March 2018

BAINES | SIMMONS
World Leaders in Aviation Safety

White Paper Plus+

Hazard Identification and Risk Management challenges throughout the Supply Chain

A paper by Principal Consultant, Duane Kritzinger at Baines Simmons.

Since the introduction of ICAO Annex 19 on Safety Management Systems (SMS), aviation organisations are expected to "*take a systematic approach to identifying aviation safety hazards, including their own organisational hazards, to assess the associated risks, and to effectively mitigate their consequences*" [EASA Terms of Reference (TOR) for rulemaking task RMT.0251(b) (MDM.055-MDM.060)].

Two of the fundamental challenges to successfully implementing an SMS is to (a) understand the basic risk management terminology to be applied to both aviation safety hazards and organisational hazards, and (b) to manage the safety management constraints and interfaces between relevant stakeholders.

The aim of this paper is therefore to raise awareness of the challenges of "*hazard identification*" and "*risk management*" throughout the supply chain. This is accomplished by first seeking a common understanding of following lexicon:

- What does the word "safety" mean?
- What is a "Management System"?
- What is a "hazard"?
- What is "risk" and why do it?

Due to the author's background, this paper may seem more Design Organisations focused, but it is hoped that it will also benefit the wider industry. After all, safety should be pro-actively built into the system in the first place and is less cost effective if added in afterwards.

1. Background

Safety Management Systems (SMS) are not new to the aviation industry:

- Many military aviation authorities have promulgated SMS principles for some time now (e.g. in standards such as Def Stan 00-56 and MIL-STD-882), which have been focussed on end user product safety risk (but not necessarily organisational hazards).
- In the civil aviation industry, Transport Canada worked closely since the mid 1990's with ICAO to issue the original ICAO SMS Manual.

Unfortunately, it is only since 2015 (when the ICAO SMS "*Recommended Practice*" became a "*Standard*" via ICAO Annex 19), that the wider aviation industry started to take it seriously. National regulatory authorities (including many military authorities) are subsequently at various stages of introducing SMS into their regulatory frameworks and industry are in turn preparing for the challenges of its successful implementation.

EASA are expected to facilitate the implementation of a single (safety) management system by multiple-approved organisations and streamline the related oversight. The EASA intent is stated in para 2.12.1 of Opinion 06/2016: "*...potential of SMS not only to address the risks of major occurrences, but also to identify and tackle production inefficiencies, improve communication, foster a better company culture, and control more effectively contractors and suppliers*" and "*...by considering SMS as something implemented not solely to prevent incidents and accidents but to ensure the success of as many elements of an organisation's business as possible, any investment in safety should be seen as an investment in productivity and organisational success.*"

This paper will therefore briefly explore the terminology impacting Risk Management within a Safety Management System by considering:

- What does the word "*safety*" mean?
- What is a "*Management System*"?
- What is a "*hazard*"?
- What is "*risk*" and why do it?

Within the context of the above terminology the ultimate objective of this paper is to explore the challenges of "*hazard Identification*" and "*risk management*" throughout the supply chain.

2. Understanding the word "safety"?

What do we understand by the term "*safety*"? From an industry point of view, the acceptability of safety is very difficult to discuss with customers, users, and, even worse, with society in general. The perception of "*safety risk*" is often influenced by any combination of biases [Kritzinger, Ch2]:

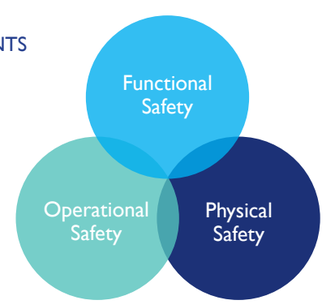
- **Ignorance** – People may unintentionally accept risk because they are ignorant of the risks (e.g. consider the manner in which tobacco companies marketed the benefits of smoking during the mid 20th century). This trust is largely based upon pragmatics [Johnson, 2003]. No individual is able to personally check that their food and drink is free from contamination, that their train is adequately maintained and protected by appropriate signalling equipment, that their domestic appliances continue to conform to the growing array of international safety regulations. On the flip side – we may, sometimes irrationally, fear that which we know little about (e.g. consider arachnophobia in countries such as the UK where indigenous spiders are harmless).
- **Familiarity** – People are more comfortable and accepting of risk when they are personally familiar with the operation. For example, is a traveller more fearful of a car accident or a plane crash? Which has the greater risk?
- **Media attention** – We fear problems that we are aware of and that we think are important and credible. Media coverage of issues increases our awareness of a problem and our belief in its credibility.
- **Cost and inconvenience** – A fear of flying was overcome in the early nineteenth century world when it took several weeks rather than a few hours to cross the Atlantic. Another good example is the preference for forward facing public transport, when it has been proven that rearward facing seats could significantly decrease injuries and increase survival rates.
- **Frequency** – Our belief in the frequency of an accident influences our risk acceptance. If we do not believe that the accident will happen, we are more likely to accept the risk.
- **Consequence** – We are not likely to accept risk for facilities that can have accidents with severe consequences. For example, an accident at a nuclear power plant could affect a large population. Therefore, we build very few such plants and we stringently regulate their safety. The risk related to coal-fired plants may be higher, but such plants are not as stringently regulated by the government.
- **Control** – Risks from sources outside their direct control are usually perceived to be more significant than they really are (e.g. nuclear power generation vs. conventional means). We accept more risk when we are personally in control, because we trust ourselves. For example, are you more afraid when you drive a car too fast or when you are the passenger in a speeding car?
- **Suddenness of consequence** – The sooner we feel the impact of an event, the less likely we are to accept the risk. Would you risk your life to save your car from a carjacker? Would you risk your life by smoking cigarettes for 40 years?
- **Personal versus societal** – We accept risk that affect only ourselves. We apply a higher standard to protect society.
- **Benefit** – Tolerance of risk can be related to perceived benefit; those who derive most benefit often tolerate greater risk than those who derive little or no benefit from the system do. As the benefit we receive from an operation increases, we are more accepting of the risk. For example, driving a car is more risky than travelling by plane. Because of personal benefit, people are usually more accepting of driving than flying.
- **Dread** – We have a strong fear or dread of risks whose severity we believe we cannot control. These risks are often thought to be catastrophic, fatal, hard to prevent, inequitable, threatening to future generations, and involuntary. An example is the risk of cancer. People are fearful of anything that may cause cancer because of the nature of the disease, its treatment, and, in some cases, the low probability of recovery.

