 4.3.3	The AMS-UK and Data Services documentation set should be reviewed to ensure that the system complexity and behaviour can be better understood by engineers and users who are not dedicated to the system. The AMS-UK operator training material and associated competency assessments should be reviewed to ensure the lessons learnt from this event are appropriately captured. There should be a high-level joint Technical Services and Operations review of key critical systems. Initially, this review should confirm that the operational documentation for each system reviewed has sufficient description and clarity to allow the system to be

		operated safely and resiliently in unexpected circumstances. Where this is not evident, a more detailed review of operational documentation and procedures should be conducted.
Ma5	In this circumstance, while escalation procedures were followed, earlier contact with the supplier would most likely have expedited resolution of the event. (Section 4.3.6.2)	NATS should update the escalation process to provide guidance on time or other key criteria that should trigger when and under what circumstances supplier support is requested. The process must consider, alongside the benefits of involving the supplier, the risk of distraction from the ongoing engineering rectification processes when briefing the supplier. NATS should create a single controlled document detailing the supplier contracts and associated contacts, who provide 24-hour support. These details should be accessible by anyone in NATS likely to be required to support an incident response. As a minimum, these should include Levels 1 through 3 of engineering support.

Positive Outcomes		**Additional notes**
PO1	Actions taken by NATS on the day to mitigate the system issue ensured that the safety of the operation was protected. (Section 4.1)	Any change from prioritisation of safety is not recommended but would in any case require associated amendments to existing statute and regulation. This would require governmental direction and stakeholder support.
PO2	The system project designed and tested an expansive and robust set of scenarios, which provided assurance that the system was highly resilient. (Section 4.2.2)	Unique combinations of attributes will challenge even the most demonstrably resilient and well-tested system. The software code has now been updated to prevent the unique combination of six attributes causing a software exception.
PO3	On-watch and on-call teams reacted professionally to the event as it evolved. They demonstrated a personal pride in rectifying issues to maintain the service. Individuals made themselves available beyond contractual requirements. Staff were appropriately trained, qualified and rostered. (Section 4.3.1)	This demonstrates the importance of employee goodwill and of maintaining effective workforce training, professional capabilities and staffing levels.

PO4	UK airspace remained accessible throughout the day, albeit at reduced capacity, with NATS continuing to offer a safe air traffic service to inbound, outbound and transiting aircraft. (Section 4.3.4)	Although approximately 75% of planned flights operated, the cancelled or delayed flights created a backlog of passengers awaiting replacement flights that lasted the rest of the week.
PO5	Throughout the period when regulations were in place, the operational teams effectively managed the application of regulations to ensure safety. They proactively worked with customers to exempt aircraft from regulations where possible, thereby allowing more aircraft to fly. (Section 4.3.4)	While largely unseen by customers, the effective and proactive management of regulations was key to maintaining safety while enabling as many aircraft as possible to operate during the incident.
PO6	NATS staff followed escalation procedures, across Technical Services, ATC Operations and the command-and-control structure. (Section 4.3.6.1)	The adherence to existing procedure is commended. Recommendations are included alongside wider findings within this report relating to where these procedures could be further improved.
PO7	The participation of the Flow Management Position (FMP) in Air Traffic Incident Communication and Coordination Cell (ATICCC) was beneficial. (Section 4.3.8)	It is recommended to explore the addition of FMP as a permanent position in Silver and ATICCC.

3. Timelines

3.1. Brief history of the FPRSA-R system

Air traffic control is the provision and operation of a safe system for controlling and monitoring aircraft.

As set out in more detail in the Preliminary Report, since the late 1990s NATS has operated an FPRS system. Initially, this was predominantly a manual process.

In 2004, the functions became largely automated and the system became known as FPRSA. This system provided automatic translation of some of the contents of a flight plan message, with the balance of data completed manually.

In December 2016, it was agreed that a replacement FPRSA was required. A supplier, Comsoft, was chosen in July 2017, following a competitive tender process. (For information, Comsoft was acquired by Frequentis in 2016).

NATS and Comsoft worked collaboratively to achieve Design Acceptance by May 2018. A comprehensive test campaign was completed in August 2018. What is known as FPRSA-R came into use on 19th September 2018.

The FPRSA-R sub-system has operated continuously since September 2018 and has processed over 15 million flight plans since then. There were no delays as a consequence of using the FPRSA-R system until 28th August 2023.

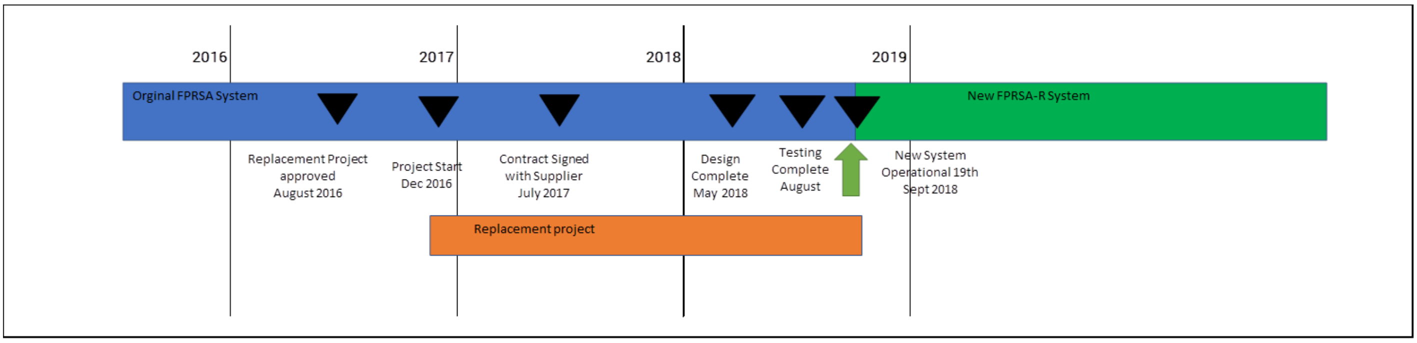


Figure 1 – FPRSA-R project timeline

3.2. Timeline – what happened on the day

Pre-incident

The 28th of August was the summer bank holiday Monday in England and Wales, one of the busiest days of the year for the UK aviation system. The operation was fully staffed to levels established by NATS' operational protocols.

The overall NATS Air Traffic Control System (ATC) was operating normally. All critical systems were operational and, as is normal for a bank holiday, no system upgrades were being implemented. All backup systems were operating as designed. All systems were being monitored by the NATS Technical Services teams in the usual manner. Everything was working in full accordance with NATS processes. Given the nature of the incident, NATS could not have reasonably forecast the subsequent software exception ahead of the incident and there were no indications that this might occur.

All but a very few flights around the world have to submit flight plan data to the relevant authorities for each journey. UK air traffic control operations typically receive flight plan data via EUROCONTROL. EUROCONTROL is a pan-European, civil-military organisation dedicated to supporting European aviation. It is the authority for the air traffic network across the continent.

EUROCONTROL sends flight plan data from its Integrated Flight Planning System (IFPS) in a format known as ATS Data Exchange Presentation (ADEXP). NATS' FPRSA-R sub-system exists to convert data from ADEXP into a format that is compatible with the UK National Airspace System (NAS). This is required because the standardised ADEXP format came into effect long after the implementation of NAS by NATS. NAS is the flight data processing system that contains all the relevant airspace and routes for most of the UK's airspace (with the exception of the upper airspace in Scotland) and was based on a similar system in use by the US Federal Aviation Administration. As can be seen below, flight plan data flows from IFPS, through a system called Aeronautical Messaging Switch (UK), (AMS-UK), onwards through FPRSA-R and into NAS. It is then sent to air traffic controllers and other systems at the Prestwick and Swanwick ATC centres.

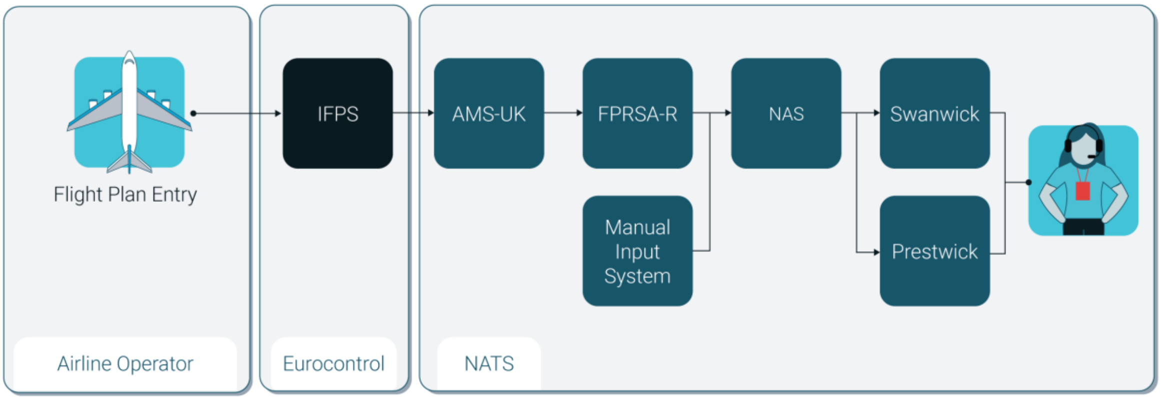


Figure 2 - flight plan data information flow

08:32 Incident occurs

At 08:32 (local time) a flight plan was received by NATS' FPRSA-R sub-system from EUROCONTROL's IFPS system.

The ADEXP route data message from EUROCONTROL was sent to FPRSA-R in a valid format. However, as set out in more detail in the Preliminary Report, the data had been constructed in such a way that it presented a unique combination of six specific attributes relating to two identical waypoint names. This unique combination and the logic applied by the system meant the FPRSA-R software constructed a route for the UK section of the planned flight that, when presented for further processing by the FPRSA-R software, could not be processed and raised a critical software exception.

When FPRSA-R raised a critical software exception it acted according to its programming and went into maintenance mode to prevent sending potentially inaccurate information to an air traffic controller. FPRSA-R also filed a simple log entry noting that it had to go into maintenance mode. It should be noted that the log entry does not describe the precise nature of an issue. Instead, it produces an array of data from which it can be ascertained that there is a problem and the time when the problem occurred. The system could not therefore identify that this issue arose from a specific flight plan such that the flight plan could be removed from the processing queue and submitted for manual handling. Similarly, the system cannot include logic that would delete or ignore complex problematic data because, for safety reasons, all flight plan data must be processed and understood to ensure that controllers have accurate real time information on aircraft they are tasked to control at their workstations.

The primary FPRSA-R system was therefore no longer available. As is common in complex real-time systems, there is a backup system whose software is located on separate hardware with separate power and data feeds. The backup exists in case of chronic failure of the primary system. Both primary and backup systems are monitored by dedicated Control and Monitoring (C&M) systems and also an aggregated central C&M system.

In the event of a failure of a primary system the backup system is designed to take over processing seamlessly.

In this instance, the primary system had not failed, but had acted as programmed. It placed itself into maintenance mode to make sure irreconcilable - and therefore, potentially unsafe - information was not sent to an air traffic controller.

The backup system applied the same logic to the flight plan with the same result. It subsequently raised its own critical exception, writing a log file into the system log, and placed itself into maintenance mode.

At this point, both the primary and backup FPRSA-R sub-systems were in maintenance mode to protect the safety of the ATC operation. Flight plans could no longer be automatically processed, and manual intervention was now required.

The entire process described above, from the point of receipt of the original flight plan message to both the primary and backup sub-systems moving into maintenance mode, took less than 20 seconds.

Further resilience is provided by NAS always storing four hours of previously filed flight data. This allows the operation to continue in the event of the loss of automatic processing of flight data. Therefore, when automatic processing stopped, NAS held the next four hours of flight plan data, which included thousands of flights and accounts for a considerable proportion of NAS storage capacity. However, as soon as automatic processing stops, the quality and accuracy of the data held within NAS inevitably begins to deteriorate. This is because flight plan data is dynamic. It changes as the planned and actual flight profiles of individual aircraft change so that customers have flexibility within the air traffic management system. These changes can happen while in the air, still on the ground at departure airports, or both. The importance of accurate flight plan data for air traffic controllers to safely deliver the service is the primary reason that ATC systems default to a safe mode in circumstances such as those that occurred on 28th August.

Therefore, in addition to the technical resilience provided by backup systems, and the four hours of stored flight data, there is operational contingency available to allow safe service to continue. This is provided through the ability to input flight data manually, directly into NAS using a manual input system. However, peak levels of automated flight processing exceed 800 flight plans per hour. Manual flight processing at that speed is impractical due to the large number of trained staff that would be required on standby at all times to match the speed and accuracy of automatic processing in the rare event of a failure. Switching to manual processing will therefore necessarily reduce the capacity of the network until automatic processing can be restored.

08:32 marks the point at which the automatic processing of flight plans ceased, and manual flight plan input commenced in order to service as much of the day's demand as possible. Additionally, in the immediate term, a large number of flights were already airborne. These would require manual data input for any associated flight plan changes to enable NATS to provide them with an air traffic control service.

HOUR ONE: 08:32 to 09:32 Initial engineering interventions and incident escalation

NATS' air traffic control centres are located in Swanwick in Hampshire and Prestwick in Ayrshire. FPRSA-R is based in the former.

The flight plan staff and the team of Swanwick Service Management Command Centre (SMCC) engineers immediately received alerts that FPRSA-R had ceased automatic processing. This engineering team forms the 1st level of a 4-level engineering support structure. The Level 1 engineering team have a broad competency to address engineering issues across the full range of NATS' circa 270 systems. They have trained competency to apply processes to known or predictable technical issues as well as processes to investigate and resolve unknown and unpredictable events. The Level 1 engineering team began to gather system data to attempt a restart using standard procedures and checklists of the General Control and Monitoring System (GCAMS).

The Level 1 engineering team analysed the data quickly. They then followed procedure, carrying out system checks and tests before attempting to reboot FPRSA-R's software at 08:59.

As is standard, the roster included on-call Flight Data Processing (FDP) Level 2 engineering support. Level 2 engineers have more detailed expertise on a narrower range of systems than Level 1 engineers, and gain and retain that expertise by working on those systems during normal office hours. Outside of those hours they are available remotely, including the 28th August bank holiday. The FDP Level 2 role therefore has greater expertise for this particular system than the onsite team. At 09:06 the team called this engineer, who provided 'remote hands' support to the onsite SMCC engineers.

At 09:23, the Duty Engineering Service Manager (DSM), who is the most senior member of the engineering team onsite, notified the Swanwick Area Control Operations Supervisor (AC OS) of the FPRSA-R situation. There are three of these operations supervisors across NATS ATC Centres, and they are the most senior on-watch air traffic controllers. The OSs were informed about the ongoing technical issue to start preparations for the possible operational impact if a resolution could not be found in a timely manner.

At 09:28, the DSM sent an SMS message to the collective major incident managers group. The purpose of the message is to pre-warn relevant internal stakeholders in the command-and-control structure about the potential requirement for the escalation of a major incident.

HOUR TWO: 09:32 to 10:32 NATS Executive notified and air traffic regulations agreed by the ATC operation

The SMCC's on-site Level 1 engineering team continued to work on identifying and resolving the issue through the expert support provided by the FDP Level 2 engineer.

Between 09:35 and 09:50 the three relevant members of NATS' executive team were contacted. They were the Technical Services Director, Operations Director and Chief Executive Officer. Their role at this stage of an incident of this kind is to assess the need for a strategic response, including when to invoke the Gold part of the command structure. From this point onwards, they were in constant contact with key internal and external stakeholders.

At 10:00 in the Swanwick operations room, a meeting took place between the DSM, the Airspace Capacity Manager (ACM) and the ATC Operations Supervisors, with the Prestwick OS joining remotely. Alongside the ACM, the Operations Supervisors decided the nature of the traffic regulations that would need to be placed on the network to protect the safety of the operation if a resolution was not achieved within a suitable timeframe.

Regulations restrict the number of aircraft entering designated areas of airspace to ensure safety. Regulations that are applied by NATS to areas of UK airspace only apply to aircraft departing from airports within the European Civil Aviation Conference region (ECAC). The ECAC region consists of 44 member states, including those in the EU, Scandinavia and neighbouring regions. When regulations are applied, therefore, aircraft originating from outside this region and due to transit UK airspace may still depart without restrictions. Furthermore, aircraft already in flight cannot be regulated and therefore must still be handled safely by air traffic control.

In the early stages of the incident, ATC had reliable system data on flights that were already airborne and in contact with controllers. However, the ATC teams recognised that as the event continued, the reliability of this data would degrade. It was decided that there would be a stepped approach to entering regulations, limiting the initial impact on customers. Therefore, restrictions were gradually increased as the data for new flights decreased in both quantity and accuracy as time went on. This meant a relatively gradual move to UK-wide regulations, which would eventually need to be applied to the whole of the UK and Scottish flight information regions. *Please note that the UK flight information region does not include Scottish airspace, which is why the two regions are identified separately.*

It was agreed that the initial regulation would be set at 300 flights per hour for Swanwick traffic and 60 flights per hour for Prestwick, levels that would restrict capacity to approximately 75% of the expected demand. These traffic counts were based on the rate at which flight plan data could be manually input to NAS. In the expert judgment of the ATC and FMP teams, only UK-wide rates provided the necessary assurance that ATC workload would remain safely aligned with data input rates. These teams had considered applying a number of individual local regulations that would have provided a similar number of network-wide flights. Local regulations are applied to smaller, more localised sectors of airspace than UK-wide regulations. Due to the number of local regulations that would be required, they judged that such regulations would be extremely difficult to put into effect and monitor.

At 10:12, it was clear that initial steps for resolving the technical issue had been exhausted. The FDP Level 2 engineer and DSM agreed the former should come onsite to undertake a full system restart including powering off the associated hardware. This is a task that requires the competencies held by the FDP Level 2 engineer and is therefore not permitted to be carried out independently by Level 1 engineers on site.

In the meantime, the SMCC's on-site Level 1 team continued to investigate and attempt to resolve the issue.

HOUR THREE: 10:32 to 11:32 Regulations come into effect and business continuity processes are stood up

During incident response, NATS runs a Bronze, Silver and Gold command-and-control structure, which mirrors emergency services and many large corporates. Bronze is typically comprised of those closest to the situation, considering the operational response including technical rectifications. Silver is stood up when tactical management of the incident is required. Gold fulfils a strategic function, includes members of the executive committee and is therefore only stood up when the situation develops to the point where strategic direction is likely to be required A diagram explaining how the command-and-control structure operates is included at the end of this section.

Gold, Silver and Bronze activities take place in parallel to the investigation and resolution workstreams conducted by engineering and operational staff.

This structure is supplemented by NATS' Air Traffic Incident Communication and Coordination Cell (ATICCC), which is activated by NATS during times of significant and/or widespread aviation disruption.

ATICCC is a communications facility, which uses scheduled teleconferences, email, text messaging and the NATS customer website to communicate. It is intended to provide an overview of the operational impact of an aviation incident on the overall network and the measures being taken to mitigate and recover. Stakeholders include airlines, business aviation, airports (both ATC and operators), the Department for Transport, the CAA and the EUROCONTROL Network Manager.

At 10:38, the Bronze meeting was convened. *Please note that terminology relating to the enactment of the command-and-control structure is included at the end of this section.*

At 10:43, EUROCONTROL was advised that regulations would be required for UK airspace.

At 10:45, EUROCONTROL's Network Manager notified airline and airport customers of the first of the air traffic flow regulations coming into effect at 11:00. This makes sure everyone has the same information, as per established and agreed processes.

At 10:58, the Bronze team discussed the likelihood of requiring FPRSA-R additional subject matter expertise from NATS' Level 3 engineering support team, because of the difficulty in finding a resolution. The Level 3 is NATS' Subject Matter Expert (SME) engineer with respect to a specific system, such as FPRSA-R.

At 11:00, UK-wide regulations became active.

The Duty Press Officer (DPO) became aware of the FPRSA-R problem at 11:02 through a phone call from the Silver team. The DPO then informed the wider NATS corporate communications team.

At 11:06, the Silver team was convened to co-ordinate tactical decisions regarding the incident.

At 11:30, ATICCC was activated, so that the team could arrange the open call with customers.

HOUR FOUR: 11:32 to 12:32 FDP Level 2 engineering support arrives on site, regulations tighten, business continuity activated

The Level 2 engineer was driving to the site. The Bronze team concluded that the benefit of this engineer being on-site would be to perform a full system restart that required the competencies held by the Level 2 engineer. The Level 2 engineer arrived on site at 11:47. His journey to the office took longer than normally expected due to traffic congestion.

At 11:47, the first customer ATICCC call started.

Given the complexity of the support required, the Level 3 SME engineer was contacted at 11:53.

For the next 35 minutes, several unsuccessful attempts were made to perform a full system restart of the FRPSA-R servers, including powering off the associated hardware. This was led by the Level 2 engineer who was now on site. For clarity, the earlier reboots were of the software, so this full system restart was a different action and the next defined logical step in attempting to resolve the issue.

At 12:20, Gold team was activated. Prior to this, individual members of the executive team held discussions with various teams to consider safety and operational resilience. Gold team activity included speaking to senior stakeholders, briefing the chairman of the NATS Board and assessing communications requirements.

