LOSS OF CONTROL: AN INHERENT FRONTIER FOR MANAGING RESILIENCE?

John Stoop[1] and Jan de Kroes[1]

[1]Kindunos Safety Consultancy Ltd

Spijksedijk 8, 4207GN Gorinchem, the Netherlands

stoop@kindunos.nl

Abstract

The contribution highlights one of the most challenging discussions on whether or not a proactive approach in complex, open and dynamic systems is possible. If pro-action is not possible, only a reactive approach remains, leaving researchers to investigating emergent properties in practice. Loss of control in aviation can be considered an inherent property if analysed simultaneously along lines of design, control and practice. Analysis from a systems perspective reveals the actual, factual, critical and potential change triggers, agents and drivers which enable sustainable intervention, dealing with the inherent characteristics of the system at all control levels. The contribution clarifies challenges in the translation across disciplines and life cycle phases as well as the transition from an event factor approach to a system vector approach. Such a transition makes the concept of resilience accessible for designers and change agents and strengthens the credibility of the notion of resilience. Selection of the Loss of Control function in aviation also indicates that a failsafe system is not likely to exist at the level of socio-technical and socio-organisational systems due to their characteristics as an open, global network configuration with delegated and distributed responsibilities. Reconsiderations at the level of notions and paradigms seem inevitable.

1 INTRODUCTION

This contribution elaborates on the development of devices that are designed to control an inherent risk of flying with potentially catastrophic consequences: stall. The tragedy with AF447 and several subsequent events have served as a wakeup call for the aviation industry to deal with a type of accident that had disappeared from the agenda. A combination of automation applications and envelope protection seemed to have tackled the phenomenon to an acceptable low level of occurrence. Based on these triggering events, multiple analyses into the causes of upset recovery have been performed, suggesting a variety of remedies to tackle the issue. Many of these solutions focus on conventional engineering, education or enforcement strategies, assuming a one to one relation between cause and solution. These strategies have reduced the stall phenomenon to an acceptable low frequency event with a high recovery potential. However, stall is a phenomenon in a highly complex and dynamic operating environment in a socio-technical systems context. Such a phenomenon can only be perceived from a combined scientific, technological and societal perspective. Exploring the potential of adaptivity and resilience engineering has revealed new solutions, covering several patents and innovations. Ultimately, this approach has materialized in a preliminary design of a water bomber aircraft.

From the early days of aviation, stall has been an inherent hazard. Otto Lilienthal crashed and perished in 1896 as a result of stall. Wilbur Wright encountered stall in 1901, flying his second glider. Stall is a condition in which the flow over the main wing separates at high angles of attack, reducing the airplanes capacity to gain lift from the wings. Stall only depends on the angle of attack, not on airspeed. Airspeed is used as an indirect indicator for approaching stall conditions. Stall speed varies depending on weight, altitude, and configuration. Many devices have been developed to postpone stall, reduce its severity or to improve recovery. Any yaw of the aircraft entering stall may result in autorotation, that may develop into an almost irrecoverable ‘flat spin’. Stall recovery is possible by training appropriate manoeuvres as a part of basic flying skills. If applied correctly, a nose down position and increasing power until smooth air flow over the wing is restored leads to a small loss in altitude. Some fixed wing aircraft configurations are more susceptible to stall because turbulent airflow may blanket control surfaces at the tail. At low altitude the dangerous aspect of stall is a lack of altitude for recovery. At high altitude, the small margins between minimal and maximum airspeed are referred to as the

