NATS Major Incident – August 2023: Reflections on a Safety Critical System Incident

Calum Murray H00402826

Edinburgh Campus

Bsc (Hons) Computer Science

NATS Systems

National Airspace System - NAS

- Receives processed flight data.
- Provides information to ATCOs for safe management of air traffic.
- Uses ADEXP format to represent flight plans

Flight Plan Reception Suite Automated - FPRSA-R

- Converts IFPS flight plan data into NAS-compatible format.
- Vital for ensuring compatibility with UK airspace.
- Incident directly impacted this subsystem's functionality.

Control and Monitoring – C&M

- Oversees the operational status and performance of systems and sub-systems of NATS.

External Systems

Eurocontrol's Integrated Initial Flight Plan Processing System - IFPS

- Central flight planning tool for European airspace.
- Processes submitted flight plans.
- Interfaces with NATS and other ANSPs
- Uses ICAO4444 format to represent flight plans

Human Factors

Air Traffic Control Officers - ATCOs

Central flight planning tool for European airspace.

Processes submitted flight plans.

Interfaces with NATS and other ANSPs.

Air Traffic Service Assistants - ATSAs

Facilitates distribution of flight plan data within the UK.

Assists ATCOs.

24/7 available 1st and 2nd line Engineers/Technicians

1st line on-site.

2nd line contactable to provide more specialized support.

3rd line Engineers/Technicians from revelant suppliers/manufacturors

For when specific technical knowhow of specific systems are required.

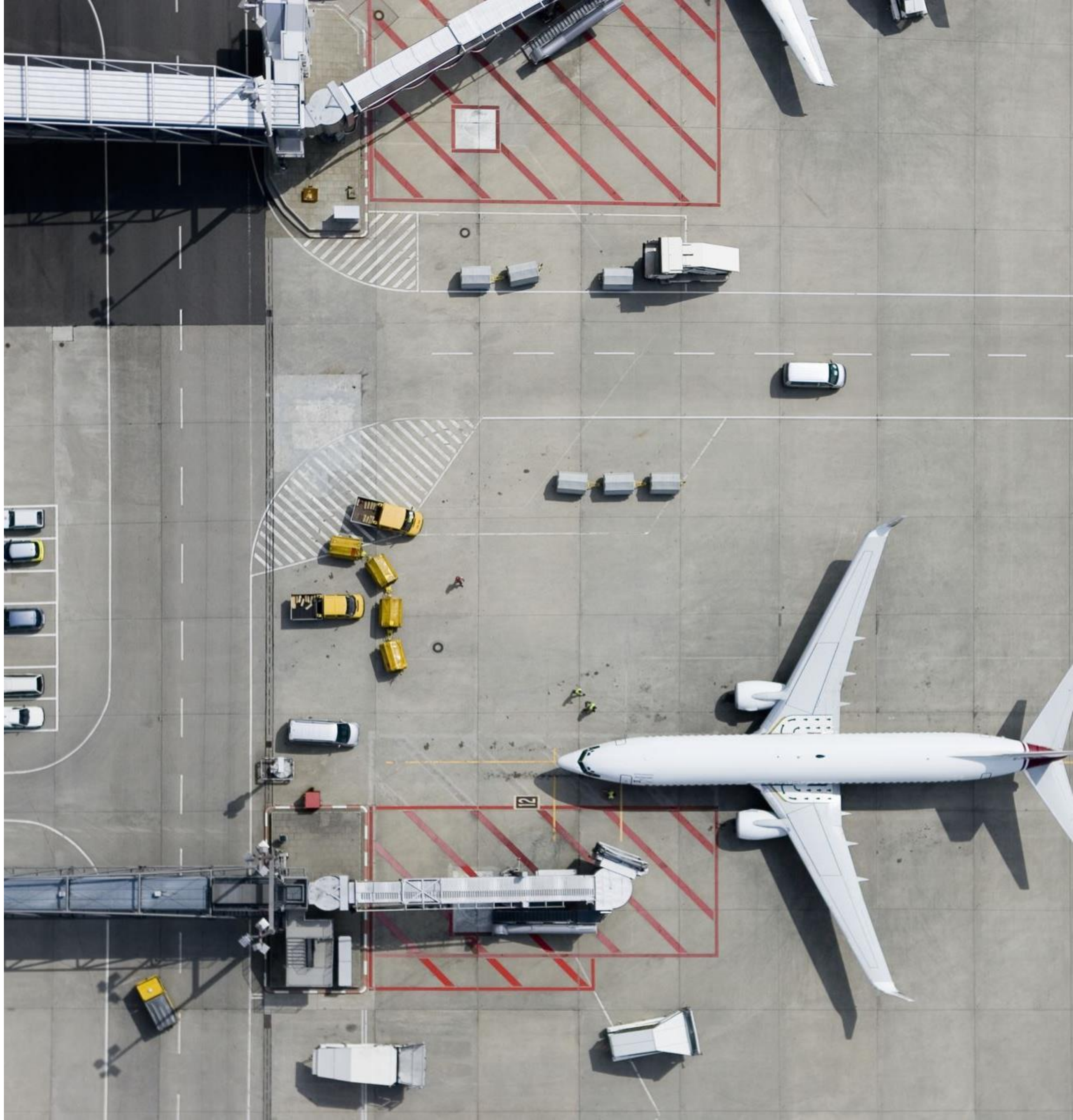
Events Immediately Preceding System Failures

