TU Delft

Delft University of Technology

How did aviation become so safe, and beyond?

Stoop, John

Publication date
2017

Document Version
Accepted author manuscript

Published in
Proceedings of the 53rd ESReDA Seminar, 14 – 15 November 2017

Citation (APA)
Stoop, J. (2017). How did aviation become so safe, and beyond? In *Proceedings of the 53rd ESReDA Seminar, 14 – 15 November 2017: European Commission Joint Research Centre, Ispra, Italy*

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

How did aviation become so safe, and beyond?

John Stoop

Delft University of Technology
Amsterdam University of Applied Sciences
Kindunos Safety Consultancy Ltd
Spijksedijk 8
4207GN Gorinchem, the Netherlands

Abstract

Aviation has been recognized as one of the ultimate safe socio-technical systems. This contribution discusses the conditions and context that moulded the system safety to its present level by applying integral safety, a sectoral approach and safety as a strategic value. At present the aviation system consists of institutional arrangements at the global level, a shared repository of knowledge and operational experiences, feedback from reality, the notion of Good Airmanship, together with the choice of technology as the flywheel for progress. This architecture made aviation a Non-Plus Ultra-Safe system characterized by a safety performance level of beyond 10^{-7} accident rate. To cross this mythical boundary in legacy systems like aviation, it is imperative to apply game changers such as socio-technical systems engineering, disruptive technologies and innovation transition management. In such a transition, a shift in focus occurs from performance to properties, from hindsight to foresight, highlighted by the case study of the stall recovery device, the Kestrel concept.

Keywords: aviation, system safety, foresight, engineering design, safety investigation

1. Introduction

A Non-Plus Ultra-Safe performance is no reason for complacency. In view of the oncoming growth and expansion a further increase of safety is required to maintain the present performance level and to assure public confidence in the system. The size of the 'City in the Sky' at 30.000 feet is prognosed to double from the present 1 million inhabitants to 2 million in 2030 (Boosten, 2017).
To cope with this prognosed growth, abolition of obsolete safety constructs is inevitable. New safety notions are required in a transition from accident contributing factors to state/space modelling with safety Eigenvectors and multiple solution domains. Despite their low frequency, prevention of physical consequences of major events in such high energy density systems remain pivotal due to their catastrophic and disruptive potential. Application of systems control theoretical approaches enable a transition from reactive and proactive towards predictive capabilities. Early interventions in the design process enable identification of intrinsic hazards and

inherent properties that have to be dealt with during normal and non-normal operations and system states.
Incorporation of higher system orders, engineering design principles and innovative and disruptive change enable a combination of both reactive, proactive and predictive responses which facilitate foresight in safety. Because in aviation, we must continue to innovate and improve to safely defy gravity tomorrow.

2. How did aviation become so safe?

2.1 Engines for enhancing foresight

Four engines for enhancing foresight and predicting safe behaviour at a systems level are identified which, each by themselves, are a necessary but insufficient condition for safety enhancement. In addition, they have to occur simultaneously in order to implement a new concept in the aviation sector on a sustainable basis.
These engines are:

- Institutional arrangements at the level of the state and its sovereignty in an supra-national context of non-governmental organisations
- feedback from reality, based on precaution and independence of investigations
- system engineering principles, technological innovation and system state transitions
- Knowledge Based Engineering, by understanding empirical and experimental data.

As these engines coincide, a structural need for timely adaptations and system change occurs. Impulses for change can be explained based on internal, structural needs of the sector itself, not only by a public concern on the credibility of a sector. In case of an external impulse, such as with aviation disaster, sometimes several similar events have to occur before a sector responds. A worldwide implementation of each these engines has not only lead to a significant increase in safety, but also contributed to developing expertise and knowledge about the actual safety performance of the sector. They served as foresight, designed into the system from the start on. A vital issue has been maintaining public confidence in the sector in order to develop a worldwide aviation industry (Kahan, 1998). On one hand, in passenger transport, the public is the customer who puts its faith in a safe, efficient and smooth performance of the services rendered. Once this faith is lost, the sector will have to face the fear of going out of business. On the other hand, the performance of the transport sector is in the public domain. Accident are visible in the public eye, being bystanders and potential risk bearers in case of a disaster, such as an air crash in an apartment building, a release of hazardous materials or a tunnel fire. Rescue and emergency in incident and disaster handling are public duties in case of a disaster. Independent Transport Safety Boards make public governance at the State level a direct stakeholder in transportation accidents at the systems level in contrast to corporate management of fixed installations in other high-tech sectors such as process industry and nuclear power supply (Vuorio, Stoop and Johnson, 2017). Due to the complexity and high-technology nature, aviation has additional specific characteristics, which necessitate a technical investigation into unexplained failure of such transportation systems. These are based on the precaution principle, creating a common body of knowledge in aviation.

2.1.1 Institutional arrangements

The first international aviation conference in 1889 raised four fundamental juridical questions with regard to national sovereignty of the airspace and safety of aviation (Freer, 1986.1):

- Should governments license civil aviation?
- Should there be special legislation to regulate responsibility of aviators towards their passengers, public and owners of the land where descent is made?
- Should the salvage of aerial wrecks be governed by maritime law?
- Should there be new rules for establishing the absence or death of lost aviators?