Also at 12:20, the UK-wide regulations further reduced capacity to 40 flights per hour for Swanwick traffic and 20 flights per hour for Prestwick. These restrictions became active from 12:30. The requirement for a reduction in traffic counts was based on the ongoing assessment of the rate at which flight plan data could be manually input to NAS, alongside the necessary assurance that ATC workload would remain safely aligned with those data input rates. Manual data input requirements were increasing as the existing data storage continued to degrade, and more new flight data was being received.

At 12:26, the investigation was progressed to the next level with the Bronze team requesting additional system logs that provided greater detail, so the FPRSA-R Level 3 SME engineer could examine them.

At 12:32, the four-hour mark passed since the software exception had occurred. The four hours of stored flight plan data (which had been degrading in quality since 08:32), was exhausted and the system was fully reliant on the data that had been, and was continuing to be, manually input.

HOUR FIVE: 12:32 to 13:32 Software manufacturer is contacted and the issue is identified, while regulations tighten further.

Having examined the system logs, the Level 3 SME engineer identified the message associated with the software exception. This message was not one that had been seen before. With no resolution having been identified through NATS engineers' investigations thus far, and being unfamiliar with the message contents, the Level 3 SME engineer decided to escalate to Level 4.

Therefore, at 12:39, the Level 3 SME engineer engaged the original software manufacturer, Comsoft. A Teams call took place. The problem and the logs were examined in further detail.

The supplier was able to determine from the logs supplied by the Level 3 SME engineer that the system had suffered the software exception because of an individual – though as yet unidentified– message being received repeatedly. At this stage, the supplier did not understand why the message was causing the exception. They did, however, know how to mitigate it because they understood in greater detail the AMS-UK system functionality, and its associated inter-operability with FPRSA-R, as expected from the original designer of both systems.

At 12:51, a further call took place between the supplier, the Level 3 SME engineer and the AMS-UK operator. During this call, the supplier established how the AMS-UK system had been configured during the event. They identified there were messages ‘pending’ in the system, outside of the ‘pause’ queue that had been established, of which the investigation teams were not aware.

At 12:58, the supplier directed the AMS-UK operator to reprocess these pending messages back into a separate queue. This served to isolate the message that had caused the software exception, while allowing the remaining messages to pass into FPRSA-R without causing a software exception. At this point, the engineering teams could not ascertain why the flight plan message had caused a software exception. However, with the message isolated, actions commenced to implement a resolution.

At 13:00, air traffic regulations tightened to 20 flights per hour for Swanwick airspace and 10 per hour for Prestwick airspace, again based on ongoing assessment of manual data input rates and alignment with ATC workload capability.

At 13:26, an initial batch of test flight plans was processed by FPRSA-R. This followed the restoration of the system, which included resolving a database issue across the two servers. The database in question was only present on one of the pair of servers. If the server without the database was inadvertently started first, it could not validate start-up requirements. This was resolved by the Level 3 SME engineer.

HOUR SIX: 13:32 to 14:32 The fix is put in place and tested

Shortly after the test flight plans were processed, a series of assurance tests were carried out by NATS systems engineers to provide confidence that the issue had been fixed, data processing was accurate and the system would operate safely.

At 14:00, the fourth Bronze team call started.

At 14:27, the system began auto-processing flight plans again. This is the point at which the technical system was restored; the next stage was the restoration of operations.

14:32 onwards: Regulations are removed and the system is fully restored

At 14:32, a second Gold call took place and the team was updated on the resolution actions that had been taken. At the same time, the third ATICCC call was starting.

The fourth Bronze call ended at 14:54, at which point Bronze was deactivated.

At 15:00, ATICCC finished its third call and was deactivated because there were no further network implications. Participants were informed that there would be no further ATICCC calls.

At 15:11, the Silver team deactivated.

Between 15:24 and 18:03, all traffic regulations were gradually eased and then removed. The most restrictive UK-wide regulations were removed at 16:10 as regulations became more locally targeted to maximise capacity during recovery. All regulations were removed by 18:03. Air traffic service resumed normal operations, though the wider impact of the incident lasted much longer for some airlines and their passengers.

There was a third Gold call at 16:00.

The CEO briefed the Secretary of State for Transport.

At 19:01, a fourth Gold call took place, during which it was agreed that a Major Incident Investigation should be formally initiated the next day. The call ended at 19:19.

A further Gold call took place the next morning - 29th August - at 09:31 and lasted until 10:33. The next Gold meeting took place at 16:00. Regular Gold meetings continued until the 1st September. During the 1st September meeting, it was agreed that the Gold meetings would be paused for the foreseeable future but that the team would remain available on call. This continued until 11th September when Gold was deactivated.

NATS' Incident Response Structure

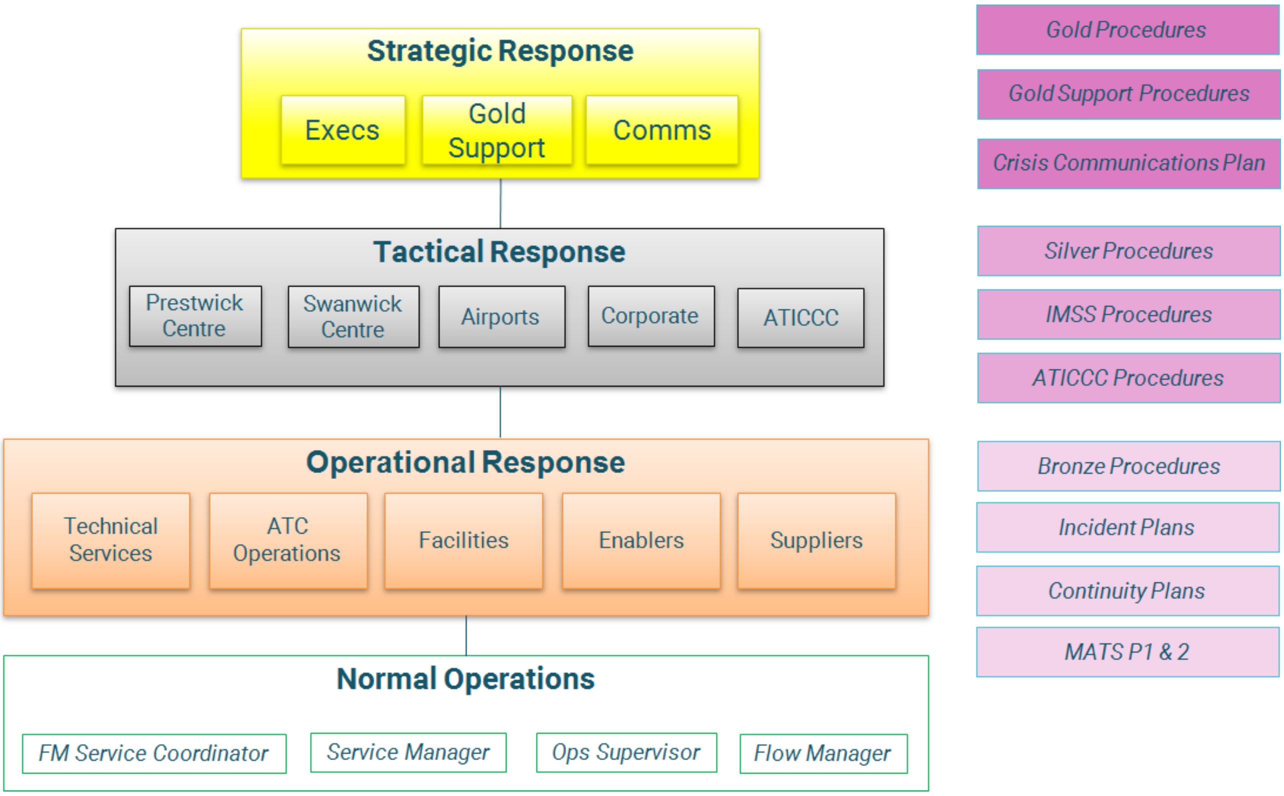


Figure 3 Incident Response command-and-control structure

NATS differentiates between the Strategic, Tactical and Operational levels involved during incident response in its Core Services Resilience Response Plan.

Strategic: The highest-level crisis management is 'Gold'. This level addresses and manages strategic issues resulting from a crisis or major disruptive event that impacts NATS' core objectives and services. Gold manages corporate/reputation management and related crisis communications.

Tactical: The 'Silver' layer focuses on coordinating the response to a disruptive event and facilitating the continuity of prioritised activities. Silver teams analyse the impact of the incident, implement the appropriate solutions from those available in the plans, ensure the continuity of prioritised activities and provide progress updates to the Gold Team. Tactical plans also cover coordination and communications across the impacted parties.

Operational: The 'Bronze' layer determines the response of the individual functional or technical areas at the core of the incident. Bronze supports the continuity of the prioritised activities, from the beginning of the incident through to the recovery of agreed levels of service and the return to business as usual.

Assess	Evaluate and consider an unfolding situation that may require the convening of incident teams to help manage what may develop into a potential incident
Convene	Inform and gather the appropriate members of the NATS incident teams to prepare for potential activation of incident response procedures
Activate	Formally invoke some or all of NATS incident procedures, including external and internal communications
Run	Follow the procedures set out in the applicable Incident Management Procedures document (GOLD, SILVER, BRONZE, ATICCC)
Deactivate/ Post Incident	Stand down incident teams and ensure that plans are in place to monitor post incident recovery progress and any on-going media interest

Figure 4 Terminology relating to Incident Response command-and-control structure

4. Outputs and themes

The outputs from this report are considered across three core themes:

- NATS' primary purpose of ensuring safety
- the technical scenario that led to the system event
- the response across the organisation to return the operation to normal

The outputs have been classified as follows:

- **Major** – The absence of this factor would have reduced the likelihood of the incident happening.
- **Minor** – The incident would have occurred anyway or had already occurred. However, this factor caused additional issues.
- **Observation** – Identification of a concern that has the potential to impact a future incident. This factor was – or may have been – present during the incident, but either had no effect or it cannot be determined.
- **Opportunity For Improvement** – A suggestion that could lead to a more efficient process or a more effective working practice.
- **Positive Output** – The presence of this factor helped to mitigate the severity of the incident.

4.1. NATS primary purpose of ensuring safety

Positive Output PO1 – Actions taken by NATS on the day to mitigate the system issue ensured that the safety of the operation was protected.

NATS is the sole provider of civilian en-route air traffic control over the UK and is regulated by the Civil Aviation Authority (CAA). NATS is licensed by the UK Government to provide core air traffic services in designated areas of the UK's airspace. Under the terms of the licence, NATS' primary responsibility is safety – specifically, to give "instructions or advice to aircraft, whether in flight or on the manoeuvring area or apron of an aerodrome, for the purpose of preventing, or assisting in the prevention of, collisions between aircraft." (NATS Licence, Part II, Condition 1.3).

This responsibility is particularly relevant when there is an issue that hampers service delivery alongside expectations that the aviation network will run at close to full capacity.

NATS' immediate actions to meet safety obligations included prioritising incoming flight-related messages to ensure the correct flight plan data was available for those aircraft closest to entering UK airspace. NATS also applied regulations. These regulations sought to protect Air Traffic Controllers (ATCOs) from potentially excessive workloads in the event of calls from aircraft for which they (the ATCOs) would have had no flight data. The likelihood of such calls increased during this incident due to the loss of automated flight plan processing, and the requirement to utilise the slower method of manual input. This increased the risk of ATCOs having to enter data for unidentified aircraft entering their sector, while also safely managing the other aircraft already under their control.

Analysis of the available radar, flight data processing, safety reports and safety nets data for the period from 08:32 until 17:00 indicated that no flight safety events occurred on the 28th August 2023 as a consequence of the FPRSA incident.

4.2. Technical issue that led to the system event

4.2.1. Technical aspects (six attributes)

System Resilience

To meet the obligation of its licence, NATS runs a range of systems that support the operation of safe Air Traffic Management (ATM). To ensure appropriate levels of safety and service, such systems must be resilient.

To achieve this requirement, specifications are developed for each system individually during the design phase. These specifications set the overall integrity and performance requirements for the systems, eliminating hazards where possible. Where elimination of hazards is not possible, either due to the complexity or predictability of system behaviour, the adoption of development standards (such as Software Standard ED-109) aims to reduce the likelihood to a level in accordance with industry standards.

NATS provides procedures, training and sufficient competent personnel to mitigate any unexpected event.

This layered approach is commonly referred to in best practice as "Hierarchy of Controls".

NATS' application of these requirements has resulted in a highly resilient network of systems, as shown in the following graph:

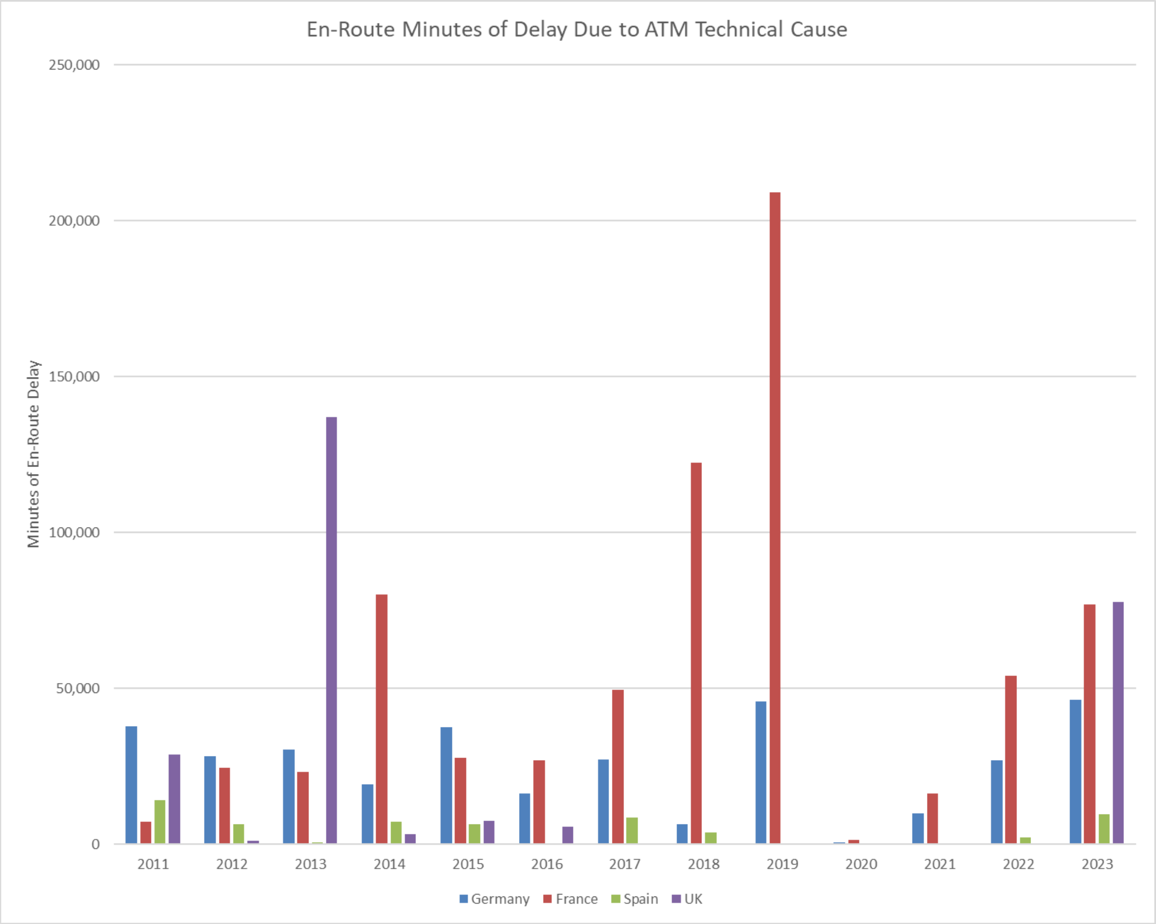


Figure 5 – EUROCONTROL data demonstrating European engineering ATM delay, 1st January 2011 to 31st October 2023

Despite this resilience, issues cannot be completely eradicated. The use of fallback procedures with appropriately trained staff is considered best practice and they are commonly integrated into various systems and processes. Many systems, especially in technology, engineering and critical infrastructure, are complex and can experience failures. Fallbacks are a pragmatic response to such complexity, offering alternative pathways to maintain operations at a safe level. Designing out every conceivable failure mode is neither realistic nor likely within financial considerations or other available resource constraints. Fallbacks allow systems to adapt to changing conditions, whether due to environmental factors, technological advancements or shifts in requirements that may not have been envisaged when first designed.

In essence, fallback procedures are standard industry practice because they align with the pragmatic recognition that uncertainties, failures and unexpected events are part of any complex system or process. They are a proactive and practical approach to handling the inherent challenges associated with operating in a dynamic and unpredictable environment.

Across NATS' operations there are approximately 270 different systems made up of around 8,000 different types of equipment. On a daily basis, NATS manages a programme of planned maintenance and resolves unexpected system challenges. The majority of these are invisible to internal users let alone the external customers. A small number of events may cause varying impacts to service, but these are a very small overall percentage.

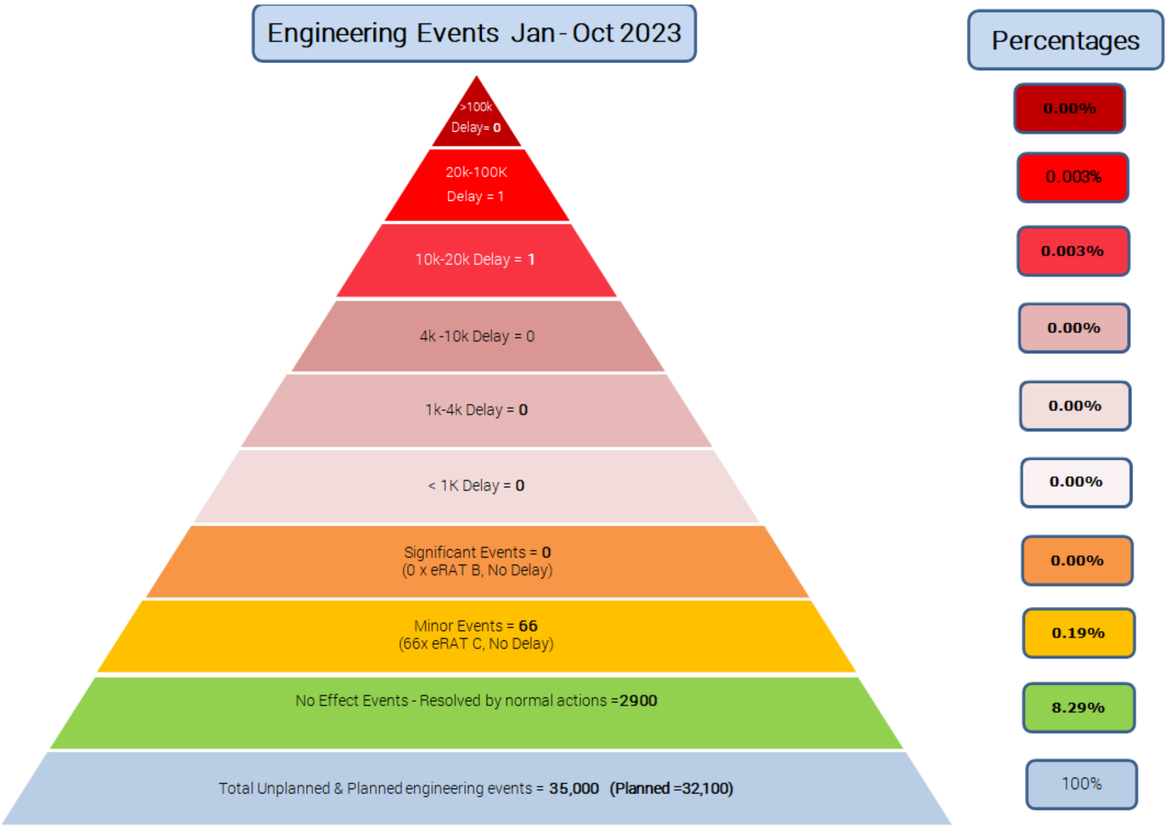


Figure 6 – NATS data demonstrating engineering events requiring fallback procedures Jan to Oct 2023

The diagram above illustrates the volume of technical events that are managed and how few of them are felt by our customers. The vast majority of events are planned (approximately 91%), with around 8.3% being classified as technical incidents. The levels increase in severity through a combination of safety levels (eRAT = engineering incident risk categories) and service impacts declared as minutes of delay.

During 2023 NATS experienced two delay events seen by the content of the upper, red bands of the pyramid in Figure 6.

The first was on the 14th June where a failure on one of our local area networks resulted in the need for manual coordination between external centres causing 12,395 mins of engineering delay. The cause for that event was identified and resolved. This was unrelated to FPRSA-R.

The second was the event on the 28th August covered by this report.

Technical causal factor

Major Ma1 – The circumstances under which this incident could occur and lead to the software exception noted are extremely rare, with a flight plan needing to include a combination of, as a minimum, six specific attributes.

These six attributes are as described within the Preliminary Report. No additional information during this investigation alters this assessment. Further details are provided in Ma2 below.

4.2.2. Design and implementation of the system

Design

Positive Output PO2 – The system project designed and tested an expansive and robust set of scenarios, which provided assurance that the system was highly resilient.

