To certify, to investigate or to engineer, that is the question

J.A. Stoop
Lund University, Sweden
Delft University of Technology, faculty of Aerospace Engineering
Kluyverweg 1, 2629 HS Delft, the Netherlands
Stoop@kindunos.nl

Abstract. Several major safety critical events have occurred in aviation in an attempt to make this matured system more efficient, mean and lean. These events have raised questions about their design and operational concepts. Simultaneously, the aviation investigation community reflects on how to cope with the second century of aviation. Events such as the Dreamliner batteries, QF32 and AF 447 have demonstrated how thin the line is between precaution, successful recovery and disaster. Modern socio-technical systems have a very high degree of complexity, dynamics and uncertainty. These uncertainties are dealt with by several professional communities during design, operation and investigation. This contribution elaborates on the potential and opportunities to feed information across these communities by creating communication loops for designing resilient systems in the early phases of systemic adaptation.

1. INTRODUCTION

Historically, safety investigations have seen a development in which a focus on technological failure has been complemented by a focus on human behavior, organizational failure and governance risk decision making. Over times, a more integral safety notion has been created by broadening the scope from pre-accident causation contributing factors towards safety enhancing and recovery factors during rescue and emergency handling in the aftermath of serious events. In the international aviation community, a gradual development took place in incorporating family assistance and victim support in dealing with the aftermath of aviation accident, first in the USA and Canada, later on in Europe (Troadec 2013). Informing the public about major accidents and incidents through independent investigations has become a Citizen's Right and Society's Duty (Van Vollenhoven 2006). Merging these safety aspects into a notion of 'integral safety' has broadened the identification of system deficiencies, which may have their origin before, during and after an occurrence. Consequently, the population at risk involved in the investigation has expanded from crew and passengers to employees at airports, residents in the vicinity of an airport, rescue and emergency services, family and relatives that may encounter traumatic damage due to an air crash.
Characteristics and properties of modern, open, complex systems can be identified and analyzed along the lines of:

- a prospective analysis of the primary processes and relevant actors during design and operation including their safety critical strategic decision making issues. However, an encompassing analysis is not always feasible in practice due to the complexity and dynamic nature of transportation systems.

Therefore, a second retrospective approach is indispensable:

- an in-depth and independent investigation into systemic incidents, accidents and disasters. Such independent investigations may provide a temporary and timely transparency as a starting point for removing inherent deficiencies before they manifest themselves as 'emergent' properties.

Accidents and incidents are the manifestations of such inherent and emergent properties and may provide evidence and explanation through investigations.

2. CASE HISTORIES

2.1 Air France AF447

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, created inconsistencies in air speed measurements that caused autopilot disconnection and reconfiguration of normal flight control law mode towards alternate law mode
- Inappropriate pilot input destabilized 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 did not identify the approach to stall, their lack of immediate response and exit from the flight envelope and the crew failure to diagnose the stall and lack of inputs to enable a recovery.

In response to the obstruction of the pitot tubes by ice crystals, various monitoring systems triggered almost instantaneously. 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 Electronic Centralized Aircraft Monitoring (ECAM). 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 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.

The final words of the BEA on the AF447 crash concluded that (Troadec 2013):

- the operating circumstances were only clarified by the flight recorder retrieval
- the occurrence was a consecutive series of critical events, starting with a loss of airspeed indications, followed by the airplane exiting the flight envelope, a loss of situational awareness of the crew, a lack of understanding of the stall situation and absence of recovery manoeuvres
- such occurrences occurred in both classic and high automation levels of aircraft design
- in which safety depends on adequacy between cognitive capacities and signals provided
- while hypotheses used for safety analysis were not always relevant, procedures not always applied and warning not always perceived
- improving quality of feedback enables detection of weaknesses in safety models as
- combination of ergonomics of warning designs, training conditions and recurrent training processes did not generate expected behavior, showing limits of current safety models.