Establishing rules for uncontrolled flights in airspace or above territorial waters led to the first international aerial congress amongst 21 states in 1910 in Paris. The First World War spurred aviation technology, leading in 1919 to the International Air Convention on technical, judicial, and military aspects of aviation and the establishment of the International Commission for Air navigation (ICAN) (Freer, 1986.2). The answers to these questions firmly establish safety and the investigation of accidents as a distinguishing feature of the aviation sector.

During the early development of public transport systems, the precaution principle has been applied as the most sophisticated engineering design approach of the 19th century (McIntyre, 2000). This precaution principle is defined in aviation as: first comprehend then control, create foresight by gaining insight. It combines a timely response to failure with an in-depth analysis in order to understand the failure mechanisms. It was only during the Second World War that a probabilistic component in safety thinking was added as a second school of thinking to this approach. Due to a lack of empirical data, probabilistic approaches should reduce uncertainty on new concepts and configurations to facilitate prioritization and cost-effectiveness estimates of safety enhancement measures. After the Second World War, corporate risk management was introduced as a third school in thinking, evolving into a public safety and governance between all actors involved in safety in the transportation area (McIntyre, 2000).

As the flywheel for progress, the level of technical harmonization has been selected focusing on navigation, communication and reliability. The precaution principle and a timely feedback of findings are pivotal. Annex 13 set the terms for cooperation between states which are involved in an aviation accident, namely the States of occurrence, operations, registry and manufacturing (ICAO, 2001). The large-scale introduction of civil aviation required a change in aircraft design. Before the war, civil aircraft were derivatives of military aircraft with respect to their design concepts as well to their construction and materials. After the war, large civil aircraft became disruptive designs because they had to transport great numbers of passengers over long distances, based on regular timetables, putting high demands on endurance, range and comfort. In contrast to these requirements, military aircraft were designed for relatively short-range combat performance, serving as airborne battle stations.

2.1.2 Feedback from reality, independence from blame and state interference

Even before the Second World War, the concept of learning from deficiencies was promulgated in aviation. Safety was viewed as an industry-wide problem, rather than one for any single operator, manufacturer or State. The concept was further developed

in wartime aviation. Flanagan et al. (1948) conducted possibly the first study of incidents and "near misses" in aviation when he surveyed U.S. Army Air Corps crews to determine what factors influenced mission success and failure. Anticipating modern insights, he found that the critical factors were to be found more in human performance than aircraft technology. In order to keep public faith in the aviation industry, a common process of learning without allocating blame was deemed necessary. In order to provide a timely feedback to all stakeholders in the sector, accident investigations had to be separated from judicial procedures, which focus on individual responsibilities and liability.
The blame-free approach has clearly borne fruit. Technical investigations into the failure of designing and operating aircraft have seen an impressive development. Based on a limited number of 'showcases' design principles were developed, such as fail-safe, safe life, damage tolerance, crash worthiness, situation awareness or graceful degradation. Several famous cases such as the De Havilland Comet, Tenerife, UA-232 Mount Erebus, TWA-800, Valuejet and Swissair 111 have identified deficiencies in the aviation system, sometimes at some remove from the proximal cause of the triggering event. They have led to many practical changes as well as new expertise on specific academic areas varying from as metal fatigue to human failure, crew resource management or life-cycle maintenance.

During the 1960s, the issue of independence was raised in order to relieve investigations from a dominant influence of the State. During investigations, the influence of State interests, secondary causal factors and circumstantial influences should also be addressed. The debate on this matter can be traced to around 1937, after a series of major air crashes. Arriving at such independence, however, proved to be a long process, and still is not completed. In responding to specific European needs in harmonizing practices current in the States of the Community, an additional procedural arrangement on ICAO Annex 13 has been developed. This development led to the EU Directive 94/56/EC on Accident Investigation, despite fundamental differences between legal systems in the various countries of the Community (Cairns 1961, Smart 2004). Conflicts of interest linked to the issue of double inquiries by technical permanent bodies and by judicial authorities were recognized, but nevertheless lead to a Community strategy to adaptation of the existing legal and institutional framework, harmonizing national legislation and strengthening cooperation between Member States (ETSC, 2001). As a consequence of the notion that incident investigation and analysis could be a source for safety recommendations, the EU has issued a Directive 2003/42/EC on mandatory incident registration in aviation. So far, the aviation sector has been unique in issuing mandatory, governmental investigations of systemic incidents beyond the corporate level of investigations (Vuorio, Stoop and Johnson, 2017).

