FAA/EUROCONTROL

Aviation System Safety Principles
Safety Action Plan-15

Authors:  
Eric Perrin (EUROCONTROL Experimental Centre)  
Barry Kirwan (EUROCONTROL Experimental Centre)  
Ronald L. Stroup (FAA)  
Michael Allocco (FAA)  
Irving C. Statler (NASA)  
Henk Blom (NLR)

Version 2.0  
June 10, 2005
Table of Contents

PREFACE .................................................................................................................................4

OBJECTIVES ..........................................................................................................................6

INTRODUCTION.........................................................................................................................6

WHAT IS SAFETY? .....................................................................................................................6

SAFETY PRINCIPLES ..............................................................................................................7

1. AVIATION [ATM AND AIRCRAFT OPERATIONS] MUST BE AND CONTINUE TO BE SAFE .................................................................................................................................11

1.1 WE MUST BUILD ON CURRENT SAFETY AND OPERATING PRACTICES .........................................................11

1.1.1 Current operations protect the system from safety-related risks (good safety results) ................................11

1.1.2 Adequate procedures are in place ...........................................................................................................11

1.1.3 Coherent Training practices are in place..................................................................................................11

1.1.4 Professional and motivated work forces value safety and construct it in operations................................12

1.1.5 Adequate safety learning practices are in place .......................................................................................12

1.1.6 ATM Characteristics ensure operation to an acceptable level of risk......................................................12

1.2 CURRENT SAFETY MUST BE ASSURED ............................................................................................13

1.2.1 Adequate identification and risk evaluation of hazards in nominal and non-nominal situations must be performed ...........................................................................................................13

1.2.2 Strategic and Tactical Safety information (trends) must be collected and analyzed ................................13

1.2.3 Action must occur before a serious safety event manifests itself ..........................................................13

1.2.4 Information and lessons learnt must be disseminated in an effective and timely manner ...................14

1.2.5 Good safety culture must exist in the industry .......................................................................................14

1.2.6 Safety training must be in place ............................................................................................................15

1.3 FUTURE SAFETY MUST BE ASSURED ............................................................................................16

1.3.1 Full lifecycle must be considered (from early stages until transition and decommissioning) .............16

1.3.2 Future risks (as yet unseen) must be identified .....................................................................................16

1.3.3 Future risks must be minimized ............................................................................................................16

1.3.4 Risks must be reduced in advance of capacity increase to maintain, at least, current level of safety. 18

1.3.5 Conflict detection capability must be improved ....................................................................................18

1.3.6 New adequate roles and working practices must be identified ................................................................18

1.3.7 Potential negative safety impacts of new and changed design must be understood and mitigated..................................................18

1.3.8 ATM must retain and improve its resilience .........................................................................................19

2. SAFETY MANAGEMENT MUST BE EFFECTIVELY ORGANIZED ..................................................19

2.1 THERE MUST BE A REAL COMMITMENT TO SAFETY ..............................................................................20

2.1.1 Organization must have a Safety Policy clearly identifying roles and responsibilities from the top downwards ...................................................................................................................................20

2.1.2 Safety progress must be measured .......................................................................................................20

2.1.3 Top management must commit to state-of-the-art safety and importance of safety ..............................21

2.1.4 Top management must understand links between safety and business (Quality and profitability of ops) .........................................................................................................................................21

2.1.5 Top management must understand risks and costs of safety ..................................................................21

2.1.6 Safety must be planned, prioritized and resourced .............................................................................22

2.1.7 Safety competence must exist in organization at appropriate levels ......................................................22

2.1.8 Safety must have high visibility and transparency ................................................................................22

2.1.9 Safety must be organized ......................................................................................................................22

2.2 SAFETY MANAGEMENT MUST BE ADAPTED TO THE NATURE OF AVIATION AND AVIATION CHANGES .............................................................................................................23