'coffin corner'. In contrast with most military aircraft, civil aircraft do not have excessive power to thrust vector an aircraft through the stall flight region.
During low speed conditions, aircraft are sensitive to stall due to the ratio between drag and power. This flight condition is caused by the fact that induced drag is a by-product of the generated lift. At high angles of attack the lift vector contains a considerable rearward component, increasing the induced drag with increasing angle of attack. Such drag cannot be compensated by steadily increasing power, which creates flying in a condition 'behind the power line'. A specific form of stall occurs when the aircraft makes steep turns with a load factor higher than 1g.
Over the decades, a wide variety of conventional stall warning and protection systems have been developed, categorized as aerodynamic devices, mechanical control devices or warning devices. Modern civil aircraft are protected against stall by flight envelope protections which limit their manoeuvrability. Specific sophisticated class of stall devices are 'canard' wings and fly by wire Flight Control Mode systems to cope with aerodynamic instability inherent to a positive lateral moment coefficient. Specific training simulators and programs have been developed for high altitude upset recovery. Each of these devices focus on a specific contributing factor in the event sequence. Stall is a specific aerodynamic phenomenon and part of a more generic failure mode, which is inherent to aviation: Loss of Control.

2 LOSS OF CONTROL

Loss of control (LOC) is the leading explanation for fatal accidents in several segments of the aviation industry, each with specific fleet composition characteristics (Veillette 2012). Several major events in large commercial aviation indicates deficient pilot knowledge and piloting skills, resulting in a lack of pilot resilience, leading to fatal loss of control accidents (West Carribean Airways 708, Air France 447, Colgan Air 3407, Turkish Airlines 1951, Asiana Airlines 214 and Air Asia 8501) (Lande 2014). Other, less public prone LOC accidents occur in the business jet, special purpose and general aviation fleet segments. Training for LOC depends on specific flight operation characteristics, such as operating environment (weather conditions), aircraft characteristics (configuration, cruising speed and altitude, cockpit layout and ergonomics) and pilot induced oscillation (attention, distraction, experience and qualification).
In the low speed region, aircraft are sensitive to loss of control by aerodynamic stall, where the critical angle of attack should provide sufficient lift to remain airborne. In the high speed region at high altitude, margins between minimum and maximum airspeed become small. Attempts to maintain altitude may result in aerodynamic buffeting and subsequent high altitude stall due to limited engine climb power. This region is known as the 'coffin corner'. In commercial aviation, standard recovery training from stall is to apply power to minimize altitude loss, while the aircraft is sensitive to generate gyrating pitch.
Several authors criticize current stall recovery approaches: the simulator aerodynamics modelling is questionable, while recovery relies on piloting skills. A transfer from manufacturer product liability to operator training liability has taken place (Den Hertog 1999, Lande 2014, Veillette 2012). Such a 'dumping ground' design philosophy with an emphasis on operators responsibilities has created a need for sophisticated operational safety concepts such as Line Operations Safety Audit, Flight Operations Quality Assurance and Safety Management Systems. Simultaneously, such a transfer causes a loss of 'know why' on design decisions and assumptions (Den Hertog 1999).
Sources for LOC are multiple (Veillette 2012). Physical sources are a constrained manoeuvring space and a loss of situation awareness regarding the total energy balance of the aircraft, combined with true airspeed, banking angle, turning radius and contaminated wing surfaces. Mental sources are cockpit mismanagement, pilot induced oscillation, spatial disorientation and timely detection of a situation. LOC occurs frequently in Non Routine Flight Operations during post-maintenance, non-revenue flights or operating in the margins of the flight envelope. which are not covered by adequate training on problem scenarios. In flight control malfunction may occur generic due to freezing or chafing of controls, or by type specific control issues that are not tested and documented in regular certification procedures. Meteorological conditions which are not fully understood and predicted may create LOC events due to low level wind shear, wake turbulence, vortices rebound and mountainous waves due to updraft and downdraft. In the upper regions of the atmosphere, where small manoeuvring margins exist and LOC accidents are major hazard. Flying should be avoided in intertropical convergence zones which create super storm cells, thunderstorms and microbursts. In particular business jets,

who fly higher and faster than commercial aircraft (M0.9 at FL 510 with clean wing configuration) are sensitive to LOC. Applying standard high upset recovery practices by giving power and maintaining pitch attitude, are sensitive to LOC accidents by high speed stall (Veillette 2012).
In general, LOC events have high dynamics. Detection, decision-making, reaction are in milliseconds, under high workload conditions, with a rapid development of the event, accompanied by abrupt automation disconnection, submitted to type specific flight handling properties and responses. Designing a failsafe solution, exclusive reliance on prevention is impossible. Stall and Loss of Control are inherent risks of flying and remain an inherent frontier to manage resilience in aviation. Consequently, recovery and resilience have to be built into the flight performance at the design phase.

