SAFETY CRITERIA FOR THE PRIVATE SPACEFLIGHT INDUSTRY

Andy Quinn [(1)], Prof. Paul Maropoulos [(2)]

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

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

ABSTRACT

The Federal Aviation Administration (FAA) Office of Commercial Space Transportation (AST) has set specific rules and generic guidelines to cover experimental and operational flights by industry forerunners such as Virgin Galactic and XCOR. One such guideline Advisory Circular (AC) 437.55-1**[1]** contains exemplar hazard analyses for spacecraft designers and operators to follow under an experimental permit. The FAA's rules and guidelines have also been ratified in a report to the United States Congress, *Analysis of Human Space Flight Safety***[2]** which cites that the industry is too immature and has 'insufficient data' to be proscriptive and that 'defining a minimum set of criteria for human spaceflight service providers is potentially problematic' in order not to 'stifle the emerging industry'.

The authors of this paper acknowledge the immaturity of the industry and discuss the problematic issues that Design Organisations and Operators now face.

1. INTRODUCTION

In the aerospace and space sectors Safety Criteria and Risk Matrices are being used by Design Organisations (DOs) and Operators in order to meet certification and safety requirements. On reviewing different Safety Criteria and Risk Matrices from governmental, military and civilian standards, it is evident that the 'Through-Life' Safety Management is not as coherent and joined-up as it could be; where sound philosophy exists (such as baseline safety objective criterion) it stops short of analysing the accident sequence in full. Furthermore where 'Operator' guidance is available, it is too generic and stops short of providing guidance on how to tackle Total System Risk. These latter aspects should primarily be the responsibility of the Operator but how can they perceive and manage the Risks if they are not provided with the guidance on how to do this? For the sub-orbital private spaceflight industry we must be more explicit in our Rules and also more explicit in providing DOs and Operators with effective Acceptable Means of Compliance and safety criteria.

2. SAFETY OBJECTIVE ORIGINS

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-06 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-01 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+02. 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-06 x 1E-01 / 1E+02 = 1E-09 per flying hour.

AC 25.1309-1A **[4]** details the acceptable means of compliance for § 25.1309(b) and of particular relevance is the 'probability versus consequence' graph. The probability classifications based on the above rationale are as follows:

- Probable failure conditions > 1E-05
- Improbable failure conditions <1E-05 but > 1E-09
- Extremely Improbable failure conditions <1E-09

The AC states that each failure condition should have a probability that is inversely related to its severity. Figure 1 below represents the AC graph (left graph) and the diagonal line shows the explicit safety objectives that DOs are to achieve. The Matrix on the right hand side represents the same information for clarification later in this paper.

As can be seen, if the DO presents an aircraft with 100 catastrophic failure conditions that meet the safety objective of 1E-09, then they will meet the overall target (for catastrophic failure conditions) of 1E-07. §25.1309 then stipulates further safety objectives: Major failure conditions are to be <1E-05 and >1E-09, and Minor failure conditions >1E-05; therefore one would assume that with a further 100 'Major' failure conditions met by the DO at 1E-05 then they will meet that overall target of 1E-03.

The range of the Major failure conditions is clearly too great, hence the FAA tasked the Aviation Rulemaking Advisory Committee (ARAC) with providing better guidance for DOs to follow. Their

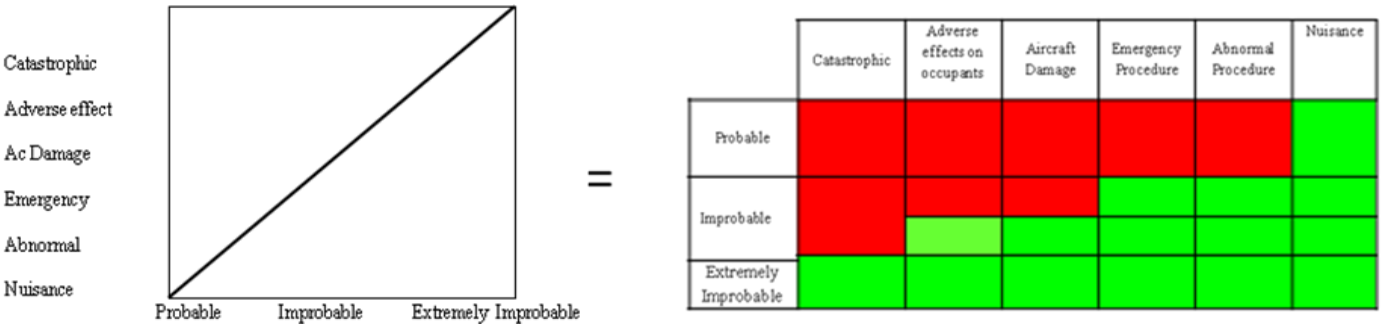

Figure 1: AC 25.1309-1A Safety Criteria (left graph) and equivalent information in Matrix format (right) – both display 'unacceptable' and 'acceptable' regions only

report **[5]** includes an updated AC 25.1309 and quite rightly splits the 'Major' failure condition criterion to the following classifications (severity/ probability):

- No Safety effect/no probability requirement
- Minor/Probable failure conditions < 1E-03
- Major/Remote failure conditions <1E-05
- Hazardous/Extremely Remote failure conditions <1E-07
- Catastrophic/ Extremely Improbable failure conditions <1E-09

This scheme has been incorporated in CS 25 **[6]**. The consequence versus probability graph is still a single safety objective/overall target line; the axis has changed i.e. probability on the vertical axis, and they have explicitly added the words 'unacceptable' above the safety objective line and 'acceptable' below. By keeping with the single line philosophy, this means that there is still an implicit 'overall target' for each type of failure condition (catastrophic/ hazardous/major/minor) as depicted in Figure 2 below.