2.2.1 Aviation must be interoperable ..............................................................................................................23
2.2.2 Changing requirements have to be understood and monitored.................................................24
2.2.3 Traceability and Connectivity (high level vs. lower levels requirements) must be provided and proved..............................................................................................................................................24
2.3 SAFETY MANAGEMENT SHALL SEEK INDEPENDENT SCRUTINY ..................................................24
2.3.1 Safety documentation must be accessible and transparent....................................................25
2.3.2 Independent third party peer review of safety documentation must be conducted........25
2.3.3 Appropriate regulatory bodies must review safety documentation and conduct safety audits 25
2.4 SAFETY MANAGEMENT MUST MAKE EFFICIENT USE OF RESOURCES THROUGH CO-ORDINATION OF EFFORTS 25
2.5 AVIATION SAFETY MUST REMAIN OPEN TO EXPERIENCE IN OTHER INDUSTRY ..................25
3. BOUNDARY ASPECTS AND INTER-DEPENDENCIES BETWEEN ATM AND AIRCRAFT OPERATIONS MUST BE AND CONTINUE TO BE SAFE ........................................................................................................26
3.1 HIGHLY INTEGRATED ATM AND AIRCRAFT OPERATIONS SYSTEMS MUST BE CO-ORDINATED .......26
3.1.1 Consensus-based operational concepts and transition strategies .........................................26
3.1.2 A comprehensive and consistent set of performance standards ......................................26
3.1.3 End-to-end certification plans and operational safety assessments ..................................26
3.1.4 System element certification/acceptance ........................................................................27
3.1.5 Operational approvals ........................................................................................................27
3.2 THERE EXISTS A COMPREHENSIVE UNDERSTANDING OF ALL RISKS AND THEIR RELATIVE IMPORTANCE AND INTERDEPENDENCIES........................................................................................................27
3.2.1 There exists a formal avenue for addressing safety issues of the integrated, end-to-end system 27
3.2.2 Commitment by stakeholders to accomplish safety activities........................................28
3.3 HAZARDS AT EDGES OF SYSTEM BOUNDARIES MUST BE IDENTIFIED.................................28
3.3.1 Common cause failures affecting different parts of the system must be identified ..........28
3.3.2 Interactions between sub-systems must be captured ...........................................................29
4. CONCLUSIONS .................................................................................................................................................29
5. REFERENCES ..................................................................................................................................................30
6. ABBREVIATIONS .............................................................................................................................................32
Version 1.0 of the Aviation System Safety Principles has been developed and validated by the team members of FAA/EUROCONTROL Action Plan 15 (Safety) who are: the US Federal Aviation Administration (FAA); EUROCONTROL; the National Aeronautics and Space Administration (NASA); UK National Air Traffic Services (NATS); the French Direction des Services de la Navigation Aérienne (DSNA); and the Dutch National Aerospace Laboratory (NLR).

The Safety Principles architecture is consistent with recent experience in safety assessment and safety management of those constituent parties.

This report contains a causally-linked set of safety principles that aims at guiding formal safety management and assessment approaches.

The interdependent nature of aviation means that it is necessary for the safety principles to cover aviation as a whole. The principles form a chain of reasoning organized in a safety ‘architecture’ that substantiate the top-level proposition ‘aviation is safe’. The architecture is made of three main paths under the above mentioned top-level statement: (1) Aviation [ATM and aircraft operations] must be and continue to be safe; (2) Safety Management must be effectively organized; and (3) Boundary aspects and Inter-dependencies between ATM and aircraft operations must be and continue to be safe.

The users of this Report are invited to provide any feedback and suggestions for improvement on this current version to AP15, which will be taken into consideration for a future updated version produced.
Objectives

Introduction

Despite the initial drop in civil air traffic following 9/11, traffic is likely to continue to increase due to passenger demand, thereby putting more stress on the system. To deal with this increased capacity, there is a range of initiatives in Air Traffic Management (ATM) and in aviation more generally, such as giving the controller computerised assistance tools, considering new ways of structuring airspace and traffic flows, and delegating separation assurance in certain situations to the cockpit crew and systems. Aviation is, therefore, under pressure (capacity increases) and is undergoing an extended period of fundamental change. To anyone who has worked long enough in safety, these two ingredients mean that a serious safety system must be in place to avoid a sharp increase in safety-related events and ultimately more accidents. This requires a structured process to ensure that safety is built into conceptualisation and design phases of projects and accompanies the overall lifecycle of a system.

Aviation safety is often called ‘implicit safety’, since it resides largely in the culture of operations, rather than in the formal safety procedures and policies that may exist, or in terms of alarm systems (although some of these exist). It is recognised however, that aviation would benefit from the addition of ‘explicit’ safety measures.

What is being achieved in this report is the development of a causally-linked set of principles to guide formal safety management and assessment approaches.

A ‘Principle’ is a fundamental truth or proposition, on which many others depend. The principles, therefore, form the chain of reasoning organized in a safety ‘architecture’ and substantiate the top-level proposition ‘aviation is safe’.

What is Safety?

For the purpose of this study, the following definition of safety will be used:

- ‘Safety’ is freedom from unacceptable risk, by their elimination or control through the application of the safety order of preference.
- ‘Unacceptable’ level of risk is a level that cannot be justified to the society (this relates to societal acceptance and willingness to pay).
- ‘Risk’ is a combination of the probability of occurrence of harm and the severity of the harm.
- ‘Harm’ is physical injury or damage to the health of people either directly or indirectly as a result of damage to property or the environment.

The definitions of an accident and an incident used in this report are extracted from ICAO, Annex 13 / Doc 9713:

- An ‘accident’ is an unintended event that results in death, or serious injury, or damage, or structural failure that adversely affects the structural strength, performance or flight characteristics of the aircraft, or a missing or completely inaccessible aircraft.
- An ‘incident’ is an occurrence, other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operation.

Finally, in line with Eurocontrol Safety Regulatory Requirements 4 (ESARR4):
A 'hazard' is any condition, event, or circumstance which could induce an accident. Whether it does or not, depends on the availability of mitigation to break the sequence of events that would otherwise lead to an accident.

The Safety Principles architecture drives the need to adopt an approach to safety that considers the risk in a broad sense, including not just the risks of harm but also the perception of hazards and associated ethical and social considerations, such as aversion to multiple-fatality accidents. Consequently, the proposition ‘Aviation is safe’ is a condition in which the risk is limited to a tolerable level. Risk-based safety criteria postulate that three regions within a continuum of quantified levels of risk may be defined. This is depicted in Figure 1.

