Methodology to Assess Future Risks

European Aviation Safety Plan (EASp)

Action EME 1.1 of the European Aviation Safety Plan (EASp)

This is the final deliverable of Action EME1.1 "Method to Asses Future Risks" of the EASp 2011-2014, page 38 of 51.

Action EME1.1 was allocated to EASA and performed together with the Future Aviation Safety Team (FAST), a team associated to the European Commercial Aviation Safety Team (ECAST) and to the US Commercial Aviation Safety Team (CAST).

> The EASp EME1.1 Methodology allows addressing in a practical manner many of the intrinsic difficulties characterising Prospective Safety and the assessment of future risks. It consists of introducing a switch of perspective from assessing future risks to ***safety assessing an appropriately scoped future system in its future context***, using an ***scenario-based approach*** *and an* ***enriched Safety Assessment methodology***.

The method offers practical guidance on conducting future-oriented project studies and the collection of relevant information using expert judgment, a suggested questionnaire, and scenario development processes.

1. A Prospective Approach

To be effective a prospective approach should combine the following approaches[1]:

- Look forward, e.g. through forecasting, trend analysis, gaming and scenarios, futurist writing, etc.
- Look across, e.g. through systemic thinking.
- Look backwards, through historical analogy, previous future-oriented studies, trend, analysis, etc. *History is important*, although it shouldn't be the sole basis for the identification and analysis of future risks.

The major advantages of a prospection-based approach include:

- It helps "build" the future despite uncertain predictive abilities;
- It offers a global/systemic approach (considering multiple perspectives & multiple disciplines);

[1] *Technical Report on a Foresight Training Course*, Editors: Cristiano Cagnin and Fabiana Scapolo, European Commission Joint Research Center, PUBSY ID - EUR 22737 EN.

- It combines qualitative & quantitative dimensions ;
- It takes into account ruptures; acknowledging the acceleration of social, technological and economic changes, etc.

Prospection should in particular identify disruptive technologies, events, and conditions within aviation, some being hard or impossible to predict, postulate surprise influences from external domains not intuitively expected to be the sources of hazards and risks, and suggest unexpected uses of technology not anticipated by the original designers.

To address such difficulties, the methodology described in this document introduces a switch of perspective from Assessing future risks to ***Safety Assessing an appropriately scoped future system in its future context***, using a **scenario-based approach** and an ***enriched Safety Assessment methodology***.

2. The Methodology

2.1. A Scenario-based Approach

One major difficulty with the assessment of future risks is to predict the future system with enough certainty and provide a good, complete and trustable description of the future.

The future can never be entirely predicted. However *certain changes are likely to happen*, such as the introduction of 4D trajectory management and System Wide Information Management (SWIM), for instance. These 'solid' elements can then be combined with less certain elements (e.g. demographics, fuel price, etc.) to form various *scenarios*.

Each scenario describes a possible future.

The following four stage approach is suggested:

Step 1 – Identify and describe the most likely scenarios defining the change or system to be safety assessed. The minimum number of scenarios to be considered is obviously one.

Guidance is provided in Appendix 1: Guidelines for Conducting a Prospective Workshop (optional) as an Aid to Scenario Development and in Appendix 2: Scenario Development Aids and Analysis Methods.

Step 2 – Assess the likelihood of the different scenarios, *adding a batch for "All other Scenarios not Considered"*, so to address entire range of uncertainty Indeed, *the actual future (system), which is unknown, can only be one as described in these scenarios or different from these: this way, the entire range of uncertainty is covered.*

Step 3 - All scenarios are safety assessed *as if they were going to occur as described,* using the standard Safety Assessment methodology described in Section 2.2 or preferably the augmented version described in Section 2.3.

Step 4 - Weight the results of the safety assessments depending on scenario likelihood.

2.2. Safety Assessment: Standard Version

Several references define the Safety Assessment methodology. For instance, the FAA/EUROCONTROL ATM Safety Techniques and Toolbox Safety Action Plan-15 summarises the basics of Safety Assessment (a standard approach, here applied to changes to an ATM system) as follows:

> "Safety assessment methodology is usually focused on ensuring that new proposed changes do not increase risk from a safety perspective. This means that all possible impacts of a new operation or system should be assessed, and their combined risks determined. These potential impacts can be intended (e.g. reducing separation minima, and therefore bringing aircraft closer together), or unintended (e.g. introducing data-link technology, which can have indirect safety impacts such as reducing the risk of call-sign confusions, but possibly introducing new errors such as up-linking messages to the wrong aircraft). Initially, a safety assessment considers the proposed operation or system definition (often called the Operational Concept), and analyses how it could impact matters, for the better and/or for worse, with respect to safety. This analysis involves considering the scope of the assessment (affecting how far the analysis is taken particularly in terms of interactions with other system elements), and then identifying all possible hazards and the severity of their consequences. The analyst then determines how probable these failures are, as well as how likely the system is to recover form such failures. This culminates in an overall risk estimate for the system." (page 7 of EUROCONTROL reference)

Note: Given the extraordinary and increasing complexity of the future aviation environment, it is not realistic to expect that all possible impacts can be uncovered and assessed. Human agents exist in the aviation system to deal with the unexpected and unanticipated. Using concepts and methods described in this document, one may be able to uncover ways in which future concepts of operations and particular technologies may make such human intervention awkward or ineffective. When parts of future systems are tightly coupled, or lack slack to minimise errors, problems that arise tend to exacerbate and may even be made more complicated rather than be solved by operator intervention[2]. The note is expanded in the Section 4 Limitations.

A standard Safety Assessment process consists of eight sequential stages[3]. The eight stages of the process are describes below:

Safety Assessment is classically defined as a 8-stage process:

Before the change is introduced or the System is implemented:

Stage 1 – Scope the System and the Assessment

[2] *Employing Adaptive Structuring as Cognitive Decision Aid in High Reliability Organisations*, Karlene Roberts, Kuo Frank Yu, Vinit Desai, Peter Madsen. The Oxford Handbook of Organisational Decision Making, Oxford University Press, 2009.

[3] A consensus generic Safety Assessment process from the FAA/EUROCONTROL AP-15 Toolbox report.

Stage 2 – Describe/Model the System and Nominal Operations

Stage 3 – Identify Hazards

Stage 4 – Combine Hazards into a Risk Framework

Stage 5 – Assess and Evaluate Risks

Stage 6 - Identify potential Risk Controls (barriers) and Reassess the Residual Risk until Acceptable or As Low as Reasonably Practicable (ALARP)

The ALARP concept is defined and illustrated in Appendix 3. The ALARP philosophy leaves open the possibility that a particular change or control may *not* be pursued because it provides only a marginal risk reduction relative to the implementation cost.

After the change is introduced or the System is implemented:

Stage 7 – Safety Monitoring and Verification

Assess actual risk, confirm actual risk is acceptable, ALARP or reducing, and introduce additional risk controls (barriers) as necessary

Stage 8 – Organisational Learning and Process Improvement

Learn through feedback and take process-improvement action as necessary though the application of Safety Management Systems

Appendix 4 provides a list of methods[4] usable for Stages 1-8. It focuses on the particular risk assessment techniques applicable to future systems identified by the FAST within the EASp EME1.1 Project.

2.2 Safety Assessment: Augmented Version

The augmented version described below consists of enriching Stages 1 to 6 by better accounting for the environment of the future as the system being assessed for safety performance.

Two enrichment options are proposed: one based on the major changes affecting the future aviation system described in the so-called FAST Areas of Change (AoCs), and a second based on visions of the future, programmes and plans, research agendas and other prospective documents.

[4] The user is expected to be knowledgeable in the selection of suitable methods and techniques for each of the stages. The specific methods available to address each stage of the process will be practical only if the users of the tools have experience in their application.

It is suggested to use these sources to better specify and account the future context in which the future system to be assessed will operate.

2.2.1 Using the FAST "Areas of Change"

The so-called FAST "Areas of Change" have been identified and are maintained by the FAST. The AoCs are generic descriptions of the major changes affecting the aviation system in the years to come.

Select the AoCs relevant to the time horizon considered in the Safety Assessment:

> The AoCs to be considered for the Safety Assessment shall correspond to the time horizon being considered.

Enrich the Hazards Identification stage

Also called "Areas of Change Analysis Method for Identification of Future Hazards", the FAST Method is a "Prognostic" or "Predictive" method aimed at discovering future hazards arising as a consequence of future changes introduced inside or outside the global aviation system.

The FAST Method published in the section Application of the SKYbrary FAST web-page provides one structured approach to enrich Hazard Identification.

Enrich the Analysis of Hazards and Risks

The approach basically consists of answering the following question: *How do the Areas of Change, in isolation or in combination, introduce or affect the hazards and risks?*

More precisely, the approach consists of *identifying hazards generated by interactions between and among AoCs* that could adversely impact the safety characteristics of the future system being assessed. A fundamental premise of the FAST Method is that interactions and overlaps/gaps among the system to be assessed and the FAST AoCs are the most likely catalysts for revealing and understanding future hazards.

Enrich the Analysis of Risk Controls

The AoCs can also affect the efficacy of the risk controls (barriers). Therefore it is recommended to also use AoCs to enrich the analysis of risk controls.

The fundamental approach consists of answering the following question: *How do the Areas of [future] Change, in isolation or in combination, affect the robustness or resilience of the risk controls (barriers) being considered?*

More precisely, the approach consists of examining *how the efficacy of the risk controls (barriers) might be modified when interacting with the AoCs*.

A key aspect of this step is evaluating potential effect of the FAST AoCs on the efficacy of proposed risk controls (barriers), considering the AoCs deemed relevant to the system to be assessed:

- What new risk controls may be required?
- Does any new (or existing) risk control affect multiple hazards? If so, which ones and how (increasing or decreasing likelihood/severity of risk)?
- How do AoCs affect the nature of risk controls (barriers)? Risk controls must take into account the future context set by the AoCs.
- How do AoCs affect the efficacy and cost of risk controls? (Effectiveness and costs, and as a result efficiency of the mitigations, may be affected.)
- How do AoCs affect the effect of risk controls over time? (Temporal pattern of effects can also be affected.)
- What changes need to be made to the new (or existing) risk controls as a result of the AoCs?

2.2.2 Using Reference Prospective Documents

Several visions of the future, programmes and plans, research agendas and other prospective documents are produced by several stakeholders who shape or design the future, such as the European Commission and ACARE, EUROCONTROL, SES and SESAR, NextGen, the FAA, NASA, aircraft and equipment manufacturers, research organisations, academia, associations, etc.

These documents, plans and programmes are used to orient, drive or support the design and implementation of the future aviation system or of sub-systems, ranging from the global ATM system to an aircraft or technology, at different time horizons.

An example list of prospective documents is provided in Appendix 5.

It is suggested that such reference documents be used for Safety Assessment in a manner similar to the Areas of Changes, i.e. to enrich the Hazards Identification and Risk Assessment and Analysis of Risk Controls (barriers) stages.

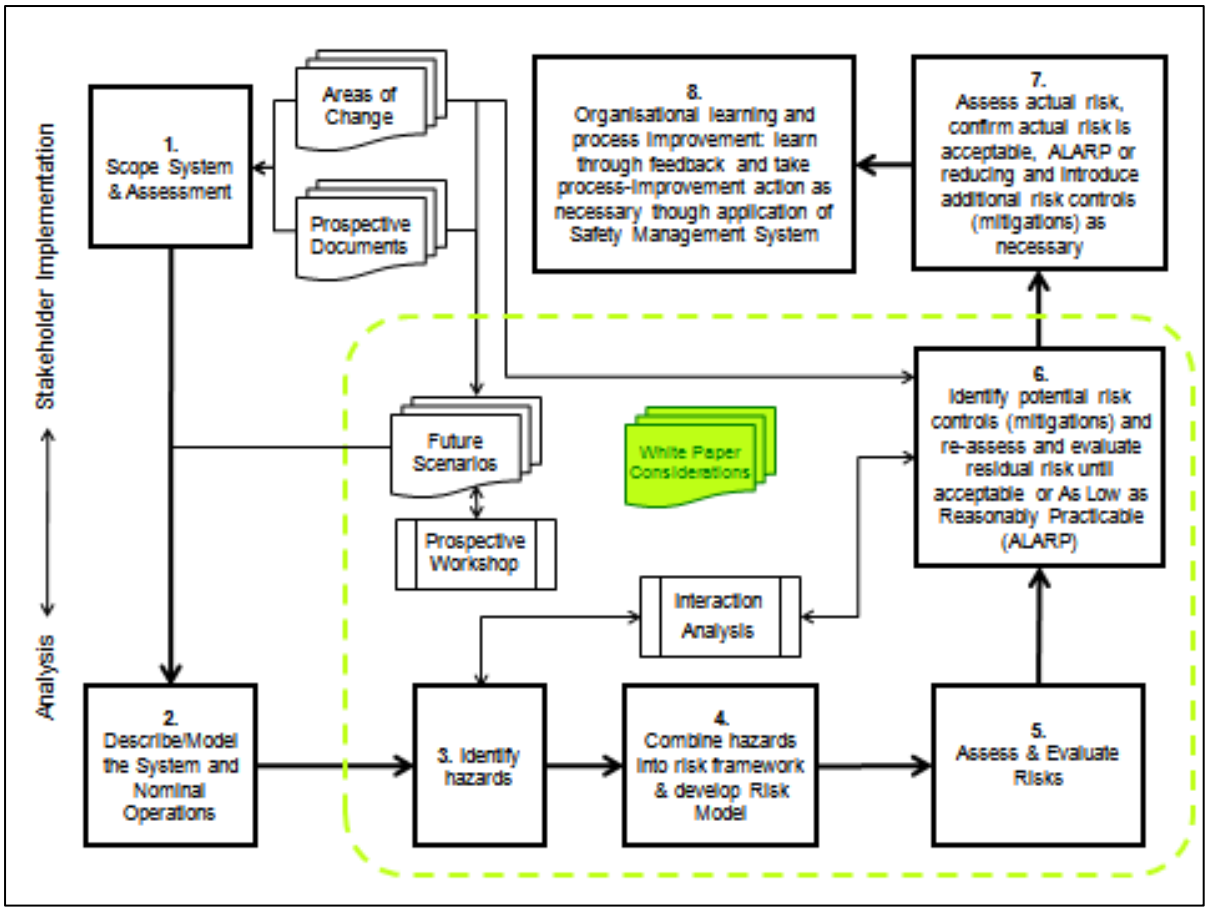
> The prospective documents to be considered for the Safety Assessment shall be relevant to the time horizon considered for the Safety Assessment.