In particular the last item revealed concerns about the basis for designing, manufacturing, simulation, certification, training and investigating human performance in aviation. In particular in emergency and unforeseen situations, human performance modeling proved to be deficient.

2.2 Qantas Flight 32

The accident occurred on the morning of 4 Nov 2010 at 10.01 hrs am by an uncontained failure of the port inboard (Number 2) engine, while en route from Singapore over Batam Island, Indonesia (ATSB 2010).
Debris from the exploding engine punctured part of the wing and damaged the fuel system causing leaks, disabled one hydraulic system and the anti-lock brakes and caused No.1 and No.4 engines to go into a 'degraded' mode, damaged landing flaps and the controls for the outer left No.1 engine.

The crew, after finding the plane controllable, decided to fly a racetrack holding pattern close to Singapore Changi Airport while assessing the status of the aircraft. It took 50 minutes to complete this initial assessment. The First Officer (FO) and Supervising Check Captain (SCC) then input the plane's status to the landing distance performance application (LDPA) for a landing 50 tonnes over maximum landing weight at Changi. Based on these inputs the LDPA could not calculate a landing distance. After discussion the crew elected to remove inputs related to a wet runway, in the knowledge that the runway was dry. The LDPA then returned the information that the landing was feasible with 100 metres of runway remaining. The flight then returned to Singapore Changi Airport, landing safely after the crew extended the landing gear by a gravity drop emergency extension system, at 11:45 hrs am Singapore time. As a result of the aircraft landing 35 knots faster than normal, four tyres were blown.
Upon landing, the crew were unable to shut down the No.1 engine, which had to be doused by emergency crews 3 hours after landing until flame out. The pilots considered whether to evacuate the plane immediately after landing as fuel was leaking from the left wing onto the brakes, which were extremely hot from maximum braking. The SCC pilot noted that in a situation where there is fuel, hot brakes and an engine could not be shut down, the safest place was on board the aircraft until such time as things changed. The cabin crew had an alert phase the whole time through ready to evacuate, open doors, inflate slides at any moment. As time went by, that danger abated and the crew was lucky enough to get everybody off very calmly and very methodically through one set of stairs. The plane was on battery power and had to contend with only one VHF radio to coordinate emergency procedure with the local fire crew.
There were no injuries reported among the 440 passengers and 29 crew on board the plane. Immediately after the accident, shares of the engine manufacturer Rolls-Royce fell 5.5% on the London Stock Exchange. Shares of AEDS, which owns Airbus, also fell. By mid-morning on Nov 8, Rolls-Royce shares had fallen by more than 10% since the accident the previous Thursday.

2.3 The Dreamliner battery case

On January 7th 2013, a B787 Dreamliner of Japan Airlines engaged a fire after landing at Boston USA in its Li-ion battery pack. On January 12th 2013, an All NipponB787 made an emergency landing after a battery fault warning and smoke smell dispersed the aircraft. No passengers were injured and no aircraft were lost. All Nippon shares fell 1.6% in Tokyo, while Boeing shares fell 3.3% in German trading and 1.9% in New York. The battery manufacturers shares fell 4.5%. Fifty jets, each 207 million$, were grounded for almost 4 months, staggering total costs to about 550 million$. NTSB and JTSB started investigating the events, during which also Thales as the designer of the battery management systems, were investigated. The Li-ion batteries were selected for reasons of weight reduction and energy density, although problems with thermal runaway and overheating were previously known. During these investigations, Boeing conducted research to create a simple cooling, fire mitigation and containment solution for the battery package in order to avoid a full time consuming and costly renewed certification process that would delay resuming flights for about one year. During its investigation NTSB was not able to identify the deficiencies on a short notice and shifted its focus on the design assumptions and the certification process as such. According to the NTSB, the direct causes for the overheating may never be found.
The main criticism focused on the assumption that a failure was due in less than one out of 10 million flight hours, while two safety critical events occurred within 52.000 flight hours. The investigations showed that the battery concept was prone to heating, based on the experiences in other applications of Li-ion batteries where fires had been noticed. During the following months, Boeing put pressure on the regulators to resume flying, indicating that the event would not happen again. During the investigation period, news releases indicate that the Federal Aviation Agency certification process relied on engineering design knowledge within the Boeing company. This procedure started in 2005, using approved outsider engineers and continued for years, even as government audits found that these procedure had poor oversight and led to errors, compromising the delegation system. While most countries followed the FAA lead in these regulatory matters, the Canadian Transport safety Board pointed to engineering certification as a possible factor in the crash of Swissair flight 111 in 1998, killing everyone on board. Engineers may have lacked sufficient knowledge of the Boeing MD-11 power grid to provide certification, the TSB found.