3 INTUITIVE DESIGN

In the cockpit, the Primary Flight Display provides the physical interface between the aircraft flight mechanics and human performance. In the design of this display, the rational logical human cognitive and decision making model, based on formal logic and mathematical algorithms are the design standard. Several major accidents have revealed limitations in dealing with unanticipated and non-normal situations. External, contextual conditions are not taken into account, while internal reasoning processes are also controlled by intuitive, empathic and social dimensions.
An intuitive human performance model is advocated, based on the following assumptions (Lande 2014) :

- Pilots are relatively autonomous, context and condition dependent operators, dealing with both normal and unanticipated non-normal situations on a frequent and regular basis
- They participate in a traffic process control in a network configuration with distributed and delegated responsibilities
- Their decision making processes deal with safety critical aspects in a hierarchical order -aviate, navigate, communicate and manage- and basic control parameters –power, pitch and performance-
- Their decision making and control processes covers all phases of perception, recognition, interpretation and action perspectives
- Their decision making processes cover both rational, professional and formal logic decision algorithms and intuitive, empathic, emotional, communication and social dimensions.

Conventional man-machine interface designs are limited by risk mitigation strategies in which manufacturers and certification authorities apply the classic concept of ‘workload’ and transfer of manual flying tasks to high reliable automation as a remedy for ‘human error’. There are sobering lessons on the effects of further automation: workload is not reduced but changed in nature or shifted, erroneous actions are not eliminated but may change in nature, and the usefulness of automation is questioned in terms of benefits versus new risks (Hollnagel, Cacciabue and Bagnara 1992). Such automation induces reduced need for pilots in flying skills training and proficiency, avoiding operations in the margins of the flight envelope (Lande 2014). However, experiences from the field demonstrate that such a conventional approach creates an illusion of a failsafe envelope protection and an inherent inability to stall, while discrepancies remain between the operating and training envelopes. Such conventional automation takes the pilots out of the control loop, hampering interpretations of cues and observables of primary flight parameters, intuitive inceptors and aircraft state transitions. In this conventional design approach, fundamental understanding of flight mechanics is also hampered by the absence of total energy management oversight and angle of attack indicators (Lambregts 1982). Taking the pilot out of the loop dissociates the pilot from proactive situation assessments in ‘flying ahead of the aircraft’. Consequently, loss of situation awareness may occur in recognition of the vicinity of performance margins, display and mode confusion, loss of tactile and emotional feedback and composure in critical situations. Such loss should be compensated by Good Airmanship principles (De Crespigny 2012)
In addition to external oriented ‘ecological’ interface design, ‘intuitive’ design of the primary flight display is advocated facilitating pilots to deal with flight mechanical and human performance characteristics by a dedicated interface design (Lambregts 1982, Den Hertog 1999, Lande 2014). Such intuitive design should incorporate aerodynamic and flight dynamics basic knowledge, piloting skills and Primary Flight Display ergonomics.

4 INNOVATIONS FOR RESILIENT ENGINEERING

In a series of projects, based on a combined analysis of safety investigations, a historical survey of innovative approaches, scientific research on human performance and experimental setups, more fundamental issues were revealed in a better understanding of HMI architecture in dynamic control of aircraft:

- Introduction of redundancy on all primary flight control functions, in particular on pitch control, introducing technical redundancy in case of damage, malfunction or emergency
- Increasing resilience by decoupling of aerodynamic performance and centre of gravity range functions, leading to a configuration change from Tube And Wing into a class of Blended Wing Body aircraft
- Increase in responsiveness to preserve control over the aircraft in case of non-normal flight, degraded states and emergency handling as an answer to procedural flight restrictions.