These enrichments and use of prospective reference documents have been incorporated into the augmented version described below.

2.2.3 Guidelines

The augmented Safety Assessment Process is an extension of the generic process of eight stages described in Section 2.2 that is applicable to a wide variety of operational concepts. The remainder of this section provides considerations regarding the application of each of the stages to future systems in a future environment using enriched inputs and processes.

The process flow[5] is illustrated in the figure below:



Note: When this Augmented Safety Assessment process is applied within a large organisation, for instance a manufacturer, a large operator or a program consortium, it may not be advisable for the same team to develop implementation strategies addressing the identified risks. Different teams[6] will bring different perspectives and competencies (problem-oriented vs. solution oriented), which is likely to produce better results.

The 8-stage process still only explains 'what' to do, not 'how' to do it. To implement the 'how', specific methods and techniques need to be selected and used that are appropriately able to address the elements and specifics of the operation to be analysed. A list of methods each having unique strengths for assessment of future risks has been identified by the FAST within the EME1.1 Action Project. The methods are described in Appendix 4 together with an assessment of the stages in the eight-stage process to which they are applicable. Typically, one method may address multiple stages; and multiple methods may be needed to successfully address all stages of the generic safety assessment process.

[5] An enriched version where Areas of Changes and Prospective Documents also play a role in the Definition of the Scenarios and in the Scoping of the System and of the Safety Assessment is presented in Appendix 9.

[6] For instance, the U.S. CAST follows this model with their separate Joint Safety *Analysis* Teams and their counterpart, Joint Safety *Implementation* Teams.

Methodologies to assess future risk should:

- Have sufficient "power of anticipation"
- Consider a range of possible futures
- Yield an integrated risk assessment
- Generate hazard/risk questions
- Evaluate normal system variation
- Consider the multiple dimensions of the system(s)
- Provide a means to prioritise hazards/risks
- Have the ability to model dynamic phenomena
- Aid in identification of unanticipated uses of technology or procedures
- Identify watch items or drift
- Be simple and/or practical to apply by knowledgeable domain experts

The user is expected to be knowledgeable in the selection of suitable methods and techniques for each of the stages. The specific methods available to address each stage of the process will be practical only if the users of the tools have experience in their application.

Besides the activities in each stage and the integration of tools and methods applicable to that stage can be customised based on the particular future system or concept of operation of interest. However this document *is not* a tutorial on how each of the suitable methods could be adapted to analysis of the particular future system of interest. This document is a pointer to modern concepts and approaches that will make existing methods more conceptually robust and more inclusive of key phenomena that are critical to assessment of the safety of future systems.

Stage 1: Scope the System and the Assessment

Scoping means describing and delimiting the system (e.g. an equipment, an aircraft, certain operations, an ATM system) to be considered for the safety assessment, and to identify it interfaces and inter-dependencies with other systems or the rest of the system as a whole (the context).

Scoping also means fixing the time horizon considered for the safety assessment.

Scoping of the analysis task may involve close collaboration between aviation forecasters in industry and government who are predicting desired ends and shaping their values, and technical specialists who are well informed about the realities of future changes within their own fields and about all the various branches of technology that may be available in the future[7]. Therefore, scoping of the safety assessment of the future system of interest may involve a wide spectrum of domain experts.

Composition of Analysis Team

An important part of the scoping process is to set up an expert analysis team. Ideally an expert analysis team should have:

[7] Berger, Gaston, « Sciences humaines et prévision », Revue des deux mondes, n° 3, Feb., 1957

- 8 to 10 individuals[8] or a size suitable for the scope of the domain of interest.
- Ability to set up and lead an adequate working group.
- Knowledge of and experience with risk management concepts, approaches, and skilled in the use of selected methods described in Appendix 2 - a critical competency.
- Experts representing diverse perspectives: engineering, operational, organisational, and human factors experience. However, the individuals participating in the analysis must divorce themselves from their own biases and influences by the field or company they represent.
- A combination of visionary and operational experience:
  - At least one individual from each manufacturing and/or source organisation and one from each end user organisation.
- Prospective mind-set: ability to project oneself into the future; i.e. reflect within a framework that is unknown/uncertain; familiarity with the FAST AoCs.
- Sufficient knowledge of the aviation system in general and specific domains of interest to the analysis at hand to do "back-of-the-envelope" calculations and checks of assumptions[9].
- Ability to doubt, take nothing for granted, play the devil's advocate, and encourage minority viewpoints.

The output of the scoping stage may include writing a Safety Analysis Plan outlining the analysis approach to be taken, ascertaining which dimension(s) of risk (e.g. death & injury, property damage, mission failure, risk perception, etc.) should be evaluated based on the system under study, determining the time horizon of interest, and determining safety/risk criteria for evaluating risk acceptability (e.g. Target Level of safety). Given the various ways that the future can evolve, the safety/risk assessment will include determining the level of uncertainty as well.

Stage 2: Describe/Model the System and Nominal Operations

Particular considerations that are vital to documenting the normal operation envisaged in the future are a) recording the many assumptions for both the current operation, b) the transition process to the new one, and c) the postulated "normal state" of the future technology or operational concept despite the range of uncertainty of that future. This includes the interdependencies within the system of interest.

In order to assess in following stages the hazards and identify the risks that may emerge when introducing new general concepts, the analysis team should draft a concept description paper outlining the salient features of the:

- Proposed novel concept or technology
- Procedural and training implementations
- Special human-systems integration considerations
- Existing control systems (barriers)
- New business and organisational models that may be relevant
- The environmental context in which the future system will operate

[8] When compatible with the size of the organisation.

[9] This is akin to logistics estimates, e.g. for introduction of new equipment, how long would it roughly take for 80% implementation and what would it roughly cost? In other cases it checks whether the implicit or explicit assumptions can be trusted; e.g. by a simple comparison with known situations.

Stage 3: Identify Hazards

Inputs to Stage 3 include the FAST Areas of Change and/or collections of documents that describe the planned future – Prospective Documents.

The analysis team should collect the standard hazard sources affecting future operations. Hazard identification should include an understanding of the potential impacts of unanticipated events, such as so-called "black swans"[10] discussed in the Risk Concepts and Limitations White Paper referenced in Section 4 Limitations.

Interaction Assessment

The augmented safety assessment framework is intended to capture the sum of the effects of significant causal factors within the gate-to-gate cycle. However, this is not a simple matter of adding up independently estimated parts of the hazard picture, because of interdependencies (common-cause failures and interactions between aviation system sub-components) among them[11]. Interactions are those reciprocal actions or influences between the future and the environmental context in which the future of interest is immersed that may generate hazards not otherwise identified by narrow safety analysis methods.

Appendix 6 expands on interaction analysis in the frame of prospective safety. A preliminary hazard interaction assessment is performed at this stage using the techniques outlines in this appendix. A sub-objective of this step is to use domain expertise to identify phenomena that would amplify or diminish the interaction effects. *It is out of the multiple interactions among contributing factors and risk controls that the ultimate precursors and emerging risks are likely to emerge – the complicated and unanticipated chains of events that have led to many historical accidents.*

The analysis team may wish to avail itself of existing Concept Hazard Assessments (CHAs) and Preliminary Hazard Assessments (PHAs) already performed by the organisations proposing the new technologies and procedures of interest. These CHAs/PHAs may provide insight to the range of predicted hazards.

At this stage is will be useful to identify common failures in the future or common events that eliminate redundancy in a system, operation, or procedure. Major components of the system should be assessed for possible failure modes, and for each failure mode the effects of the failures and how critical these effects are should be estimated. These failure modes should be identified for both technology- and human-related hazards in the future. How the factors shaping the performance of the human agents in the system may change in the future must also be addressed. An example of this is the changing demographics of humans in the system due to attitudes and acceptance of technology and personnel retirements.

Depending on the concept of operations being analysed, the relative importance of the different phases of flight - e.g. the influences of strategic versus tactical airborne conflict resolution on safety – must be determined by consensus of the analysis team.

[10] http://en.wikipedia.org/wiki/Black_swan_theory developed by Nassim Nicholas Taleb.
[11] *Predicting the Future: The Integrated Risk Picture*, E Perrin*, Barry Kirwan, EUROCONTROL, France

Various industries have discovered that structured brainstorming approaches can identify a high percentage of hazards that ultimately are realised in the future operation. An augmented version of brainstorming analysis enables identification of hazards that are difficult to identify using a functional approach.

When identifying hazards, the system should not be treated as a static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its future environment.

Stage 4: Combine Hazards into a Risk Framework

The objective of this stage is to combine hazards into a risk framework and develop a risk model that as fully as possible accounts for and assesses the important interactions within the future aviation system (this is a non-trivial task but key to uncovering latent vulnerabilities in socio-technical systems that have yet to emerge).

Contributing Factors to Emerging Risk

The analysis team should compile a list of factors identified in Appendix 7: Contributing Factors to Emerging Risks that can influence the risks that may emerge in the future system of interest including postulating how those factors may manifest themselves. The generic types of contributing factors to emerging risks from the table in this appendix must be constantly kept in mind during the risk assessment as a practical checklist to ensure nothing important to the assessment process is inadvertently skipped.

During this stage, based on the nature of the future "system," the risk framework should be customised at an appropriate level of abstraction: e.g. conceptual, top-down, detail design, or actual implementations of hardware, software, procedures or combinations.

The risk model provides a framework for assessing the effects of major changes to current operational concepts that may be envisioned by system designers and those advocating improvements in aviation system capacity or throughput. For certain future concepts, it may be necessary to use an expert system that captures novel risk factors and their interrelationships.

Because the future comes with many unknowns, gaming approaches in which competing visions are elucidated and contrasted, can serve to reveal plausible strategies and actions that competing operational concepts might generate in the future. As mentioned previously, a competition or challenge-based approach helps overcome the bias of decision makers to ignore evidence that runs counter to their current beliefs, including the possibility of low-probability future scenarios that might disrupt the initial safety strategy.

For instance, the predictive ATM Integrated Risk Picture developed several years ago by Eurocontrol uses a 4-stage approach that may be useful for this methodology: Stage 1: Identify the future ATM situation, i.e. identify the ATM changes that might be implemented in Europe the period up to 2020. Use HAZOPs and on-going safety assessments for the different future ATM components to identify which aspects will positively influence safety, and which aspects will negatively influence safety (hazards).

Stage 2: Make a functional model including the main actors, the information flow between them, and interdependencies, for the future situation, using SADT (Structured Analysis and Design Technique). Stage 3: Use this and the current risk fault tree to evaluate the future situation. Stage 4: Refine and quantify the future IRP by assessing correlated modification factors for the values in the IRP fault tree and the IRP influence model, thus modelling positive interactions, negative interactions, and migration of risk.

Risk Prioritisation

During this stage, the expert team should establish criteria for prioritising the many future hazards that will be discovered in Stage 3; Identify hazards. In addition, the risk framework should identify and categorise the possible interactions discussed in Stage 2 and Stage 3.

A helpful strategy at this stage is the Affinity Grouping Method[12]. The Affinity Grouping Method groups risks that are naturally related and identifies the one concept that ties each grouping together. Groups of risks may share a common mitigation plan.

Because the future is a moving target, the risk analysis framework may need to include capabilities for dynamic assessment using tools that are based on Monte Carlo-style simulations or that estimate dynamic changes in variables over time. Such methods can "discover" emergent phenomena that are characteristic of the future threat vector.

Any method attempting to assess risks in future systems will benefit from incorporating modern concepts for the assessment of emergent risk that have been developed in the past several years. These include the following recent guidelines developed by other individuals and organisations interested in future risk assessment:

A. For purposes of managing safety performance in a future timeframe, risk may not be capable of being captured in 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[13].

B. It is suggested that users of the tools and methods described in this document identify how specific 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. Within the general categories of these factors[14] shown in the Table 2 above, the analysis team should identify which are relevant to the concept of interest and how those contributing factors may manifest themselves in the emergence of future risk. This

[12] *Continuous Risk Management Guidebook*, Software Engineering Institute at Carnegie Mellon University, 1996, NTIS#: AD-A319533KKG, DTIC#: AD-A319 533\6\XAB

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

[14] International Risk Governance Council (http://www.irgc.org/IMG/pdf/irgc_ER_final_07jan_web.pdf)

will be important information to carry forward into the risk assessment process of Stage 5.

Stage 5: Assess & Evaluate Risks

During the risk evaluation process, a number of questions should be used to assess the impact of changes internal and external to the aviation system. These helpful prompts are listed in Appendix 8 Interrogatives for Assessment of Internal and External Phenomena.

This stage employs the likelihoods, impacts and risks established in the previous stages, together with statistical information and expert judgement, etc., to make an assessment of the risks corresponding to the scope determined in Stage 1. Depending on the particular future system under consideration certain methods may be better suited for risk assessment than others. Future risk assessment is challenging because no historic risk probabilities are available. In some cases methods may need to be adapted to make them useful for the future such as using current estimates of incident and operational event data to infer worst-case future outcomes.

Interaction Assessment

The interaction assessment process that was referenced in step 3 is revisited for purposes of analysing and evaluating risk. *It is out of the multiple interactions among contributing factors and controls/mitigations that the ultimate precursors and emerging risks are likely to emerge – the complicated and unanticipated chains of events that have led to many historical accidents.*

This stage is completed with an uncertainty assessment that collects and evaluates all assumptions adopted during Stages 1-5, and furthermore explains the bias and uncertainty in the results. If there are unacceptable future uncertainties, iterations to previous Stages may be necessary. This uncertainty estimate is needed to give decision makers confidence in the findings and to provide recommendations from the analysis team on safety risk bottlenecks and priorities for the identification of mitigating measures (Stage 6).