Between 1998 and 2004, 700 designated engineers were removed from the FAA approval procedure. In several news bulletins a failure to spot certification issues may have been responsible for 70% of the deaths in the past 20 years with US carriers (FSI 2013). This raises the question whether complexity could outpace manufacturing and regulation ability to spot deficiencies in design and certification. Earlier deficiencies in the Boeing 737 rudder actuator inverse functioning, the Boeing 747 explosive fuel tanks and several icing issues with fatal consequences may have been caused by this certification approval procedure, where all designs were certified as fail safe. A mismatch between resources in FAA, lacking sufficient design knowledge, and manufacturers expertise may have created a situation where certification standards and assumptions have not been challenged adequately.
Eventually, public confidence in the aviation system was challenged. The use of Lithium-ion batteries was addressed by a public forum of NTSB on 11-12 April 2013, questioning the principles of industrial self-certification. As FAA announced a return to flight for the Dreamliner on may 13th, ETOPS use was blocked by passenger advocacy groups, requesting flight limitations on the extended use of the Boeing 787. While FAA did not wait for the results of the NTSB investigations, public concern was raised and supported by prominent aviation safety experts in the USA. In conclusion, the strive for recapturing dominance in a world market, competing with Airbus, FAA lost face in public credibility, while Boeing lost about 50 million$ per week due to the grounding. All Nippon Airways had to cancel over 3600 flights for its 17 Boeing 787's, potentially requiring cash refunds from Boeing to compensate for the losses. The Japanese FAA formulated additional and more stringent requirements before resuming flight with the Boeing 787 by requesting monitoring systems on board for the Li-ion batteries.
Failures to spot and anticipate safety flaws during certification of new aircraft have been linked to 70 % of US airline-crash death in the past 70 years (FSI 2013). The Dreamliner lithium-ion battery fires have renewed questions whether complexity and new technologies of new aircraft have outpaced a manufacturers' and regulators' ability to identify deficiencies during design and certification. Although certification standards have preventing fatal US airline crashes since 2001, occasions have occurred where assumptions were incorrect and not conservative enough. The use of 'special conditions' in the absence of regulations for new technologies, as applied in the Dreamliner case, have proven the need to modernize certification processes and standards (FSI 2013).

3. A ROLE FOR ACCIDENT INVESTIGATIONS

There is a specific role for accident investigations as a partner in a more institutionalized network as a prerequisite for a further professional development, sharing professional expertise and participating in knowledge management.
In such a network, safety investigations may serve as:
- a repository for information dissemination and common learning
- a problem provider for knowledge development and systems change
- a public safety assessor and public spokesman beyond and above parties involved.

Safety investigations represent a specific analytic instrument with its own characteristics:
- independent from blame and vested interests of third parties and stakeholders
- a cased based approach, based on a systems perspective
- evidence based with respect to its findings and recommendations
- pro-active learning by developing generic principles, notions and knowledge, combined with dissemination of findings and recommendations on domain and sector specific solutions and change strategies.

Safety investigations serve a triple goal:
- Vision Zero: prevention of fatalities and injuries among the population at risk
- First Time Right and Zero Defects: no socio-economical losses during the introduction of new products and processes that jeopardize business continuity
- A Citizens' Right and Society's' Duty: providing society a timely transparency on the factual functioning of systems.