![Figure 1: Levels of Risk](image)

The three regions depicted in Figure 1 may be defined as follows: ① Unacceptable level of risk, i.e. the risk cannot be justified; ② Tolerable level of risk, i.e. attempts must be made to reduce the level of risk towards region ③, and any shortfall must be justified by the impracticality of further reducing the risk; and ③ Broadly Acceptable level of risk, i.e. the level is such that effort to achieve further reductions is likely to be grossly disproportionate (although the duty holder is still expected to demonstrate this). The value of LoR₁ (e.g. ESARR4 figure of $1.55 \times 10^{-8}$ accidents per flight hour for the most severe class) is principally concerned with the tolerability of risk. Levels of risk that are < LoR₁ are considered to be tolerable and ultimately acceptable, but where the boundary between these (LoR₂) should be is not usually specified. Reducing the level of risk towards region ③ is normally done without reference to a quantified acceptable level of risk (LoR₂), given the difficulty of assigning a value. This means that LoR₁ and LoR₂ are separated by the magnitude of the risk reduction measures that can be achieved.

**Safety Principles**

The process of developing a safety architecture started with an initial hierarchical mapping of the problems and challenges in safety. This then grew into a more formalised safety architecture, starting with the top-level proposition ‘aviation is safe’. This proposition is a formal statement of truth to be demonstrated. This proposition has been decomposed into sub-claims (sets of branches and ramifications). Therefore, the architecture provides for a structured decomposition of arguments into lower-level arguments logically. For an argument structure to be valid, it is essential to ensure that, at each level of decomposition:
• The family of arguments is sufficient to show that the parent argument is true; and
• There is no valid (negative) argument that could undermine the parent argument.

Therefore, termination points are solutions and the structure is not complete until every ramification has a solution. Having said that, it was realised in many cases that research was needed to create foundations in key areas that were otherwise unfounded. Consequently, it is intended that this report will feed forward into a Gap Analysis under Action Plan 15 (AP15). The end result is a Safety Principles Architecture made up of three main paths under “Aviation is safe”: (1) Aviation [ATM and aircraft operations] must be and continue to be safe; (2) Safety Management must be effectively organized; and (3) Boundary aspects and Inter-dependencies between ATM and aircraft operations must be and continue to be safe.

**Note:** Although the report covers ATM and aircraft operations, it is acknowledged that it is incomplete for non-ATM aspects.

Figure 2, Figure 3, and Figure 4 below show the decomposition of the proposition into sub-claims and solutions.

The various safety principles are further explained in Sections 1, 2 and 3.
Figure 2: Safety Principles architecture for Aviation (Part 1)
3. Boundary aspects and inter-dependencies between ATM & a/c ops must be and continue to be safe

Figure 3: Safety Principles architecture for Aviation (Part 2)

Figure 4: Safety Principles architecture for Aviation (Part 3)
1. **Aviation [ATM and Aircraft Operations] must be and continue to be safe**

Aviation is currently seen by other industries as a ‘High Reliability Organization’ (HRO), although it is not fully understood why aviation is so safe. Safety, in the levels of aviation, is something of an ‘emergent property’, built on the professionalism within the industry, and decades of trial and error in evolving best practices and procedures. It is obviously desirable that aviation retains this hard-won HRO status.

The Air Traffic Management (ATM) community consists of the research, acquirer and operator components of Air Traffic Service Provider (ATSP). ATM is defined by ICAO as “The aggregation of the airborne functions and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operation”. ATM systems are systems that contribute to safe movement of air traffic, including ground-based and air-based Communications, Navigation and Surveillance (CNS) equipment, and ATC-related equipment on aircraft (e.g. ACAS). The non-ATM community consists of the non-ATM related aspects of flight operations (e.g. aircraft design but excluding airspace users operational information made available to ATM systems).

1.1 We must build on current safety and operating practices

Systems and operations should be evaluated to identify, assess and document current safety levels and requirements.

1.1.1 Current operations protect the system from safety-related risks (good safety results)

A good overall system design and procedures, professional and very involved controllers, well-trained cockpit crews and good systems, and a healthy safety margin in the sky, are therefore no doubt part of the reasons aviation is safe.

1.1.2 Adequate procedures are in place

ICAO Annex 11 provides Standards and Recommended Practices (SARPs) for Air Traffic Services (ATS), whose main objectives are (a) preventing collisions (1) between aircraft, and (2) on the manoeuvring area between aircraft and obstructions; and (b) expediting and maintaining an orderly flow of air traffic. The Procedures for Air Navigation Services — Air Traffic Management (PANS-ATM, Doc 4444) specify, in greater detail than in the Standards and Recommended Practices, the actual procedures to be applied by air traffic services units in providing the various air traffic services to air traffic, and in particular the prevention of collisions between aircraft and between aircraft on the manoeuvring area and obstructions on that area.

