Introduction to EME1.1 Task Philosophy

Brian E. Smith, Code TH, NASA Ames Research Center
Corinne Bieder, Airbus Product Safety Department

7 September 2011

Purpose of this Document

The purpose of this document is to describe and discuss the foundations on which the prognostic methodology under development by the Future Aviation Safety Team (FAST) will be built. Indeed, unless a hazard and risk analysis methodology is based on an agreed-upon definition of terms and an explicit conceptual framework, it is likely to be ineffective or misused.

This document is intended to define the philosophical underpinnings of the proposed methodology, clearly define and tease out the subtle meanings of terms that are commonly used but often not fully understood, and to identify the key elements that must be part of any useful method for future aviation hazard analysis.

This document will also be useful in articulating the important characteristics of existing risk analysis methods that could be taken onboard by the new methodology requested by the European Aviation Safety Agency (EASA). The first step in the development of the methodology is a review of existing risk analysis methods for the applicability of certain of their capabilities to the FAST method under development.

Problem Statement

Addressing emerging issues in air transport safety or more specifically coming up with a methodology to assess future risks (as stated in EME 1.1) combines a number of challenges:

- Dealing with safety, hence risk and even uncertainty in the case of a complex system such as the air transport system
- Dealing with the future, adding its share of uncertainty
- Covering the whole range of players in air transport safety and all levels, up to the air transport system as a whole.

To take up the first challenge, a significant number of risk assessment methods already exist. However, each of them has a specific scope, a formal objective and even a definition of risks that may not be compatible with/suitable to the objective of task EME 1.1.

Likewise, dealing with the future can be achieved through a variety of approaches, relying on incompatible fundamental assumptions, from a crystal ball perspective to a modest viewpoint acknowledging that the future cannot be anticipated.

Coming up with a methodology usable by all players of the air transport system, at all levels of this system, can also be achieved in different ways, from assuming it is possible to embed all the required knowledge and experience in the methodology itself, to remaining at a rather general level in the methodology and calling for domain specific expertise and knowledge throughout its implementation.

In other words, there is no unique answer to the task. Therefore, before proposing any answer, it is essential that FAST carefully clarify:

- The concepts that will be used
- The conceptual framework on which it will be based
- The possible expected outcome for task EME 1.1

Concepts

Comment [E1]: *For each of the concepts, the idea could be to present a literature review and end up with the definition adopted by FAST where several definitions exist.*

Risk, Uncertainty, and Predictability

The terms risk, uncertainty, and predictability must be clearly defined in order to be useful within methodology constructs developed by the Future Aviation Safety Team under task EME1.1, *"Methodology to assess future risks - Adapt or create a robust method to assess future risks based on expert judgment, project studies, questionnaires and scenarios"* within the European Aviation Safety Plan. It is important to distinguish among the characteristics of these commonly used, but misunderstood terms(Claycamp, Risk, Uncertainty, and Process Analytical Technology, 2006).

Risk

Risk is often defined as two-dimensional vector combining the severity of the outcome/ consequences of an unwanted event/accident and its probability of occurrence. It is sometimes simplified and represented by the multiplication of both dimensions (severity of consequences x probability of occurrence).

More generally risk is an uncertainty, threat or opportunity that the system or activity considered has to anticipate, understand and manage to protect its value and meet its strategic objectives. (Alain Desroches, 2009)

Risks are often represented on a two dimension matrix, as follows:

LIKELIHOOD OF OCCURRENCE	L5					
	L4					
	L3					
	L2					
	L1					
		S1	S2	S3	S4	S5
		SEVERITY OF CONSEQUENCES				

Note: Risk tables and accepted definitions of risk categories useful in the aviation domain are listed in the appendix. The terms and definitions in these tables are in common use among passenger aircraft designers, operators, organizations, and manufacturers/maintainers. The FAST proposes to use this foundation for development of its future risk assessment methodology.

Harm

Human injuries and fatalities, classified by severity and accumulated, property loss and damage, environmental loss and damage including pollution; any other loss of worth considered by regulation or stakeholders to be deleterious (Ladkin, 2008).

Severity (of harm)

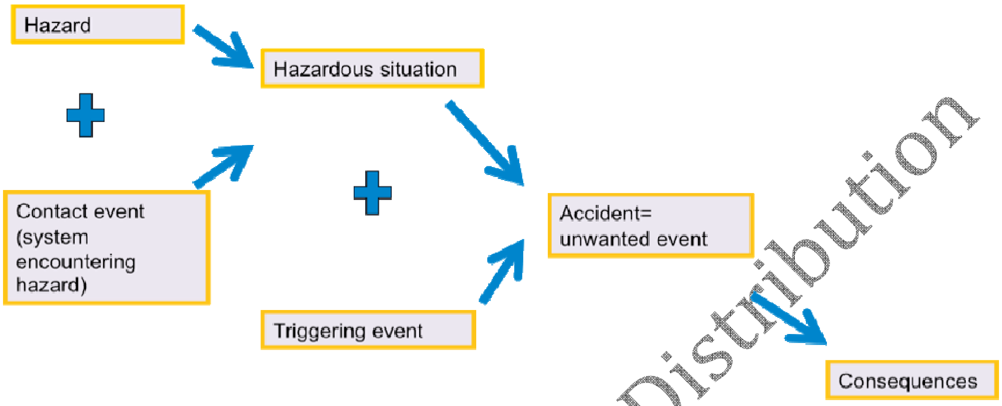
Amount of harm stated in terms of agreed units (for example, numbers of fatalities, severe injuries, minor injuries; damage to property or objects in terms of amortised replacement cost where applicable; expected cost of cleanup of environmental damage) (Ladkin, 2008).

Hazard

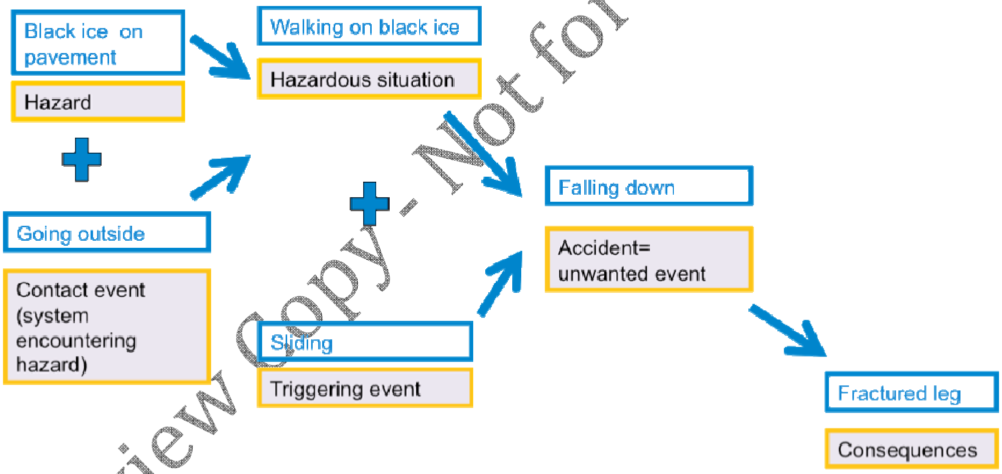
Proposed methodologies will employ the standard definition of a hazard: A hazard is defined in FAA Order 8040.4 (FAA Order, 2004) as a "Condition, event, or circumstance that could lead to or contribute to an unplanned or undesirable event." Seldom does a single hazard cause an accident. More often, an accident occurs as the result of a sequence of causes. A hazard analysis will consider system state, for example operating environment, as well as failures or malfunctions. A hazard is a: condition, object, or activity with the potential of causing injury to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function when it appears in the context of a particular operational situation. It takes both the hazard itself and a triggering situation to generate an operationally significant safety event. Others (Leveson, 1995) emphasize the importance of contextual factors and require that “a hazard is a state or set of conditions of a system that, *together with other conditions in the environment of the system* [author emphasis], may lead to an accident [loss event].”

Accident scenario

In order to better understand the various concepts and how they articulate, it can be useful to refer to an accident scenario.



For example, if the system considered is a walker, a possible accident scenario is:



Other concepts related to risk include:

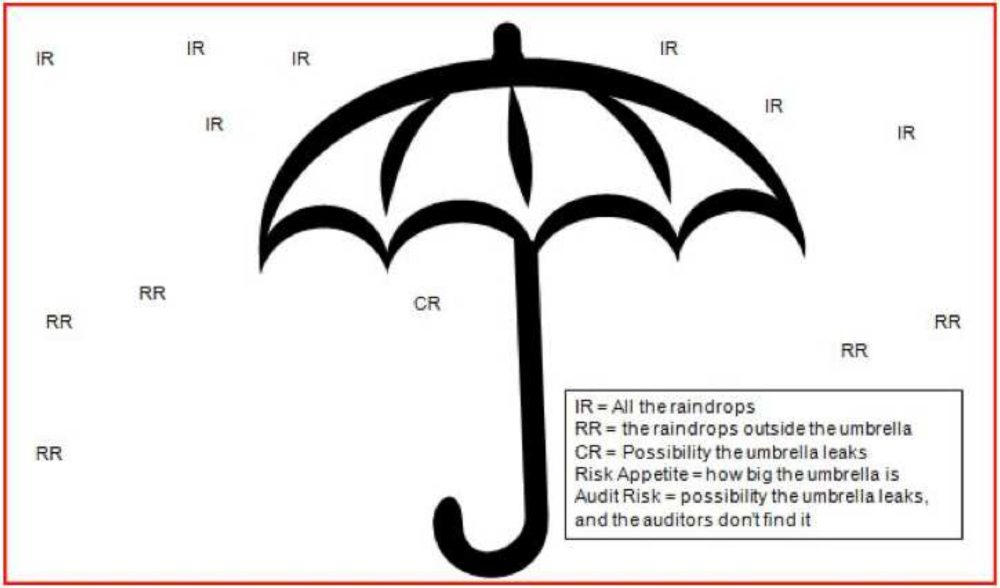
Comment [b2]: Do these definitions really serve directly our purpose?

