Time as a safety critical system integrator for flight control recovery in aviation

John A. Stoop
Lund University, Sweden
Delft University of Technology, the Netherlands

Abstract

Stall is an inherent unsafe flight control state that caused catastrophes in civil aviation. Solutions were gradually introduced, such as aerodynamic devices, pilot training, stick shakers and stall warnings. These mitigating, stand alone solutions seemed to have solved the problem to an acceptable level. However, stall as a phenomenon has recurred in a new form, due to changes in operating conditions, flight envelope protection, cockpit automation and crew competence qualifications. Stall accidents, as unintentional loss of pitch control, deal with malfunctioning of primary flight control surfaces, automation mismanagement and hostile environmental influences during all weather operations. As pitch control is the only primary flight control that has no design redundancy, a new flight recovery approach is proposed, introducing new and uncorrupted aerodynamic forces by combining a technical recovery device with enhancing diagnostic abilities for the crew. In designing such a device, synchronizing time required and time available for flight control recovery is a critical design dimension This contribution elaborates on a control recovery device as an integrated system, consisting of a technical design device, computerized flight control and crew qualifications. A practical application of such a device focuses on a stall shield device, as a specific category of flight control recovery.

Introduction

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 for the first time in 1901, flying his second glider. Over the following decades, stall has remained as a fundamental hazard in flying fixed wing aircraft. Stall is a condition in which the flow over the main wing separates at high angles of attack, hindering the aircraft to gain lift from the wings. Stall depends only on angle of attack, not on airspeed. Because a correlation exists between loss of lift and minimal airspeed, a "stall speed" is usually used in practice. This is the speed below which the airplane cannot create enough lift at maximum angle of attack to sustain its weight in 1g flight. Airspeed is often used as an indirect indicator of approaching stall conditions. The stall speed will vary depending on the airplane's weight, altitude, and configuration. Fixed-wing aircraft have been equipped with devices to prevent or postpone a stall, to make it less more severe or to make recovery easier. Stall is an umbrella concept that covers various scenarios, aircraft configurations and has seen

In D. de Waard, K. Brookhuis, F. Dehais, C. Weikert, S. Röttger, D. Manzey, S. Biede, F. Reuzeau, and P. Terrier (Eds.) (2012). Human Factors: a view from an integrative perspective. Proceedings HFES Europe Chapter Conference Toulouse. ISBN 978-0-945289-44-9. Available from http://hfes-europe.org

a wide variety of dedicated solutions. In practice, stall may occur under various conditions, configurations and can be caused by various failure modes. Consequently, various stall scenarios exist.

Although stall is a prominent issue in loss of flight control, loss of flight control as a wider issue is related to more phenomena than pilot performance (Veilette, 2012). Firstly, hostile operating conditions may occur, dealing with icing, weather conditions, wake turbulence, thunderstorms or micro bursts. Non-revenue flight operations, flight training, pilot competences and automation mismanagement represent a second category of pilot related contributing factors to loss of control. Technical malfunction of flight control surfaces by internal or external threats pose a third category of factors, sometimes with catastrophic consequences. Recovery from loss of control situations depends on the competences of the crew under these specific conditions and on the nature and extend of the technical damage and loss of integrity of the airplanes' flight control functions. If the available recovery resources are insufficient and the time required for recovery lacks, the event becomes unsurvivable (Stoop, 2011).

Stall scenarios

A fixed-wing aircraft during a stall may experience buffeting or a change in attitude. Most aircraft are designed to have a benign stall with characteristics that will warn the pilot. Because air no longer flows smoothly over the wings during a stall, aileron control of roll becomes less effective and may incline the aircraft to enter into a spin. The dangerous aspect of a stall is a limited recovery capability due to a lack of altitude. Such stalls may cause accidents at a low altitude. At high altitude, upper and lower speed limitations become critical as the speed range reduces. The upper limit is defined by structural integrity demands, while the lower speed limits depend on air density and available engine power setting. As stall is reached, the aircraft will start to descend and the nose will pitch down. Recovery from this stalled state involves the pilot's decreasing the angle of attack and increasing the air speed, until smooth air-flow over the wing is restored. The maneuver is normally quite safe and if correctly handled leads to only a small loss in altitude. During training, a pilot is required to demonstrate competency to recognize, avoid, and recover from stalling the aircraft.

