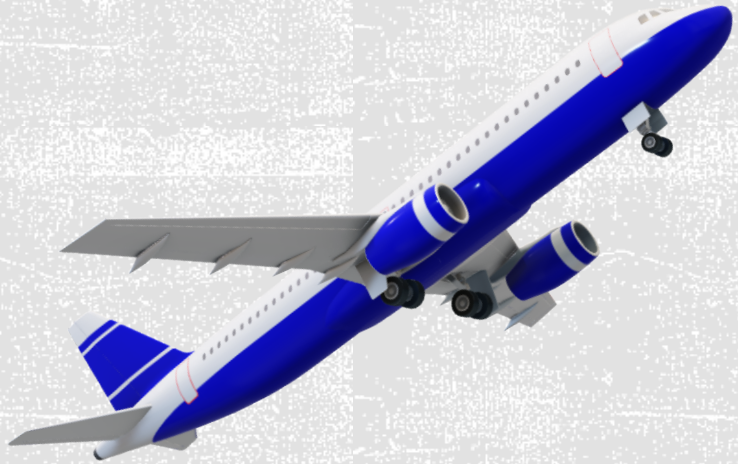
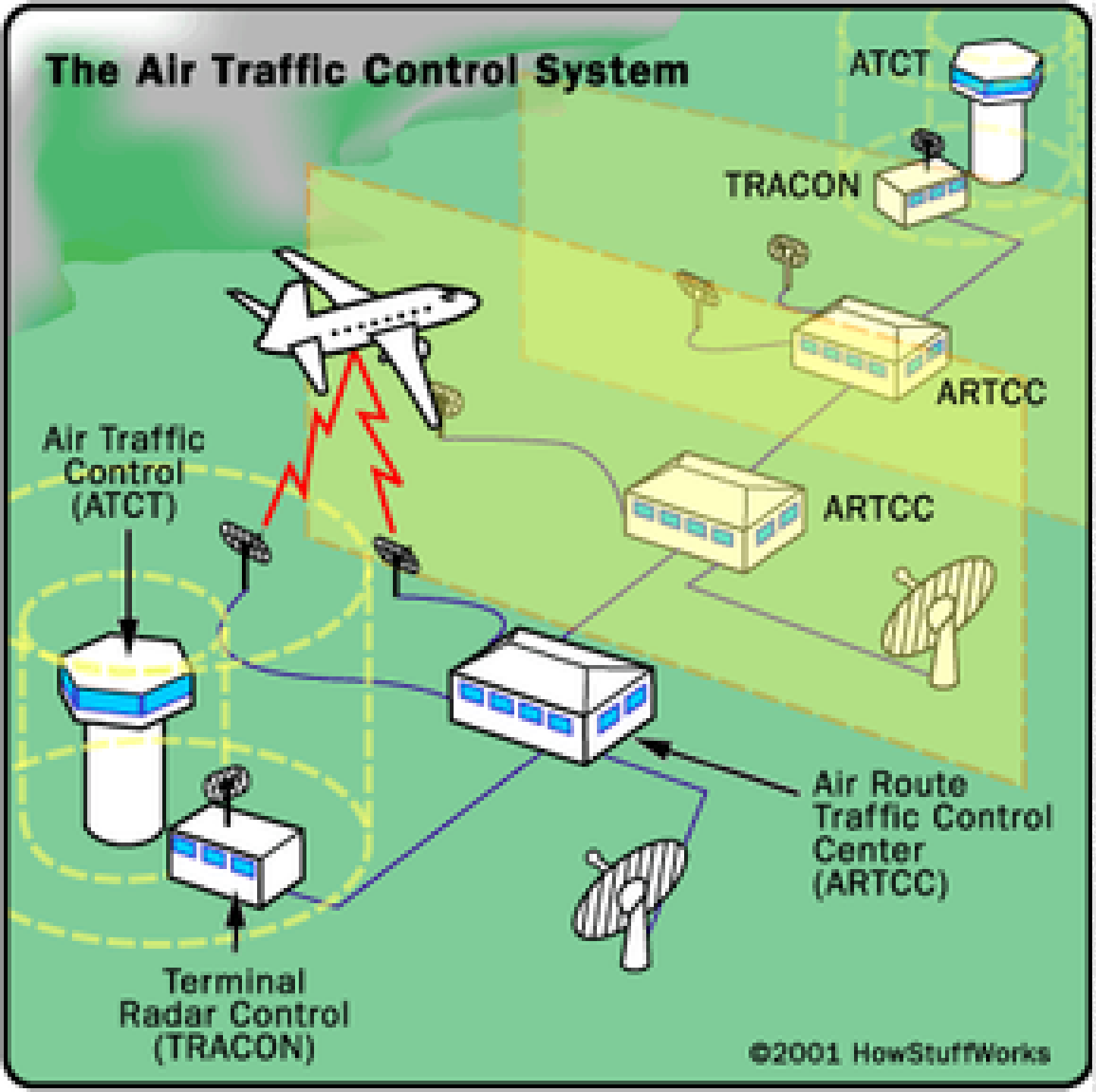
NATS MAJOR INCIDENT - AUGUST 2023: REFLECTIONS ON A SAFETY CRITICAL SYSTEM INCIDENT