2.2 System engineering principles

2.2.1 Multiple safety performance indicators

Historically, safety in aviation is not only expressed in institutional arrangements and policy targets, but also in international, technical airworthiness requirements. Taking into account that zero risk is unachievable in any human activity, acceptable safety target levels had to be established in the perspective of an unbalance between safety and expected growth (Hengst, Smit and Stoop, 1998). An array of potential units for

measuring risk can be used, discriminating *relative* safety related to the traffic volume and *absolute* safety, related to the annual number of fatalities. Differences across fleet segments and services, scheduled, non-scheduled flights and general aviation, accident rates per aircraft class and world region, as well as life expectancy of aircraft have to be taken into account. Risk acceptance by the general public and personal appreciation of risk depends on convenience and pleasure in the various types of private and public risk taking activities. For each activity, a unit of measurement has to be selected since it makes a large difference whether safety is related to the absolute number of fatalities, a critical flight phase or the distance and time flown. For *air services*, as the criterion for safety performance the fatality rate per passenger km is used, while for *airworthiness* the level of safety is expressed per aircraft hour of flight. These two criteria are related by the number of passengers per aircraft, the survivability rate per aircraft and the blockspeed of the aircraft (Wittenberg, 1979).
This relation can be derived from statistics of air transportation quantitative data by:

- Number of passengers km P
- Aircraft flying hours U
- Aircraft flying kilometres S
- Assuming K passenger fatalities in R fatal accidents, the fatality rate per passenger km is K/P and the fatal accident rate per flight hour R/U.

For the relation between these quantities holds:

Eq (1) $K/P = R/U*K/R*U/P$

In this expression are introduced:

$k = K/R$ = average number of fatalities per fatal accident
$p = P/S$ = average number of passengers per aircraft
$V_B = S/U$ = average block speed

Then for equation (1) can be written:

Eq (2) $K/P=R/U*k/p*1/V_B$

Or in words: Pass.fatalities/pass.km = fatal acc./flight hours *fatal per acc./pass per aircraft*1/blockspeed. This dimension analysis shows that the introduction of long haul flights, increased survivability rate per accident, increase in blockspeed and larger aircraft have had a major influence on the decrease of the fatality rate per passenger km.
These dimensions apply an aircraft design and certification perspective, while later developments applied an operational perspective. Safety management systems and maintenance, repair and overhaul established safety performance indicators for normal situations throughout the operational life of aircraft.

2.2.2 Towards a systems engineering perspective

In addressing the issue of acceptable safety levels, two assumptions are made:

- With the expected increase of traffic volume, safety levels may not fall below the achieved levels for reasons of public acceptance
- The level of growth is linear related to the number of accidents.

Consequently, the percentage of the total growth of the traffic volume expressed in passenger km must be compensated by an equivalent decrease in percentage of the fatality rate per passenger km. In the past, safety improvements have been accomplished pragmatically changes in technology, aircraft operations and ground equipment. These achievements have been a combined effort of all parties involved: manufacturers, airline operators, authorities and research institutes.

Advocating a more rational tool for establishing a safety level -such as cost-benefit analysis- such approaches are confronted with hardly comparable costs for value of life, operating costs and cost for safety investments. While costs of individual accident are relative low on a sectoral level of costs, the overall safety enhancement measures following from such accidents may be excessive for the sector. A target safety level for aviation based on a rational cost-benefits approach seems hardly achievable (Wittenberg, 1979).
More rational approaches had to be developed in the 1970's for the introduction of civil jet aircraft and new technologies such as the supersonic Concorde and Automated Landing System development. The allowable probability of failures is inversely related to their degree of hazard to the safety of the flight. No single failure or combination of failures should result in a Catastrophic Effect, unless the probability can be considered as Extremely Improbable, in effect lower than a 10^{-7} accident rate. Interesting in this approach is the total amount of flight hours per year that are produced by the aviation industry as such. Only a few aircraft types can surmount the 10^{7} requirement, accumulating sufficient flying hours. Consequently, accomplishment to the overall safety target of the airworthiness code *can never be proved by actual flight data* but should be settled by a System Safety Assessment approach. Due to the effect of the increase of aircraft speed and aircraft size, the passenger fatality rate expressed per passenger km has decreased in the past far more than the fatal aircraft accident rate per flight hour. In the coming decades, the favourable effect of aircraft speed will not occur and only the effect of aircraft size may remain. This parameter analysis demonstrates that changes in aircraft size and long range flights will consequently have an important impact on the improvement factor required for the fatality rate per *passenger km* versus the fatal accident rate based on the *aircraft flying hours.*

2.3 Knowledge Based Engineering (KBE) design

In assessing the fulfilment of the societal values and acceptance of designs, the prediction of tolerable loads and acceptable behaviour of designs is not so simple and well-defined as it seems. In the striving for excellence, the concept of failure is central to understanding engineering, for engineering design has as its first and foremost objective the obviation of failure (Petroski, 1992). As stated by Petroski, to understand what engineering is and what engineers do, is to understand how failures can happen and how they can contribute *more than successes* to advance technology (Italics added). As a challenge in the Science, Technology and Society debate on Human Values, engineering has as its principal objective not the given world, but the world that engineers themselves create. Extra-engineering motives and considerations of these values result in a continuous change that arises from these challenges. This means that there are many more ways in which something can go wrong than in the given world.
In his analytical study on aerospace engineering methodology, Vincenti indicates the transition from craftsman thinking in experimental progression towards knowledge based design of artefacts (Vincenti, 1990). In the 1930's the empirical and experimental design of aerofoils was gradually replaced by analytical and mathematical understanding of the mechanisms that ruled aerofoil design. Such transition towards a knowledge based design was supported by wind tunnel testing of scale models and flight tests. Scientific research focused on the role of viscosity,

