F28SD - INTRODUCTION TO SOFTWARE ENGINEERING - CW2

NATS MAJOR INCIDENT – AUGUST 2023

SHYAM SUNDAR VELMURUGAN
H00418621
DUBAI

OVERVIEW ABOUT THE INCIDENT

Name and date of incident:

NATS Major Incident
August 28, 2023.

Cause:

Software system failures, specifically the malfunction of the Flight Plan Reception Suite Automated (FPRSA-R) sub-system.

Impact:

Disrupted air traffic control processes, affecting flight plan reception and processing.

Sequence of Events:

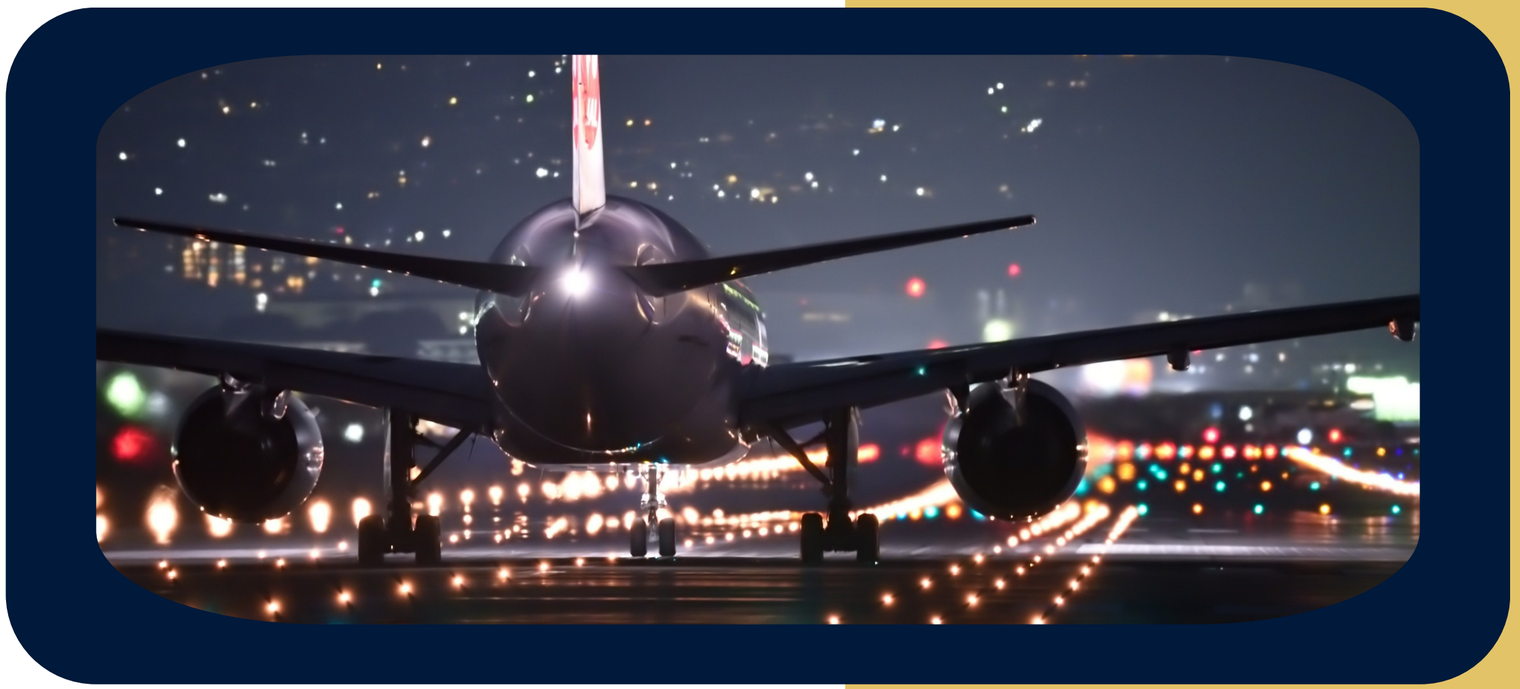
Technical failures within NATS systems hindered personnel's ability to manage air traffic effectively.