In order to achieve changes, a fundamental shift in focus is inevitable, creating resilience at an innovative level of research findings and patents on:

- Strategic decision making support by the introduction of a Total Energy Management based control system, dealing with the total energy rate and energy rate distribution of the aircraft (Lambregts 1982)
- Introduction of an angle of attack as a primary flight display in the context of a human factor centred approach, including its ergonomic cockpit layout and intuitive design features (Lande 2014)
- Introduction of a recovery shield as a redundancy in pitch control by enhanced physical control over aerodynamic forces in a 4 D operating environment, supported by computerized rapid deployable recovery shields, as an independent fall-back for the regular FMS (De Kroes 2011).

Flight safety by further development of the flight envelope protection is served by the introduction of a recovery shield (De Kroes 2011). These generic notions are applied to the recovery shield:

- redundancy. The implementation of a recovery function for pitch control is necessary because of the loss of aerodynamic forces on the aircraft by disruption of the air flow across the wing and empennage. In addition, malfunctioning of the regular control surfaces may occur due to external or internal damage, failure of control actuators or as collateral damage due to other malfunctions such as structural collapse. Such a recovery function focuses on technical redundancy. Additional redundancy is provided by an overlap between technical redundancy and enhanced emergency handling capacity of the pilot in the recovery control mode of the flight management system
- resilience. The decoupling of a tight relation between the aerodynamic center and center of gravity range of the whole aircraft can create a more flexible range for the aerodynamic center by adding two small eccentric forces, deployed by two small extractable control surfaces. A further optimization of the center of gravity range is possible beyond the conventional cg range, facilitating a more economic and flexible use of the aircraft. This device does not replace the elevators, but reduces their size, reducing weight and parasite trim drag. Such resilience focuses on performance efficiency and eventually may lead to reconfiguration of the aircraft geometry as foreseen in the EU Framework program of smart wing development or into new concepts such as the Beechcraft Starship and application of canard wings
- responsive. There is a growing concern in the pilot community with respect to the reduction of flying and emergency handling skills under automated flight conditions and continuing degree of automation. Such a transfer from pilot controlled recovery action to aircraft controlled recovery devices seems the only option for commercial aircraft in the absence of the powerful thrust vectoring which exists in military aviation. In such a strategy, a human centered design in maintaining overall control over the situation seems preferable over a fully automated solution. The focus is on redistribution of the decision authority between aircraft and pilot and requires careful design of the man-machine interfacing. Such a transfer is to be accompanied by a simulator training program. By making the aircraft-pilot interface more responsive to degraded flight conditions and emergency conditions, the aircraft becomes less dependent of fluctuations and unforeseen situations in normal conditions. Such a responsiveness may reduce planning continuation errors and procedural flight performance (De Crespigny 2012).

In order to introduce such innovations, several transition strategies have to be applied simultaneously:

- change from descriptive and explanatory variables towards change and design variables
- change in focus from events and factors to systems and vectors
- change from human error notions to Good Airmanship principles
- change from control terminology and notions to engineering design language and principles
- identification of game changers as critical agents to identify market niches, economic constraints, feasibility and lead time considerations.

Innovative design consists of new concepts in handling flight dynamics and control of the aircraft. A multi-layered Loss Of Control mitigation strategy is required to cope with both man, machine and their interface.

In such an innovative design, three conceptual restrictions in present aircraft design have to be eliminated:

- adding a second line of defence for the aerodynamic recovery in pitch control and aircraft handling by introducing the physical device of the ‘recovery shield’ (De Kroes 2011)

- loosening the tight coupling between aerodynamic centre and centre of gravity range to improve the lateral stability control range in non-normal situations
- make the transition from a classic formal logic and Tayloristic pilot control model towards a human centred design of 'intuitive' interface design.

The feasibility of the project will be demonstrated with an integral and innovative design of a dedicated emergency and rescue aircraft: the Water Bomber.

