View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by City Research Online

Quinn, A., Bond, S.J. & Maropoulos, P. (2011). New safety model for the commercial human spaceflight industry. Paper presented at the Fifth IAASS Conference: A Safer Space for a Safer World, 17-10-2011 - 19-10-2011, Versailles, France.

CITY UNIVERSITY LONDON

City Research Online

Original citation: Quinn, A., Bond, S.J. & Maropoulos, P. (2011). New safety model for the commercial human spaceflight industry. Paper presented at the Fifth IAASS Conference: A Safer Space for a Safer World, 17-10-2011 - 19-10-2011, Versailles, France.

Permanent City Research Online URL: http://openaccess.city.ac.uk/605/

Copyright & reuse

City University London has developed City Research Online so that its users may access the research outputs of City University London's staff. Copyright © and Moral Rights for this paper are retained by the individual author(s) and/ or other copyright holders. Users may download and/ or print one copy of any article(s) in City Research Online to facilitate their private study or for non-commercial research. Users may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain. All material in City Research Online is checked for eligibility for copyright before being made available in the live archive. URLs from City Research Online may be freely distributed and linked to from other web pages.

Versions of research

The version in City Research Online may differ from the final published version. Users are advised to check the Permanent City Research Online URL above for the status of the paper.

Enquiries

If you have any enquiries about any aspect of City Research Online, or if you wish to make contact with the author(s) of this paper, please email the team at publications@city.ac.uk.

NEW SAFETY MODEL FOR THE COMMERCIAL HUMAN SPACEFLIGHT INDUSTRY

Andy Quinn [(1)], Dr Steve Bond [(2)], Prof. Paul Maropoulos [(3)]

[(1)]Saturn SMS, 1 Newton St Loe, Bath, UK, BA2 9BR, E-mail: andyquinn@saturnsms.com

[(2)]City University, London, UK, E-mail:S.J.Bond@city.ac.uk

[(3)]University of Bath, UK, E-mail: P.G.Maropoulos@bath.ac.uk

ABSTRACT

The aviation and space domains have safety guidelines and recommended practices for Design Organisations (DOs) and Operators alike. In terms of Aerospace DOs there are certification criteria to meet and to demonstrate compliance there are Advisory Circulars or Acceptable Means of Compliance to follow. Additionally there are guidelines such as Aerospace Recommended Practices (ARP), Military Standards (MIL-STD 882 series) and System Safety Handbooks to follow in order to identify and manage failure conditions. In terms of Operators there are FAA guidelines and a useful ARP that details many tools and techniques in understanding Operator Safety Risks. However there is currently no methodology for linking the DO and Operator safety efforts. In the space domain NASA have provided safety standards and guidelines to follow and also within Europe there are European Co-operation of Space Standardization (ECSS) to follow. Within the emerging Commercial Human Spaceflight Industry, the FAA's Office of Commercial Space Transportation has provided hazard analysis guidelines. However all of these space domain safety documents are based on the existing aerospace methodology and once again, there is no link between the DO and Operator's safety effort.

This paper addresses the problematic issue and presents a coherent methodology of joining up the System Safety effort of the DOs to the Operator Safety Risk Management such that a 'Total System' approach is adopted. Part of the rationale is that the correct mitigation (control) can be applied within the correct place in the accident sequence. Also this contiguous approach ensures that the Operator is fully aware of the safety risks (at the accident level) and therefore has an appreciation of the Total System Risk.

The authors of this paper contend that it is better practice to have a fully integrated safety model as opposed to disparate requirements or guidelines. Our methodology is firstly to review 'best practice' approaches from the aviation and space industries, and then to integrate these approaches into a contiguous safety model for the commercial human spaceflight industry.

1. INTRODUCTION

Within the aerospace and space sectors there are regulations, standards and guidance material to govern the activities and to assist the designers and operators in attaining the required level of safety. In the first instance, aircraft designers build aircraft such that they can sell their certified product to many operators; thus when they deliver the aircraft their main part of the job is done and they then provide additional information such as Service Bulletins (in the event of serious issues) and so on. The operator then begins their involvement in the safety effort by identifying operator risks and then managing Air Safety Reports (ASRs) when incidents occur. However the operator analysis may be qualitative or based on different metrics than the designer analysis i.e. it is focused only on the operations. As this has been the case for many years some may ask why this approach should be questioned. Others may state that one cannot merge the designer and operator analysis. This paper attempts to address this problematic issue because of the perceived nature (role) of the emerging suborbital players; meaning that suborbital designers such as XCOR[1], EADS (Astrium)[2] and Rocketplane[3] will not only design the vehicles (only a handful of vehicles initially) but will also operate them. Herein lays the issue whereby civil aerospace aircraft designers do not operate vehicles and so there is no guidance to achieve this.

2. CURRENT DISPARATE SAFETY ANALYSIS APPROACH

The current approach towards safety is to undertake analysis to meet requirements and targets (objectives) as applicable to the boundaries of said requirements. The metrics involved are different for designers and operators and therefore a contiguous approach is not employed. The disparate approach is illustrated in *Figure 1* below:

[1] http://www.xcor.com/

[2] ttp://www.astrium.eads.net/en/programme/space-plane.html

[3] http://www.rocketplane.com/

Figure 1: Disparate Relationship between Design Analysis and Operator-based Analysis

In particular there are different probability classifications between DO and operator in that the DO is analysing failure conditions and operators are analysing safety risk through flight data monitoring. There may be similar severity classifications although catastrophic is seen by some as a single death whereas its severity relates to multiple deaths in other classifications. The operator thinks in terms of specific accident or Safety Significant Event (SSE) i.e. a near mid-air collision (MAC), whereas the DO works to failure conditions with associated severity i.e. no specific accident detailed rather it is implicit.