3.1 A socio-cultural context

However, some safety scientists are critical about the notion of Vision Zero (Hale 2006):
As an objective it seems to be a shining example of altruism and concern for mankind. Being an ideal, it is too far off to be motivating, but more fundamentally, ignores the fact that safety is not an independent property of a system. Claiming zero accidents as a goal denies conflicts and tradeoffs with other goals. Claiming zero accidents is the safety equivalent of the cries of fundamental religious groups, subordinating all other goals to their one vision of the right path to salvation or paradise. Zero accidents is a pure, hard and shining ideal – almost 'one worth dying for' (Hale 2006).

This opinion is not shared by many others. It is possible to establish a School of Thinking in identifying safety deficiencies and system change (Stoop and Dekker 2012). It is possible to reconcile conflicts and to overcome contradictions by establishing independent investigations as a Citizen's Right and Society's Duty (Van Vollenhoven 2006).
It is possible to achieve a safer aviation system than ever before, aiming at the goal of no fatalities and injuries in commercial aviation, where no fatal US air carrier accidents have occurred since 2009 . Such systems represent a separate category of non-plus ultra-safe systems.
The aviation investigation community considers accident investigation a unique incentive for safety changes through the release of reports and recommendations, especially those who deal with systemic and knowledge deficiencies (Arslanian 2011).
Are such trade-offs purely personal or can they be traced back to underlying socio-cultural differences between world regions; are they imposed by higher order social, cultural or economical values? An exemplary discussion is provided by the debate on road safety developments in Europe, with the Vision Zero principle.
In a debate on how far a Vision Zero can be effectuated, differences of opinion on whether such a goal can be achieved, clarify underlying differences in a socio-economical perspective on safety as a social value. While some emphasize the ethical approach to human life in averting fatalities and injuries and addressing responsibilities at a societal level, others emphasize the inevitability to balance safety against other societal values. They emphasize the need to make cost-effective decisions in terms of a rational socio-economical policy and a human desire for fulfillment, where risk of death and serious injury is a matter of degree. At the operational level, such a balancing values dilemma is formulated as the ETTO principle: the Efficiency-Thoroughness-Trade-Off (Hollnagel and Woods 2006). Such differences can be traced back to differences in socio-economical models and the value of life in each of these models.

Three competing socio-economical models exist in the Western hemisphere, which are seldom made explicit in debates on safety culture and organizational culture:

- the Anglo-Saxon model of liberal values, dealing with self-relianceness, private entrepreneurial initiatives, freedom and limited social security, with a dominant position for market mechanisms. In this context, safety and risk are based on cost-effectiveness considerations, taking into account probabilities of occurrences and responsibilities of corporate management
- the Scandinavian model of humanitarian values, where social cohesion, common wealth, human rights, and stability of the economy leave more room for governmental control and participation. Safety and risk in such a model, deals with preserving the unprotected from hazards beyond their control. This includes a Vision Zero regarding inflicting death and injury on road users.
- The Rhineland model, dealing with providing a human face to socio-economical, political and power relations. In this model a role for governmental control and guidance is foreseen, aiming at a welfare state, achieving consensus between social partners, providing stability on a medium and long terms. With respect to safety, continuity on the long term prevails over short term profit and cost-effectiveness and democratic participation in policy making decisions is stimulated.

Unfortunately, subsequent organizational structures and their functioning at an entrepreneurial as well as governmental level, have not yet been studied extensively by scientific research with respect to the safety performance and failure mechanisms of these models.