Risk event is the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of impact and probability (also called consequences and likelihood).

Inherent risk (IR) is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.

> **Residual risk (RR)** is the risk that remains after management's response to the inherent risk of a particular technology or human-related change. Once controls have been developed another risk assessment is necessary. Controls may come in the form of engineered barriers, training and procedures to avoid or take certain actions to reduce severity or likelihood of a hazard. Other factors influencing net risk is the extent of implementation of controls and the effectiveness of the outcomes of targeted research projects. Control Risk (CR) is the risk that the full suite of controls fail to reduce risks to an acceptable level. The resulting net risk level is called Residual Risk (RR) – this is a key interest area for the European Aviation Safety Agency.

These terms are easily demonstrated by thinking of an umbrella (a control or risk response); raindrops (a risk event); and an objective to stay dry.



Safety

The contrary of risk (Ladkin, 2008).

Comment [b3]: Not so convinced by this definition. My understanding of safety is: the absence of unacceptable risk.

Acceptable risk

It is the value of risk resulting from an explicit decision and established in an objective way by comparison to existing known and accepted risks in other industrial fields, be they natural or technological.

In practice, three classes of risks are defined according to their criticality:

Comment [E4]: Michael Kavoliunas:
High threats to safety are the most important. So why not have them first (first column) and why not have the most probable ones at the top of the column? Acceptable level of risk is the threshold for the given Severity level. For design these are defined internationally per FAA and EASA Advisory Circular 25.1309 as per the Risk Matrix Definition document I have attached. A catastrophic event must not be a single event and the probability of the combination of events must be Extremely Improbable or 1E-09. Therefore, if safe for the design it must be safe in service and that means then level 1 in Column A (bottom of the column has to be green or Low risk otherwise something potentially catastrophic will never be acceptable). The same logic is used for the remaining columns. On page 6 for Acceptable risk it states yellow is acceptable with monitoring. Then why is it yellow. The stoplight colour idea is red is bad, yellow is getting bad and green is good. This is why we took the colours of our matrix as the colours get misinterpreted. In our matrix L is Low risk not no risk and is Acceptable (again it must always be monitored), M is Medium - a 2 order of magnitude shift more probable which is unacceptable, H is high and needs immediate mitigations and Extremely High is STOP.

- In red: unacceptable as such i.e. risk reduction actions must be taken or the activity stopped
- In yellow: acceptable under monitoring
- In green: acceptable as such

		SEVERITY OF CONSEQUENCES				
		S1	S2	S3	S4	S5
LIKELIHOOD OF OCCURRENCE	L5	🟨	🟥	🟥	🟥	🟥
	L4	🟨	🟨	🟥	🟥	🟥
	L3	🟩	🟨	🟨	🟥	🟥
	L2	🟩	🟩	🟨	🟨	🟥
	L1	🟩	🟩	🟩	🟨	🟨

For users of risk management techniques, acceptable residual risk may be set at a level As Low As Reasonably Practicable (ALARP).

Risk Controls, Mitigations and Countermeasures (3 Types)

Physical controls (engineered controls) monitor and control the environment of the work place. They encompass a variety of engineered remedies to contain and/or reduce access to hazardous environments and/or physical barriers intended to limit access to system control functions. They also monitor and control access to switches, levers, and input devices. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the work place into functional areas is also a type of physical control. An important physical control that is frequently overlooked is the **separation of duties**. Separation of duties ensures that an individual cannot complete a critical task by himself. This is important in flight deck and air traffic control settings.

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed. Administrative controls are often the weakest of the possible control measures.

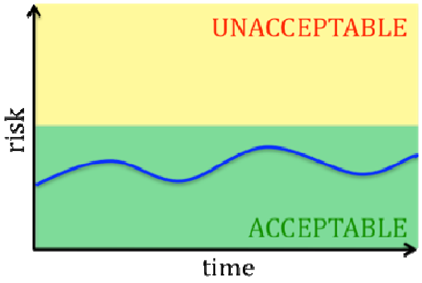
Using an approach that implements engineering controls to create an initial low-hazard environment is the first step for effective risk management. Engineering controls are those things you do to ensure safety by design and include elements such as machine guards, proper lighting, security systems and environmental controls.

Administrative risk management control is a less effective means for controlling risk, however engineering controls cannot be implemented for all events. Administrative risk management is the second line of defense for prevention and mitigation of potential hazards. Administrative controls include written policies and procedures to ensure employees follow safe practices and include identification and implementation of an effective employee-training program (Risk Management, 2011).

Institutional controls are a variety of legal or regulatory devices imposed to ensure that the engineered controls remain in place or, where there are no engineered controls, to restrict prohibited actions by individuals or groups.

Risk Evolution

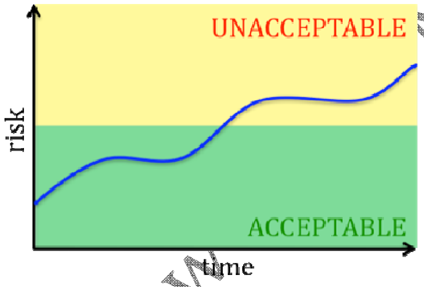
Effect of Future Factors on Risk Acceptance



<u>Scenario 1</u>

- Current hazards controlled by existing mitigations despite changes over time.
- Risk fluctuates within an acceptable band.
- Risk remains acceptable due to resilience of system.
- No new mitigations required.

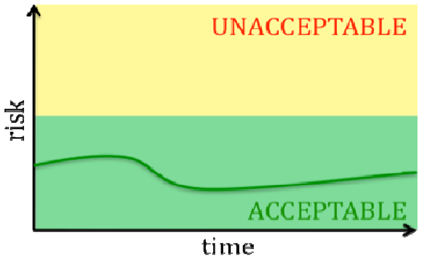
Unacceptable Risk Arising from Future Factors



<u>Scenario 2</u>

- Due to changes over time *and* the absence of key mitigations, risk becomes unacceptable.
- New mitigations required.

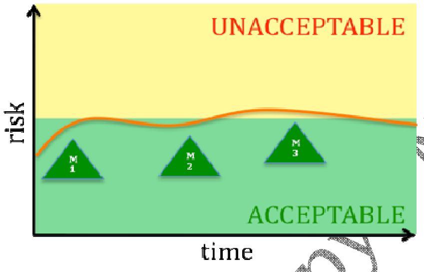
Acceptable Risk Despite Emergence of Future Factors



Scenario 2a

- Despite changing conditions and small increasing trends, risk remains acceptable or decreases due to resilience and responsiveness of existing mitigations.
- No new mitigations required.

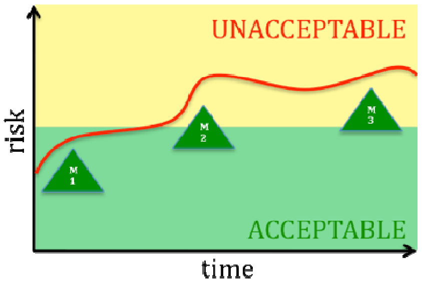
Marginally Acceptable Static Risk due to Future Factors



Scenario 2b

- Over time, risk is static despite existing and new mitigations.
- New mitigations (M1, M2, M3) are marginally effective.

Unacceptable Increase in Risk due to Future Factors



Scenario 2c

- Over time, residual risk becomes unacceptable in critical domains despite existing and new mitigations.
- Drivers behind this phenomenon must be understood.
- Effectiveness of proposed mitigations should be assessed; M1, M2, M3

To be effective, a prospective methodology should identify how specific future factors affecting aviation are changing in the future that will influence the vector of residual risk . The vector (magnitude and direction) will permit decision-makers to determine if the future risk is sufficiently controlled. The general categories of these factors identified by the International Risk Governance Council (http://www.irgc.org/IMG/pdf/irgc_ER_final_07jan_web.pdf) are listed below.