transition between laminar and turbulent flow, laminar flow aerofoils and elliptic lift distribution. This application of scientific research in order to reduce uncertainty in the attempts to achieve increased performance created a growth in knowledge. Increased knowledge in turn acts as a driving force to further increase knowledge. As defined by Constant (quote by Vincenti, 1990) the phenomenon of 'presumptive anomaly' may stimulate better understanding of the behaviour of an artefact.

"Presumptive anomaly occurs in technology, not when the conventional system fails in any absolute or objective sense, but when assumptions derived from science indicate either that under some future conditions the conventional system will fail (or function badly) or that a radically different system will do a much better job."

Vincenti concludes that presumptive anomaly, functional failure and the need to reduce uncertainty in design act as driving forces to a growth of engineering design knowledge.

In aviation engineering design, safety investigations have been providing feedback from reality by exploratory reconstructions and analytical interpretations of facts and findings derived from accident investigations. Challenging design assumptions, model simplifications and operational restrictions in examining the validity of this knowledge store have contributed to the growth of design knowledge. Through safety investigations, systemic and knowledge deficiencies were identified, leading to novel safety principles in engineering design. Eventually, this has led to Knowledge Based Engineering as a specific school of design thinking (Torenbeek, 2013).

The search for performance optimization and reduction of uncertainties has created a continuous exploration of design variations and selection of better performing design solutions. This has created generations of commercial and military aircraft designs with similar morphology, configurations and properties. Such solutions can either have a derivative or disruptive nature. Vincenti elaborates on the role of this *variation-selection* process in the innovation of aerospace design (Vincenti, 1994). Developing 'anomalies' should be considered in a historical context of design requirements, gradual changes in the operating context and consequences of design trade-offs. Although 'anomalies' may temporarily deviate from prevailing engineering judgement, specific concerns may force to deviate from this mainstream in exploring innovations. The variation-selection model of Vincenti takes it for essential and unavoidable that any search for knowledge that is new, that is not attained before, must involve an element of what is called 'unforesightedness'. The outcome cannot be foreseen or predicted when the variant is proposed. Foresight on performance has been both tested at the component and subsystem level prospectively by modelling and simulation and retrospectively by flight testing and operational feedback. Such 'unforesightedness' comes with balancing gains as well as costs. The outcomes of such a balancing may favour specific design trade-offs, but should be considered in their historical context and operational demands. As speed increased, drag became dominant in the design trade-offs in designing retractable gears. The generalized knowledge that retractable gears were favourable, was the product of an unforesighted variation-selection process and was valid for a specific class of aircraft designs (Vincenti, 1994). Similar trade-offs in context can be observed in the design of modern commercial aircraft in balancing weight and fuel consumption versus structural integrity and dynamic stability (Torenbeek, 2013). Flight envelope protection was introduced to refrain the pilot from entering the margins of the operational envelope at the cost of loss of pilot situation awareness in critical situations (De Kroes and Stoop, 2012). The application of automation in cockpits has

a proven track record of substantial gains in safety, efficiency and accuracy, but comes at a cost of loss of pilot situation awareness in critical situations, increased cognitive task loads and loss of basic flying skills. The notion of 'unforesightedness' has not yet been expanded from the component to the systems level.

3 Socio-technical systems engineering challenges

The driving forces for enhancing safety foresight come from both within a sector and without. From within, improvements in technology and a need for awareness of potential negative effects of technology drive the need to understand the causes of accidents. From without, public trust, political pressure and international coordination drive the need to prevent and mitigate accidents. For commercial aviation, all of these came together at the same time -as the need for interoperability, punctuality and reliability, international determination of responsibility and responding to the inherent human fear of being in the sky- and converged to demand the highest standards of proactive safety. Such safety foresight had to cope with system properties of both a legal, social and technical nature.