Finally, a loss of pitch control may occur due to other causes than aerodynamic stall, but may result in a stall. Such stall modes origin from technical failure of rudders, exceeding the allowable centre of gravity range due to shifting cargo or fuel imbalances, damage to pitch control rudders by external impact from space debris or bird strikes, loss of critical air data due to Pitot port blockage by frost, foreign objects or insect intrusions. Despite all efforts to reduce stall and deep stall to acceptable levels of occurrence, such events still happen occasionally in commercial aviation. They raise concern about their emerging complexity, dynamics and impact on public perception on safety of aviation. Such events have been subjected to major accident investigations and serve as triggers for change throughout the aviation industry.

Stall mitigation

Over the years, a wide range of devices has been developed to prevent, postpone or recover from a stall. Although a distinction is required between the various configurations, several generic aerodynamic wing devices and pilot controlled mechanical warning and recovery devices have been applied.
In order to recover from a stall, pilots have to be knowledgeable about the attitude and state of the aircraft and its dynamic behavior. Stall contributing factors should be familiar to pilots, such as the angle of attack, the air speed and the positioning of the center of gravity. During the flight, pilots depend on reliable air data information in order to interpret and monitor their flight performance. In modern fly by wire cockpits with flight envelope protection, impaired air data information may degrade normal protection systems. In many modern aircraft, an air data computer is applied to calculate airspeed, rate of climb, altitude, Mach number and rudder travel limits. Such a computer derives its information from the Pitot static system, measuring the forces acting on the aircraft as a function of temperature, density, pressure and viscosity of the air. Errors in the Pitot static system can be very dangerous because the information is critical to a successful flight performance. The Pitot tube is sensitive to disturbances, such as clogging by water or ice, insects or other obstructions. Blocking the static port is a serious problem, because it affects all Pitot static instruments. Such blocking will influence the horizontal and vertical airspeed indicator as the static tube is blocked at the altitude at which freezing occurred, misinforming the pilot about the actual horizontal and vertical airspeed. Erroneous data information will have its effect on the aircraft computer system by impairing the air data functions such as flight director, autopilot, auto throttle, rudder travel protection, speed calculations, wins shear protection and switches control authorities between Control Modes.

Towards loss of flight control prevention?

Recent major accidents indicate the potential for loss of flight control, at a high altitude as well as low altitude. A timely recognition is critical, but may be hampered by the ability of the crew to recognize and diagnose an event in a timely manner and respond accordingly, based on available time and resources. Transparency of the automated flight management system for the crew is a safety critical factor in the ability to diagnose and recover from an event. Under all flight circumstances a stable and controllable flight performance should be maintained.

A case history: the AF447 crash

The BEA report on the AF447 accident demonstrates the complexity and dynamics of man-machine interfacing in which a continuous adaptation to a rapidly changing information display had to be taken into account. The eventual crash results from a succession of events in which (BEA, 2012):

- A temporary obstruction of the Pitot tubes, creating inconsistencies in air speed measurements that caused autopilot disconnection and reconfiguration of normal flight control law mode towards alternate law mode
- Inappropriate pilot input destabilizing the flight path

- The lack of linking between loss of indicated airspeed and appropriate crew procedures and the late identification of deviation from the flight path and insufficient correction applied by the PF
- The crew not identifying the approach to stall, their lack of immediate response and exit from the flight envelope and the crew failure to diagnose the stall situation and lack of inputs to enable a recovery.

Information on angle of attack is not directly accessible to pilots. The angle of attack in cruise is close to the stall warning trigger angle of attack in another law than normal law. Under these conditions, manual handling can bring the aeroplane to high angles of attack. Only a direct readout of the angle of attack could enable crews to rapidly identify the aerodynamic situation and take the required actions.

Alternate 2B law represents a specific case of flight control law configuration and occurs when flight computers have rejected the three Air Data References (ADR). The high and low speed protection that exists in normal law and the high and low speed stability in alternate law, are lost. The Electronic Centralized Aircraft Monitoring (ECAM) message associated with the reconfiguration indicates ‘PROT LOST’, while the load factor protection remains. Consequently, the precise identification of the consequences of a reconfiguration is complicated.

In alternate law, the longitudinal control law remains a load factor law, while the lateral law is a direct law. In relation to lateral control, direct law implies a pilot input to counter any possible roll tendency, such as with cross winds and turbulence. In case of autopilot disconnection, a pilot input becomes necessary to control roll. However, maintaining the load factor law according to the longitudinal axis makes it possible not to have to make inputs along the longitudinal axis in order not to destabilize the aircraft. It requires a really high level of turbulence for the aeroplane to become significantly unstabilized. Pilot inputs therefore must be moderate and essentially on the lateral axis. The relatively strong nose-up of the pilot flying (PF) may have originated in a certain difficulty in integrating the various types of control laws and the differences in handling inputs to adopt between the two axis. The cockpit voice recordings indicate a preoccupation of the PF with keeping the aeroplane level and keeping altitude with the thrust setting.