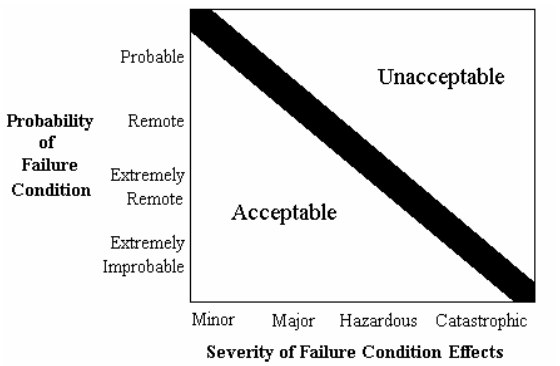

Figure 2: Relationship between Probability and Severity of Failure Condition Effects – from CS-25

2.1. Safety Objectives for Part 23 Airplanes

Recognising that smaller aircraft will have different characteristics than large aircraft a certification specification (CS) and AC were introduced. CS 23 **[7]** covers Normal, Utility, Aerobatic and Commuter Category airplanes. It details the applicability and provides a breakdown of categories of aircraft stating that an aircraft can be certified under more than one category so long as it meets all of the relevant and identified requirements. AC 23.1309 **[8]** follows the same rationale as §25.1309 with the aim as:

> 'to improve the safety of the airplane fleet by fostering the incorporation of both new technologies that address pilot error and weather related accidents and those technologies that can be certificated affordably under 14 CFR Part 23'

Although the AC covers all of the categories stated above, it concentrates on the General Aircraft (GA) aspects in rationalising the decision regarding the setting of safety objectives. The historical accident rate is predominantly associated with flying in Instrument Meteorological Conditions (IMC). The evidence indicates that the probability of a fatal accident in restricted visibility due to operational and airframe-related causes is 1 in 10,000 (1E-04) for single-engine aeroplanes under 6000lbs. Additionally (as per §25.1309) evidence shows that 10% of accidents are due to system failure conditions therefore the probability of a fatal accident from all causes is 1E-05 per flight hour. As opposed to large aircraft with many complex systems, Part 23 Class I aircraft are 'arbitrarily' derived to have 10 potential failure conditions that could be catastrophic thus the safety objective is 1E-06 per flying hour. The AC continues to state that larger aircraft (than Class I) have a lower failure rate and therefore have lower probability values for catastrophic failure conditions:

- Class II = 1E-07
- Class III = 1E-08
- Class IV = 1E-09

Although there is no 'severity versus likelihood' chart as per §25.1309, the chart would be exactly the same – see Figure 2 (left/above).

2.2. Design Organisation Risk Reduction

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 will implement the fail-safe design concept in order to achieve the desired safety objectives.

3. TRANSLATING SAFETY OBJECTIVES TO SAFETY RISK MANAGEMENT

The DO's aim is to meet their safety objectives in order to comply with FAR certification requirements; they have circa 100 catastrophic failure conditions, 100 hazardous (critical) failure conditions and arguably 100 major failure conditions (quantitative analysis is not required for Minor failure conditions as per §25.1309 & §23.1309). So what now for the Operator? How do we translate these failure condition's safety objectives into safety Risk? The answer is to explicitly 'split' the safety objective line and to have a Risk Matrix in order to manage and make decisions about Safety Risk. This aspect of 'calibrating' a Risk Matrix is extremely important.

There are many different Risk Matrices in use across the aerospace and space sectors and these are based on different standards such as MIL-STD 882D **[9]**, Tech America Standard **[10]**, FAA System Safety (SS) Handbooks **[11]** and for Operators, the FAA AC 120-92 **[12]**; all of these use Risk Matrices with acceptance criteria of High, Medium and Low Risk levels using a Hazard Risk Index (HRI) scheme (as opposed to the failure condition's 'single line' approach). The FAA SS Handbook **[11]** details this approach as a 'Comparative Safety Assessment' in which four 'Regions' are depicted (R1-R4); these are acceptability criteria:

- Unacceptable (R1)
- Must Control or mitigate (Management Authority [MA] Review) (R2)
- Acceptable with MA Review (R3)
- Acceptable without Review (R4)

There appears to be little or no explanatory guidance on how to produce a Risk Matrix *based on safety objectives*, hence there are different 'examples' within the various standards. The Aerospace Recommended Practice 5150 **[13]** also has a generic Hazard Risk Matrix. Figure 3 below is an exemplar Safety Risk Matrix for Operators (such as airliners, air taxi operators, corporate flight departments and pilot schools) as suggested in Advisory Circular 120-92 **[12]**:

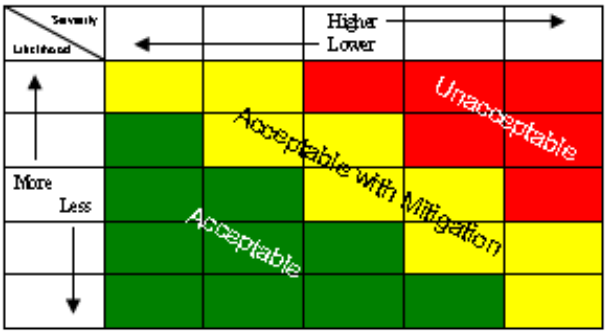

Figure 3: Safety Risk Matrix from AC 120-92

However the authors contend that a Risk Matrix is actually 'self-calibrating' as it should be based on the safety objectives. Table 1 below details the author's exemplar matrix based on §25.1309 with an additional level of likelihood to provide equally proportioned increments:

		Catastrophic	Hazardous	Major	Minor
Frequent	>10-3				
Probable	10-3 to 10-5				
Occasional	10-5 to 10-6				
Remote	10-6 to 10-7				
Extremely Remote	10-7 to 10-8				
Improbable	10-8 to 10-9				
Extremely Improbable	<10-9				

Table 1: Author's Exemplar Risk Matrix; self-calibrated based on standard safety objectives detailed in §25.1309

This approach bases the acceptability on the analysis of single Risks and to do this the Operator must assess the hazard to accident 'pair' in order to arrive at a HRI to plot onto the matrix.

Although this approach enables management to prioritise mitigation measures based on the single Risks, it does not provide senior management with detail of the platform's cumulative Risk – or Total System Risk. This will be discussed in Section 6.4.

4. OPERATOR MANAGEMENT OF RISKS & HAZARDS

Although DOs will have their own Hazard Log (or appropriate hazard/failure condition tracking tool) Operators should also have a Hazard Log/Risk Management tool that enables functional and inherent hazards to be tracked in order to undertake Risk Management. ARP 5150 **[13]** suggests an 'Operator Hazard Level' (OHL) to assess Risks. The OHL approach focuses on event severities that are lower than catastrophic levels as they suggest that the existing regulatory oversight process is used to identify root causes and necessary mitigation recommendations. This approach is meant to include qualitative assessment. The guidelines also include safety assessment monitoring parameters relating to safety events such that Operators can attempt Risk Management. These relate to Safety Significant Events (SSE) which are categorised based on individual specific events as follows:

- Category 1 – Catastrophic/Near Catastrophic
- Category 2 – Airworthiness/Safety Significant
- Category 3 – Impact on perceived safety
- Category 4 – Impact on operation, reliability or passenger discomfort

This type of classifying accidents and 'less than catastrophic' incidents is covered in more detail in Section 6.3.