3.1 Legacy systems and 'early warnings' of safety performance

In designing complex socio-technical systems, due to their legacy nature and dependences on other systems, there is no opportunity for real time and full scale testing during introduction and adaptation. Apart from their complexity, there are unacceptable consequences of fault and failure propagation of disruptions through a global network that operates on a 24/7 basis. The vulnerability of such systems is a critical parameter in assessing the consequences of change and adaptation. Such vulnerability is assumed to be caused by unpredictable and unnoticed interactions between system components. According to Dekker, 'drift into failure' is a gradual, incremental decline into disaster driven by environmental pressure, unruly technology and social processes that normalize growing risk (Dekker, 2011).
However, due to a lack of understanding of its incubation, 'drift into failure' inevitably makes a conventional trial and error approach inapplicable in high technology network systems. Such a trial and error approach should be replaced by a predictive approach on a systems level of performance. Applying 'early warnings' of mishaps to prevent a 'drift into failure' during final phases of the design and construction or during normal operations is too late an intervention. Huge costs will occur for control and modification in case of detection of unacceptable deficiencies and deviations. Consequently, 'drift into failure' is an obsolete construct in controlling and explaining 'emergent properties' in high technology systems. This construct should be replaced by structuring system development and positioning of safety assessment tools and techniques at specific points in each phase of the design, development and operations of such systems. In creating new solutions with predictive potential on safety foresight, several with respect to safety so far unchartered scientific domains and disciplines have to be mobilized. Based on aerospace engineering experiences serious candidates are simulation and prototyping, forensic engineering, value operations methodology and state/space vector modelling (Vincenti, 1990; Torenbeek, 2013).
Analysing the complexity of socio-technical systems, the notion of 'drift into failure' is frequently used as an explanation of 'emergent' behaviour (Dekker, 2011). The

underlying notion of the 'incubation period' of such a drift before it emerges as a unanticipated property, remains undefined, unmeasurable and does not cover the dynamics of such a drift. This 'drift into failure' lacks the description and explanation of a triggering event and conditions that sets a sequence of events in motion. The margins and boundaries that separate regular performance from emergent failure remain undefined and hence, uncontrollable. The concept of state/space vectoring of safety events has been conceptually formulated as a potential answer to these issues of safety margins (Stoop and Van der Burg, 2012). State-space modelling serves the identification of performance boundaries and dissimilarity distances between safe and unsafe performance by introducing vulnerability and margins to system boundaries under specific conditions (Van Kleef, 2017). To communicate about safety, actors have to agree on system states and margins to boundaries, using design requirements and specifications as starting points. Introduction of limit states, operating envelopes and viable envelopes facilitate understanding of margins for prevention and recovery. Such a state/space modelling approach defines safety as a social construct within physical boundaries and operational conditions. Simultaneously, such an approach defines the resilience margins for system recovery and complies with the European codes for technical safety directives and safety integrity levels (Van Kleef, 2017). This state/space vector approach enables quantification of survivability margins to operating limits and a measurable comparison between various system states. Such an approach does neither rely on a normative judgement on acceptability of risks, nor on quality of design or performance.

An adequate definition of the notion of 'state' is given by systems theory. The state of a vector $\vec{x}(t)$ in its present situation can be described, based only on the information and control based on the previous situation. We only need this information to predict the future state of the vector. The dynamics of the system can be described with a state-space equation:

$$\frac{d}{dt}\vec{x}(t) = f(\vec{x}(t), \vec{u}(t), \vec{d}(t), t) \text{ and } \vec{x}(k+1) = f\left(\vec{x}(k), \vec{u}(k), \vec{d}(k), k\right).$$

In this equation $\vec{u}$ is the control vector and $\vec{d}$ the disturbance. This first equation is the continuous time version, while the second is the discrete or event based version, in which k is the actual event.

Rather than just stating *safety factors* we now have a concept of real system safety related *events* having an impact magnitude and a directional bias relative to the dimensions of the system model. The model suggests multi-vectorial design solution spaces which have meaning relative to the dimensions of safety in terms of the contribution or impact within each dimension and the overall resulting orientation or direction of the safety issue being considered. Consequently, safety is significantly elevated from the very basic consideration of factor, to a new level where it is being quantified as a multi-dimensional quantity with a resulting orientation that defines the choice of the designer or operator relative to their values regarding safety. With reference to the Value Operations Methodology, this leads us to the position where safety can be integrated into the general design approach of the air transport system according to an equation relating KPI to some delta value of the form:

$$\Delta V = \alpha_C(C_1/C_0) + \alpha_U(U_1/U_0) + \alpha_M(M_1/M_0) + \alpha_E(E_1/E_0) + \alpha_P(P_1/P_0) + \alpha_S(S_1/S_0) + \varepsilon$$

where Cost efficiency is represented by *C* (revenue/cost), Utilization by *U*, Maintainability by *M*, Environmental Quality by *E*, Passenger Satisfaction by *P*, Safety by *S* and finally including an error *ε*, consideration. Consequently, safety as a function of: safety = fn (context, culture, content, structure, time), can be

characterised with the individual drivers associated with each dimension so that safety in its vectorial and most realistic form can be integrated into the overall integrated system of systems design solution space. In shifting from factor towards vector, safety critical behaviour of open and dynamic systems can be analysed by identifying inherent properties during design before they manifest themselves as emergent properties during operations. By doing so, safety can be assessed and optimized pro-actively as a critical strategic value against other system values in a dynamic and complex systems perspective. This approach substantiates the notion of foresight.

3.2 High energy density systems

Socio-technical systems must be safeguarded by design due to their specific characteristics as a distinct category of high energy density complex systems. Management of the operational energy that is stored in the system is a challenge that must be controlled proactively throughout all system states, mission phases and operating constraints.
Due to the increase in size and scale of modern socio-technical systems, the uncontrolled release of energy in a specific event can result in catastrophic material consequences and loss of all lives of a large population at risk, both inside and outside a system. The operational energy stored in complex systems can be expressed in Megawatts as the sum of kinetic and potential energy. The energy content of a High Speed Train and a Jumbo jet that has to be controlled during operations can be compared to nuclear power plants with respect to their catastrophic potential, as depicted in table 1.