Flight Plan Submission

- An airline submitted an ICAO4444 compliant flight plan to Eurocontrol's IFPS.
- Intended for departure at 04:00 on August 28.
- Flight plan was accepted and stored to be submitted to NATS when appropriate.

IFPS transfers flight plan to NATS' FPRSA-R system

- The flight plan is received at 08:32
- The FPRSA-R converts the flight plan from ICAO4444 format to ADEXP format (which includes additional geographical waypoints outside of UK airspace, required for previous and later sections of the journey)



System Failure

FPRSA-R attempts to process the flight plan

- As FPRSA-R is processing the flight plan, it encounters duplicate waypoint names.

Critical Exception is raised

- This means that after exploring all other exception handling option the issue wasn't resolved.
- The critical exception writes a log file into the system, then enters maintenance mode to prevent transmission of dangerous flight data.
- The C&M system then notices that the system is down.
- The backup system takes over, yet encounters the same error and enters maintenance mode as well.

Recovery Attempts

The 1st line engineers attempted a standard sub-system reset procedure.

Upon multiple failed attempts 2nd line engineers were called, with which they began a staged analysis.

Only after additional support was requested from the manufacturer, was the issue identified.

- **As the manufacturer accessed low-level logs, which illuminated the specific flight plan that caused the exception.**

The manufacturer then gave instructions to safely fix the system.

Immediate Aftermath

Air Traffic Flow Restrictions

- To ensure that ATCs were not overwhelmed during the manual processes, the number of aircraft allowed in each airspace sector was limited.

Flight Cancellations

- Hundreds of flights were cancelled on 28th August as a result.

Flights Disrupted

- Thousands of flights were otherwise disrupted.

Short-Term Prevention

Operator Training

- The operators of the systems mention have been instructed on how to resolve that problem should it reoccur.