2.1. Design Organisation Analysis

In the Civil Aviation industry the designers must meet certification baseline requirements and in terms of safety this includes meeting specified safety objectives for failure conditions i.e. for a catastrophic failure condition the designer must meet 1E-9 per flying hour. The Aircraft Loss target stated in Federal Aviation Regulations (FAR)/Certification Specification (CS) 25.1309[3] is based on the world-wide accident rate which is about one per million flight hours, i.e. a probability of 1E-6 per hour of flight. The accident rate was first analysed in the UK for the British Civil Aviation Requirements (BCAR). It was deduced that 10% of accidents were attributed to failure conditions involving critical aircraft systems, i.e. 1E-1 therefore the overall target is 1E-7. Arbitrarily it was deduced that there were approximately 100 system catastrophic failure conditions assumed to exist on civil aircraft, i.e. 1E+2. Therefore to prevent a deterioration of the current fatal accident rate, DOs must show that the probability of occurrence of each catastrophic failure condition was at least $1E^{-6}$ x$1E^{-1}$/$1E^{+2}$ = $1E^{-9}$ per flying hour.

This criteria and logic follows to 'hazardous', major and minor failure conditions and these have apportioned safety objectives per §25.1309[3]. Figure 2 shows the relationship between probability of a failure condition and its associated severity classification.

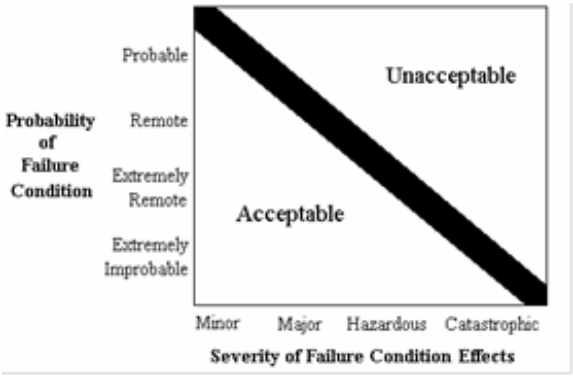

Figure 2: Relationship between Probability and Severity of Failure Condition Effects – from CS-25

Failure Conditions are recognised events from standard Functional Hazard Analysis (FHA) such that DOs must meet the associated safety objective. The following examples are from §23.1309 [4]:

- Catastrophic Failure Condition;
  - Misleading attitude information to control roll and pitch
- Hazardous Failure Condition:
  - Total Loss of altitude information

The above failure condition within the DO analysis (such as using Fault Tree Analysis) consists of lower-level system hazards and these in turn have contributory events (causes or base events). This explicit relationship is shown in Figure 3:

Figure 3: Design level sequence to Failure Condition

The DO's Risk Reduction methodology is based on the 'fail-safe' design concept, which considers the effects of failures and combinations of failures in defining a safe design. This paper recognises this and assumes that DOs implement the fail-safe design concept in order to achieve the desired safety objectives and therefore provide an airworthy aircraft that meets its certification requirements.

Guidelines for designers are comprehensive in the aircraft domain such as ARP 4754 [5] and ARP 4761 [6] for system safety analysis and also MIL-STD 882-D [7].

2.2. Operator Safety Analysis

In terms of operator analysis there are various guidelines on implementing a Safety Management

System (SMS) and employing a Flight Operations Quality Assurance (FOQA) process. However unlike their designer counterpart there are no specific safety targets or safety objectives to meet from a regulatory standpoint.

The FOQA process gathers data from a Quick Access Recorder (QAR) and identifies flight activities that are problematic in an operational sense because they are unsafe, inefficient or inconsistent with standard operating procedures. Operators then use the data in different ways and typically present these in 'Risk Profiles' to show the most frequent (and severe) events. Operator's safety department may also employ a hazard log and identify operator hazards; these will tend to be qualitative based. Guidelines to assist operators in undertaking safety analysis is contained in ARP 5150 [8], FAA AC 120-92 [9] and also AC150-5200 **[10]**. Figure 4 below details a suggested Risk Matrix for operators:

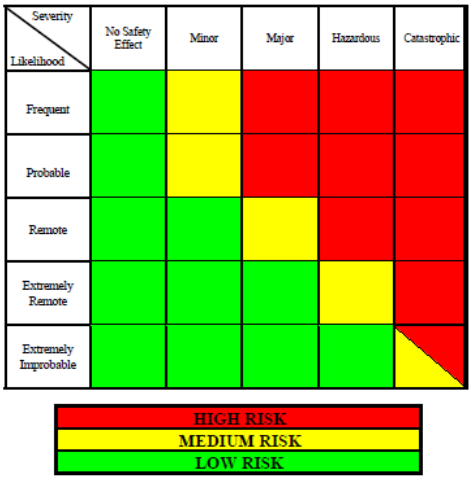

Figure 4: AC150-5200 SMS for Air Operators

In terms of understanding accident sequences other guidance material is available for operators such as the Global Aviation Information Network (GAIN) [11] whereby they indicate an operator based sequence leading to a primary hazard as depicted in Figure 5.

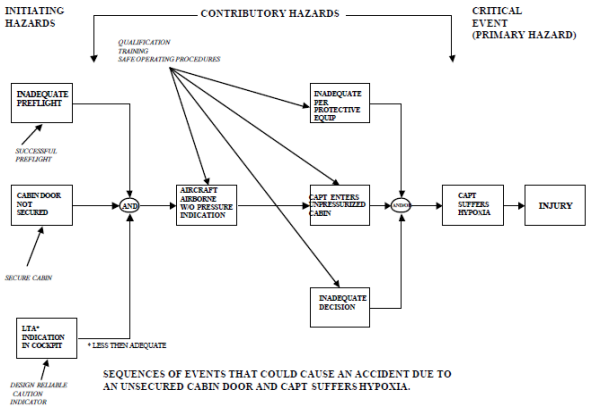

Figure 5: GAIN's operator accident sequence

The Aviation Risk Management Solution (ARMS) methodology [11]: **Global Aviation Information Network, Operator's Flight Safety Handbook, Issue 2, December 2001** **[12]** is a reasonable attempt at providing a system for operators to assess their risks by introducing an Operational Risk Assessment (ORA) process. The ARMS methodology and Excel spread-sheet (tool) is aimed at airlines and other air operators and is based on a two-tiered approach including a preliminary Event Risk Classification scheme followed by a more specific Safety Issues Risks Assessment (SIRA). The rationale stated in the methodology is that *'pre-ARMS' standard methodology is not anchored to any recognised industry reference'* (in terms of Operator Risk Management Matrices with severity and probability); this is correct and hence this paper has also recognised this but has focused on a new safety model that provides a contiguous safety approach i.e. the operator analysis **is** anchored to the design analysis and the metrics (per flying hour) are constant.

