# Managing Aviation System Safety A Sofema Aviation Services White Paper

## Introduction

The future of aviation rests on the safe and effective integration of complex, interdependent systems—where human performance, technological advancement, and organizational resilience must harmonize.

As we embrace increasing levels of automation, advanced software, and artificial intelligence, we also face unprecedented challenges.

This white paper explores the essential considerations for managing aviation system safety, focusing on maintaining control over automation, keeping humans in the loop, and achieving system assurance across the entire aviation ecosystem.

## Maintaining Control Over Automation and Advanced Technology

**The Challenge of Automation Overload -** Whilst Advanced Flight Management Systems (FMS), Autoland functions, automatic flight controls, predictive maintenance systems, and even emerging AI-driven diagnostic tools have revolutionized the efficiency, precision, and safety of flight operations, they also introduce a subtle yet critical risk: the erosion of human engagement and situational awareness, leading to automation overload.

- Automation overload occurs when operators, whether pilots, maintenance engineers, or dispatchers, become so accustomed to system-driven processes that they begin to defer responsibility, relying on automation to manage tasks without fully understanding or questioning its outputs.
- The problem is not that automation itself is inherently unsafe, indeed, it has vastly improved aviation safety, rather that human operators are no longer as deeply engaged in the decision-making loop.
- As trust in automation grows, there is a tendency for operators to become passive monitors rather than active participants, leading to a phenomenon known as automation complacency.

**Safety Concerns -** This disengagement has profound implications for safety.

- Pilots may assume that an autopilot system is maintaining the correct speed and altitude, but if a sensor malfunctions or a mode is misunderstood then it may not be noticed until it’s too late.

- Automation overload also affects ground maintenance and operational support. Engineers may depend heavily on automated fault detection systems without fully understanding the diagnostic logic or potential blind spots.
    - When these systems generate ambiguous or misleading alerts, technicians may replace components unnecessarily or miss underlying root causes, increasing both maintenance costs and the risk of unresolved failures.

- Our human brain is not designed for passive monitoring over extended periods, sustained vigilance in low-activity environments typically leads to attention drift, reduced information processing capacity, and delayed reaction times (known as the vigilance decrement.)

- In high-stakes aviation environments, this decline in mental engagement can have catastrophic consequences when an unexpected event occurs and the operator must suddenly transition from passive observation to rapid, decisive action.

**Automation Overload Mitigations**

The goal is to foster a healthy relationship between humans and automation—one where automation supports human performance, but never replaces the need for engagement, oversight, and informed intervention.

- Training programs must emphasize manual flying skills for pilots
- Training programs to focus on diagnostic reasoning for maintenance teams
- All Training programs to promote critical thinking across all aviation roles.
- System designers must create interfaces that provide clear feedback, make system logic transparent, and involve the operator in critical decision-making processes.

**Case Study: Asiana Airlines Flight 214 – Automation Confusion and Lessons for Safer Flight Operations – (**H**uman-Centered Automation Design)**

**Introduction** The Asiana Airlines Flight 214 accident remains a landmark case in aviation safety, demonstrating the risks of automation complacency and the dangers of mode confusion. It serves as a powerful reminder that while automation has dramatically improved safety, it cannot replace the critical role of the human pilot in maintaining situational awareness and intervening when systems fail.

By learning from this tragedy, the aviation industry continues to adapt—designing safer systems, enhancing pilot training, and fostering a safety culture that prioritizes understanding, vigilance, and proactive intervention in the face of complex, automated environments.

**Background** On July 6, 2013, Asiana Airlines Flight 214, a Boeing 777-200ER, was on final approach to San Francisco International Airport (SFO) when it struck a seawall just short of Runway 28L, resulting in the deaths of three passengers and injuries to more than 180 others. The aircraft was operating a visual approach after a long trans-Pacific flight from Seoul, South Korea.

The accident investigation revealed a critical breakdown in situational awareness and a misunderstanding of automation behavior, highlighting vulnerabilities in the human-machine interface in modern flight decks.

**Key Contributing Factors**

**Misunderstanding of Autothrottle and Autopilot Interaction**

- The pilots believed that the autothrottle system would maintain the target approach speed even when the autopilot was disengaged.
- In reality, the autothrottle "HOLD" mode had disengaged, and the thrust levers remained at idle, allowing airspeed to decay below safe limits.
- The absence of clear feedback or warnings about the autothrottle mode change compounded the crew’s misunderstanding.