5 AERAIL FIRE FIGHTING: THE WATER BOMBER

Over the past decades, aerial firefighting has evolved from conversion of military aircraft to special purpose applications in recue and emergency missions to designing dedicated aircraft configurations (DSE 2014). Such an evolutionary development has drawbacks in the efficiency and effectiveness of converted designs. Present water and fire retardant dropping strategies are risky and have a short lived effect in short passes. Serious accidents have occurred, despite the very skilled pilotage of former naval and aerobatic pilots. Aircraft such as the Bombardier CL-415 are capable of scooping 6 m^3 of water at a speed of 130 km/hr in 12 seconds in a 400 m run, but date from 1993 and are to be replaced by a next generation of special build utility aircraft. Top level requirements aim at multifunctional aircraft for rescue and emergency, firefighting, relief and evacuation purposes. The design aims at an aircraft of an amphibious nature with STOL characteristics, high scooping capacity, removable hold configuration for equipment and excellent handling qualities for low altitude, low speed and all weather conditions. The aircraft operates in complex terrain situations in mountainous areas, forests, near oil rigs, highways and other high risk, aggravated operating conditions. Sudden scooping and release of large loads requires robust, reliable dynamic behaviour and fast, adaptive control characteristics. To fulfil such a wide and flexible range of functionalities, the aircraft will be a modular design. Certain modules are deemed necessary for the aircraft handling and operations, while others are optional for specific missions. With a modular design, clients have more freedom to design, repair and update the aircraft for specific functions and missions (DSE 2014).