Analysis:

Examination of technical, operational, and human factors essential for understanding implications on air traffic control and passenger travel.

Immediate Response:

NATS personnel focused on recovery and mitigation efforts.



AIR TRAFFIC CONTROL (ATC)

-Air Traffic Control (ATC) ensures the safe operation of aircraft by monitoring and controlling their movements within controlled airspace.

-NATS, as the UK's Air Navigation Service Provider (ANSP), is responsible for ATC in most of the UK's airspace, prioritizing safety.

-ATC maintains safe separation between aircraft laterally and vertically, with en route services provided by regional control centers like NATS' facilities in Swanwick and Prestwick.

-Controlled airspace requires aircraft to adhere to Instrument Flight Rules (IFR) and file flight plans.

-ATC divides controlled airspace into sectors, with controllers overseeing aircraft within each sector.
Eurocontrol, based in Brussels, coordinates flight plans and ATC services across Europe.

Voice communications are done for two-way communication between ATCOs and pilots, and controllers and other ATC units.

Providing radar information to ATCOs.

Flight planning information to plan and coordinate traffic in each sector of airspace

Providing the radar display, flight information and ancillary information to ATCOs

Controlling and monitoring systems so that engineers are allowed to monitor and support maintenance/rectification as required

Data communications for the network connectivity and data exchanging

Time-distribution systems for providing the accurate time signals across systems

Flow management are the tools used for managing the controller workload.

- Operators, typically airlines, submit flight plans with essential details like aircraft type, speed, callsign, and route for traversing controlled European airspace.

- Flight plan data enables Air Navigation Service Providers (ANSPs) to plan and control aircraft movements safely.

- Eurocontrol's Integrated Initial Flight Plan Processing System (IFPS) serves as the central tool for managing these flight plans in Europe.

-Accepted flight plans by IFPS are distributed to relevant ANSPs, such as NATS in the UK, through systems like Aeronautical Message Switch – United Kingdom (AMS-UK).

- This process ensures efficient air traffic management and safe operations within controlled airspace.

Flight Plan Reception Suite Automated (FPRSA-R)

- The Flight Plan Reception Suite Automated (FPRSA-R) is integral to air traffic control infrastructure, especially within organizations like the UK's National Air Traffic Services (NATS).

- It functions as a software system designed to receive and process flight plans from airlines and other aviation entities.

- FPRSA-R automates the handling of flight plans, ensuring they are received promptly, accurately processed, and integrated into the air traffic management system.

- Malfunction or failure of FPRSA-R can lead to disruptions in air traffic control processes, potentially causing delays, rerouting of flights, and operational challenges.

- It plays a crucial role in coordinating aircraft movement by providing controllers with vital information such as planned routes, departure times, and aircraft specifications.

Within NATS En-route operations at Swanwick Centre, data is transmitted to the Flight Plan Reception Suite Automated (FPRSA-R) subsystem.

FPRSA-R's primary function is to convert data received from Eurocontrol's IFPS (in ADEXP format) into a format compatible with the UK National Airspace System (NAS), which contains all pertinent airspace and routing information.

In 2018, the previous FPRSA subsystem was replaced with new hardware and software developed by Frequentis AG, a leading global provider of Air Traffic Control (ATC) systems.

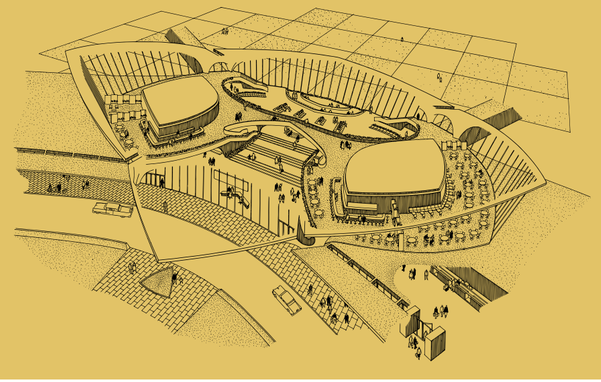
Frequentis AG's ATC products are widely used, operating in approximately 150 countries, and are recognized for their expertise in aeronautical information management (AIM) and message handling systems.