**Inadequate Monitoring and Situational Awareness**

- Both pilots failed to monitor airspeed and descent profile adequately, leading to the aircraft slowing well below the approach speed.
- Despite multiple cues, such as decreasing airspeed and increasing pitch attitude, corrective action was not taken in time to prevent a stall.

**Complexity of Automation Design**

- The interaction between autopilot, flight director, and autothrottle modes in the Boeing 777 was not intuitive, especially under high workload and visual approach conditions.
- The system did not provide an explicit, prominent alert when autothrottle disengaged due to the mode change.

**Training and Cultural Factors**

**Critical Note -** The pilots were accustomed to managed approaches using full automation. The visual approach with automation partially disconnected was outside their comfort zone, and the training system may not have adequately addressed scenarios involving partial automation failures or mode confusion.

**Lessons Learned**

The Asiana Flight 214 accident underscored several key lessons for the aviation industry:

- H**uman-Centered Automation Design is Critical -** Systems must be designed with clear feedback mechanisms and transparency to avoid "mode confusion." Critical changes—such as autothrottle disengagement—must be explicitly communicated to pilots through clear alerts, both visual and aural.

- **Enhanced Training on Automation Modes and Manual Flying Skills** - Pilot training programs must emphasize automation behavior, limitations, and recovery techniques. Scenarios involving partial automation disengagements, manual approaches, and non-precision approaches must be integrated into simulator training to improve pilot confidence and competence.

- **Active Monitoring and Cross-Checking as a Core Skill** - The accident highlighted the need for rigorous monitoring discipline during critical phases of flight. Flight crews must continuously verify speed, attitude, and power settings, even when automation is engaged.

- **Simplifying Automation Interfaces** - Manufacturers must consider reducing complexity in mode logic and ensuring intuitive system behavior. Features that can lead to hidden system states (such as "HOLD" mode) should be redesigned or mitigated with enhanced cues.

- **Cultural Factors in Flight Deck Communication -** The accident revealed potential deference to authority and hesitation to challenge decisions in multi-crew environments. CRM (Crew Resource Management) training must address assertiveness, encouraging pilots to speak up and intervene decisively when safety margins erode.

**Changes Introduced After the Accident**

Following the Asiana 214 crash, several safety initiatives and procedural changes were introduced across the industry:

- **Boeing's Software and Alerting Enhancements** - Boeing revised its guidance for 777 operators, emphasizing the limitations of autothrottle "HOLD" mode and the importance of manual thrust management during certain phases of flight. Boeing also worked on improving system feedback and updating training materials for better awareness of automation behaviors.

- **FAA and ICAO Training Recommendations** - The FAA and ICAO issued recommendations for airlines to strengthen manual flying skills and automation management training. Many operators have since introduced additional simulator scenarios that replicate partial automation failures and low-speed approaches.

- **Pilot Training Curriculum Revisions** - Asiana Airlines, and other carriers, updated their training programs to include more manual handling practice and automation failure scenarios. Emphasis was placed on monitoring skills and go-around decision-making.

- **CRM and Safety Culture Reforms** - The accident prompted a renewed focus on open communication in the cockpit, particularly between captains and first officers. Airlines enhanced their CRM training to address authority gradients and promote assertiveness in safety-critical situations.

- **Regulatory Reviews of Automation Dependencies -** The accident triggered discussions within regulatory bodies (including the FAA and EASA) on automation dependency in modern cockpits. Safety advisories were issued to encourage balanced use of automation and manual flying competence.

**Unintended Consequences:**

Automation logic often handles thousands of variables—far beyond what humans can track. However, when the logic is poorly understood, unexpected failure modes can emerge, especially during corner cases or unforeseen combinations of inputs.

**Case Study: Air France Flight 447 – Automation Masking and Loss of Situational Awareness**

## Introduction

The Air France Flight 447 accident is a profound example of how automation masking and system complexity can erode pilot situational awareness and decision-making. It reinforces the principle that while automation enhances safety under normal conditions, it must be designed to empower, not disempower, human operators during failures.

This tragedy catalyzed a global shift in pilot training, system design, and safety culture—one that prioritizes resilience in the face of uncertainty, manual flying competence, and an unbroken link between pilot, machine, and environment.

The legacy of Flight 447 serves as a powerful reminder: automation is a tool, not a crutch, and pilots must remain fully engaged, informed, and prepared to take control when needed.