Two general types of future uncertainty suffice for most risk management purposes:

a. Uncertainty deriving from lack of knowledge about the future system, and
b. Uncertainty due to normal variation: the variability that occurs over time.

Stage 6: Identify potential Risk Controls (barriers) and Reassess the Residual Risk until Acceptable or As Low as Reasonably Practicable (ALARP)

The risk evaluation forms the basis for deciding on risk control (mitigating) measures and in assessing the effectiveness of these measures.

Risk control measures identify the consequences associated with both an unacceptable risk and tolerable risk and where further risk reduction measures are feasible and reasonable,

Identification of possible risk controls is based on the risk description and evaluation, considering in particular any uncertainties identified and critical assumptions made.

Controls that may eliminate the consequence of a hazard, likelihood-reducing measures and severity-reducing measures are identified. The measures should address the human factors (e.g. training and competence), equipment or organisational factors (e.g. procedures).

Risk control priorities

Risk control measures are implemented based on the following priorities:

- *Eliminate the consequences of the hazard,*
- *Reduce the likelihood of occurrence, and*
- *Reduce the severity.*

Risk Control Effect Assessment

The risk mitigating effect of the controls are assessed with respect to:

- *Functionality: Does the measure influence the ability to perform the activity?*
- *Robustness: Will the measure be effective under varying conditions and over time?*
- *Possible other effects such as introduction of new risks.*

When identifying risk control measures, any new risks that may arise from the implementation of such measures ('substitution risks') should be identified.

For any look-ahead safety assessment it is not sufficient to simply assess the effectiveness of isolated, singular risk controls in future circumstances. The combinations of controls and the future concept of operations must be analysed as a whole for the residual risk remaining if those control and mitigation measures perform as expected or fail. The importance of interaction assessment processes discussed extensively in the previous stages is equally valid here.

Failure (or ineffectiveness) of the future risk controls in a system is here defined in a very wide sense, in the following three perspectives:

- Known inability of a risk control to address or remove a particular type of precursor
- Unexpected technical, organisational or human operator failures to prevent the next-stage precursor from occurring
- Unexpected technical, organisational or human actions that introduce a new next-stage precursor that would otherwise not be present – i.e. system generated risk[15].

Residual risk (in the future) is the risk that remains after management's response to the inherent risk of a particular technology or human-related change. Once system designers have developed controls and mitigations in response to identified risks

[15] Fowler, D., Perrin, E., Pierce, R., *Success is not merely Absence of Failure – a Systems-engineering Approach to Safety Assessment*, Proceedings of the 4th IET International Conference on System Safety, London, October 2009

emerging from the analysis process another risk assessment is necessary (i.e. iteration from Stage 2 onwards).

Future controls may come in the form of engineered barriers, training and procedures to avoid or to implement, organisational changes, policy changes, or other actions that may reduce the severity or likelihood of the hazard. The objective here is to look for interventions that simplify the issues and provide progressive a growth path to the future (e.g., incremental introduction adding robustness and resilience). Other factors influencing net risk are the extent of implementation of controls and the effectiveness of the outcomes of targeted research projects.

> Risk is re-assessed considering the effects of the proposed risk control effects. The measures are not necessarily sufficient to bring the risk level back to an acceptable or tolerable level in a first round: if further risk reduction is required, new risk controls are added, or existing risk controls are modified, until the risk is as low as reasonably practicable (ALARP). See Appendix 3.

To be effective, a prospective methodology should identify how specific controls and mitigations are changing in the future that will influence the vector of residual risk. The risk vector (magnitude and direction) will permit decision-makers to determine if the future risk is sufficiently controlled.

The FAST Areas of Change are to be used an input to this stage for assessment of the effect of future circumstances on controls/mitigations effectiveness.

Controls Failures

As a result of the increasing reliability of components and systems in aviation, the majority of future accidents will likely not arise from component failures, but from inadequate control or enforcement of safety-related constraints on the design, development, and operation of the system. Future safety should be viewed as a control problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled[16].

During this stage, it may well be the case that the analysis team discovers favourable interactions that reduce the magnitude of the future residual risk.

Stage 7: Safety Monitoring and Verification

Programs and plans, for instance by SES and NextGen, are developed and implemented to design and shape the future, but unpredictable events and emergent conditions can affect the future: *the future never/rarely entirely realises as planned*.

To address the issue, a monitoring process is introduced to identify over time what future is coming true and introduce the necessary adjustments in the in the safety assessments.

[16] Leveson, Nancy, Systems-Theoretic Accident Modelling and Processes (STAMP)

The benefit of a monitoring process is well illustrated by the following metaphor based on a clothing zipper metaphor:

> The Clothing Zipper Metaphor: the future is open - the farther we look ahead, the wider the uncertainty. But as times passes by, the zipper pulls together the edges of the "future": a wide range of possible futures reduces through the present to one single past. While tomorrow is uncertain and open, yesterday is closed: *the passage of time reduces uncertainty.*

The implication here is that the overall risk assessment process for future aviation systems outlined in this methodology must be repeated periodically to enable fresh insights resulting from monitoring evolving conditions.

Monitoring and verification is part of the "Check" in the Plan Do Check Act (PDCA) cycle of safety management. Under the Check step, analysts study the actual results (measured and collected in "DO," Stages 2-6 above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. They look for deviations in implementation from the plan and also look for the appropriateness/completeness of the plan to enable the execution i.e., "Do". Charting data can make this much easier to see trends over several P-D-C-A cycles and in order to convert the collected data into information. Information is needed for the next step, "ACT".

Watch Items

A key means to enable the monitoring process is the development of Watch Items. These are the tell-tale indicators of enabling or disruptive technologies, policy or regulatory changes, and/or societal expectations that may foreshadow which future or futures are coming about, and therefore which hazard(s) may appear. These leading indicators may consist of events and trends either within or external to the aviation environment.

Stage 8: Organisational learning and Process Improvement

The expected outcomes of this emerging risk analysis framework are to:

- Identify future deficiencies and discrepancies in the evolving Global Airspace System with the objective of improving the resilience of the future aviation system;
- Provide actionable insight to management for planning improvements to the future Global Aviation System;
- Enhance the basis for research relevant to the performance of human agents in the aviation system and to formulate recommendations for future aviation procedures, operations, facilities, and equipment.

Learning Paradigm

- As this methodology is applied, each organisation must identify and take into account the stovepipes that prevent shared learning due to the complex landscape of legacy safety systems. This is particularly important for safety assessment of evolving future system(s).

A major characteristic of a learning organisation is that it requires a pro-active, organisation-wide, integrated approach so that all of the human, organisational, industry and environmental considerations associated with future safety are managed in a well-coordinated way. Centrally organising and delivering shared safety services is efficient, removes perceived bias, facilitates confidentiality, and helps to promote better cross-functional integration.

Without an organisation-wide sharing of safety system information, the true scope of future changes, hazards, their impacts and likelihoods, and the controls and mitigations put in place to manage them may not be available for key stages of the augmented safety assessment process described above.

3. Application to Change Management

Management of Change as an SMS Requirement

The European implementing rules ORO.GEN.200(a)(3) point (e) on Management Systems states that the Company shall manage safety risks related to a change. The management of change is a documented process to identify external and internal changes that may have an adverse effect on safety. It makes use of existing hazard identification, risk assessment and mitigation processes.

Changes include organisational changes with regard to safety responsibilities.

Changes may have various positive or negative safety impacts. Any change that may have an adverse effect on safety shall be identified and managed through the Company's existing processes for hazard identification, risk assessment and mitigation.

Change Impact Assessment Procedure

A straightforward change impact assessment procedure is described below. The Methodology described in this document can be used in support to point 8 - Identify the hazards and assess and evaluate the risks:

1. *Identify the nature and scope of the change(s).*
2. *Differentiate between large & small changes; define criteria.*
3. *Look for the less obvious, e.g. when the change occurs gradually over the years (slow drift does create new hazards).*
4. *Arrange initial planning meeting*
5. *Apart from the usual issues (definition, reason of the change, etc.) look also at the transition phase, how to introduce the change*
6. *Organise coordination with external & internal stakeholders*
7. *Perform an initial Impact Assessment study covering:*

- *The Company's operational procedures (Operations Manual, Standardisation Manual, Maintenance Training Organisation Exposition (MTOE), etc.),*
- *Work organisation (staffing, composition of the teams, scheduling, additional training, etc.),*
- *Infrastructure (relocation, parking base, etc.),*
- *Maintenance of equipment or the aircraft.*

8. Identify the hazards and evaluate and assess the risks

- *Identify hazards related to implementing the proposed change and their possible consequences,*
- *Look at the interactions and dependencies with other parts of the organisation and external stakeholders (e.g. airport, regulator, service providers).*
- *Identify exiting risk controls and define, as appropriate, additional risk control measures.*

9. *Identify key personnel who will assist in implementing the change and the mitigation measures required and involve them in the change management process.*
10. *Define an implementation plan.*
11. *Assess related financial costs.*
12. *Communicate the proposed change to the staff and involve them in the project in an effort to garner their support.*
13. *Implement the actions as defined in the plan; hold a post implementation review.*
14. *Check the overall effects through the established Safety Performance Monitoring and Measurement process.*

4. Limitations

This Methodology has been developed to address in a practical manner, without fully resolving them, the difficulties, opportunities, challenges and paradoxes listed by the FAST in the White Paper developed in the context of this EASp EME1.1 Action.

This paper highlights a number of limitations related to the uncertain future. Additionally, it defines safety terminology, introduces concepts of risk, and predictability, describes sources of uncertainty in prediction frameworks, and introduces the concept of prospection; a distinctly different concept than prediction. Without a proper understanding of the limitations and concepts articulated in that paper, the risk assessment produced using this document may not be as robust as desired.

The first remark is that emerging risk assessment methods or any safety analysis approach will not yield valid results if they utilise incomplete or invalid input information.

If the effectiveness of a particular change (safety enhancement or mitigation) due to future factors is the objective of the analysis, it is not sufficient to simply put that singular change into a model and calculate the effect.

The crux of the matter is that better safety technologies and new hazards plus their associated mitigations will not occur in today's world but in tomorrow's intended yet uncertain world(s). Therefore, to analyse the effect one needs a realistic description of tomorrow's world(s). This is where analysis of emerging risks becomes difficult, because there may be changes in tomorrow's world(s) that have an influence on the effectiveness of the future safety enhancements and proposed – but not yet implemented - mitigations that may be required in the future. *The problem is not the modelling but our ability to adequately describe tomorrow's world(s) with all their associated effects and uncertainties.* This is where a reliable list of the characteristics of the future can be useful.[17] The descriptions of the future offered by the Areas of Change list (Section 2.2.1) and other authoritative references (Section 2.2.2) contain many of the common-cause factors that will influence changes in the future risk landscape.

The second remark concerns complexity. The European Aviation Safety Plan (EASp, 7 February 2011) describes the analytical challenges posed by the complexity of the aviation system in all its potential future evolutions.

> *"Complexity is an attribute of systems or items which makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships."*[18]

Because aviation is a highly complex system, users of the tools and methods referenced in this document must articulate the simplifying assumptions used to achieve workable, practical safety analyses for particular scenarios of interest.

This is especially important for the assessment of risks that in future systems that is the focus of this methodological framework. Organisations proposing to use this framework must fully account for the implications of the complex landscape that will characterise the future aviation system during any risk analysis.

A caution with any prospective method is that this way of thinking should not isolate elements/dimensions from one another. But striving to address all conditions and dependencies may lead to overly complex interrelationships. For this reason, risk analysts and decision-makers might get lost among possible futures – an undesirable outcome that a scenario-based approach may however avoid.

[17] Position articulated by the NLR Air Safety Institute, July 2012
[18] EUROCAE/ SAE Doc ED-79/ ARP4754

Despite the rigor of traditional safety assessment frameworks, it is unlikely that any methodology can fully uncover the subtle tipping points and/or ruptures that can take a highly safe aviation system into a vulnerable future state largely, due in particular to human and organisational influences.

Limitations arise due to the unpredictable ruptures in socio-technical systems that can, do, and will continue to happen in aviation.

Of necessity, the methodology described in this document is based on the concept of forecasting the future – a prospective approach. But, forecasting future safety risk, in its widest sense, includes a variety of methods of perceiving the future; the methodology therefore could borrow from conceptual constructs in other high-reliability industries and take advantage of a range of advanced methods being developed by entities seeking to address risk in industries that face high-consequence events.

These methods[19] include:

- Explorative and normative[20] methods (outward bound; inward bound)
- Quantitative methods (reliance on numerical representations of developments)
- Qualitative methods (used when there is lack of data)
- Expert-based methods (used to draw out informed opinion and elicitation of knowledge)
- Assumption-based methods (elaboration of visions and priorities)

Depending on the input assumptions, various safety models may or may not have the ability to capture the effect of events that are "outside the model". This is because some safety models only consider averages or expected values and ignore the variability of performance. This variability may come into play only in black swan events that happen in future contexts.

5. Concluding Observations

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 hazards and risks. One must understand the factors driving the future risk landscape: changes in needs, interests, visions, hopes, and fears.

As with any safety assessment process, the users of this methodology are invited to take into account how the results of the analyses and possible recommendations for corrective action will be used within the stakeholder organisation. It may be necessary to pre-condition the recipients of the analysis to ensure that the results produce the needed response.

The present safety landscape is "rugged" – it has many local peaks and valleys. Yet for a certain short period of time it is fixed and easy to navigate. The safety landscape of

[19] The review and use of these methods falls outside the scope of this document.
[20] *The Language of Forecasting, Futuribles*, S.É.D.é.I.S, 205, boulevard Saint-Germain, Paris, 1969

the future will literally dance and shift beneath our feet as local optimisations and risks come and go or move in new directions[21].

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 if sufficient testing and operational evidence is available[22].

For complex systems, however, accurate predictions are challenging. No one can predict 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, say the next year or two. Using the approach outlined in this document, one may have increased confidence in looking down the road somewhat farther.

The real difficulty of future risk assessment is not complexity per se, but in the accelerated rate of change of complex systems. The faster the risk landscape changes or "dances," 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 recognise undesirable tendencies as soon as they appear and then adopt strategies to minimise their impact. The framework described in this document is a step along that path.