- By: Zondwayo Mtine
- BSc Computer Science (Cyber Security)
- H00373945
- Heriot-Watt Dubai Campus



NATS OVERVIEW & ROLE

- NATS is a public-private entity, that holds the responsibility for UK's air traffic control.
- NATS manages UK's controlled airspace, ensuring safe and efficient air travel.
- The goal of NATS is to ensure Safe navigation of aircraft using state-of-the-art surveillance and communication technologies.
- They coordinate air traffic under IFR within controlled airspace, divided into geographical sectors.
- All flights must have a flight plan, which is usually managed by Eurocontrol for European airspace.



THE ROLE OF FLIGHT PLANS IN ATC

- FPRSA-R translates flight data from the Eurocontrol format into the UK's National Airspace System (NAS) format.
- This is critical for processing and translating Eurocontrol flight plans into the UK's National Airspace System (NAS) format.
- The incident in focus was triggered by a specific flight plan with duplicate waypoint names, causing system failure.
- Flight plans guide ATCOs in traffic management, critical for aircraft separation.
- FPRSA-R system, vital for translating Eurocontrol's data into the NAS format, underpins flight safety.
- Both primary and backup systems ensure continuity, with a 4-hour data storage for emergencies.

HUMAN ELEMENTS AND OPERATIONAL PROTOCOLS

- ATCOs manage flight safety and traffic flow, making crucial real-time decisions.
- ATSAs support ATCOs by managing flight data and communications, essential during manual operations.
- Established fallback procedures for maintaining air safety and managing traffic during system failures.
- Manual processes for entering flight data and coordinating flights ensure continuous safe operation.
- ATCOs and ATSAs form the core of operational safety, making critical decisions in real-time.
- Technical teams provide 24/7 system support, crucial for identifying and resolving system anomalies.
- Manual override capabilities exemplify the blend of human expertise and technological resilience.

PREPAREDNESS AND PROTOCOLS

- Fallback procedures illustrate NATS' preparedness for unforeseen events, ensuring air traffic management remains resilient and effective despite technological disruptions.
- Manual operations highlight NATS' ability to sustain control and guarantee safety, showcasing the vital role of human expertise when technology is compromised.
- The incident emphasizes the critical need for solid contingency planning and the agility to adapt swiftly, maintaining operational integrity under challenging circumstances

SYSTEM INTEGRITY AND INCIDENT ANTICIPATION

- Before the incident occurred, NATS' systems were performing efficiently and without any sign of errors, which showed the reliability of the system integrity and the high standards it conformed and maintained to.
- The structured approach to managing emergencies by NATS effectively minimizes operational disruptions, embodying a principle of continuous improvement and resilience in crisis management.
- The incident showed that even the most fail proof system are not perfect and perfectly demonstrated the unpredictability that come along with complex systems, which shows the need for contingency plans and various strategies ready to be adapted in a moment