However, when there are no protections left, the aeroplane no longer possesses positive longitudinal static stability, even on approach to stall. This absence specifically makes it not necessary to make or increase nose-up input to compensate for a loss of speed while maintaining altitude. This neutral longitudinal static stability behavior was judged acceptable by the certification authorities because of the presence of flight envelope protections. However, a positive longitudinal static stability can be useful because it provides pilot sensory returns on the situation in terms of speed in relation to its point of equilibrium at constant thrust. In contrast with a classic aeroplane, the approach to stall in an A330 in alternate law is not associated with a more or less pronounced nose-up input. The consequence is that in this specific control law, the aeroplane would end up in a stall without any inputs on the side stick. It appears that this absence of positive static stability could have contributed to the PF not identifying the approach to stall.

In response to the obstruction of the pitot tubes by ice crystals, various monitoring systems triggered almost instantaneously. As the flight management systems detected differences between the various speed measurements, they reconfigured to alternate law. This monitoring is designed into the system to detect the obstruction of pitot tubes. The crew is only informed of the consequences of the triggering by observing the disconnection of the automated pilot and the automated throttle and the shift to alternate law. No failure message is provided that identifies the origin of these failures, in particular the rejection of the ADR's and of the speed measurements. No ECAM message enabled the crew to perform a rapid diagnosis of the situation, initiating the appropriate procedures. However, the crew is trained to read the ECAM as soon as the flight path is controlled, in order to analyze the situation and to organize a course of action to deal with the failures. Between the disconnection of the autopilot and the STALL 2 warning, numerous messages were displayed on the ECAM, but none helped the crew to identify the problem with the anomalous airspeed. Furthermore, the rapid change-over of the displayed information which was created by the flight computer in managing the priorities further complicated the crew's analysis and understanding of the situation. The reading of the ECAM by the pilots was time consuming and used up mental resources to the detriment of handling the problem and monitoring the flight path.

Current training practices do not cover manual flying at high altitude and do not compensate for lack of training of experience on conventional aeroplanes. Training schedules, based on full flight simulator training, limit the pilot's ability to acquire or maintain basic airmanship skills with respect to stall recovery due to the flight envelope protection constraints during such training.

In conclusion, two main sources for failure can be identified from this description:

- The available time window to deal with the situation was limited. The event took only 263 sec from the beginning to the very end
- Understanding the complexity and dynamics of the event consumed many resources to the detriment of the primary task to control the flight path.

Theoretical notions on time as an analytical dimension

Analysis of a complex and dynamic flight pattern as occurred with the AF447 has to take into account the dynamic environment in which the event took place. The crew had to adapt continuously and simultaneously to various changes in order to regain control and return to a desired stable and safe flight. Linear and static models of man-machine interfacing do not comply with diagnosing modern avionic systems that are designed on a 4D basis. This means that time has to be introduced as a 4th analytical dimension. Hollnagel and Woods have developed a model that deals with dynamic developments in their environment (Hollnagel & Woods, 2006). To apply the conceptual terms Anticipation, Attention and Response of their conceptual and aggregated model, these terms are defined as system safety value levers (De Graaf, 2012). The terminology of the model as used in 3 case studies (ElAl1862, SW111 and QF32) define Anticipation as Codified information within the system, Attention as the Ability of capturing real time information and Response as the Totality of system reactions reducing deviation from the desired state.

Time has to be introduced as a dimension to deal with the dynamics of the event. While the original model assumes a sequential processing, processing the system safety performance in the revised model essentially becomes simultaneous and continuous. Resilience is defined as the potential of the system capacity regarding available resources and time available to recover. Changes in recovery potential during the development of the event may be identified as deterioration or augmentation. The feasibility to avoid disaster is bounded by performance limits of technical and human resource nature and identified by performance requirements for anticipation, attention and responses. If the available recovery time windows do not comply with the minimal required recovery demands, the system will fail to recover from the event.

Available versus required resources: three case studies

This resource allocation concept has been applied to three recent major events in aviation: ElAl1862, SW11 and QF32 (RvL 1992, TSB 1998, ATSB 2010,). For the 3 case studies, exceeding the discrepancy between available and required time and resources defined the survivability of the event (De Graaf, 2012). A severity index was assigned to each of the occurrences in the sequence of events, indicating the required and available recovery capacity for anticipation, attention and responses.