## Background

On June 1, 2009, Air France Flight 447, an Airbus A330-200, disappeared over the Atlantic Ocean during a scheduled flight from Rio de Janeiro to Paris. All 228 people on board perished when the aircraft entered an aerodynamic stall from which it never recovered.

The tragedy, occurring at cruising altitude in clear air, shocked the aviation community and became a defining case in understanding the hidden vulnerabilities of automated flight systems and the critical role of human factors.

## Key Contributing Factors

### Pitot Tube Icing and Autopilot Disengagement

While flying through an area of convective weather, the aircraft’s pitot tubes iced over, resulting in unreliable airspeed data. The Airbus A330's design logic, in response, disconnected the autopilot and autothrust, shifting control to the flight crew in Alternate Law, a degraded flight control mode. The system provided limited visual or auditory warnings, masking the severity of the situation.

### Misunderstanding of System Behavior

The pilots did not recognize the aircraft was in a stall. Despite the stall warning activating 75 times, the crew misinterpreted the situation, believing they were in an overspeed condition. The lack of clear, intuitive feedback from the automation obscured the true state of the aircraft.

**Inadequate Manual Flying Skills at High Altitude**

The pilots, long accustomed to automated flight, were unprepared to manage a high-altitude upset manually. Their inputs—particularly excessive nose-up commands—exacerbated the stall condition. The inability to recover from an aerodynamic stall at cruise altitude demonstrated a gap in manual flying competence.

**Breakdown of Crew Resource Management (CRM)**

Communication and coordination within the cockpit deteriorated under stress. The first officer flying did not verbalize his actions, and the captain, upon returning from a rest break, struggled to grasp the situation. The crew lacked a shared mental model of the emergency.

**Lessons Learned**

The Air France Flight 447 disaster underscored the following critical lessons:

- **Transparency of System States is Vital** - Automation must be designed to provide clear, unambiguous feedback during failures. In complex, degraded situations, pilots must be able to quickly understand system status, identify failure modes, and make informed decisions.
- **High-Altitude Manual Flying Skills Cannot Be Neglected -** The accident revealed a gap in pilot training: manual aircraft handling in rare but critical scenarios, such as high-altitude stalls. Regular simulator training for manual flight under degraded conditions is essential to maintain competence.
- **Understanding of Automation Logic Must Be Integral to Training** - Pilots must thoroughly understand the logic, protections, and limitations of automated systems, especially under abnormal conditions. Misconceptions about system behavior (e.g., when protections are lost in Alternate Law) can have fatal consequences.
- **CRM Must Foster Shared Situational Awareness** - Effective cockpit communication is critical, especially during high-stress events. The breakdown of CRM on Flight 447 demonstrates the need for assertive communication, clear role delineation, and collaborative decision-making.
- **Design Should Minimize Hidden Failure Modes** - System designers must strive to avoid mode confusion and hidden failure states. When automation

disengages, clear and immediate alerts are essential to draw pilots' attention to critical tasks.

**Changes Introduced After the Accident -** In the wake of the AF447 tragedy, the aviation industry implemented several key changes:

- **Enhanced Pilot Training for Manual Handling** - Airlines and regulators mandated greater emphasis on manual flying skills, particularly upset recovery, high-altitude stall recovery, and flight without reliable airspeed indications. The Upset Prevention and Recovery Training (UPRT) program became a standard feature in pilot curricula globally.
- **Revised Procedures for Airspeed Discrepancies** - Standard operating procedures were updated to ensure rapid and correct responses to unreliable airspeed scenarios. Simulator exercises now routinely include pitot tube icing failures and transitions to Alternate Law.
- **Improvements in System Feedback and Design** - Manufacturers, including Airbus, reviewed flight deck interfaces to enhance feedback during critical failures. Efforts were made to ensure alerts are clear, timely, and actionable, reducing ambiguity in degraded modes.
- **Stronger Focus on CRM and Non-Technical Skills** - CRM programs were revised to emphasize assertive communication, cross-checking, and leadership in emergencies. The need for a shared mental model in the cockpit became a core theme in training.
- **Regulatory Oversight on Automation Reliance** - Authorities, including EASA and the FAA, issued guidance to reduce over-reliance on automation and ensure pilots maintain manual flying proficiency throughout their careers.

- **Loss of Human Skills -** The paradox of automation is that it reduces the need for manual operation, but this very reduction erodes operator skills—often referred to as "deskilling." When systems fail and manual intervention is needed, degraded human proficiency can prove fatal.