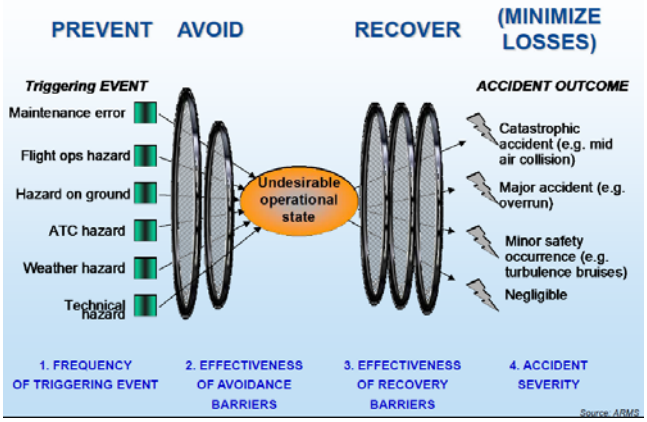

Figure 6: ARMS model

3. CONTIGUOUS SAFETY MODEL

Having identified that a gap exists between DO analysis and operator analysis the way forward would point to a function that could link to two disparate methods. As can be seen in Figure 7 below there are clear boundaries between systems, failure conditions and the aircraft.

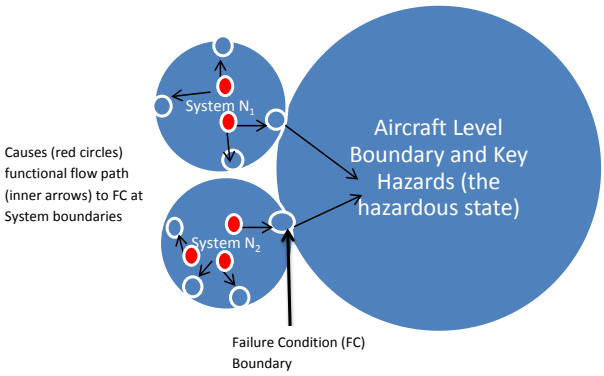

Figure 7: Boundaries between Systems and the Aircraft

Figure 8 below introduces a platform level hazard (the Key Hazard) that provides this function of linking the failure condition to an explicit accident. This is required such that the operator acknowledges their role in the accident sequence so that they can implement the operator controls and limitations more effectively. They will then explicitly know their accident risks and arguably if these were summed and shown to be independent accidents then the Total Risk for the aircraft and its personnel would be known.

Figure 8: Extended sequence to the accident via a platform level 'Key Hazard'

3.1. Aircraft Level Hazards

The DO analyses scope is up to the failure condition level in order to demonstrate that they have met the safety objectives. So it is here where we must start to continue the accident sequence and the obvious place to look is within the existing guidelines. ARP4754 [5] for example shows that there are indeed higher-level 'aircraft hazards' and these would equate to the 'key hazards' in the contiguous safety model.
So these higher-level aircraft hazards are key in that they are a not a function but a state of the aircraft and in particular within the accident sequence is when a 'hazardous state' occurs. For example misleading airspeed is a known failure condition but in itself does not directly lead to an accident and requires other events to occur. These other events such as change of flight parameter (height, angle of attack etc.) are then controlled by the pilot procedures and training; which is in the remit of the operator analysis.

As an example let us call this hazardous state a key hazard (at the aircraft level); for instance undetected (by pilot) vertical position error. Here we have a hazardous state whereby the failure condition has occurred AND the aircraft is not on its intended vertical level AND the pilot has not noticed or corrected (controlled) sufficiently.

The contiguous model is depicted in Figure 9 whereby the DO analysis (using Fault Tree Analysis for instance) demonstrates the vehicle meets the failure condition. The operator analysis would then use the failure condition as the starting point (either within a FTA or Event Tree Analysis)