This assessment can be displayed graphically in the performance-time capacity relationships. The deficient flight control recovery capacity in the case of ElAl1862 and SW111 resulted in the eventual loss of control over the aircraft (See figure 1).

For each of the cases (ElAl 1862, SW111, QF32), critical resources and time scales are identified, with respect to anticipation, attention and responses (De Graaf, 2012) as depicted in figure 2.

- In the ElAl1862 case the flight control response capacity was critical, due to the engine separation on the right wing with massive structural damage to the aeroplane. The crew had neither control nor time resources at the low flying level to recover from the split flap roll. The structural weaknesses of the fuse pin design were not anticipated, leaving the crew unaware of the engine separation and collateral damage. The aircraft crashed into an apartment block near Amsterdam.
- In the SW111 case, the recovery potential was critical due to a progressive fire on board, leaving the crew no time required to land safely at their diversion destination. The concealed deficiencies in the fire resistance were not anticipated, eliminating an appropriate diagnosis for the crew to control the fire effectively. The aircraft crashed into the Atlantic Ocean near Halifax, Canada.
- In the QF32 case, a coincidental presence of two master pilots on board facilitated appropriate diagnosis of the complexity and dynamics of the event due to an increase in attention and diagnostic capabilities. Due to a robust design, Cockpit Resource Management (CRM) skills and diagnostic capabilities, the available recovery capacity of the A380 exceeded the

anticipated capacity despite the massive damage to flight control systems. The aircraft was landed safely at Singapore Airport.

t	UTC	Event	ANTICIPATION			ATTENTION			RESPONSE		
			required	system		required	system		required	system	
				machine	human		machine	human		machine	human
<0		Take off and ascending flight	0	0	0	+	0	0	0	0	0
0	17:27:30	Departing E3&4, LE damage	+++	-	0	0	-	0	+++	---	0
25	17:27:55	Crew mayday call & takeover	0	0	0	0	0	+++	0	0	++
30	17:28:00	ATC response for assisting	0	0	++	0	0	0	0	0	0
35	17:28:05	Notion: fire in engine no 3	0	0	0	0	0	0	0	0	0
40	17:28:10	Notion: reduced thrust E3&4	0	0	0	0	0	0	0	0	0
85-205	17:28:55	Components falling off the ac	+++	-	0	+	0	0	+	--	0
210	17:31:00	Recognition: flaps problems	0	0	0	0	0	+	0	0	0
270	17:32:00	Ac does not respond to input	0	0	0	0	0	0	0	-	0
275	17:32:05	Unawareness: non-response ac	0	0	0	0	0	-	0	0	0
450	17:35:00	Recognition: control problem	0	0	0	0	0	++	0	-	0
470	17:35:20	POINT OF NO CONTROL	0	0	0	0	0	0	0	---	0
475	17:35:25	Recognition: going down	0	0	0	0	0	0	0	0	0
490	17:35:40	Crash	0	0	0	0	0	0	0	0	0

Figure 1. Capacity changes over time for ElAl 1862

In these case studies, all aircraft designs were similarly sophisticated, crew performance was on a comparable high professional level and substantial damage had occurred. The recovery depended on identification of a drift into failure and the ability to divert timely from the point of no return.

However, conceptual deficiencies exist. First airspeed indications rely on the use of pitot tube technology alone. Applications of a new, independent technology -such as GPS- might provide necessary technological redundancy for air data information supply

Second, in contrast with roll and yaw control, pitch control of aircraft is not redundant. There are no substitute strategies for controlling the pitch of commercial aircraft, Such conceptual deficiencies leave room for integrating time as a dimension for designing anticipation, attention and responses in the man-machine interfacing and to introduce new control forces in the flight handling of fixed wing aircraft. An innovative approach may eliminate inherent properties before they manifest themselves as emergent properties in practice with unavoidable catastrophic consequences.