- **Risk Consideration** - Routine reliance on autopilot means that many airline pilots may not manually hand-fly the aircraft for extended periods. In a sudden, high-stakes situation—such as severe turbulence, crosswind landings, or unexpected system failures, this skill atrophy becomes a critical risk.

**Best Practices:**

- **Implement Robust Training Programs -** Training must focus not just on system operation but on failure mode recovery and manual reversion skills.
- Operators should regularly practice scenarios where automation fails, such as simulated autothrottle disengagement during takeoff, or autopilot disconnection during approach in marginal weather.
- Some operators now mandate periodic manual flying exercises during routine operations, such as requiring pilots to hand-fly the aircraft at least once per flight segment. Airlines like Cathay Pacific have incorporated such policies to maintain pilot handling proficiency.
- For maintenance personnel, simulation-based training that includes troubleshooting software-driven systems is essential, such as resolving discrepancies in avionics interfaces or handling ambiguous fault codes from integrated health monitoring systems.

**Automation Audits and Failure Mode Analysis:**

A formal Automation Hazard Analysis should be part of safety assurance activities. This involves systematically identifying and simulating edge-case scenarios where automation could behave unpredictably or fail silently.

- During the design of the Airbus A350's systems, extensive simulation testing was used to model interactions between flight control laws, auto flight systems, and pilot inputs under abnormal conditions
    - Such as dual engine failure at high altitude, or flight in turbulent wake conditions. This proactive analysis allowed the identification and mitigation of risks before certification.

- For operators, regular Line Operations Safety Audits (LOSA) can reveal situations where crews are over-reliant on automation, leading to targeted training or procedural changes.

- Design Systems for Transparency - Operators must have clear, intuitive feedback on the status, limits, and operational modes of automated systems. Human-machine interfaces (HMIs) should avoid "black box" behaviours where the system takes action without clear explanation.

The Airbus ECAM (Electronic Centralized Aircraft Monitor) philosophy provides structured, prioritized information to pilots during abnormal situations. It shows why the system is acting, what it has done, and what action is required by the crew.

- This design promotes shared situational awareness and facilitates faster, more accurate decision-making.

**Important Note for Comparison -** Boeing 737 MAX MCAS system failed in this regard, as pilots were unaware of its existence, its triggers, and its logic—highlighting the critical importance of system transparency.

**Maintenance Control Centers (MCCs)** should have real-time dashboards showing system health, with alerts for parameter deviations and potential failure modes—enabling proactive maintenance decisions rather than reactive interventions.

**Keeping the Human in the Loop**

Humans Are Often Removed from Real-Time Decision-Making as Systems Become More Autonomous:

- As aviation technology advances, there's a natural tendency to shift from human-led decisions to system-driven autonomy.
- While this can improve efficiency, it also displaces human operators from the critical decision-making process.
- Humans can become passive monitors rather than active controllers—leading to an "automation out-of-the-loop" problem.

In advanced aircraft like the Airbus A350 or Boeing 787, automated flight management and auto-thrust systems handle most flight phases. While this reduces workload, it also disengages pilots from active control.

- When sudden failures occur—like dual engine failure or unreliable airspeed—pilots must rapidly transition from passive monitoring to active control, often without sufficient mental readiness or system context.

**Reduced Engagement Can Erode Critical Thinking, Leading to Delayed or Incorrect Interventions:**

- When humans disengage from system operations, critical thinking and situational awareness decay.
- Operators become less practiced in cross-checking system performance, identifying discrepancies, or questioning unexpected behaviours.

- This can lead to confirmation bias, where pilots trust system outputs even when anomalies exist, or intervention delays during emergent failures.

**Qantas Flight 72 – Lessons Learned**

The Qantas Flight 72 incident remains a sobering reminder of how automation, while enhancing safety and efficiency, can introduce new risks—particularly when system behaviour becomes opaque or unpredictable. It underscored the importance of:

- Human resilience and the need for robust manual flying skills.
- The necessity of system redundancy and fault tolerance in critical systems like the ADIRU.
- The importance of continuous learning, both in terms of system design improvements and pilot training.