To assist in the Operator SMS the Flight Operational Quality Assurance (FOQA) programme is a vital tool in capturing events as it gathers data from a Quick Access Recorder (QAR) with hundreds or thousands of parameters. The FOQA 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. These can then be analysed in order to determine whether mitigation can be applied; usually in the form of procedures, training or even limitations.

The authors acknowledge that a qualitative approach may be more suited to Operators due to resource and skill-set levels and also due to the amount of Air Safety Reports (events) that they have to deal with. However these events will have causes linked to the hazard and as the probability of the cause increases then the hazard's probability will increase and therefore its contribution to an accident (or SSE) may increase. Hence, along with Risk Profiling, a soundly constructed hazard log would arguably assist in understanding and managing their Safety Risks.

5. RESIDUAL RISKS REDUCED TO ALARP

In the UK, the Health & Safety Executive's (HSE) **[14]** approach to Risk Management is based upon the As Low As Reasonably Practicable (ALARP) principle. In essence this involves identifying Risks and applying appropriate risk reduction methods to drive Risks down to a more Tolerable level i.e. more 'reasonably practicable' (using Cost Benefit Analysis [CBA] when Tolerable Risks are identified). A CBA can help Operators make judgements on whether further Risk Reduction measures are 'reasonably practicable'. In this sense, something is 'reasonably practicable' unless its costs are grossly disproportionate to the benefits gained. ALARP Arguments are often produced on Single Risks (either 1 x Accident with many hazards) or separate ALARP Arguments for each Hazard to Accident 'pair'. This is still only for a Single Risk and therefore presents a more acceptable Risk to senior managers. Figure 5 depicts the ALARP triangle from UK Defence Standard 00-56 **[15]** based on risk per person per year (left figure) and also per Risk Class.

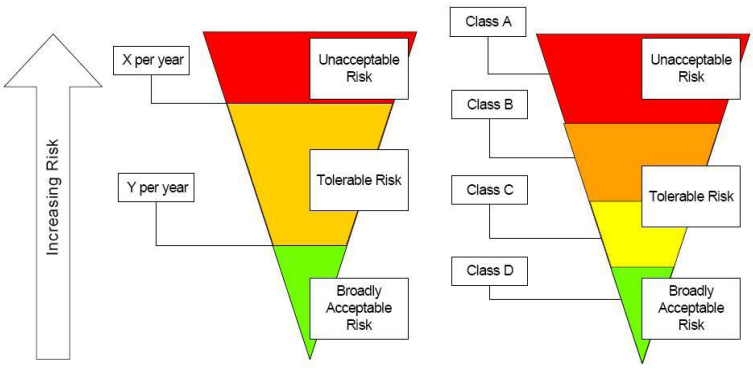

Figure 5: ALARP triangle based on UK Def-Stan 00-56

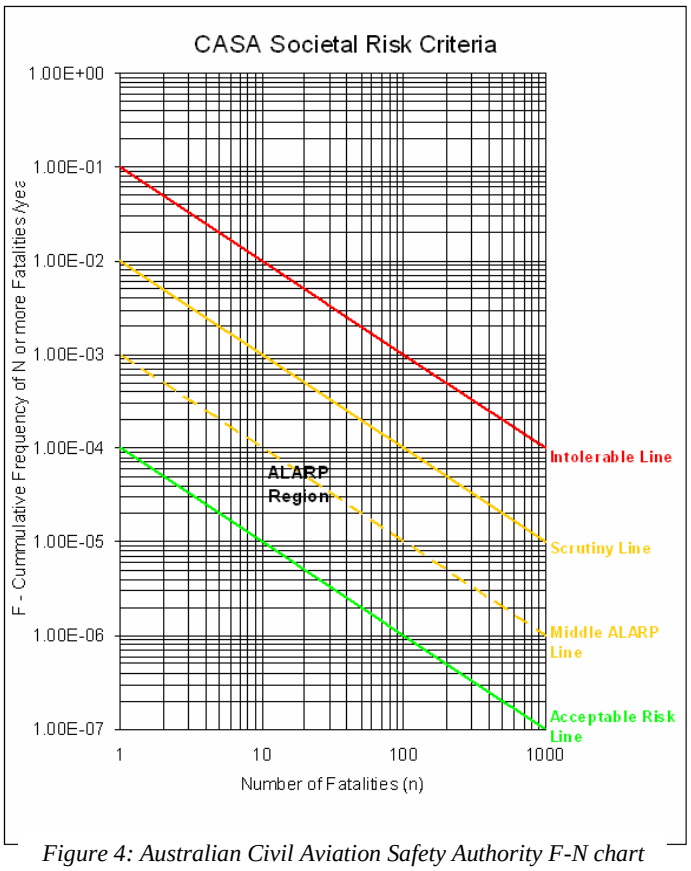

Figure 4: Australian Civil Aviation Safety Authority F-N chart

Although the exemplar classification schemes above appear similar, care must be taken when using the ALARP principle in that analysts must ensure they know whether the Risk Reduction is applied to meet failure condition's safety objectives (per flying hour-based) or indeed to meet the HSE-based Lower Level of Tolerability (risk of death per person per year). The authors contend that the ALARP *principle* can be applied to both cases but when trying to estimate the risk of death per person per year (rpppy) then a separate matrix or chart is required using the appropriate values. The HSE-based methodology is not just about the ALARP Triangle. Companies then use the ULT and LLT as a baseline for their analysis using 'F-N' curves and tables/graphs (see Figure 4) for Societal Risks and Individual Risks.

It is important that Operators consider a separate aerospace (spaceflight) chart or table that represents the Risk of death pppy. This can be used for the following:

- Plotting types of people at Risk (1st, 2nd, 3rd Parties)
- Plotting groups of people at Risk Pilots, Spaceflight Participants or Maintainers, and so on
- Plotting F-N data for predicted scenarios, such as aerodromes (Spaceports), Bulk Fuel Installations, etc
- For the new Commercial Spaceflight Industry; to provide a metric in order to let people know the Risk they face – especially when they are signing a 'Waiver'

In general, if the risk reduction is impracticable or the cost is grossly disproportionate to the improvement gained, then the risk is said to be 'tolerable' – this is the case for both the Operator's Accident Risk Matrix (based on safety objectives) and for any type of chart for plotting risk per person per year.