Each of the above aspects all lead to the delusory concepts of "*safe*" and "*unsafe*", which of course have no real meaning, and very little acknowledgement of a measured response to achieve an acceptable level of safety [Murphy (1991)]. The U.S. Supreme Court once stated, "*Safe is not the equivalent of risk free*". This is certainly true in aviation where risk is inherent and safety performance can be expressed in terms of how well risk is managed [Eurocontrol, Hindsight 25]. All systems have a probability of transitioning to a dangerous state, even though the probability may be extremely small. Miller (2003, p105) advises that we should think realistically of safety in relative terms, and he recalls the old vaudevillian exchange in which a man asks, "*How's your wife?*", to which the comic responds, "*Compared to what?*"

Safety is certainly important, but important relative to what? The problem is that safety is non-deterministic; that is, it cannot be measured directly. The common dictionary definition of safety is "*freedom from harm*" (i.e. freedom from those conditions that can cause death, injury, occupational illness or damage to or loss of property, or damage to the environment). But does such an absolute application exist in the real world where we accept, live with, or otherwise integrate hazards into our everyday lives? Furthermore, does is provide for the full range of our "*own organisation hazards*"? It is probably *safe* to proclaim that there is no such thing as a safe system (and by "*system*" I do not only imply products, but also management systems and services).

However, we can postulate that safety is "*the ability to avoid an undesired event and/or reduce the harm(s) that might ultimately result from its manifestation*", and for purposes of stakeholder management (refer sections 5.2 and 5.3 below) we can loosely distinguish between three overlapping segments of safety [Kritzinger, Ch2]:

FIGURE 2:
THREE SAFETY SEGMENTS



- **Functional Safety**: This is part of the overall safety that depends on the system, equipment or services under consideration operating correctly in response to its inputs. It considers functional hazards caused by loss of intended function, malfunction, response time, accuracy, etc. Systems may be "*safe*" in one application, but "*unsafe*" in another (e.g. consider loss of altitude display during a clear day, versus the same failure under IMC conditions). Functional safety is strongly connected to the technical system's performance and its reliability.
- **Physical Safety**: This is usually directly recognisable by examination of the system and operating environment and is strongly connected to the physical characteristics of the components in the system. Examples are intrinsic hazards (such as hot surfaces or sharp edges) and physical failures (e.g. explosion, decompression, short circuits).
- **Operational Safety**: There are safety concerns which are directly related to the type on operations undertaken. Typical examples include deciding to fly with inoperative systems. Changing maintenance practices or flying into combat. To address one of the Annex 19 objectives, another example would be failing in organisational outputs (after all, it can be postulated that one man's output is another man's hazard). To protect our organisation outputs, we thus need to consider the robustness of our "Management Systems"

3. What is a "Management System"?

A management system can be defined as the framework of policies, processes/procedures and tools/techniques used by an organisation to ensure that it can fulfil all the tasks required to achieve its objectives. So, if the objective of the *safety* management system (SMS) is to manage safety[1], then we need:

- Strategic direction and culture via policies and active leadership (not in the scope of this paper)
- Documentation defining *who* does *what* and *when* for the repeatable and consistent management of safety (also not in the scope of this paper)
- Tools and techniques which ensure that we effectively know *how* to do safety. Within the scope of this paper (see section 1), this topic is further explored in section 4 below.

4. So How Do We Do Safety?

The evidence of safety in an SMS is most often realised via "*hazard Identification*" and "*risk management*" techniques. These seem like obviously understandable terminologies, but they do require careful consideration:

4.1 What is a "hazard"?

The word hazard is often used but seldom adequately defined and less consistently applied. A widely acceptable definition of a hazard has various iterations around the theme of "*any source of potential damage or harm*". This is useful as it does segregate the hazard from the accident. However, it is in the vagueness of words such as "*any source*" that most risk assessments become unmanageable, so it is important to also segregate the "*hazard*" from its contributing "*causes*" as shown in the example below [Kritzinger, Ch6]:

Example: Making the distinction between hazards and their causes

Is "*aircraft brakes overheat*" a hazard?
No, it may be argued that it is a cause, and that the potential hazards are:

- *loss* or *braking* (i.e. a functional hazard),
- *uncontrolled fire* (i.e. a physical hazard),
- *runway overrun* (i.e. an operational hazard).