1. Scientific unknowns
2. Loss of safety margins from a variety of internal and external pressures
3. Positive feedback (Systems with positive feedback amplify [future] changes or perturbations affecting them. Positive feedback can be destabilizing for these systems.)
4. Varying susceptibilities to risk among different populations or stakeholder groups
5. Conflicts about interests, values and science (Efforts to manage risks may encounter resistance on the grounds of contested science or incompatible values.)
6. Social dynamics
7. Technological advances that outpace scientific understanding of the risk being assumed by regulatory efforts (including new capabilities, barriers, controls, and mitigations)
8. Temporal complications (for instance, risks that emerge in advance of planned mitigation efforts due to accelerated change)
9. Incomplete, misleading or absent communication
10. Information asymmetries when one stakeholder group has information not available to others

11. Perverse incentives to either foster overly risk-prone behaviors or discourage risk prevention efforts
12. Malicious motives and acts (the 'intentional' rather than unintentional components)

Uncertainty

As mentioned in the definition of risk, risk is an uncertainty. Two general types of uncertainty suffice for most risk management purposes: uncertainty deriving from lack of knowledge about the system and uncertainty due to normal variation: variability. The former is sometimes referred to as "epistemic" uncertainty and the latter, "aleatory" uncertainty. For considerations of future risk, there may be a third type of uncertainty related to the inability of even the most knowledgeable domain experts to know which of several possible branches of the future will occur. Within Process Analytic Technology schemes one might parse uncertainty into five potentially useful categories (Walker, 1998).

Formatted: Justified, Space After: 0 pt, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

- **Concept uncertainty** that arises when variables or potential consequences are selected from a vast array of potential choices. For example, in quality-by-design, there is uncertainty about whether or not the optimal design space has been defined. Due to its open-endedness, generally speaking, concept uncertainty cannot be measured.
- **Measurement uncertainty** arising from both variability and a lack of complete knowledge associated with measuring the selected monitoring variables. For example, how reliable are measurements from a temperature probe over time?
- **Sampling uncertainty** captures the uncertainty from sampling a small subset of the entire population of possible samples and making statistical inferences about the variability or other parameters for the whole population
- **Modeling uncertainty** arises when a mathematical or qualitative decision model is derived to project risk. Often, different mathematical or statistical models will fit existing measurements, but might lead to substantially different risk predictions, particularly when they are used to extrapolate risk beyond the existing observations. Not knowing which model might be ultimately correct creates uncertainty.
- **Causal uncertainty** occurs when inferences about the causes of adverse events are made. In complex systems, alternative causal pathways and confounding can exist and may not be readily detected during analysis.

However, when it comes to the Future, another component of uncertainty becomes key: that of the unknown evolution of not only the system, but also its environment and their interactions. Several ways to apprehend this uncertainty exist, relying on different conceptual approaches. Prediction and prospection are among the possible approaches. These concepts are defined and discussed in the next section.

Environment (of a system)

The collection of objects which do not belong to the system, but which have relations with some of the objects constituting the system. Usually specific relations are of concern, and others not. In this case, we speak of the *world* as containing all objects which have some relation or other, and the environment as the sub-collection of the world containing those objects which have relations of concern (Ladkin, 2008).

Conceptual Framework

Up to this point, the generally accepted definitions of common safety terms have been discussed. In some cases there are subtle nuances to these definitions that are commonly used but not fully understood. In the following section two additional concepts are defined and discussed: prediction and prospection. An understanding and appreciation for the key differences between these two concepts will be critical for development of an effective methodology for assessing future risks. The method or methods may have fundamentally different characters depending on whether they approach future risk from a predictive or prospective viewpoint.

Prediction

- Estimates of the nature of the future environment informed by expert subject-matter opinion
- Results from simulation models based on known, deterministic relationships, and
- Quantitative trend extrapolations.

Prospection

“The act of looking forward in time or considering the future" (Gilbert, 2006). It has also been used for several years in the field of Futures Studies, and is defined to be "the activity of purposefully looking forward [i.e. into the future] in order to create forward views and/or images of the future" (Voros, 2009). Prospection identifies disruptive technologies, events, and conditions within aviation, some being impossible to predict, surprise influences from external domains not intuitively expected to be the sources of hazards and risks, and suggests unexpected uses of technology not anticipated by the original designers, etc. Unexpected uses of technology or disruptive events can be revealed by the construction of scenarios. These are the two fundamental approaches to identifying hazards and risks in the future:

In contrast to prediction, prospection assumes that the future cannot be derived only through extrapolation but that unanticipated ruptures may occur.

Prediction	**Prospection**
Aims at predicting the future	Aims at helping “build” the future
Focuses on one field	Global/systemic approach (considering all perspectives & multidisciplinary)
Essential to quantification	Combines qualitative & quantitative dimensions

Utilizes the continuity principle	Takes into account ruptures, acknowledging the acceleration of social, technological, & economic changes
GIGO effect: whatever the sophistication of the simulation model, predictions cannot be of better validity than initial assumptions	CHAOS effect: this way of thinking does not isolate elements/dimensions from one another and uses conditional tense leading to complex rationales. For this reason, the CHAOS effect may lead decision-makers to get lost among all possible futures – an undesirable outcome.

Single predicted scenario, set of possible "certain" scenarios, uncertainty as an input: a key determinant of the outcome… and of the method itself

Since the objective of EME 1.1 is to come up with a methodology addressing the future, it is important to understand the implications of the underlying conceptual framework on the method itself and on the kind of outcome one can expect.

Conceptual framework 1: The simplest conceptual framework would consider a *single* predicted (most likely) scenario as input.

Conceptual framework 2: A refinement of this conceptual framework would consider a set of *possible scenarios (the most likely ones)*, each of them being studied and considered as certain when studied, the final result being a combination of the various independent analyses of the various scenarios.

Conceptual framework 3: A more sophisticated conceptual framework would consider that *there is no way to define a scenario or a set of scenarios (fixed or considered certain when studied)*, but that uncertainty is part of the very nature of the input.

Whether the method is developed considering conceptual frameworks 1 and 2 or 3 has an impact on the methodology itself, hence on the results. The difference between CF1 and CF2 lies more on the implementation of the method and on the results than on the nature of the method.

Let's consider a simple example where the method supports decision making in packing luggage for a trip taking place in a month-time, minimizing the risk of becoming sick by being either too hot, too cold and/or wet (the assumption being here that the associated diseases are of equal severity). A constraint is that of budget since all the clothes need to be bought.

Looking up weather forecast at destination leads to a variety of forecasts. One source forecasts a cold and rainy weather. Another one forecasts a mild and dry weather. Such discrepancy between forecasts is all the more likely that we are looking at a distant future.

If the method relies on **conceptual framework 1**, the most likely scenario between the two aforementioned is to be determined.

Let's imagine it is the cold and rainy scenario. In such case, the hazards are cold temperatures and rain. The risk is to become sick by exposing one's body to the cold and rain. Risk mitigation would be to wear warm and waterproof clothes. The budget would then be allocated to buying such kind of clothes and packing them.

If the scenario turns out to be wrong (which again is all the more probable that we are talking about a far distant future), then the risk of becoming sick by maintaining one's body at too high a temperature is extremely probable if not certain, with consequences that are assumed to be as severe as for diseases due to low temperatures or wetness. In other words, the results of the implementation of the method do not at all help mitigate the actual risk.

If the method remains the same, but is implemented on a set of scenarios (the most likely ones), i.e. results from **conceptual framework 2**, then two sets of different results will come out. One for the scenario considering cold and rainy weather with risk mitigation measures corresponding to warm and waterproof outwear; and one for the hot and dry scenario with risk mitigation recommendations corresponding to light and breathable clothes. Since the budget is limited, an additional process would need to be applied to come up with an acceptable package, maybe not suited to any other weather forecast than the two initially considered.

If the method relies on **conceptual framework 3**, then no definite weather option will be taken for granted and anything between cold and hot temperatures and dry and wet weather will be considered possible, the possibility of unexpected snow or heat wave not being excluded in case an extraordinary meteorological phenomena should occur. The range of possible futures i.e. weather conditions will be reexamined on a regular basis. Minimizing the risk of being too cold or too hot would then lead to buying a set of clothes that would be flexible enough to face any scenario i.e. a light raincoat, a sweater and tee-shirts.

In other words, depending on the conceptual framework underlying the method and the way it is implemented, for similar budgets the risk mitigation measures would be different.

Chaos, Wildcards & GIGO

The modeling and simulation community has made great strides in predicting near-term future trends for well-behaved, deterministic systems. When variables are known and confined to a manageable set, the simulation results can be quite useful for sensitivity studies, and, in some cases, quantitative predictions of key phenomena.

Systems of forces, equations, aviation accident event sequences or financial trading, can exist effectively in two states: one that is amenable to mathematics, where the future states of the systems can be easily predicted, and another where seemingly random behavior occurs. This second state is termed chaos. It can happen occasionally in many systems. Generally, chaos is an unusual occurrence, and where engineers have the tools they will attempt to "design it out", i.e. to make it impossible (Edmonds, 2011).

Simulation engines represent models of reality, not reality itself. All modelers can honestly say is this: "We've created models that are our best attempts to match up to the real world, but we cannot prove them to be correct. We appreciate that small errors in our models would create dramatically different predictions, and we cannot say if we have errors or not. In our models the relationships that we have publicized seem to hold." (Edmonds, 2011)

What is a "wildcard?" For a label that is becoming part of every day (English) language, there is little information available to help a foresight practitioner make an informed decision about what wildcards are. In regards to foresight, the definition that seems to have the greatest clarity is:

> Wildcards are "low probability, high impact events that happen quickly" (Petersen, Anticipating Global Futures, 2001)

Such events (Petersen, 1999)…

- Have a direct impacts on the human condition
- Have broad, large, important and sometimes fundamental implications
- Move too fast for the whole of the system to adjust to the shock

Wildcard events and conditions do not led themselves to modeling and simulation analysis.