1.1.3 Coherent Training practices are in place

The training of controllers is excellent, and the controllers themselves as a cultural entity embody the hallmarks of professionalism and care about safety. This is not surprising since controllers have safety very directly in their hands – their actions,

---

1 **Important**: Throughout this document, aircraft operations refer to the non-ATM aspects of those operations (e.g. aircraft design, airworthiness and operational approval). Collaborative Decision Making Processes to refine the planning activities are not covered by this term since they belong to the boundary aspects dealt with in Section 5.

2 It may also cover the space segments (satellite constellations) that are not under the direct control of States’ department of transport.
second to second, dictate whether aircraft stay apart or not. Additionally, it has to be said that pilots and cockpit systems (most notably TCAS, the traffic alert and collision avoidance system) add significant safety to our air travel also and are being seen as a largely independent safety net on top of those used on the ground by air traffic controllers.

1.1.4 Professional and motivated work forces value safety and construct it in operations

Aviation must remain a highly safety conscious industry.

1.1.5 Adequate safety learning practices are in place

Every day, somewhere in Europe, there is an incident we can learn from. Perhaps it contains some elements of a precursor to an accident, perhaps not. We need to know. It is necessary to record incidents, to have controllers able to report and discuss them openly, and to be able to have them analysed at a sufficient level to learn from them. There are now sufficient tools to detect incidents (losses of separation) automatically (e.g. Automatic Safety Monitoring Tool, ASMT), and sufficient analytical tools to be able to dissect them and reach both local and more widely applicable conclusions. What is missing, in many states, is the commitment and/or resource to carry out such collection and analysis.

The analysis of incidents to generate lessons for future systems and tools must be in place. This enables two things to happen: first, known problem areas should become avoidable with future systems (leading to safety progress), and second the analysts can look for ways to actually enhance safety further, perhaps going beyond the proposed system element’s original safety ‘role’.

1.1.6 ATM Characteristics ensure operation to an acceptable level of risk

ATM is made up of a number of safeguards (barriers) that prevent the precursors turning into accidents. They are the equipment, procedures, or processes that can be managed so as to minimize the risks. This includes:

- Strategic conflict management:
  - Airspace organisation and management
  - Demand and capacity balancing
  - Traffic synchronisation

- Tactical conflict management
  - Tactical separation provision (preventive)
  - Collision avoidance (recovery)

- Information services (AIS, MET etc)

1.1.6.1 Airspace design and management allow processing free from unacceptable risks

Airspace is classified to allow different types of air activity to safely co-exist. This also covers all forms of airspace structuring, routing systems and flight level conventions. Airspace management configures the airspace and route system to maximise capacity as demand changes. Rules and procedures by which airspace is structured and managed contribute to strategic conflict management.

In addition, there is a lot of space up there, even today, so there is a degree of luck or space (often called providence), which undoubtedly has occasionally saved the day.
Traffic Flow management ensures that protection matches hazards of productive ops

Traffic flow management contributes to a safe, orderly and expeditious flow of air traffic by ensuring that ATC capacity is utilised safely to the maximum extent possible, and that the traffic volume is compatible with the capacities declared by the appropriate ATC authority.

1.2 Current safety must be assured

Appropriate processes and procedures should be followed and updated when necessary. This requires, in particular, a continuous monitoring of performance against expectations.

1.2.1 Adequate identification and risk evaluation of hazards in nominal and non-nominal situations must be performed

Hazards can be deviations from standards, codes, regulations, or requirements; they can be failures within systems or human errors throughout the system life cycle, oversights, omissions, or procedural deviations, inappropriate designs, inappropriate procedures, inappropriate hazard controls, unplanned single events, or abnormal energy effects. Adequate identification, assessment, mitigation and tracking of those hazards must be performed.

1.2.2 Strategic and Tactical Safety information (trends) must be collected and analyzed

A safety learning approach must be developed to extract and record the lessons learnt from the collected data related to trends. Design and operational stages in the system lifecycle must be in a position to access such databases to see what has happened before, that is related to a particular design project or operational system.

1.2.2.1 Data collection and analysis processes must be formalized

The data collection and analysis processes must be systematic and must use a standardized taxonomy to benefit the entire aviation industry by enabling effective dissemination of safety information across the industry.

1.2.2.2 Impediments to effective data collection must be removed

It is necessary for ATM to remove certain ‘legal impediments’ that could see controllers prosecuted if they report honest mistakes. Other industries (e.g. the nuclear power industry) have this ability to collect safety information, analyse it, and share the safety knowledge. Aviation needs it, and it needs it soon.

1.2.2.3 Operationally significant events or trends (both expected/prescribed and unexpected) are extracted to identify underlying causes

Operationally significant events or trends must be investigated to determine their causes and to understand the dynamics that had occurred. The causes identified are events that must be mitigated. Analysis must proceed to the level where effective preventive measures can be specified.

1.2.3 Action must occur before a serious safety event manifests itself

With sufficient preliminary planning and correct ways of action, most incidents jeopardising safety can be avoided. Hazard identification and risk assessment are included in preliminary phases of a project. Safety work must stay connected with the real safety issues that the States’ Safety Managers are concerned with. Key
findings must be passed rapidly to the aviation industry, so they can benefit from the insights gained.