So, do not confuse causes with hazards if you want to avoid duplication of effort.

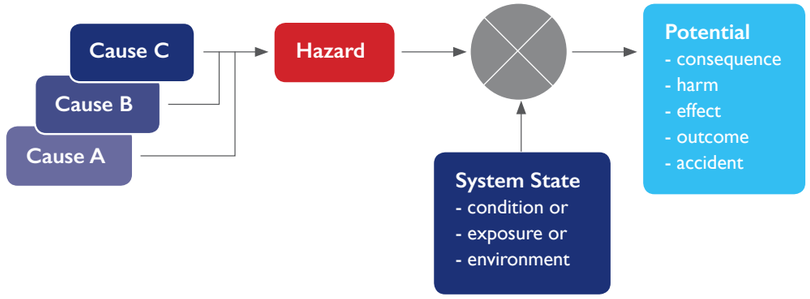
[1] Note: In accordance with ICAO Annex 19, a safety management system (SMS) is a systematic, proactive and explicit approach to managing safety, including the necessary organisational structures, accountabilities, policies and procedures.

It is for this reason that I proposed [Kritzinger, Ch6] that a hazard might rather be defined as "*a prerequisite condition that can develop into an accident[2] through a sequence of failures, events and actions in the process of meeting an objective*". These failure, events and actions are the threats to safety, and need robust management/mitigation.

The FAA [refer ASD-100-SSE-1, see Fig 3 below] also make this distinction between hazards and its causes as illustrated in Figure 3 below and where:

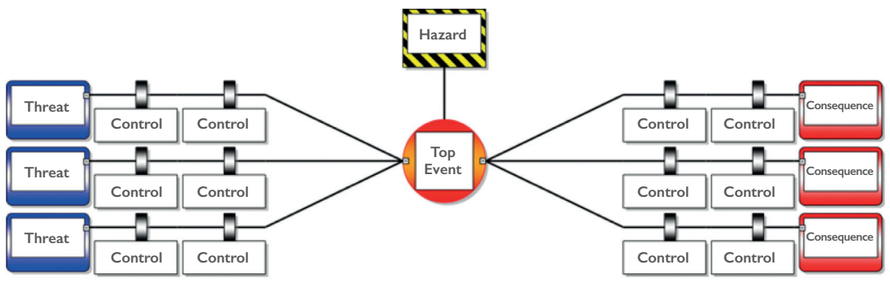
- The causes are events that lead to a hazard or hazardous condition. Causes can occur by themselves or in combinations and can be technical and procedural in nature.
- A hazard is "*anything real or potential, that could make possible or contribute to an accident. A condition that is a prerequisite to an accident.*"

FIGURE 3:
HAZARDS VS CAUSES



Sharp eyed readers might note that the model above could also be replicated in a Bow Tie Analysis, but this is not the only approach. Figure 4 thus also shows the relationship between a hazard, the causes/threats that can lead to it occurring and the consequence (or accident) that follows the occurrence.

FIGURE 4:
ACCIDENT, HAZARD & CAUSE/THREAT RELATIONSHIP



Whichever modelling technique is chosen, understanding this causal relationship leads to better management of the term "*hazard*" by separating (but not ignoring) its consequences and its causes.

[2] Or "unwanted outcome", which might be more appropriate when we consider "enterprise risk" (see section 5.1)

4.2 How do we identify hazards?

Systematic hazard identification is an extremely important feature of a robust management system. After all, it is the hazard we do not know about which should concern us most! There are many different approaches/techniques which may be useful and which are not within the scope of this paper[3]. Whichever technique is used it is often useful to distinguish between 2 distinct groups of hazards when considering the organisation interfaces in the supply chain:

Endogenous Hazards	Exogenous Hazards
Arise from causes within the system	Causes by external influences outside the system boundary
It implies that something has gone wrong due to: • system faults, which are a specific state of a system (e.g. cross connection of wires), or • physical hazards, which are always present in a system (e.g. hot surfaces, sharp corners, etc), or • functional failures, which usually require an initiating event (e.g. components or equipment failures), or • human failures (e.g. controlling errors, maintaining errors, monitoring errors, etc), both with or without function failures	Results from the following environmental causes: • physical (e.g. weather), or • peer platforms (e.g. other aircraft) • people (e.g. sabotage, hijacking, etc)

Sharing information could also be extremely useful for the hazard identification process. After all, operators of large civil transport aircraft should surely all be managing many of the same type of hazards? The difference between these common hazards is down to the individual causes, mitigations and probabilities of occurrence. This does, however, assume that all operators have defined hazards at the correct system level. Hazards are properties of an entire system and may be defined at any system level. However, it is essential to select the right level:

- A common mistake is to select it too low, which results in too many hazards, no system properties and expensive (impossible) manage.
- If you select it too high, then it is hard to ensure the identification and management of all hazards.

Example of Hazard Levels

To continue our braking example from paragraph 1 above, the hazards can be broken down into its constituent elements subsystems as follows:

1. Loss of controllability - Level A
   - 1.1 Braking
     - 1.1.1 Loss of braking - Level B
       - a. Brake pipe ruptures - Level C
       - b. No brake fluid - Level C
       - c. Brake booster failure - Level C
     - 1.1.2 Uncommanded braking - Level B
   - 1.2 Steering
     - 1.2.1 Loss of steering control - Level B
     - 1.2.2. Over-steer - Level B
     - 1.2.3. etc

This example demonstrates that the Level B hazards would probably (but not necessarily so) be the appropriate hazard level to manage, because:

- Level A might be too vague by not focusing on any specific system, and
- Level C being designated as contributing causes/failures to the Level B hazard
- Level B directly leads to the accident

[3] For more information, see Appendix A in Kritzinger (2006), which lists a number of approaches along with their advantages and limitations.