If the wrong information is used in forecast process model or the information is biased in some way by the process or by "wildcards" then the final result will not be as dependable as desired. (Think Garbage-in, Garbage-out - GIGO).

Various biases distort our percepts to fit our belief constructs about the [predicted] future. Among them are (List of cognitive biases, 2011), (Shermer, 2011):

> **Anchoring bias**: Relying too heavily on one reference anchor or piece of information when making decisions (or predictions).
>
> **Authority bias**: Valuing the opinions of an authority, especially in the evaluation of something we know little about.
>
> **Belief bias**: Evaluating the strengths of an argument based on the believability of its conclusion.

Confirmation bias: Seeking and finding confirming evidence in support of already existing beliefs and ignoring or reinterpreting disconfirming evidence.

These biases have greater impact for prediction than for prospection since prediction focuses on the most "likely" scenario as opposed to a set of possible scenarios (prospection).

Characterization

One of the main objectives of system characterization is prediction of dynamic behavior. Behaviors and outcomes are directly linked to safety planning, particularly in regard to risk management. Early characterization tends to be generic and generally avoids presumptions about the future engineering and system design. Later site characterization and modeling needs to consider the specifics of engineering and system design. Iteration may be required as evolving characterizations/descriptions may lead to a re-evaluation of the overall technology and implementation plan. Also, the timing of the plan must be synchronized with the safety risk management efforts so that the findings of the characterization, prediction, and prospection efforts can be linked at the earliest design stages.

Risk Perspectives

Safety experts and the population at large impose certain values on comparisons of high and low risk events. Not all risks having the same product value are created equal. A high severity/low probably event such as a crash of commercial aircraft with loss of life of all aboard is not necessarily viewed as equivalent to a low severity/high probability event such as the side effects of a medication used by a large fraction of the population. This is despite the fact that the fatality risk may be identical.

The methodology emerging from the FAST development activity must acknowledge the notion of uncertainty hence flexibility versus risks or even recommendations. The methodology must help the user think on a continuous basis about risk rather than apply a "one-shot" assessment based on allegedly valid assumptions.

A fundamental principle of risk management is to define *what risk phenomenon is to be managed* (Claycamp, 2006). The methodology under development will require that safety risk managers identify the specific, measureable events or outcomes that must be managed. Absent such concrete variables, risk management is sometimes referred to as *decision making under uncertainty* (Claycamp, Perspective on Quality Risk Management of Pharmaceutical Quality, 2007). The mention of "uncertainty" in regulatory environments such as in clinical trial for drugs, can be unsettling to both the regulator and the regulated alike. Risk management is the process of systematically confronting uncertainty in the assessment of risk and in the evaluation of risk management measures (Kahneman, 1982).

Decision making paradox for prognostic methods

This paradox comes from the rather straightforward observation that there are numerous decision-making methods (both normative and descriptive) each one of which claims to be the "best" one. Furthermore, often times these methods may yield different results when they are fed with exactly the same decision problem and data.

Finding the best decision-making method leads to the formulation of a decision problem itself for which the alternatives are the decision-making methods themselves. Naturally, it would be ideal to know the best method a-priori in order to select the best method from the available ones (Decision Making Paradox, 2011).

Looking only at past events, probability is defined as the number of successful trials divided by the total number of (successful and unsuccessful) trials. But probability in the future sense of risk is a “degree of belief” about the likelihood of future events. Risk estimation for the future chance of loss might come from highly sophisticated modeling and simulation derived from statistical analyses of past experiments. But despite the apparent sophistication of mathematical modeling, risk estimation models are ultimately manifestations of scientifically- founded beliefs about how past knowledge of a system can predict the system’s future behavior. Because future events are unknown in advance, risk estimates (projections) are inherently uncertain (Claycamp, 2006).

Aviation managers often face situations in which a risk management decision does not have a clear direction. Sometimes they refer to uncertain decisions as “risk,” thus confusing the two terms. Often in regulatory settings, risk estimates, uncertainties, and consequences involving expert judgment, uncertainty is sometimes associated with risk (Hammond, 1999). For any methodology that is looking toward risk in future conditions, understanding the important distinctions between risk, uncertainty and predictability is crucial. Not only must the central tendency of the postulated risk such as average, median or mode be communicated but also the associated uncertainty in confidence intervals, percentiles of the risk distributions, or some other assessment of the dispersion of the data (Claycamp, 2006).

For purposes of managing safety performance in a future timeframe, risk cannot be a single number due to inherent uncertainty in prediction. Managing uncertainty can improve precision in the risk estimation while not necessarily reducing the risk; and, managing risk without consideration of uncertainty in the risk estimate can communicate overconfidence, i.e., certainty in the future risk estimate. The negative connotation of risk is not a property of risk analysis, but only a human valuation on the potential outcome of the predicted event. (Claycamp, 2006).

Communication is widely viewed as essential in executing risk management programs (Pidgeon, 2003). A risk that can be assessed and managed by “back of the envelope" approaches does not warrant exhaustive written analysis. However, other risks may require more rigorous analysis methods. However there is a danger that if the analytical technique appears quantitative because it translates expert judgment into risk rankings, it may communicate more certainty than is actually there. It has been recognized since at least 1957 that sophisticated risk analyses can miscommunicate the certainty of the assessment (Hassenzahl, 2006).

The methodology under development within the project represents a new approach to risk management. As such the developers are seeking from the very earliest stages to identify the most appropriate means to communicate the inherent uncertainty of the method to avoid miscommunication itself. This is perhaps the greatest challenge for the FAST – to identify credible failure scenarios that have minimal uncertainty.

Scenarios

When the world is highly unpredictable and we are working from a limited range of expectations, however, our expectations will frequently be proved wrong. Scenario planning offers a framework for developing more resilient conservation policies when faced with uncontrollable, irreducible uncertainty. A scenario in this context is an account of a plausible future. Scenario planning consists of using a few contrasting scenarios to explore the uncertainty surrounding the future consequences of a decision. Ideally, scenarios should be constructed by a diverse group of people for a single, stated purpose. Scenario planning can incorporate a variety of quantitative and qualitative information in the decision-making process. Often, consideration of this diverse information in a systemic way leads to better decisions. Furthermore, the participation of a diverse group of people in a systemic process of collecting, discussing, and analyzing scenarios builds shared understanding (Peterson, 2003).

Hidden risks that we can't name a priori maybe revealed by construction of scenarios. A scenario may be an especially important ingredient for the prospection process: postulating the intersection of unpredictable disruptive technologies, events, and conditions within aviation and the surprise influences from external domains. Scenarios can suggest unexpected uses of technology – plus attendant novel hazards and risks - not anticipated by the original designers.

Perceived Risk in Uncertain, Complex Futures

Risk and uncertainty are two concepts that are challenging to specify and employ in quality risk management systems. The generality of the concepts means that they are flexible enough to find application to a future timeframe of interest. The cost of this flexibility is that the concepts can be too vague and easily confused if they are not defined in context at the outset of a proposed methodology (Claycamp, 2006).

When contemplating a methodology to assess future risks, it must be kept in mind that the level of effort, rigor, and documentation of the assessment technique should be commensurate with the level of perceived risk (Claycamp, Perspective on Quality Risk Management of Pharmaceutical Quality, 2007). Within this perceived future risk there are four components of quality in aviation systems:

1. Component and system design,
2. Procedures for use of systems by humans,
3. Training of humans in proper procedures, and
4. Maintenance and sustainability of the systems.

Management of future risk, uncertainty, and predictability demands that practitioners link estimates of risks with appropriate variables and parameters to monitor that may permit qualitative or quantitative assessment of the three related concepts; risk, uncertainty, and predictability (Claycamp, Perspective on Quality Risk Management of Pharmaceutical Quality, 2007).

In some cases it may be necessary to devise surrogate measures of the risk since the foundation of aviation safety is to develop risk mitigations strategies at the earliest stages of design and procedures development. These surrogate measures may better communicate the future risk than more direct measures that are possibly harder to understand. Often the telltale signs of risk do not manifest themselves in actual exposure to, say fatal accident circumstances, but may be found in processes and decisions by maintenance personnel, weather predictions, training records, and host of other phenomena. As mentioned previously, it is critical to establish *what* parameters to manage to control risk.

Quality risk management must ultimately be based on:

- Scientific knowledge that can be linked back to the safety of passengers, crew, and property
- A level of effort, formality, and documentation within the safety management system that is commensurate with the level or risk (Claycamp, Perspective on Quality Risk Management of Pharmaceutical Quality, 2007).

As the aviation community looks into the future, key questions must be addressed within the risk control process:

- Does the risk exceed an acceptable level (eg, regulatory standards, action levels)?
- What steps might be taken to reduce or eliminate the remaining risks?
- What is the effectiveness of those risk countermeasures?
- What is an appropriate balance among risks, benefits, and resources to manage risks?
- Will new risks appear in the future as a result of present or planned management steps to control the identified risks?

- What is the net effect of risks, mitigations, and new hazards introduced by the mitigations – residual risks?