[21] Page, Scott E., *The Evolution of Diversity*, University of Michigan, July 28, 2006

[22] The life of components may be adversely affected if they are operated in unexpected environments, procedures, or conditions. At one point in history, structural fatigue was based on static loads and pressures until failure modes caused by dynamic changes such as repeated pressurization cycles began appearing.

Appendix 1: Guidelines for conducting a Prospective Workshop (optional) as an Aid to Scenario Development

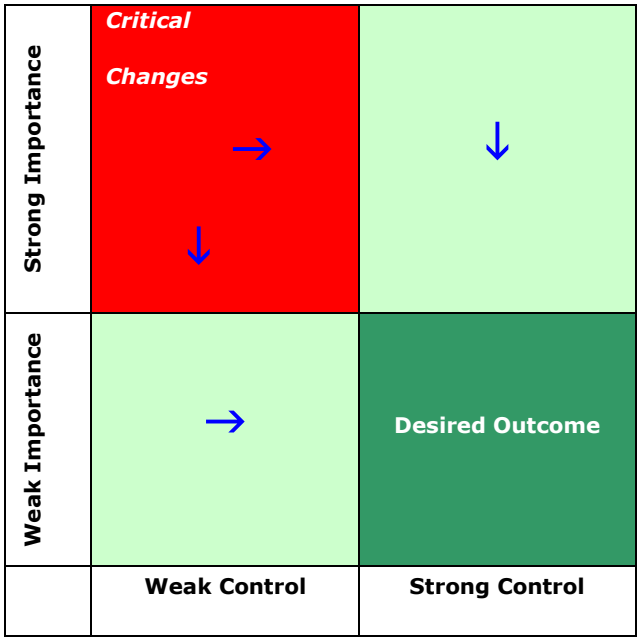
The Godet's 12-step workshop approach described below[23] can be used as a practical supplementary process enabling an analysis team to identify and form into a hierarchy the main objectives, enabling capabilities of the future system of interest as well as the importance and degree of control over germane changes and possible points of rupture.

This is a suggested starting point to activate a futures mind set; it does not replace the detailed risk and controls assessments of earlier stages of the augmented process. The high-level scenarios, risks, and controls outputs of this exercise may be a useful pre-requisite to Stage 1, Scope the assessment, of the augmented safety assessment process described in Section 2.2:

1. The leader of the analysis team asks participants to identify a. expected, b. desired, and c. feared changes based on their understanding of the future aviation system as they understand it and their notions of the future environment in which that system will be immersed. The FAST Areas of Change list and reference prospective documents (see Appendix 3) will provide useful input information.
2. Identify the inertias – those forces which will tend to keep the system moving its current direction whether safe or vulnerable.
3. Individual results are presented to the group in order to build a common list of changes and inertias through several rounds of discussions. To be effective and to limit bias, the individual results should be written, compiled, and completed by each individual (devoid of interaction with others in the group) before beginning discussion.
4. Aggregate the individual preferences among the group in order to identify the five to ten major changes that appear to be, according to blind voting consensus, major issues for the future.
5. Place the consensus changes and inertias within a matrix of *importance* (weak or strong along the ordinate) versus *level of control* of those inertias (weak or strong along the abscissa).

[23] Godet, Michel, *GUIDELINE FOR STRATEGIC PROSPECTIVE WORKSHOPS*, National Conservatory for Arts and Industries - LIPSOR

6.



7. For *critical changes* – those that are both *important* and over which we have *weak control*, conduct a group brainstorming session asking two questions to achieve the *desired outcome*:
    a. How can we reduce the importance of the controls?
    b. How can we increase their control?
8. Identify the stakes and objectives for the future aviation system under study.
9. Identify the necessary actions in order to reduce the stakes and reach current system objectives.

Critical Changes	**Stakes, Visions, Priorities**	**Objectives toward Stakes**	**Ideas of Possible Measures to Implement Objectives**
1			
2			
.			
.			
n			

10. Using the above table, conduct a discussion of and record the answers to the following questions:
    a. Who are the other actors affected by these changes?
    b. What are the points of leverage (acting for or against action)?
    c. How to improve the control over major changes?
    d. How to reduce the importance of uncontrolled changes?
    e. How to reduce system weaknesses and better exploit system strengths?

11. Based on the critical issues identified in above, list probable solutions as well as possible ruptures.

Critical Changes	Solutions	Possible Ruptures
1		
2		
.		
.		
n		

12. Using the information from the above two tables and knowledge of probable future environments, create two or three exploratory scenarios involving the future system under study.
13. Using these scenarios, identify the major prospective risks and possible revisions to or augmentations of control measures.

Appendix 2: Scenario Development Aids and Analysis Methods

In order to assess in following stages the hazards and identify the risks that may emerge when introducing new general concepts, the analysis team could draft a Concept Description paper outlining the salient features of the:

- Proposed novel technology,
- Procedural and training implementations
- Special human-systems integration considerations
- Existing risk control systems (barriers)
- New business and organisational models that may be relevant
- The environmental context in which the future system will operate

Despite the fact that the future can never be predicted with full certainty, certain changes are quite likely to happen, such as the introduction of 4D trajectory management, Automatic Dependent Surveillance-Broadcast (ADS-B), and System Wide Information Management (SWIM), for instance. These known and planned elements can then be combined with less certain elements (e.g. changing personnel demographics and non-linear scientific advances) to form various *scenarios of the future*.

Scenarios of the future fitting one or more of the conceptual frameworks described above can be formulated using domain experts and knowledge of intended as well as unintended changes as described in the reference documents and FAST AoCs, for example. Nevertheless these scenarios may not adequately capture the complex web of safeguards, the safety organisational, management and regulation, and variable human behaviours that more often than not contribute to accidents due to the ruptures they generate. Scenarios address blind spots by challenging assumptions, expanding vision and combining information from many different disciplines.

Expert judgement will be useful to identify the most likely scenario and to assess their likelihood. Methodologies exist to consolidate the opinions or judgements of multiple experts. One of the most well-known one is the Delphi Method.

The scenario planning approach originally developed by Shell Oil[24] in the 1960s is a systematic process for defining the plausible boundaries of the future states of the aviation world. Though the future is "terra incognita", we may be able to guess the outcome of events that lie close to us, as we project beyond this we enter an unmapped zone full of uncertainty. Paradoxically, the range of options this reveals can seem paralysing. No one can definitively map the future, but we can explore and limit the possibilities in ways that are specifically intended to support effective decision-making.

Scenario developers examine technological, regulatory, socio-political, economic, and environmental forces affecting aviation and select some number of drivers or motivators – typically four – that may have the most significant effect on the desired goals and objectives. In the Shell scenario development approach, the development team is drawn from a multi-disciplinary set of experts. For each of the selected drivers, participants

[24] *Scenarios: An Explorer's Guide, Exploring the Future*, © 2008 Shell International BV
http://www-static.shell.com/static/public/downloads/brochures/corporate_pkg/scenarios/explorers_guide.pdf

estimate the maximum and minimum anticipated values of each driver over the future timeframe of interest, say five to ten years out. The matrix of values for each of the four drivers lead to sixteen system scenarios; about half of which tend to be implausible and are discarded. The team then performs the safety analysis on the remaining scenarios.[25] The objective is to estimate the credible worst-case harm that can occur.

Alternatively, the safety analysis team can employ a *war-gaming* approach in which participants break up into three or four teams and each devises plausible strategies and actions that competing operational concepts in aviation might manifest. This technique is usually employed in a shorter future timeframe of interest, say one to two years out. A competition or challenge-based approach helps overcome the bias of decision makers to ignore evidence that runs counter to their current beliefs, including the possibility of low-probability future scenarios that might disrupt the initial safety strategy[26].

> Challenge-based scenarios are vital since even present-day accidents and incidents involve sequences of failures of technology and human actions/reactions not anticipated by designers.

It is suggested that as part of the scenario development process, the multi-disciplinary analysis team complete Table 1 for each of the significant variables or drivers that are part of the system under study that may influence future risk. This practical exercise will help crystallise the focus of the analysis team on the primary safety issues within later scenarios and yield a broad understanding of the historical evolution of those major issues – an essential, pragmatic starting point for prospective safety analysis. *This table could also be used by the analysis team for conducting* ***structured interviews*** *with knowledgeable experts outside the team regarding specific drivers within the aviation system of interest. This could also form the basis of questionnaires directed to similar constituencies.*

TABLE 1: DESCRIPTION OF FUTURE DRIVERS	
1. Definition of the variable or phenomenon	
2. Briefly describe the evolution of the particular phenomenon over an appropriate timeframe: • 30 years ago • 20 years ago • 10 years ago	
3. Describe the current situation or safety issue of concern	
4. How is the current situation measured? • Counts of events? • Existence of specific conditions?	

[25] *Managing Risks: A New Framework*, Harvard Business Review, Reprint R1206B, June 2012
[26] ibid.

5. Future evolution
 	
• What will this phenomenon look like in 20XX, 20YY, etc.?
• Does it point to a fundamental
  ○ Trend?
  ○ Major uncertainty?
  ○ Possible rupture?
Definition of the "Future State" of aviation:
 	
• What will the people be like in 20XX?
  ○ Includes demographics, culture, background, communication styles, training, etc.
• What will the equipment look like in 20XX?
  ○ Includes human factors, maintainability, etc.
• What will the airspace look like in 20XX?
  ○ Includes operations, air and ground procedures, etc.
• What will regulations and regulators look like in 20XX?
  ○ Includes oversight factors, certification, legal concerns, etc.
• What will the external environment look like in 20XX?
  ○ Includes climate, world markets, tort considerations, influences outside the control of the aviation system, etc.
• How will different regions of the world differ in 20XX?
  ○ Unique regional safety challenges for North America, Central/South America, Europe, Australia/South Pacific, Russia/CIS, Middle East, Asia, China, Africa	

6. What are the assumptions regarding how the phenomenon will evolve?	
7. With what other key variables will this phenomenon interact?	
8. References and/or experts consulted	

Appendix 3: The ALARP Concept

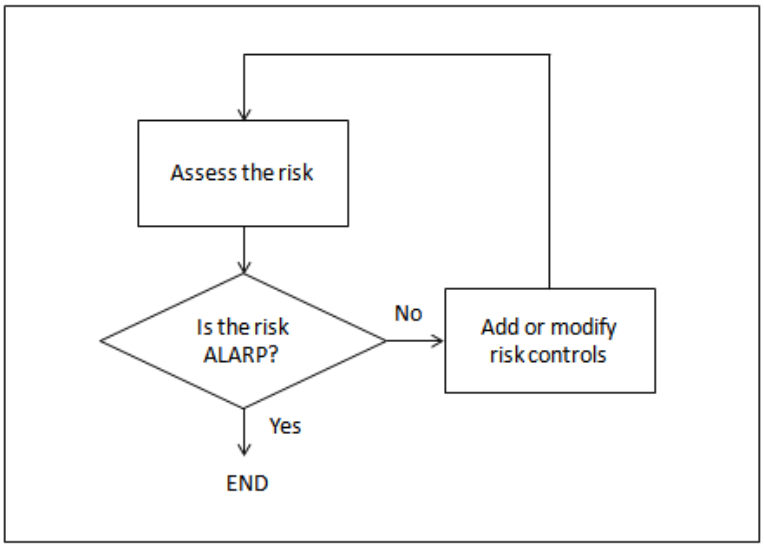
The ALARP approach consists of reducing risk until *"reasonably practicable".* ALARP means that the safety risk is being managed to as low a level as reasonably practicable whilst at all times staying below the maximum allowed risk.

An ALARP risk acceptance criterion is not exclusively based on fixed risk level targets but is a systematic and documented process to reduce safety risks below the maximum allowed by regulations or standards.

Risk is re-assessed considering the effects of the proposed risk control effects, as illustrated in the table below:

Risks Assessed	Initial Risk Level	Risk Controls (Barriers)	Resulting Risk Level (Residual Risks)
Risk 1			
Risk 2			
Risk 3			
Risk n			

The measures are not necessarily sufficient to bring the risk level back to an acceptable or tolerable level in a first round: if the risk acceptance criteria require further risk reduction, the comparison (iterative process) describes the optimisation process. So new risk controls are added, or existing risk controls are modified, until the risk is as low as reasonably practicable (ALARP).



Iterative Risk Reduction Process

The ALARP concept combines the technical feasibility of further reducing the safety risk and the cost; demonstrating that the safety risk is ALARP means that any further risk reduction is either impracticable or grossly outweighed by the cost.

ALARP does not mean that every measure that could possibly be taken (however theoretical) to reduce risk must be taken. Sometimes, there is more than one way of controlling a risk. These controls can be thought of as barriers that prevent the risk being realised and there is a temptation to require more and more of these protective barriers, to reduce the risk as low as possible. ALARP means that a barrier can be required only if its introduction does not involve grossly disproportionate cost. A multiplicity of barriers and controls can provide increased redundancy and resilience.

ALARP does not represent zero risk. We have to expect the risk arising from a hazard to be realised sometimes, and so for harm to occur, even though the risk is ALARP.

Note: One challenge of using an ALARP approach to analysing aviation risks is the cascade effect. If a risk is of very low probability (but potentially catastrophic or very high consequence), the probability of adverse impacts may be deemed so low that they are not considered in planning and resource management processes. An alternative approach is that of *hazard-based analysis of risk*. Such an approach evaluates the character of events *regardless of their low (or high) probability*. Using this approach, a potential impact would not lose significance even if the risk is reduced through new technologies and practices[27]. Such an approach can also be used for vulnerability- or threat-based safety assessments that don't depend on estimated hazard probabilities even if low.

[27] Scarlett, Lynn, Linkov, Igor, and Kousky, Carolyn, *Risk Management Practices, Cross-Agency Comparisons with Minerals Management Service*, Resources For the Future, RFF DP 10-67, January 2011

Appendix 4: Example List of Methods usable for Future Safety Assessment

There is a wide variety of risk assessment conceptual frameworks, methodologies, and methodologies catalogues.