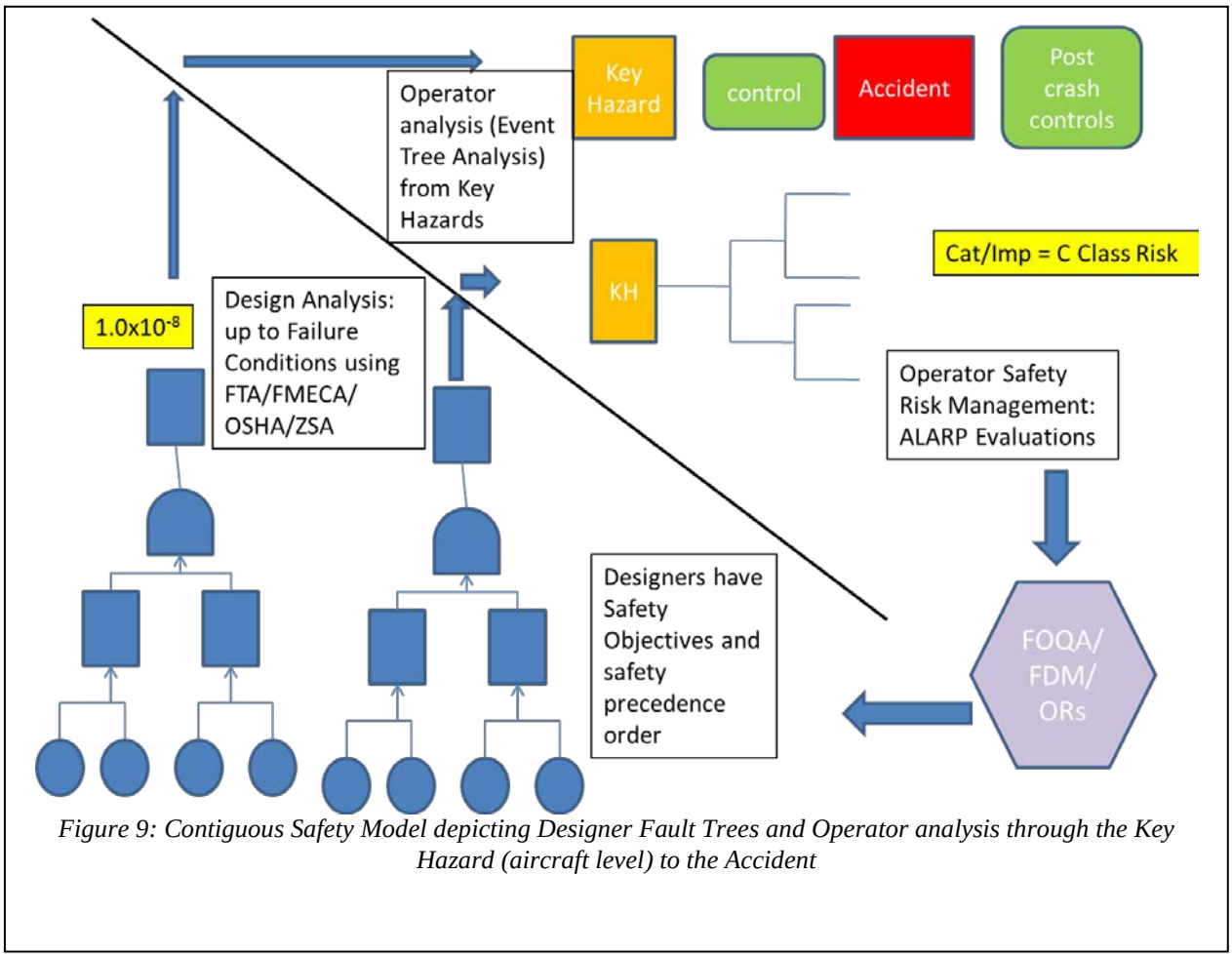

Figure 9: Contiguous Safety Model depicting Designer Fault Trees and Operator analysis through the Key Hazard (aircraft level) to the Accident

to continue the sequence by linking the failure condition via the key Hazard to the explicit Accident (or SSE). The operator is then well placed to link the relevant pilot procedural/training controls or Limitations within the sequence. This will then enable the operator to determine an Accident Risk (based on probability and severity).

3.2. Specific Accidents

There are specific recognised International Civil Aviation Organisation (ICAO) Accidents such as 'Mid-Air Collision (MAC) and Controlled Flight into Terrain (CFIT). These can be explicitly linked via the aircraft level hazardous state (the key hazard) and also the post-accident controls can be detailed more effectively (both designer-based and operator-based). The explicit accidents from ICAO [13] are:

1. Loss of Control – In flight (LOC-I)
2. Loss of Control – Ground (LOC-G)
3. Controlled Flight into Terrain (CFIT)
4. Mid Air Collision (MAC)
5. Explosion (Fuel Related)
6. Fire/Smoke (Non-Impact)
7. Fire/Smoke (post impact)
8. Loss of Thrust (system/component failure or malfunction – power-plant)
9. Structural Failure
10. System/Component failure or malfunction – non-power-plant

Additionally there are specific recognised ICAO Safety Significant Events (SSE). These are the non-catastrophic events that occur occasionally and are reported via the ASRs. Once again these can be explicitly linked via key hazards to SSEs and the controls can then be examined more closely as to their effectiveness. The ICAO list is as follows:

1. CFIT only marginally avoided
2. Near Mid Air Collisions
3. Events requiring the emergency use of oxygen by the flight crew
4. Aircraft structural failure/engine disintegrations not classified as an accident
5. Crew Incapacitation
6. Emergency Oxygen Use
7. Near Structural Failure
8. Fuel Emergency
9. Near LOC-I (performance)
10. Near LOC-I (Ops)

3.3. Specific Mitigation

3.3.1. Design Controls

The design mitigation is well documented and structured in the system safety analysis and this follows the best practice 'safety precedence sequence':

- *Eliminate the hazard*
- *Reduce the likelihood*
- *Reduce the severity*
- *Implement safety features*
- *Implement Warning Devices*
- *Provide procedures*
- *Provide Training*

3.3.2. Operator Controls

In terms of operator mitigation this takes the form of operator procedures, training and limitations. The reason for detailing and linking specific controls within the accident sequence is to be able to manage the controls more effectively. When a significant incident occurs (SSE) such as 'CFIT only marginally avoided' then the 'failed' controls can be scrutinised and improved (or new controls added).

Figure 10 below depicts a contiguous accident sequence with controls (green). From the sequence we can see that in order for an accident to occur would require the prime equipment (system) to fail, failure of the operating procedures (to use the design [redundancy] control) which then leads to the key hazard (hazardous state) and finally failure of any emergency procedures, lack of training and/or breach of any limitations.

It is important for both designer and operator to understand whether they are dealing with a 'barrier' control or 'recovery' control and that they form influencing factors within an accident sequence. Without the operator understanding the explicit sequence and how much 'credit' is taken for the operator controls then catastrophic accidents and hazardous events will continue (when in actual fact they could be prevented – this is proactive and cohesive safety management).