1.2.3.1 Key risk areas (urgent) are identified and resolved
Aviation must improve safety in key near-term risk areas.
There are certain ‘key risk areas’ in aviation, for example ‘level busts’, ‘interactions between safety nets’ (ground and airborne), and ‘runway incursions’. There are measures being applied to try to reduce these events, but there is also a residual uncertainty about why they occur and how to prevent them more effectively. Therefore work is required to identify short-term key risk areas, to try to understand them in terms of explicit and implicit barriers and assumptions, and reduce their risk.

1.2.3.2 Key risk areas (longer-term) are identified, monitored and resolved
Aviation must plan for key longer-term risk areas. There will also always be key risk areas that emerge during the changes, and work must be done to support better understanding and deeper treatment of such problems, so that their causes are effectively dealt with, otherwise they will re-surface as new operational and safety problems. For instance, airspace and traffic patterns lead to complexity for the controller that may lead to safety-related events.

1.2.3.3 Key risk areas are prioritized (pro-active approach to safety benefits)
Enhancements to aviation safety must be maximised in the most cost efficient manner and in the shortest possible time. Consequently, those key risk areas that will have an immediate impact on the aviation safety levels in the considered States, must be prioritized. This shall lead to a risk-informed implementation strategy.

1.2.4 Information and lessons learnt must be disseminated in an effective and timely manner
Lessons learnt from operational experience of safety-related events must be disseminated for operational, design and assessment purposes within an appropriate time-frame based on an understanding of the probability and temporal distribution (exhibited trends) of accidents.

1.2.5 Good safety culture must exist in the industry
Aviation is currently a ‘High Reliability Organisation’ (HRO). The most likely way it could lose this characteristic is via fundamental change, i.e. changes at the core of aviation (e.g. radical changes to roles and responsibilities of ATCO and air crew, radical changes to the airspace). There is an obvious need for good safety culture in operations (e.g. separation assurance). Good safety culture refers to the personal dedication and accountability of individuals engaged in any activity that has a bearing on the safe provision of air traffic services. It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters. Considering the need to identify safety critical issues early on, safety culture must also be an important aspect of conceptualization, design, development and implementation activities. It is of the utmost importance that the aviation industry strives for high levels of safety awareness, positive attitudes and continuous commitment to safety.
1.2.5.1 Commitment of Senior Management
A Safety Policy must convey the commitment of all directors and managers to achieving acceptable safety performance within the organization in a non-punitive environment.

1.2.5.2 Involvement of all employees in safety
Staff must share responsibility for improving safety. It is therefore equally important that both air carrier and ATM employees and relevant subcontractors (e.g. maintenance companies) be thoroughly versed and trained on the safety issues related to their business.

1.2.5.3 Safety management structure and procedures are in place
A management system is required for safety just as it is for other aspects of an organisation's business (e.g. financial aspects). A formal Safety Management System (SMS) is required to drive a systematic approach to safety thereby ensuring that all safety risks have been identified, assessed and satisfactorily mitigated.

1.2.5.4 There is a networking, sharing and application of best practices and lessons learnt across the industry and with other industries
Through a process of data gathering, investigation, analysis and exchange, safety professionals are able to build up knowledge and understanding of safety problems.

1.2.5.5 A non-punitive organizational culture establishes an environment built on trust
Incidents provide excellent learning opportunities. Incidents are, in any type of hazard-prone industry or organisation, a most important vehicle for safety improvement. For years now, the nuclear, chemical and oil industries have used incidents as a basis for successful prevention campaigns. Major safety improvements can be made, thanks to these lessons – lessons that need to be learned. One of the greatest impediments to good incident reporting is fear of retribution. Air traffic controllers and pilots are often afraid of the legal consequences if they report incidents. They are afraid that what they report will be used against them. In the worst case, they are afraid of legal prosecution. The implementation of a safety just-culture based on trust for data reporting and sharing must be implemented.

1.2.5.6 The industry works together as one Team and believes that effective team work improves safety
The aviation industry must work together as a team to make more explicit and comprehensive statements about the safety properties and adequacy of new systems or tools.

1.2.6 Safety training must be in place
A comprehensive system must be in place within the organization for all recruitment, training, coaching and competence activities. Training in particular, is of the utmost importance where it is impractical to eliminate risks through design selection, new procedures, or specific safety and warning devices.

1.2.6.1 Formal Training
Formal training and coaching shall be provided to a high standard using assessed internal and external resources. Licences or certificates of competence must be required for controllers, student air traffic controllers and on-the-job training
instructors to enable them to carry out their duties as already occurs in the airline industry.

1.2.6.2 Team Resource Management working practices are widely acknowledged and used
Team-working principles shall be put into practice so that the team as whole works effectively and safely, sharing information and tasks appropriately. There must be a way of auditing such practices to ensure that they are working and are resilient. It must be recognized that the team responsible for the safety of ATM includes the air carrier and the cockpit crew as well as the controller on the ground.

1.2.6.3 Adaptive training
Adaptive training is required for management, system safety working group members, safety teams, inspectors, operators, technicians, engineers, or anyone conducting activities within the program.