6. RELEVANCE TO SUB-ORBITAL SPACEFLIGHT

The above sections highlighted the need to understand the origins of safety objectives and then what is required in the next steps of the analysis (by Operators) in undertaking Safety Risk Management activities. It also highlighted that there are different standards in use and that the Risk Matrices (as applied by Operators) are not consistent with the failure condition's safety objectives.

Sub-orbital spaceflight DOs and Operators have been provided with the AC 437.55-1 [[**1**] as guidance and the authors contend that similar issues may arise per the aviation industry as described above. The following section discusses the problematic issues:

6.1. Safety Objectives

The criteria for a 'catastrophic' event resulting in death or serious injury to the public must be 'extremely remote' (probability of 1E-06 in any one mission) as stated in AC 437.55-1. Table 2 below details the Risk Acceptability Matrix within AC 437.55-1; note that the likelihood for the catastrophic failure condition is 'Extremely Remote' as opposed to 'Extremely Improbable' per §25.1309 & §23.1309.

As the sub-orbital industry has not had historical accidents upon which to base safety objectives, it is assumed that the 1E-06 probability was based on the AC23.1309 **[8**] criteria for Part 23 aircraft. In terms of knowledge of the US space launch industry the FAA may also have thought about their current Expected Casualty Calculations for Commercial Space Launch and Re-entry **[16**]. However their 'acceptable objective' is an Expected Casualty rate (Ec) of $\leq$ 30E-06; this value is per mission i.e. a rate of 30 casualties per million missions (human casualty being defined as a fatality or serious injury in AC431-35-2A **[18**]). As can be seen this is 30 times different to the proposed safety objective in AC 437.55-1 **[1**]. Herein lays the problematic issue of defining suitable criteria. The FAA remit covers 'Commercial Space Launch and Re-entry' activities and this includes sub-orbital *and* orbital; these are two hugely different categories of vehicle. For orbital operations one could argue to continue with the current Ec acceptable objective as launches would commence from similar locations and latitude as per current governmental launches. Indeed the IAASS Independent Space Safety Board (ISSB) 'Space Safety Standard' for Commercial Human Rated Systems **[17**] suggests 1E-03 as the Orbital Safety Risk target (for the probability of a catastrophic event per entire mission). The justification for selecting this value should be stated in order to assist the DOs and Operators in their Hazard and Risk Management approach.

Sub-orbital vertical launches should be from remote sites and hence the likelihood of third party (public) casualties will be less. In this instance the author suggests that the safety objective of 1E-06 could be argued as long as the applicants follow the well-trusted Ec guidelines and principles contained in **[16**]. This somewhat corroborates the §23.1309 catastrophic failure condition safety objective (although the likelihood definitions differ – see Table 4 for the author's exemplar Safety Risk Matrix). One could argue that the 'Ec' safety objective derivation is more relevant to spaceflight than the rationale of §23.1309 based on flying in restricted visibilty as a contributor to the historical GA accident rate. The rationale is that neither approach covers (for instance) the Virgin Galactic

	Severity			
Likelihood/Probability	Catastrophic	Critical	Marginal	Negligible
Frequent $> 10^{-2}$	1	3	7	13
Probable $10^{-2} > X > 10^{-3}$	2	5	9	16
Occasional $10^{-3} > X > 10^{-5}$	4	6	11	18
Remote $10^{-5} > X > 10^{-6}$	8	10	14	19
Extremely Remote $<10^{-6}$	12	15	17	20

Table 2: Risk Acceptability Matrix; based on AC437.55-1 safety objectives

model whereby they will fly in Visual Meteorological Conditions (VMC) to a remote area at 50,000ft to launch their spacecraft; hence the Ec will not to be a 'driver' for a safety objective (though one would clearly include third party analysis) and neither will flying in restricted visibility. The author's knowledge of military 'fast jets' would suggest that high performance aircraft have more than the 10 'arbitrary' GA aircraft failure conditions (per §23.1309); indeed these may be more towards the 100 failure conditions (for catastrophic and hazardous events); however their flight profile is not compatible with SoA for instance. Therefore consideration could be given to a catastrophic failure condition for SoA based on a more 'equivalent' aircraft Class (such as Class III Part 23 aircraft); here a better accident rate is considered i.e. 1E-05, and following the standard logic of 10% for critical systems and 100 failure conditions, the resultant catastrophic safety objective is 1E-08 per flying hour rather than 1E-06. However, SoA will have unique and novel critical systems and therefore we would suggest a margin is applied to the specific novel aspect's failure conditions to account for uncertainty. The DO and Operator will be able to apportion the 'budgets' of the failure conditions to account for these novel and uncertain aspects. It is suggests that the authorities (both in the US and Europe) should engage more closely with the DOs and Operators to determine more rationalised safety objectives based on these Equivalent Levels of Safety (ELOS) but applying rationale in apportionment of failure conditions. The IAASS-ISSB **[17**] suggest a Sub-Orbital Safety Risk target as a not to exceed **1E-04** per mission for catastrophic events; the definition does not state whether this is the cumulative probability (and whether it is based on 10 or 100 failure conditions) or whether this is the safety objective for a single failure condition; it is assumed that this is based on the 1E-06 per mission for 100 catastrophic failure conditions. This Safety Risk target must be explicitly rationalised in order to assist DOs and Operators better understand the safety issues and to provide a pragmatic approach.

6.1.1. Derived Safety Requirements

In order to meet the catastrophic failure condition's safety objective (and therefore the critical and major safety objectives) the DO will have undertaken a Functional Hazard Analysis (FHA) at the platform level in order to apportion sub-system 'objectives'. Arguably, applying novel technology to a vehicle that will be operating in extreme environments and at extreme velocities may mean some of the sub-systems may not meet their quantitative 'objectives'. In this instance the DO (and subsequently, the Operator) will have to defend this with qualitative engineering judgement based on sound arguments and backed up with test evidence. Also, the Operator (in conjunction with the DO) may have to apply Limitations, Procedures and additional training as part of their Risk Reduction effort – see Section 5.3 below.