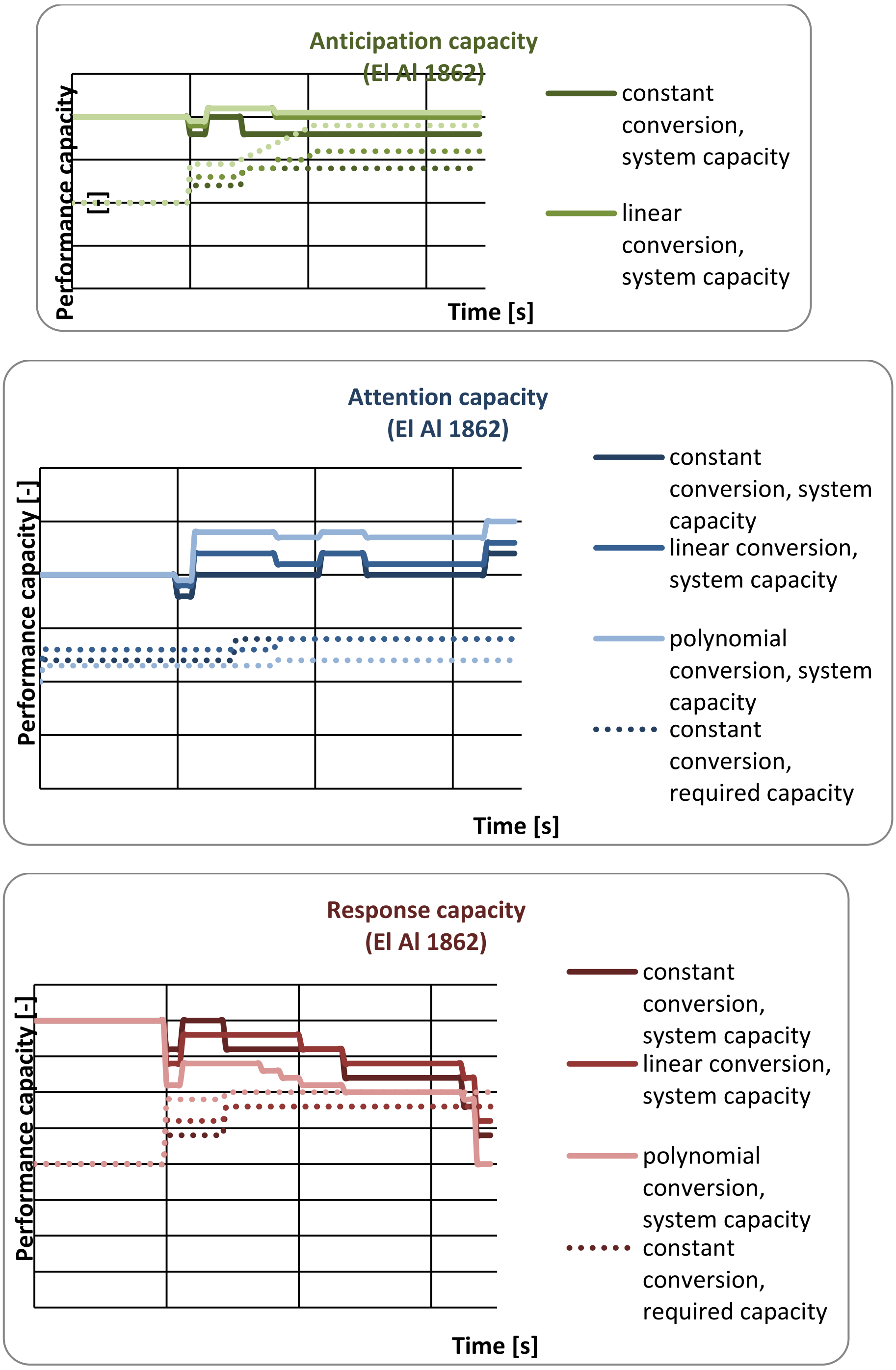

Figure 2. Capacity changes over time for specific characteristics

Towards innovative designs: a control recovery device

While pragmatic and dedicated solutions have achieved a high level of sophistication in stall mitigation and recovery, a more fundamental approach to loss of flight control avoidance could be developed in order to deal with systemic deficiencies in loss of flight control avoidance. A timely deployment of new resources creates recovery potential and facilitates operating in a new and safe flight control state.

An innovative solution should comply with principles of dynamic flight control over the fundamental aerodynamic forces that are exercised on general aviation and commercial aircraft:

- introducing new aerodynamic forces instead of manipulating existing forces
- introduction of such aerodynamic forces in uncorrupted air flow
- generating high pitching moments by small forces combined with long arms
- introducing correcting forces only in case of emergency
- a timely and fail safe deployment in a 4D operating environment.