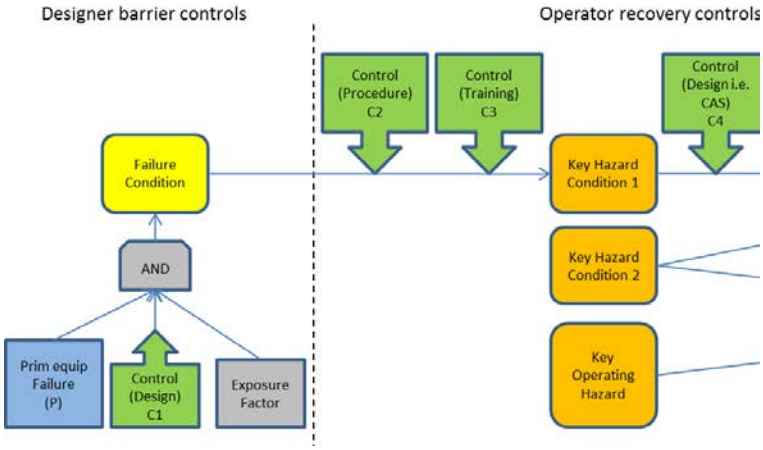

Figure 10: Explicit controls shown in the accident sequence

3.4. Case Study – Air France AF447

This section provides an example of the operator not fully understanding the explicit accident sequence and the importance of the 'credit' taken for operator controls (or lack of). This case study builds on the current facts that are known from the Bureau d'Enquêtes et d'Analyses (BEA) Interim Reports No.2 [14] and No.3 [15]. The case study of the AF447 disaster is representative of the disconnect that exists between Design Organisations and Airline Operators. The authors acknowledge that they do communicate, particularly in the form of Service Bulletins (SB) when a Safety Significant Event (Serious Incident) requires changes to design or procedural/ maintenance inspection strategies (as per the TWA flight 800 that resulted in Special Federal Aviation Regulation 88 requirements and subsequent SBs). The case study shows that previous Serious Incidents (from the Automatic Communication Addressing and Reporting System [ACARS]) resulted in SBs concerning a new design for the pitot-tubes yet Air France were still flying aircraft with the standard pitot-tubes

By using the *SATURN SAFETY MODEL* we can examine the sequential components and determine those that failed. In Figure 11 below we can see that the following controls failed:

- Redundant sensors – the 3 pitot tubes were the same and therefore were subject to common mode failures
- Key hazard procedural control failure – operating procedure to control the aircraft (at 5 degrees nose up and 85 per cent power is the standard procedure)
- Emergency recovery procedures (and training) – once passed the hazardous state of undetected speed error the pilot should have recovered the aircraft before the onset of stall i.e. the warnings of stall normally include 'stick-shakers' and warning horns
- No Limitations in place either to;
  - Avoid the altitude that the pitot-tubes could be subject to super-cooled water droplets and icing i.e. fly below Flight Level 310 (this would require more fuel to be carried to cross the Atlantic)
  - Avoid Flight in Icing conditions and flight in or near thunderstorms i.e. fly around (divert off track) any Cumulonimbus clouds (this would require more fuel to be carried if the forecast indicated clouds)

In this instance any of these design or operator controls could have broken the accident chain.

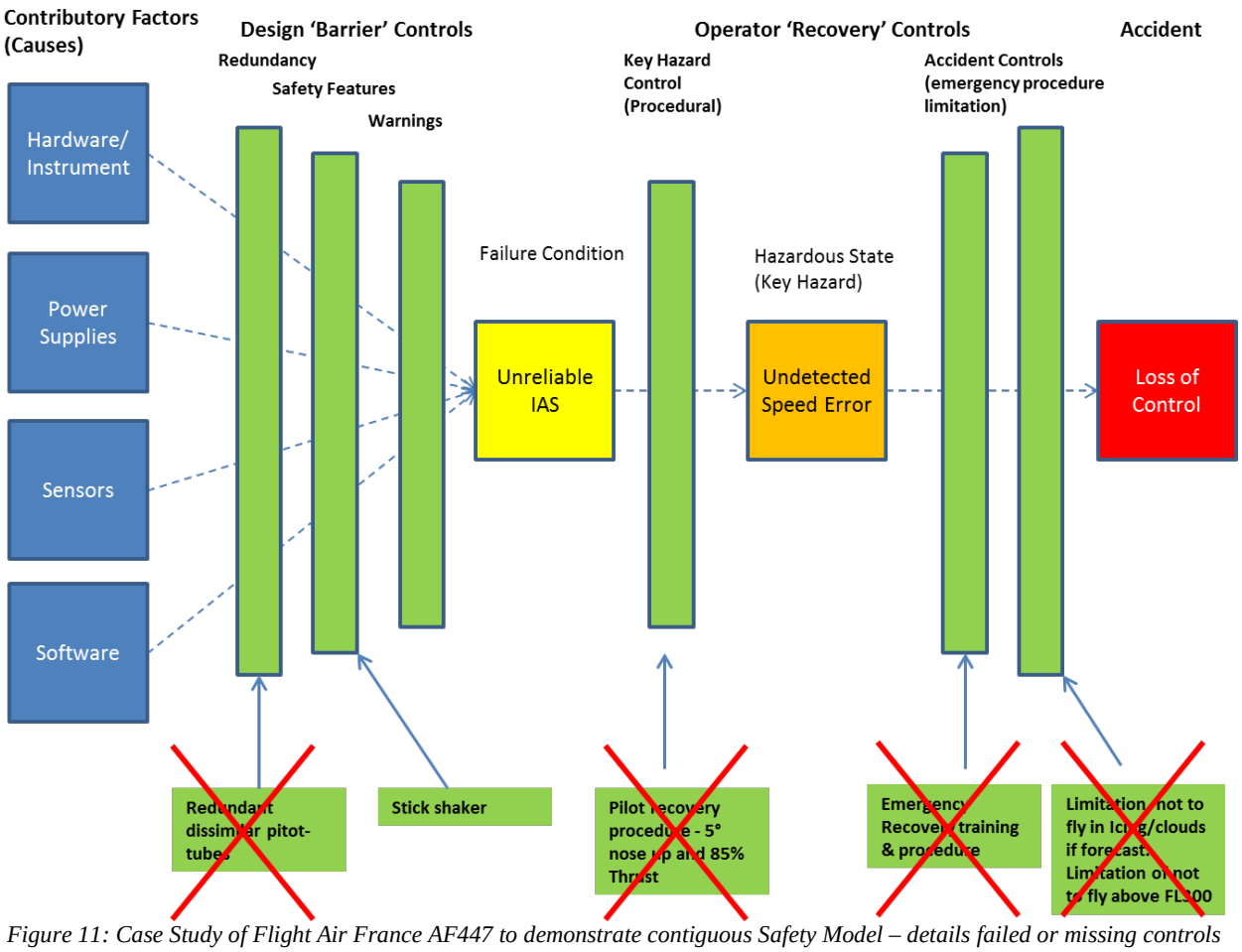

Figure 11: Case Study of Flight Air France AF447 to demonstrate contiguous Safety Model – details failed or missing controls