6.2. Severity Classifications

The severity criteria within AC 437.55-1 **[1**] are mainly concerned with the consequence to the general public. This approach naturally continues the methodology adopted for the vertical-launch industry. However, the different types of launch capabilities currently under construction or planning include:

- Airborne Launch – Virgin Galactic have a Mother-Ship which carries the spacecraft to an altitude of 50,00ft in a 'safe area' prior to releasing it for rocket initiation **[19**]
- Horizontal Take-Off – XCOR will initiate rocket take-off from the runway **[20**]
- Vertical Launch – Blue Origin **[21**] are developing a vertical launch spacecraft and this will possibly pose more of a Risk to the public, but arguably the choice of launch site (or limitation imposed on the Operator) should be well clear of the public; it is not like a Space Shuttle whose trajectory will overfly the public due to its orbital profile and necessity to launch from a specific latitude.

Figure 6 below is an exemplar 'multi-purpose' Risk Assessment Matrix from the Tech America Standard. Applying this sort of scheme to the different business modes (Vertical, Horizontal, and Air-Launch) may be worth considering for the FAA (AST). This would then consider the acceptable Risks for the different operator- models rather than giving the operators a 'Risk Score' as a possible suggestion in the report to the United States Congress **[2**].

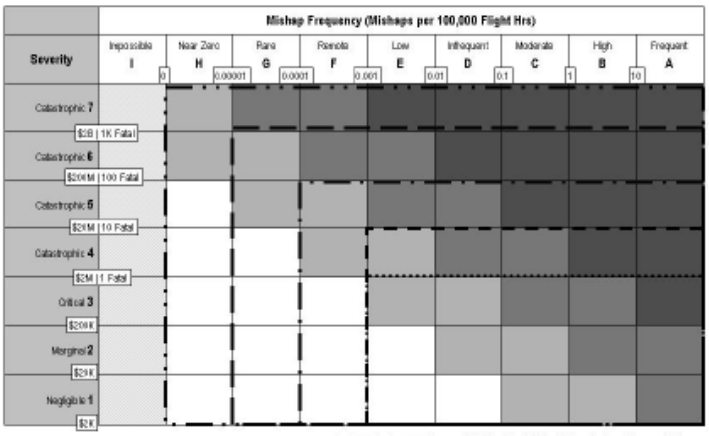

Figure 6: Tech America Standard exemplar 'Multi-Purpose' Aircraft Family Mishap Risk Assessment Matrix

Description & Category	Actual or Potential Occurrence	Effect To People			Effect to Asset	Effect to Environment
		1st Parties	2nd Parties	3rd Parties		
Catastrophic	Accident	Multiple 1st Party deaths	Multiple 2nd Party deaths	Single 3rd Party death	Loss of spacecraft	Extreme widespread environmental damage
Critical	Serious Incident - Asset or Accident (people death)	Single 1st Party death Physical distress or excessive workload impairs ability to perform tasks	Single 2nd Party death	Multiple Serious injuries 3rd Party	Severe damage to spacecraft Large reduction in Functional capabilities or safety margins	Severe environmental damage
Major	Major Incident	Multiple Serious injuries/ illnesses to 1st Parties Physical discomfort or a significant increase in workload	Multiple Serious injuries/ illnesses to 2nd Parties Physical discomfort	Serious injury to 3rd Parties	Major damage to spacecraft Significant reduction in functional capabilities or safety margins	Major environmental damage
Minor	Minor Incident	Minor injuries/illnesses to 1st Parties Slight increase in workload	Minor injuries/illnesses to 2nd Parties	Minor injury to 3rd Party	Minor damage to spacecraft Slight reduction in functional capabilities or safety margins	Minor environmental damage
Negligible	Occurrence without safety effect	Inconvenience	Inconvenience	Inconvenience	Less than Minor damage System	Less than minor environmental damage

Table 3: Exemplar Safety Event Severity Classification

Within these different sub-orbital business models, the authors would consider the safety of the following different groups; sub-orbital pilots (as 1st Party), passengers (as 2nd Party) and the 'public' (as 3rd Party). The rationale takes cognisance of the UK HSE approach in that an individual's exposure to Risk is key in the analysis; ergo the 'public' (3rd Party) are exposed to considerably less Risk than the 1st and 2nd Parties of a sub-orbital flight because the hazardous 'rocket' phase should be from a remote launch site. If this was not the case then additional mitigation would be required for not only the 1st & 2nd Parties, but also for the 3rd Parties. The proposed severity classification is as follows:

- **1st Parties** – individuals directly involved in operating the spacecraft i.e. flight crew
- **2nd Parties** – individuals directly involved in supporting the spacecraft (i.e. maintainers) and individuals participating in the flight who are not members of the flight crew (i.e. passengers)
- **3rd Parties** – the uninvolved public
- **Asset** – Loss of, damage to and degradation of performance of the spacecraft
- **Environment** – damage to the environment (from explosions or rocket fuel leaks)

The exemplar severity classification scheme is included at Table 3 above. Note that the severity levels for single death (1st & 2nd Party) are considered 'Critical'; this is based not only on UK principles but also in the FAA SS Handbook.

6.3. Sub-Orbital Operator Safety Management

Section 2 detailed the role of the Design Organisation in terms of meeting safety objectives based on failure conditions with known severity classifications. Section 3 then detailed how these safety objective probability values can then calibrate the Risk Matrix for the benefit of Operators and Section 4 discussed the Operator Safety Management aspects. We now need to consider a pragmatic for Sub-Orbital Operators based on the DOs hazard analysis and incorporating Safety Risk Management, along with a FOQA-based approach. Risk is defined in AC 437.55-1 **[1]** as:

> 'Measure that takes into consideration the likelihood of occurrence and the consequence

