NATS Major Incident – August 2023:

Reflections on a Safety Critical System Incident

Computer Science
Dubai Campus

João Francisco Bianchi Labriola · H00411696

Air Traffic Control (ATC) is the activity of managing aircraft from the ground (Cambridge University Press, n.d.). The Flight Information Regions (FIR) covering the UK (*Figure 1*) is managed by the Civil Aviation Authority and NATS provides them with ATC services.

Figure 1. What is airspace? Source: NATS (n.d.).

The incident

According to NATS (2023), on August 28th, 2023, there was a major disruption in the UK airspace. NATS provides ACT services using multiple sub-systems, one being a flight plan processing sub-system called Flight Plan Reception Suite Automated – Replacement (FPRSA-R). The disruption roots from a flight plan containing two waypoints that were identically named, but geographically different causing FPRSA-R to raise a critical exception and entering fail-safe mode. The secondary system raised the same exception, leading to NATS systems being unable to process flight plans.

The disruption resulted in around 575 delays and the number of cancellations in the 28th of August exceeds 1500., in total 5,500 flights did not operate in UK airspace NATS(2023).

Actors, systems and their roles in the incident

Actors

NATS, considered the main actor in the incident provides ACT services for flights in UK airspace.

The Civil Aviation Authority (**CAA**) is the UK's aviation regulator which oversees NATS.

Eurocontrol is a pan-European, civil-military organisation dedicated to supporting European aviation.
Eurocontrol. About us. (2024). The organization oversaw the flight and system in control of sending NATS the flight plan which led to the incident.

Systems

C&M are Control and Monitoring backup systems. In the incident it was used once the primary FPRSA-R system failed. However, it resulted in the same exceptions.

The Integrated Initial Flight Plan Processing System (IFPS) is a centralised service of the Network Manager operations centre (NMOC) designed to rationalise the reception, initial processing and distribution of flight plan data related to instrument flight rules (IFR) flight within the ICAO EUR Region known as the IFPS Zone (IFPZ). Eurocontrol. (2024). IFPS sent the flight plan to NATS' systems ahead of the aircraft entering UK airspace.

FPRSA-R is a sub-system that 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) NATS (2023). This system received a flight plan from IFPS and searched for entry and exit points in UK airspace, finding the UK portion of the flight plan invalid, it raised a critical exception, stopping it from processing any flight plans, being the root of the incident.

Humans role in the incident

Air Traffic Controllers (**ATCOs**) are critical professionals in the aviation industry, responsible for the safe, orderly, and efficient movement of air traffic SKYbrary. (2024). They were the first line when the sub-system failed and provided support throughout the incident.

1st and 2nd line engineers monitor, maintain and underpin the delivery of the air traffic services, 24/7.

Technical Design Teams and sub-systems **manufactures**, played a major role. When 1st and 2nd line engineers were unable to detect the system failure, the teams and manufactures helped identify the cause and actions to restore the sub-systems.

NATS **CEO**, who launched the investigation of the incident.

London Terminal Control (LTC) **Operations Supervisor** (OS) who was submitted an MOR through the ATC operation, the morning of the incident.

Engineering Service Manager which submitted an MOR with a detailed overview on the incident.

An overview showing the end-to-end flight data processing information flow and highlights who manages the systems involved. NATS (2023).