One of the key areas of concern for the initial FPRSA project set-up in 2016 was setting adequate integrity and performance requirements. This was a system replacement within a complex operational and technical architecture, and it would need to cope with a wide range of possible inputs.

The existing system had been in place since 2004 and had evolved over the years. This meant parts of the system had grown in complexity. Therefore, there was a significant number of new and complex requirements for the replacement system that were not fully developed. To manage these, the project took an agile development approach.

Agile software development is an internationally recognised approach. It is considered faster and more effective, in the right circumstances, than the traditional 'waterfall' model that depends on specifying a complete set of requirements at the beginning of a project. Agile is an iterative and incremental approach to software development that emphasises the importance of delivering a working product quickly. It involves close collaboration between the development team and the customer to ensure that the product meets their needs and expectations and allows for new requirements throughout development.

NATS worked collaboratively with the supplier Comsoft to define and refine the requirement specifications.

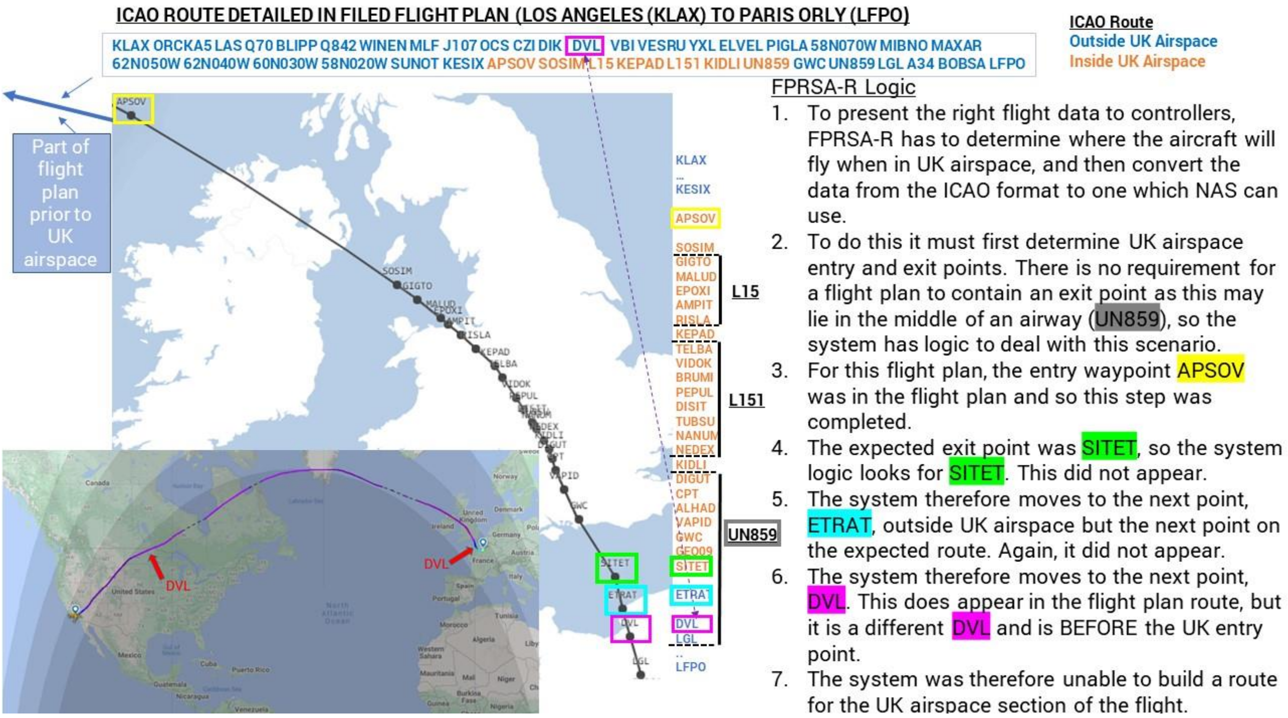
One of the key requirements was defining the Route Translation logic. This defined how the system would translate the route an aircraft intended to fly, to a format the NATS systems could understand, using the details submitted in flight plans. This was one of the most complex areas of the previous system and the associated documentation was deemed not specific enough for the requirements of the new system. Therefore, in the early part of the project an additional Route Translation guide was produced by NATS to provide more detail about how this information should be processed.

Major Ma2 – The requirements for the design of the system included NATS' understanding of a logical approach to processing flight plans. One specific part of that logic would have dealt with the issue that presented itself on the 28th August but inadvertently was not incorporated into the FPRSA-R software code by the manufacturer. The unique combination of flight plan attributes that led to this event would be extremely difficult to predict, however, and was therefore not part of the formal test programme.

The Route Translation guide for the new system contained a detailed description of how the FPRSA-R logic should perform when extracting the part of the flight plan pertaining to UK airspace. This is the logic relevant to how the system performed on the 28th August.

The formal requirement of the system was that it could calculate the NAS route for the UK element of the flight plan using the entry and exit points of UK airspace. The numerous specific steps to achieve this requirement, as described within the Route Translation guide, were not fully formalised as requirements in their own right. The manufacturer has acknowledged that the supporting design document provided by NATS was used to generate the detailed requirements and that it depicted the condition relevant to this event. However, this condition was inadvertently missed during the coding process.

Testing every single combination of specific scenarios was not feasible because of the sheer quantity of combinations. Instead, testing focused on the output of the overall process using an expansive set of scenarios, using large volumes of historic and simulated flight plan data.



ICAO ROUTE DETAILED IN FILED FLIGHT PLAN (LOS ANGELES (KLAX) TO PARIS ORLY (LFPO)

KLAX ORCKA5 LAS Q70 BLIPP Q842 WINEN MLF J107 OCS CZI DIK DVL VBI VESRU YXL ELVEL PIGLA 58N070W MIBNO MAXAR 62N050W 62N040W 60N030W 58N020W SUNOT KESIX APSOV SOSIM L15 KEPAD L151 KIDLI UN859 GWC UN859 LGL A34 BOBSA LFPO

ICAO Route
Outside UK Airspace
Inside UK Airspace

Part of flight plan prior to UK airspace

FPRSA-R Logic

1. To present the right flight data to controllers, FPRSA-R has to determine where the aircraft will fly when in UK airspace, and then convert the data from the ICAO format to one which NAS can use.
2. To do this it must first determine UK airspace entry and exit points. There is no requirement for a flight plan to contain an exit point as this may lie in the middle of an airway (UN859), so the system has logic to deal with this scenario.
3. For this flight plan, the entry waypoint APSOV was in the flight plan and so this step was completed.
4. The expected exit point was SITET, so the system logic looks for SITET. This did not appear.
5. The system therefore moves to the next point, ETRAT, outside UK airspace but the next point on the expected route. Again, it did not appear.
6. The system therefore moves to the next point, DVL. This does appear in the flight plan route, but it is a different DVL and is BEFORE the UK entry point.
7. The system was therefore unable to build a route for the UK airspace section of the flight.

Figure 7 FPRSA-R system logic to extract UK airspace details, and how it was applied on 28th August

The figure above demonstrates the unique combination of the six specific steps that caused the software exception on the 28th August. The circumstances under which this incident could occur and lead to the software exception noted are extremely rare and specific, needing to include, as a minimum, all the following:

- The intended flight route including duplicate waypoints.

- Those duplicate waypoints both being outside of UK airspace and on either side of UK airspace.
- One of the waypoints needs to be near to the UK airspace boundary exit point, in order to be eligible for potential use by FPRSA-R search logic.
- The first duplicate waypoint needs to be present in the ICAO4444 flight plan segment of the ADEXP flight plan message.
- The second duplicate waypoint (the one near the UK FIR exit point) needs to be absent from the ICAO4444 flight plan segment of the ADEXP flight plan message.
- The actual UK exit point needs to be absent from the ICAO4444 flight plan segment of the ADEXP flight plan message.

If any one of these six attributes had not been present in relation to the flight plan on the 28th August, FPRSA-R would not have raised a software exception.

Testing

Observation Ob1 – The testing of the system followed standard NATS process and was reasonable based on the premise that it is impractical to test every single scenario within complex systems.

The project (reference L5337 FPRSA Replacement) created a verification plan at the outset as per standard process. This is the top-level plan and detailed all the verification, integration and validation phases to be executed throughout the lifecycle of the project, until deployment.

Test activities all took place during the project lifecycle and passed, though took longer than expected due to a large volume of required changes being raised during the development process. This was largely because of challenges with both software and hardware stability, which led to increased testing by both Comsoft and the NATS team. Resolution involved significant work by both parties which, whilst challenging, ultimately resulted in a successful test programme.

There are no readily available metrics by which to compare either the level of test cases, or hours of testing against industry standards. The system was built from a number of pre-existing components that had their own test programmes independent of the project. This added to the complexity of the situation. The depth and coverage of testing on FPRSA-R was believed by both the supplier and independent NATS Test Manager to be comprehensive. This judgment is based on their experience and the investigation has seen no evidence to the contrary.

4.3. The response across the organisation to return the operation to normal

4.3.1. Response

Positive Output PO3 – On-watch and on-call teams reacted professionally to the event as it evolved. They demonstrated a personal pride in rectifying issues to maintain the service. Individuals made themselves available beyond contractual requirements. Staff were appropriately trained, qualified and rostered.

The investigation has found:

- Evidence of individuals arriving early for shift, staying on after shift, and attending when not rostered to do so
- Individuals accepted calls and offered assistance, during a public holiday, when not on-call and therefore under no obligation to do so
- Teams and individuals worked pro-actively to minimise the impact to customers.

4.3.2. Four hours flight plan data storage

Background

NAS (National Airspace System) is the flight data processing system used by NATS. Its purpose is to translate the flight plan data provided by FPRSA-R into information that is displayed to air traffic controllers. This information is critical for providing a safe control service to the aircraft. It includes the aircraft's planned route, its entry point into UK airspace, the aircraft type and equipment carried, and the estimated times, speeds and altitudes of the flight.

NAS ensures that the information is displayed to the right controllers, at the right time. It also provides updates, and transfers flight information onward to adjacent sector controllers and neighbouring operational units.

Observation Ob2 - There appears to be little-to-no benefit in increasing flight plan data storage to longer than four hours.

In order to provide for service resilience in the event of an interruption to the flow of flight plan data, an adequate store of projected flight plan data is necessary. NAS holds a rolling four hours of flight plan data in its memory. This means NAS holds the data for all aircraft that are planned to be in contact with NATS controllers over the following four hours.

Therefore, when there is an interruption to the supply of data – as happened on 28th August – the data stored within NAS will be fully depleted four hours after the interruption occurred, unless:

- the supply is restored within that four-hour period through restoration of the system; or
- data is input manually into NAS

Flight plan data is dynamic in nature. Therefore, NAS normally provides updates for changes it receives from FPRSA-R and that affects the flight data it has already received. These updates to flight data already stored in NAS can contain information that is critical to the safe control of the flight.

During an interruption to the supply of data, these updates also require manual input to manage the degradation of the stored data.

The figure of four hours of data reflects the effective data storage capacity of NAS. To increase this level of storage is a significant undertaking, involving the redevelopment of system architecture.

Even so, it is uncertain whether increasing capacity to allow for five, six or more hours of data storage would positively impact levels of service disruption in the event of a lengthy system outage. This is due to the degradation of data over time, as explained above, and the increased level of manual input workload required as the data continues to degrade. More data at the start of an event, simply means more degraded data further into an event. By the four-hour mark, the vast majority of flight plan data needed by controllers will either be for new flights or updates to the oldest data held in the system. In both cases, the data needs to be manually input.

Therefore, a longer data storage period would not substantially alter the point at which regulations would need to be applied, because after four hours the correlation of remaining data to actual flight operations would be minimal.

Further, regulations need to be applied significantly in advance of the expiry of the four-hour window to ensure that the flow of aircraft entering UK airspace at the expiry of the window is no greater than the rate of manual flight plan processing that is achievable. Due to many flights departing their origin several hours before reaching the boundaries of UK airspace, regulations that could apply to those flights will need to be promulgated before the four hour window expires. On the day the expert judgement of the operations team was to publish regulations just after two hours of the four-hour window had passed.

Minor Mi1 – The understanding and experience of how much operational resilience was provided by the four hours of stored flight plan data varied among teams and individuals. This, in turn, led to several different interpretations of how soon there would be an operational impact, although awareness and alignment improved as the incident progressed.

Most people understood that they wouldn't have a full 4 hours before any operational impact was felt. Some, however, thought that regulations would only be applied towards the end of that period if a resolution still hadn't been implemented. Those in the ATC operation were planning to apply regulations earlier due to the expected workload of manual input required to maintain the quality of the flight plan data. They understood that the quality of the data would begin to degrade more quickly as time passed.

Major Ma3 – NATS operates a joint decision-making model through the pre-invocation, escalation, and invocation phases. In this circumstance, a blend of joint decision making with a single individual providing overall incident oversight could have led to a quicker critical escalation path.

In incident management, the incident command can be an individual or a group responsible for all incident activities, including the development of strategies and tactics and the ordering and release of resources. The incident command has overall authority and responsibility for conducting incident operations and is responsible for management of tactical operations at the incident site.

The command-and-control responsibilities and structure should be closely aligned with the existing management and organisational structure. The result is clearly defined roles and responsibilities when responding to an incident.

NATS operates a joint decision-making (JDM) model through the pre-invocation, escalation and invocation phases. This model is common in many crisis response structures because it supports effective joint decision making by multiple responsible stakeholders through shared situational awareness and a common operating picture.

The investigation identified that there are responsible positions within the NATS command structures but there was no single role accountable for oversight of the entire incident.

To ensure effective management of an incident, an alternative model of operation identifies such a role or individual who has accountability to oversee the incident and its various stages to conclusion. This accountability remains with them alone unless they formally hand this accountability over to another individual. Such a model allows one individual to maintain an overarching view of all rectification activities. This 'helicopter view' means they are able to assess the likely impact to customers and wider factors, such as time constraints. The risk of this model however is that in complex incident response scenarios the accountable individual cannot effectively maintain situational awareness.

Alternative models include a blend of joint decision making with a single role to oversee the incident. An example of this is seen within the emergency services, which operate a joint decision-making model. The three "blue light" services will each have a Bronze Commander overseeing their respective disciplines but, dependent on the type of incident, one of the Bronze Commanders will have overall responsibility.

In this particular circumstance, there may have been opportunities to expedite elements of the escalation process had there been a single role accountable to oversee the incident on the 28th August.

4.3.3. Technical resolution

Pause queue

Observation Ob3 – The pause queue was established in accordance with procedures.

When flight plan data stopped flowing between the Aeronautical Messaging Service system (AMS-UK) and FPRSA-R, AMS-UK started queueing data and raised an alarm when this queue reached a defined level. Part of the standard procedure in reaction to this alarm is to consider creating a "Pause Queue" in the AMS-UK to temporarily hold the data. This action was undertaken.

Major Ma4 – A subset of unprocessed data remained in the system but was outside the established pause queue. This required further escalation to identify the root cause of the issue.

Under normal operations the routing function within the AMS System sends incoming messages from external parties, such as IFPS, to the intended receiver, such as FPRSA-R, in real time.

The AMS-UK System also features a sophisticated message queue handling function. After establishing the desired routing, messages that cannot be transmitted immediately (for example, in the event of an external issue) are automatically placed in a pending queue. The system also allows manual queues, such as pause queues, to be created.

In addition to the queuing of the data, the other key process is the ability to move a message back a step in the routing process through an action called 'reprocessing'. This message is then subject to whatever queues are in place.

The behaviours of pending and pause queues are different.

- The pending queue will automatically send messages to the end system when there is a valid connection available.
- Messages in the pause queue will not be sent even when there is a valid connection available, and requires messages to be reprocessed back to the main routing part of the system.

Typically, the combination of actions would be that a pause queue is set up to allow an end system to temporarily pause processing data for a maintenance reason. Once that maintenance was complete, and the end was ready for service, the messages held in the pause queue would be reprocessed into the pending message queue and the pause queue would be removed.

On the 28th August, a pause queue was established to prevent new data being sent from AMS-UK to FPRSA-R. However, the flight plan message that couldn't be processed by FPRSA-R remained in the pending queue.

Every time the connection was established between AMS-UK and FPRSA-R, the message would be automatically sent, as per the behaviours of established pending queues. This caused the same outcome of FPRSA-R entering maintenance mode.

Essentially the message was caught in a cycle that was repeated whenever the connection was re-established.

This message could only be removed from the pending queue if FPRSA-R had processed and sent an acknowledgement receipt back to AMS-UK. FPRSA-R could not do this because it moved from operational to maintenance mode. Therefore, the flight plan remained at the front of the pending queue.

The creation of the pause queue by the AMS-UK operator only acted upon new messages arriving in the system and did not change where the problematic message was located. Frequentis/Comsoft is the supplier of both the AMS-UK system and FPRSA-R. It was only the knowledge of the supplier as to how the two systems worked with each other that identified and provided a solution such that the set of messages in the pending queue was reprocessed into a pause queue for later disposal. This reprocessing allowed new messages to flow unimpeded through the pending queue.

This understanding of the status of the data within AMS-UK was a key factor impacting the recovery length as the investigation progressed through the various escalation stages. The assertion that AMS-UK was not sending any data to FPRSA-R led staff to incorrectly rule out the possibility of it being a single flight plan issue. They therefore focused their efforts on investigating the possibility of more complex faults within FPRSA-R.

Wider architecture documentation

Minor Mi2 – The complexity of the system architecture across NATS - and its regular changes and upgrades - results in any attempt to maintain up-to-date overall system mapping becoming effectively impossible.

NATS has comprehensive documentation for the numerous individual systems that it operates and maintains. However, due to the complexity of the entire NATS system architecture, and its constant evolution as required by enhancement and sustainment, there is a lack of readily available system-wide diagrams and wider documentation to support incident resolution.

In this incident, there were some misunderstandings of the system design and a lack of readily available documented design information that the team could use. The confusion lay around which networks were connected to which system and there were no readily available sources of information to confirm these connections.

Knowledge and documentation tend to be focused on NATS' individual systems. Complex faults, when experienced, often lie at the interfaces between those individual systems.

Consideration should be given to improving the end-to-end knowledge and documentation and to enable processes that more rapidly map related architecture during incidents. This will help find faults that might be upstream or downstream from the system of initial focus.

System recovery

Observation Ob4 – Using the Control and Monitoring system to access a non-operational FPRSA-R server in a situation where both servers were in maintenance mode, had not been previously identified as a potential issue.

The purpose of GCAMS (Global Control and Monitoring System) is to control and monitor the health of any systems to which it is connected. It is used by the Level 1 engineers to quickly ascertain the health of systems and perform basic control actions, such as restarting servers or switching between main and standby systems. During implementation in 2018, the testing scenarios for GCAMS did not consider the scenario of having to control FPRSA-R when it was itself experiencing multiple faults. This was due to a design feature that was intended to reduce complexity. As such, in this incident where both servers were in maintenance mode, FPRSA-R was unable to be controlled by GCAMS. This issue did not affect recovery time in this event because the FPRSA-R servers were accessed directly through the 'remote hands' process as conducted by the Level 2 engineer. However, this issue may impact future scenarios and therefore is captured in this report for completeness.

Login issues

Minor Mi3 – Password login issues contributed to a delay in the restoration time.

There was a 26-minute delay between the AMS-UK system being ready for use and FPRSA-R being enabled. This was in part caused by a password login issue for the Level 2 Engineer. At this point, the system was brought back up on one server, which did not contain the password database. When the engineer entered the correct password, it could not be verified by the server. The correct operation has since been amended by change request, reference CR49547.

4.3.4. Flow management

Background

Aviation, like other infrastructure networks, is overseen and operated by three main groups of stakeholders:

- Accountable authorities - e.g. governments, regulators and emergency services
- Infrastructure providers - e.g. National Highways for roads, Network Rail for trains, and NATS for aviation
- Users and operators - e.g. private vehicle owners and transportation companies for roads, train operators for rail, and airlines (as well as military, private pilots and others) for aviation.

All these stakeholders have responsibilities for safe operations of the infrastructure:

- Owners/operators can decide to take alternative routes or not to operate services:
    - Vehicle owners, for example, should not drive if their vehicles are unfit for purpose, or may select an alternative route if traffic delays dictate
    - Train operators will limit their service if they cannot roster the correct number of qualified staff, possibly offering alternative service by bus if they cannot access part of the network
    - Airlines will cancel flights if their aircraft have technical issues beyond acceptable resilience levels, or re-route their aircraft around weather or restricted airspace

- Overseeing national authorities can impose restrictions as required to maintain safety:
    - The emergency services will close roads when traffic accidents dictate that this is the safest course of action to safeguard other users
    - The security services will close down rail services where security intelligence requires
    - Government can close airspace, for example as was seen during 9/11 and the Iceland volcano event in 2010

- Infrastructure providers aim to provide maximum access to the infrastructure they are regulated to manage. However, they will limit access if there are challenges to safely managing demand. These factors can include technical issues, weather or staffing limitations:
    - National Highways will impose speed restrictions or close lanes on motorways when roadworks are taking place or when obstructions have been reported
    - Network Rail limits access to certain parts of the network when signals are not working properly or when weather risks impact safety
    - NATS will restrict the number of aircraft permitted to access certain parts of airspace when required by weather, staffing, technical problems or other factors.