3.2 Human performance in emergency monitoring

Several major events such as AF447 and QF32 indicate the thin line between successful skilled professional responses and a catastrophic outcome in a Fly By Wire environment. The classic notion of 'human error' as undesirable deviation from a normative concept of flight control is predominant among human factor specialists. Human error is commonly accepted among psychologists as the leading artifact in causing accidents. Human error should degrade the system from its optimal performance, creating mishap that could be prevented by safety management interventions. For psychologists, the rejection of the concept of 'human error' is difficult to rationalize with the perspective of the system designer employing a formal prediction methodology to help avoid actions that will degrade the system. *When considering human error, first of all pick your perspective then choose your label (Harris 2011, pp 100].*
Consequently, automation would be the solution to human error, resulting in full automated flight. In this concept, there is no space for a critical reflection on the design of a supervisory role and discretionary responsibility of the pilot [7, 9]. Leaving aviation, navigation, communication to automated systems, pilots should restrict themselves to a managerial responsibility, balancing safety against efficiency and costs (Harris 2011). However, such concepts rely on almost flawless automation and extreme low failure probabilities, irrespective of technological imperfections and harsh operating conditions. In practice, such an approach might not be the most appropriate perspective to analyze and understand complex and dynamic interactions between flight management systems and operators (Stoop and Dekker 2012, Stoop 2012). It is a question whether it is possible to incorporate the know-how of operator experience into the design of safer systems (Morel, Amalberti and Chauvin 2008). Such a design could preserve craftsmanship and native resilience of such systems, relying on a high level of adaptability and professional expertise of the operators. These studies indicate potential adverse effects of classical safety interventions in terms of professional reluctance to accept further automation or through the emergence of new risks (Morel, Amalberti and Chauvin 2008). Constraining operator behavior in order to improve safety makes systems more rigid to the detriment of self-managed safety.
Such a role of the pilot as supervisor with oversight and control over the aircraft fits in well with the delegated responsibility of operators in a global network with distributed control over the primary production processes in a time critical environment, based on good airmanship (Stoop 2012).

In analogy with Paries, three main sources for failure or success can be identified (Paries 2011):

- The available time window to deal with the situations was critical. The AF447 event took only 263 sec from the beginning to the very end, while the QF32 event took 4 hours and 45 minutes before the crew could declare the situation to be safe.
- Understanding the complexity and dynamics of the event consumed many resources. Diagnosing the event was to the detriment of the primary task to control the flight path in the AF447 event, while additional crew resources enabled to a high extend a successful handling of the QF 32 event.
- The availability of resources, redundancy and flexibility in responses determined the outcome of the events to a very high extend. Regaining oversight over the situation by strictly following procedures and check lists on a compliance based level would not have helped an understanding of the situation due to the damage to the Flight Management System and the structural damage to the aircraft or the adherence to quantitative risk analysis standards.

4. RESILIENCE AND INNOVATION

In particular where dealing with innovations is suggested, designs should be based on principles of resilience. Introducing such designs intend to serve flight safety by further development of the flight envelope protection, based on three notions:

- 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
- 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.

4.1 Reality checks

Safety investigations serve the goal of knowledge deficiency identification. Safety investigations are the problem providers for knowledge development.

Historically, on a case basis, investigations have disclosed failure phenomenon that had not been understood before. Examples in various high-tech industrial sectors provide show cases that have triggered scientific developments, establishing new disciplinarian domains. The De Havilland Comet is associated with metal fatigue in jet engines with pressurized cabins, Tenerife and Harrisburg are related to human error and human resource management issues, while the Challenger is linked to organizational learning.

In their criticism on current practices in accident investigation and risk assessment modeling, scientists link the criticism on models such as FTA, FME, Event trees and others to the conduct of investigating accidents itself, in particular to the investigation of events. The simplicity of analysis, the linear causality, loss of the time as analytic dimension and limited focus on the operational level and role of the operator should make event models inappropriate during investigations. Their descriptive nature and limitation in the number of failure mechanisms they encompass, reduces the usefulness and quality of event investigations (Hollnagel and Woods 2006). The lack of coupling to a systems approach reduces the validity of their findings and consequently, their solution potential.