Message Filters Implemented

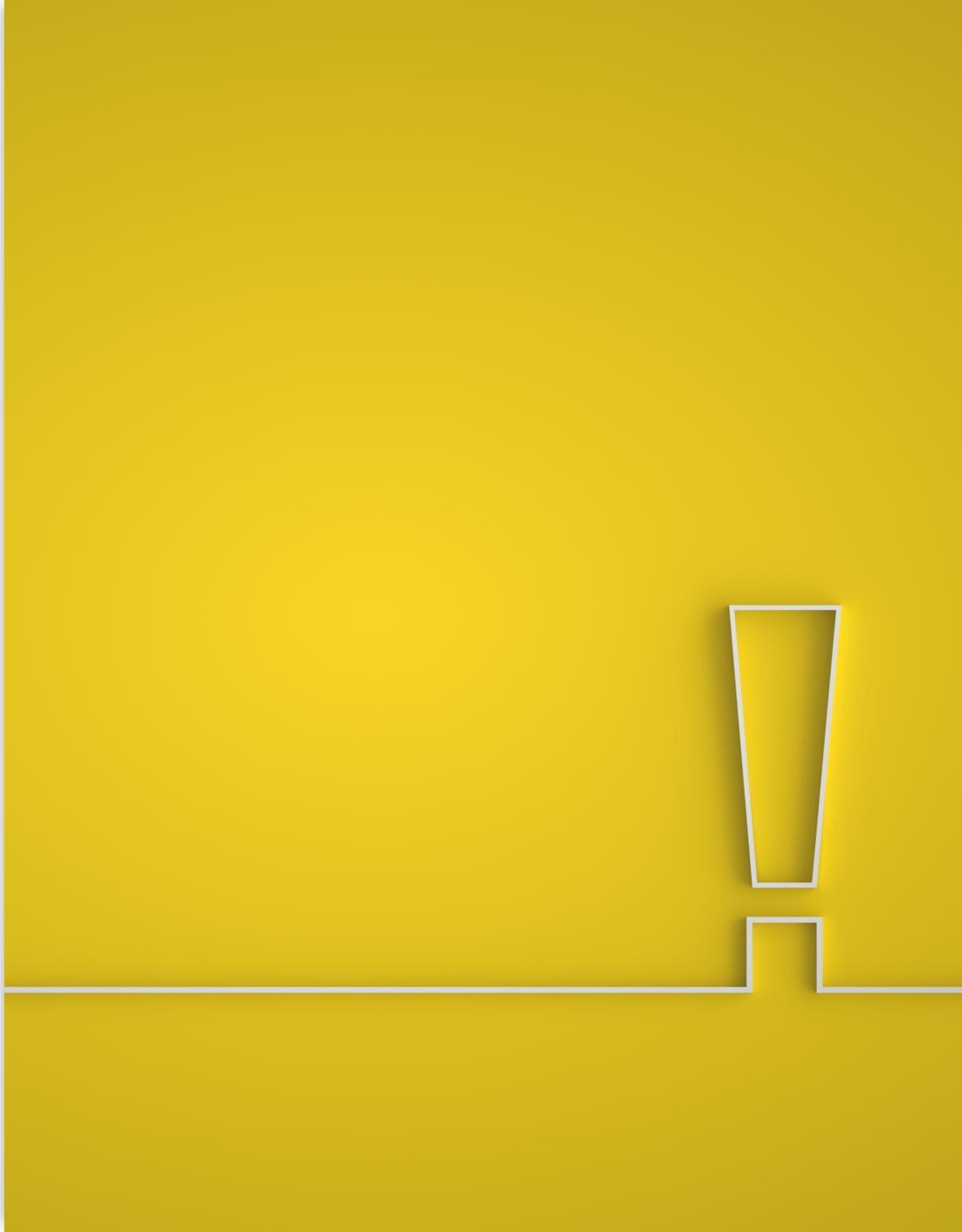
- Filters have been added to the flight plans transferred from the IFPS to the FPRSA-R.
- These are dsigned to identify and filter out any flight plans that would cause the same problem.

Long-Term Prevention

Permanent Change to the Software

- The manufacturer will fix the underlying software to address the root cause of the incident.

Considering the incredibly specific nature of the system failure, these prevention measures should be sufficient to prevent such an issue reocurring.



Lessons drawn from this incident

Thorough Testing

- This has highlighted the neccessity of thorough testing in the development of systems, especially edge case testing for duplicate inputs.

Safe Exception Handling

- This has emphasized the importance of robust error handling, as if no exception had been thrown dangerous flight plans may have been submitted.

Unique Identifiers

- When appropriate, unique identifiers for objects such as waypoints should be strictly applied.

Redundancy

- Back-up systems and error state control flows should be implemented to minimize singular points of failure, such as 1 invalid input.

Sources

- NATS Major Incident Preliminary Report: Flight Plan Reception Suite Automated (FPRSA-R)Sub-system Incident 28th August 2023. Issued by NATS 4th September 2023:
  - https://publicapps.caa.co.uk/docs/33/NERL%20Major%20Incident%20Investigation%20Preliminary%20Report.pdf
  - (also available via the "Additional Reading Material" module on Canvas)
- NATS introduction to Understanding Airspace:
  - https://www.nats.aero/airspace/introduction/
- AeroResource: AeroResource UK Waypoints map:
  - https://www.aeroresource.co.uk/resources/uk-waypoints-map/