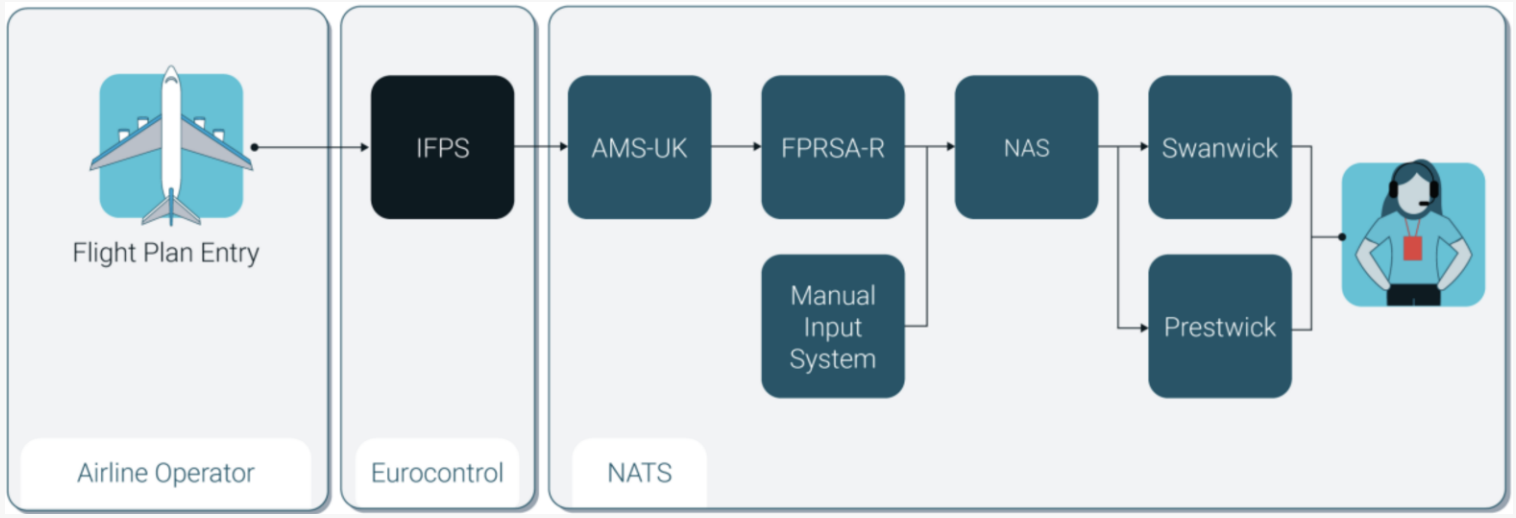
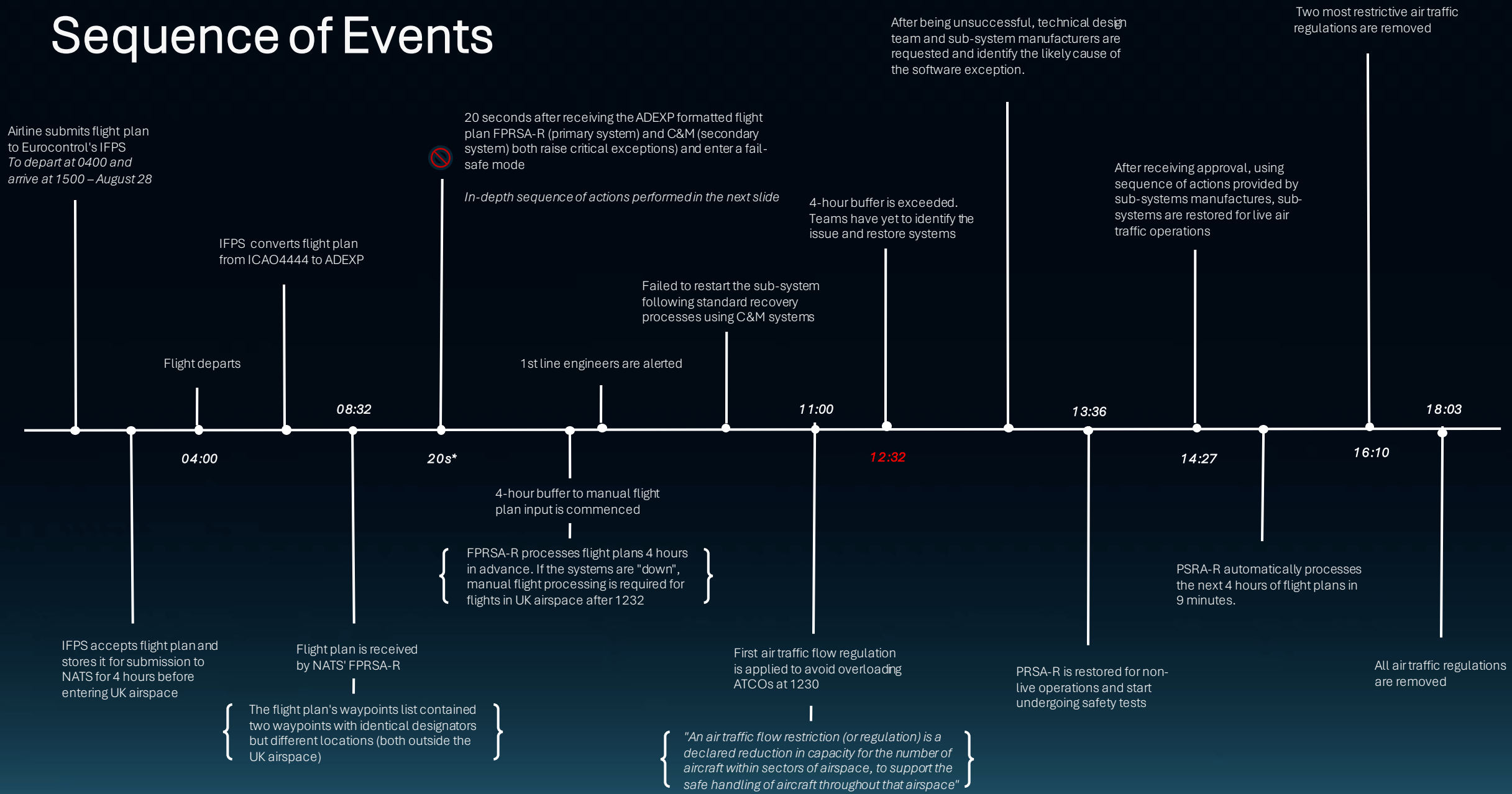