THE TRIGGER EVENT

- On 28 August 2023, the FPRSA-R system's failure was triggered by an unusual flight plan, leading to significant disruptions across over 2000 flights.
- Early diagnoses pointed towards a faulty flight plan as the culprit, with suspicions focusing on an error potentially originating from a French airline, highlighting the interconnected risks within international air traffic operations.
- The incident emerged as a major operational and financial challenge for NATS, with the repercussions of the system failure leading to estimated cost surpassing £100 million, underscoring the extensive impact of such disruptions.

BREAKDOWN AND IMMEDIATE EFFECTS

- The disruption occurred as both the primary and backup FPRSA-R systems failed to handle a specific flight plan, showing that despite all the extensive maintenance and regular checks the system is not perfect and can be vulnerable especially in the system redundancy measures

- The need to use manual intervention, highlighted the system's design limitations, unable to segregate and manage the problematic flight plan without a full system halt.

- This costly error resulted in long delays and cancellations, the breakdown impacted the travel plans of hundreds of thousands of passengers, showcasing the far-reaching consequences of such system failures.

MANUAL INTERVENTIONS

- NATS' quick shift to manual processing of flight plans demonstrated a high level of emergency preparedness, underscoring their ability to adapt rapidly to maintain operational continuity.

- Even in the face of technological challenges, the integrity of safety and order in UK airspace remained uncompromised, highlighting the indispensable role of human expertise in crisis management.

- This incident served as a reminder of the crucial need for robust manual systems and protocols, which play a pivotal role in safeguarding continuous and safe air traffic operations.

DIAGNOSTICS AND COLLABORATIVE EFFORT

- Technical teams collaborated closely with the FPRSA-R system's manufacturer, using their combined expertise to swiftly diagnose and rectify the failure, demonstrating a proactive and technical approach to crisis resolution.

- The comprehensive incident report documented the sequence of events leading up to the failure, pinpointing the exact cause, thereby enabling a focused and effective response to prevent future occurrences.

- The concerted efforts to resume normal operations highlighted the critical importance of teamwork, collaboration, and specialized knowledge in navigating and overcoming crisis situations efficiently.

RECOVERY AND FUTURE MITIGATION

- In response to the incident, immediate actions were taken, including critical software updates and modifications to operational procedures, aimed at strengthening the system against similar future disruptions.

- A thorough system review conducted in the aftermath of the incident resulted in the implementation of improved protocols, more rigorous training for staff, and enhanced system resilience, reflecting a commitment to continuous improvement.

- The incident served as a catalyst for a deeper exploration of potential system vulnerabilities, leading to significant technological and procedural enhancements, thereby reinforcing the robustness of future response strategies.

SHORT-TERM ACTIONS: IMMEDIATE TECHNICAL REMEDIATIONS

- Prompt Recovery Instructions Implemented: A new set of operating instructions has been developed, equipping operators with clear guidelines for rapid recovery in similar scenarios, supplemented by comprehensive training and increased engineering supervision.

- Message Filtering Addition: To prevent recurrence, specialized message filters have now been installed between IFPS and FPRSA-R, designed to intercept and block any flight plans that exhibit characteristics like those that triggered the incident.

- Enhanced Monitoring: The system has been immediately upgraded with advanced monitoring capabilities, ensuring closer oversight and faster response times to identify and rectify potential threats or anomalies before they escalate.

SHORT-TERM ACTIONS: SOFTWARE MODIFICATIONS AND TESTING

- Permanent Software Change: The system has received a software update from the manufacturer that addresses and prevents the issue by managing and eliminating conflicts between duplicate waypoints, enhancing system stability.

- Rigorous Testing and Assurance: Before its integration into live operations, the updated software is subjected to exhaustive testing by its manufacturer and then undergoes NATS' stringent assurance process to ensure its reliability and effectiveness.