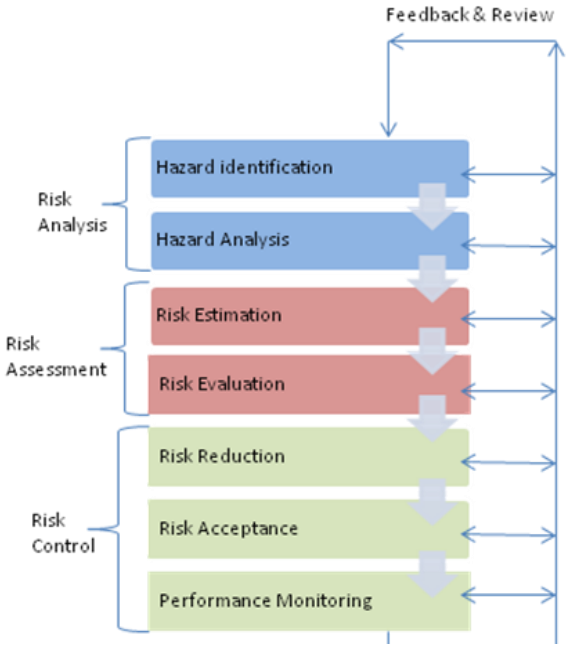

Figure 7: Exemplar Risk Management Model based on the UK DEF-STAN 00-56

of a hazard to people or property'

It is important to distinguish that in the UK aerospace defence field Risk Analysis is generally conducted at the Accident level within the accident sequence. Part of the rationale is that it is the Operator who is responsible for the post-hazardous event mitigation such as procedural, limitation and training controls. The DOs on the other hand undertake risk assessment at the hazard level and they implement 'pre-hazardous event' controls in accordance with the fail-safe design concept i.e. eliminate the hazard, provide safety features, warning devices, procedures and training. The DO-Operator analysis can be shown in Figure 7 below.

The accident sequence can best be presented pictorially and this was the case for Haddon-Cave QC as part of his report into the Royal Air Force Nimrod aircraft accident **[22]**. One could argue that it is the responsibility of the DO to provide analysis of failure conditions (and other analysis such as Operating & Support Hazard Analysis, etc) up to the 'event' – as depicted in Haddon-Cave's 'Bow-Tie' analogy in Figure 8 further below. Typically the DO analysis employs the use of Reliability data at the base events of Fault Tree Analysis. Then continuing the accident sequence (depicted below in Figure 8) it would be the responsibility of the Operator to undertake analysis (possibly in conjunction with the DO) to the right of the 'event' i.e. up to (and beyond) the Accident; this could be achieved using Event Tree Analysis.

To do this, Operators must know the Accidents and Incidents to which they must apply the Risk Analysis (Risk Estimation and Risk Evaluation activities as depicted in Fig. 6). Within aviation there are known catastrophic Accidents and indeed the International Civil Aviation Organisation (ICAO) Safety Team have derived occurrence categories **[23]**. Some of these are relevant to Sub-Orbital flights and include:

1. Controlled Flight Into Terrain – CFIT
2. Mid-Air Collision (MAC)
3. Loss of Control – In flight (LOC-I)
4. Loss of Control – Ground (LOC-G)
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

There are circa 10 aircraft (Sub-Orbital Aircraft [SoA]) -related 'Accidents' and with an arbitrary 10 failure conditions per Accident, we can see why the original BCAR analysis arrived at 100 catastrophic failure conditions.

Operator's analysts will then be able to link the DO's failure conditions with the relevant Accident in order to build the accident sequence (using Event Tree Analysis for instance). Once this is achieved the authors contend that the hazardous and major failure conditions also require linking to defined Incidents (sliding severities of Safety Significant Events [SSE]). Table 3 above includes Incidents (Serious, Major, Minor) and these can be further refined in accordance with the International Civil Aviation Organisation (ICAO) Annex 13 **[24]**.The ICAO definition of a 'Serious Incident' is:

> 'An incident involving circumstances indicating that an accident nearly occurred'.

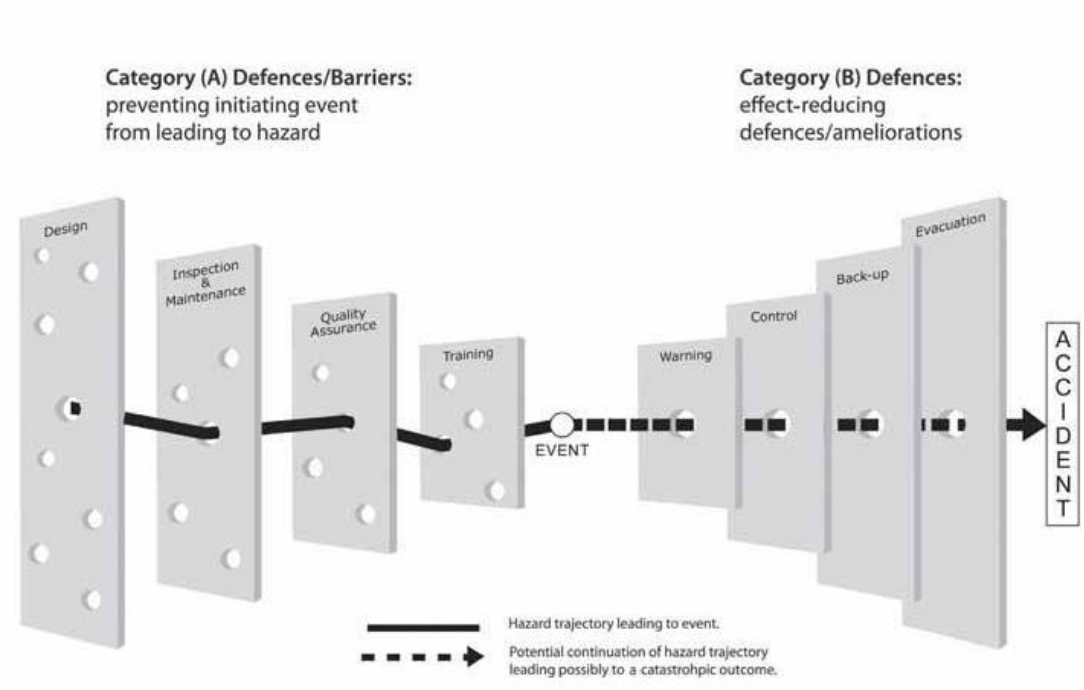

Figure 8: Haddon-Cave Report's 'Bow-Tie' analogy

	Severity (Safety Event)				
Likelihood/Probability	Catastrophic (Accident)	Critical/ Hazardous (Serious Incident)	Major (Major Incident)	Minor (Minor Incident)	Negligible (no safety effect)
Frequent $> 10^{-2}$	A	A	A	B	C
Probable 10^{-2} to 10^{-3}	A	A	B	C	D
Occasional 10^{-3} to 10^{-4}	A	B	C	D	D
Remote 10^{-4} to 10^{-5}	B	C	D	D	D
Improbable 10^{-5} to 10^{-6}	C	D	D	D	D
Extremely Improbable $<10^{-6}$	D	D	D	D	D