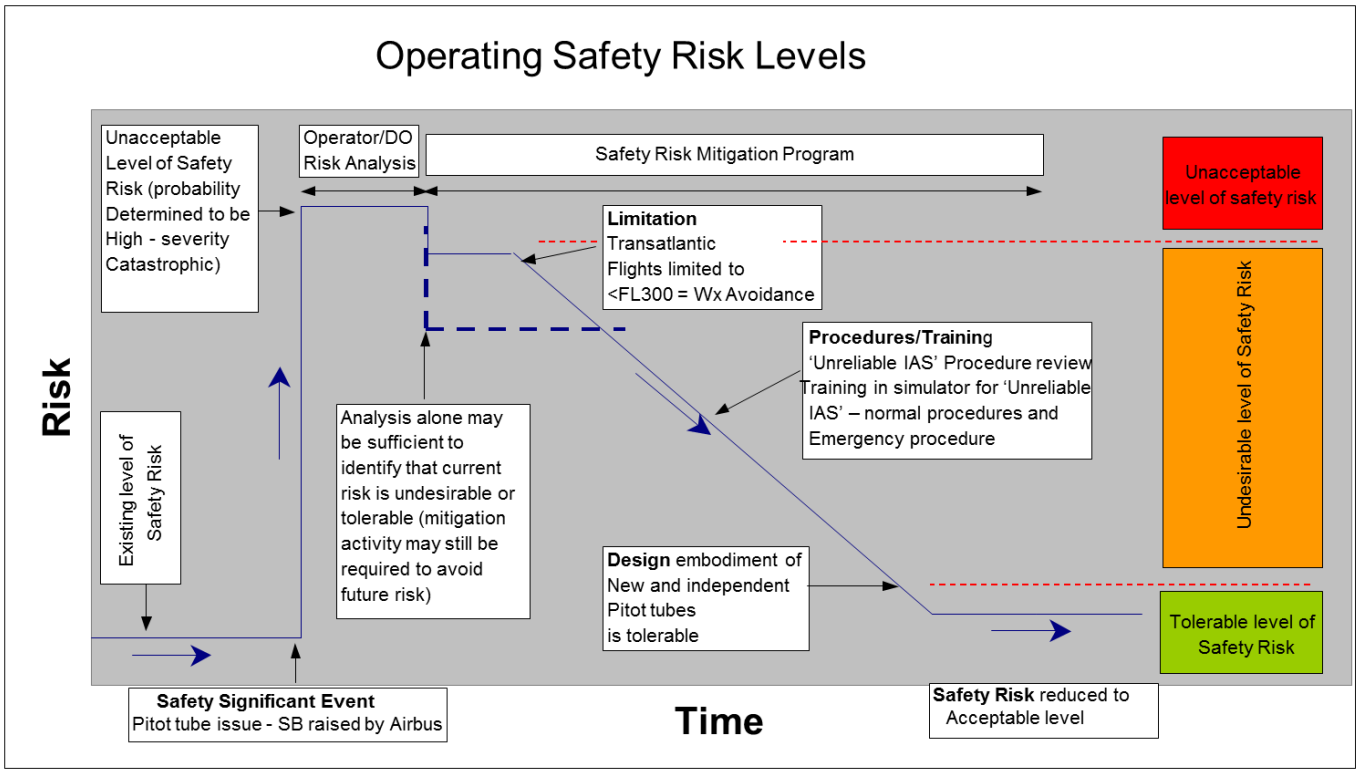

Figure 12: Waterfall diagram depicting the change in Risk due to a Safety Significant Event and subsequent mitigation strategies to reduce the Risk

A Waterfall diagram can be useful to show the existing level of Risk followed by the Risk as a result of a serious event. Then the proposed Risk reduction is detailed over an appropriate timescale. Figure 12 shows a tolerable level of risk (say for an individual accident of Loss of Control) and a new risk being identified i.e. a pitot-tube issue. A design organisation would initiate a Service Bulletin due to the fault but where does that leave the operator (instantaneously) in terms of risk? The designer normally gives a time period for implementing the SB but in the case of Air France AF447 they were still flying ten days after the issue of the SB (to change the pitot-tubes). The operator could have reviewed the previous occurrences in a 'Hazard Review Board' with the safety manager, chief pilot and design representative as a minimum. Then they could have identified the following control failures:

- Design Control failures:
  - Redundant system failures – design organisation issued pitot-tubes
- Operator Control failures:
  - Amend or re-brief normal procedures (this has now been done by Air France)
  - Amend the specific training or ensure pilots are trained more often (this has now been done by Air France)
  - Amend or re-brief emergency procedures (this has now been done by Air France)
  - Amend the emergency training or ensure pilots are trained more often (this has now been done by Air France)
  - Add a Limitation – this was not done and is not required now because the design control has effectively reduced the risk

These could be plotted on the Waterfall diagram to show proactive safety management in dealing with the risk whilst awaiting the design to be fully implemented (across the fleet).