Qantas Flight 72 was an Airbus A330-303, operating a scheduled international service from Singapore to Perth with 303 people onboard. While cruising at 37,000 feet over the Indian Ocean, approximately 150 km from Learmonth, Western Australia, the aircraft experienced two uncommanded pitch-down events. Without warning, the autopilot and auto thrust disconnected, and the aircraft suddenly pitched nose-down, descending approximately 650 feet in around 20 seconds. A few minutes later, a second pitch-down event occurred, with the aircraft descending another 400 feet.

**The Technical Failure: A Faulty ADIRU**

The root cause was traced to a malfunction of one of the aircraft's Air Data Inertial Reference Units (ADIRUs), specifically ADIRU 1. The ADIRU, part of the aircraft's Air Data and Inertial Reference System (ADIRS), provides critical information such as airspeed, altitude, and attitude to the flight control systems.

ADIRU 1 intermittently generated erroneous data, particularly spurious high Angle of Attack (AoA) values. These incorrect signals triggered the aircraft's Flight Control Primary Computers (FCPCs) to believe the aircraft was in a stall condition, prompting automatic nose-down commands as part of the Airbus flight envelope protection logic. However, the aircraft was not actually in a stall—this was a false perception caused by faulty sensor input.

**Investigation Findings: System Vulnerabilities Exposed**

The Australian Transport Safety Bureau (ATSB) conducted an extensive investigation, concluding that the incident was primarily caused by:

- A failure within ADIRU 1, which generated a series of spurious and intermittent data spikes—including false AoA readings.
- The Airbus flight control system logic, which did not adequately filter or reject these erroneous data inputs, leading to repeated and inappropriate nose-down commands.
- The crew's inability to fully comprehend or mitigate the automated responses, given the lack of clear system feedback and the unpredictable nature of the faults.

The investigation raised serious concerns about single-point failures in critical flight control systems and the need for enhanced protections against false sensor inputs.

**Lessons Learned: Towards Safer Automation**

The Qantas Flight 72 incident sparked significant changes in both design philosophy and training priorities:

System Redesign: - Airbus implemented software updates to its flight control logic, introducing additional filtering and data validation layers to detect and reject spurious sensor inputs before they could trigger inappropriate flight control commands.

  - New safeguards were added to prevent single-point failures in systems like the ADIRU from compromising flight safety.

Crew Training Enhancements- The event highlighted the need for pilots to develop a deeper understanding of automation behaviour, system dependencies, and potential failure modes.

  - Emphasis was placed on manual flying skills and troubleshooting complex system anomalies under high-stress conditions.

Awareness of Automation Limitations - The incident reinforced the notion that automation is only as reliable as the data it receives. Human pilots must be prepared to intervene decisively when systems behave unpredictably.

  - The industry recognized the need to bridge the knowledge gap between system design assumptions and crew understanding in real-world scenarios.

**Design Interfaces That Promote Active Engagement:**

Human factors engineering must prioritize interfaces that encourage operators to actively monitor, question, and engage with system status. This means avoiding "silent" automation—where systems make decisions without notifying the user—and requiring explicit human confirmation for critical decisions.

- In modern fly-by-wire aircraft, systems like takeoff configuration warnings and engine mode selections require explicit pilot input, ensuring that critical actions—such as engine power settings or flap configurations—are deliberate.

- Similarly, in Maintenance Control Systems, fault isolation tools should provide progressive prompts, requiring engineers to validate each step rather than passively accept system-diagnosed faults.

**Incorporate Human-in-the-Loop Simulations -** Regular simulation exercises must replicate complex, multi-layered system behaviours to test how humans interact with automated systems under stress.

- Integrated scenario training develops mental models, reinforces decision-making, and builds resilience for unexpected system failures.
- For maintenance teams, simulated troubleshooting of integrated avionics systems—where fault codes interact across subsystems—helps technicians build diagnostic confidence and identify systemic errors rather than relying solely on automated maintenance messages.

**Ensure Human Operators Have Clear Authority and the Ability to Override Automated Systems Without Excessive Barriers:**

Achieving system assurance is not a one-time task it’s a continuous, integrated discipline. It requires a commitment to holistic safety thinking: understanding the relationships between humans, machines, and environments, and recognizing that system safety depends on more than just individual component reliability.

By applying rigorous assurance practices, engaging with cross-disciplinary expertise, and embedding cyber and human factors into every layer of the system, aviation organizations can build resilience into the heart of their operations.

System design must ensure that human operators retain ultimate decision-making authority. They must be able to interrupt or override automated actions promptly and without complex or hidden procedures.