Risk is not easy to control in complex systems. Especially in aviation, risk derives from multiple competing objectives, stovepipe programs, an extended web of organizational and technical interrelationships that virtually defy analysis, and parallel activities intended to manage the same risk. This complexity will only increase in future operational settings. It is vital to determine the appropriate analytical tool for managing risk in such settings. Risk management tools can be organized from high-level, general to low-level, specific. Exemplar tools listed in descending order from high-level to low-level are shown below (Claycamp, Perspective on Quality Risk Management of Pharmaceutical Quality, 2007).

- Brainstorming or storming-forming-norming, SFN
- Preliminary Hazard Analysis capturing basic, high-level hazards
- Hierarchical holographic modeling, HHM
- Risk ranking and filtering, RRF
- Risk matrices, RM
- Failure modes and effects (criticality) analysis, FMEA and FMECA
- Variation risk management, VRM
- Root cause analysis, RCA
- Decision trees, DT
- Probabilistic risk analysis, PRA
- Event trees, ET
- Fault tree analysis, FTA

These tools provide capabilities for risk assessment, but it must be remembered that assessment is a different animal than management. Risk management includes decision(s) to either mitigate risk, accept existing risk (e.g., as “below a level of concern”), or even to maintain the status quo (“do nothing”). To effectively manage risk it has been observed that systems having built-in mechanisms and procedures for detecting both obvious and “weak signals” events that contribute to increasing the severity or probability of the risk have lower eventual risk outcomes (Claycamp, Perspective on Quality Risk Management of Pharmaceutical Quality, 2007).

Regardless of the method or technique used to manage future risk, two essential ingredients are necessary for insight and practicality; 1. a sufficiently broad picture of the future including contributing factors that users of the method might not naturally consider and 2. guarantees that key front-line personnel with knowledge of the hazard environment participate in the application of the method. Without them, any method no matter how theoretically robust will not yield practical results. That’s been the experience of the FAST.

Detection is critically important for managing risk. In addition, future risks must be characterized and emphasized in a way that affected stakeholders will stand up and take notice and not just dismiss expert opinion as being overly speculative. One could argue that the eventual outcome risk score should include a "detection factor" between 1.0 and zero; where zero represents a very high likelihood of detection. This factor would be in addition to a "strength of mitigation" factor having similar values; where zero implies very strong mitigation effects.

Risk not [just] a numbers game (Hubbard, 2009)

During the course of this project, the best we can do is to make educated guesses preparing for the most likely happenings that will make the biggest impact on the aviation system. Developing a risk map may be helpful in discussions about future risk with those managers responsible for achieving organizational objectives. It permits consideration of the most likely scenarios and their impact and allows for timely preparation so the organization can readily deal with events as they arrive.

There can be confusion, even among auditors and safety management system professional, about the exact meanings of the many types of "risk." Most of the confusion is clarified within an organization by simply agreeing on consistent definitions. But other times the confusion can be more serious, because it impedes the overall effectiveness of the risk assessment processes, or at its worst can provide misleading results. The Hubbard article examines the typical terms used in risk assessment processes, and helps auditors avoid one of the biggest risks of all, which is thinking that risk assessment is solely a mathematical exercise.

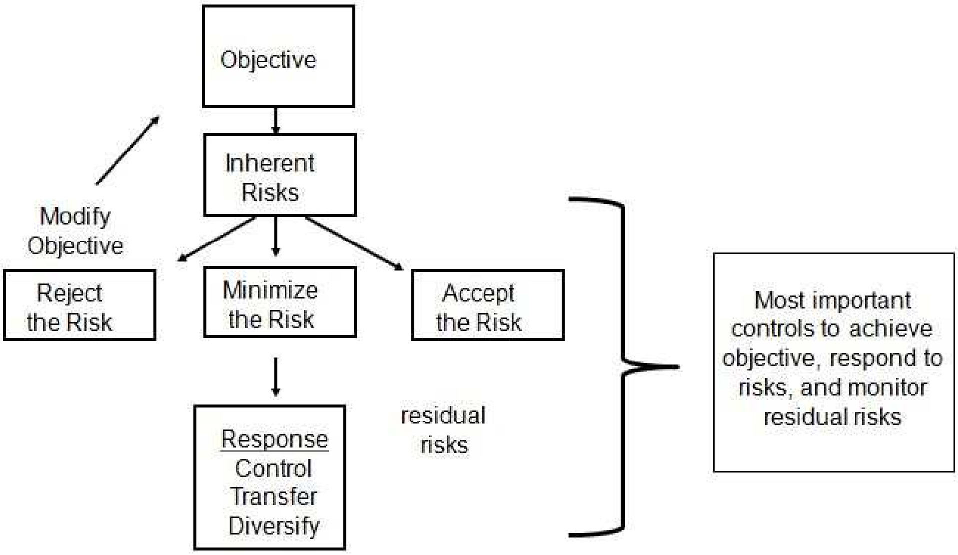
SMS auditors tend to base their auditing on an assessment of risks, and to focus on the most important objectives of the organization. This is known as risk-based auditing, and it applies to the selection of audits to perform. Auditors use Risk Factors to help determine which audits to perform each year, and weight these factors based on their importance.

However, regardless of the number of risk factors used or the weighting applied to each, it is impossible to predict, with certainty, which areas of an organization will need to be audited regardless of how we may define such a need. Similarly, while auditors do forecast the time an audit will require different auditors always forecast different (sometimes wildly different) time budgets for similar engagements. So, at best, deciding on the audits to perform each year, and the number of auditors needed to perform those audits is an educated guess. This is the first math game some departments engage in – by trying to select audits as a purely mathematical exercise rather than a decision based on discussions between the auditors, managers and the board. Those discussions are the valuable piece of the risk-based audit selection process, and being overly analytical can actually get in the way of good discussions.

Applying some twenty factors, each weighted differently and scored from 1 to 10, and then multiplied by a factor representing the anticipated length of the audit (retaining the decimal points) is a math game not worth playing! *Using five equally weighted Risk Factors, which all measure different aspects of risk, and using simple*

High, Medium, Low scores can provide all the analytical input needed to support the discussions of what to audit.

Risk events are measured in terms of impact and probability, and often Risk Maps are used to determine the importance of a potential risk event based on those two terms. Mapping is used to determine whether to accept or respond to the risk event. Again, this is better depicted in pictures. Below is an Inherent Risk Assessment. This identifies all the inherent risks that might impact achieving a particular organizational objective. Then based on the importance of each risk, management determines the action to take (e.g. change the objective to avoid or reject the risk; minimize the risk with a response; or accept the residual or remaining risk). Making an avoid/minimize/accept decision is the purpose of a risk map, shown below.



What is most critical in this risk map is deciding which are the most important controls needed to achieve the organizational objective, responding to the perceived highest risks, and monitoring the residual risks (the raindrops outside the umbrella!).

FAST Methodology Possible Outcomes

As the FAST methodology will reveal, *risk events are about the uncertain, complex futures, which cannot be predicted precisely*. If an event does occur, then maybe it is a problem to be solved and avoided in the future, but it is no longer a potential risk event.

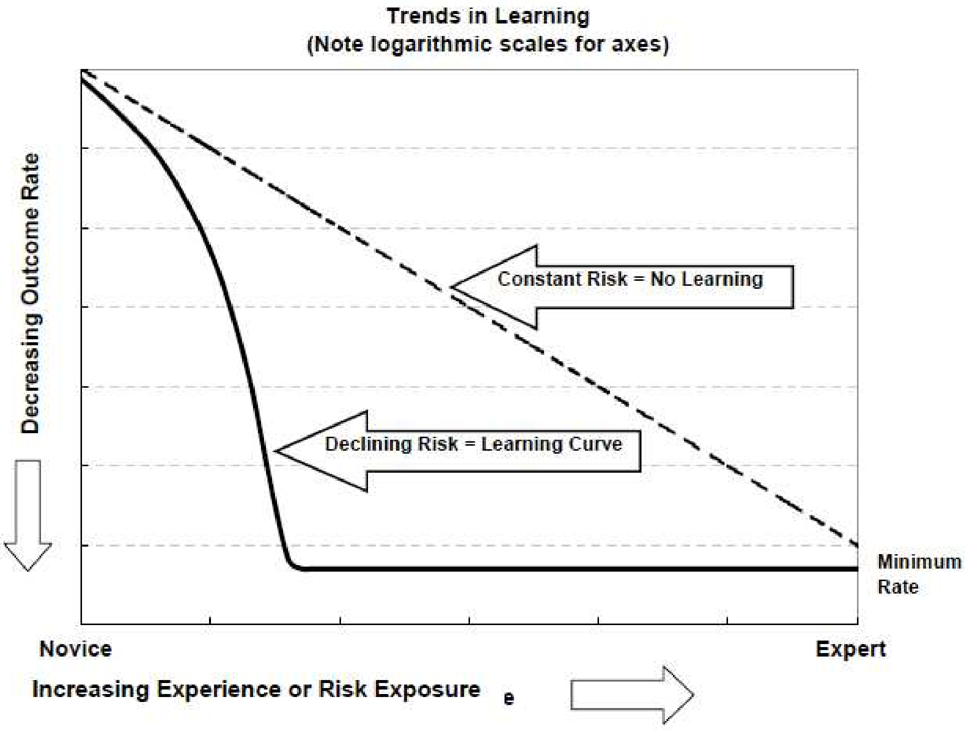
So, while we cannot accurately predict the future, we know there will be a future, so we had better be ready for whatever happens[1]. The economy will get better or worse or stay the same, but we don't know which. An event may happen or may not happen, at some unknown interval. At best we need to make educated guesses about those things, and prepare first for the most likely risks with the biggest potential impact recognizing that the major risks may be a moving target that changes over time. Ideally, the assessments will be a moving grid, i.e. biggest potential impacts moving with time. *The aviation community must prepare for the most common and most important things that could go wrong in future settings.* But, just as no one can be sure they know all the inherent risks, because risk is about the future, neither can anyone really know how likely the risks are to occur. Regardless of the time spent, we simply cannot identify all risks in advance. So, risk assessment is about being ready for the future, not trying to predict it. This is where the range of possible futures offered by the prospection process comes in.

