NATS Major Incident Preliminary Report

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

Immediate feeling!

If the people who put this together went to college to learn Safety Critical Systems... they should press for a refund!

TAKEN FROM NATS INCIDENT OF 12-12-2014

ES14. Two critical factors enabled this rapid fault detection and system restoration. First, the Lockheed Martin engineers (who had played a major role in the development of the code) in the UK and USA had secure real-time access to data logs, and thus contributed fully to the diagnosis of the Incident. Second, the NATS team at Swanwick, as exemplified by the ETIC, operates a collaborative culture, and their working is not hindered by organisational or commercial boundaries.

Well I'm sure that's all absolutely peachy! ...they should be much more aware of the impact of NATS failure & recovery!

Issued by:
NATS: 4th September 2023

Table of contents

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.

Wrong word surely?

operation

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.

The system is, by obvious conclusion we must draw... not resilient. It shuts itself down if its data is a bit rubbish!

3. Overview of NATS' Air Traffic Control System

3.1. 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.

3.2. 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.

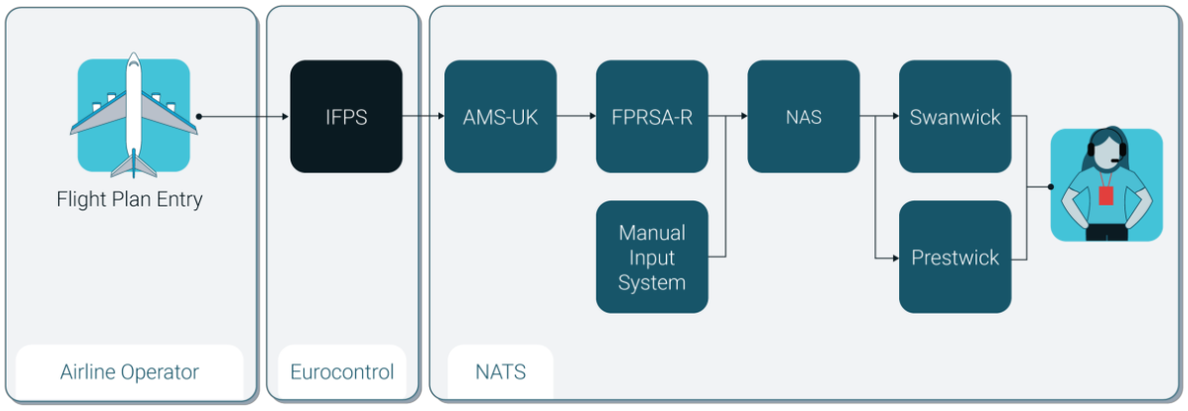
If the submitted flight plan is accepted by IFPS, i.e. it is compliant with IFPS defined parameters, it will inform the airline that filed the flight plan that it has been accepted. This is sufficient for a flight to depart with local ATC approval. The flight plan will be sent from IFPS to all relevant 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

4.1. 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 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 into Eurocontrol's flight planning distribution system, IFPS. The flight was planned to depart at around 04:00 on 28th August, and arrive at around 15:00. 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.

At 08:32 the flight plan 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 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.

The ADEXP waypoints plan included two waypoints along its route that were geographically distinct but which have the same designator.

What is a 'designator'? Why does this event precipitate a closure?

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.

So... why was duplication of such a 'designator' simply ignored by the IFPS/FPRSA-R interface?

[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. FPRSA-R was able to specifically identify the character string as it appeared in the ADEXP flight plan text.

Having correctly identified the entry point, the software moved on to search for the exit point from UK airspace in the waypoint data.

Having completed those steps, FPRSA-R then searches the ICAO4444 section of the ADEXP file. It initially searches from the beginning of that data, to find the identified UK airspace entry point. This was successfully found. Next, it searches backwards, from the end of that section, to find the UK airspace exit point. This did not appear in that section of the flight plan 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 the ADEXP file to search for the next nearest point beyond the UK exit point. This was also not present. The software therefore moved on to the next waypoint. This search was successful as a duplicate identifier appeared in the flight plan.

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. 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.

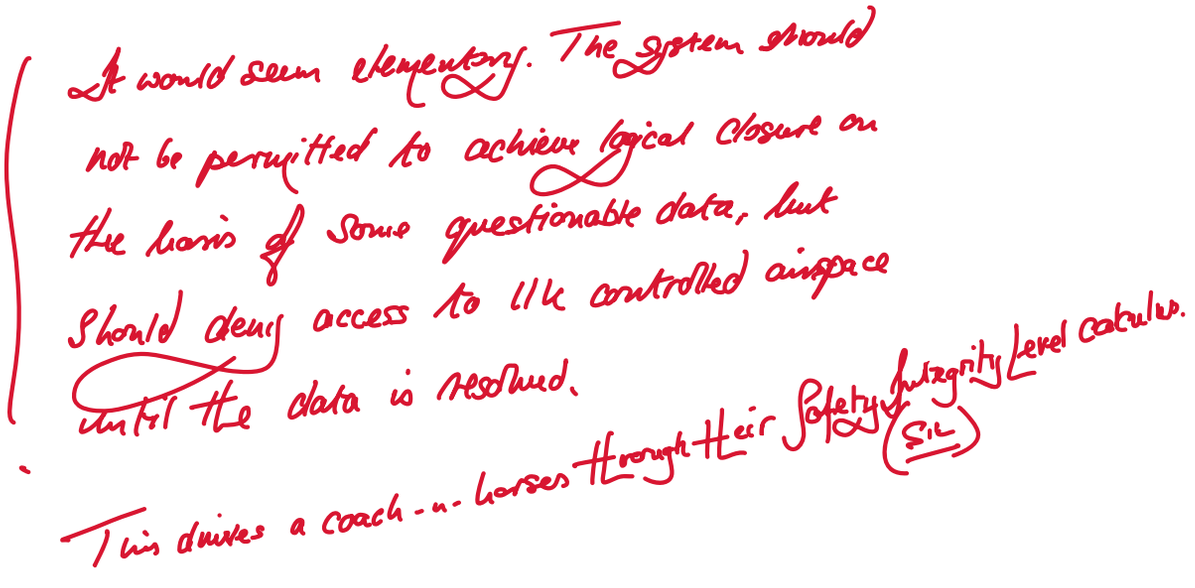
Therefore, on taking over the duties of the primary server, the backup system applied the same logic to the flight plan with the same result. It subsequently raised its own critical exception, writing a log file into the system log and placed itself into maintenance mode.

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 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

5.1. 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.

5.2. 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.

Why is the NATS computer blindly accepting flight plans?

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.

Well... the principal factor is that a system with high SRC & availability should NOT under any circumstances, foreseeable or otherwise... Stop!

The erroneous data should not be allowed to contribute to UK ATCOs work schedule with erroneous data.

A pre-process of verification might be efficacious? Can you imagine if a clearing bank just allowed erroneous data in the UK clearing processes, and then STOPPED... if something got through?!

6. Operational Recovery

6.1. 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.

6.2. 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

7.1. 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.

7.2. 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.

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

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 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 correlate directly 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

8.1. 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 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.

No! The System must be properly FAULT TOLERANT

It is amazing that this was previously allowed to operate with such toxicity!

CM

Well Yes! But....

What about a full review of all possible combinations and permutations of automatic flight plans... please!

REMOVE THE SHUT DOWN PROCEDURE... NOW!

Implement a process of constant reporting data confidence and graceful Service degradation... Now!

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 28th August. 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.