- Expected Deployment Schedule: The deployment of the software update is planned for rapid execution, with a clearly defined schedule outlining each phase of the rollout to ensure a smooth transition into active service without disrupting ongoing operations.

LONG-TERM ACTIONS: SYSTEMIC IMPROVEMENTS AND INVESTIGATIONS

- Software Development Cycle Review: A thorough review of the FPRSA-R sub-system's entire development lifecycle, from initial specifications through design, coding, testing, to validation, is underway to identify and implement potential enhancements for future robustness.

- Enhanced Recovery Procedures: Due to the extended recovery period experienced during the incident, an in-depth analysis of the restoration process is being conducted to identify opportunities for accelerating recovery times, ensuring quicker return to normal operations.

- Resilience Enhancement via Data Storage: Efforts are being made to assess the practicality of increasing the flight plan storage capacity beyond the current 4-hour limit, aiming to significantly enhance the system's resilience and operational continuity in face of unexpected disruptions.

LONG-TERM ACTIONS: OPERATIONAL AND COMMUNICATION ENHANCEMENTS

- Operational Management Review: An in-depth review of air traffic control (ATC) operation management, including the application of traffic regulations and existing incident management protocols, is being conducted to identify areas for efficiency and performance improvements.

- Stakeholder Communication Review: The effectiveness of communications with critical stakeholders, such as airlines, airports, and Air Navigation Service Providers, is under evaluation to enhance the clarity, accuracy, and timeliness of information exchange during incidents.

- Global Coordination for Waypoint Clarification: Efforts are underway to collaborate with the International Civil Aviation Organization (ICAO) and other global entities to resolve the issue of duplicate waypoint names worldwide, thereby reducing data ambiguity and improving navigational safety.

IMPORTANCE OF EXCEPTION HANDLING AND SYSTEM RESILIENCE

- Robust Exception Handling: The incident shows the necessity of designing systems with robust exception handling mechanisms that can isolate and manage unexpected inputs without halting operations of the overall systems.
- System Resilience through Redundancy: Having both primary and backup systems fail simultaneously highlights the need for more redundancy strategies, including diversified backup systems that aren't faulty to the same failure modes.
- Pre-emptive Problem Identification: The importance of identifying and addressing potential data anomalies through comprehensive pre-deployment testing and ongoing anomaly detection mechanisms.
- Fail-Safe Design Principles: Safety-critical systems must default to a safe state that requires manual intervention when automatic processes fail, making sure that safety is maintained even when the system cannot proceed normally.

SOFTWARE TESTING, VALIDATION, AND CONTINUOUS IMPROVEMENT

- Comprehensive Testing and Validation: The need for extensive testing that includes rare but possible scenarios, ensuring software can handle unexpected or non-standard inputs without critical failures.
- Continuous Software Improvement and Monitoring: The incident shows the importance of continuous monitoring, regular updates, and the willingness to adapt and improve software based on operational experience and emerging threats.
- Enhanced Communication Protocols: Effective communication channels between software engineers, operators, and third-party vendors are crucial for quick diagnosis and resolution of software issues.
- Global Coordination on Data Standards: Collaborating on international standards can prevent data ambiguities that lead to system failures, emphasizing the role of software engineering in global operational consistency.

REFERENCES:

- Haydon, J. (no date) The UK air traffic control crash, James Haydon. Available at: https://jameshaydon.github.io/nats-fail/ (Accessed: 1 April 2024).

- Milmo, D. (2023) UK air traffic control: inquiry into whether French error caused failure, The Independent, 28 August. Available at: https://www.independent.co.uk/travel/news-and-advice/flight-air-traffic-control-failure-nats-b2513127.html (Accessed: 1 April 2024).

- NATS (no date) Introduction to Airspace, NATS. Available at: https://www.nats.aero/airspace/introduction/ (Accessed: 1 April 2024).

- NATS (2023) 'NATS Major Incident Preliminary Report: Flight Plan Reception Suite Automated (FPRSA-R) Sub-system Incident 28th August 2023', 1(1), pp. 1-18. (Accessed 1 April 2024).