Figure 2. Source: NATS (2023).

Sequence of Events



The 20 seconds...

All the steps FPRSA-R underwent before raising a critical exception

FPRSA-R receives ADEXP formatted flight plan

System searches waypoint data list in flight plan for the entry point into UK airspace

System finds entry point

System searches list backwards, looking for a UK airspace exit point

Fails

System searches for nearest point beyond the UK airspace

"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"

System moves on to the next nearest FIR and finds a waypoint

The waypoint found is the present duplicate (waypoint before the UK airspace entry point) resulting in the UK portion of the flight plan being invalid.

"In the event the system cannot proceed in a demonstrably safe manner, it 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"

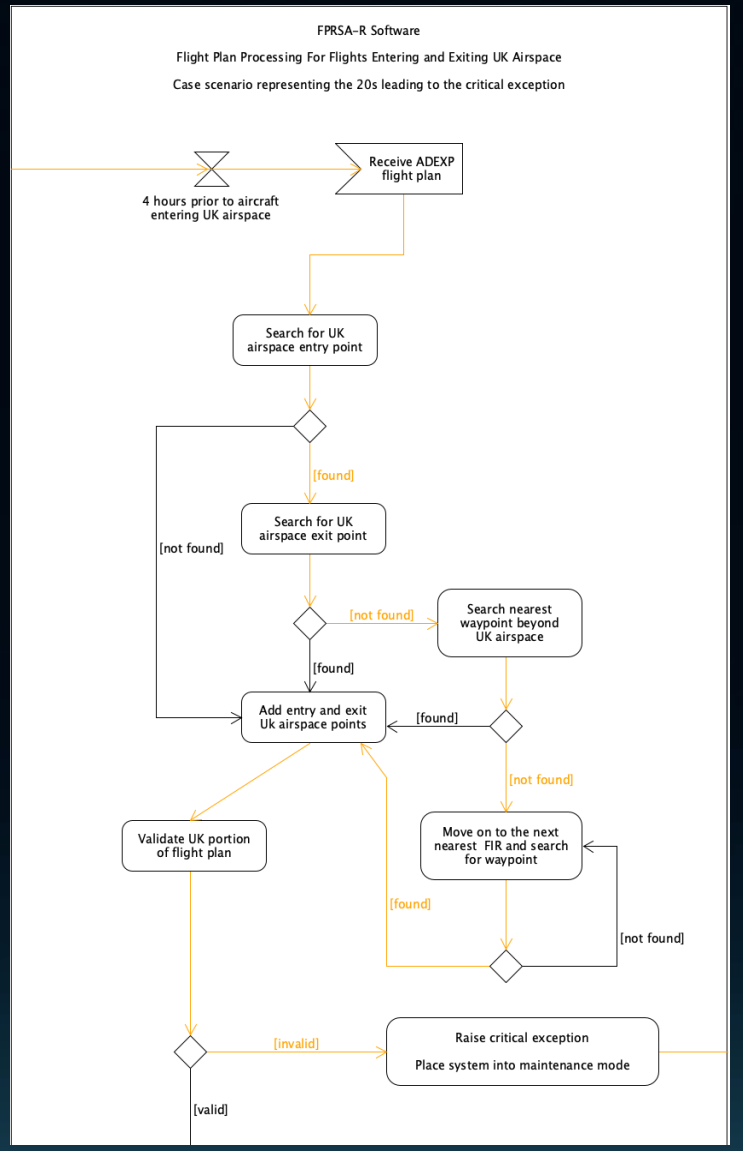
Writes log file to system and places itself into maintenance mode