The most promising catalogues of safety methods are:

1. NLR Safety Assessment Methods Database, Version 0.9, 7 December 2010; http://www.nlr.nl/documents/flyers/SATdb.pdf

2. FAA/Eurocontrol AP-15 Safety Methods Toolbox: http://www.eurocontrol.int/eec/gallery/content/public/documents/EEC_safety_documents/Safety_Techniques_and_Toolbox_2.0.pdf

3. "Guide to Methods & Tools for Airline Flight Safety Analysis" [GAIN, 2003] http://www.skybrary.aero/bookshelf/books/237.pdf

Selected Methods and How Each Fits into the 8-Stage Framework

Stage 1 – Scope the System and the Assessment

Stage 2 – Describe/Model the System and Nominal Operations

Stage 3 – Identify Hazards

Stage 4 – Combine Hazards into a Risk Framework

Stage 5 – Assess and Evaluate Risks

Stage 6 - Identify potential Risk Controls (barriers) and Reassess the Residual Risk until Acceptable or As Low as Reasonably Practicable (ALARP)

Stage 7 – Safety Monitoring and Verification

Stage 8 – Organisational Learning and Process Improvement

	Framework Steps							
Future Safety Analysis Technique	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ASRM (Aviation Safety Risk Model)				x	x			
Bias and Uncertainty Assessment					x	x		
Bow-Tie Analysis				x	x	x		
BBN (Bayesian Belief Networks				x				
CATS (Causal model for Air Transport safety)	x							x
CapSA (Capability Safety Assessment (CapSA)		x		x	x	x		

CIA (Cross Impact Analysis)				x	x			
CSA (Comparative Safety Assessment)					x	x		
CCA (Common Cause Analysis)			x					
DBN (Dynamic Bayesian Network)				x				
DYLAM (Dynamic Logical Analytical Methodology)				x				
Data Mining			x		x		x	x
ERM (Emerging Risks Methodology)			x					
External Events Analysis				x	x			
ETA (Event Tree Analysis)				x				
FAST Method (Future Aviation Safety Team) 2006,7,12	x	x	x					
FHA (Functional Hazard Assessment) acc to ARP 4761			x					
FORAS				x	x	?		
FMECA (Failure Modes Effects and Criticality Analysis)			x		x			
FRAM (Functional Resonance Accident Model)				x				
Gael Risk Analysis	x	x	x	x	x	x	x	x
HAZOP (Hazard and Operability study)			x					
HRA (Human Reliability Assessment)				x	x	x		
HAMECA (for human related hazards)			x		x			
IRP (Integrated Risk Picture)		x	x	x	x			
Multi-Agent Dynamic Risk Modelling	x	x	x	x	x	x		x
MASCA (Managing System Change in Aviation)								x
NextGen Future Safety Assessment Game				x	x			
PHA (Preliminary Hazard Analysis)			x					
Pure Hazard Brainstorming			x					
PRA (Probabilistic Risk Assessment based on FTA/ETA)				x	x			
Petri Nets				x				

PSSA (Preliminary System Safety Assessment)				x	x	x		
Quantification of systemic risk and stability: New methods and measures					x			
Risk AHP method					x			
Scenario Analysis	x		x		x			
SAFMAC (SAFety validation framework for MAjor Changes)	x							
STAMP (Systems Theoretic Accident Modelling and Process)			x		x	x		x
SOCRATES (Socio-Organisational Contribution to Risk Assessment and the Technical Evaluation of Systems)				x				
TRIAD Tool for Risk Identification, Assessment, and Display (TRIAD)			x	x	x	x	x	?

Beside, several software utilising bow tie diagrams offer the prospect of addressing all eight stages described herein. A bow tie representation of risk is highly effective in communicating and getting a deep understanding of threats, risks, and consequences. Bow ties also highlight the relationships and importance of barriers and controls that are in place to prevent incidents from occurring or limiting damage should they occur. The visual simplicity of bow ties make them highly effective and their use in many form factors makes them practical ways to depict risk for decision makers.

Another capability is the Tool for Risk Identification Assessment, and Display (TRIAD) developed by Dr. Immanuel Barshi, NASA Ames, and Dr. Robert Mauro, Decision Research. It has two major modules: Current Risk and Forecast Risk. In addition, TRIAD captures different possible outcomes and displays different types of consequences, as well as the associated confidence intervals around the estimates - ideal characteristics for a desired EME1.1 capability.

On a general level, there are several expectations regarding the desirable traits for a potential safety modelling approach:

- It should provide understanding of how safety depends on different elements of the current operation. With this understanding, it should be able to indicate the big risks, strong and weak areas, and provide strategic directions for safety improvements and safety research.
- It should be used as a monitoring/evaluation tool.
- It should be able to determine the safety effects of future changes in the aviation system or subsystem, thereby supporting decision-making and policy development.
- It should have an appropriate level of sophistication to achieve credible results in the eyes of stakeholders. An important feature that has not been addressed in traditional safety assessment techniques is the need to identify all the probabilities of occurrences whose confluence result in a hazard.

Other key characteristics include[28]:

- One single model cannot be used to answer each question of every possible user. Depending of the problem at hand, some parts of the model may have to be developed further in order to answer the question.
- Modelling involves numerous assumptions. If initial assumptions are no longer valid due to evolving conditions, the initial model cannot be used without taking new or modified assumptions into account.
- A risk model should not be used as the sole input for assessing compliance with regulation unless the relevant stakeholders agree to the model and its use.
- Professionals within the aviation industry use sophisticated risk models. Such models are not suitable for use by non-experts or as instruments for safety communication from the government to the general public.
- A potential strength of a risk model is that it can assemble information from different disciplines. It is therefore specifically suitable to support decision making for situations involving multiple actors or disciplines.
- A potential strength of a risk model is that it systematically assembles current knowledge.

The following table describes the risk assessment methods recommended by the FAST in Phase 1 plus the additional methods described above as well as some new tools under development.

The table identifies particular stage(s) of the augmented Safety Assessment process (Section 2.2) that each of these methods can potentially address.

Method Name	**Description**	**Stage in augmented safety assessment process**
ASRM (Aviation Safety Risk Model)	The Aviation System Risk Model is an aircraft accident causal model that can be used to calculate a relative safety risk metric. In the ASRM, a type of accident is represented as a binary node Bayesian Belief Net. 20 models have been developed for 6 types of accidents. These models are developed using case studies coupled with knowledge gained during sessions with subject matter experts. The conditional probability of one causal factor given the presence of other factor(s) is estimated using the 'beliefs' of subject matter experts or data if available. The model can be used to evaluate the potential risk impact of new technologies.	Stage 4: Combine hazards into risk framework Stage 5: Evaluate risks
BBN (Bayesian Belief Networks)	BBN (also known as Bayesian networks, Bayes networks, Probabilistic cause-effect models and Causal probabilistic networks), are probabilistic networks derived from Bayes theorem, which allows the inference of a future event based on prior evidence. A BBN consists of a graphical structure, encoding a domain's variables, the qualitative relationships between them, and a quantitative part, encoding probabilities over the variable. A BBN can be extended to include decisions as well as value or utility functions, which describe the preferences of the decision-maker. BBN provide a method to represent relationships between propositions or variables, even if the	Stage 4: Combine hazards into framework

[28] Roelen, Alfred L. C., Causal risk models of air transport: Comparison of user needs and model capabilities, PhD. thesis, Technical University Delft, 2008 and others

	relationships involve uncertainty, unpredictability or imprecision. By adding decision variables (things that can be controlled), and utility variables (things we want to optimise) to the relationships of a belief network, a decision network (also known as an influence diagram) is formed. This can be used to find optimal decisions, control systems, or plans.	
Bias and Uncertainty assessment	Aim is to get insight into the assumptions adopted during a model-based accident risk assessment, and on their effect on the assessment result. Technique assesses all model assumptions and parameter values on their effect on accident risk, and combines the results to get an estimate of realistic risk and a 95% credibility interval for realistic risk.	Stage 5: Evaluate risks Stage 6 - Identify potential risk controls
Bow-Tie Analysis	Aim is to enhance communication between safety experts (who construct a Bow-Tie diagram) and operational experts (who identify hazard mitigating measures using the Bow-Tie diagram). The knot of the Bow-Tie represents a releasing event or a hazard. The left-hand side wing shows threats and pro-active measures, which improve the chances of avoiding the hazard; the right-hand wing shows consequences and reactive measures to improve the chances of avoiding the hazard prior to its escalation.	Stage 4: Combine hazards into framework Stage 5: Evaluate risks Stage 6 - Identify potential risk controls
CapSA (Capability Safety Assessment)	CapSA is a very high-level analysis framework that has some useful characteristics, benefits, and limitations described below. It does not offer the sophistication of an ideal method for assessing future risk as embodied by the selection criteria applied to the methods survey in Phase 1. Though it is perhaps the simplest of the methods frameworks identified in Phase 1 of EME1.1, the aforementioned CapSA analysis of TBO required identification and assessment of a total of 94 hazards including assumed mitigations. The CapSA is intended to provide NextGen/SESAR designers and implementers a preliminary assessment of whether capabilities, operational improvements, and enablers described in the planning documents can be operated safely, given the state of maturity of the concepts being addressed, as modified and/or enhanced by known or planned mitigating technologies, procedures, and other measures. Lacking specifics of architecture and design, the CapSA is by necessity an assessment based on concepts and many assumptions. A more detailed hazard assessment, along with the rest of the system safety assessment process, must be an integral piece of the design of equipment and procedures. CapSA process uses the hazards identified by Concept Hazard Assessment (CHA) teams. These hazards must be categorised to more easily organize them for a concurrent, integrated review and disposition. The TBO categorisations are loosely organized by external hazards, hazards associated with the manoeuvring aircraft, hazards associated with Air Navigation Service (ANS) operations, and hazards associated with other local aircraft. Outcome risk estimations are based on the successful qualitative approach used by the Joint Implementation Measurement Data Analysis Team (JIMDAT) within the U.S. Commercial Aviation Safety Team (CAST), assuming the mitigations listed in each CHA hazard are properly implemented. Outcome risk is developed, based on significance of the hazard, its likelihood, and the strength of hazard mitigations. This outcome risk	Stage 2: Learning the normal operation Stage 4: Combine hazards into risk framework Stage 5: Assess and Evaluate Risks (static) Stage 6 - Identify potential risk controls

	is based on operations conducted with the listed mitigations from the CHAs in place. A primary difference between a CHA and a CapSA is the attempt by the CapSA to make projections concerning the risk associated with the hazards identified, rather than just identifying them. The primary goal of the CapSA analysis is to produce a list of rated hazards and additional mitigations to reduce the risk associated with those hazards. The CapSA also looks at combinations and interactions among the identified hazards. It is important to determine if combinations of lower-rated hazards may develop into a combined hazard that poses significantly more risk to the system.	
CATS (Causal model for Air Transport Safety)	The Causal Model of Air Transport Safety is an aircraft accident causal model. All potential accidents, divided into accident categories, are represented in a single Bayesian Belief Net. This allows the model to take into account dependencies. The model is quantified using accident and incident data and expert judgement. The consequences of the accidents in terms of expected fatalities and aircraft damage are also represented in the model. For each number in the model, the uncertainty in the estimate is expressed by a standard deviation. The model is intended to enable comparative judgements (e.g. over time and to prioritise potential safety measures (e.g. on the basis of expected effectiveness).	Stage 1: Scoping (input to setting safety targets) Stage 8: Organisational learning
CCA (Common Cause Analysis)	Common Cause Analysis will identify common failures or common events that eliminate redundancy in a system, operation, or procedure. Is used to identify sources of common cause failures and effects of components on their neighbours. Is subdivided into three areas of study: Zonal Analysis, Particular Risks Assessment, and Common Mode Analysis. Root Cause Analysis is a form of CCA that focuses on a single cause.	Stage 3 (Identify hazards)
CIA (Cross Impact Analysis)	Cross Impact Analysis is based upon the premise that events and activities do not happen in a vacuum and other events and the surrounding environment can significantly influence the probability of certain events to occur. It attempts to connect relationships between events and variables. These relationships are then categorised as positive or negative to each other, and are used to determine which events or scenarios are most probable or likely to occur within a given time frame. The Futures Forecasting Style of CIA is based on several strict steps. • First, analysts must consider the number and type of events to be considered in the analysis and create an event set. Because each event will have an interaction with every other event, only 10 to 40 events should be used. • Second, analysts must take the initial probability of each event into account. The probabilities of events must be taken in isolation from one another. • Third, analysts need to generate conditional probabilities that events have on each other. Basically, this asks the question, "If event 'A' occurs, what is the new probability of event 'B' occurring?" This must be done for every possible interaction between events. • Fourth, analysts must test their initial conditional probabilities to ensure that there are no mathematical errors. Running simulations in a computer several times is the usual process. • Fifth, analysts can run the analysis to determine future	Stage 4: Combine hazards into framework Stage 5: Evaluate risks

	scenarios, or determine how significant other events are to specific events. Two general styles of CIA are used: 1. The **Futurist Forecasting Style** of Cross Impact Analysis relies heavily on probabilities and mathematics in its processes. Initial probabilities and conditional probabilities are calculated using either percentages or factor numbers equivalent to percentages. 2. The **Intelligence Analysis Style** of Cross Impact Analysis goes beyond comparing events to include variables like environment, political and economic circumstances, and public risk perception to influence probabilities of certain events.	
CSA (Comparative Safety Assessment)	Each safety hazard is investigated in the context of investment alternatives. The result is a ranking of alternative solutions by reduction in safety risk or other benefits. Steps are to: • Define the alternative solutions under study in system engineering terms (mission, human, machine, media and management); • Develop a set of hierarchical functions that each solution must perform; • Develop a Preliminary Hazard List (PHL) for each alternative solution; • List and evaluate the risk of each hazard for the viable alternative solutions; • Evaluate the risk; • Document the assumptions and justifications for how the severity and probability of each hazard condition was determined.	Stage 5: Evaluate risk Stage 6 - Identify potential risk controls
Data Mining	Data mining is a generic term for systematically analysing large amounts of data to find previously unknown trends, patterns or associations. State-of-the-art methods are being developed to identify non-prescribed patterns of atypicality and novel interrelationships that may be indictors of emerging risk. These are being employed for analysis of quantitative data in settings such at the Aviation safety Information Analysis and Sharing System (ASIAS) and within various Flight Operations Quality Assurance (FOQA) and Flight Data Monitoring (FDM) programs in the industry. Similarly, new, machine-learning algorithms are being developed to automatically classify events from the mining of narrative data. In all cases, data mining is used to draw the attention of the expert analyst to interesting patterns of events that may portend future safety problems.	This technique requires a database of information and data as input. Depending on the type of data in such database, the technique could be useful in Stages 3 (to identify hazards), 5 (e.g. for parameter values), 7 (to monitor actual risk) and 8 (organisational learning)
DBN (Dynamic Bayesian Belief Networks)	Dynamic Bayesian Networks (or Dynamic Bayesian Belief Networks) are a method for studying state-transition systems with stochastic behaviour. A DBN is a Bayesian network that represents sequences of variables. These sequences are often time-series (for example, in speech recognition) or sequences of symbols (for example, protein sequences). DBBNs comprise a large number of probabilistic graphical models, which can be used as a graphical representation of dynamic systems. With this, they provide a unified probabilistic framework in integrating multi-modalities.	Stage 4: Combine hazards into framework
DYLAM	Implementation of concept of Dynamic Event Tree Analysis. A	Stage 4: Combine