Several major factors and useful measures that influence the prediction of risk and stability in financial systems, based on what we observe for all other systems with human involvement (Duffy, 2011). These factors must be considered in any predictive methodology developed by the FAST.

1. The Universal Learning Curve provides a comparative indication of trends;
2. The probability of failure/loss is a function of experience or risk exposure;
3. The relevant measure of failure is the rate of fatal aircraft accidents;
4. A relevant measure of experience and risk exposure may be the accumulated flight hours for a crew member;
5. Stable systems are learning systems that reduce complexity;
6. An absolute measure of risk and uncertainty is the Information Entropy, which reflects *what we know about what we do not know*;
7. Unique condition exists for systemic stability;
8. Repeat events are likely – the so-called "cosmic cycles of accidents" in which the people who remember the lessons learned from major accidents move on and the organizations do not consciously retain those lesson learned. Re-awareness maybe one of the biggest issue facing safety.
9. Existing systems are unstable unless learning is occurring; and
10. new systems are unstable during initial periods when experience is negligible.

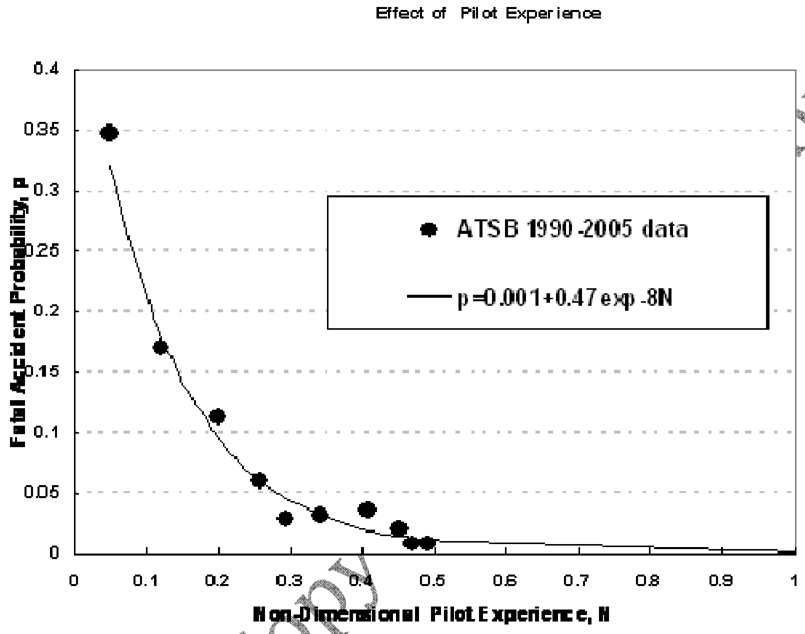
---

[1] The earlier a control or mitigation is implemented the cheaper it will be. For instance: there are still no certification requirements against cyber attack for Electronic Flight Bag installations, flight deck automation still not fully understood by pilots, effective training maybe a bigger obstacle than is currently believed, inadequate certification requirements for Unmanned Aerial Vehicles, absence of hard requirements for the integrated Air Ground Space System (AGS), and progress on SESAR/Next Gen is being questioned by some. As a result, OEM's and equipment suppliers cannot move forward.



The ULC and Constant Risk Lines; Failure rates with increasing experience and/or risk exposure - Used with Permission (Duffy, 2011)

In the aviation domain, fatal accident probability is directly correlated with pilot experience (Duffey, 2008). The following figure illustrates how much experience the pilot population had before dying in accidents. *The total number of pilot deaths observed and the probability of when the death occurs among all the deaths can be distributed to first order as decreasing exponentially with the increasing depth of experience as measured by pilot-time-on-type in any given interval (such as the 15-year period for which the data in the figure below was based).*



The exponential distribution with depth of experience of the probability of the death of commercial pilots - Used with Permission (Duffey, 2008)

The common features of major accidents fitting into the rare event category, or as they have been called - the Seven Themes – that cover the aspects of causation, rationalization, retribution, and prevention are all too familiar:

First, these major losses, failures and outcomes all share the same very same and very human Four Phases or warning signs:

1. Unfolding of the precursors and initiating circumstances;
2. Confluence of events and circumstances in unexpected ways;
3. Escalation where the unrecognized unknowingly happens; and, afterwards,
4. Denial and blame shift before final acceptance.

Second, as always, these incidents all involved humans, were not expected but clearly understandable as due to management emphasis on production and profit rather than safety and risk, from gaps in the operating and management requirements, and from lax inspection and inadequate regulations.

Third, these events have all caused a spate of media coverage, retroactive soul-searching, "culture" studies and surveys, regulation review, revisions to laws, guidelines and procedures, new limits and reporting legislation, which all echo perfectly the present emphasis on limits to the "bonus culture" and "risk taking" that are or were endemic in certain financial circles.

Fourth, the failures were so-called "rare events" and involved obvious dynamic human lapses and errors, and as such do not follow the usual statistical rules and laws that govern large quasi-static samples. Static samples, or the multitudinous outcome distributions (like normal, lognormal and Weibull) that dominate conventional statistical thinking, but clearly require analysis and understanding of the role of human learning, experience and skill in making mistakes and taking decisions.

Fifth, these events all involve humans operating inside and/or with a system, and contain real information about what we know about what we do not know, being the unexpected, the unknown, the rare and low occurrence rate events, with large consequences and highlighting our own inadequate predictive capability, so that to predict we must use Bayesian-type likelihood estimation.

Sixth, there is the learning paradox, that *if we do not learn we have more risk, but to learn we must perversely have the very events we seek to avoid*, which also have a large and finite risk of re-occurrence; and we ultimately have more risk from events we have not had the chance to learn about, being the unknown, rare or unexpected.

Seventh, these events were all preventable but only afterwards - with 20/20 hindsight soul-searching and sometimes massive inquiries reveal what was so obvious time after time; the same human fallibilities, performance lapses, supervisory and inspections gaps, bad habits, inadequate rules and legislation, management failures, and risk taking behaviors that all should have been and were self-evident, and were uncorrected.

We claim to learn from these each time, perhaps introducing corrective actions and lessons learned, thus hopefully reducing the outcome rate or the chance of re-occurrence. All of these aspects were also evident in the financial failure of 2008, in the collapse of major financial institutions and banks. These rare events are worth examining further as to their repeat frequency and market failure probability: recessions have happened before but 2008 was supposedly somewhat different, as it was reportedly due to unbridled systemic risk, and uncontrolled systemic failure in credit and real estate sectors. This failure of risk management in financial markets led to key analysis, extending the observations, new thinking and methods developed for understanding other technological systems to the prediction and management of so-called "systemic risk" in financial markets and transactions. We treat and analyze these financial entities as "systems" which function and "behave" by learning from experience just like any other system, where we observe the external outcomes and failures due to the unobserved internal activities, management decisions, errors and risks taken (Duffy, 2011).

Summary of The Risk Landscape of the Future

For several years, the Future Aviation Safety Team has postulated that much insight could be gained in understanding future hazard exposure and risk by looking to the insurance and actuarial industries. Several documents and organizations have recently been identified that reflect important thinking not only about risk in general but also the public perception of risk acceptance. The following section contains excerpts and quotes from a 2004 study report from the major European reinsurance company, Swiss RE, entitled “The risk landscape of the future.” (Brauner, 2004)

The FAST employs a method of anticipating emerging risks that is becoming increasingly popular with governments called horizon scanning. Horizon scanning is “a policy tool that systematically gathers a broad range of information about emerging issues and trends in an organization’s political, economic, social, technological, or ecological environment. It is also used as a synonym for a variety of so-called ‘foresight activities’ that aim to develop the capabilities of organizations to deal better with an uncertain and complex future”(Habbeger, 2009). This tool does not specifically focus on risks, but can be used to improve the anticipation of emerging risks and opportunities (Emerging Risks: Sources, drivers, and governance issues, 2010).

The Swiss Reinsurance Company (Swiss RE, Zurich, Switzerland) has huge vested interests in the insurability of future risks. They refer to the term “risk landscape” to the “totality of risks faced by a specific community, such as a nation, a business enterprise or a family.” It behooves the aviation community to borrow concepts and recommendations from such an entity whose major focus in managing the economic consequences of future risk.