Such actions inevitably result in delays and therefore the decision to enact them is never taken lightly. When possible, restrictions are carefully planned in advance to limit disruption. When unexpected events occur, however, safety must remain paramount. Capacity must be restricted quickly to safely manage the demand placed upon the system.

Proactive regulation management

Positive Output PO4 – UK Airspace remained accessible throughout the day, albeit at reduced capacity, with NATS continuing to offer a safe air traffic service to inbound, outbound and transiting aircraft.

To maintain safety, air traffic regulations were applied.

It should be noted that manual processing of flight plans is a required fallback mitigation to maintain an acceptable level of safety. FPRSA-R automatically processes data at maximum rates of over 800 flight plans per hour. To maintain a standby cadre of trained staff that could attempt to match that automatic processing speed is impractical and uneconomic, particularly given that it would only address one specific failure mode of the NATS system.

The relevant operational managers agreed that there was a requirement to establish traffic regulations, increasing in severity as the four-hour dataset deteriorated and required further manual intervention.

Regulations were required because the operational platforms in use across the NERL environment rely on accurate flight data so that controllers are able to correctly identify aircraft. Any degradation in this dataset due to incomplete or inaccurate flight data, would significantly impact controller workload and therefore their ability to safely manage aircraft under their control.

A number of NATS ATC systems also utilise accurate flight data to correctly predict flight trajectories and identify future potential conflictions to be resolved.

The first of these regulations was enacted across London Centre airspace at 10:46.

Positive Output PO5 – Throughout the period when regulations were in place, the operational teams effectively managed the application of regulations to ensure safety. They proactively worked with customers to exempt aircraft from regulations where possible, thereby allowing more aircraft to fly.

Regulations were applied in a stepped manner to limit the severity of the initial stages, especially to those aircraft already airborne. UK-wide restrictions were ultimately required to ensure all flights would be included.

Regulations were increased to protect the safety of UK airspace. More restrictive regulations were needed because the manual flight plan input workload increased as the event progressed, primarily driven by an uplift in Advanced Boundary Information (ABI) messages from those air traffic control authorities managing airspace adjacent to the UK. ABIs relate to airborne aircraft due to enter UK airspace (normally within the next 30 to 40 minutes), for which NATS did not have the latest flight plan information due to the FPRSA-R event. Prioritising the manual input of the associated data was critical because of the timebound nature of these inbound aircraft.

As system recovery was initiated, regulations were eased and carefully targeted to safely manage the return of traffic through the network. As per standard working practices, the Flow Management department worked with the ATC operational teams to optimise the traffic regulations and support maximum utilisation of the declared airspace capacity. Flow Management communicated its plan and continually liaised with airfields and operators on a tactical level to support and promote this capacity optimisation.

Flow Management and the respective ATC staff identified individual aircraft that could be exempted from applicable traffic regulations.

These tactical interventions saw the NATS FMP team liaising with airports and operators to ensure 'ready' (for departure) messages were still sent as early as possible even for flights impacted by regulations. This provided FMP with a live list of ready aircraft. Utilising their expertise and experience, this list could be cross-checked against the specific details of the regulations in place and current ATC workload. Where possible, flights from this list would be exempted from regulations which would have been applicable to them.

These pro-active exemptions ultimately facilitated air traffic levels consistently above the declared traffic regulations. The EUROCONTROL Network Manager's data indicates that during the period of the UK-wide traffic regulations (between 10:00 until 16:09), 365 individual flights were exempted by the operational teams. In other words, 365 flights were operated in addition to those that flew in accordance with the applicable traffic regulations.

Communication of flow rates

Observation Ob5 – EUROCONTROL was informed by FMP. EUROCONTROL then published rates via established methods, i.e. via the portal.

Processes for communicating regulations are detailed by EUROCONTROL and reflected in NATS' processes. For the regular and routine application of regulations this communication is achieved electronically. Details for more complex or high impact regulations are communicated by telephone. In either circumstance, EUROCONTROL verifies the regulation and publishes it on the Network Operations Portal (NOP) to ensure aligned awareness across all operational units. In this instance, due to the forecast severity of impact, the FMP position in Swanwick contacted EUROCONTROL by telephone. Subsequently the regulation was published on the NOP.

Subsequent capacity versus demand post-rectification

Observation Ob6 – Spare capacity was available in the air traffic network once a rectification had been implemented and regulations were removed.

When the regulations were lifted, airline demand initially met the capacity available. However, as the evening progressed, the traffic situation was significantly quieter than expected, or as is normal.

This was primarily a result of airlines and airports affected by the regulations deciding how best to protect their operations in light of reduced air traffic control capacity for an unspecified period of time. The regulations had, of course, been implemented following a system event with no known rectification time. This is not unusual with technical issues due to their singular nature. Whenever a unique technical failure mode is encountered, resolution times cannot be accurately forecast due to having no previous experience of dealing with the specific fault.

For example, at 20:30 there were four Gatwick arrivals predicted per hour whereas we would normally expect around 20.

Effectively there was little demand and therefore no further traffic management required.

4.3.5. Staffing

Staffing levels

Engineering staffing levels were within normal operating levels and in accordance with the planned roster, which includes Level 2 and Level 3 engineers on call outside their normal office working hours.

ATCOs, ATSAs and ATC Operational Support staff were resourced appropriately. As such, the ATC operation was staffed so as to be able to effectively carry out all duties throughout the event. Therefore, resourcing from within ATC operation was not a causal factor related to the technical issue. Neither did it unduly affect the manifestation or the subsequent recovery of the failure.

Data Services staffing level was not a causal factor to the incident or its resolution.

The command-and-control structure positions were suitably rostered and staffed on the day.

Data Services function

During the investigation, concerns have been raised about the Data Services function and whether some aspects of these concerns might have adversely affected the performance of the unit's role in the technical recovery process. These include, but are not limited to:

- Historic and recent restructuring of the function, including moves between directorates
- Changes to watch pattern and rostering procedures
- A higher than usual workforce turnover, leading to staffing level concerns
- A reduction in overall training and a shift from TAD training to a greater reliance on OJTI
- A lack of clarity regarding which directorates were providing administrative and training support to the function

It is beyond the scope of this investigation to assess these concerns against comparative organisational change issues experienced in other parts of the business during a period of restructuring due to COVID and post-COVID requirements. However, the issues listed above are included in this report for completeness.

Additionally, the investigation team is aware that the above items are being considered separately, as noted in 'Actions underway' at paragraph 4.3.10.

The investigation has concluded that, despite concerns raised, two key factors are relevant. Firstly, the position was staffed on the day of the incident by a qualified individual. Secondly, there is no evidence of a lack of competence for tasks that could have been expected to be carried out, in accordance with existing procedures, to deal with the scenario.

As a result, the investigation assesses that the above concerns played no causal factor in the manifestation of the incident, nor did they impact the resolution beyond the specific findings and observations highlighted elsewhere in this report.

Rostering considerations

Observation Ob7 – Technical Services staffing and rostering is based upon the level of engineering work planned, rather than the traffic forecast (and therefore the increased risk of impact in case of an event).

On 28th August the team were operating a combined Service Manager (SM) and Technical Services Manager (TSM) mode. This is an allowable role under the existing Engineering Method of Operations (EMOPS). This is usually operated when a lower workload shift is expected, as it was on this bank holiday in the absence of project or other maintenance work.

The workload on the SMCC team was manageable throughout the incident and the team performed their duties professionally and effectively.

4.3.6. Escalations

4.3.6.1. Escalation procedures

Positive Output PO6 – NATS staff followed escalation procedures, across Technical Services, ATC Operations, and the command-and-control structure.

The Technical teams followed the standard escalation process, as defined in the Engineering Method of Operations. The Level 1 engineering team used standard procedures in initial attempts to recover the system. On realising this was not possible they contacted the Level 2 support and enacted remote support. After the Level 2 support actions were deemed to have been exhausted, the Level 3 SME engineer for the system was called to support the incident resolution. As per procedure, 4th line support - the supplier - was then contacted. The roles of the lines of support are outlined in section 4.1.8.2 below.

Within the ATC operation, individual areas followed their appropriate escalation process immediately after the system event. For example, the Flight Plan team followed the FPRSA-R failure checklist, which defined those who were required to be immediately notified and to whom the event was to be escalated. ATC operations' escalation of the system event continued to be carried out in line with defined process, with the Service Manager initially advising the AC Operations Supervisor. Other ATC teams and en-route units were advised accordingly and the Duty on Call Manager was advised in line with the defined escalation process.

The command-and-control structure was activated in accordance with published processes, progressing through Bronze, Silver and Gold activation, while also activating ATICCC.

Opportunity for Improvement OFI-1 – In carefully defined circumstances, there may be opportunities to improve escalation processes to enable more expedient escalation through key positions. This would facilitate quicker onward situational awareness of an event, while retaining overall management of the situation.

There is little reference to - or suggestion of - "time-bound" activity through the incident escalation process identified within the NATS resilience plan, or within other escalation processes, for example, establishing what critical decisions, including escalation, should be actively considered when notable time windows have elapsed. The risk of not time binding, or alternatively capping, activities is that escalation and decision-making may be impeded. There is a risk that the decision to escalate becomes dependent on an individual's perception of time to resolution, impact and appetite of risk.

4.3.6.2. Technical escalation

Technical escalation within NATS follows an industry standard model of four support levels of increasing system knowledge and experience.

The 1st level, (Level 1 engineers) who are the first responders in SMCC, possess a very broad knowledge level and have managed around 60 different systems.

The 2nd level (Level 2 engineers) is staffed by the Service Delivery groups, who provide greater specialised knowledge in specific system domains, such as Flight Data, Communications and Surveillance. These teams provide on-call support and remote hands to the 1st line teams outside of office hours.

The 3rd level (Level 3 SME engineers) consists of NATS technical subject matter experts (SMEs) in the design teams. They work standard office hours, so are not a rostered or on call resource. As SMEs, they will support a major incident when required.

The 4th and final support level is the supplier or manufacturer of the system. The supplier will hold the most detailed knowledge of the system.

Support Level	Definition
1st Line	24/7 Incident response by the SMCC teams, Facilities Management (FM) or Data Services H24 (DS)
2nd Line	Service Delivery SDM teams (Support Groups) providing specialist restoration support and or advice to the SMCC teams where 1st line Response is not able to resolve service incidents
3rd Line	Specialist support from Service Design teams (Technical Subject Matter experts)
4th Line	Supplier in-depth support for asset/systems

Consideration of concurrent activities

Opportunity for Improvement OFI-2 – There is little evidence of consideration having been given to the benefits and risks from performing concurrent escalation activities. While this may have divided the focus of the team, equally there is a possibility that aspects of the escalation process could have been expedited as a result.

Neither the Standard Operating Procedure (SOP) - nor any other procedure - sets out or suggests concurrent routes to intervention. Therefore, some response activities are exclusively performed on a task-and-finish basis before others are started. This is essential in many circumstances, for example assurance testing cannot commence until a technical fix has been implemented.

While concurrent resolution activities might deliver benefits by accelerating the escalation process, such considerations must also balance the risk of additional complexity due multiple work streams.

There are certain areas, however, where a concurrent approach is likely to have expedited resolution in this circumstance. For example, while waiting for the Level 2 engineer to arrive on-site, and while investigation actions continued, the Level 3 SME engineer could have been contacted. On the day, this Level 3 SME engineer contact took place 15 minutes after the Level 2 Support Engineer arrived on site.

Concurrent escalation activities (beyond ongoing rectification attempts), during the period the Level 2 engineer was driving to site might have reduced the period to resolution in this circumstance. However, if the 1 hour 35-minute travel time had been removed from the timeline, and assuming the same rate of activity and escalation had taken place, then a resolution through escalation to the supplier would still not have provided a likely solution until 11:23am. On this occasion, that alternative timeline is unlikely to have changed the judgement that regulations needed to be promulgated at 10:45am.

Considerations regarding improved awareness of escalation options should note that there is a lack of clarity of the escalation route to the supplier within the Level 1 and Level 2/3 Engineering teams. There is also no single controlled document accessible to those that need it that contains the support contract details, in terms of what support we have in place and how to contact the supplier.

Minor Mi4 – Focus on finding a resolution led to delays in escalation.

During the Bronze calls there were suggestions to escalate either to NATS Technical SMEs or to the Supplier. This was acknowledged, but the associated escalation was actioned later. In the immediate term, the Bronze team remained focused on the technical detail as they attempted to solve the issue.

System supplier support

Major Ma5 – In this circumstance, while escalation procedures were followed, earlier contact with the supplier would most likely have expedited resolution of the event.

Once the supplier had been contacted, a plan for resolution was identified within 20 minutes. While any exact impact on this timescale is hard to quantify, NATS' investigations, including following supplier-approved recovery processes prior to contact with the supplier, enabled faster briefing as to the nature of the problem.

A full restoration of the technical system, including the requisite assurance testing, was in place within two hours of the supplier being contacted.

In future, guidance must be provided regarding considerations for when the supplier should be contacted. This guidance should include both the benefits and risks of engaging third party support too early, because it is also important that this does not become the standard response to any scenario. Such a standard response might lead to supplier fatigue with consequent unresponsiveness, a reduction in the experience and confidence of NATS engineering staff in resolving incidents, and potentially slower resolutions if simple fixes are applicable but there are delays due to briefing the supplier.

The reasons the supplier was not contacted earlier in this particular event are linked to other findings in this investigation, specifically:

- No formal guidance about skipping escalation levels
- A command-and-control model where no single person maintains an overall view of all elements of the incident response activities and requirements
- Limited concurrent escalation activities undertaken
- A lack of guiding principles that cover unspecified scenarios

These were all potentially contributory and it is not possible to isolate one specific factor that resulted in the call to the 4th level supplier support taking place when it did.

4.3.7. Command-and-control

Joint Situation Awareness

Observation Ob8 – The command-and-control teams involved in the incident response did not share Joint Situational Awareness. This led to suboptimal understanding of priorities, communication, and response activities.

The organisation has a tooling platform, "Clio Manager™" by badgersoftware, in place to provide situational awareness from all parts of the organisation involved in a response. Use of the tool was inconsistent throughout the incident. This is because of a range of factors, including confidence of the user, the availability of administrative support to enter data into the system and a general consideration that entering information into Clio is not viewed as a priority.

Training and exercises

Opportunity for Improvement OFI-3 – Improved command-and-control training and exercising would optimise responses when required. This includes providing consistent levels of capabilities, familiarity and confidence of utilising tools and processes during a live incident.

The organisation has a published document, BRC102, that provides guidance on frequency and content of exercises for command-and-control training. Although records show that the organisation meets the suggested periodicity of training, the guidance provided within BRC102 is not embedded in wider company processes relating to command-and-control training and exercising. Nor is BRC102 cross-referenced to or from the Resilience Plan. There is an opportunity to embed this document and monitor progression of training and exercising as a Key Performance Indicator.

Resilience plan improvements

Opportunity for Improvement OFI-4 – Further consolidation across the range of agreements with personnel required to be on-call to support the command-and-control structure would provide more consistency and clarity.

A comprehensive, reliable and capable command-and-control structure is critical to enable an organisation to react effectively to events that would require such a structure to be activated.

Staff who are proactively engaged, well trained and fully aware of expectations relating to their role, are key to achieving such a structure.

At present, the arrangements for members of staff to be included as incident management response team members vary between the command levels. Some individuals have signed agreements in place covering areas such as expected availability, competency and training requirements, while some do not.

The 28th August event has undoubtedly caused some to reflect upon the tasks they may be expected to undertake in any future event. Ensuring consistent terms of involvement has the potential to positively impact the retention of colleagues in response structures, as well as attracting new members to response teams.

4.3.8. Communications

Airlines, airports, and other ANSPs, including via the Operations Room

Observation Ob9 – Operational staff, especially in the Flow Management Position (FMP), were not provided with a 'line to take' / 'holding statement' to respond to customer queries.

Formal notification procedures are made via EUROCONTROL and the NATS Air Traffic Incident Communication and Co-ordination Cell (ATICCC), both of which were followed. Customers have direct lines of communications into the operation. These are normally for use during standard operations but are inevitably utilised when information is needed during incidents.

The FMP team issued the appropriate information to EUROCONTROL at 10:45, when the regulations were applied. There was a period prior to this, and certainly after the regulations were in place, that the FMP found that customers were contacting them directly in the operations room. The team was uncertain of what information could be passed to customers that wasn't already available on the Network Operations Portal (NOP). In fact, the demand for information from the FMP was such that it impeded their ability to have controlled proactive conversations with customers about a phased recovery.

ATICCC

The process for notification to customers was followed, through EUROCONTROL and ATICCC. It is recognised that there is a difficult balance between engaging with individual customers every time there is a potential impact to their operation and only communicating once sufficient detail is available.

The primary function of ATICCC is "to provide an overview of the Air Traffic operational impact of an incident on the overall network and the measures being taken to mitigate and recover" [NATS ATICCC Procedures BRC500. Issue 19].

Observation Ob10 – The effectiveness of ATICCC in communicating key aspects of the event to customers was limited, primarily due to technical problems. The performance and functionality of the teleconferencing system "LoopUp" impeded the effectiveness of interactive communications to customers. This also made the chairing of the forum extremely difficult.

The effectiveness of the ATICCC facility, and of the primary function of facilitating communication calls, was constrained by the unreliable performance and functionality of the teleconferencing system "LoopUp". This is reflected by the recordings that demonstrate poor audibility, poor call connection quality, difficulty in handling and prioritising customer enquiries, and a high number of participating internal colleagues and external customers. The participants' understanding and familiarity with ATICCC's core function and methodology may have been limited. Given the constraints listed, the efforts of the ATICCC chair should be noted.

Observation Ob11 - It may have been beneficial to customers and stakeholders to have held a further, final ATICCC call at 15:30. This would have allowed customers time to prepare any questions they might have had regarding the return to normal ATC operations.

ATICCC was closed down quickly once a technical resolution had been achieved and a plan was in place for regulation removal. This closing down of ATICCC was not communicated in a timely manner to customers, who were facing ongoing impacts to their own operations. While there may have been little further information to be provided by NATS, it would have been appropriate for at least one more opportunity for customers to ask questions regarding the operational resolution.

Positive Output PO7 – Participation of the Flow Management Position (FMP) in Air Traffic Incident Communication and Coordination Cell (ATICCC) was beneficial.

By joining the Silver calls, the Network Operations Delivery Manager provided additional expertise and guidance in relation to capacity, impact, night regulations and recovery, and assumed the role of liaison between the FMP team and Silver. Value was also provided by them joining the ATICCC calls to answer any specific questions relating to these areas, more specifically, from airports.

Notice of impacts to stakeholders

Opportunity for Improvement OFI-5 – NATS followed established processes regarding notification of regulations, utilising both EUROCONTROL and ATICCC procedures. However, consideration should be given to what further pre-warning might be possible in the future, and what further support might be useful to external stakeholders after the situation has been rectified. Such additional pre-warning and support should take into account the level of regulations that are being applied and the likely wider impact upon customers beyond pure air traffic delay.

As previously described, the complexity of the aviation eco-system results in issues experienced by one stakeholder impacting the operations of others. On the 28th August 2023, those impacts were significant.

While maintaining safety is paramount, and reducing risk to airborne aircraft is a priority, such risk then inevitably transfers to the situation on the ground. This can still be related to aircraft moving around airports but also includes risks handled by external stakeholders, such as passengers in airport terminals being unable to fly.

NATS' performance, beyond safety obligations, is measured against air traffic delay minutes caused by issues directly attributable to the organisation. Therefore, levels of air traffic delay become a focus during incidents such as the events of the 28th August.

The ongoing operational impacts of those delays upon airport and airline customers, and their passengers, are not within NATS' ability to directly control. Therefore, NATS' incident management processes do not incorporate consideration of economic or safety risk/reward trade-offs across the network.

On the basis that levels of risk are effectively moved around the aviation eco-system during such events, a more collaborative approach should be considered. This could have led to airlines and airports having more options than the cancellations and delays to their schedules that were the only effectively available possibilities on this occasion. This cannot be allowed to prevent NATS taking action to ensure safety when required but should include actions that best support wider stakeholders and that are demonstrably useful to airport and airline customers. One potential benefit from such an approach would be fewer flight cancellations, decreasing impact to passengers and increasing ATC network demand post-event.

This approach would require agreement from all key stakeholders. Earlier notification and extended support activities will result in more regular co-ordination regarding potential issues. This would inevitably increase resource requirements. A differing approach to sharing risk amongst stakeholders would also potentially require changes to existing protocols.

4.3.9. Wider observations

This section includes factors that had limited impact during the 28th August incident, but which were part of the investigation process, may be more relevant in the future, and are therefore captured here for completeness and transparency.

4.3.9.1. Processes, procedures, documentation, systems

Prestwick RIOT workstations

Observation Ob12 – Flight plans were not manually input via the Prestwick RIOT workstations.