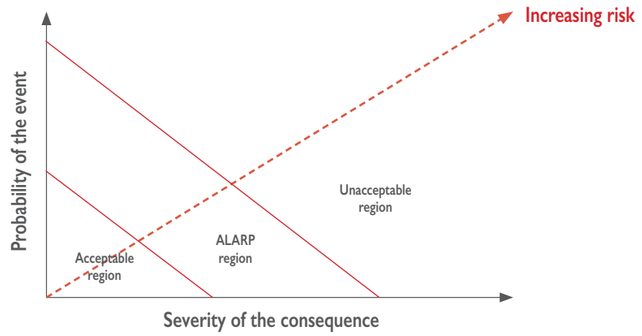
4.3 What is "risk"?

The term "*risk*" has long become widely accepted to mean "*the combination of the probability of harm and the severity of that harm*" [refer, inter alia ISO/IEC Guide 51 (1999)]. So, this implies that risk can be expressed as the combined effect of the probability of occurrence of an undesirable event, and the severity of the consequence of that event. This can be expressed mathematically as follows:

R = S x P, with:
R = Risk
S = Severity of the consequence (i.e. not the hazard)
P = Probability of occurrence of the consequence

So, risk increases with either severity or the probability of the consequence (i.e. accident) as illustrated in the following diagram:

FIGURE 5:
INCREASING RISK



In any accident there is rarely only one single causal path, rather more a unique combination of factors (such as system failures, errors, equipment failures etc) that create the outcomes we see. This concept is illustrated in Figure 6 below:

FIGURE 6:
SIMPLE ACCIDENT SEQUENCE MODEL

So, to estimate risk we are thus not only interested in the probability of a specific hazard and/or cause (such as equipment failure, or human error), but also in all the factors that lead to the undesired consequence. Accidents happen when the characteristics of different factors (such as component failures, procedural shortcomings, and environmental effects) combine[4]. Manipulating any of the causes/hazards/events in the accident sequence can influence the risk, and this includes the series of human behaviours (e.g. pilot error when exposed to increased stress) which may contribute to the accident.

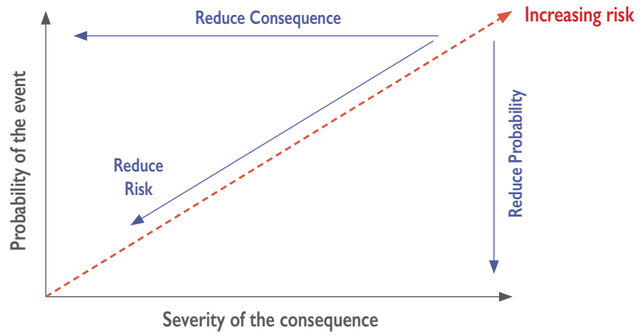
Safety risk therefore relates to accidents (i.e. the event causing the harm) rather than hazards (i.e. the situation with the potential to cause harm) or failures of any individual piece of equipment. This is often misunderstood when risk criteria in incorrectly applied to the failures or hazards instead of to their harmful outcomes.

[4] An ARINC advert sums this up nicely: "*The passenger in seat 16F depends on pilot awareness, which depends on the tower, which depends on the satellite, which depends on the data link, which depends on the ground station, which depends on ARINC*"

4.4 Why do safety risk management?

The purpose of risk management is to reduce and maintain risk at an acceptable level. It is as simple as that! We reduce risk by either reducing the severity, or the probability, or both. This is illustrated in the figure below:

FIGURE 7:
REDUCING RISK



Risk Assessment seeks to answer the following relatively simple questions although, like many other questions, these are far easier to pose than to respond properly to:

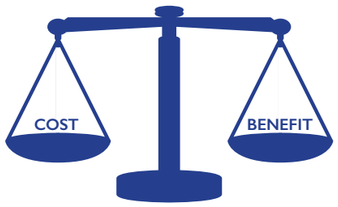
- What can go wrong?
- How badly can it go wrong?
- How often can it happen?
- So what (i.e. what is the level of risk)?
- What can I do about it?

The key to effective safety risk management is to allocate our management effort where it is most needed. For that we need to know when risk is elevated from its desired state, which relies upon our understanding of when risks may be accepted to be as low as reasonably practicable (ALARP).

4.5 What is ALARP?

We often hear pundits pontificate phrases such as "*safety at all costs!*" and "*safety is our number one priority!*". Unfortunately, that is not strictly true. There is always a balance to be struck between what is considered to be acceptably safe versus the cost implication of ensuring it is so.