Table 1 Operational system energy content

	weight	speed	altitude	Energy
High Speed Train	430 tons	250 km/h	ground level	1053 MW
		320 km/h	ground level	1740 MW
A380 Jumbo jet	MTW 575	900 km/h	10.000 m	75 000 MW
	at take-off MTOW 575 tons	260 km/h	ground level	1500 MW
	at landing MLW 386 tons	260 km/h	200m above ground level	1252 MW
Nuclear power plant	Average size			800 MW
	Borsele (Neth)		Sea level	450 MW
	Chernobyl		Sea level	600 MW
	Fukushima		Sea level	784 MW

Such an operational energy management strategy is interesting in particular in aviation with respect to the balance between kinetic energy due to the airspeed control and potential energy due to the altitude and attitude control. The operational energy of an aircraft has to be controlled and dissipated back to zero in order to bring the flight to a safe end. This kinetic and potential energy distribution varies across the various flight phases. This means that the energy balance management in the cruise

flight phase is based for 25% on the speed control and for 75% on the altitude and attitude control. During final approach and landing, the potential energy reduces from 75% at cruising altitude to 19.6% of the total energy content. The energy ratio between theses phases subsequently changes from potential energy management towards a predominant kinetic energy management by keeping control over speed and attitude.

3.3 Intrinsic systemic hazards

From the early days of aviation, stall has been an inherent system 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. These experiences convinced the Wright brothers to design their aircraft in a 'canard' configuration, facilitating an easy and gentle recovery from stall. Over the following decades, stall has remained as an intrinsic 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. Fixed-wing aircraft can be equipped with devices to prevent or postpone a stall or to make it less (or in some cases more) severe, or to make recovery easier by training and certifying pilots.
A further analysis reveals some more fundamental flight performance issues (Obert, 2009):

- All stall recognizing and mitigating strategies have not eliminated the stall as a phenomenon; major stall related accident still occur
- Airspeed indications rely on the use of Pitot tube technology. Applications of a new technology such as GPS provides redundancy in air data information
- In contrast with roll and yaw control, pitch control of aircraft is not redundant. There are no substitute strategies for controlling pitch of commercial aircraft, in contrast with the military, where thrust vectoring is an option
- Angle of Attack in commercial aviation is a secondary parameter, derived from Indicated Air Speed. There is no direct alpha indicator, in contrast with the military
- 4^{th} generation civil aviation aircraft lack the ability to create a negative pitch moment throughout the flight performance envelope by having direct access to speed and attitude as safety critical flight parameters.

Despite all efforts to reduce stall and deep stall to acceptable levels of occurrence, such events still happen occasionally in the commercial aviation community, raising concern about their emerging complexity, dynamics and impact on public perception on safety of aviation (Salmon, Walker and Stanton, 2016). Such events have been subjected to major accident investigations are swerve as triggers for change throughout the industry. Most recent cases are Turkish Airlines flight TK1951, Colgan Air flight 3407, Air France flight AF 447, Air Asia flight 8501 and Air Algerie flight 5017.
In a debate on high-altitude upset recovery, Sullenberger –captain of the Hudson ditching of flight US 1549- described stall as a seminal accident. "We need to look at it from a systems approach, a human/technology system that has to work together. This involves aircraft design and certification, training and human factors. If you look at the human factors alone, then you're missing half or two-thirds of the total system failure...".