There is the facility to input flight plans into NAS at Prestwick through two Replacement Input Output Terminal (RIOT) workstations. However, staff at Prestwick are only qualified to make minor flight plan route amendments. The competency and skills to manually input entire flight plans are based at Swanwick. This is because, as explained in Section 3, NAS does not directly impact the upper airspace managed by the Prestwick centre. Traffic levels in Prestwick's lower airspace allow flight plan input to be managed by Swanwick's centralised capability. Being able to input flight plan data via RIOT terminals is a significantly slower process than the rate of electronic flight plan processing available from a fully functioning FPRSA-R system. Therefore, any pragmatic solution to manual flight plan processing, including making these additional terminals available, would have only provided marginal benefits during the 28th August incident and serves a safety function rather than a fallback to maintain significant traffic flows.

Documentation

Observation Ob13 – Detailed procedures for handling FPRSA outages are not specifically and consistently provided across appropriate documentation and checklists within Technical Services and ATC Operations.

Documents exist for both the operational failure of FPRSA, FMP MATS Part 2 and also the technical response procedures E21682/1 & 2. However, there is no evidence of an end-to-end response plan, standard operating procedure or business continuity plan that provides guidance from failure to reinstatement and recovery.

In the ATC operation, there is documentation for NAS failure, but not specifically FPRSA failure. While the operation knew the likely impact of the FPRSA failure, they lacked operational checklists for appropriate staff e.g. the Network Operations Delivery Specialists (NODs)/Air Traffic Services Assistants (ATSAs).

In FMP, the fallback FPRS checklist states 'expect outage for up to one hour'. At that point they were looking four hours ahead and searching for operator flight plan change (CHG) and delay (DLA) messages, to support maintaining the accuracy of the data.

The Data Services (DS) H24 documentation neither described this specific scenario nor offered solutions for differing scenarios.

Opportunity for Improvement OFI-6 – There is a lack of guidance regarding principles to apply in unspecified scenarios.

It is not reasonable to provide plans for every scenario. However, there should be guidance for dealing with unspecified scenarios based on degraded systems or constrained loss of the core services within the organisation's operating licence. This could be achieved by establishing Guiding Principles for such events.

Limitations of the manual process

Minor Mi5 – The methodology of the manual process limited the capacity to input data.

Although there are seven RIOT terminals available at Swanwick, there was only one Aeronautical Fixed Telecommunications Network (AFTN) terminal, which was now receiving the data and feeding a single printer. Flight data was normally received in ADEXP format. Through the local terminal the format specified was ICAO publication 4444 "Air Traffic Management" (ICAO4444). Therefore, data entry was slowed because of the manual translation required between formats. This single printer was where all data was now being received into the suite, thereby allowing limited workforce interaction with this data feed. This hardware set-up is specific to the system; the printer is hard-wired into that system and therefore adding additional printers is not a simple option. Neither is it easy to effectively quantify what additional benefit this could deliver. As noted above, manual processing is not intended to provide standby capacity, only to maintain an acceptable level of safety, which was achieved.

Opportunity for Improvement OFI-7 – Misunderstanding was evident regarding competency levels and allowable tasks of different ratings. While this did not impact the recovery time in this event, it may do so in the future.

Upon realising the event was beyond the scope of their role, the SMCC TSE activated the Level 2 engineer via telephone. There was a brief pause while the on-call FDP Level 2 engineer gathered the required system procedures and started the remote hands process. Remote hands is a valid process that allows a higher rated competency engineer to guide a less expert engineer through a more technical procedure. During the initial triaging of the situation, it was clear there was some misunderstanding around the differing levels of expertise between the SMCC TSE Level A rating and the Level B rating held by the Level 2 teams. This included what were allowable tasks by the SMCC TSE and how General Control and Monitoring System (GCAMS) is used in practice.

FMP operational position layout

Observation Ob14 – Limitations of the current FMP set-up within the joint Operations room limited the ability to operate at a heightened level when required by an event such as this.

Several members of the FMP team came in to assist. In fact, there were more people than workstations available. The ergonomics and technological set up of the workstations constrained the possibility of deploying additional positions in their current state.

The Tactical Operational Management System (TOMS) application used on the Computer Assisted Slot Allocation Delay Monitor (CDM) – which monitors delays – is reportedly slow. This is a function of the delays in receiving inputs and processing them which means there can be an information lag of up to 20 minutes. This lack of a real-time tool to aid decision making impedes the effectiveness of FMP to respond to optimal recovery of NATS licenced services.

These constraints limited the team's ability to redirect and answer customers, as well as their ability to manage a collaborative and phased recovery.

Despite these constraints, the proactive efforts of those in FMP should be noted.

4.3.9.2. Our people

Training for incidents

Opportunity for Improvement OFI-8 – Not all engineering staff who may be involved in an incident receive the same level of associated response training as ATC operational staff, or those in the command-and-control structure.

NATS trains ATC operational staff and command teams so that they are regularly exposed to operational incident management environments. These exercises are not, however, extended to other relevant functions, such as the on-call engineering teams and design SMEs.

Similarly, the technical teams have limited experience of unusual events, outside of the standard fault-finding documentation, primarily due to the generally high-level of performance and resilience of NATS systems. While some unusual event training does take place, it is not clear this is equitable and consistent.

Post-event support

Opportunity for Improvement OFI-9 – Support to individuals was inconsistent post event.

NATS has a comprehensive and easily accessible suite of support mechanisms for employees, including Critical Incident Stress Management (CISM), Peer Support and the Employee Assistance Programme.

During the interview process, interviewees were asked whether such support was offered to them. Equally, the investigation team asked relevant interviewees if they had pro-actively told others about available support.

The responses to these questions indicated that awareness of support mechanisms is varied, and that the application, provision and take-up of support following the 28th August incident was inconsistent.

4.3.9.3. Duplicate waypoints

Opportunity for Improvement OFI-10 – The NATS system incident experienced on the 28th August 2023 has already been mitigated. NATS should continue engagement with ICAO supporting current custom and practice to mitigate / remove global duplicate waypoints.

NATS has a consistent approach in line with the published ICAO process for establishing waypoints. The duplicate waypoint issue is an ongoing conversation internationally and not a UK issue to resolve. While NATS will always seek to take a leading role - and will continue to proactively engage on the subject - we must also be careful not to commit to solutions that are beyond our remit to deliver.

4.3.9.4. ATICCC desktop PC software updates

The ATICCC desktop PCs were not immediately ready for use. After gaining entry, the ATICCC chair could not utilise the PCs in the facility due to updates being installed, a problem that has occurred in the past. Whilst there is a dedicated person within the organisation to check the PCs are functional and up to date, it should be noted that this is done on a ‘best endeavours’ basis when the individual is working at Swanwick. The software updates did not delay the customer call in this circumstance, nor could it in the future because there are now docking stations for laptops instead of using desktop PCs.

4.3.9.5. Previous findings

Continuous Improvement

Observation Ob15 – Like any large organisation with complex operations, NATS has a significant number of recommendations from previous events, audits and training exercises. It is beyond the scope of this investigation to cross-check every one of these earlier recommendations. However, due to the process-driven nature of NATS’ work culture, it is expected that the majority will have been actioned. Equally, many will have been overtaken by other circumstances and therefore no longer be required. Even so, there is a lack of readily available evidence of key lesson learning points, the associated business decisions regarding these points, and information showing that the organisation has consistently followed up and closed out actions.

Best practice refers to mixed methodologies in monitoring and adopting continuous improvement activities. These include preventative and corrective actions arising from exercises, reviews and internal and external audits following changes to relevant critical processes. However, a recurring theme is the lack of clarity about whether actions from previous reports have been undertaken.

To make sure actions are followed through (or whether they were superseded by events), they should be formally recorded in the organisation’s risk registers and acted upon where needed. This process is necessary to ensure that maximum value is derived from commissioned reports, be they incident investigations, audits, or training exercises.

4.3.10. Actions to date, rectifications complete, and improvements underway

Alongside the SAF013 investigation process, NATS has been assessing both immediate and shorter-term opportunities to improve resilience ahead of any formal recommendations. The following is a list of actions taken to date. They cover changes to systems, people and processes. While this list is comprehensive at the time of writing, NATS is consistently looking to improve resilience and additional initiatives may be started by the time the SAF013 investigation report is published.

Systems Actions

- In the immediate aftermath of the incident, it was recognised that it would be some time before an identified software fix could be made. This left the system vulnerable to a repeat of the software exception in the unlikely event that a flight plan was filed containing the same route anomalies. Therefore, engineering procedures and additional system message filtering were immediately put in place. These were designed to ensure that engineering staff would be able to swiftly resolve the issue without any impact being felt by the ATC operation.

- An FPRSA-R Software patch was quickly identified and created to remove the risk of the same, or similar, route anomalies causing the problem to reoccur. The patch was deployed on the 19th September 2023. This swift resolution was achieved by close collaborative working across the teams from NATS and the supplier, as well as with both the UK CAA and EASA regulatory bodies. This ensured that all due diligence was applied to deliver a patch that was tested and safety assured.

- An equipment review of ATICCC has been undertaken to replace “LoopUp” with an MS Teams solution. Desktop PCs are being replaced with docking stations for laptops ensuring that periodic updates will not impede the facilities’ start-up.

- The login issues experienced on FPRSA-R due to the configuration on the day have been formalised in the current set of procedures via a change request (reference CR49547).

Process Actions

- A wide-ranging review of the processes and equipment currently used by ATICCC and Silver team is underway. This review seeks to identify and enact possible improvements to the effectiveness of both, with a focus on how to improve the customer interaction.

- A study is being conducted into how best to provide additional management support to the Data Services team. The scope includes a review of training, documentation and rostering levels and will also consider the option of hiring additional staff where appropriate.

- A change request (CR49821) has been raised against the GCAMS’ FPRSA operational response document, to include details of the scenario encountered on 28th August.

- A review is being undertaken of the ‘X’ traffic volumes documentation. The review seeks to add to the options presented within the documents and to make available a range of pre-populated traffic scenarios. This will include appropriate examples of when to exempt traffic from regulations.

- Work is underway to identify appropriate triggers for escalation and timeliness of decision making.

- A review of Bronze, Silver and Gold level incident response, on-call rostered resource, operating protocols and practices to improve coordination and joint working is underway.

- Plan walk-through and refresh / enhance or create (where necessary) current SOPs.

- Situational awareness improvements, including Clio training and Gold / Silver briefings are underway on a rolling basis.

- Review of supplier contacts and support agreements has already commenced.

People Actions

- A review is underway of training materials and work instructions relating to AMS-UK and its connections to other systems. The review will focus on how data is held within the system and the impact on those systems when the data flow is turned back on after an interruption. This will enhance employee knowledge of how to clean up any unwanted data in these circumstances. As part of this review, the MATS was published on 1st December 2023 with an updated section on FPRSA-R and AMS-UK.

- TRUCE (Training for Unusual Circumstances and Emergencies) exercises are being created and will involve major systems and multiple stakeholders from different interfacing departments e.g. SMCC, FMP, DS, and other relevant support groups. These exercises aim to increase knowledge and bolster resilience within the operational teams.

- A review of FPRSA training materials is underway to include information on how data connections are made between systems.

A wash-up exercise between NATS and EUROCONTROL Network Management, with a view to further supporting the interface, took place on 5th September 2023. The meeting was chaired by Head of EUROCONTROL ATM Operations and attendees included NATS Head of Network Operations, Manager Network Operations Delivery and FMP operational staff who had been on duty during the event. EUROCONTROL operational managers who had been on duty on 28th August were also in attendance.

EUROCONTROL's feedback was positive overall. It did, however, emerge that EUROCONTROL does not rehearse Network Management TRUCE scenarios. EUROCONTROL accepted NATS' offer to include EUROCONTROL Network Management staff in TRUCE activities which are scheduled to take place in 2024.

5. Recommendations

5.1. Recommendations

5.1.1. Major Findings

Major Ma1 – The circumstances under which this incident could occur and lead to the software exception noted are extremely rare, with a flight plan needing to include a combination of, as a minimum, six specific attributes.

A technical fix to prevent the occurrence of this software exception was implemented on the night of the 18th-19th September, within 21 days of this event.

Technical Services Director to note.

Major Ma2 – Requirements for the design of the system included NATS' understanding of a logical approach to processing flight plans. One specific part of that logic would have dealt with the issue that presented itself on the 28th August but inadvertently was not incorporated into the FPRSA-R software code by the manufacturer. The unique combination of flight plan attributes that led to this event would be extremely difficult to predict, however, and was therefore not part of the formal test programme.

No recommendation, beyond the need for ongoing, effective application of NATS' existing comprehensive design requirement development methodology which follows industry best practice. It is not possible to foresee and test for every possible scenario that may transpire due to complex interactions of multiple attributes. NATS has teams and procedures in place to mitigate against unexpected events. *Technical Services Director to note.*

Major Ma3 – NATS operates a joint decision-making model through the pre-invocation, escalation, and invocation phases. In this circumstance, a blend of joint decision making with a single individual providing overall incident oversight could have led to a quicker critical escalation path.

It is recommended that NATS reviews the current command structure, its supporting technology and processes. This should analyse whether the current model is likely to lead to the best outcomes in the majority of incidents, or whether it can be optimised further with the addition of alternative options.

The review should include, as a minimum:

- Options for alternative models and examples of other effective command structures, including the use of a single incident manager model. Such options should include guidance about when the use of each option is most appropriate.
- Training requirements to maximise operational oversight capabilities during incidents.
- System and process requirements to support selected structures, including decision-making, escalation and creation of a common operating picture.

Owner: Chief Operations Officer

Major Ma4 – A subset of unprocessed data remained in the system but was outside the established pause queue. This required further escalation to identify the root cause of the issue.

It is recommended that the AMS-UK and Data Services documentation set should be reviewed to ensure that the system complexity and behaviour can be better understood by engineers and users who are not dedicated to the system.

Owner: Technical Services Director

It is recommended that the AMS-UK operator training material and associated competency assessments should be reviewed to ensure the lessons learnt from this event are appropriately captured.

Owner: Technical Services Director

It is recommended that there should be a high-level joint Technical Services and Operations review of key critical systems. Initially, this review should confirm that the operational documentation for each system reviewed has sufficient description and clarity to allow the system to be operated safely and resiliently in unexpected circumstances. Where this is not evident, a more detailed review of operational documentation and procedures should be conducted.

Owner: Chief Operations Officer

Major Ma5 – In this circumstance, while escalation procedures were followed, earlier contact with the supplier would most likely have expedited resolution of the event.

It is recommended NATS should update the escalation process to provide guidance on time or other key criteria that should trigger when and under what circumstances supplier support is requested. The process must consider, alongside the benefits of involving the supplier, the risk of distraction from the ongoing engineering rectification processes when briefing the supplier.

Owner: Technical Services Director

It is recommended that NATS should create a single controlled document detailing the supplier contracts and associated contacts who provide 24-hour support. These details should be accessible by anyone in NATS likely to be required to support an incident response. As a minimum, these should include Levels 1 through 3 of engineering support.

Owner: Technical Services Director

5.1.2. Minor Findings

Minor Mi1 – The understanding and experience of how much operational resilience was provided by the four hours of stored flight plan data varied among teams and individuals. This, in turn, led to several different interpretations of how soon there would be an operational impact, although awareness and alignment improved as the incident progressed.

It is recommended that processes are implemented to ensure that an aligned view on potential operational impacts is agreed between key stakeholders during the early phases of an incident. This should then be communicated to all appropriate staff involved in the incident response teams via the agreed central portal (currently Clio).

Owner: Chief Operations Officer

It is recommended that, where possible, likely operational impacts are pre-determined and documented.

Owner: Chief Operations Officer

Minor Mi2 – The complexity of the system architecture across NATS - and its regular changes and upgrades - results in any attempt to maintain up-to-date overall system mapping becoming effectively impossible.

It is recommended that there is an assessment of the feasibility of using new technology, or a model-based engineering process, to rapidly produce the required system schematic information to the teams during the early stages of an incident.

Owner: Technical Services Director

It is recommended that a review takes place of the current operational documentation in support of implementing new technology, or a model-based engineering process that supports rapid mapping. This must ensure that there is sufficient and accurate detail for the various levels of engineering support to see the high level, key interfacing systems and methods by which they connect. The key aim of this review is to assist the identification of problems that might be upstream or downstream of the specific system where a fault first occurs.

Owner: Technical Services Director

Minor Mi3 – Password login issues contributed to a delay in the restoration time.

It is recommended that the immediate FPRSA-R password database issue should be addressed through updates to procedures and training.

Owner: Technical Services Director

It is recommended that a review takes place of other major critical systems to ensure a similar situation cannot occur.

Owner: Technical Services Director

Minor Mi4 – Focus on finding a resolution led to delays in escalation.

It is recommended that ‘Pause for Thought’ and ‘Take 5’ processes be amended to include guidance for escalation considerations and options.

Owner: Technical Services Director

It is recommended that relevant personnel be trained to understand how effective early actions can lead to the successful resolution of incidents.

Owner: Chief Operations Officer

Minor Mi5 – The methodology of the manual process limited the capacity to input data.

It is recommended that the methodologies, processes and systems used for manually entering data into NAS during fallback scenarios are reviewed. The output of this review must be to identify amendments so that, under similar circumstances, increased rates of data input improve NATS' ability to minimise the impact to the ATC operation and the customer.

Owner: Chief Operations Officer

5.1.3. Observations

Observation Ob1 – The testing of the system followed standard NATS process and was reasonable based on the premise that it is impractical to test every single scenario within complex systems.

Technical Services Director to note.

Observation Ob2 - There appears to be little-to-no benefit in increasing flight plan data storage to longer than four hours.

Chief Operations Officer to note.

Observation Ob3 – The pause queue was established in accordance with procedures.

Technical Services Director to note.

Observation Ob4 – Using the Control and Monitoring system to access a non-operational FPRSA-R server in a situation where both servers were in maintenance mode, had not been previously identified as a potential issue.

It is recommended that a review is conducted of the key critical systems, such as safety and resilience. Failure scenarios should ensure that systems are able to be controlled or monitored during an incident. Where this is not technically possible, alternative means should be provided to the 1st line Engineers to allow a level of initial intervention.

Owner: Technical Services Director

It is recommended that Control & Monitoring (C&M) documentation is updated to highlight that there should be consideration of multiple failure scenarios, not just single failures, when designing the C&M interface.

Owner: Technical Services Director

Observation Ob5 – EUROCONTROL was informed by FMP. EUROCONTROL then published rates via established methods, i.e. via the portal.

See OFI-5

Observation Ob6 – Spare capacity was available in the air traffic network once a rectification had been implemented and regulations were removed.

See OFI-5

Observation Ob7 – Technical Services staffing and rostering is based upon the level of engineering work planned, rather than the traffic forecast (and therefore the increased risk of impact in case of an event).

It is recommended that NATS ensures the Method of Operations for SMCC and the use of combining positions is revised. The decision to combine positions should be based on the service delivery importance to the customer as well as the perceived engineering workload on the day.

Owner: Technical Services Director

It is recommended that all decisions to combine positions and associated rationales are recorded in an agreed template/format.

Owner: Technical Services Director

Observation Ob8 – The command-and-control teams involved in the incident response did not share Joint Situational Awareness. This led to suboptimal understanding of priorities, communication and response activities.

It is recommended that incident response processes and training are amended by NATS. Appropriate staff involved in incident response teams should enter all working hypotheses into the agreed central portal (currently Clio) in real time.

Owner: Chief Operations Officer

Observation Ob9 – Operational staff, especially in the Flow Management Position (FMP), were not provided with a 'line to take' / 'holding statement' to respond to customer queries.

It is recommended that relevant staff are briefed on how to respond to external enquiries when disruptive events cause significant and widespread customer impact.

Owner: Chief Operations Officer

Observation Ob10 – The effectiveness of ATICCC in communicating key aspects of the event to customers was limited, primarily due to technical problems. The performance and functionality of the teleconferencing system "LoopUp" impeded the effectiveness of interactive communications to customers. This also made the chairing of the forum extremely difficult.

It is recommended that NATS ensures appropriate updates are made to ATICCC processes and equipment.

Owner: Chief Operations Officer

It is recommended that NATS implements a regular ATICCC exercise involving relevant industry stakeholders. This could possibly be aligned with wider command-and-control exercises. Appropriate briefing material should be provided to the stakeholders beforehand.

Owner: Chief Operations Officer

Observation Ob11- It may have been beneficial to customers and stakeholders to have held a further, final ATICCC call at 15:30. This would have allowed customers time to prepare any questions they might have had regarding the return to normal ATC operations.

It is recommended that procedures be implemented stating that ATICCC cannot be closed down unless this intention has been previously notified in an earlier ATICCC call. The procedure should also note that intention to close down ATICCC should be reviewed if there is significant customer objection to doing so.

Owner: Chief Operations Officer

Observation Ob12 – Flight plans were not manually input via the Prestwick RIOT workstations.

It is recommended that consideration be given to conducting a cost-benefit analysis of training and maintaining competency in using the Prestwick based RIOT workstations to manually input flight plans. The output of this analysis should inform the operation as to whether this is an appropriate course of action.

Owner: Chief Operations Officer

Observation Ob13 – Detailed procedures for handling FPRSA outages are not specifically and consistently provided across appropriate documentation and checklists within Technical Services and ATC Operations.

It is recommended the ATC and TS departments review operational fallback procedures against identified credible failure states to ensure they have been suitably captured in operational documentation. Where appropriate, guidance and / or documentation / checklists should be provided.