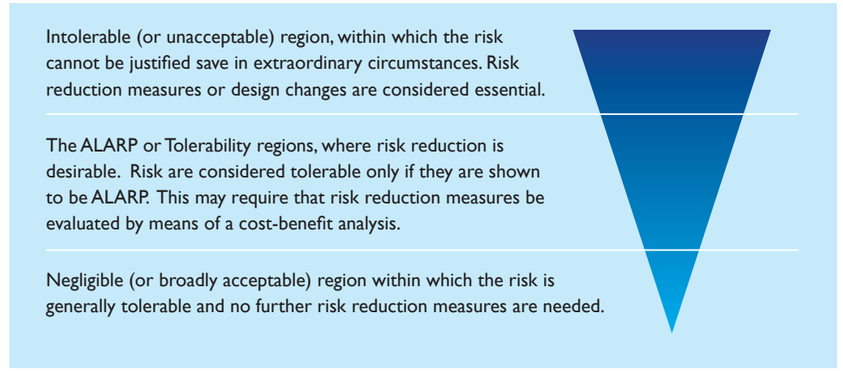
FIGURE 8:
COST-BENEFIT ANALYSIS



The UK's Health and Safety Executive (HSE) provides a useful model in this regard and it is called the ALARP triangle[5]. ALARP is based on the legal standard of "*as low as reasonably practicable*". This standard has acquired its meaning in case law (i.e. the decisions made by judges in court) and has come to mean that the degree of risk of injury or adverse effect must be balanced against the cost in terms of money, time, and physical difficulty, of taking measures to reduce the risk. If the quantified risk of injury is insignificant compared with measures needed to mitigate the risk, then no action need be taken to satisfy the law. However, the greater the risk, the more likely it is to be reasonably practicable to go to substantial expense to do something about it.

[5] The triangle illustrates the concept of diminishing proportions (i.e. level of risk, societal concerns, and level of effort needed to reduce it).

FIGURE 9: ALARP TRIANGLE



From a UK legal perspective, here are the key drivers to all organisations (whether they are approved or not) having to manage safety/environmental risk:

- The Health and Safety at Work Act (HSWA), impose duties on persons who design, manufacture, import or supply articles for use at work to ensure (so far as reasonably practical) that they are "*safe*"; to test them; provide proper information; carry out research with a view to eliminate risks; etc. Breach of this obligation in typically enforced via criminal law.
- Criminal law does little for the victims of a crime. Civil law (the law of Tort) regulates the relationship between individuals and thus provides the mechanism whereby the wrongdoers have to compensate the victims. Guilt is determined through the application of the "*balance of probability*" principle. Civil liability for a defective system/services can arise under the laws of contract, misrepresentation, tort, other common law doctrines and under current UK legislation. Liability can fall on the manufacturer, supplier, distributor, certifier or user of products.
- Suppliers of components or services can also be liable (not just "Duty Holders", to use UK MoD terminology). Under Civil Law (Tort), individuals can claim compensation if they can show that a duty of care was owed; this duty has been breached; and that a loss has been suffered. Note: The claimant does not have to prove negligence on the part of the supplier. All professional work is done under contracts containing either an express or implied term that professional person will use reasonable skill and care in the performance of the work.

So, SMS becomes the organisation's enabler to manage the safety risks (this is surely the intent behind Annex 19). In assessing those risks they need:

- to consider which risk they own (and need to mitigate) and which they transfer (or hand over) to their customer(s) to own and manage
- how they ensure that all these risks are acceptably low (i.e. by managing the probability and/or the severity of the potential consequence).

5. So where does it get complicated?

When it comes to risk management there are at least three areas which are challenging to many organisations: The terminology they use, their SMS commitments to their Board, and their simultaneous supply chain SMS obligations[6].

5.1 Terminology and Criteria

Management confusion start with terminology confusion. What lies between sorcery and science is often a matter of having a common lexicon. To make advances into the age of SMS, we need to make sure that our terminology is defined and the criteria we use to judge "*safety*" is standardised and consistency applied. Paragraph 4 above discussed terminology, whilst paragraph 5.2 below highlights the issues with the criteria we apply.

5.2 The Board needs to execute an integrated SMS.

We all know by now that an SMS needs to be taken seriously at Board level if it has any chance in becoming effective[7]. However, at Board level their safety management obligations extend beyond aviation safety to also include other safety concerns (such as security, health and environmental impacts) as well as the ICAO expectation of organisational safety (see paragraph 1). In itself this is not a challenge, but it does require a standardised set of safety risk criteria to facilitate effective safety risk management across the whole organisation (often referred to as Total Safety) and to develop a robust safety culture.

An example of how this can be approached is illustrated in the following matrix by Shell, which was published in the mid-1990s:

Potential Consequences of the Incident					Increasing Probability				
Rating	People	Environ.	Assets	Reputation	A Unknown but possible in the aviation industry	B Known in the aviation industry	C Happened before in Corp.	D Reported > 3x / year in Corp.	E Reported > 3x / year in location
0	No injury	Zero effect	No damage	No exposure	Manage through normal procedures				
1	Slight injury	Slight effect	Slight damage < US$ 10K	Slight exposure					
2	Minor injury	No effect	Minor damage < US$ 50K	Regional exposure					
3	Serious injury	No effect	Significant damage < US$ 250K	Industry exposure	3		Incorporate risk reduction measures		
4	Single fatality	No effect	Extensive damage < US$ 1M	National exposure		2		Intolerable	
5	Multiple fatality	No effect	Major damage > US$ 1M	International exposure			1		

This standardised criterion is very effective at Board level, but it does present significant challenges to other parts of the organisation. For instance:

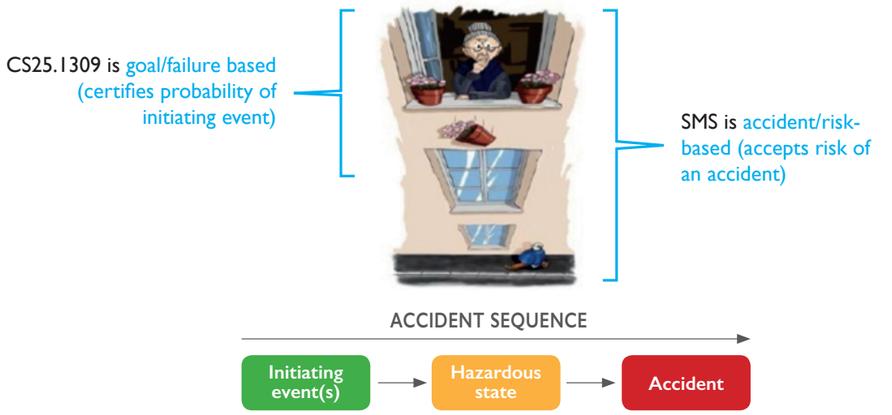
- If a civil Design Organisation is designing to meet the safety criteria of CS25.1309 (which is goal/failure based and is measure in probabilities per flight hour), then how do they relate this to the risk/accident based criteria of the SMS? This is not an insurmountable obstacle but does require consideration and, when it comes to CS25.1309, is most usefully illustrated in the following carton which shows that CS25.1309 feeds the SMS. The two approaches compliment, they do not replace, each other[8].

[6] Refer, inter alia, to para 2 in EASA Terms of Reference (TOR) for rulemaking task RMT.0251(b) (MDM.055-MDM.060) TOR, which has an aim for organisations to "*take a systematic approach to identifying aviation safety hazards, including their own organisational hazards, to assess the associated risks, and to effectively mitigate their consequences*".

[7] SMS is supposed to be structured process that obligates organisations to manage safety with the same level of priority that other core business processes are managed.

[8] Think of it this way: The designer needs to design a ledge for the pot and argues safety of that ledge. That does not mean that all hazards are totally mitigated and the operator has a responsibility to manage the operational hazards. Bird strike is a real example: The Designer Organisation will prove that the engines can survive a single 4lb bird strike at a certain velocity (and hence meet his safety objective). The operator needs to implement wildlife controls and Emergency Response Planning (ERP) as part of his SMS.

FIGURE 10:
GOAL VS RISK BASED CRITERIA



Source: ICAO Safety Management Manual (2nd edition, page 28, figure 2.8)

- If an organisation's activities cover multiple domains (e.g. Air, Land and Sea), a conversion factor may need to be defined for each so as to simultaneously satisfy the particular Regulator Authority's safety criteria and the Board's SMS safety criteria. This "conversion factor" has to be integrated in the supporting process and should not have to be additional effort or lead to duplication of data.
- The above two bullet points assume that hazards communicated to our customers are also directly translated to our own Board. This approach might not be always be appropriate, especially if we consider (a) the inability to control the complete accident sequence, and (b) the scope of our responsibilities (or the scope of barriers/mitigations that we are liable for). It may be more appropriate to for the Board to consider a different level of safety risk[9] which will not be communicated to our customers, such as:
  - For a Design Organisation: "*There is a hazard/risk that, in spite of meeting our design safety targets (i.e. $1x10^{-9}$ or $1x10^{-7}$), probabilistically our system can still be a primary cause of an accident tomorrow*"
  - For a Production Organisation: "*There is a hazard/risk that our suppliers provide defect materials*"
  - For a Maintenance Organisation: "*There is a hazard/risk that we make an HF error and release non-conforming parts*"
  - For a CAMO: "*There is a hazard/risk that we are unaware of an important Service Bulletin*"

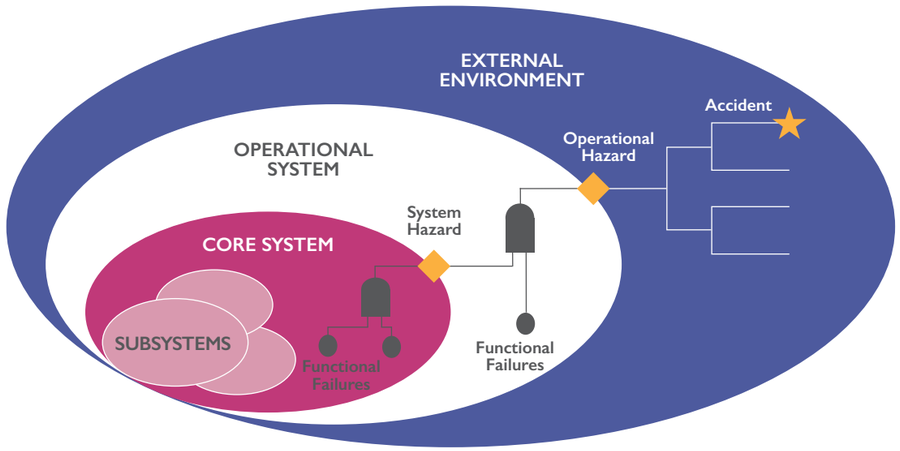
A consolidated risk matrix provides a company (which might be a component provider who is far removed from the operational deployment of their technology) with visibility of the safety, environmental reputational, etc. risks they are exposed to in their sphere of influence.