4. RELEVANCE TO COMMERCIAL SPACEFLIGHT

The previous sections highlighted a gap between the design safety analysis and operator safety analysis within the commercial aviation domain. A 'Key Hazard' was identified at the platform level that could bridge the gap and therefore result in a contiguous safety approach. Is this approach applicable for the commercial spaceflight domain? In the commercial spaceflight domain the designer and operator are arguably have a much closer relationship than their aviation counterparts and in a lot of cases may be the same organisation i.e. in the suborbital domain XCOR will design and operate their 'Lynx' vehicle and for orbital flights 'Space X' will design and operate their Falcon spacecraft.

4.1. Aid to Certification/Launch License Approval

This close relationship can only assist in gaining certification or gaining a launch license approval from the authorities. Not only will the company be able to demonstrate the design (system safety) analysis they will be able to explicitly detail the accident risks involved with the vehicle. They will be able to demonstrate the 'barrier' controls in the design analysis (such as in Fault Trees) and also demonstrate the operator controls within the contiguous accident sequence.

4.1.1. Safety Target

This contiguous safety model approach is designed to assist in demonstrating that requirements and targets have been met.

The NASA Commercial Crew Development Program is a chance to enforce proper design and safety requirements in a formal and recognised approach (as opposed to a disparate approach for Space Shuttle and the International Space Station). Here is a new development and the safety model can arguably be applied for the orbital domain. The 'System' is a vertical reusable launch vehicle with expendable rocket boosters. Using the IAASS-ISSB Space Safety Standards Manual [16] we have a catastrophic (loss) safety target of 1 $x10^{-3}$ per mission. The next question to ask is can we use the same methodology per aviation to derive system level risk budgets? i.e. 10% of failures are due to critical systems therefore the catastrophic target is 1 $x10^{-4}$ per mission. Then in aviation there are 100 arbitrary critical systems and therefore in this case the safety objectives for catastrophic failure conditions would be in the order of 1 $x10^{-6}$ per mission. Is this practical? – some may say not when considering the Rocket Propulsion System (RPS) would be in the order of 1 $x10^{-4}$ per mission (thereby using up the entire risk budget).

But by using this safety target approach (with implicit safety objectives for lower level failure conditions) it drives the designer to build in redundancy; only then will the safety targets be close to being met from the design perspective.

Then we use the safety model to continue the accident sequence to the Spacecraft level key hazards and up to the accident and then beyond the accident (fire/explosion) with abort system and survivability systems as mitigation; thereby reducing the risk of multiple deaths (1st party crewmembers) and/or deaths to the support personnel (2nd parties) or the public (3rd parties).

The operator controls, training and limitations (flight profile, temperature limitations etc.) can be explicitly shown in the safety model and therefore the Accident Risks can be calculated. Also the abort systems and survivability systems can be shown 'post' the Accident in the sequence and appropriate credit taken within the analysis (further risk reduction). This is even more important to demonstrate this explicitly and in a contiguous manner should the safety target not be met i.e. the design fails to meet the safety target (but is within an order of magnitude for instance) and therefore the claims are on operator procedures, limitations and post-accident controls; this will therefore provide a more convincing argument to the authorities as to why the Spacecraft is 'acceptably safe'.

The same approach can also be used in the suborbital domain; even more so where some designs are aircraft-based and employ similar known sub-systems. Here a catastrophic (loss) safety target may be in the order of 1 $x10^{-4}$ per mission (flight hour equals a mission in this case). This is also challenging in that the RPS will be the main contributor once more and the design analysis will have to include the exposure factor (circa 90 seconds) which will assist in the calculations. Once again the safety model can explicitly detail the failure conditions and then accident risks via key hazards at the platform level; thus assisting with certification or launch license approval.

4.2. Spaceflight Case Study

To demonstrate the use of the contiguous safety model in the spaceflight domain we will use the Space Shuttle Challenger disaster as a case study. On 28 Jan 1986 Space Shuttle Challenger launched at 0500hrs (US time) after having been delayed from previous launches. Seconds after Launch Challenger's Expendable Rocket Boosters exploded, destroying the Space Shuttle System; all on board were killed in the 'mishap'. According to Diane Vaughan [17] the management played a large part in the Challenger disaster in that they authorised a Launch when the temperatures were extremely low and this was against the advice of the engineers who knew that the O-Ring seals had a history of blow-backs at low temperatures.

Figure 13 below details the sequence using the safety model and the control failures can clearly be identified as:

- Pressure sensors not providing sufficient data in time
- Flight Termination System – not able to protect the astronauts in time
- Crew Pod ejection – not able to protect the astronauts in time
- Limitation ignored – the 53° F limitation for the O-Rings was ignored by the management against the engineer's advice

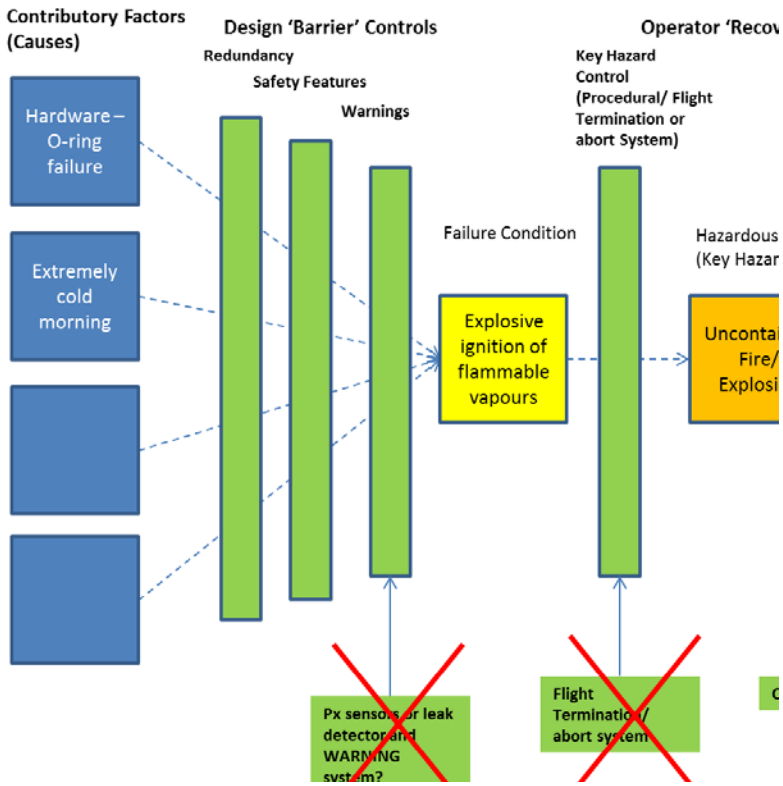

Figure 13 : Case Study of Space Shuttle Challenger to demonstrate contiguous Safety Model – details failed or missing controls

Arguably the first three controls above are design controls and it is the last control (the operator-based limitation) that could have easily averted the accident. This clearly shows the importance of recognising the 'soft' operator-based controls in an explicit accident sequence.