**Achieving System Assurance: Human, Hardware, Software, Firmware, Logic, and Environmental Integration**

**Interdependency Blindness -** Modern aviation systems are highly integrated and interdependent—an aircraft is no longer a collection of standalone components but a network of interconnected systems.

- Failure to consider how these systems interact can create hidden vulnerabilities that only emerge under specific combinations of failures or environmental conditions.

- Software Complexity - As aviation systems increasingly rely on software and embedded logic, ensuring complete, robust testing becomes exponentially more difficult. Software logic may exhibit emergent behaviours that are not explicitly programmed, especially when interacting with multiple inputs across subsystems.

**Cyber Threats and System Integrity:**

The growing connectivity of aircraft systems, such as through satellite communications, Wi-Fi, and integrated maintenance networks, increases the attack surface for cyber threats. Without a robust assurance framework, it's difficult to maintain system integrity in the face of both inadvertent and malicious inputs.

- In 2019, the FAA issued a cybersecurity alert for Boeing 787 aircraft, warning that certain onboard systems could be vulnerable to external network connections. The integration of flight-critical systems with broader networks (e.g., maintenance or passenger services) raises concerns about data integrity, potential interference, and malicious exploitation.

**System Assurance Best Practices:**

- Develop a Holistic System Assurance Framework - Effective assurance requires a multi-dimensional approach that encompasses hardware, software, firmware, human factors, and environmental considerations. This means moving beyond component-level compliance to a system-wide, end-to-end validation strategy.
- The EASA Certification Specifications for Large Aeroplanes (CS-25) emphasize integrated safety assessments like the Functional Hazard Assessment (FHA) and System Safety Assessment (SSA).

- These require manufacturers to analyze how failures propagate across the system, considering crew workload, environmental factors, and interaction with other systems.

For operators, a Safety Management System (SMS) must include oversight of contracted organizations and suppliers to ensure that system assurance extends beyond the immediate organization.

**Implement Multi-Layered Validation and Verification (V&V) -** No single test or assessment can guarantee system safety. V&V must include a range of strategies, such as:

- Simulation of failure modes and system interactions
- Human-in-the-loop testing to understand real-world decision-making
- Stress testing under extreme environmental conditions
- Code reviews and static analysis for software safety

**Integrate Cyber Safety and Cyber Security into Safety Cases -** Modern system assurance cannot separate cyber threats from overall safety. Safety cases must explicitly consider cyber vulnerabilities, mitigation strategies, and residual risks.

**Account for Human Factors and Environmental Influences -** True system assurance must embrace variability—from human performance under stress to environmental extremes. Systems must be designed and tested to accommodate the full range of operational contexts.

Consider an avionics system that integrates terrain awareness, weather radar, and autopilot inputs. Assurance testing must simulate scenarios like:

- Rapid weather changes affecting radar returns
- Unexpected pilot inputs during turbulence
- Delayed sensor data under degraded satellite communication links

**Applying System Safety, Software Safety, Cyber Safety, System Reliability, Logistics, Availability, Human Factors, and Survivability**

Aircraft like the Boeing 787 have sophisticated electrical systems designed for efficiency, but this introduces complex failure modes where power distribution, software

control, and hardware health are deeply interwoven. A focus on efficiency and weight reduction without fully addressing failure scenarios can lead to latent safety risks.

**Challenges - Siloed Thinking and Compartmentalization:**

- A critical challenge in aviation system safety is the tendency to treat disciplines in isolation—system safety in one corner, cyber in another, human factors elsewhere.
- This fragmented approach creates blind spots, as interactions across domains—such as how a software fault can affect flight control or how logistics delays impact system availability—are not adequately addressed.

**Competing Priorities -** Balancing safety, reliability, performance, and cost is inherently complex.

- Under operational pressures, there's often a temptation to optimize for availability or cost at the expense of robust safety assurance, or to prioritize new features over cybersecurity hardening.

**Emergent Risks in Complex Systems -** Complex systems exhibit behaviours that cannot always be predicted by examining parts in isolation. Interactions between software, hardware, humans, and the environment create emergent risks that may only become visible during rare scenarios or cascading failures.

**System Safety Best Practices:**

EASA's Part-21 Safety Assessment Process mandates that design organizations provide integrated safety justifications, considering not just failure rates, but also human error probabilities, cyber risk exposure, and logistical supportability over the aircraft's lifecycle.