In particular dealing with stall, an innovative design is suggested, based on these principles of dynamic vehicle control (De Kroes, 2012). Such a design as depicted in figure 3 is called a ‘stall shield device’ and consists of the following features:

- on the fuselage of the aircraft, control surfaces are located at the nose and tail section in order to minimize the size of the surfaces, providing the largest momentum arm to the center of gravity
- these stall shields are only deployed in case of near stall and emergent unstable flight to eliminate parasite aerodynamic drag in normal flight conditions
- these surfaces can be operated by either select nose or tail shields or combine a nose and tail mode of operation to provide a stable flight performance, depending on the stall scenario, flight phase, aircraft configuration and operating conditions
- a stall shield control system is integrated in the flight management system, supported by dedicated computer software, depending on the level of sophistication of the aircraft control systems
- As a commercial application, it may serve as a safety asset in creating safety performance beyond legally required performance standards.

Such devices and their control systems should benefit from deploying satellite system by developing avionics applications for ground speed, acceleration, altitude, positioning and flight attitude identification to provide redundancy in technology over the Pitot static data supply. In addition, a direct angle of attack indicator in the cockpit display is preferred to inform the pilot on the actual flight attitude of the aircraft while the stall shield device is operational.

Figure 3. Stall shields at the nose end of a T-tailed aircraft (This figure is taken from Flight Path 2050, Europe's Vision for Aviation. Report of the High Level Group on Aviation Research. European Union 2011.)

Several scientific uncertainties should be addressed in developing a stall shield device:

- the man-machine architecture and interfacing should address questions such as: manual versus full automation, when and how fast deployable, establishing eventual crisis work loads, maintaining oversight over the actual aircraft state and attitude, identification of critical performance parameters such as angle of attack, speed, attitude, system mode
- providing a proof of concept throughout each phases of design, varying from conceptual assessment until certification processes and standards, testing and flight taking into account validation criteria of safety, costs and lead time, acceptable performance envelope limits
- establishing critical load cases for an encompassing range of loss of pitch control, damage tolerance limits, center of gravity range extensions and limits, aircraft stability, trim and fuel economy constraints, structural aspects, construction weight and maintenance issues
- fail safe performance of the device as a ''full envelope protection device'', preventing inadvertently and unanticipated deployment, training requirements, pilot certification and proficiency demands.

Conclusions

Improving the recovery from loss of flight control, an additional recovery strategy should be provided if containment within the flight performance protective envelope is impossible. Expansion of the flight envelope protection is necessary, by introducing new and uncorrupted aerodynamic forces, redundancy in pitch control surfaces and expansion of flight management parameters. The rate of excursion from the protection envelope, available crew qualifications, the nature and extend of mechanical damage to control surfaces and required recovery time will limit the potential for successful application of such a recovery device.

Assessment of the flight control recovery device as a feasible and desirable innovation should be done in the early phases of its conception. Feedback from operationally highly experienced people such as pilots and accident investigators provide insights in the actual responses of the system under specific conditions that cannot be covered by an exhaustive proactive survey during design and development. A multi-actor assessment should identify strengths and weaknesses, opportunities and threats of the device, providing a safety impact assessment before the concept is released for operations. Otherwise, the cure could be worse than the cause.

References

ATSB (2010). In-flight engine failure - Qantas, Airbus A380, VH-OQA, overhead Batam Island, Indonesia, 4 November 2010 Australian transport Safety Bureau

BEA (2012). Final report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France Flight AF447 Rio de Janeiro – Paris. Bureau d'Enquete et Analyses pour la securite de l'aviation civile. Paris, July 2012

De Graaf M. (2012). The safety value lever. Complementing the Airside value Function with a safety objective. MSc Thesis Delft University of Technology, August 2012

De Kroes J.L. (2012). Commercial plane or flight simulator, adjustable fuselage control surface, computer program product and method. Patent P96519NL00. Deposited on 10 Jan 2012

Hollnagel E. and Woods D. (2006). Resilience engineering: Concepts and Precepts. Aldershot: Ashgate Publishing Ltd

RvL. (1999). Raad voor de Luchtvaart. Een beladen vlucht: eindrapport Bijlmer enquête. Sdu Uitgevers, 1999. (Final report on ElAl1862, in Dutch)

Stoop J.A., (2011). Timeliness, an investigators challenge. Investigation – A shared process, ISASI 2011, 12-15 Sept, Salt Lake City Utah, USA

TSB (1998). *In-Flight Fire Leading to Collision with Water. Report on flight SW111*, Transport Safety Board of Canada

Veilette, P., (2012). Investigation and preventing the loss of control accident. ISASI Forum, Part I, July-September 2012, 5/9 Part II, October-December 2012, 19-24.