Table 4: Exemplar Safety Risk Matrix; derived from authors analysis, including Risk Management ALARP regions – the quantitative values are from current FAA/IAASS probability values; these need to be rationalised. Under EASA certification, the probability value for 'Extremely Improbable' could be in the order of 1E-08 per flying hour (similar to a Class III aircraft)

These Incidents can be categorised as per ICAO definitions and include:

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

This is in accord with the ARP 5150 **[13]** approach mentioned in Section 4. However, in the Sub-Orbital (Commercial) spaceflight industry, the DOs and Operators will initially be working quite closely with each other. The authors contend that the Operator safety analysts should link the DO failure conditions (along with their own identified Inherent and Environmental/operating hazards that are 'less than catastrophic') to these SSEs. Once this has been achieved they will be able to ensure that all Risks have been identified and are being managed to ALARP.

6.4. Total System Risk

Now that the DO analysis is complete and the Operator has constructed Accident (& Incident) sequences, the Operators will be able to estimate and evaluate the single Accident/Incident Risks (r) effectively (as per Fig. 4) and also undertake Risk Reduction activities. Once all of the identified single (Accident/Incident) Risks (r) have been accepted, their cumulative probabilities will be known i.e. the sum of contributing hazards (failure conditions) equates to the Accident/Incident's probability. The single (Accident/Incident) Risks (r) could then be summed to determine the Total System Risk (R) presented by the platform. However great care must be applied when undertaking this task as the different Accidents and Incidents will have different severity classifications; these will require a 'weighting' scheme to be applied (typically 10, 1, 0.1 and 0.01) Another example could be summing the Risks (r) in each severity column and then one could see the level of Risk (R) by joining the cumulative points by drawing a line. This approach is akin to the 'iso-risk' lines in Figure 9 below.

By having a Risk Matrix, the Operator will be able to determine:

- Whether the DO's failure conditions meet their respective safety objectives
- Where each 'single Risk' (r) (Accident/Incident) is classified. Where Risks are 'B' or 'C' class Risks the Operator will be able to determine which failure condition(s) is the main contributor in order to undertake Risk Reduction to ALARP
- What the cumulative 'Total System Risk' (R) is and whether it meets the determined Total Safety Target.

So what is the Tolerable Level of Safety (Equivalent Level of Safety) for a commercial spacecraft? What Safety Target can we set for the whole platform(s)? It is considered that this is the only real problematic area for further consideration. At present, Total System Risk Target is not considered by Design Organisations or Operators in the aviation industry and there is no guidance on achieving this. One such method could employ the use of 'iso-risk' lines as suggested by Tech American Standards **[10]**. Their scheme dictates that to measure the total system risk (R), one needs to provide a measure of severity (in terms of fatalities) and a measure of probability of the occurrence. The 'measures' of total system risk (R), include:

- Expected Loss Rate
- Maximum Loss Rate
- Most Probable Loss Rate
- Conditional Loss Rate

In relation to 'Conditional Loss Rate' the sum of the probabilities for all hazards is considered (with the assumption of independence) and this could be most appropriate.

Understanding the Total System Risk (R) is even more important within an emerging and novel industry where immature technology is yet to be rigorously proved; but first a Target (ELOS) must be set.

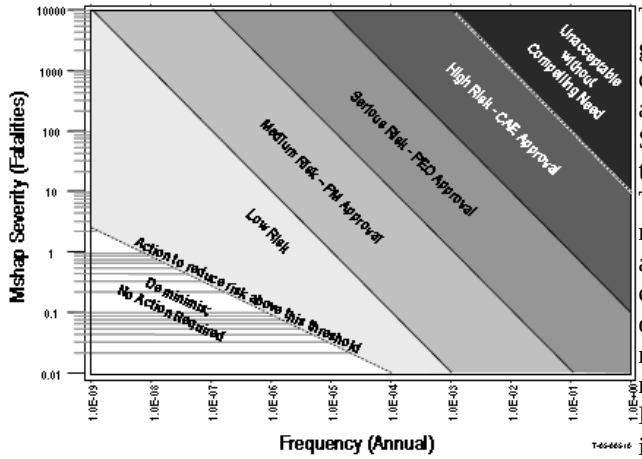

Figure 9: Tech America Standard exemplar Total System Risk Assessment Criteria incorporating 'Iso-Risk' lines

Arguably DOs will undertake a combined test and evaluation process (with Operators) but this will still not provide sufficient quantitative evidence of failure condition probabilities in some cases; instead qualitative engineering judgment may be used and hence the 'confidence' level of this type of analysis will need to be clearly stated. Thus, Operators in the United States will need to take the DO's analysis (that may have met safety objectives that do not have the standard high confidence levels per aviation) and apply their Safety Risk Management efforts as described above. This approach is considered necessary in order to fully understand the Risk presented by the whole platform(s). In Europe however, a different approach will be taken; one which is based on known certification processes.

7. SUB-ORBITAL CERTIFICATION

The FAA approach is that certification is not required due to the immaturity of the industry; instead they will require 'waivers' of consent from the passengers (also known as participants and 2nd Parties). Instead, to obtain a Launch License, Operators will have to demonstrate they have followed the intent of the Regulatory requirements and, in particular to safety, they will have to demonstrate they have followed the intent of AC 437.55-1 **[1**]. The European Aviation Safety Agency (EASA) have not yet formulated their Rules & Regulations however in a paper *Accommodating sub-orbital flights into the EASA Regulatory System* **[25**] their intent is to apply certification specification requirements to SoA that have wings and fly to the upper limits of the atmosphere which can also be considered as the lower limit of outer space. Their paper suggests a Restricted Type Certificate (RTC) with adaptations to existing airworthiness codes; in essence a pragmatic and stepped approach. In taking these 'small steps' EASA may learn much from the FAA whilst maintaining their own regulatory framework. The question is whether the FAA (AST) safety guidelines remain applicable within the certification requirements of the EASA §23.1309 approach for Part 23 aircraft. It was discussed in Section 6.1 that it is important to define and justify the catastrophic failure condition's safety objective. The §23.1309 rationale was due mainly to restricted visibility accidents (for Class I aircraft) and the FAA (AST) AC criteria may have also considered the Ec issues during launch and re-entry. The authors contend that these criterion may not be applicable to Virgin Galactic operating in a remote location in VMC in America. Within Europe a similar SoA Operator will be certified including restricted visibility flights and therefore the §23.1309 rationale may apply; though the authors contend these vehicles will be more akin to a high-performance/ high-altitude aircaft rather than a GA aircraft. To that end their catastrophic failure condition's safety objective should be based on at least on a Part 23 Class III aircraft but with margins applied due to novel technology (as described in Section 6.1). Essentially, further analysis is required to justify the safety objectives of Commercial Spacecraft and SoA.