- **Adopt a Unified Safety Strategy -** Safety must be viewed as an integrated system property, not a collection of isolated checks. This means developing a holistic safety case that addresses:
- **System Safety Design:** Ensuring design meets functional hazard assessments and mitigates known risks.
- **Software Safety:** Verifying software logic, code integrity, and fail-safe behaviours.
- **Cyber Safety & Cyber Security:** Embedding protections against malicious actions, ensuring system integrity and resilience.

- **System Reliability:** Designing for redundancy, graceful degradation, and robust recovery pathways.
- **Logistics and Availability:** Ensuring spare parts, tools, and support systems are in place to maintain operational continuity.
- **Human Factors:** Designing for the limitations, capabilities, and cognitive load of humans.
- **Survivability:** Building systems that can withstand failures, attacks, and environmental extremes without catastrophic outcomes.

**Embed System Safety into Design Processes:**

Integrated Modular Avionics (IMA) on Airbus and Boeing platforms require software partitioning and strict validation to ensure that a non-critical function (e.g., cabin lighting) cannot interfere with a critical system (e.g., flight controls).

These design principles protect against unintended interactions and maintain safety even in degraded modes.

Proactive design reviews must address how safety requirements flow down into every subsystem. This includes:

- Applying FTA (Fault Tree Analysis) and FMEA (Failure Mode and Effects Analysis) across hardware and software.
- Using STPA (System-Theoretic Process Analysis) for complex, socio-technical systems.
- Validating safety integrity levels (SIL) for software in critical control functions.
- Designing fail-operational / fail-safe modes that prioritize human survivability over system functionality.

**Integrate Cyber Risk into the Safety Case -** Cyber threats must be treated as safety hazards. This means:

- Mapping cyber-attack vectors into fault trees and risk assessments.
- Incorporating cyber testing into validation protocols.
- Ensuring secure supply chains for software and hardware components.

The FAA's and EASA's guidance on Aircraft Systems Information Security Protection (ASISP) emphasizes that cybersecurity is not separate from safety—it is a fundamental aspect.

- For instance, an unauthorized modification of software affecting flight-critical systems is as much a safety issue as a hardware failure.

**Design for Survivability:**

- Systems must not only function during normal operations but survive adverse events—including failures, cyber intrusions, and extreme environmental conditions.
- Account for Logistics and Availability in Safety Planning:
    - Safety is not just about design—it's about sustaining safe operations. This means
    - Ensuring spare parts availability for time-critical systems.
    - Maintaining calibrated tools and qualified personnel.
    - Planning for obsolescence management of hardware and software components.

**Designing Systems to Accommodate Humans**

Challenges - Systems Often Reflect Technical Priorities Rather Than Human Capabilities:

In many aviation systems, design decisions are primarily driven by technical performance, regulatory compliance, or cost efficiency—while the human operator's cognitive and physical limitations are overlooked. This creates usability barriers that can undermine safety, leading to operational errors, delays in response, or failure to act appropriately in critical situations.

- The classic mode confusion problem in Flight Management Systems (FMS) illustrates this challenge.
- Pilots may struggle to determine exactly which automation mode is active—whether the system is controlling speed, altitude, or heading—and how it will respond to future inputs.
    - This ambiguity can lead to incorrect assumptions, delayed interventions, or contradictory inputs.
    - The design prioritizes complex system capabilities but fails to present information in a way that aligns with human mental models.

- Human Limitations (e.g., Stress, Fatigue, Distraction) Are Not Always Adequately Considered:

- Aviation environments are inherently high-stress and high-stakes. Yet, systems are often designed as if operators will always be attentive, calm, and rational.
- In reality, fatigue, workload spikes, and distractions can degrade human performance leading to lapses, misjudgments, or omitted actions.

**Apply Human-Centered Design (HCD) Principles from the Earliest Stages of System Development:**

Designing systems to accommodate humans is not just about user-friendliness—it is a safety imperative. By respecting human cognitive and physical boundaries, we reduce the likelihood of error, enhance system resilience, and empower operators to make better decisions under pressure.

HCD ensures that systems are designed around human capabilities and limitations rather than expecting humans to adapt to machines. It involves early involvement of end-users in design discussions, iterative prototyping, and validation of usability under realistic conditions.

- **Conduct Human Factors Integration (HFI) Studies -** HFI studies assess the cognitive, physical, and environmental interactions between humans and systems. This means understanding how operators perceive information, process it, make decisions, and act—especially under stress or fatigue.