(Dynamic Logical Analytical Methodology)	physical model for the system is constructed which predicts the response of system process variables to changes in component status. Next, the undesired system states are defined in terms of process variable levels. At the end of the first time interval all possible combinations of component states are identified and their likelihoods are calculated. These states are then used as boundary conditions for the next round of process variable updating. This is continued until an absorbing state is reached. The dynamic event logic analytical methodology (DYLAM) provides an integrated framework to explicitly treat time, process variables and system behaviour. A DYLAM will usually comprised of the following procedures: (a) component modelling, (b) system equation resolution algorithms, (c) setting of TOP conditions and (d) event sequence generation and analysis. DYLAM is useful for the description of dynamic incident scenarios and for reliability assessment of systems whose mission is defined in terms of values of process variables to be kept within certain limits in time[19]. This technique can also be used for identification of system behaviour and thus, as a design tool for implementing protections and operator procedures.	hazards into framework
ERM (Emerging Risks Methodology)	As a direct follow-up to its work on risk governance deficits, IRGC is now focussing on emerging risks. IRGC defines as "emerging" a risk that is new, or a familiar risk in a new or unfamiliar context or under new context conditions (re-emerging). Emerging risks are issues that are perceived to be potentially significant but which may not be fully understood and assessed, thus not allowing risk management options to be developed with confidence This project takes place in two phases. Its purpose is not to develop a list of risks or possible future changes but, instead, to focus on how and why risks emerge (phase 1), and to develop practical guidelines for practitioners in business and the public sector, helping them improve their own capabilities to understand, anticipate and respond to emerging risks (phase 2).	Stage 3: Identify hazards
ETA (Event Tree Analysis)	An Event Tree models the sequence of events that results from a single initiating event and thereby describe how serious consequences can occur. Can be used for developing counter measures to reduce the consequences. The tool can be used to organise, characterise, and quantify potential accidents in a methodical manner. The analysis is accomplished by selecting initiating events, both desired and undesired, and develop their consequences through consideration of system/ component failure-and-success alternatives. A bottom-up, deductive system safety analytical technique Applicable to: • Physical systems, with or without human operators • Decision-making/management systems Complementary techniques: • Fault Tree Analysis • Failure Modes and Effects Analysis	Stage 4: Combine hazards into framework
External Events	The purpose of External Events Analysis is to focus attention on those adverse events that are outside of the system under study. It	Stage 4: Combine hazards into

Analysis	is to further hypothesise the range of events that may have an effect on the system being examined. The occurrence of an external event such as an earthquake is evaluated and effects on structures, systems, and components in a facility are analysed.	framework Stage 5: Evaluate risk
FAST Methodology - 2011	The FAST Method is aimed at identifying future hazards that have not yet appeared because the changes within the aviation system that may produce these hazards have not yet taken place. The method process flow consists of 12 steps; 1) Be responsible for implementation of global aviation system changes; recognise your need for systematic prediction of hazards associated with changes and to design those hazards out of the system or avoid or mitigate the hazard; 2) Clearly define scope of expert team study; 3) Assemble an expert team; 4), 5) and 6) Communicate with FAST and Customer to understand the complete task; to understand pertinent Areas of Change (AoC); to determine key interactions; 7) Refine the visions of the future; 8) Compile the hazards; 9) Determine the watch items; 10) Compile recommendations; 11) Inform FAST regarding results; 12) Inform customers regarding results.	Stage 1: Scoping Stage 2: Learning the normal operation Stage 3: Identify hazards
FHA (Functional Hazard Assessment) according to ARP 4761	FHA according to ARP 4761 examines aircraft and system functions to identify potential functional failures and classifies the hazards associated with specific failure conditions. The FHA is developed early in the development process and is updated as new functions or failure conditions are identified. FHA is applied at two different levels: an aircraft level and a system level. The former is a qualitative assessment of the basic known aircraft functions, the latter examines each system which integrates multiple aircraft functions. An aircraft level FHA, which is a high level FHA, is applied during an activity to determine functional failure consequences and applications; i.e. to determine the classification of the failure conditions associated with each function. This classification is based on hazard severity. A system level FHA is applied during an activity in which functions are allocated to systems and people; this stage consists of establishing the appropriate grouping of aircraft functions and the allocation of the related requirements to people or systems. The allocation should define inputs, processes performed and outputs. From the function allocations and the associated failure consequences, further specific system requirements necessary to achieve the safety objectives are determined. The output is a set of requirements for each human activity and aircraft system together with associated interfaces.	Stage 3: Identify hazards
FMECA (Failure Modes Effects and Criticality Analysis)	In a Failure Modes Effects and Criticality Analysis (FMECA), each individual component of the system is assessed for its possible failure modes, and for each failure mode it is determined what the effects of the failures are and how critical these effects are. Criticality is defined as the combination of the probability of the failure mode and the severity of its effect. The objective is to rank the criticality of components that could result in injury, damage or system degradation through single-point failures in order to identify those components that might need special attention and control measures during design or operation**.**	Stage 3: Identify hazards Stage 5: Assess risks (criticality)
FORAS (Flight Operations Risk Assessment	The Flight Operations Risk Assessment System (FORAS) is a risk modelling methodology that represents risk factors and their interrelationships as a fuzzy expert system. A FORAS risk model provides a quantitative relative risk index representing an estimate of the cumulative effects of potential hazards on a single flight operation. The quantitative relative risk index generated by FORAS	Stage 4: Combine hazards into framework Stage 5: Evaluate

System)	allows comparisons between flights, and facilitates the communication of safety issues throughout the organisation.	risks (Note that Stage 6: Identify potential mitigating measures to reduce risk is part of FORAS further research)
FRAM (Functional Resonance Accident Model)	FRAM is a qualitative accident model that describes how functions of (sub)systems may under unfavourable conditions resonate and create situations that are running out of control (incidents / accidents). It can be used in the search for function (process) variations and conditions that influence each other and then may resonate in the case of risk analysis, or have resonated in the case of accident analysis. The model syntax consists of multiple hexagons that are coupled. Each hexagon represents an activity or function. The corners of each hexagon are labelled (T): Time available: This can be a constraint but can also be considered as a special kind of resource; (C): Control, i.e. that which supervises or adjusts a function. Can be plans, procedures, guidelines or other functions; (O): Output, i.e. that which is produced by function. Constitute links to subsequent functions; (R): Resource, i.e. that which is needed or consumed by function to process input (e.g., matter, energy, hardware, software, manpower); (P): Precondition, i.e. system conditions that must be fulfilled before a function can be carried out; and (I): Input, i.e. that which is used or transformed to produce the output. Constitutes the link to previous functions.	Stage 4: Combine hazards into framework
Gael Risk Analysis	Initial Review: A. The scope is determined by the customers' needs and capability recognising that one size does not fit all. At the heart of the Gael Risk solution is an assessment of the organisation support for risk management, an assessment of the assurance framework to maintain an effective management system on an on-going basis and a review of its capability to effectively manage both individual and multiple risks from across the organisation. B. An initial review is carried out to determine the current situation and identify what is possible and practical. It seeks to identify how best to progress and, where necessary, will continue to provide guidance, support and project management services through to successful completion. C. A range of tools and techniques are used to review the current level of understanding and consistency of application of Risk Management techniques across the organisation. Where necessary, we will provide insight into how Risk Management disciplines can be of significant benefit not only in protecting value and in managing uncertainty, but also in decision making, delivering business objectives and in creating value across the organisation. D. Access to the most senior of executives and also to those responsible for managing key disciplines to judge consistency of understanding and application. It requires a review of past records associated with incidents, audits and competencies. Strategic Review: Having established a baseline of the current situation a strategic review is carried out with relevant stakeholders to identify and agree what would be of benefit to the organisation having considered need, resources, capability and desire. Ultimately this exercise provides an assessment report highlighting understanding, consistency, needs, gaps and recommendations.	Potentially all Stages

	In addition this report provides a clear picture of what can be achieved, the end goal, the road ahead, the steps needed to make progress and the resources, commitment and executive management support to make it happen. Roadmap Preparation: If the project is seen as viable a roadmap is prepared identifying how progress can be made to progress the organisation from the current situation to where it ultimately wants to be. A key component is in identifying the deliverables and milestones to make that possible. The roadmap makes it clear how best to proceed to ultimately deliver the end objective(s) given the resources available and constraints in place. It also serves to provide direction and focus along the way. Project Delivery: Gael provides the option to leave the project with the internal team to deliver or to assist with a range of interactions from occasional progress reviews through to complete project management or in supplying all appropriate resources to achieve milestones and successful conclusion. The level of involvement is determined by the needs, capability and desire of the organisation. Addresses: Uncertainty http://www.gaelrisk.com	
HAZOP (Hazard and Operability study)	Group review using structured brainstorming using keywords such as NONE, REVERSE, LESS, LATER THAN, PART OF, MORE. Aim is to discover potential hazards, operability problems and potential deviations from intended operation conditions. Also establishes likelihood and consequence of event. Hazardous events on the system should be identified with other technique.	Stage 3: Identify hazards
HRA (Human Reliability Assessment)	The likelihood of a human error in a task is directly related to the way the task itself is designed and the quality of the following key factors: • Workplace design (including the working environment, tools, controls, displays etc.), • Documentation (written procedures, signs, labels) and • Operator competence (level of training, qualification, experience etc. in the task) Human reliability analysis is used to gather and present information on these factors in a logical way. Organisations use human reliability analysis to examine the extent to which they have those factors under good control. If the level of control (and therefore human reliability) can be improved, the analysis will point to how this can be achieved. Certain techniques can generate 'human error probabilities' for tasks giving an estimate of the chance of a human error.	Stage 4: Combine hazards into framework Stage 5: Evaluate risks Stage 6 - Identify potential risk controls
HEMECA (for human related hazards)	A Human Error Mode, Effect and Criticality Analysis is an FMECA-type approach to human error analysis. It uses a Hierarchical Task Analysis (HTA) followed by error identification and error reduction. Performance Shaping Factors PSF (Performance Shaping Factors) used by the analyst are primarily man-machine interface related, e.g. workplace layout, information presentation, etc. Each task is assessed for possible human errors, and for each error it is determined what the effects are and how critical these effects are. Criticality is defined as the combination of the probability of the error	Stage 3: Identify hazards Stage 5: Assess risks (criticality)

	and the severity of its effect. Typically, an FMEA approach identifies many errors, primarily through detailed consideration of these PSF in the context of the system design.	
IRP (Integrated Risk Picture)	Intends to provide an integrated risk picture for the current and an adopted (2015) ATM concept using fault tree analysis [IRP, 2006]. Starting point is a fault tree for the current situation. The predictive IRP for the adopted 2015 ATM concept uses a 4-stage approach: Stage 1: Identify the future ATM situation, i.e. identify the ATM changes that might be implemented in Europe the period up to 2020. Use HAZOPs and on-going safety assessments for the different future ATM components to identify which aspects will positively influence safety, and which aspects will negatively influence safety (hazards). Stage 2: Make a functional model including the main actors, the information flow between them, and interdependencies, for the future situation, using SADT (Structured Analysis and Design Technique). Stage 3: Use this and the current risk fault tree to evaluate the future situation. Stage 4: Refine and quantify the future IRP by assessing correlated modification factors for the values in the IRP fault tree and the IRP influence model, thus modelling positive interactions, negative interactions, and migration of risk. The current risk IRP [IRP, 2005] accumulates overall risk from five kinds of accident risk categories (CFIT, Taxiway collision, Mid-air collision, Runway collision, Wake turbulence). For each category there is a fault tree that represents the specific causal factors. And below each fault tree there is an influence model that is used to represent more diffuse factors such as quality of safety management, human performance, etc. Quantification is done by mixture of historical data and expert judgement. Specifically it is capable of showing: • the overall, positive contribution of ATM to aviation safety - ie the reduction in pre-existing accident risk that is inherent in aviation • the negative contribution of ATM to the risk of an accident the relative importance of different accident categories and the causal factors underlying the ATM contribution to risk • the relative importance of the different phases of flight - e.g. the influences of strategic versus tactical conflict management on safety • how that above points might change in the future and where risk-reduction effort should be expended • the effects of interdependencies between different ATM sub-systems the safety impacts of changes to the ATM system that are planned for other (e.g. capacity) reasons. The IRP model is deductive in the sense that it based on real, historical accident and incident data. However, in order to meet the above objectives, it has been developed such that it can also be used inductively – i.e. to predict what effect changes postulated for the future ATM system would have on the accident and incident rate.	Stage 2: Learn the normal operation Stage 3: Identify hazards Stage 4: Combine hazards into risk framework (dynamic) Stage 5: Evaluate risks
MASCA (Managing System Change in Aviation	MASCA proposes to deliver a structure to manage the acquisition and retention of skills and knowledge, through training on organisational processes for managing organisational change in the 'whole air transport system.' Different stakeholders in a common operational system (airlines, airports, maintenance companies, etc.) will come together to change the shared operational system to deliver a better service. An Original Equipment Manufacturer (OEM), and software designer will offer technology solutions that support more effective	Stage 8: Organisational learning