1.3 Future safety must be assured
Operations should be monitored to identify precursor trends and minimize future risks.

1.3.1 Full lifecycle must be considered (from early stages until transition and decommissioning)
The safety assessment stages must accompany the overall system life cycle beginning with the concept design and including transfer to operations, operations and maintenance, and decommissioning. The safety and development processes are iterative in nature. For instance, as the design evolves, changes are made and the modified design must be reassessed and the reassessment may create new design requirements that may, in turn, necessitate further design changes.

1.3.1.1 ‘Finishing touches’ that can have safety implications (positive and negative), must be managed
There is a need to ensure that new systems about to be implemented are still safe. The ‘finishing touches’ can have safety implications (positive and negative), and must be managed. A form of ‘Operational Readiness Testing’ is therefore needed.

1.3.2 Future risks (as yet unseen) must be identified
There must be an understanding of past accidents to estimate future accidents. Future accidents must be constructed in hazard analysis. In particular, for those accidents as yet unseen, contributors, combination of errors, failures and malfunctions of future systems must be comprehensively understood in order to construct future potential accident scenarios.

1.3.2.1 System-wide effects of new technologies, procedures, or training must be predicted reliably before implementation
New systems and/or changes to existing systems must be addressed from a safety viewpoint. Changes can introduce new unfamiliar risks and unless adequately analyzed they may not be adequately controlled. Procedures, tasks, and operations that are habitual may have to be changed along with the system, and as a result, error may occur and new uncontrolled risks may be introduced.

1.3.3 Future risks must be minimized
The achievement of the Target Level of Safety (TLS) under anticipated traffic conditions requires an increase in safety. Future risk must be minimized.
1.3.3.1 Application of acceptable safety assessment methodologies to all risk types at system and sub-system level

There are different ways available of carrying out some of these safety assessment tasks or functions. The globalization of aviation systems demands that common safety techniques or tools be identified to support a more efficient interoperability of safety analysis. The most suitable techniques and methods for the aviation industry (including those developed in other domains and industries such as nuclear, chemical, telecommunication, railways, and software design) must be identified and evaluated.

1.3.3.1.1 Safety assessment must be supported by adequate safety tools

The most relevant safety techniques and tools to support a holistic approach to safety assessment must be identified. A screening process must additionally identify techniques that could be significantly important for further investigation, and that can support the safety process on the longer term. The identification of new technique requirements for safety assessment comes from these sources: (i) safety assessment development (cross-boundary and ATM/aircraft operations specific); (ii) identification of gaps in methodology from incident and accident analyses; and (iii) deep analysis and understanding of the evolutions of the aviation system itself.

1.3.3.1.2 Risk assessment is supported by modelling, prototyping, simulations and trials

A combination of quantitative (e.g. mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgement) arguments can be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met. For the former, model-based simulations will essentially consist of emulating tasks and workload of the controller and pilot in the new environment. Human-in-the-loop simulations will cover real-time simulations of operations. Both model-based simulations and real-time simulation will be used to support the derivation of objectives and requirements and to provide arguments that those are met in Definition, Design, and Development and Implementation. They will enable to validate safety assumptions and requirements as identified during the risk assessment and mitigation process.

1.3.3.1.3 Quantitative safety must be supported by data

Remote, yet potentially catastrophic, events are very difficult to evaluate subjectively, which is why any useful risk picture for aviation must be quantitative. Quantifying the risk model requires data. Moreover, a separate dataset must be used to make an independent "calibration" of the risk model. Finally, beyond the use of point estimates, uncertainties in the results shall be highlighted. Probabilistic uncertainty modelling using techniques such as Monte Carlo analysis and/or illustrative sensitivity testing, showing how results vary as a result of individual changes in key data, must be used to better define uncertainties.

1.3.3.1.3.1 Reliability data exist

Reliability is, according to IEEE (Institute of Electrical & Electronics Engineers) 90 definition, the ability of a system or component to perform its required functions under stated conditions for a specified period of time. Equipment reliability data must be used – when available – to quantify equipment failures in the fault tree.

1.3.3.1.3.2 Human Errors Probabilities (HEP) database exists

Given that many of the operational errors relate to human errors of various kinds, a database of human-error probabilities and their probable causal factors must exist. To date, HEP databases (e.g. CORE-Data) essentially contains human error data that have been collected from a variety of sources through various industries. However, currently there is a lack of directly relevant data for aviation safety assessment (although, in the future CORE-DATA could be extremely useful for ATM safety assessment). Consequently, today, as the result of the relative data unavailability, generating human-reliability data is done from experts (expert judgements techniques), which can be quite unreliable when applied to new environments of design or procedures.
1.3.3.1.3 Safety occurrence data and precursors are used to develop and update design

Safety occurrence data must be used to improve design practices, so that future designs build on previous safety experience (so we do not repeat mistakes), and for improving risk assessment practices so that they remain in touch with the real types of failures/errors that actually occur.

1.3.3.1.4 Safety must be demonstrated

A Safety Case must be developed to show by means of argument and supporting evidence that the system under evaluation will be tolerably safe.

1.3.3.2 Effective learning from incident experience

Safety lessons and information must be fed into the design process throughout the design life cycle, from concept development to transition to operations.