Owner: Chief Operations Officer

It is recommended that guiding principles are established to provide support in the event of an incident scenario without dedicated documentation and checklists.

Owner: Technical Services Director

Observation Ob14 – Limitations of the current FMP set-up within the joint Operations room limited the ability to operate at a heightened level when required by an event such as this.

It is recommended the FMP operational workstations and toolsets within the Swanwick AC operations room are assessed against:

a. Their technological capabilities and associated functionality.
b. The ergonomic layout when operated by several users.
c. Suitability against current operations.
d. Future systems and capabilities.

This review has the specific aim to support the efficient use of available and future resources within the operational FMP and to implement improvements as appropriate.

Owner: Chief Operations Officer

Observation Ob15 – Like any large organisation with complex operations, NATS has a significant number of recommendations from previous events, audits and training exercises. It is beyond the scope of this investigation to cross-check every one of these earlier recommendations. However, it is expected that the majority will have been actioned. Equally, many will have been overtaken by other circumstances and therefore no longer be required. Even so, there is a lack of readily available evidence of key lesson learning points, the associated business decisions regarding these points, and information showing that the organisation has consistently followed up and closed out actions.

It is recommended that outputs from this report are not automatically allocated to the existing NSSG process, given that this is not a safety incident.

Owner: Safety and Sustainability Director

It is recommended that the NATS CEO appoints a single individual accountable for tracking progress of all recommendations made in this report. They will also be accountable to the CEO for detailed documentation of all decisions relating to the recommendations, including reasons for not acting. The tracking and documentation should also include all progress on the actions detailed in section 4.3.10 of this report.

Owner: Chief Executive Officer

5.1.4. Opportunities for Improvement

Opportunity for Improvement OFI-1 – In carefully defined circumstances, there may be opportunities to improve escalation processes to enable more expedient escalation through key positions. This would facilitate quicker onward situational awareness of an event, while retaining overall management of the situation.

It is recommended that NATS reviews the process, method and means of notification and escalation during incident response.

Owner: Chief Operations Officer

Opportunity for Improvement OFI-2 – There is little evidence of consideration having been given to the benefits and risks from performing concurrent escalation activities. While this may have divided the focus of the team, equally there is a possibility that aspects of the escalation process could have been expedited as a result.

It is recommended NATS ensures that training and exercise scenarios, along with supporting processes, for Incident Managers, and Bronze, Silver and Gold Chairs, include the consideration of concurrent and sequential options. Such consideration must balance the benefits gained from accelerated escalation with the risk of additional complexity due multiple work streams.

Owner: Chief Operations Officer

Opportunity for Improvement OFI-3 – Improved command-and-control training and exercising would optimise responses when required. This includes providing consistent levels of capabilities, familiarity and confidence of utilising tools and processes during a live incident.

It is recommended NATS ensures document BRC102 is embedded across related processes and all aspects are monitored via Key Performance Indicators.

Owner: Chief Operations Officer

Opportunity for Improvement OFI-4 – Further consolidation across the range of agreements with personnel required to be on-call to support the command-and-control structure would provide more consistency and clarity.

It is recommended that incident response arrangements and roles are revised by NATS. The amendments should ensure clear expectations are set around the commitment required of the individuals involved and the levels of training and exercises that are undertaken. Clear, documented and consistent descriptions of command-and-control roles – and their responsibilities – will provide enhanced capability and business resilience.

Owner: Chief Operations Officer

Opportunity for Improvement OFI-5 – NATS followed established processes regarding notification of regulations, utilising both EUROCONTROL and ATICCC procedures. However, consideration should be given to what further pre-warning might be possible in the future, and what further support might be useful to external stakeholders after the situation has been rectified. Such additional pre-warning and support should take into account the level of regulations that are being applied and the likely wider impact upon customers beyond pure air traffic delay.

It is recommended that there is a review of the notification to, and support of, customers and stakeholders when significant traffic regulations are required and where the specific situation permits. This should ensure appropriate expedition of messaging and level of detail when increasing or decreasing traffic regulations. This review should be conducted collaboratively between NATS, DfT, CAA and wider airport and airline stakeholders. It should include agreement on cross-industry training and exercising requirements. The identified stakeholders must also consider how best to implement appropriate oversight that provides and supports effective and fair stakeholder expectations and actions in such circumstances.

Owner: Chief Operations Officer

It is recommended that guidance for the media response to crisis is reviewed following the 28th August incident. *Please note that this recommendation is indicative because it is beyond the scope of the investigation, and of the investigation team's expertise.*

Owner: Communications Director

Opportunity for Improvement OFI-6 – There is a lack of guidance regarding principles to apply in unspecified scenarios.

It is recommended NATS updates the organisation's current plans/processes to include a range of possible scenarios that are outside of existing recovery procedures. They should develop integrated quick guides of all critical systems and their operational and maintenance procedures. Guiding principles should be established for use in unforeseeable scenarios.

Owner: Technical Services Director

Opportunity for Improvement OFI-7 – Misunderstanding was evident regarding competency levels and allowable tasks of different ratings. While this did not impact the recovery time in this event, it may do so in the future.

It is recommended that NATS ensures arrangements are put in place to provide a clear definition and scope of the SMCC Level 1 role (and others, where deemed appropriate). This should include the role's duties, system scope and the tools used to fulfil their job. This definition and scope should be shared among the other levels of engineering support.

Owner: Technical Services Director

Opportunity for Improvement OFI-8 – Not all engineering staff involved in an incident receive the same level of associated response training as ATC operational staff or those in the command-and-control structure.

It is recommended a review take place of all ATSEP engineers' compliance with the requirements for TRUCE training.

Owner: Technical Services Director

It is recommended that consideration be given to providing TRUCE training for non-ATSEP staff who might have to support an incident in the future. This may include technical design teams, safety staff and the supply chain.

Owner: Technical Services Director

It is recommended that access prioritisation to TAD is reviewed, including a gap analysis, to ensure technical teams' exposure to unusual events training is optimised. Such optimisation should include an improved balance between competency training and project utilisation.

Owner: Technical Services Director

It is recommended that a function independent of either Service Delivery or Project Delivery implements an oversight and governance framework to maximise the equitable allocation of TAD access.

Owner: Technical Services Director

It is recommended that a wider review of the training strategy for engineers handling unusual circumstances should take place. OJTI and TAD experience should be equally considered in related training programmes.

Owner: Technical Services Director

Opportunity for Improvement OFI-9 – Support to individuals was inconsistent post event.

It is recommended NATS improves the transparency of the colleague support network and its availability during and after an incident of this magnitude. Changes could include:

- Organisational support being provided pro-actively as part of a post-incident standard procedure, rather than upon request
- Incident response and/or pressured scenario awareness training for non-incident response colleagues

Owner: Safety and Sustainability Director

Opportunity for Improvement OFI-10 – The NATS system incident experienced on the 28th August 2023 has already been mitigated. NATS should continue engagement with ICAO supporting current custom and practice to mitigate / remove global duplicate waypoints.

It is recommended that NATS tables a proposal to ICAO that seeks agreement on removing all duplicate waypoints.

Owner: Chief Operations Officer

5.1.5. Positive Outputs

Positive Output PO1 – Actions taken by NATS on the day to mitigate the system issue ensured that the safety of the operation was protected.

Additional note - Any change from prioritisation of safety is not recommended but would in any case require associated amendments to existing statute and regulation. This would require governmental direction and stakeholder support.

Chief Executive Officer to note.

Positive Output PO2 – The system project designed and tested an expansive and robust set of scenarios, which provided assurance that the system was highly resilient.

Additional note - Unique combinations of attributes will challenge even the most demonstrably resilient and well-tested system.

The software code has now been updated to prevent the unique combination of six attributes causing a software exception.

Chief Executive Officer to note.

Positive Output PO3 – On-watch and on-call teams reacted professionally to the event as it evolved. They demonstrate a personal pride in rectifying issues to maintain the service. Individuals made themselves available beyond contractual requirements. Staff were appropriately trained, qualified and rostered.

Additional note - This demonstrates the importance of employee goodwill and of maintaining effective workforce training, professional capabilities and staffing levels.

Chief Executive Officer to note.

Positive Output PO4 – UK airspace remained accessible throughout the day, albeit at reduced capacity, with NATS continuing to offer a safe air traffic service to inbound, outbound and transiting aircraft.

Additional note - Although approximately 75% of planned flights operated, the cancelled or delayed flights created a backlog of passengers awaiting replacement flights that lasted the rest of the week.

Chief Executive Officer to note.

Positive Output PO5 – Throughout the period when regulations were in place, the operational teams effectively managed the application of regulations to ensure safety. They proactively worked with customers to exempt aircraft from regulations where possible, thereby allowing more aircraft to fly.

Additional note - While largely unseen by customers, the effective and proactive management of regulations was key to maintaining safety while enabling as many aircraft as possible to operate during the incident.

Chief Executive Officer to note.

Positive Output PO6 – NATS staff followed escalation procedures, across Technical Services, ATC Operations and the command-and-control structure.

Additional note - The adherence to existing procedures is commended. Recommendations are included alongside wider findings within this report relating to where these procedures could be further improved.

Chief Executive Officer to note.

Positive Output PO7 – The participation of the Flow Management Position (FMP) in Air Traffic Incident Communication and Coordination Cell (ATICCC) was beneficial.

Additional note/recommendation - It is recommended to explore the addition of FMP as a permanent position in Silver and ATICCC.

Owner: Chief Operations Officer

6. Glossary of Terms

TERM	DEFINITION
AC	Swanwick Area Control Centre
ACM	Airspace Capacity Manager
ADEXP	ATS Data Exchange Presentation the content of which is based on the ICAO PANS ATM 4444 doc Amendment 1
AE	Asset Engineering
AFTN	Aeronautical Fixed Telecommunications Network
AIRAC	Aeronautical Information Regulation and Control - the regulated maintenance of Aeronautical Information Publications (usually on a 28-day cycle)
AM	NAS Amendment message
AMHS	Aeronautical Message Handling Service (Protocol to be used between AMS-UK and FPRSA Replacement)
AMS-UK	Aeronautical Messaging Switch
Analysis Suite	Collection of servers and tools used to support the NERC system.
ANSP	Air Navigation Services Provider (e.g. NATS)
AOR	Area Of Responsibility
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATICCC	NATS' Air Traffic Incident Communication and Coordination Cell
ATM	Air Traffic Management
ATS	Air Traffic Services
ATSA	Air Traffic Services Assistant
ATSEP	Air Traffic Safety Electronics Personnel
Bandbox	To combine one or more operating positions into one
C & M	Control & Monitoring
CAA	The UK Civil Aviation Authority (The UK's aviation regulator)
CACC	Civil Aviation Communications Centre
CAPSIN	Civil Aviation Packet Switching Integrated Network
CASA	Computer Assisted Slot Allocation
CDM	CASA Delay Monitor
CHG	ICAO Change Message (Change to a Flight Plan)
CISM	Critical Incident Stress Management (NATS' peer support programme)
CoP	Co-ordination Point - a designated airspace point (fix) at which ATC responsibility for a flight is transferred and at which automated processing is initiated by a specific flight processing system
Corrupt Message	A message received by the FPRSA system that is recognisable in terms of being a message, but which does not conform with a recognisable message structure or content. Any data stream sequence which cannot be established as a message will be ignored.
COTS	Commercial Off the Shelf
CTC	Corporate & Technical Centre
DPO	Duty Press Officer
DS	Data Services
DSM	Duty Service Manager (the most senior engineer on duty)
EASA	European Union Aviation Safety Agency (European Safety Regulator)
Entry CoP	The CoP at which a flight enters FPRSA airspace

EO	Engineering Ops – Swanwick Day team
EMOPS	Engineering Method of Operation
EUROCONTROL	The organisation responsible for the air traffic management network in Europe
Exit CoP	The CoP at which a flight exits FPRSA airspace
FDP	Flight Data Processing
Filter Messages	The use of defined conditions to identify messages that require no further system processing, but are retained for later 'as required' user access
FMP	Flow Management Planning
FPL	Flight Plan (more specifically a non-repetitive Flight Plan)
FPRSA	Flight Plan Reception Section Automation (System) – Project 2038
FPRSA Airspace	Airspace within the designated bounds of an FPRSA system. These bounds by defined by FDP(SG) provided entry CoPs / Departure Airfields, and exit CoPs / Destination Airfields
FPRS Auto	Flight Plan Reception Section Automation (System) – Project 2038
FPRSA database	The system contained database of specific CoP, Airfields, and ATC/NAS acceptable routes
FPRSA Route	The component elements of an IFPS filed route identified as being within FPRSA Airspace
FPRSA Recognised Route	A set of FPRSA Route Elements that match an ATC route provided to the system
GCAMS	Generic Control And Monitoring System (Provides a single control and monitoring facility for many systems on a single HMI.)
HMI	Human Machine Interface
ICAO	International Civil Aviation Organisation
ICD	Interface Control Document
IFPS	Integrated Flight Planning System
JDM	Joint Decision Making
LAN	Local Area Network
MATS	Manual of Air Traffic Service, which contains the local Air Traffic rules and procedures for an operational unit
Missing Message	A message believed not to have been received by the FPRSA system from CACC, and established as missing based on the message sequence number present in a subsequently received message
Message Translation	The translation of data from specific ICAO format messages into specific and corresponding NAS format messages
MEP	Message Exchange Protocol
NAS	National Airspace System (Implemented on the Host Computer System)
NAS Direction Fix	A NAS recognised Fix after which NAS strip processing is not performed
NAS Start Processing Fix	The Fix entered into NAS in the NAS field 6
NAS Route	The Route elements entered into NAS in the NAS field 10
NATS	Used interchangeably with NERL in this report – see below
NERC	New En-Route Centre
NERL	NATS En Route Limited
NFS	Networked File System
NMOC (CFMU)	Network Manager Operations Centre (was Central Flow Management Unit)
NOD	Network Operations Delivery
NOP	Network Operations Portal
NSA	Networked Storage Array (essentially a highly resilient, large capacity NFS storage facility)
NTP	Network Time Protocol

OJTI	On-the-Job Training Instructor
OS	Operations Supervisor *or* Operating System
PAD	Packet Assembler / Dis-assembler Device (use within context)
PC	Prestwick Area Control Centre
POMS	Pre Operational Message Switch
PSU	Power Supply Unit
Post FPRSA Route Elements	All route elements after the exit CoP
RIOT	Replacement I/O Terminal
Route	Element Individual Fix or Airway element within a route
RPD	Route Pairing Database
SE	Service Engineer
SIEM/SOC	Security Information and Event Management / Security Operations Centre
SM	Service Manager
SMCC	Service Management Command Centre
SME	Subject Matter Expert
SMF	Service Management Framework
SPRINT	Strategic Peripheral adapter module Replacement Incorporating Network Technology
SRS	System/Supplier Requirement Specification (document)
TAD	Test and Development Service Hub
TC	Swanwick Terminal Control Centre
TCP	Transmission Control Protocol
TNA	Training needs analysis
TOMS	Tactical Operational Management System
TRUCE	Training for Unusual Circumstances and Emergencies
TSM	Technical Services Manager
UID	User Interface Design
'X' Traffic	The generic term for air traffic which ATC manually exempts from regulations

Appendix A – Initiating Instruction SAF 013 – System Failure – 28th August

On 29th August 2023 NATS CEO initiated an SAF 013 Major Incident Investigation into the Flight Plan Reception Suite Automation (FPRSA) failure that occurred on 28th August 2023.

Objective

The principal area of focus will be to establish the causes of the event, to consider its implications across NATS operations, and to ensure that remedial actions taken and planned will minimise the risk of recurrence and thereby assure relevant stakeholders that impacts of such an event in the future will be mitigated as far as practicable.

Full Terms of Reference for the investigation are at the Appendix [to this initiating instruction].

Schedule

The Review will commence on 29th August 2023. At this stage it is expected that the reports produced resulting from the investigation will be split into a Preliminary Report focusing on immediate cause, impact, response and application of internal process, and a Final Report which will provide further detail following consultation with the CAA and other relevant stakeholders that NATS and the CAA identify based upon the conclusions of the Preliminary Report:

- The Preliminary Report will be issued by 1400 hrs on 4th September 2023.
- The Final Report will be issued on a date to be confirmed, dependent on the output of the consultation. For planning purposes currently, the date of this is assumed to be the 29th September 2023.

The Preliminary and Final Reports will be provided to the NATS CEO and NATS Safety Director.

The Preliminary and Final Reports will be issued further, at a minimum to the CAA, after receipt and action of the associated factual accuracy check, stating the findings and their status.

The findings of the investigation will be presented to the NSSG in Nov 23.

The investigation will be managed in accordance with NATS Procedure SAF 013.

Team

The SAF 013 Review Team will consist of:

Investigation Initiator	Martin Rolfe	NATS CEO
Investigation Lead	Guy Allison	Director of Corporate Strategy
Investigation Team		Head of Quality, Risk & Investigation (TS) Manager Operations Safety Investigations Head of Safety Oversight

Other Investigation Team members will be added as deemed necessary by the Investigation Lead.

Terms of Reference

The SAF 013 Major Incident Investigation into the NATS System failure on 28th August 2023, as initiated by the NATS Chief Executive Officer, Martin Rolfe, will enable the causes of the event to be established, will consider the implications across NATS operations, will explain the actions taken to rectify the failure, and will assess whether remedial actions taken and planned will minimise the risk of recurrence thereby providing assurance that impacts of such an event in the future will be mitigated as far as practicable.

The Preliminary Investigation will cover the areas detailed below in bullets 1-5 and will be completed by 1400 hrs on 4th September 2023:
1. Determine the immediate cause(s) and sequence of events that led to the incident including any contributory or aggravating factors or opportunities to prevent the interruption recurring.

2. The safety and operational impact to the NATS operation.

3. The response by ATC, Technical Services, and business continuity teams to minimise disruption.

4. The extent to which the applicable NATS internal processes were applied.

5. The actions taken to diagnose and mitigate the failure and to restore the operational service to full redundancy.

A Final Report providing more detail on the conclusions of the Preliminary Report will subsequently be produced on a date yet to be agreed through consultation with the CAA; the current planning assumption is for issuance on the 29th September 2023. The full scope requirements of the Final Report will be discussed with the CAA and other relevant stakeholders that NATS and the CAA identify, following review of the Preliminary Report conclusions, but is expected to include the following areas in addition to those covered by the Preliminary
Report:

6. The effectiveness of all actions taken by NATS to restore and mitigate the NATS operation, following the failure and considering associated assessment of the level of residual risk as well as the risk of a re-occurrence with current systems.

7. The timeliness and effectiveness of the internal communications.

8. The timeliness and effectiveness of airline, airport and other customer stakeholder notification and communication methods.

9. The timeliness and effectiveness of the internal and external notification and communications methods with other ATM stakeholders, including CAA and EUROCONTROL.

10. Recommendations following assessment of longer-term options, to further manage the risk of potential further failures

Appendix B – Preliminary Report

Flight Plan Reception Suite Automated (FPRSA-R)

Sub-system Incident 28th August 2023

Table of contents

1. Introduction 63

2. Scope of this report 64

3. Overview of NATS' Air Traffic Control System 65

3.1. Overview of Air Traffic Control System 65

3.2. Overview of Flight Plan Processing 66

4. Description of the issue 68

4.1. Sequence of events leading to the failure 68

5. Technical Recovery 71

5.1. Actions taken to diagnose and mitigate the failure 71

5.2. Response by Technical Services team 71

6. Operational Recovery 73

6.1. Air Traffic Control Team Actions 73

6.2. Application of Business Resilience Processes 73

7. Impact on the NATS Operation 75

7.1. Safety impact 75

7.2. Service Delivery impact 75

8. Steps Taken to Prevent Recurrence 77

8.1. Actions taken or underway to prevent the interruption recurring 77

9. Areas for Further Investigation 78

10. Appendices 79

1. Introduction

NATS (En Route) Plc, referred to in this report as NATS, was created in 2001 with an associated operating licence in which the clear primary purpose is to deliver a safe air traffic control system in the UK. NATS' secondary but important purpose, as defined in Condition 2 of its licence, is to enable reasonable levels of air traffic to take place in the UK controlled airspace environment.

On 28th August 2023, significant disruption was experienced across UK airspace following an incident affecting part of the technical infrastructure that supports NATS' safe controlling of aircraft. In keeping with its primary purpose, NATS delivered a safe operation throughout. However, the reduced levels of flights that resulted from the measures needed to maintain safety due to the technical incident caused significant disruption to the UK aviation system.

While it is not yet clear exactly how many flights were cancelled by airlines, it is likely that the number exceeds 1,500 for Monday 28th August, with more cancelled on Tuesday 29th August as the airlines strived to recover their schedules. This number is in addition to the delays to flights on 28th August; of the 5,500 flights that did operate in UK airspace around 575 were delayed as a result of the incident.

The Board of NATS has read and discussed this preliminary report and is working with the executive team to ensure that such an incident does not recur. The Board and management would like to reiterate our apology to all those affected. NATS is fully aware of the distress and frustration that the incident last week caused and nothing in this report is intended to downplay the disruption. NATS takes operational resilience very seriously and therefore we are committed to a transparent investigation process overseen by the Civil Aviation Authority (CAA), NATS' independent regulator, in order to provide answers to stakeholders as well as identifying opportunities to reduce the likelihood and impact of the same or similar incidents occurring again.