	integrated operations. The work programme takes an action research approach with a primary focus on the transfer of change management capability into the organisations that are responsible for and involved in change. It is organised in 7 work packages to deliver two complementary objectives: • The development of a system to deploy an integrated change management capability (Change Management System - CMS) • The deployment and evaluation of the CMS in selected change management initiatives, both simulated and actual.	
Multi Agent Dynamic Risk Modelling	Multi-agent Dynamic Risk Modelling uses scenario-based Monte Carlo simulations and uncertainty evaluations to analyse the safety risk of future or current air traffic operations. It includes the development of a Multi-Agent Dynamic Risk Model scenario, which defines the stochastic dynamics of agents (human operators and technical systems), using a compositional specification. Within this formalism a hierarchically structured representation of the agents in the scenario is developed, including: Key aspects of the agents; Modes within the key aspects of agents; Dynamics within modes; Interactions between modes within key aspects; Interactions between key aspects of an agent; Interactions between agents. Here, the dynamics and interactions include deterministic and stochastic relationships, as is appropriate for the human performance or system considered. The methodology incorporates a risk bias and uncertainty assessment, including sensitivity analysis, which gives insight into the extent to which the various agents contribute to both safety and safety risk.	Stage 1: Scoping Stage 2: Learning the normal operation Stage 3: Identify hazards Stage 4: Combine hazards into risk framework Stage 5: Evaluate risk Stage 6 - Identify potential risk controls Stage 8: Organisational learning
NextGen Future Safety Assessment Game	NextGen Future Safety Assessment Game is A method to generate a holistic approach to alternative subject-matter expert (SME) elicitation and data collection for future socio-technical systems. The methodology is tailored to future air traffic management decision-making environments. The methodology for estimating risks within a future system combines various approaches. Because the air transportation system includes extensive interactions between multiple stakeholders, which can be difficult to track, and because of the lack of historical data, SMEs from diverse backgrounds are the main source of data for this study.	Stage 4: Combine hazards into risk framework Stage 5: Evaluate risks
Petri Nets	A Petri Net is a graphical and mathematical instrument to model discrete event systems. It consists of places (circles), transitions (squares) and arcs (arrows) that connect them. A token inside a place denotes that the corresponding discrete state is the current one. Petri Nets can be used to model system components, or sub-systems at a wide range of abstraction levels; e.g. conceptual, top-down, detail design, or actual implementations of hardware, software or combinations.	Stage 4: Combine hazards into risk framework
PHA (Preliminary	Identification of unwanted consequences for people as result of dysfunctions of the system. Aim is to determine during system concept or early development the hazards that could be present in the operational system in order to establish courses of action. PHA	Stage 3: Identify hazards

Hazard Analysis)	was introduced in 1966 after the US Department of Defence requested safety studies to be performed at all stages of product development. PHA is considered for specification of systems that are not similar to those already in operation and from which much experience has been gained. Design and development phase. Use with FTA, FMEA, HAZOP. Initial effort in hazard analysis during system design phase. Emphasis on the hazard and its effects. Inductive and deductive.	
PRA (Probabilistic Risk Assessment based on FTA/ETA)	A Probabilistic Risk Assessment uses a combination of event trees and fault trees to analyse the risks associated with a particular system. Event trees represent possible accident scenarios and each event in the event trees is represented as a fault tree. PRAs are used extensively for analysis of risks associated with nuclear power plants.	Stage 4: Risk Framework & Risk Model (dynamic) Stage 5: Evaluate risks
PSSA (Preliminary System Safety Assessment) according to ARP 4761	The PSSA according to ARP 4761 establishes specific system and item safety requirements and provides preliminary indication that the anticipated system architecture can meet those safety requirements. The PSSA is updated throughout the system development process. A PSSA is used to ensure completeness of the failure conditions list from the FHA and complete the safety requirements. It is also used to demonstrate how the system will meet the qualitative and quantitative requirements for the various failure conditions identified.	Stage 4: Combine hazards into framework Stage 5: Evaluate risk Stage 6 - Identify potential risk controls
Pure Hazard Brainstorming	Hazard identification through brain storming with subject matter experts. Scenarios are often used to structure the brainstorming. Rule 1: no analysis during the session and no solving of hazards; Rule 2: criticism is forbidden; Rule 3: use a small group; Rule 4: brainstormers should not be involved in the operation's development; they need to play devil's advocates; current expertise is better than past experience; Rule 5: moderator should watch the basic rules; should make the brainstorm as productive as possible; needs to steer the hazard identification subtly; write short notes on flip-over or via beamer; Rule 6: short sessions and many coffee breaks and...bottles of wine for the most creative hazard; the last hazard; and inspiration, if necessary. An augmented version of brainstorming analysis enables identification of hazards that are difficult to identify using a functional approach.	Stage 3: Identify hazards
Quantification of systemic risk and stability: New methods and measures	Predicting the "next" recession or crisis becomes simply equivalent to determining the probability of and risk interval for the "next" event or outcome. This probability must be based on relevant and correlated measures for experience and risk exposure, which include the presence or absence of learning. Risk is caused by our uncertainty, and the measure of uncertainty is probability. The risk of an outcome (accident, event, error or failure) is never zero, and the possibility of an outcome always exists, with a chance given by the future (posterior) probability. The key is to include the human involvement, and to create and use the correct and relevant measures for experience, learning, complexity and risk exposure. The measure adopted and used and relevant for estimating risk exposure is key. Over some seven to eight decades (orders of magnitude) variation in the rate and in the risk exposure or accumulated experience, for the rare event the negligible learning	Stage 5: Evaluate risk

	prediction holds. At any future experience or risk exposure, the error (or uncertainty) in the risk prediction is evidently about a factor of 10 in future crisis occurrence probability, and about a factor of two in average crisis frequency.	
Risk AHP Method	The Risk AHP Method utilises an Analytical Hierarchy Process (AHP) to separately rate likelihood and impact of risks. Under "likelihood" the method uses hazards and controls. The "impact" element can take on board a variety of factors not just a single dimension of risk. The outcome is an overall prioritization of undesirable events.	Stage 5: Evaluate risks
SAFMAC (SAFety validation framework for MAjor Changes)	SAFMAC: The SAFety validation framework for MAjor Changes Framework provides a framework for the development of a validated operational concept for a major change in air transport operations. It combines four synchronised processes: 1) Joint goal setting by all stakeholders involved; 2) Development of operational concept; 3) Allocation of tasks and information flows to individual stakeholders; 4) Validation.	Validation framework that includes all Stages (with particular emphasis on Stage 1), but does not prescribe a specific assessment method.
Scenario Analysis	Scenario Analysis identifies and corrects hazardous situations by postulating accident scenarios where credible and physically logical. Scenario analysis relies on the asking "what if" at key phases of flight and listing the appropriate responses. The steps are: 1) Hypothesize the scenario; 2) Identify the associated hazards; 3) Estimate the credible worst-case harm that can occur; 4) Estimate the likelihood of the hypothesized scenario occurring at the level of harm (severity).	Stage 1: Scope the assessment Stage 3: Identify hazards Stage 5: Evaluate risks
SOCRATES (Socio-Organisational Contribution to Risk Assessment and the Technical Evaluation of Systems)	Analysis of organisational factors. Is intended to aid conceptualising the role that organisational factors play in shaping plant performance and how they influence risk. Developed by Idaho National Engineering and Environmental Laboratory (INEEL). According to [Oien et al, 2005], US NRC terminated the project and no final report exists.	Stage 4: Combine hazards into risk framework
STAMP (Systems-Theoretic Accident Modelling and Processes)	Accident models based on system theory consider accidents as arising from the interactions among system components and usually do not specify single causal variables or factors. Accidents are conceived as resulting not from component failures, but from inadequate control or enforcement of safety-related constraints on the design, development, and operation of the system. Safety is viewed as a control problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled. Accidents involving engineering design errors, may in turn stem from inadequate control over the development process, i.e., risk is not adequately managed in the design, implementation, and manufacturing processes. Control is also imposed by the management functions in an organisation. The role of all of these factors must be considered in accident analysis. While events reflect the effects of dysfunctional interactions	Stage 3: Identify hazards Stage 5: Assess and Evaluate Risks Stage 6 - Identify potential risk controls Stage 8: Organisational learning

	and inadequate enforcement of safety constraints, the inadequate control itself is only indirectly reflected by the events—the events are the result of the inadequate control. The control structure itself, therefore, must be examined to determine why the controls were inadequate to maintain the constraints on safety behaviour and why the events occurred—for example, why the designers arrived at an unsafe design and why management decisions were made to launch despite warnings that it might not be safe to do so. Systems are viewed, in this approach, as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. A system is not treated as static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original design must not only enforce appropriate constraints on behaviour to ensure safe operation, but it must continue to operate safely as changes and adaptations occur over time. Accidents then are viewed as the result of flawed processes involving interactions among system components, including people, societal and organisational structures, engineering activities, and physical system components. STAMP is constructed from three basic concepts: constraints, hierarchical levels of control, and process models. Safety is viewed as a control problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled. Inadequate controls or enforcement of safety-related constraints on design can result from unidentified hazards, inappropriate, ineffective or missing control actions for identified hazards, inadequate executions of control actions (communications breakdown, inadequate actuator operation & time lag), and inadequate or missing feedback (not provided in initial design, communication breakdown, time lag, and inadequate sensor operation).	
Tool for Risk Identification, Assessment, and Display (TRIAD)	The Tool for Risk Identification, Assessment and Display (TRIAD) is designed to make risk assessments for specific identifiable problems. It can be used to produce rough assessments using a limited amount of time and effort or to produce more precise estimates when the organisation is able to invest more time and resources. TRIAD has been programmed into a Microsoft Excel workbook. It has two major modules: Current Risk and Forecast Risk. TRIAD address the problem of attempting to combine ordinal scales. Because the same numerals are typically used as markers for relative positions on different scales, users are sorely tempted to treat markers with the same numerical representation as if they were identical and to perform inappropriate arithmetic operations on them. For example, individuals often attempt to multiply the ordinal ratings obtained from two different scales. In addition, TRIAD captures different possible outcomes and displays different types of consequences, and the associated confidence intervals around the estimates.	Stage 3: Identify hazards Stage 4: Combine hazards into risk framework (dynamic) Stage 5: Evaluate risks Stage 6 - Identify potential risk controls Stage 7: Safety monitoring and verification Possibly Stage 8: Organisational learning

Appendix 5: Example List of Prospective Documents

Several visions of the future, programmes and plans, research agendas and other prospective documents are published by players who shape or design the future, such as the European Commission and ACARE, SES, SESAR, NextGen, the FAA, NASA, aircraft, and equipment manufacturers, research organisations, academia, associations, etc.

These documents, plans and programmes are used to orient, drive or support the design and implementation of the future aviation system or of sub-systems at different time horizons.

The NLR FAST website (http://www.nlr-atsi.nl/fast/"prosepctive documents - placeholder) contains a list of references such as SESAR/NextGen plans, Boeing/Airbus market forecasts, etc. These point to concrete plans by aviation system stakeholders that should form the basis of safety analysis of future systems.

Several uses for these documents are suggested below:

- Cross check of current design, regulatory, and operational assumptions. How is the future changing that could invalidate the going-in assumptions?[29]
- Enhancement of the Hazards Identification and Risk Assessment and Analysis of Risk Controls (barriers) in a similar manner as the AoCs:
    - As a checklist to be used for hazard identification and risk assessment: under the conditions set in these 'Visions of the Future' (e.g. with the implementation of SESAR and NextGEN), certain hazards can disappear, other hazards can be introduced and the risks reduced, augmented or modified.

      Note: Global plans like SESAR and NextGen pursue various high level *partially competing objectives* such as increasing capacity, safety, and security and reducing delays, costs and environmental impacts. *Hazards and risks can arise from the competition between objectives and the trade-offs adopted*: for instance, tailwind landings are good for noise abatement but not safety.

    - As a checklist against which the strengths of existing and planned risk controls (barriers) for positive or negative effects.[30]
- Analysis of critical functions: Interactions among these intended – and in some cases competing – 'Visions of the Future' may weaken critical functions that must be maintained to ensure safe operations. Critical functions are defined as potential pathways leading to successful management of emerging risk rather than simply preventing failure.

It will be clear to users of this EME1.1 methodology that the reference documents present a varied and in some cases differing view of the future. It will be a non-trivial

[29] Similar to the findings of the Boeing study about how changing operational usage, environment, personnel demographics, and evolving infrastructure rendered original design assumptions invalid.

[30] Similar to the work that FAST conducted in 2012 for the CAST Joint Implementation Data Analysis Team (JIMDAT) on the vulnerabilities of current CAST Safety Enhancements.

task to synthesise these documents into a common vision for how the future will evolve given the complexity of the operational concepts identified in them, the geographical differences that exist across implementing stakeholder organisations, and the uncertain nature of technology evolution in the modern world.

A set of website links to various descriptions of the future can be found on http://www.nlr-atsi.nl/fast/documentation. These will be regularly updated.

Appendix 6: Interaction Analysis and Prospective Safety

The aviation system involves a complex interaction among human and non-human agents operated by a wide range of different stakeholders (authorities, manufacturers, airlines, airports, ANSPs, MROs, etc.). Each organisation is responsible for managing the hazards that fall within its managerial control, but that organisation should also co-operate with other stakeholders to help manage interactions, interfaces, and changes using tools such as Safety Management Systems[31]. Combinations of individual lower-rated hazards may develop into a combined hazard that bring significantly more risk to the system.

When identifying and evaluating interactions, physical interactions may not be adequately modelled by "process tools" and vice versa. The interactions discussion below is relevant to a number of stages within the Safety Assessment process.

The major forms of interactions that must be evaluated fall into three broad categories:

Interactions between the various actors and system elements: A fundamental premise of this category is that major hazards can arise at the interactions between the vision of the future system and its human/organisational actors. Here, the dynamics and interactions include deterministic and stochastic relationships, as is appropriate for the human performance or system considered.