1.3.3.3 Safety benefits pro-actively sought and ‘built-in’

The development of new concepts carries with it a responsibility to determine not only the potential weaknesses that these concepts might incur when implemented in operational centres and cockpits, but also the safety benefits of those concepts.

1.3.3.4 Quantitative demonstration that new development add safety in the larger aviation picture

How the risks from all the various aviation changes will add up and interact must be considered. Such an ‘integrated risk assessment’ must show not only the interactions, but also the dependencies between different aviation components. The resulting integrated risk ‘picture’ must demonstrate the relative benefits of each proposed change, and also show where safety needs most improvement.

1.3.4 Risks must be reduced in advance of capacity increase to maintain, at least, current level of safety.

If capacity doubles by 2015 as is projected, the rate of accidents per flight hour must be halved. It cannot simply be assumed that this can be achieved by trying harder. There must be a strategic planning of safety benefits of the various changes being introduced in the gate-to-gate ATM process so that these safety benefits are realised. Achieving future safety objectives must be afforded the highest priority with respect to commercial, operational, environmental or social pressures.

1.3.5 Conflict detection capability must be improved

As all current (ground and air) safety net barriers are very close to an accident in temporal terms, more medium-term conflict reduction tools must be identified to reduce the reliance and ‘loading’ on short-term safety nets. Moreover, possible interactions of existing and future safety nets must be identified carefully.

1.3.6 New adequate roles and working practices must be identified

The most likely way aviation could lose the HRO characteristics is via fundamental changes to roles and responsibilities (e.g. for the separation assurance process). Therefore it is of the utmost importance that safety is considered to ensure that such changes will not result in losing the property of safety.

1.3.7 Potential negative safety impacts of new and changed design must be understood and mitigated

Safety impact of changes brought to aviation must be considered at every step of the design and implementation process, leaving no room for ‘latent’ problems to
take root only to surface later as accident causes. There will also always be key risk areas that emerge during the changes, and safety work must support better understanding and deeper treatment of such problems, so that their causes are effectively dealt with, otherwise they will re-surface as operational and safety problems. Lastly, safety assessment needs to ensure that no change degrades the good safe performance culture that exists in the ‘Ops rooms’ and cockpits.

1.3.8 ATM must retain and improve its resilience

The challenge for safety management of future ATM is one of coping with complexity and uncertainty, since future inter-relationships must be captured, unplanned interactions must be addressed as well as many permutations and dynamicity (non-stability) in the system. The challenge for ATM Safety Management is therefore a significant one, and one with relatively little time to deliver appropriate methodologies to overcome the difficulties raised above.

1.3.8.1 Current low ATM propensity must be understood

Propensity is the likelihood of occurrence of a safety-related event during nominal (fault-free) and normal operations. The current low ATM propensity must be understood.

1.3.8.2 Current ATM resilience must be understood

Resilience is the extent to which the ATM system responds to a safety significant event without causing more such events. However, there is a lack of basic theory on why ATM is a HRO and ‘resilient’ in safety terms. This must be understood to enable future changes to be better apprehended.

1.3.8.3 Future role of controller must remain safety prioritized (including productivity-safety trade-offs)

Safety ‘investment’ in the future must not only consider technology, it must also determine what the optimal safety role and responsibilities of the controller should be. This is particularly important since at present a significant part of ATM safety rests in the hands of controllers. This shall include productivity (i.e. capacity) trade-offs.

1.3.8.4 ATM fundamental changes (automatic tools, ATCO role, airspace structure) are captured in new design envelope

The envisaged changes fall into three major types: provision of automated tools to help the controller deal with increased traffic density and complexity; changes to airspace structures and procedures; and at least a partial delegation of responsibility for separating aircraft from the controllers to the cockpit. During these changes, it is imperative that safety is not compromised, and is actually improved against a steady rise of traffic movements.

1.3.8.5 Risk Compensation tendencies must be understood and accounted for

Potential safety problems must be carefully considered when implementing device-induced (systems, procedures) risk compensation.

2. Safety Management must be effectively organized

Safety Management conducts activities of planning, organizing, directing, coordinating, and controlling to meet objectives defined within each program safety-related attribute.
2.1 There must be a real commitment to safety

Both safety culture and safety management go hand in hand to achieving safe practices in an organization. If there is only an SMS but no real commitment to safety, then the SMS will not be effective, as decisions will not prioritise safety. Similarly, if there is a good safety culture but no SMS, then in a complex organization the way safety is applied runs the risk of being inconsistent, under or mis-resourced, and not seen as business driven.

2.1.1 Organization must have a Safety Policy clearly identifying roles and responsibilities from the top downwards

Roles and Responsibilities shall be clearly stated for each level of the organization, and executed by each level of the organization from the top downwards.

2.1.2 Safety progress must be measured

Organizations shall identify, monitor, track, analyze and investigate safety data to improve the quality of products, processes, training or services and ensures compliance with safety policy and requirements.

2.1.2.1 Tolerable level of risk has to be identified

The TLS is a fundamental quantitative safety concept in aviation. It represents the tolerable level of risk. Safety targets are what we want to make happen in the operational environment. The TLS is consequently a quantified risk level that the aviation system shall deliver. This is, therefore, a design hurdle to be considered throughout the definition, design, development, and operation cycle.