Three major phenomena characterize the risk landscape of the future:

1. Continuing acceleration of change,
2. Range of possible consequences is broader and more severe at the extreme end, and
3. Increasing uncertainty is making risks less capable of analytical calculation.

Furthermore, today’s technology and business networks disseminate innovation faster and over wider areas. Historical models of technology influence led to gradual change and local damage. However, the rapid dissemination of technology and its associated complexity means that hidden risks may trigger accumulation of widespread losses.

If the dimensions of such technology dispersion are not known or understood, risk financing is virtually impossible. The remaining residual risks may not be discovered until a loss event occurs.

Risk assessment is knowledge of possible losses

More than at any other time in history, present-day risks are multivariate. For this reason, predictions about the likelihood of multi-causal losses depend on a sound understanding of cause-and-effect relationships in the aviation industry or on a detailed loss history (harder to come by with fewer and fewer accidents occurring). The future risks in aviation do not share either of these characteristics.

Much effort is currently expended attempting to drive down the probability of occurrence of adverse events. However, as will be discussed later, there is an undeniable trend toward greater severity in accidents and greater visibility to the public – the perception phenomenon.

Warn earlier, react faster

Insurers can function as an early warning system because – by their very nature – they may have more loss data than any other institution. In the aviation sector, airlines and manufacturers - if the airlines proactively share operational data with them – also can act as early warning systems because of the wealth of service difficulty information that is accumulating in ever greater amounts.

Swiss RE has assembled expert teams to address all aspects of risk for which they have an economic stake. They have discovered that adopting an interdisciplinary approach to risk analysis allows them to discover the intricate contours of the risk landscape. They typically hold workshops with experts from multiple conceivable fields in an effort to uncover new risks or changes to existing ones. This multi-disciplinary analysis team model will be essential for management of future risk in aviation.

The near-term future can be known with greater certainty. The distant future is only dimly definable. Because of this inability to predict the distant future with any degree of certainty, it is of utmost importance to *identify the drivers and mechanisms of change*, because those twin phenomena will determine the hazard and risk vectors in the coming months and years.

In the absence of the capabilities to detect early signals of risk, there is a large chance that the risks will materialize with maximum impact, given that no-one saw them coming in time to undertake prevention or mitigation efforts.

Of particular importance are (Emerging Risks: Sources, drivers, and governance issues, 2010):

- detecting “hidden” concentrations or accumulations of exposures whose size, scale and impact could have a material adverse effect;

- complex and “opaque” products or services which are understood by only a few experts;
- looking for discontinuities or tipping points which indicate either unclear ”rules of the game” or a likely change;
- lengthy dependent “chains” of any type, since they are only as strong as the “weakest link”;
- more scenario analysis and “stress testing” outside the range of “business as usual”;
- imagining unintended consequences of public policy and regulation, and looking for connections which could arise between “seemingly unrelated” trends; and
- measuring trends in diverging views between groups on critical issues such as automation implementation, flight crew training and demographics, and the changing regulatory landscape, as such diverging views can be precursors to emerging risks or can complicate efforts at taking precautionary or mitigation measures.

Future risks are in the present

Experience in aviation and in other sectors shows that the initial phases of innovation cycles are the most risky because humans and the institutions made up of them must learn to cope with the new hazards introduced by the innovations. Duffy makes this same point earlier in this paper.

The increased speed of technology dissemination, societal mobility, and global shipping creates vulnerabilities across many domains. Computer viruses need just hours to propagate; biological pathogens, days; components containing manufacturing defects, a few days for shipment and installation.

An important trend bearing on the public perception of risk is the increase in numbers of natural and manmade disasters since 1970.

The number of catastrophes between 1970 and 2003 (Brauner, 2004)

In contrast, although the number of commercial aircraft flying hours increased by a factor of ten between 1965 and 2002, the number of serious accidents per million departures fell dramatically (The Boeing Company, 2003). Counterbalancing this favorable trend is the phenomenon mentioned previously; the trend toward accidents with greater severity. The number of fatalities per accident has more than doubled from 12.5 to 29.2 since 1945. Large aircraft being employed in certain markets increase the potential severity and visibility of accidents.

Similarly, the introduction of high-speed trains has multiplied the possible consequences since a doubling of speed results in a quadrupling of energy that is released in the event of an impact.

Consequences may be qualitative as well as quantitative. In the course of 1977, the set of air transport accidents that led to a loss of 1605 souls was completely overshadowed by the Tenerife runway collision of two 747 aircraft with a total of 583 deaths (Aviation Safety Network, 1977).

On September 21, 2001, a chemical factory in Toulouse, France, was the scene of one of the most devastating explosions in the history of the chemical industry. The detonation created a crater 10 meters deep and 50 meters wide on the factor premises. Window panes within a radius of five kilometers were shattered. Thirty people were killed and more than 2,400 injured.

Had it not been for the events in New York and Washington DC only a few days before, this chemical disaster would certainly have generated extensive press coverage and discussion of the safety of the chemical industry in Europe. Yet this explosion was not even registered by many international media outlets.

These illustrations indicate that consequences (severity) and probabilities must be considered separately for a complete description of the risk landscape. Higher frequency risks involving low to moderate loss may not require systemic risk management. However, risks whose consequences are extreme may create an existential threat despite their low probability of occurrence.

Risks are [just] a matter of definition

Risk implies possible loss. Value perceptions also determine the distribution of risk or loss burdens within society. Physical and mental pain is assigned only a low monetary value. In continental Europe, liability claims are largely limited to compensation for medical expenses and loss of income. In contrast, the Anglo-Saxon legal system provides for punitive damages, which may grant satisfaction to the injured party far in excess of any measureable losses.

From the perspective of practical risk management, it is vital to recognize that the increasing interdependence of socio-technical systems is triggering new risks. Modern science sees end effects as the result of the complex interplay of many individual factors and circumstances, none of which is the sole cause in the classical sense, but just makes a greater or lesser contribution to the total effect. In the recent FAST report on the vulnerabilities of key Safety Enhancements that have been recommended for implementation by the Commercial Aviation Safety Team, a key finding was that "Unusual performance and unusual circumstances are almost always the result of unanticipated interactions of multiple phenomena that, if they were to occur individually, are relatively benign." (Smith, 2011)

The aviation community must guard against attributing fatal accidents to simplistic, single-variable causes.

The legal system compounds this problem. Under current law, evidence identifying possible aggravating factors is not strong enough to enforce liability claims. There must be unambiguous proof that a particular phenomenon was the actual cause of the illness or accident.

The "common sense" of democratic societies determines what is considered to be true and real. Risk acceptance is not only a question of objective measurement, but of individual and collective perceptions of risk. No civilian technology kills and maims more people or contributes more noise and pollutants to the environment than automotive transportation. And yet automobile travel continues to be widely accepted. Experts themselves often fail to agree on new risks; risk evaluation is becoming less of a question of what to believe than whom to believe.

In order to form a reliable picture of the future risk landscape in aviation, it is not enough to enquire about objectively measureable, rationally comprehensible risk factors. One must understand the factors driving the future risk landscape: changes in needs, interests, visions, hopes, and fears.

For simple, linear systems, loss events can be precisely predicted if all cause-and-effect relationships are known and all variables can be measured with sufficient accuracy. That is why fatigue life of certain aircraft components can be accurately predicted.

For complex systems, however, accurate predictions are extremely difficult. No one can predicts where and in what context the next aviation accident will occur. Yet it is possible to estimate the risk, or average frequency and severity of aviation accidents over the next year.

The real difficulty of risk assessment is not complexity per se, but in the accelerated rate of change of complex systems. The fast the risk landscape changes, the more risks remain largely unidentified by current methods or become incalculable. It is no longer just individual parameters but entire systems that are changing with increasing speed. For this reason, the potential for unpleasant surprises becomes greater.

Thus it is not that future risks cannot be assessed at all, but merely that they cannot be assessed definitively and conclusively. Only if we subject new technologies, operational concepts, and business/regulatory practices to scrutiny at the earliest stages will we be able to recognize undesirable tendencies as soon as they appear. The FAST has termed these phenomena, “Watch Items.”

Works Cited

(2011, June 22). From Risk Management: http://www.safetyinfo.com/Safety/Risk%20Management.htm

Alain Desroches, D. B. (2009). *L'analyse préliminaire des risques.* Paris: Lavoisier.

Aviation Safety Network. (1977). From Fatal Airline Hull Loss Accidents: http://aviation-safety.net/statistics/period/stats.php?cat=A1

Brauner, C. (2004). *The risk landscape of the future: risk perception.* Swiss Reinsurance Company.

Claycamp, H. G. (2007). Perspective on Quality Risk Management of Pharmaceutical Quality. *Drug Information Journal , 41*, 353-367.

Claycamp, H. G. (2006). Risk, Uncertainty, and Process Analytical Technology. *The Journal of Process Analytical Technology , 3* (2), 8-12.

Decision Making Paradox. (2011, January 1). From http://en.wikipedia.org/wiki/Decision_making_paradox

Duffey, R. B. (2008). *Managing Risk: The Human Element.* John Wiley & Sons, Ltd.