Interaction of Controls and Mitigations: The synergistic interactions among controls and mitigations for identified and future can create a whole new set of hazards. For example, multiple caution and warning systems on the flight deck - intended to alert the crew to undesired conditions and events - have contributed to loss of aircraft energy state awareness and resulted in high-visibility historic accidents and incidents. Hazards identification should be repeated when risk control measures have been identified in order to detect unforeseen interactions between such measures and other elements of the system or in the light of the outcomes of internal investigations[32]; this would imply iterating from Stage 6 (below) back to Stage 3.

Interaction of Contributing Factors: A repeatable framework is needed to reliably assess the interactions among hazards, risks, and projected characteristics of the future aviation system and the environment in which it will operate. The difficult identification and quantification of causal links – interactions - between components of complex systems presents significant risk assessment challenges. Assessments that do not appreciate or reflect the

[31] *Safety Management System and Safety Culture Working Group (SMS WG), GUIDANCE ON HAZARDS IDENTIFICATION*, ECAST/European Safety Strategy Initiative.

[32] Section 3.3: Hazards Identification Documentation and Review, *Safety Management System and Safety Culture Working Group (SMS WG), GUIDANCE ON HAZARDS IDENTIFICATION*.

consequences of complexity will not be fully informative and can lead to inappropriate trade-offs and increases in other risks[33].

Depending on the resources available to the analysis team, several potential systematic methods for performing the interaction assessment are included in the methods described in Appendix 4. Among these techniques is **Cross Impact Analysis**, a methodology developed to help determine how relationships between events would impact resulting events and reduce uncertainty in the future.

Retrospective hazard identification can also be a useful tool for identifying trends leading to future hazards. This can be accomplished for instance using data-mining techniques. Data mining is a generic term for systematically analysing large amounts of data to find previously unknown trends, patterns or associations. State-of-the-art methods are being developed to identify non-prescribed patterns of atypicality and novel interrelationships that may be indictors of emerging risk. Automated queries of large, heterogeneous datasets can thus reveal interrelationships not capable of being identified by human analysis or safety models.

Hazard identification shouldn't however be solely based on retrospection:

Limits of Retrospective Assessment

A challenge for proactive safety assessment of future systems is overcoming the shortcomings of approaches based on retrospective analysis of the accident, incident, and operational data within the well-known Heinrich pyramid. This pyramid theory postulates that the number of events occurring in a lower level of the pyramid is a precursor for the number of events occurring in the level above. As both the reliability of components/systems and the complexity of those systems increases especially in newer fleets, the dynamic interactions and interdependencies among the technical, human, and organisational factors will become the dominant sources of risk in the future aviation system.

[33] *Risk Governance Deficits – Analysis, illustration, and recommendations*, Policy Brief, International Risk Governance Council, 2011

From a prospective viewpoint, there are weaknesses in risk analysis *based solely on event occurrences*[34]:

- Unless information across and within each level is effectively integrated, the analysis may not encourage the broad systems thinking[35].
- It is reactive to existing threats buried in mounds of data and may not be predictive beyond a near-term timescale.
- It does not have the ability to identify deep systemic problems such as organizational or external factors in the surrounding environment *that are not part of any of the datasets*.
- It captures only unsatisfactory workplace conditions and events not "system" functional problems.
- It may not fully identify mitigations for emergent hazards arising within complex systems. The demonstrated precursors of unacceptable risks today could very well be among the precursors whose confluence will influence the safety risks of the future.

Opportunities Provided by "Prospection"

The prospective approach enables teams to identify and form into a hierarchy the main strategic "stakes" – the visions and priorities of the future for aerospace companies and regulators in the evolving landscape of tactical safety. A typical "stake" may be a target level of safety (TLS) or a given percentage reduction in fatal aviation accidents or a desired increase in system throughout or flight delay reduction.

As mentioned in Section 1., a prospective approach should actually combine[36] looking forward, e.g. through forecasting, trend analysis, gaming and scenarios, futurist writing, etc., looking across, e.g. through systemic thinking, and look backwards, through historical analogy, previous future-oriented studies, trend, analysis, etc.

[34] Fletcher, Robert, *The Next Step: A Fully Integrated Global Multi-Modal Security and Safety Management System*, International System Safety Conference, 2012

[35] Many times, accident "lessons learned" have demonstrated a requirement for broad systems thinking. It can be vital to make use of broad systems thinking. Typical examples are the intricacies of ground icing accidents, the vulnerabilities of the Concorde fuel tanks to foreign object damage (FOD) from tyre propelled debris, tail strength vulnerability due to unusual pilot rudder inputs and minimum control speed in the air issues for propeller driven aircraft.

[36] *Technical Report on a Foresight Training Course*, Editors: Cristiano Cagnin and Fabiana Scapolo, European Commission Joint Research Center, PUBSY ID - EUR 22737 EN.

Appendix 7: Contributing Factors to Emerging Risk

The analysis team should compile a list of factors identified that can influence the risks that may emerge in the future system of interest including postulating how those factors may manifest themselves. The generic types of contributing factors to emerging risks from the table shown below must be constantly kept in mind during the risk assessment as a practical checklist to ensure nothing important to the assessment process is inadvertently skipped.

Tabulation of Contributing Factors to Emerging Risk[37]

Title	Relevant? Y/N	How is this manifested?
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 future risks may encounter resistance on the grounds of contested science or incompatible values.)		
6. Social dynamics changes that result in either potential harm or attenuation of those effects		
7. Technological advances that outpace scientific understanding of the risk being assumed by regulatory efforts (including new capabilities, barriers, controls, and mitigations) especially changes in how the technology is being used		

[37] *The Emergence of Risks: Contributing Factors*, Report, International Risk Governance Council, Geneva, 2010, ISBN 978-2-9700672-7-6

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 behaviours or discourage risk prevention efforts		
12. Malicious motives and acts (the 'intentional' rather than unintentional threats)		

In addition to the above sources of emerging risks, users should identify and catalogue the following key considerations that must be understood for future systems[38]. These items can serve as an additional catalyst for identification of hazards and threats within a particular system or concept of operation of interest. They can also help identify organisational vulnerabilities that may create unexpected risk.

1. Detecting "hidden" concentrations or accumulations of exposures whose size, scale and impact could have a material adverse effect;
2. Complex and "opaque" products or services which are understood by only a few experts;
3. Looking for discontinuities or tipping points which indicate either unclear "rules of the game" or a likely change;
4. Lengthy dependent "chains" of any type, since they are only as strong as the "weakest link";
5. More scenario analysis and "stress testing" outside the range of "business as usual";
6. Using approved or "certificated" products for unintended purposes outside their original certificate action. This can open a new and unforeseen sample set that can shift the norm from acceptable to unacceptable.
7. Imagining unintended consequences of public policy and regulation, and looking for connections which could arise between "seemingly unrelated" trends; and
8. Measuring trends in diverging views between groups on critical issues such as automation implementation, flight crew training and demographics, and the changing regulatory landscape. *Such diverging views, even in how to approach the risk assessment itself, can themselves be precursors to emerging risks or can complicate or delay efforts at taking precautionary or mitigation measures*.

[38] *Emerging Risks: Sources, drivers, and governance issues*, International Risk Governance Council, 2010

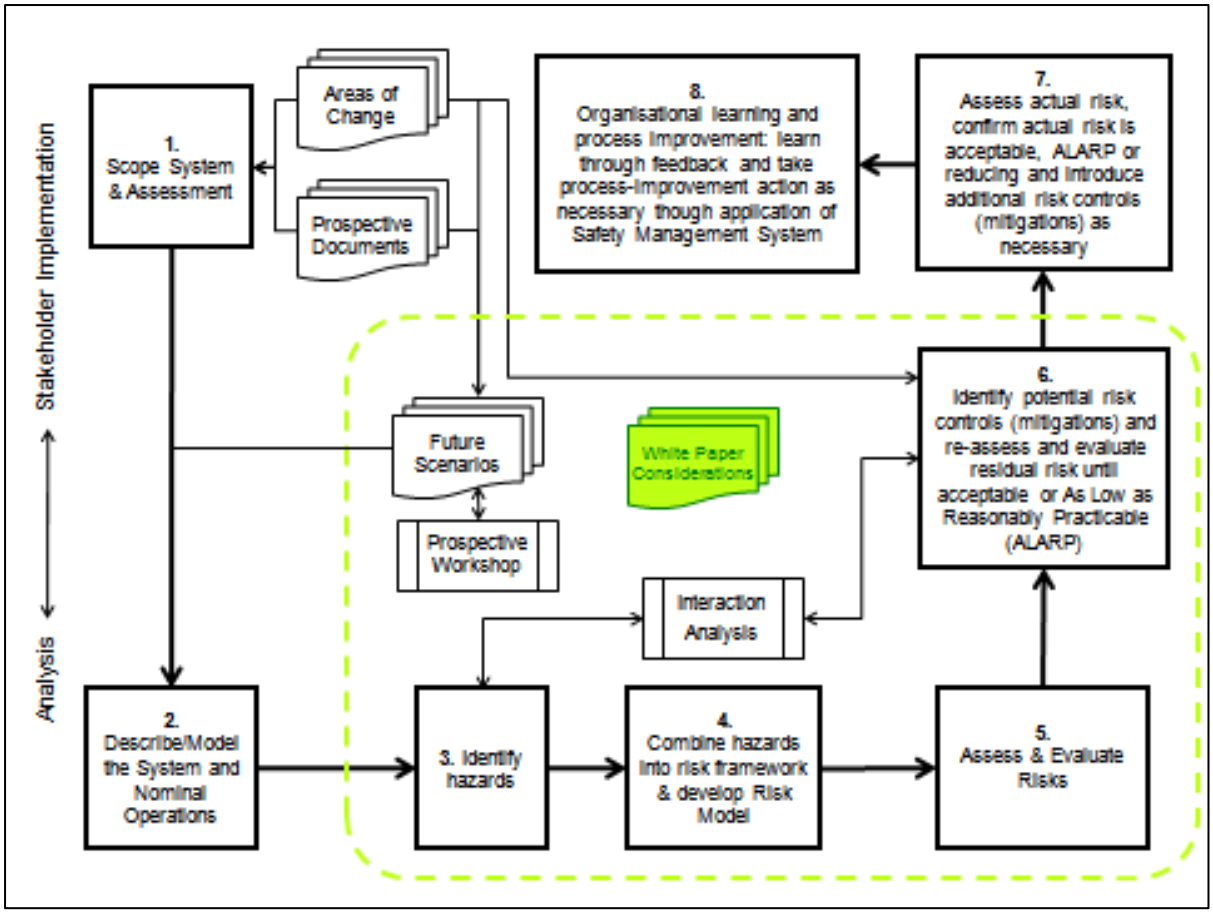
Appendix 8: Interrogatives for Assessment of Internal and External Phenomena

The analysis team should utilise the following criteria for identifying phenomena relevant to the system that is the focus of the safety assessment:

1. Does this phenomenon increase the likelihood of well-understood current hazards that will exist in the Future? If so, by what mechanism?
2. Does this phenomenon, create new hazards synergistically via interactions with other phenomena or with elements of the future system of interest that would not have come into being without the presence of the phenomenon? If so, by what mechanism?
3. Does this phenomenon increase the subjective likelihood of future hazards to an unacceptable level? If so, by what mechanism?
4. Does this phenomenon create increased potential for human error, procedural non-compliance or equipment failure? If so, by what mechanism?
5. Does this phenomenon decrease the resilience of the projected safety system? If so, by what mechanism?
6. Does this phenomenon render the projected safety systems more brittle to off-nominal conditions? If so, by what mechanism?
7. Does this phenomenon decrease safety levels during non-normal or emergency operations within the projected future system of interest? If so, by what mechanism?
8. What current and projected safety assurance measures within the future system of interest may be lost or rendered ineffective as a result of this phenomenon? If so, by what mechanism?
9. Does this phenomenon require creation of new control measures for critical aspects of the future system? (Definition: A control measure is an action or procedure that will reduce, prevent or eliminate a potential hazard.) If so, by what mechanism?
10. Does this phenomenon adversely affect critical control points or critical limits? (Definitions: A critical control point is a step at which a control measure is applied. A control limit is a maximum and/or minimum value for controlling a physical parameter.) If so, by what mechanism?
11. Will this phenomenon create new conditions that are currently not part of the design assumptions for pre-defined future systems and procedures? If so, by what mechanism?
12. Will this phenomenon result in decreased skill levels and judgment among operators of future systems? If so, by what mechanism?

Appendix 9: Enriched Process and Process Chart

An enriched version where Areas of Changes and Prospective Documents also play a role in the Definition of the Scenarios and in the Scoping of the System and of the Safety Assessment is presented below:



6. References

European Aviation Safety Plan, Edition 2011-2015, Action EME 1.1 "Methodology to assess future risks."
http://www.easa.europa.eu/sms/docs/European%20Aviation%20Safety%20Plan%20%20(EASp)%202011-2014%20v1.2.pdf

ECAST
http://www.easa.europa.eu/essi/ecast/

CAST
http://cast-safety.org/
http://www.skybrary.aero/index.php/Commercial_Aviation_Safety_Team_(CAST)
http://www.skybrary.aero/index.php/Portal:CAST_SE_Plan

FAST article on SKYbrary
http://www.skybrary.aero/index.php/Future_Aviation_Safety_Team_(FAST)

White Paper Introduction to EME1.1 Task Philosophy, Smith, B.E., NASA Ames Research Center, Bieder, C., Airbus Product Safety Department, 15 October 2011
http://www.nlr-atsi.nl/fast/Introduction_EME1dot1_7Sept2011.pdf

FAST NLR website
http://www.nlr-atsi.nl/fast/search.php

FAST Areas of Change repertoire on the NLR website
http://www.nlr-atsi.nl/fast/search.php?searchfield=%25

FAA/EUROCONTROL ATM Safety Techniques and Toolbox Safety Action Plan-15
http://www.eurocontrol.int/eec/gallery/content/public/documents/EEC_safety_documents/Safety_Techniques_and_Toolbox_2.0.pdf

The other references have been identified in the footnotes.