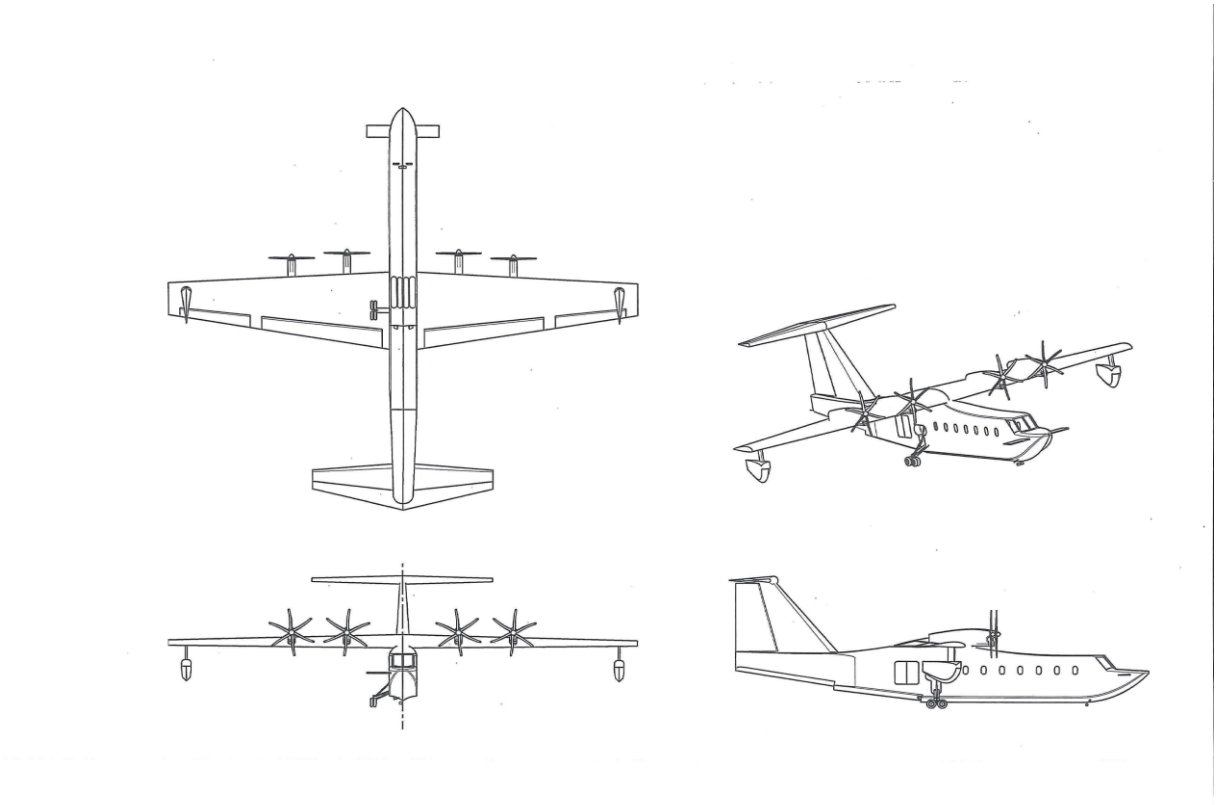

Figure 1: *Water Bomber preliminary design*

The price of the aircraft will vary, dependent from basic to enhanced versions. Such an adaptive and flexible design creates the necessary resilience for operations and sets the aircraft apart from previous generations. An integrated set of innovations contain the basics of the amphibious platform function with hydrofoils, control canards, electrical actuation of control surfaces, inflatable or retractable wing tip floats and intuitive cockpit design. Mission specific innovations cover functionalities regarding water cannons, multiple types of retardant and multiple, swappable retardant tanks and CADAS, the Computer Augmented Detection and Aiming System. The introduction of location based 3D printing of spare parts and components serves increased maintainability and flexibility in field operations.

6 CONCLUSIONS

The contribution demonstrates the practical application of resilience engineering to the design community in aviation. Feedback from reality -such as safety investigations and accident scenario thinking- is practically applicable in an empirical approach of such a complex phenomenon as stall and LOC prevention. In addition to the design requirements for a sustainable and resilient approach to stall and LOC, system change drivers and change agents are identified as constraints and operating conditions imposed by higher system level dynamics. Coping strategies with safety performance of the overall system beyond the level of robustness, redundancy and reliability are identified, identifying niche markets, fleet segments and macro-economic conditions for a sustainable development of innovative solutions. In addition, several conceptual changes have to be made regarding the human behaviour modelling, the role of automation and a discrimination between a focus on event occurrence and system change. The contribution also indicates the potential for safety investigations to serve as input for resilience engineering practices, considering stall and LOC scenarios as the ultimate load concept for system failure identification and type certification. Since stall is an inherent property, it forms an inherent frontier for managing resilience. A retrospective approach remains indispensable.
Finally, involvement of aerospace students and the use of patents in the project highlights the potential for engineering design initiatives to get acquainted with resilience engineering principles and concepts as a perspective to create innovative and integral solutions.

REFERENCES

De Crespigny R. (2012) *QF32 The captain's extraordinary account of how one of the world's worst air disasters was averted.* Macmillan, Pan Macmillan Australia.

Den Hertog R. *Safety starts at the Manufacturer*. Presented to the Netherlands Association of Aeronautical Engineers (NVvL) on May 27, 1999

DSE Water Bombers. (2014) *Towards a Next Generation of Water Bombers*. Final Report Design Synthesis Exercises. Delft University of Technology. Aerospace Engineering, Jan 2014

De Kroes J.L. (2011) Patent 2008049. *Subsonic plane or flight simulator thereof, adjustable fuselage control surface, computer program product and method*. Jan L. de Kroes

Hollnagel E., Cacciabue P. and Bagnara S. (1994) *The limits of Automation in Air Traffic Control and Aviation.* Report from a Workshop held at Certosa di Pontignano, Italy, November 25-27, 1992.

Lambregts A. (1982) Patent US 4536843. *A Total Energy based flight control system*. Antonius A. Lambregts

Lande K. (2014) *Aircraft Controllability and Primary Flight Displays* – A Human Factors Centred Approach. European 46th and 25th SFTE Symposium, 15-18 June 2014, Lulea, Sweden

Stoop J.A.(2013) *Towards a failsafe flight envelope protection: the recovery shield.* Advances in Risk and Reliability Technology Symposium 21st – 23rd May 2013 Loughborough, Leicestershire, UK

Veillette P. (2012) *Investigating and preventing the Loss of Control Accident*. ISASI Forum July-September (Part 1) and October-November (Part 2) 2012.