This Preliminary Report is the first step in that process, but its production is necessarily time constrained in order to provide initial answers to CAA, DfT and aviation stakeholders including the travelling public. Its contents include areas identified for further investigation.

2. Scope of this report

This Preliminary Report has been produced from information gathered under an internal Major Incident Investigation initiated by the NATS CEO. In accordance with the Terms of Reference of that investigation, as shared with the CAA, the focus of this Preliminary Report is on the following five areas:

1. Determine the immediate cause(s) and sequence of events that led to the incident including any contributory or aggravating factors or opportunities to prevent the interruption recurring.

2. The safety and operational impact to the NATS operation.

3. The response by Air Traffic Control, Technical Services, and business continuity teams to minimise disruption.

4. The extent to which the applicable NATS internal processes were applied.

5. The actions taken to diagnose and mitigate the failure and to restore the operational service to full resilience.

The incident occurred 7 days prior to the publication of this report. As a result, the investigation to date has focused on the root causes of the incident in order to ensure that mitigating action can be taken promptly to prevent recurrence. This report reflects that focus and sets out areas of further investigation that are already ongoing and others that have been identified in the course of the investigation to date.

3. Overview of NATS' Air Traffic Control System

a. Overview of Air Traffic Control System

Air Traffic Control (ATC) is the provision and operation of a safe system for controlling and monitoring aircraft.

NATS, as an Air Navigation Service Provider (ANSP), is responsible for the provision of ATC in the majority of controlled airspace across the UK. Its principal objective is to deliver safety in the sky. NATS has a strong history of being at the forefront of ATC safety developments and has an international reputation for its approach to safety, which is deeply embedded in the culture of the company.

In the UK, commercial flights operate within controlled airspace. Within controlled airspace Instrument Flight Rules (IFR) apply, whereby aircraft fly by reference to instruments on the flight deck and are required to file a flight plan. Controlled airspace is divided up for ATC purposes into geographical areas called sectors. An Air Traffic Control Officer, or team of controllers (ATCOs), is assigned to an individual sector and have responsibility for controlling all aircraft within that sector.

All IFR flight plans in European airspace are received by EUROCONTROL's Network Manager, which is based in Brussels. On a practical level, EUROCONTROL processes all flight plans requiring services from its member state ANSPs, such as NATS, managing the co-ordination of air traffic control throughout Europe-wide airspace and helping to prevent air traffic congestion.

ATC ensures that aircraft are safely separated laterally and vertically. For most of its flight an aircraft in controlled airspace will receive an en route ATC service from a control centre in the flight region through which it is flying. NATS has two area control centres: one at Swanwick in Hampshire and the other at Prestwick in Ayrshire.

The main ATC systems utilised by ATCOs in providing the service include, amongst others:

- voice communications: for two-way communication between ATCOs and pilots, and controllers and other ATC units;
- surveillance: providing radar information to ATCOs;
- flight data processing: flight planning information to plan and coordinate traffic in each sector of airspace;
- workstations: providing the radar display, flight information and ancillary information to ATCOs;
- control and monitoring systems, allowing engineers to monitor and support maintenance/rectification as required;
- data communications: for network connectivity and data exchange;
- time-distribution systems; providing accurate time signals across systems; and
- flow management: tools for managing controller workload.

Licensed ATCOs are responsible for safely controlling flights and communicating with pilots and other controllers. Air Traffic Service Assistants (ATSAs) support ATCOs by updating flight data and carrying out other support tasks. The technical systems that underpin the delivery of the air traffic services are monitored and maintained 24/7 by a team of 1st and 2nd Line engineers and technicians with 3rd Line support available from appropriate suppliers.

Since this report relates specifically to the Flight Plan Reception Suite Automated (FPRSA-R) sub-system and its immediate connectivity to other systems, it is important to understand that this is one small part of the overall NATS technical system. There are many hundreds of sub-systems that make up the full NATS operational estate. All of these sub-systems operated normally before, during and after the incident.

b. Overview of Flight Plan Processing

Operators, usually airlines, wishing to fly through controlled airspace within participating European Countries must submit a flight plan, either directly or through third parties.

This Flight Plan will contain key information such as aircraft type, speed, callsign and intended routing that enables ANSPs to plan for, safely control and communicate with the aircraft. ATC systems are dependent on accurate flight data to understand the intended route of aircraft so that ANSPs can assess air traffic demand upon their airspace and support the safe and efficient handling of multiple aircraft within that airspace.

The airlines determine which airfields or points within the airspace they wish to fly between using published route information. For flights that will operate within the European flight regions, they submit the plan into EUROCONTROL's Integrated Initial Flight Plan Processing System (IFPS), which is the central Flight Planning tool for the International Civil Aviation Organization (ICAO) European Region.

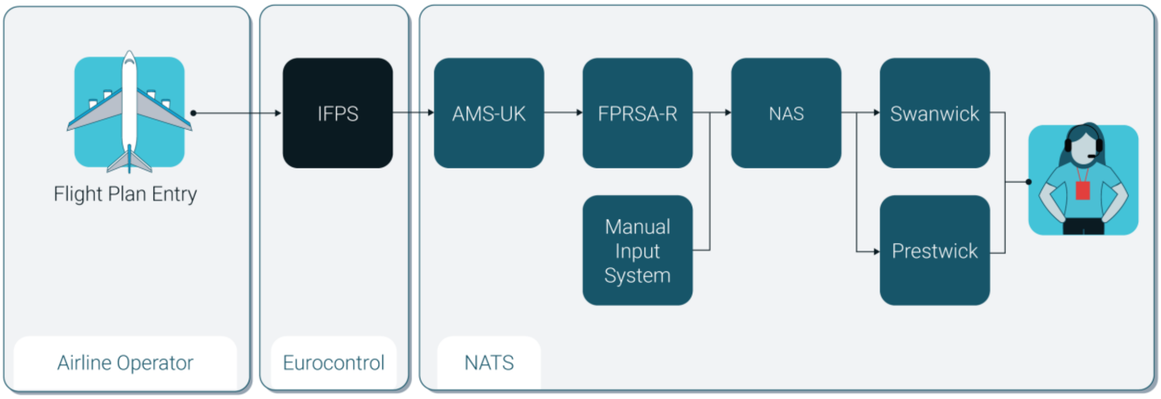
If the submitted flight plan is accepted by IFPS, i.e. it is compliant with IFPS defined parameters, it will inform the airline that filed the flight plan that it has been accepted. This is sufficient for a flight to depart with local ATC approval. The flight plan will be sent from IFPS to all relevant ANSPs who need to manage the flight. For the UK this data is received at NATS, and then distributed to relevant UK operational ATC units using a system called Aeronautical Message Switch – United Kingdom (AMS-UK).

Within the NATS En-route operations at Swanwick Centre, the data is passed to FPRSA-R. The FPRSA-R sub-system exists to convert the data received from IFPS (in a format known as ATS Data Exchange Presentation, ADEXP) into a format that is compatible with the UK National Airspace System (NAS). NAS is the flight data processing system which contains all of the relevant airspace and routings.

An FPRSA sub-system has existed in NATS for many years and in 2018 the previous FPRSA sub-system was replaced with new hardware and software manufactured by Frequentis AG, one of the leading global ATC System providers. The manufacturer's ATC products are operating in approximately 150 countries, and they hold a world-leading position in aeronautical information management (AIM) and message handling systems. Since the introduction in NATS of the replacement FPRSA sub-system in 2018, the system has been known as FPRSA-R. This system has processed over 15 million flight plans and had not suffered a loss of both primary and backup systems prior to the incident.

NAS then provides flight data and other information to the relevant ATCO at their working position.

The figure below shows the end-to-end flight data processing information flow and highlights who manages the systems involved.



FPRSA-R has a primary and backup system monitored both by dedicated Control and Monitoring (C&M) systems and also an aggregated central C&M system.

Further resilience is provided by NAS storing 4 hours of previously filed flight data to allow the operation to continue in the event of the loss of automatic processing of flight data.

In addition to the technical resilience provided by backup systems, and the 4 hours of stored flight data, there is operational contingency available to allow safe service to continue. This is provided through the ability to input flight data manually, directly into NAS using a manual input system.

4. Description of the issue

a. Sequence of events leading to the failure

The NATS ATC System was operating normally. No system upgrades were being implemented and no critical systems were out of operation. All backup systems were operating as designed. All systems were being monitored by the NATS Technical Services teams in the usual manner. Everything was in full accordance with NATS processes. No system warnings or errors related to the incident were observed ahead of the incident.

The start of the sequence of events leading to the incident can be tracked back to the point at which a flight plan of the airline French Bee was entered into the flight planning system. In the hours ahead of 04:00[1] on 28 August the airline submitted an ICAO4444 compliant flight plan for flight FBU37M into EUROCONTROL's flight planning distribution system, IFPS. The flight was planned to depart Los Angeles International Airport at around 04:00 on 28th August and arrive at Paris (Orly) around 15:00 (see Appendix 3). The flight plan was accepted by IFPS and stored for subsequent onward submission to NATS systems at the appropriate time. This would be scheduled to happen 4 hours before the aircraft reached the boundary of UK domestic airspace. With the flight plan accepted, the aircraft was cleared to depart at 04:00 by US ATC.

At 08:32 the flight plan for FBU37M was received by NATS' FPRSA-R sub-system from EUROCONTROL's IFPS system. This is consistent with the 4 hour rule mentioned above. The purpose of the FPRSA-R software is to extract the UK portion of the flight plan from UK airspace entry to exit point and to pass that to the flight data processing system for onward presentation to ATCOs.

The flight plans delivered to FPRSA-R by IFPS are converted from an ICAO document 4444 (ICAO4444) format to a format known as ADEXP. ADEXP is a European-wide flight plan specification that includes, amongst other data, additional geographical waypoints within the European region specific to the route of a flight. For flights transiting through UK airspace, rather than landing in the UK, this will include additional waypoints outside of UK airspace required for its onward journey. Following this conversion, the ADEXP version of a flight plan includes, amongst other aspects, the original ICAO4444 flight plan plus an additional list of waypoints and other data.

The flight plan for FBU37M delivered to FPRSA-R by IFPS had been converted in the usual way into ADEXP. Following the IFPS processing of the flight plan, the ADEXP format of the flight plan contained the original ICAO4444 flight plan plus additional waypoints relevant to its route. Appendix 1 includes an extract of the ADEXP file which shows the ICAO4444 detail. Appendix 2, is a further extract of part of the ADEXP file, showing the list of additional waypoints now included.

The ADEXP waypoints plan, per Appendix 2, included two waypoints along its route that were geographically distinct, but which have the same 3-letter designator, DVL. One DVL represents the waypoint Devil's Lake in North Dakota, USA, the second DVL represents Deauville in France.

Although there has been work by ICAO and other bodies to eradicate non-unique waypoint names there are duplicates around the world. In order to avoid confusion latest standards state that such identical designators should be geographically widely spaced. In this specific event, both of the waypoints were located outside of the UK, one towards the beginning of the route and one towards the end; approximately 4000 nautical miles apart.

[1] Times have been converted to British Summer Time for consistency with other times quoted in the report, unless stated otherwise.

Once the ADEXP file had been received, the FPRSA-R software commenced searching for the UK airspace entry point in the waypoint information per the ADEXP flight plan, commencing at the first line of that waypoint data. For this flight as filed, this was a waypoint designated as 'APSOV'. FPRSA-R was able to specifically identify the character string APSOV as it appeared in the ADEXP flight plan text. (Appendix 2: [A])

Having correctly identified the entry point, the software moved on to search for the exit point from UK airspace in the waypoint data. For this flight route the anticipated exit point would be the waypoint known as SITET (Appendix 2: [B]).

Having completed those steps, FPRSA-R then searches the ICAO4444 section of the ADEXP file (Appendix 1). It initially searches from the beginning of that data, to find the identified UK airspace entry point, in this case APSOV. This was successfully found (Appendix 1: [C]). Next, it searches backwards, from the end of that section, to find the UK airspace exit point, looking for SITET. This did not appear in that section of the flight plan, as shown in Appendix 1, so the search was unsuccessful. As there is no requirement for a flight plan to contain an exit waypoint from a Flight Information Region (FIR) or a country's airspace, the software is designed to cope with this scenario.

Therefore, where there is no UK exit point explicitly included, the software logic utilises the waypoints as detailed in Appendix 2 of the ADEXP file to search for the next nearest point beyond the UK exit point. The next nearest waypoint after the UK boundary is the waypoint ETRAT (Appendix 2 [D]). The software therefore subsequently searched data per Appendix 1 for ETRAT. This was also not present. The software therefore moved on to the next waypoint, which is DVL (Deauville) (Appendix 2 [E]). This search was successful as a duplicate 3-letter identifier, DVL, appeared in the Appendix 1 section of the flight plan (Appendix 1 [F]).

However, the DVL that appears at Appendix 1[F] relates to Devil Lake, North Dakota. This is an earlier point in the flight, passed before reaching the entry point to UK airspace. Having found an entry and exit point, with the latter being the duplicate and therefore geographically incorrect, the software could not extract a valid UK portion of flight plan between these two points in Appendix 1. This is the root cause of the incident. We can therefore rule out any cyber related contribution to this incident.

Safety critical software systems are designed to always fail safely. This means that in the event they cannot proceed in a demonstrably safe manner, they will move into a state that requires manual intervention. In this case the software within the FPRSA-R subsystem was unable to establish a reasonable course of action that would preserve safety and so raised a critical exception. A critical exception is, broadly speaking, an exception of last resort after exploring all other handling options. Critical exceptions can be raised as a result of software logic or hardware faults, but essentially mark the point at which the affected system cannot continue.

Clearly a better way to handle this specific logic error would be for FPRSA-R to identify and remove the message and avoid a critical exception. However, since flight data is safety critical information that is passed to ATCOs the system must be sure it is correct and could not do so in this case. It therefore stopped operating, avoiding any opportunity for incorrect data being passed to a controller. The change to the software will now remove the need for a critical exception to be raised in these specific circumstances.

Having raised a critical exception, the FPRSA-R primary system wrote a log file into the system log. It then correctly placed itself into maintenance mode and the C&M system identified that the primary system was no longer available. In the event of a failure of a primary system the backup system is designed to take over processing seamlessly. In this instance the backup system took over processing flight plan messages. As is common in complex real-time systems the backup system software is located on separate hardware with separate power and data feeds.

Therefore, on taking over the duties of the primary server, the backup system applied the same logic to the flight plan with the same result. It subsequently raised its own critical exception, writing a log file into the system log and placed itself into maintenance mode.

At this point with both the primary and backup FPRSA-R sub-systems having failed safely the FPRSA-R was no longer able to automatically process flight plans. It required restoration to normal service through manual intervention. The entire process described above, from the point of receipt of the ADEXP message to both the primary and backup sub-systems moving into maintenance mode, took less than 20 seconds. 08:32 therefore marks the point at which the automatic processing of flight plans ceased and the 4 hour buffer to manual flight plan input commenced. The steps taken to restore the FPRSA-R sub-system are described in section 5 of this report.

On no occasion prior to the 28th August have both FPRSA-R primary and backup sub-systems failed. It is therefore certain that this specific flight plan, with its associated characteristics (including duplicate waypoint names), has never previously been filed.

The investigation has established that the circumstances under which this incident could occur and lead to the software exception noted are extremely rare and specific, needing to include, as a minimum, all of the following:

- The waypoints segment of the ADEXP Flight Plan Message containing duplicate waypoints.
- Those duplicate waypoints both being outside of UK airspace, and on either side of the UK airspace.
- One of the waypoints needs to be near to the UK airspace boundary exit point, in order to be eligible for potential use by FPRSA-R search logic.
- The first duplicate waypoint needs to be present in the ICAO4444 flight plan segment of the ADEXP flight plan message,
- The second duplicate waypoint (the one near the UK FIR exit point), needs to be absent from the ICAO4444 flight plan.
- The actual UK exit point needs to be absent from the ICAO4444 flight plan segment of the ADEXP flight plan message.

The FPRSA-R sub-system has operated continuously since October 2018 and has processed over 15 million flight plans.

Now that the root cause has been identified further work needs to be undertaken to trace back through the development and testing of the FPRSA-R sub-system to understand whether the combination of events that led to the incident could have been mitigated at some point in the software development cycle. It is our understanding from the manufacturer that the specific area of software related to this investigation is unique to NATS.

5. Technical Recovery

a. Actions taken to diagnose and mitigate the failure

The initial diagnosis of the fault was complex due to the way it was presenting to the on-site engineers. The immediate actions taken were based on a combination of standard processes and lessons learnt from previous experience. However, it took the greater technical knowledge of the NATS design authority and manufacturer to establish the recovery approach.

b. Response by Technical Services team

As described in section 4, the specific scenario that caused the FPRSA-R sub-system to fail safely was complex and had not been experienced since it was put into operation in October 2018.

NATS operates a rostered, 24 hour team of 1st Line support engineers onsite at our Swanwick Air Traffic Control Centre. This onsite 1st Line team is supported by 2nd Line on-call system experts and access to 3rd Line manufacturer support through established support contracts. This enables NATS to monitor and respond to technical issues 24/7 with the intent to resolve them without impact to the airlines and the travelling public.

The 1st Line support team were alerted to the incident through the C&M systems that directly monitor operational systems as well as through direct feedback from the Operational teams using the FPRSA-R sub-system at the time. The initial response for the team followed standard recovery processes using the centralised C&M systems to restart the sub-system. Following multiple attempts to restore the service, which were unsuccessful, the 2nd Line engineering team was mobilised and supported the on-site engineers remotely via video link. The process deliberately utilises remote support technology to ensure that issues can be investigated immediately without time lost to travel by support engineers.

The on-call teams working remotely with the on-site engineering teams followed a staged analysis, involving increasingly detailed procedures to attempt to resolve the issue, none of which were successful. As per standard escalation procedures, 2nd Line engineers were engaged to provide further access to advanced diagnostics and logging capabilities.

Additional support was then requested from the Technical Design team and sub-system manufacturer as 1st and 2nd Line support had been unable to restore the service or identify the precise root cause, which was unusual. The manufacturer was able to offer further expertise including analysis of lower-level software logs which led to identification of the likely flight plan that had caused the software exception. Through understanding which flight plan had caused the incident the manufacturer was able to provide the precise sequence of actions necessary to recover the system in a controlled and safe manner.

Before restoring any sub-system into live air traffic operations following a failure, a period of isolated non-live operations is performed. This focuses on stability testing and to ensure there are no unexpected safety implications. Once this process was complete, the system was approved to go back into live air traffic operations with full automatic processing of flight plans.

Following restoration, the next four hours of flight plans were processed automatically by the FPRSA-R sub-system in approximately 9 minutes. Since the data included a significant number of modified flight plans as a result of the disruption to airline operations the technical teams then supported the ATC teams through the data reconciliation process. This was undertaken to ensure the data integrity required to support safe service provision.

The FPRSA-R sub-system, both primary and backup versions, were restored to isolated non-live operations at 13:36 and to fully automated live operations at 14:27.

The FPRSA-R sub-system has continued to function normally since the point of recovery. Enhanced engineering monitoring and oversight has been in place since the restoration of service.

To provide a buffer of time for engineering analysis and rectification of faults, the system has been designed to store 4 hours of flight plans to allow continuous operation while faults are diagnosed and resolved. On this occasion the 4 hours was insufficient to diagnose and resolve the fault. The final investigation will include further analysis of this issue, including the sufficiency of the 4 hours' contingency period. Furthermore, the investigation will need to include an analysis of any factors that may have led to the recovery taking as long as it did.

6. Operational Recovery

a. Air Traffic Control Team Actions

The ATC operational responses to the incident are detailed within established (and trained for) 'fallback' procedures and processes detailed within the Manual of Air Traffic Services (MATS). The MATS details the specific procedures that the units and individual sectors are to apply to maintain safety and ensure that UK Airspace remains open.

The fallback procedures for this incident include specific actions for the manual entry of flight plan data into the system and manual coordination of flights between sectors. In the event of a reversion to manual process, it is necessary to reduce the UK traffic flow by implementing air traffic control restrictions. This ensures that aircraft will be safely handled during the phase of reduced capacity arising from the manual processes in use.

An air traffic flow restriction (or regulation) is a declared reduction in capacity for the number of aircraft within sectors of airspace, to support the safe handling of aircraft throughout that airspace. In circumstances where airlines have received confirmation of acceptance of their flight plan from IFPS, they will proceed to fly their route as planned unless a flow regulation has been applied to their flight by any ANSP on their route. This means that, as a result of the incident, NATS would have expected to provide an air traffic service to multiple flights for which it had incomplete information, which significantly increases the complexity of the air traffic control task. In order to preserve the safety of the operation, it was therefore critical to restrict the number of flights using UK airspace to match the information available.

The first air traffic flow regulations instigated, to match the rate of information being provided by manual processing, were applied to commence from 11:00 to avoid overloading ATCOs from 12:30, when the store of automatically processed flight plans would be exhausted. The two regulations applied were universal restrictions across the whole of Swanwick and Prestwick centre airspace, i.e. not individual sectors, airports or routes.