EASA Human Factors Certification Requirements (e.g., CS-25.1302) mandate that design organizations assess how human performance is affected by factors such as lighting, noise, vibration, and ergonomics. For instance, the placement of cockpit controls and displays must support quick and accurate access under turbulent conditions, while maintenance task design must consider reachability, tool compatibility, and line-of-sight.

HFI studies in aircraft design may explore scenarios such as:

- Cognitive overload during multiple simultaneous alerts.
- Physical strain when accessing components in tight spaces (e.g., avionics bays).
- Environmental stressors such as heat, vibration, or glare in maintenance areas.

**Build in User Feedback Loops to Refine Systems Based on Operational Experience:**

- Continuous user feedback is essential to identify unanticipated challenges and improve system design iteratively.
- Feedback mechanisms should be formalized, such as through post-incident reviews, routine surveys, and user observation programs.

**Recognizing Failure as Inevitable: Designing for Safe Failure and Human Monitoring**

**Challenges-** Systems Can Fail, Humans Can Make Errors, and Complexity Increases Risk:

- No matter how advanced or well-designed, systems are not infallible. The more complex a system becomes—combining automation, software, hardware, and human interaction, the greater the likelihood that unexpected interactions, latent design flaws, or human errors will lead to safety events.

**Example Note for Reference -** The crash of Air France Flight 447 exposed the cascading effect of a relatively minor system failure (pitot tube icing) triggering multiple automated system failures, compounded by pilot confusion and lack of manual flying proficiency. The system's complexity masked the failure's root cause until it was too late.

- **Failure Modes Are Often Only Discovered in Operation, Leading to Reactive Safety Measures:**
    - Despite best efforts in design and testing, certain failure modes emerge only in real-world use, under specific combinations of factors that were not fully anticipated during development.

**Example Note for Reference -**The Boeing 737 MAX MCAS incidents revealed a fundamental gap in system safety assurance. The reliance on a single sensor input, without adequate pilot information or redundancy, became apparent only after operational experience exposed its vulnerabilities—prompting a global grounding and reactive system redesign.

**Design Systems to Fail-Safe, Ensuring Failures Default to the Safest Mode Possible:**

Failure is not a hypothetical risk—it is an operational certainty. The question is not if systems will fail, but when and how. The key to aviation safety lies in designing systems that anticipate failure, isolate its effects, and allow humans to recover safely.

A fail-safe design philosophy ensures that when systems fail, they do so in a way that minimizes risk to human life and the overall system. This may involve reducing functionality to essential operations, locking out hazardous commands, or defaulting to stable states that allow time for human intervention.

- Aircraft fuel systems are designed to fail towards shut-off rather than uncontrolled flow.
- Fly-by-wire systems—like those on the Airbus family—are built with laws of control that degrade gracefully: if certain systems fail, the aircraft reverts from Normal Law to Alternate or Direct Law, maintaining control authority even in a degraded mode.
- For maintenance systems, an engine control unit (ECU) might revert to a limp-home mode in case of a sensor discrepancy—allowing continued safe flight to a diversion airport rather than complete shutdown.

**Enable Early Detection, Isolation, Correction, and Recovery:**

- Modern systems must incorporate advanced diagnostics, self-checks, and redundancy to detect anomalies before they escalate into safety-critical failures. The sooner a problem is identified and isolated, the greater the chance of safe recovery.

**Equip Human Operators with the Tools and Data Needed to Detect Anomalies and Intervene Effectively:**

- Humans remain the final line of defense. For operators to act decisively, they must have clear, timely, and actionable information, not a deluge of raw data or obscure error codes. Systems must prioritize relevant alerts, provide unambiguous indications of failures, and offer pathways for intervention.

**Conclusion**

The safe management of aviation systems in the 21st century demands a proactive, integrated approach that acknowledges both human and system limitations. At Sofema Aviation Services, we advocate for a safety-first mindset—one that embraces human

factors, system assurance, cyber resilience, and survivability as interconnected pillars of aviation safety.

By designing for failure, empowering humans, and ensuring systems are transparent, explainable, and adaptable, we can build a future where aviation safety is not left to chance but is a deliberately engineered outcome.

**Next Steps**

Sofema Aviation Services www.sassofia.com and Sofema Online www.sofemaonline.com provides Classroom, Webinar a Online Training offering a combined 1000 Regulatory Compliant & Vocational Training Courses