Duffy, R. B. (2011). *THE QUANTIFICATION OF SYSTEMIC RISK AND STABILITY: NEW METHODS AND MEASURES.* Working Paper, NATIONAL BUREAU OF ECONOMIC RESEARCH.

Edmonds, A. P. (2011, June 27). *The Chaos theoretic argument that undermines Climate Change modelling*. From http://wattsupwiththat.com/2011/06/13/the-chaos-theoretic-argument-that-undermines-climate-change-modelling/

FAA Order, 8. (2004, December). *GUIDANCE System Safety Management Program / Section 2.* From http://fast.faa.gov/toolsets/SafMgmt/section2.htm

Gilbert, D. (2006). *Stumbling on Happiness.* New York: Knopf.

Hammond, J. K. (1999). *Smart Choices: A Practical Guide to Making Better Life Decisions.* New York: Broadway Books.

Hassenzahl, D. (2006). Implications of excessive precision for risk assessments: lessons from the past four decades. *Risk Analysis , 26*, 265-276.

Hubbard, L. C. (2009, February). Skip the Numbers: Assessing Risk is not a Math Game! .

Kahneman, D. S. (Ed.). (1982). *Judgment Under Uncertainty: Heuristics and Biases.* Cambridge, UK: Cambridge University Press.

Ladkin, P. B. (2008). *Definitions for Safety Engineering.* Causalis Limited and University of Bielefeld.

Leveson, N. (1995). *Safeware: System safety and Computers.* New York, NY: Addison-Wesley Publishing Company.

List of cognitive biases. (2011, June 30). Retrieved July 5, 2011 from http://en.wikipedia.org/wiki/List_of_cognitive_biases

Petersen, J. L. (2001). Anticipating Global Futures. The Arlington Insittute.

Petersen, J. L. (1999). *Out of the Blue - How to Anticipate Big Future Surprises.* Madison Books.

Peterson, G. D. (2003). Scenario Planning: a Tool for Conservation in an Uncertain World. *Conservation Biology , 17* (2), 358-366.

Pidgeon, N. K. (Ed.). (2003). *The Social Amplificiation of Risk.* Cambridge, UK: Cambridge University Press.

Shermer, M. (2011, July 5). The Believing Brain: Why Science Is the Only Way Out of Belief-Dependent Realism. *Scientific American Magazine* , p. ?

Smith, B. E. (2011). *A Saftey Vulnerability Assessment of Select CAST Safety Enhancements - Final Report.* Future Aviation Safety Team.

The Boeing Company. (2003). *2002 Statistical Summary.* www.boeing.com.

Voros, J. (2009). Morphological prospection: Profiling the shapes of things to come. *Foresight , 11* (8), pp. 4-20.

Walker, V. (1998). Risk regulation and the "faces" of uncertainty. *Risk, Health, Safety and Environment , 9*, 27-38.

APPENDIX – Risk Matrices in use by the Aviation Industry

Severity Level / Probability Level	Level A	Level B	Level C	Level D	Level E
Level 5	5A - EH	5B - EH	5C - H	5D - M	No Safety Effect
Level 4	4A - EH	4B - H	4C - M	4D - L	
Level 3	3A - H	3B - M	3C - L	3D - L	
Level 2	2A - M	2B - L	2C - L	2D - L	
Level 1	1A - L	1B - L	1E - L	1D - L	

A.1 AIRCRAFT DESIGN RISK MATRIX DEFINITIONS

HAZARD SEVERITY LEVEL	HAZARD CLASSIFICATION DEFINITION	EFFECT ON AIRCRAFT AND OCCUPANTS	CAR525.1309 FAR25.1309 CS25.1309 Requirement	PROBABILITY CLASSIFICATION DEFINITION	Acceptable HAZARD PROB. LEVEL
A	Failure conditions, which would prevent continued safe flight and landing.	Multiple deaths, usually with loss of aircraft.	Catastrophic Extremely Improbable $P \leq 1 \times 10^{-9}$	Individual item – so unlikely it can be assumed it will not occur in the life of the aircraft or system Fleet or inventory – unlikely to occur in the life of the aircraft or system Individual airman – so unlikely it can be assumed it will not occur in a career. All airmen exposed – occurs very rarely.	**1**
B	Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with normal operating conditions.	Large reduction in safety margins; crew extended because of workload or environmental conditions; serious injury or death of small number of occupants; substantial aircraft damage.	Hazardous Extremely Remote $1 \times 10^{-9} < P \leq 1 \times 10^{-7}$	Individual item – unlikely but could occur in the life of the aircraft or system Fleet or inventory – unlikely but could occur in the life of the aircraft or system Individual airman – unlikely but could occur in a career. All airmen exposed – occurs seldom	**2**
C	Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions.	Significant reduction in safety margins; difficult for crew to cope with adverse conditions; minor occupant injuries; major aircraft damage.	Major Remote $1 \times 10^{-7} < P \leq 1 \times 10^{-5}$	Individual item – will occur in the life of the aircraft or system Fleet or inventory – occurs several times in the life of the aircraft or system Individual airman – will occur in career All airmen exposed – occurs	**3**

				sporadically	
D	Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that is well within their capabilities.	Slight reduction in safety margin; physical discomfort of occupants; minor or no aircraft damage.	Minor Probable $1 \text{ X } 10^{-5} < P \leq 1 \text{ X } 10^{-3}$	Individual item - occurs several times in the operational life of each airplane or system Fleet or inventory – occurs several times in the operational life of the airplane or system Individual airman – occurs several times in career All airmen exposed – occurs several times	**4**
E	No Safety Effect	No significant reduction in safety with regard to Aircraft, crew or passengers during operation	Frequent $P > 1 \text{ X } 10^{-3}$	Individual item – occurs often in the life of the aircraft or system Fleet or inventory – continuously experienced Individual airman – occurs often in career All airmen exposed – continuously experienced	**5**

1

A.2 FLIGHT OPERATIONS RISK MATRIX DEFINITIONS

HAZARD SEVERITY LEVEL	HAZARD Severity	HAZARD CLASSIFICATION DEFINITION	Acceptable Probability of Occurrence	PROBABILITY CLASSIFICATION DEFINITION	Acceptable HAZARD PROB. LEVEL
A	Catastrophic	Death or Hull Loss	Extremely improbable	So unlikely it can be assumed it will not occur in the operational life. Example ≥ 1000000000 departures	**1**
B	Hazardous (Critical)	Severe Injury, Severe Occupational Illness or Substantial System Damage / Loss	Extremely Remote	Unlikely but could occur in the operational life. Example1000001 to 1000000000 departures	**2**
C	Major (Marginal)	Minor Injury, Minor Occupational Illness or Minor System / Sub-System Damage	Remote	Will occur sometime in the operational life. Example 100001 to 1000000 departures	**3**
D	Minor (Negligible)	Less than minor injury or illness or no system loss or damage	Probable	Occurs several times in the operational life. Example 1001 to 100000 departures	**4**
E	No Safety Effect	Negligible effect on safety	Frequent	Occurs frequently or continuously. Example 1 to 1000 departures	**5**

A.3 ORGANIZATIONAL / SRS RISK MATRIX DEFINITIONS

HAZARD SEVERITY LEVEL	HAZARD SEVERITY	HAZARD CLASSIFICATION DEFINITION	ACCEPTABLE Probability of Occurrence	PROBABILITY CLASSIFICATION DEFINITION	ACCEPTABLE HAZARD PROB. LEVEL
A	Catastrophic	Conditions that could result in errors causing loss of life or severe damage to equipment while operating or servicing the product	Extremely Improbable (P≤1E-9)	So unlikely it can be assumed it will not occur in the product life	**1**
B	Hazardous	Conditions that could result in injury or damage to equipment while operating or servicing the product	Extremely Remote (P≤1E-7)	Unlikely but could occur	**2**
C	Major	Conditions that could degrade the safe operation or cause minor damage to the product	Remote (P≤1E-5)	Will occur occasionally	**3**
D	Minor	Conditions that would affect the normal operation resulting in nuisance and a very small degradation in safety	Probable (P≤1E-3)	Occurs several times (monthly event)	**4**
E	No Safety Effect	No Effect on product or services safety	Frequent (P>1E-3)	Occurs often (weekly or daily event)	**5**

A.4 MANUFACTURING / AMO RISK MATRIX DEFINITIONS

HAZARD SEVERITY LEVEL	HAZARD Severity	HAZARD CLASSIFICATION DEFINITION	Acceptable Probability of Occurrence	PROBABILITY CLASSIFICATION DEFINITION	Acceptable HAZARD PROB. LEVEL
A	Catastrophic	Failure conditions that would affect PCCN1 components or Structures.	Extremely improbable	So unlikely it can be assumed it will not occur in the production life of the aircraft model	**1**
B	Hazardous	Failure conditions that would affect PCCN 2 Components or Structures	Extremely Remote	Unlikely but could occur in the production life of the aircraft model	**2**
C	Major	Failure conditions that would affect PCCN 3 Components or Secondary Structures	Remote	Will occur in the production life of the aircraft model	**3**
D	Minor	Failure conditions that would affect the normal operation resulting in the use of backup systems/secondary structure	Probable	Occurs several times in the production line (monthly event)	**4**
E	No Safety Effect	Negligible affect on safety	Frequent	Occurs often in the production line (weekly or daily event)	**5**