Following the restoration of the FPRSA-R sub-system and the resumption of automatic flight plan processing, regulations were incrementally removed in a way that ensured safe return to normal traffic levels. The two most restrictive universal regulations were removed by 16:10 with all regulations removed by 18:03.

b. Application of Business Resilience Processes

In response to the publication by the CAA in 2018 of CAP1682 ('Decision on modifications to Condition 2 of NATS (En Route) plc licence in respect of resilience planning, policy statement on enforcement and resilience plan guidance'), NERL published a resilience plan.

The NERL Resilience Plan aligns to international standards and best practice guidance including ISO22301 (Business Continuity), ISO22316 (Organisational Resilience), ISO31000 (Risk Management), ISO 22320 (Incident Response), BS11200 (Crisis Management), and The Business Continuity Institute Good Practice Guidelines 2018.

The NERL Resilience Plan 2023 recognises that "there will be failures in complex environments with highly inter-dependent systems and processes, despite the extensive proactive barriers to prevent disruption". In order to manage such failures reactively, the NERL Resilience Plan includes an Incident

Management Framework. This framework is a 'Command and Control' management structure and is based on a system used extensively by the UK civil emergency services. It consists of a hierarchical structure of GOLD, SILVER, and BRONZE Incident Management Teams, (Gold and Silver teams are rostered on a continuous basis as a contingency, even during normal operations.)

The NERL Resilience Plan also details the NATS Air Traffic Incident Communication and Coordination Cell (ATICCC). This is a communications facility intended to provide an overview to airline and airport customers, and other stakeholders, of the air traffic operational impact of an incident on the overall network and the measures being taken to mitigate and recover.

On 28th August, the Gold, Silver and Bronze incident management teams and ATICCC were activated and began responding in accordance with the NERL Resilience Plan. When it was apparent that the standard engineering restoration activities were insufficient, the incident was escalated to Bronze. Subsequently, Silver, Gold and ATICCC were activated. Bronze, Silver and Gold remained active throughout the duration of the incident.

7. Impact on the NATS Operation

a. Safety impact

Analysis of the available radar, flight data processing, and safety data for the period indicates no ATC safety events occurred during the incident.

Under UK legislation, ATC operational and engineering staff are required to submit Mandatory Occurrence Reports (MOR) to the CAA for defined safety related occurrences. These reports are sent directly to the CAA and are also stored within the NATS Safety Tracking and Reporting System (STAR). In keeping with NATS' open reporting culture, NATS staff are encouraged to submit safety observation reports for events that are not mandated by UK legislation. As these reports may also provide safety related information, they are also stored within STAR.

During the incident, one MOR was submitted by the ATC operation and entered into STAR by the London Terminal Control (LTC) Operations Supervisor (OS) of the morning shift concerned. This report was distributed to the CAA at 19:15 the following day, 29th August 2023 and indicated that there were no reports of safety concerns from ATC operational staff during the incident.

Beyond the ATC operation, one MOR was submitted by Engineering and entered into STAR by the Engineering Service Manager. This report was distributed to the CAA at 07:55 on 30th August 2023. The MOR detailed an overview of the FPRSA-R failure, the operational effect and aspects of the subsequent actions taken from a technical perspective on the day.

b. Service Delivery impact

UK Airspace remained open throughout the incident and NATS continued to operate traffic, although it introduced air traffic flow restrictions in order to maintain safety in accordance with its license.

The first NATS air traffic flow regulations resulting from the incident were applied to commence at 11:00 with all regulations removed by 18:03. During this period, there were 22 such regulations applied to different parts of UK controlled airspace to ensure the safe handling of aircraft.

These regulations contributed to a total delay of **65,250**[2] minutes attributable to NATS. This delay total is the cumulative impact of the 575 delayed flights, experiencing an average delay of approximately 1hr 50 minutes to their departure. Delay is the difference between the planned and actual departure times.

The most restrictive traffic regulations enacted within the UK on 28th August 2023 were those applied to reduce the traffic in Prestwick and Swanwick Centres. These two regulations created 15,270 and 12,567 minutes respectively of delay attributable to NATS.

Following the restoration of the FPRSA-R sub-system and the resumption of automatic processing of flight plans, the two most restrictive universal regulations (EGPXAL28, EGTTCF28) were removed by 16:10, having affected 197 aircraft.

At the time the regulations were applied there were already the expected number of flights for a summer bank holiday in the air. Manual processing of flight plans was prioritised to provide information for these flights. As the regulations came into effect, they served their purpose of reducing

[2] This figure of 65,250 minutes has not yet been ratified by EUROCONTROL.

the number of flights in UK airspace to ensure that the ATC service remained safe. As a result, the number of aircraft in UK airspace was at its lowest between 15:00-16:00; the point at which the amount of flight plan information available for our controllers was most limited.

During the recovery to full operations phase, the 20 regulations applied collectively created 37,413 minutes of delay across 378 aircraft. All regulations were removed by 18:03.

Cancellations and Re-Routes

Due to the nature of ATC flight plan messaging regarding cancellations and flight plan modifications, it has not yet been possible to directly correlate all of these changes to the incident under investigation. This applies particularly to flight cancellations, which are determined by airlines and may be necessary for a number of reasons.

On 28th August 2023, EUROCONTROL data showed 5,592 flights (arrivals, departures and overflying) operated within UK airspace. This was 2,000 fewer (approximately 25% less) than the 7,536 flights that had been predicted by the NATS Analytics short term forecast. The 2,000 fewer flights will consist of a combination of cancelled flights and flights avoiding UK airspace.

Due to the timing of the FPRSA-R incident at 08:32, the majority of eastbound transatlantic flights were already airborne and as such were unable to be delayed or stopped. These flights along with other airborne long-haul arrival aircraft from outside the European Civil Aviation Conference (ECAC) area are deemed to be ‘out of area’ and therefore were not subject to the same level of restrictions as aircraft operating wholly within the ECAC.

Transatlantic Arrivals and Departures were therefore less affected with estimated cancellations of around 4%.

8. Steps Taken to Prevent Recurrence

a. Actions taken or underway to prevent the interruption recurring

As described already, the flight plan that led to the incident has never been encountered by the FPRSA-R sub-system for the 5 years it has been in live operation.

However, now that the exact circumstances that can give rise to the incident are understood a number of actions have been taken, and more are in progress, to prevent recurrence.

The actions already undertaken or in progress are as follows:

1. An operating instruction has been put in place to allow prompt recovery of the FPRSA-R sub-system if the same circumstances recur. Each of the technical operators have been trained to implement the new process. With enhanced monitoring in place, additional engineering expertise will also be present to oversee the activity.

2. The addition of specific message filters into the data flow between IFPS and FPRSA-R to filter out any flight plans that fit the conditions that caused the incident.

3. A permanent software change by the manufacturer within the FPRSA-R sub-system which will prevent the critical exception from recurring for any flight plan that triggers the conditions that led to the incident. This change will prevent the software from searching back beyond the entry waypoint into UK airspace and thus eliminate the possibility of finding a duplicate waypoint that could cause an incident. The software is expected to complete testing by the manufacturer and be delivered to NATS on Monday 4th September. The software will then be fully assured by NATS prior to deployment into the live air traffic operation overnight on 5th September.

9. Areas for Further Investigation

The severity of this incident led the NATS CEO to commission a Major Incident Investigation immediately. The major incident investigation was intended to focus on the events of 28thAugust. In particular, it was commissioned to find the root cause of the incident and to ensure that immediate action could be taken to prevent recurrence. Any incident of this nature provides NATS with an opportunity to review its response with a view to further improving resilience for the future. As a result, at the point of publication of this report many lines of enquiry remain ongoing. These include, but are not limited to:

1. The initial requirements specification of the software in the FPRSA-R sub-system.
2. The detailed design, coding, testing and validation of the FPRSA-R software by the manufacturer.
3. The NATS testing of the FPRSA-R sub-system when delivered in 2018.
4. The processes and procedures used to restore the sub-system for opportunities to speed up recovery, given the unusually long nature of the incident.
5. The feasibility of storing more than 4 hours of flight plans to further enhance the resilience of the system in the event of failure of automated processing of flight plans.
6. The processes and procedures used to manage the ATC operation, including the application of traffic regulations.
7. The processes and procedures used to activate and manage incidents of this type.
8. The effectiveness of communications with stakeholders, especially airlines, airports and ANSPs.
9. The feasibility of working through the UK state with ICAO to remove the small number of duplicate waypoint names in the ICAO administered global dataset that relate to this incident.

This Preliminary Report highlights the key issues identified to date and importantly provides prompt assurance that NATS' protocols and systems were effective to ensure that at no time was safety compromised. Furthermore, this report details the steps that have been taken to ensure similar levels of disruption will not occur again if the same flight plan or variations of it occur.

Our understanding is that following its review of this report, the CAA will decide what further areas it would like to examine. NATS would welcome any further independent oversight by the CAA. It is not within NATS' remit to address any wider questions arising from the incident such as cost reimbursement and compensation for the associated disruption; no discussion of this is included in this report or the ongoing NATS investigation.

10. Appendices

Appendix 1 – ADEXP File Extract 1: ICAO4444

ROUTE N0501F370 ORCKA5 LAS Q70 BLIPP Q842 WINEN DCT MLF J107 OCS
DCT CZI DCT DIK/N0495F390 DCT DVL DCT VBI DCT VESRU DCT YXL DCT
ELVEL DCT PIGLA DCT 58N070W DCT MIBNO/M085F390 DCT MAXAR/M085F410
DCT 62N050W/M085F410 62N040W 60N030W 58N020W/M085F410 DCT
SUNOT/N0497F410 DCT KESIX DCT APSOV DCT SOSIM L15 KEPAD L151 KIDLI
UN859 GWC/N0499F290 UN859 LGL A34 BOBSA/N0408F130

[F]

[C]

Appendix 2: ADEXP File Extract 2: Waypoints

```
-BEGIN RTEPTS
    -PT -PTID KLAX -FL F001 -ETO 230828031000
    -PT -PTID LAS -FL F370 -ETO 230828033939
    -PT -PTID IFEYE -FL F370 -ETO 230828034253
    -PT -PTID BLIPP -FL F370 -ETO 230828034540
    -PT -PTID WINEN -FL F370 -ETO 230828035557
    -PT -PTID MLF -FL F370 -ETO 230828035952
    -PT -PTID OCS -FL F370 -ETO 230828043005
    -PT -PTID CZI -FL F370 -ETO 230828045106
    -PT -PTID DIK -FL F370 -ETO 230828051747
    -PT -PTID DVL -FL F390 -ETO 230828053820
    -PT -PTID VBI -FL F390 -ETO 230828060246
    -PT -PTID VESRU -FL F390 -ETO 230828060910
    -PT -PTID YXL -FL F390 -ETO 230828061325
    -PT -PTID ELVEL -FL F390 -ETO 230828062350
    -PT -PTID PIGLA -FL F390 -ETO 230828071200
    -PT -PTID GEO04 -FL F390 -ETO 230828075624
    -PT -PTID MIBNO -FL F390 -ETO 230828082704
    -PT -PTID MAXAR -FL F390 -ETO 230828084300
    -PT -PTID GEO05 -FL F410 -ETO 230828090900
    -PT -PTID GEO06 -FL F410 -ETO 230828094200
    -PT -PTID GEO07 -FL F410 -ETO 230828101700
    -PT -PTID GEO08 -FL F410 -ETO 230828105300
    -PT -PTID SUNOT -FL F410 -ETO 230828111124
    -PT -PTID KESIX -FL F410 -ETO 230828111500
    -PT -PTID APSOV -FL F410 -ETO 230828113200
    -PT -PTID SOSIM -FL F410 -ETO 230828115653
    -PT -PTID GIGTO -FL F410 -ETO 230828115901
    -PT -PTID MALUD -FL F410 -ETO 230828120135
    -PT -PTID EPOXI -FL F410 -ETO 230828120224
    -PT -PTID AMPIT -FL F410 -ETO 230828120354
    -PT -PTID RISLA -FL F410 -ETO 230828120535
    -PT -PTID KEPAD -FL F410 -ETO 230828120754
    -PT -PTID TELBA -FL F410 -ETO 230828120906
    -PT -PTID VIDOK -FL F410 -ETO 230828121113
    -PT -PTID BRUMI -FL F410 -ETO 230828121128
    -PT -PTID PEPUL -FL F410 -ETO 230828121225
    -PT -PTID DISIT -FL F410 -ETO 230828121347
    -PT -PTID TUBSU -FL F410 -ETO 230828121403
    -PT -PTID NANUM -FL F410 -ETO 230828121425
    -PT -PTID NEDEX -FL F410 -ETO 230828121540
    -PT -PTID KIDLI -FL F410 -ETO 230828121633
    -PT -PTID DIGUT -FL F410 -ETO 230828121725
    -PT -PTID CPT -FL F410 -ETO 230828121833
    -PT -PTID ALHAD -FL F410 -ETO 230828121918
    -PT -PTID VAPID -FL F410 -ETO 230828122022
    -PT -PTID GWC -FL F290 -ETO 230828122326
    -PT -PTID GEO09 -FL F273 -ETO 230828122415
    -PT -PTID SITET -FL F270 -ETO 230828123000
    -PT -PTID ETRAT -FL F270 -ETO 230828123312
    -PT -PTID DVL -FL F265 -ETO 230828123608
    -PT -PTID LGL -FL F179 -ETO 230828124046
    -PT -PTID BOBSA -FL F130 -ETO 230828124335
    -PT -PTID LFPO -FL F003 -ETO 230828130415
-END RTEPTS
```

Devil's Lake, North Dakota, USA

[A]

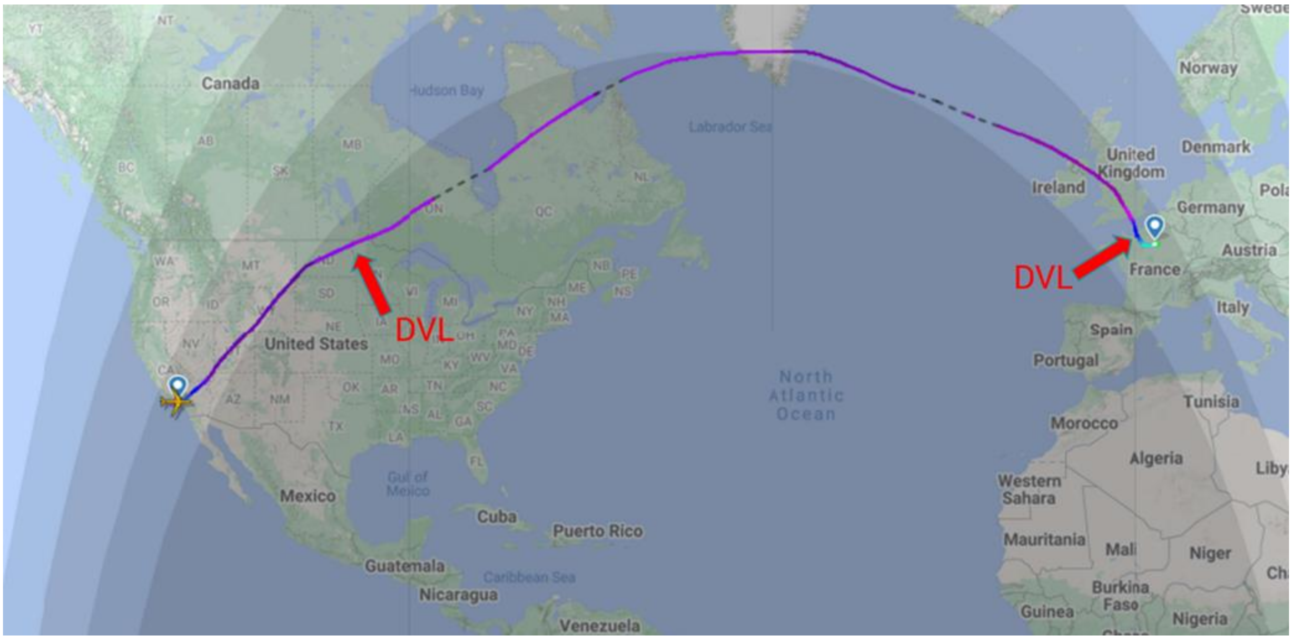
UK elements

[B]

[D]

Deauville, France [E]

Appendix 3: Flight FBU37M



Appendix 4:

Update on SAF013 Major Incident Report – July 2024

Following additional testing taken place in May and June of 2024 on the original as-delivered Frequentis Comsoft FPRSA-R software from 2018, new information regarding the evolution of the software has been established. The new information does not alter the conclusions and recommendations of the original investigation report and therefore does not warrant re-opening the closed investigation, it is important that this report contains all of the facts available.

Facts as Set out in the Report

Major recommendation Ma2 concludes that a line of software logic was omitted by Frequentis Comsoft in its initial delivery of the FPRSA-R software build in 2018. Had that software logic been included then the FPRSA-R system would not have entered maintenance mode and the 28th August incident would not have occurred. A subsequent urgent change request with Frequentis Comsoft introduced the missing code such that the issue could not recur.

At the time, the investigation team was made aware by NATS system engineers that there had been subsequent software change requests, including one for the initial implementation of Free Route Airspace (FRA) in 2021. However, the investigation team relied on Frequentis as the software experts to identify the source of the coding error and they were clear that the error was due to an omission in the initial 2018 FPRSA-R code, which was then carried through to all subsequent software drops following change requests, until the fix was applied after the incident.

Subsequent Additional Information established by the NATS Level Three FPRSA-R Engineer

In June of 2024 the Level 3 FPRSA SME recreated the full 2018 operational environment in the NATS simulator facility and retested the original 2018 FPRSA-R software build with the flight plan that caused the August 2023 incident. It was discovered that this version of the software was capable of handling the 28 August 'problem' flight plan by directing it for manual processing, while continuing automatic processing of subsequent flight plans i.e. FPRSA-R did not enter maintenance mode nor cease automatic flight plan processing. We escalated this discovery with Frequentis Comsoft software specialists who have now established that:

(a) The 2018 FPRSA-R build did not contain the appropriate coding logic to prevent a search for the UK airspace exit point before the UK entry point. To this extent, the new information matches what is described in the Report.

(b) However, unknown to NATS, the 2018 FPRSA-R build did contain a separate logic test that was capable of recognising that the output of the processing of the problem flight plan was nonsensical (because the UK airspace exit point preceded the UK airspace entry point) and hence directing it for manual processing. This separate logic test was not identified at the time the initial investigation was finalised as it was not in the software in use at the time.

(c) There were 2 subsequent change requests after 2018 in which this logic test remained in the FPRSA-R coding. But in 2021 there was a major change request delivered to facilitate the introduction of Prestwick Upper Airspace Free Route Airspace.

(d) That FRA related change request led Frequentis Comsoft to materially re-write the code related to searching for, and matching, airspace entry and exit points to NAS route pairs. The logic test referred to at (b) above was not included in the final version of the 2021 FPRSA-R software. Further, the software logic to prevent a search for the UK airspace exit point before the UK entry point (as set out in (a) above), was still missing from the 2021 FPRSA-R build. As a result of the absence of both the coding logic described at (a) above and the logic test described at (b) above in the final version of the 2021 FPRSA-R software, the software became susceptible to entering maintenance mode when it was asked to process a flight plan with the 6 specific attributes, exactly as identified in the Report.

Relevant Process and Testing

The NATS Engineering team has therefore subsequently applied the investigation processes that were initially applied to the 2018 software build, to the 2021 software build. That has involved reviewing the requirements for, and testing of the deliverable of, the 2021 build. That review, with the close co-operation of Frequentis Comsoft, has established that:

(a) The problem flight plan was not 'seen' by the 2018-2021 versions of the FPRSA-R system and so the probability of failure remains as quoted in the Report – 5 years of flight plans or approximately 15 million.

(b) NERL was aware of the significance of the 2021 change request in terms of the scale of the changes required pursuant to the introduction of the FRA requirements. The FAT and SAT tests were therefore equally as extensive for acceptance of the 2021 build as they were for the 2018 build. However, as established in the Report, NATS was not aware of the detailed changes to the software code and the 6 attributes did not arise in over 400,000 test flight plans successfully processed (or identified for manual processing) by the FPRSA-R system, including flight plans containing other variations of dual waypoint data.

(c) The software fix required for the 2021 build was exactly the same fix as required by the 2018 build and so the urgent fix installed after the 28th August still permanently fixes the issue.

(d) While it remains regrettable that the required software logic was missing, the requirements and testing responsibilities of NATS as user of the Frequentis Comsoft 2021 software did not extend to analysing and checking the actual code provided in the solution and so the fact that the logic was missing from the 2021 code as well as from the 2018 code does not highlight any need for further or different recommendations from those in Ma2 of the Report.

Conclusions and Next Steps

1. The review of these new facts and circumstances has not indicated any material inaccuracy or change to the findings or recommendations in the Report.

2. If these facts had been available to the investigation team at the start of the investigation they would have led to slight variations in the text of the Report and timetable describing the history of the FPRSA-R software and the logic error but would not change the nature of the omission by Frequentis Comsoft or the efficacy of the fix ultimately provided by Frequentis Comsoft.

3. Taking the above into consideration NATS has decided that it not necessary, nor a good use of time to rewrite any sections of the report at this stage, particularly since it has already been provided in final form to the CAA and the CAA's Independent Panel.

4. It is however, appropriate that the updated facts are appended to the report and that the CAA is made aware of them.