C&M (secondary system) takes over and applies the same logic to the flight plan, resulting in a critical exception

The secondary system is backup system software is located on separate hardware with separate power and data feeds

FPRSA –R is no longer able to automatically process flight plans and requires manual intervention

20 seconds



Non-immediate plans and actions to recover

Following the events of August 28th NATS CEO immediately commissioned a Major Incident Investigation

An investigation was launched to further understand the reason the 4-hour contingency period was not sufficient

Further analysis was done on the reasons and factors that affected the time required for the recovery of sub-systems

ATC operations created a Mandatory Occurrence Report (MOR) to NATS' Safety Tracking and Reports System (STAR) on August 28th, and submitted it to the CAA at 1915, August 29.

Engineer also submitted an MOR at 0755, August 30, with a detailed overview of the FPRSA-R failure, the operations effect and aspects of the subsequent actions taken.

Preventing recurrence

The CEO launched an immediate investigation into the incident which found its causes.

NATS has introduced a new operational guideline to address any future issues with the FPRSA-R subsystem. Technical staff have received training on this updated protocol to ensure rapid response. Additionally, NATS has enhanced its monitoring systems and brought in extra engineering experts to supervise the process.

NATS has integrated targeted message filters to enhance the data exchange between IFPS and FPRSA-R, effectively removing any flight plans that could trigger the previously encountered issue.

Preventing recurrence

NATS set implemented a crucial software update from the manufacturer for the FPRSA-R subsystem to block a specific error linked to past incidents, particularly addressing issues with duplicate waypoints, which underwent NATS validation before its live deployment to enhance air traffic safety.

Martin Rolfe, CEO of NATS said: “Keeping the sky safe is what guides every action we take, and that was our priority during last week’s incident. I would like to reiterate my apology for the effects it had on so many people, including our airline and airport customers. Incidents like this are extremely rare and we have put measures in place to ensure it does not happen again" NATS 2. (2023).