[9] Tongue in cheek, in this context it is useful perhaps to think of the SMS as a "*Surprise Management System*"

5.3 SMS needs to consider the whole supply chain

Industry is required to acquire, integrate, operate and maintain products which are sufficiently safe at the point when the user interfaces with it. An unsafe product (actual or perceived) will result in retribution in law, contracts and/or the market place. Risk management is relatively uncomplicated if the whole accident sequence (refer Figure 11 below) is under the control of a single organisation, but that is seldom the case. There are a number of "fingers in the pie" and the challenge is to manage the interfaces between affected (and impacted) stakeholders, as illustrated below by Sandom & Fowler (2006):

FIGURE 11:
OUR SYSTEM BOUNDARIES



When it comes to operator safety (i.e. the ability to continue safe flight and landing), factors to consider therefore include:

- The Sharp End: Operators are at the end of the supply chain and need to manage the hazards which have been communicated to them via the aircraft supply chain (e.g. failure modes predicted by the Design Organisation, ATC (e.g. bad weather), Airports (e.g. wind shear) as well as from operational experience. Ultimately, the operator needs to accept the risk to safety and many of the factors discussed in section 1 above come into play in their decision making. Key questions to ask:
  - Are we involving those at the sharp end enough?
  - Are we making ALARP statement on behalf of someone else whilst sitting in a nice warm cosy office?

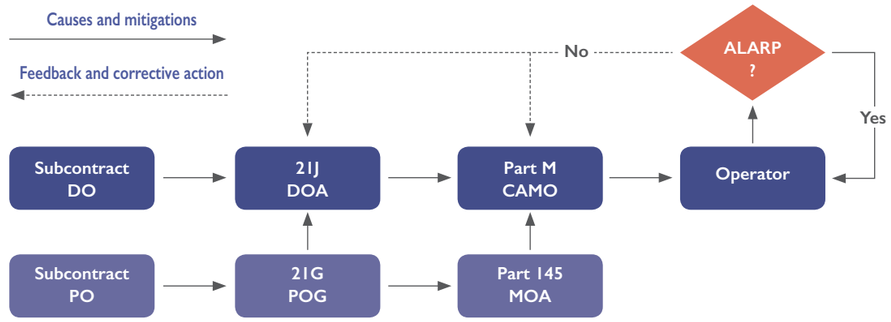
[10] See GM4 ORO.GEN.200(a)(3) Management system COMPLEX ORGANISATIONS — SAFETY RISK MANAGEMENT — INTERFACES BETWEEN ORGANISATIONS which states:

(a) Hazard identification and risk assessment start with an identification of all parties involved in the arrangement, including independent experts and non-approved organisations. It extends to the overall control structure, assessing, in particular, the following elements across all subcontract levels and all parties within such arrangements:
  (1) coordination and interfaces between the different parties;
  (2) applicable procedures;
  (3) communication between all parties involved, including reporting and feedback channels;
  (4) task allocation responsibilities and authorities; and
  (5) qualifications and competency of key personnel.

(b) Safety risk management focuses on the following aspects:
  (1) clear assignment of accountability and allocation of responsibilities;
  (2) only one party is responsible for a specific aspect of the arrangement — no overlapping or conflicting responsibilities, in order to eliminate coordination errors;
  (3) existence of clear reporting lines, both for occurrence reporting and progress reporting;
  (4) possibility for staff to directly notify the operator of any hazard suggesting an obviously unacceptable safety risk as a result of the potential consequences of this hazard.

- The Supply Chain: The whole supply chain needs to manage safety[10] but, when it comes to aviation safety (i.e. the ability to continue safe flight and landing), how can a Maintenance or a Production Organisation determine the severity or the probably of the end event? I can be argued that, at most, they can offer input into the contributing causes and their mitigations. This requires a closed loop SMS process (i.e. one with feedback) which involves the whole supply chain, maybe something approaching the model illustrated below:

FIGURE 12:
RISK MANAGEMENT IN THE SUPPLY CHAIN



Key questions to be asked by/from each organisation's SMS include:

- Which aviation safety hazards are you managing?
- How are these communicated to the board?
- How are these communicated to the end user?
- Do we have adequate feedback mechanisms to hold all contributing stakeholders accountable for safety?
- Who pays to fix it if it is not ALARP?
- When is a procedural fix not good enough and an architectural modification is required?

We need to widen our view to explore each approved organisation's assumptions, obligations, interfaces and how a full system understanding will benefit the aviation industry. The benefits obtainable from the implementation of ICAO Annex 19 can only be exploited collaboratively.

6. Conclusions

We have shown that there is no such thing as absolute safety. Yet, industry is required to develop, operate and maintain products which are sufficiently safe. An unsafe product (actual or perceived) will result in retribution in law and/or the market place. It is therefore essential for our Management System to ensure that effective procedures and practices are in place to ensure that a product/service is "*safe enough*" and the SMS is intended to be the vehicle which does just that. The SMS must ensure the law is satisfied and must also protect against the fallibility of the human (i.e. producer, maintainer or consumer) involvement.