4.2 Modeling and prediction

This shift from event investigation to event modeling however, is disputed by investigators: accident investigators do not apply models in the fact finding phase of an investigation, they are applied during design of systems and in the analysis phase of investigations. During fact finding and recomposition of the occurrence, forensic principles prevail (Stoop 2012).

During the design, probabilistic models are used in a generic and context free manner to describe a limited set of ‘top events’ which are allocated a certain frequency of occurrence. The eventual risk should to stay within acceptable limits or risk levels. If such a frequency is very low, such failure mechanisms are considered acceptable and are not designed out of the system. This is based on the assumption that their occurrence will be fed back to designs and certification processes to enable further mitigation. In practice

however, such feedback may be absent by a lack of feedback mechanisms, or fade as weak signals in an increasing information noisy environment. Such failure mechanisms may go unnoticed, until an accident occurs. Several accident have demonstrated that there is no guarantee that pilots will detect failure modes in a timely manner that have been overlooked or accepted as negligible during the design and certification process.
As stated by Arslanian: *it is not possible to rely only on a predictive approach. Prediction is not a replacement for correction, but prediction and correction are in fact two sides of the same coin. A permanent screening of available data to identify unforeseen hazards or to better assess risks needs feedback data, sometimes from the unpredictable (Arslanian 2013).*

5. CONCLUSIONS

In the investigative community, critiques focuses on the practical use of models for investigation purposes, discriminating between their application in the fact-finding phase and analytical phase. For the benefit of collecting and structuring information it is required to apply a specific investigation methodology. An investigation should take into account each of the events as building blocks, sequencing in a temporal and spatial order to create mental representations for investigators in an advancing time frame. This should facilitate a quality control over the reasoning process and inferring logic in the relations between events. Using predefined models in accident investigation deprive an investigator from verifying and falsifying models that have been used in design and certification phases and have proved not to be fail safe in practice (Troadec 2013).
Safety investigations bear the element of *serendipity*; finding something out by accident through an open-minded, systemic and in-depth investigation of unpredicted events. Safety investigations are a reality check since preceding modeling, simulation and systemic decomposition during design, development, testing and certification all have their assumptions and limitations. It is necessary to make capital out of experience, to get feedback from the unpredictable, to learn from what we encounter in the field (Arslanian 2011).

REFERENCES

Arslanian P.L. (2011). ISASI Forum 2011. Pp 12-13
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
FSI (2013). Flight Safety Information 2013. *Several Bulletins* Jan–May 2013.
Hale A.R. (2006). *Is there a system in your madness*. Valedictory lecture Delft University of Technology
Harris D. (2011). *Human performance on the flight deck*. Ashgate
Hollnagel E. and Woods D. (2006). *Resilience engineering: Concepts and Precepts.* Aldershot: Ashgate
Morel G., Amalberti R. and Chauvin C. (2008). *Articulating the differences between safety and resilience: the decision-making process of professional sea-fishing skippers.* Human factors, Feb 2008 Vol 50 issue 1
Paries J. (2011). *Lessons from the Hudson*. Resilience Engineering in Practice. A Guidebook. Edited by Erik Hollnagel, E., Paries J., Woods D. and Wreathall J. Ashgate (2012). Studies in Resilience Engineering.
Stoop J. and Dekker S. (2012). *Are safety investigations pro-active?* Special Issue Safety science 50. Future challenges of accident investigation, some insights from the 33rd ESReDA Seminar. Safety Science 50 (2012) 1422-1430.
Stoop J.A. (2012). *Time as a safety critical system integrator for stall recovery in aviation.* Human Factors and Ergonomics Society Europe Chapter, Human Factors: a view from an integrative perspective. October 10-12, 2012, Toulouse, France
Troadec J.P. (2013). *The final word: Air France flight 447*. ISASI Forum Jan-March 2013 pp 6-8
Van Vollenhoven P. (2006). *RisicoVol.* Inaugural Lecture University of Twente.