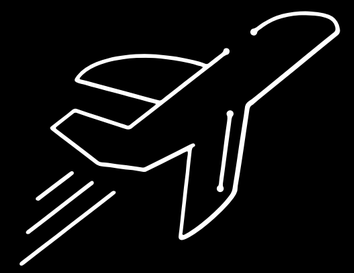
PRESENTATION ON A COMPREHENSIVE RESEARCH



Enhancing Aviation Safety

Human-Computer Interactions and Cyber Security in Next-Generation Aircrafts

Engineering Innovations for Safer Skies

Overview & Case Studies

NTSB statistics show that up to 83 per cent of all aviation accidents can be attributed to human error. Most often, pilots struggle to understand the information provided by their onboard sensors.

Being a major contributing factor in several high-profile crashes, it emphasises the importance of improving HCI in aviation.

Air Transat Flight 236 (2001)

Captain Robert Piché misinterpreted the unusual low oil temperature warning and blindly turned on the Cross-Feed valve, which in turn resulted in a state-of-the-art A330 with 306 people on board running out of fuel midway across the Atlantic Ocean.

Air France Flight 447 (2009)

The A330 plunged into the Atlantic Ocean killing all 228 people on board resulting from a combination of factors, including temporary inconsistencies in airspeed measurements due to pitot tube icing and the flight crew's misinterpretation of the stall situation, leading to an inappropriate response.

Asiana Airlines Flight 214 (2013)

A Boeing 777 crashed during landing at San Francisco International Airport, killing 3 people onboard and injuring nearly 200. The pilots mismanaged the aircraft's descent and failed to recognise the decreasing airspeed until it was too late.

https://artofflying.netlify.app/

HCI & Engineering Solutions

Reducing cognitive workload and providing tailored guidance during high-stress situations.

Onboard Sensor Systems

Flight Instruments, Navigation System, Engine and System Monitoring, Weather Radar and Sensors, TCAS, TAWS, FMCs, and FDs.

Challenges in HCI

1. **Complexity** in Modern Aircraft Systems
2. Information **Overload**
3. **Usability** Issues and Interface Design
4. Effective management of **automation** and **manual** control

Engineering Solutions

1. **Intuitive** Interface Design
2. **Prioritising** Critical Alerts
3. **Adaptive** Automation
4. Advanced Decision-**Support Systems**
5. **Change** in Training and Education

Cyber Security Threats in Avionics

Denial of Service: Avionics systems may be targeted by DoS attacks that overwhelm or incapacitate targeted systems, rendering them unable to function properly and causing disruptions to flight operations.

GPS and Navigation System Spoofing: Hackers may attempt to manipulate or interfere with GPS or other navigation system signals to mislead aircraft about their position, potentially causing disorientation, airspace violations, or even accidents.

Data Breaches: Confidential data stored on aircraft systems, such as passenger information or sensitive operational data, can be targeted by cybercriminals for identity theft, corporate espionage, or other nefarious purposes.

Malware and Viruses: Malware can be introduced through software updates, maintenance processes, or onboard systems such as in-flight entertainment. These threats could disrupt or impair the performance of critical avionics systems.

Unauthorised Access to Avionics Systems: Malicious actors may attempt to gain unauthorised access to aircraft systems or networks, potentially compromising their functionality or integrity.

Engineering Strategies for Enhancing Cyber Security

IMPLEMENTING ROBUST **DEFENSES** AND **BEST PRACTICES** FOR SECURE AVIONIC SYSTEMS

Hardware Security: **TPMs HSMs**

Secure Boot and Firmware Update

Intrusion Detection and Prevention Systems

Security Information and Event Management

Network Segmentation

Data Encryption

Personal Reflections & Lessons Learned

- Avionics System Architecture Design with a focus on Security
- Threat Modelling & Risk Assessment
- Security Testing Models

Effective Collaboration

Learning the value of interdisciplinary collaboration and clear communication among team members to address complex security challenges.

Balancing Security and Usability

Gaining insight into the importance of balancing security measures with usability and operational efficiency to ensure the successful adoption of secure avionic systems.

Incident response preparedness:

Acknowledging the need for robust incident response planning and execution to minimise the impact of cyber security incidents on aviation safety and operations.

Recap

1. **Enhancing Human-Computer Interaction:** Improve intuitive interface design, prioritise critical alerts, and implement adaptive automation.
2. **Strengthening Cyber Security in Avionics:** Incorporate robust defence measures, such as secure boot processes, data encryption, network segmentation, and hardware security.
3. **Future Approach:** Emphasise effective collaboration, balance security and usability, and prioritise incident response preparedness.

Do you have any questions?

Thank you for your valuable time and attention...