Since its introduction in 2018, the replacement FPRSA subsystem, now called FPRSA-R, has processed over 15 million flight plans without any prior incidents involving the loss of both primary and backup systems.

NAS then delivers flight data and relevant information to Air Traffic Control Officers (ATCOs) at their respective workstations, enabling them to effectively manage air traffic within their designated airspace.

SEQUENCE LEADING TO THIS INCIDENT

- Despite normal operation of the NATS Air Traffic Control (ATC) system, an incident occurred.
- No ongoing upgrades or critical system outages were reported.
- All backup systems were functioning, and standard monitoring procedures were in place.
- The issue originated when an airline submitted a flight plan compliant with ICAO regulations to Eurocontrol's flight planning system (IFPS).
- The plan was accepted and stored for submission to NATS systems, adhering to the standard 4-hour rule before the aircraft entered UK airspace.
- Upon receipt by NATS' Flight Plan Reception Suite Automated (FPRSA-R) subsystem, the flight plan was converted to ADEXP format.
- However, the ADEXP version contained two waypoints with the same designator but different geographical locations.
- Both waypoints were situated outside UK airspace, approximately 4000 nautical miles apart.
- Despite efforts to eliminate duplicate designators, they still exist globally, leading to regulations ensuring geographical distinctiveness.



- Upon receiving the ADEXP file, the FPRSA-R software initiated a search for the entry point of the flight plan in UK airspace and successfully located it.
- However, it failed to find the exit point within the designated UK airspace segment, as flight plans are not obligated to include an exit waypoint.
- The software then searched for the next nearest point beyond the UK exit point, which was also missing.
- Moving to the next waypoint, a duplicate identifier was discovered, leading to the software's inability to extract a valid UK portion of the flight plan and causing the incident.
- In such scenarios, safety-critical software systems are designed to transition into a state requiring manual intervention if they cannot proceed safely.
- The FPRSA-R subsystem raised a critical exception as it couldn't establish a safe course of action.
- Although preferable to identify and eliminate the problematic message for flight data accuracy, the system ceased operations to prevent incorrect data transmission to air traffic controllers.

After both the primary and backup FPRSA-R subsystems safely failed, the automatic processing of flight plans ceased, requiring manual intervention to restore normal operations.

This transition from automatic to manual processing took less than 20 seconds, marking the commencement of a 4-hour period where flight plans would be input manually.

The incident on August 28 was the first instance where both primary and backup FPRSA-R subsystems failed simultaneously, indicating that this specific combination of circumstances had never occurred before.

Despite operating continuously since October 2018 and processing over 15 million flight plans, this incident highlighted a unique scenario that hadn't been encountered previously.

Moving forward, further investigation is needed to examine the development and testing of the FPRSA-R subsystem to determine if measures could have been taken to mitigate this incident during the software development cycle.

The specific area of software related to this investigation is believed to be unique to NATS, according to the manufacturer.

LONG-TERM MEASURES

Promoting a culture where ongoing assessment and adjustment improve air traffic control operations, making them stronger and more adaptable.

For identifying and addressing threats in advance across the air traffic control system, a strong risk management system is implemented

For encouraging teamwork's and ensuring everyone is aware of the safety objectives, a stakeholder engagement program has been created.

Staff trainings and development programs are being invested for the betterment of the crisis management capabilities and the technical skills.

Developing contingency measures to maintain the functionality of essential components in the event of failures.

Setting up a program to examine problems and prevent them from occurring again.

Performing frequent checks to make sure that aviation rules and standards are being followed.

Creating a plan to use technology to reduce risk and enhance the performance of the system.

Enhancing monitoring and alert systems to catch problems early in the flight planning system for prevention.

Quickly investigating to find out what caused the incident and then applying the correct fixes.

Emergency response protocols have been revised for making incident handling and responding more effective

Offering specific training to employees so they can deal with technical problems swiftly.

Creating a straightforward communication strategy for our teams, those involved, and the public during incidents to keep everyone informed.

Creating a specialized team with defined responsibilities to help recover the system efficiently during incidents.

Finding weaknesses and areas to make better by checking for risks.