5. CONCLUSIONS

This paper has highlighted that a gap exists between design safety analysis and operator safety analysis. This lack of contiguous safety approach has meant that operators are not fully aware of the specific accident and near-accident risks and this has resulted in catastrophic losses in the space and aviation domains – losses that could have been avoided by effective, proactive and contiguous safety management. There are currently no guidelines on how to achieve a contiguous safety model but there are effective and separate guidelines for designers and operators.

The model presented by this paper employs a 'key hazard' in joining the failure conditions (from designers) to the accidents and safety significant events that operators should be managing. This 'key hazard' represents a hazardous state at the aircraft level, whereas a failure condition is below this level (but above a system hazard level). This is important within a contiguous safety model because it is important to place the controls in the correct place so that they can be managed more effectively who are responsible for them i.e. that an operator manages the operating procedures, training and actively enforce limitations that are derived through design or from operations.

The paper concludes that the contiguous safety model can be applied in the aviation domain but states that it is important that it is applied in the commercial spaceflight domain because the designer and operator will be the same organisation in most cases. This being the case will assist in the certification or approval of launch licenses where it is envisaged that a safety target approach will be required i.e. a catastrophic (loss) safety target of 1 $x10^{-3}$ per mission for orbital operations and 1 $x10^{-4}$ per mission for suborbital operations. Here the designer/operator will be able to demonstrate the achieved failure condition probabilities and then demonstrate the explicit contribution of operator controls (procedures, training and limitations) within the accident sequence. This may be an important factor because the Rocket Propulsion System will no doubt be the main contributor to the catastrophic loss case and the analyst will have to include exposure factors (along with safe design measures) to assist in achieving the required level of safety.

The paper demonstrated the use of the contiguous safety model in aviation and space case studies and concludes that by employing such an approach that future disasters could be avoided.

ABBREVIATIONS & ACRONYMS

AC	Advisory Circular
ACARS	Automatic Communication Addressing and Reporting System
ALARP	As Low As Reasonably Practicable
AMC	Acceptable Means of Compliance
ARAC	Aviation Rulemaking Advisory Committee
ARP	Aerospace Recommended Practice
AST	Commercial Space Transportation
BAE	Bureau d'Enquêtes et d'Analyses
CBA	Cost Benefit Analysis
CFR	Code of Federal Regulations
CS	Certification Specification
CFIT	Controlled Flight Into Terrain
DO	Design organisation
EASA	European Aviation Safety Agency
ELOS	Equivalent Level of Safety
FAA	Federal Aviation Administration
FHA	Functional Hazard Analysis
FOQA	Flight Operations Quality Assurance
GAIN	Global Aviation Information Network
HRI	Hazard Risk Index
ICAO	International Civil Aviation Organisation
LOC	Loss of Control
MAC	Mid-Air Collision
OHL	Operator Hazard Level
QAR	Quick Access Recorder
SoA	Suborbital Aircraft
SIRA	Safety Issues Risks Assessment
SS	System Safety
SMS	Safety Management System
SSE	Significant Safety Event

REFERENCES

[1]: Federal Aviation Administration, Advisory Circular 437.55-1, dated April 20, 2007

[2]: Report to Congress, *Analysis of Human Space Flight Safety*, The ARES Corporation, George Washington University, Massachusetts Institute of Technology, 11 November 2008

[3]: Federal Aviation Administration, Code of Federal Regulations, Title 14, Part 25.1309(b)

[4]: Federal Aviation Administration, Advisory Circular 23.1309-1C, *Equipment, Systems and Installations in Part 23 Airplanes*, 3/12/1999

[5]: SAE, Aerospace Recommended Practices (ARP) 4761, *Certification Considerations for Highly Integrated or Complex Aircraft*, ARP 4754, 1996

[6]: SAE, Aerospace Recommended Practices (ARP) 4761, *Guidelines and Methods for conducting Safety Assessment Process on Civil Airborne Systems and Equipment*, December 1996

[7]: Department of Defense, *Standard Practice for System Safety*, MIL-STD-882D, February 10, 2000

[8]: SAE International, *Aerospace Recommended Practice* 5150, 2003

[9]: Federal Aviation Administration, Advisory Circular 120-92, dated 6/22/06

[10]: Federal Aviation Administration (FAA), *AC 150/5200-37, Introduction to SMS for Airport Operators.* s.l. FAA, 2007.

[11]: Global Aviation Information Network, Operator's Flight Safety Handbook, Issue 2, December 2001

[12]: ARMS Working Group, Operational Risk Assessment, 2007-2010

[13]: International Civil Aviation Organisation (ICAO) Annex 13, Chapter 1

[14]: Bureau d'Enquêtes et d'Analyses. Interim Report No.2 on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, 30 November 2009

[15]: Bureau d'Enquêtes et d'Analyses. Interim Report No.3 on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, 30 November 2009

[16]: International Association for the Advancement of Space Safety, Independent Space Safety Board, *Space Safety Standard for Commercial Human-Rated Systems*, March 2010

[17]: Vaughan, D. The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA. Chicago; University of Chicago Press Ltd, 1996