4 Beyond 10^{-7} safety

4.1 Derivatives versus disruptives: the Valley of Death

The responses of aircraft manufacturers to stall have been different. Airbus took a different approach in designing the Primary Flight Display (PFD) than Boeing with eventually, equal safety performance levels. Airbus designed alpha floor protection in the fly by wire concept, which should greatly reduce opportunities for stall by automatically adjusting pitch and power to counteract the stall. Boeing choose to address pilot recognition of an impending stall. The Asiana B 777 accident demonstrated that pilots my fail to recognize low energy states preceding a stall, much as the Air France A330 accident demonstrated that alpha floor protection may fail due to unreliable speed and altitude sensors. By applying existing technology and design features that are incorporated to mitigate stall consequences, neither approaches are fail safe.
The introduction of Glass Cockpits and 3D Flight Displays have improved the navigation task of pilots considerable, but have not simultaneously improved the pilots' attitude towards spatial and situational awareness (Lande, 2016).
Manufacturers have reduced the workload of pilots and introduced the flight envelope protection to avoid entering a stall situation. However, stall and deep stall as a low speed/high alpha flight condition are inherent to the physical properties of fixed wing aircraft, similar to vortex ring state conditions for helicopters. A safe escape from such inherent flight conditions requires basic knowledge of pilots on aerodynamics and flight mechanics. Disorientation and confusion may lead pilots into loss of attitude awareness. The availability of a large and intuitive PFD with an Angle Of Attack indicator, integrated in the Basic-T configuration may enable a pilot in a quick regain of control by providing the pilot with situational awareness (Lande, 2016). According to Lande, future PFD's should be based on a synthetic picture of the outside world with overlaid prominent and transparent primary flight instruments, including an AOA indicator. It enables the pilot to gain a 3D attitude awareness. Apart from flying in non-normal conditions spatial disorientation may also be caused by somatogravic and somatogyral illusions. The strongest visual cue a pilot has becomes absent in visual flight in darkness, where reliance on flight instruments becomes critical in absence of a natural horizon.
In the discussion on a recent series of accidents, the focus has been on pilot knowledge and skills and less on Primary Flight Display design. Developments in glass cockpits and data integration provide an opportunity to explore issues in situation awareness, spatial disorientation, automation attitude and team work for a next generation of aircraft handling and cockpit design (Mohrmann et.al., 2015). Trade-offs, based on cost-benefit considerations however, depend on customer acceptance, cost awareness and public confidence in the safety of aviation. Introducing safety enhancement design solutions is submitted to a complex interaction between design, manufacture, operation costs and societal appreciation of safety. The outcomes of such trade-offs define whether it is possible to introduce either a derivative or a disruptive solution. Most innovative and disruptive solutions that are developed technically successful, do not survive the Valley of Death in their implementation phase due to such considerations (Berkhout, 2000).

In elaborating visual interpretation of information, a series of disruptive concepts can be considered potential game changers in enhancing flight safety. These game changers supersede the level of intervening either in the man or the machine component of complex and dynamic sociotechnical systems. They are frequently discussed in attempts to cross the 10^{-7} boundary. Such concepts deal with Angle of Attack indicators, Intuitive Primary Flight Display, recovery from non-normal flight situations, asymmetric flight, Total Energy Management Systems and Good Airmanship substantiation. These disruptive designs however, died in beauty in the Valley of Death between their invention and implementation due to a lack of a transition strategy and integration at a systems level.
While pragmatic solutions have achieved a high level of sophistication in stall mitigation and recovery, a more fundamental approach to stall avoidance should be developed in order to deal with this intrinsic system property. A new unit of analysis of flight control should be applied, combining both design of man, machine and their interfaces (Woods, 2016). Such a unit of flight control enables integration of disruptive designs into a new man-machine-interface concept. An innovative solution to this more fundamental issue should comply with principles of dynamic flight control over the fundamental forces that are exercised on general aviation and commercial aircraft and the feedback to the pilot in a combined intuitive and cognitive decision making (Stoop and De Kroes, 2012).

4.2 The Kestrel concept

In leaving the Valley of Death, similarities with bird flight control enable a integration of several of the disruptive designs into the Kestrel concept, consisting of:

- 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.

Fig 1. The Kestrel concept

An innovative design is suggested, based on these principles of dynamic vehicle control (De Kroes, 2012). The design combines four building blocks as engines for foresight; understanding flight dynamics, integral systems approach, total energy management and intuitive man-machine- interface design. This design is called the 'Kestrel' concept, aiming at creating redundancy for physical lift generation by stall shields during high Angle of Attack conditions, supported by dedicated software for the integral man-machine-interface flight control unit.
Assessment of the 'Kestrel' concept as a feasible and desirable innovation can only be done in the early phases of conceptual design on a consensus base. Discussing the issue of stall and remedies for stall related accidents cannot be allocated to a single actor or isolated contributing factor. Feedback from operationally 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 encompassing proactive survey during design and development. A multi-actor assessment should identify strengths and weaknesses, opportunities and threats of the Kestrel concept shield, providing a safety impact assessment before the concept is released for practical use (Stoop and De Kroes, 2012).

5 Conclusions

In answering the initial question, *How did aviation become so safe*, an analysis of the history of aviation shows a preoccupation with safety from the beginning, because of the intrinsic hazards involved in flying. Foresight has been designed into the aviation system from the start on.

Several characteristics have favoured a foresight on safety as a strategic design value, based on retrospective experiences:

- Institutional arrangements at a sectoral level, such as ICAO and its Annexes structure
- Harmonized legal responsibilities at the national State level
- Integral safety performance indicators throughout the system life cycle phases
- Feedback from reality by learning from mishaps, accidents and incidents
- Selecting technology as the flywheel for progress created a shared body of knowledge during design and operations, substantiated in a KBE design methodology
- Application of a 'variation-selection' process in experimental exploration of technological innovation and disruptive design solutions.

In replying to *And Beyond* and to enable crossing the mythical 10^{-7} risk boundary in aviation, innovative strategies should be explored to facilitate a prospective foresight on safety:

- Application of system engineering principles and state-space modelling approaches
- Shifting from safety performance indicators to system properties and design principles
- Recognition of game changers and transition strategies in order to surpass Valley of Death traps in implementing innovations and disruptive solutions
- exploring disruptive variations to substantiate their integration at the conceptual design level in creating a new unit of man-machine-interfacing design concepts, such as the 'Kestrel' concept.