Looking at recent actions to see what was successful and what could be done better.

SHORT-TERM MEASURES

SOFTWARE ENGINEERING LESSONS

- Thorough testing and validation processes are essential in software engineering.

- Proactive measures are crucial to prevent incidents from escalating.

- Continuous monitoring helps identify and address potential issues early.

- Software reliability is paramount in ensuring smooth operations.

- Robust error handling mechanisms are necessary for system resilience.

- Comprehensive risk management strategies are vital in software development.

KEY NOTES TO BE TAKEN

- Work closely with software development teams to proactively identify and address potential issues before they escalate into incidents.

- Establish standardized terminology, structures, and procedures for identifying, classifying, and reporting incidents.

- Ensure that systems meet or exceed industry standards for speed and capacity to maintain optimal performance.

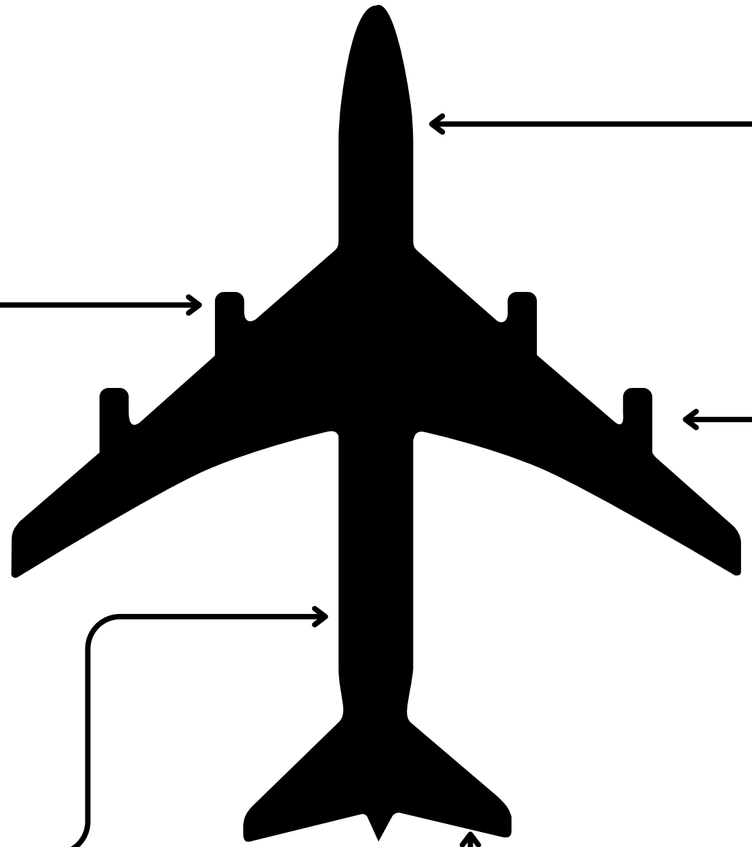
- Continuously update incident reports, action plans, checklists, and guidelines based on lessons learned from data analysis and documentation gathered during the incident response process.

- Foster a culture of open communication and feedback within the incident response team, valuing diverse perspectives and solutions.

In case of primary system failure, it's crucial to swiftly implement the backup or alternative plan to minimize time delays.

NATS must improve the process and learn from their mistakes as this incident shows how important it is to have a strong incident reporting process and analyzing the process for solutions

The FPRSA , ATC and other systems should be fixed and updated by NATS so that they are reliable for processing upcoming flight plans without any hinderance.



More stronger alert systems should be implemented for detecting the flaws and monitoring and working on the existing systems continuously for the betterment .

For setting any performance targets or better safety in future , NATS should review their performance with other peers and the lessons or mistakes of each incident must be taken in consideration and should be included into the framework

REFERENCES

https://vatix.com/blog/corrective-action-plan/

https://www.caa.co.uk/publication/download/21478

https://www.atlassian.com/blog/productivity/how-to-set-short-term-goals

https://aviationsafetyblog.asms-pro.com/blog/5-ways-to-stop-repeat-safety-incidents

https://www.iata.org/contentassets/47cf4788ca6c4968a07607c3202b9621/nats-report.pdf