Lessons

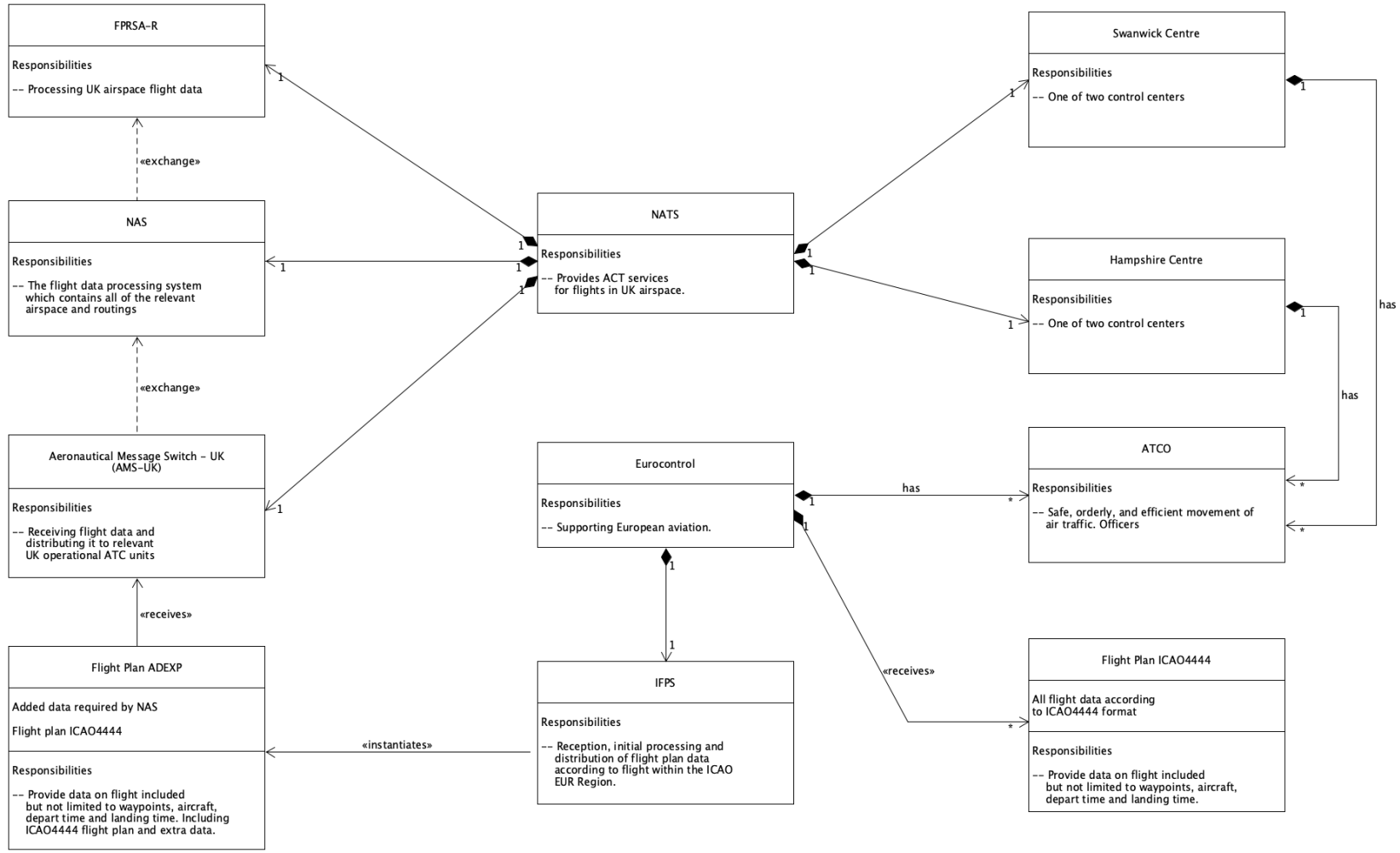
Firstly, it is important to note that this incident displays the complexity of software and systems engineering. The systems involved in the incident are highly complex and involve multiple actors, use cases, activities, safety and security issues.

It can be noted that this was a safety issue rather than security. The incident occurred due to an accidental fault in the software, rather than a malicious attack against it.

Lessons

A more robust FPRSA-R system could have mitigated the issue more gracefully, avoiding a critical failure. Achieving such resilience is challenging, yet aiming for less severe fail-states is a practical approach.

Software communication – the incident was significant due to extensive flight disruptions—thousands affected, hundreds delayed or canceled. This stemmed from both primary and secondary systems encountering critical errors and switching to maintenance mode, exacerbated by exceeding the four-hour contingency limit. Difficulty in diagnosing the issue by first and second-line engineers led to prolonged downtime. Enhanced error communication within the software could have expedited root cause identification and system restoration, thus reducing the impact on flights.



A high-level overview of the classes included in the incident and their responsibilities. In these scenarios there are dozens of actors, sub-systems, data information and responsibilities. This simplified class diagram aims to portray the main actors and their relationships

References

Cambridge University Press. (n.d.). *Air traffic control*. Available at: https://dictionary.cambridge.org/us/dictionary/english/air-traffic-control (Accessed: 6 April 2024).

NATS. (n.d.). Introduction to airspace. Available at: https://www.nats.aero/airspace/introduction/ (Accessed: 6 April 2024).

NATS (2023) . NATS Major Incident Preliminary Report (2023) . Available at: https://www.caa.co.uk/publication/download/20648 (Accessed: 6 April 2024).

SKYbrary. (2024). ATCO Licensing. Available at: https://skybrary.aero/articles/atco-licensing (Accessed: 6 April 2024).

Eurocontrol. (2024). Integrated initial flight plan processing system. Available at: https://www.eurocontrol.int/system/integrated-initial-flight-plan-processing-system (Accessed: 6 April 2024).

Eurocontrol. About us (2024). Available at: https://www.eurocontrol.int/about-us (Acessed: 6 April 2024).

NATS 2 (2023) . NATS report into air traffic control incident details root cause and solution implemented . Available at: NATS report into air traffic control incident details root cause and solution implemented - NATS (Accessed: 6 April 2024).