8. CONCLUSIONS

This paper has highlighted the need for further discussion regarding safety criteria for the emerging Commercial Spaceflight Industry, which includes sub-orbital flights. It is hoped that as a result of this paper the FAA may (in the future) separate the orbital and sub-orbital regulatory requirements in order to apply appropriate criteria to appropriate Operator business models. The paper has shown that the 'Commercial' spaceflight industry needs to be explicit in its guidance to Operators so they can implement their own Safety Risk Management (Risk Evaluation, Risk Estimation and Risk Acceptance). Operators will need to consider the accident sequence fully and manage single Accident/Incident Risks but then sum these along with Inherent Hazards to Accidents/Incidents in order to appreciate the Total System Risk; only then will US Operators be able to provide a clear view of the Risk posed to the paying participants (and also inform them of the prospective risk of death per person per year based on their one flight).

In Europe it is suggested that EASA is willing to certify aeroplane-based spacecraft (SoAs) under the

existing regulatory framework with special conditions as appropriate. Within this framework, safety criterion is an essential component and the Equivalent Level of Safety for the SoA needs to be robust and defendable. The extant §23.1309 catastrophic failure condition criterion for Class I aircraft is the same as the proposed FAA (AST) criterion (1E-06 per flying hour), though there are differences in likelihood classifications. The IAASS-ISSB Safety Risk target for Sub-Orbital spaceflight is 1E-04; it is assumed that this is for the cumulative probability. Should this be the case then consideration must be given for 'proven' versus 'novel' technologies in the apportionment of Risk budgets.

Further analysis is clearly required to justify the safety objectives stated within guidelines because in the case of Virgin Galactic, their vehicle is more akin to a high-performance, high-altitude aircaft than a GA aircraft or a vertical launch vehicle with higher Ec considerations. For SoA certified aircraft in Europe, it is considered that the catastrophic safety objective commensurate with a Class III Part 23 aircraft could be more appropriate; this is 1E-08 per flight hour. Howwever this is to achieve the cumulative safety objective of 1E-06 per flight hour and consideration must be made (such as reduced margins) for novel technologies.

ACKNOWLEDGEMENTS

The authors would like to thank the following people for their most valued contribution to the paper:

Clive Lee, a safety colleague at Cobham Technical Services whom shares a passion for safety and has endured many conversations regarding general safety criteria over the past year.

David Barry, a Safety Manager at British Midland Airways and Masters Degree colleague who shared his valuable insight into the Operational Safety Management aspects.

Chris Quinn, a dear son to Andy, for his editorial and general comments.

ABBREVIATIONS & ACRONYMS

AC	Advisory Circular
ALARP	As Low As Reasonably Practicable
AMC	Acceptable Means of Compliance
ARAC	Aviation Rulemaking Advisory Committee
ARP	Aerospace Recommended Practice
AST	Commercial Space Transportation
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
F-N	Frequency-Number
GA	General Aviation
HRI	Hazard Risk Index
HSE	Health & Safety Executive
ICAO	International Civil Aviation Organisation
LOC	Loss of Control
IMC	Instrument Meteorological Conditions
LLT	Lower Level of Tolerability
MA	Management Authority
MAC	Mid-Air Collision
OHL	Operator Hazard Level
QAR	Quick Access Recorder
RTC	Restricted Type Certificate
SoA	Sub-Orbital Aircraft
SS	System Safety
SMS	Safety Management System
SSE	Significant Safety Event
ULT	Upper Level of Tolerability
VMC	Visual Meteorological Conditions

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 25.1309-1A, *System Design and Analysis*, 6/21/1988

[5]: Federal Aviation Administration, Advisory Material Joint 25.1309, 6/10/2002 (Aviation Rulemaking Advisory Committee Task, Systems Design and Harmonization Working Group Task 2)

[6]: European Aviation Safety Agency, *Certification Specifications for Large Aeroplanes*, CS-25, Book 2, Acceptable Means of Compliance, 27 December 2007

[7]: European Aviation Safety Agency, *Certification Specifications for Normal, Utility, Aerobatic and Commuter Aeroplanes*, CS-23, Book 1, Airworthiness Code, 14/11/2003

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

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

[10]: Tech America, *Standard Best Practices for System Safety Development and Execution*, GEIA-STD-0010, October 2008

[11]: Federal Aviation Administration, *System Safety Handbook*, December 30, 2000

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

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

[14]: URL; UK Health and Safety Executive, *ALARP at a glance*, http://www.hse.gov.uk/risk/theory/alarpglance.htm

[15]: UK Defence Standard 00-56, Issue 4, Part 2

[16]: Federal Aviation Administration, Advisory Circular 431.35-1, 8/30/2000, *Expected Casualty Calculations for Commercial Space Launch and Re-entry*

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

[18]: Federal Aviation Administration, Advisory Circular 431-35-2A, 7/20/2005, *Reusable Launch and Re-entry Vehicle System Safety Process*

[19]: URL; Virgin Galactic, http://www.virgingalactic.com

[20]: URL; XCOR, http://www.xcor.com

[21]: URL; Blue Origin, http://www.blueorigin.com

[22]: Charles Haddon-Cave QC, *The Nimrod Review*, 28th October 2009

[23]: International Civil Aviation Organisation (ICAO), Commercial Aviation Safety Team, *Aviation Occurrence Category Definitions and Usage Notes*, June 2004

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

[25]: Marciacq J-B ., Morier Y., Tomasello F., Erdelyi Zs., Gerhard M., *Accommodating sub-orbital flights into the EASA regulatory system*, in Proceedings of the 3rd IAASS Conference 'Building a Safer Space Together', 21-23 October 2008