The general principles of safety risk management are [FAA System Safety Handbook (2000)]:

- All system operations represent some degree of risk. Recognise that human interaction with elements of the system entails some element of risk.
- Keep hazards in proper perspective. Do not overreact to each identified risk, but make a conscious decision on how to deal with it. Dr Trevor Kletz is known to have said: "*To maintain the balance in your risk exposure levels, when confronted by a new risk, just smoke one or two less cigarettes a day.*"
- Weigh the risks and make judgments according to your own knowledge, inputs from subject matter experts, experience, and program need. There may be no "single solution" to a safety problem. There are usually a variety of directions to pursue. Each of these directions may produce varying degrees of risk reduction. A combination of approaches may provide the best solution.
- Risks are reduced asymptotically. Thus the closer to zero we get the more effort is needed. We thus need to know when enough is enough. A good decision made quickly is much better than a perfect decision made too late. Also, a good decision does not always result in a good outcome. The best we can hope for is to equip intelligent decision makers with good information based on a number of decision factors and the interests of stakeholders. On average, and over time, good decisions made through this process should provide the best outcomes. They will also provide logical explanations for decisions when the outcomes are not favourable.

Remember that producing a risk assessment is simple enough, the challenge lies in demonstrating that risks have been identified in a structured and systematic way and that the risks are managed throughout the product life-cycle, i.e.:

- Implement Risk Control: Risk Management activities have no effect on Risk until the process of Risk Control is implemented to actually change the design; to add safety protective features; or to alter working practices.
- Assess Risk Continuously: Assessment of technical risk depends on the quality and quantity of information available as well as the decision making and associated potential biases. There may be very little data available in the preliminary stage of a decision-making process. As the process progresses, the results of system safety analysis; failure mode, effects and criticality analysis; and compliance testing may provide the necessary information and details required to refine the risk assessment. Ultimately, actual operational use and airworthiness-related occurrences will provide the most valuable information. Even then, the risk changes as the socio-technical system evolves, or the technical system ages, or perhaps as operating or maintenance procedures (and personnel) alter.

Final point to ponder: Are we spending too much time on justifying that something is acceptably safe, rather than trying to prove that is in unsafe? Confirmation bias is the tendency to search for, interpret, favour, and recall information in a way that confirms one's pre-existing beliefs or hypotheses, while giving disproportionately less consideration to alternative possibilities.

7. References

7.1 Kritzinger, D.E. Aircraft system Safety: *Civil and Military Aeronautical Applications,* Woodhead Publishing Ltd, UK, 2006.

7.2 Murphy C. S, *Hazard Analysis*. Paper presented at Design for Safety: Proceedings of One Day Conference held at the Aeroplane and Armament Experimental Establishment, Boscombe Down, Thursday 11 April 1991, Royal Aeronautical Society, London.

7.3 Miller, C. O. *System Safety*, Proceedings of the 11th Safety Critical Systems Symposium (page 105), Bristol, UK, 406 Feb 2003.

7.4 ASD-100-SSE-1 (Rev 7D), *NAS Modernisation System Safety Management Programme*, US Department of Transportation, FAA .

7.5 Safety Handbook, 2000, http://www.asy.faa.gov/Risk/SSHandbook/contents.htm

7.6 Sandom, C and Fowler, D, *People and Systems: Striking a Safe Balance Between Human and Machine*, as quoted in Redmill F and Anderson T, *Developments in Risk-based Approaches to Safety*, Proceedings of the 14th Safety-critical Systems, Symposium, Bristol, UK, 7 – 9 February 2006, Springer-Verlagomr.

7.7 Eurocontrol, Hindsight 25, Work-as-imagined and work-as-done: a Safety Management Reality Check for Regulators, Summer 2017

7.8 EASA Opinion No 06/2016, "*Embodiment of safety management system (SMS) requirements into Commission Regulation (EU) No 1321/2014 — SMS in Part-M*"

7.9 EASA Terms of Reference (TOR) Terms of Reference (TOR) for rulemaking task RMT.0251(b) (MDM.055-MDM.060)] - *Embodiment of safety management system requirements into Commission Regulations (EU) Nos 1321/2014 and 748/2012 'Phase II — SMS*

7.10 ICAO Safety Management Manual Doc 9859 (2nd Edition) 2009

BAINES | SIMMONS
World Leaders in Aviation Safety

White Paper Plus+

About Baines Simmons

We are specialists in aviation regulations, compliance and safety management and partner with the world's leading civil and defence aviation organizations to improve safety performance.

As trusted advisors to businesses, armed forces, governments and regulators across all sectors of aviation, we help to advance best practice, shape safety thinking and drive continuous improvement to safety performance through our consulting, training and outsourced services.

We have a range of white papers available, sharing our expertise in aviation safety issues, from views on industry news, to more in-depth papers designed to stimulate discussion and debate.
View and download them at **www.bainessimmons.com/papers**

Baines Simmons is the consulting arm of the LSE-listed global aviation services group, Air Partner PLC
www.airpartner.com

Author

Duane Kritzinger
Principal Consultant, Baines Simmons

Duane Kritzinger is an experienced Certification and Safety Engineering specialist. His distinguishing safety expertise lies in the ability to differentiate and integrate the Safety Assessments in the design phase with the Safety Management activities in the operational phase. His certification skills cover both the military and civil aviation domains, where he not only provides expertise in the certification of products/parts/appliance, but also assists with EASA/EMAR Part 21 Design Organization Approvals (which includes the establishment of organization processes and structures to move beyond minimum compliance towards organizational performance).

Since the publication of EMAR 21, Duane has been assisting both the military regulators (in their adoption of EMAR 21) and the regulated community (in demonstrating compliance in the most efficient manner with due consideration of other approvals held).