References

Berkhout, A., (2000). *The Dynamic Role of Knowledge in Innovation*. The Netherlands Research School for Transport, Infrastructure and Logistics TRAIL, June 2000. Delft University of Technology.

Boosten, G., (2017). *The (Congested) City in the Sky. The capacity game: Finding Ways to Unlock Aviation Capacity.* Amsterdam University of Applied Sciences.

Cairns, (1961) *Report of the Committee on Civil Aircraft Accident Investigation and Licence Control*. Ministry of Aviation, Her Majesty's Stationary Office, London.

Dekker, S., (2011). *Drift into Failure. From Hunting Broken Components to Understanding Complex Systems.* Ashgate Publishers

De Kroes J.L., (2012). *Commercial plane or flight simulator, adjustable fuselage control surface, computer program product and method.* Patent P96519NL0, deposited on 10 Jan 2012

ETSC, (2001). *Transport accidents and incident investigation in the European Union.* European Transport Safety Council. ISBN 90-76024-10-3, Brussels

Flanagan, (1948). *The aviation psychology program in the Army Forces*. Washington D.C. Air Force, 1948

Freer, (1986.1). The roots of internationalism 1783 to 1903. *ICAO Bulletin, Vol.41 No.3, March 1986,* pp.3-32.

Freer, (1986.2). En-route to Chicago, 1943-1944, *ICAO Bulletin, Vol.41, No 7, July 1986*, pp.39-41

Freer, (1994). ICAO at 50 years: Riding the Flywheel of Technology. *ICAO Journal Vol.49 No 7,* September 1994, pp.19-32

Hengst S., Smit K. and Stoop J., (1998). Eds *Proceedings of the Second World Congress on Safety of Transportation. 18-20 February 1998.* Delft University of Technology.

ICAO, (2001). Aircraft Accident and Incident Investigation, *Annex 13 to the Convention on International Civil Aviation. International Standards and Recommended Practices.* Ninth Edition, July 2001

Kahan J., (1998). Safety Board Methodology. In: S. Hengst, K. Smit and J.A. Stoop (Eds) *Proceedings of the Second World Congress on Safety of Transportation. 18-20 february 1998.* Delft University of Technology.

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

McIntyre, G., (2000). *Patterns in safety Thinking*. Ashgate

Mohrmann F., Lemmers A. and Stoop J., (2015). *Investigating Flight crew recovery Capabilities from System Failures in Highly Automated Fourth generation Aircraft.* Aviation Psychology and Applied Human Factors, Vol 5(2), 2015

Petroski, H., (1992). *To Engineer is Human. The Role of Failure in Successful Design.* Vintage Books, New York

Roed-Larssen, Stoop and Funnemark (2005). *Shaping public safety investigations of accidents in Europe.* An ESReDA Working Group Report. Det Norske Veritas.

Smart, K., (2004). Credible investigation of air accidents. *Special Issue of the Journal of Hazardous Materials. Papers from the JRC/ESReDA Seminar on Safety*

Investigation of Accidents, Petten, the Netherlands, 12-13 May, 2003. Vol 111 (2004), 111-114.

Obert, E., (2009). *Aerodynamic Design of Transport Aircraft*. IOS Press 2009

Salmon, P.M., Walker, G.H. and Stanton, N.A., (2016). *Pilot error versus socio-technical systems failure: a distributed situation awareness analysis of Air France 447.* Theoretical Issues in Ergonomic Science, 17 (1), pp 64-79

Stoop, J.A. and De Kroes J.L., (2012). *Stall shield devices, an innovative approach to stall prevention?* Proceedings of the Third International Air Transport and Operations Symposium 2012. Delft, 18-20 June 2012. Ed. R. Curran, Delft University of Technology.

Stoop, J.A. and Van der Burg, R., (2012). *From factor to vector, a systems engineering design perspective on safety.* PSAM 11 and ESREL 2012 Conference on Probabilistic Safety Assessment June 25-29, Helsinki, Finland

Torenbeek, E., (2013). *Advanced Aircraft design. Conceptual design, Analysis and Optimization of Subsonic Civil Airplanes*. Wiley Aerospace Series

Van Kleef, E. and Stoop J.A., (2016). *Life cycle analysis of an infrastructural project.* 51th ESReDA Seminar on maintenance and Life Cycle Assessment of Structures and Industrial Systems, 20-21 October, Clermont-Ferrand France

Vincenti, W., (1990). *What Engineers Know and Hoe They Know* It. Analytical Studies from Aeronautical History. The John Hopkins University Press.

Vuorio A., Stoop J., and Johnson C., (2017). *The need to establish consistent international safety investigation guidelines for the chemical industries.* Safety Science 95:62-74, July 2017

Wittenberg, H., (1979). *Safety in aviation; achievements and targets.* Memorandum M-353, Faculty of Aerospace Engineering. Delft University of Technology.

Woods, D.D., (2016). *Origins of Cognitive Systems Engineering*. P. Smith and R. Hofman (Eds). Cognitive Systems Engineering: A Future for a Changing World.