2.1.2.2 Achieved Level of Safety (ALS) must be monitored against Target Level of Safety (TLS)

The safety level that is, or would be, achieved is referred to as ALS. The Safety Case shall provide arguments and supporting evidence that the ALS is better than the TLS. This is the objective to be fulfilled by hazard analyses, safety monitoring and safety audits.

2.1.2.3 Leading and Lagging indicators are identified and monitored

Considering the life cycle of accidents, latent hazards as well as real-time unsafe acts shall be identified and addressed in hazard analyses, and control systems for monitoring performance shall be established and implemented.

2.1.2.4 Appropriate calibration of safety indicators is performed

A probability number is not always a system risk control. Reliance on probability and statistics can be inappropriate. Consider that adverse events can occur at any time and accidents are the result of many contributors, from management oversight, design error, or inappropriate assumptions, not just unsafe acts, blunders or random failures. Consequently, appropriate safety indicators shall be defined to enable further monitoring of performance against safety requirements.

2.1.2.5 Operational indicators of safety are recorded

Special safety tests shall be conducted to verify system operations. Testing of operational safety performance against requirements is a fundamental aspect associated with Hazard Tracking and Risk Resolution. Moreover, it must be remembered that changes in procedures or systems can introduce additional hazards. Operational performance, accidents, or incidents shall be tracked to determine system safety. Factors associated with system unavailability and
integrity, operational deviation, accidents, and incidents shall be identified, investigated and hazards determined.

2.1.3 Top management must commit to state-of-the-art safety and importance of safety

The Safety Policy should convey the commitment of all managers to achieving tolerable safety performance. Managers should demonstrate this commitment through visible actions (e.g. participation in safety surveys, rewarding safe decisions in the face of commercial pressures, etc.). In addition, each individual shall be responsible for the safety of his/her actions and communicate relevant safety-related information to appropriate stakeholders.

2.1.4 Top management must understand links between safety and business (Quality and profitability of ops)

Safety must be integrated into business planning and adequate resources must be allocated for current and future safety initiatives. Safety is the main consideration in any activity undertaken by the organization. Safety must have input to the organization’s decision process.

2.1.5 Top management must understand risks and costs of safety

The consequences of safety-related actions in terms of resources and budgets need to be integrated into business plans.

Top management must understand that risks have to be minimised “as far as is reasonably practicable”, i.e. bearing in mind the benefits flowing from its acceptance and taking into account the resources (cost, time, staff) needed for any further reduction. Finding and controlling risk early assists in seeking the lowest possible cost and increases the probability of program success and operator acceptance of the final product.

2.1.5.1 Safety must support quality and profitability of air transport

Every accident and incident that jeopardises safety is a disruption to the aviation community. By acting safely and investing in the promotion of safety, we support the quality and profitability of operations.

2.1.5.2 Safety culture must be measured and increased

Safety Management Systems only work effectively when safety awareness is embedded into the operating culture. This should be developed through the establishment of effective communications, lesson dissemination, safety promotions and behavioural programmes. Safety culture builds on a voluntary reporting system in a non-punitive environment.

2.1.5.2.1 Safety implications of management decisions must be understood

Some accidents are very simplistic in logic since they appear to be the result of a single event or single point failure but upon investigation there may have been many systemic problems that initiated the so-called “single event”. For example, consider initiators that stem from management oversight, risk misperception, or LTA resources. There are latent hazards that should be considered. Consequently, managers who make decisions that can affect safety must understand and accept problems that stem from their decisions. This will ensure that they can predict the outcomes of such decisions.

2.1.5.2.2 Safety must move from implicit to explicit consideration

Implicit safety is less amenable to management. To help ensure that aviation is not losing its status as a HRO, measures including formal safety management systems, risk
assessment approaches and attempts to develop an industrial safety learning system, must be taken.

2.1.5.2.3 A "Just-Culture" needs to be implemented across the organisation/industry

A "Just-Culture" in safety reporting is required. “A “Just Culture” is an atmosphere of trust in which people are encouraged to provide essential safety-related information, and in which they are clear about where the line must be drawn between acceptable and unacceptable behaviour.”, (James Reason, 1997). What makes a just-culture is threefold: (1) Unsafe acts (errors and violations) must be understood in order to minimize their re-occurrences; (2) Wilful violations and reckless conducts cannot be tolerated; and (3) The workforce knows and agrees on what is acceptable and unacceptable.

2.1.5.3 Safety is for the benefit of the customer, employee, and other Stakeholders

Safety expertise and ways of action help reduce customers’ safety risks.

2.1.6 Safety must be planned, prioritized and resourced

Safety guidance shall integrate organized safety policies, procedures and processes for accomplishing safety in an efficient manner.

2.1.6.1 Staff must commit to safety

All members of staff should be well informed and recognise their contribution to safety performance.

2.1.6.2 Contractors and partners must adopt similar safety principles

Contractors and other co-operation partners shall be required to follow the agreed safety principles when performing work and services. When choosing co-operations partners, their safety performance shall be considered in order to find partners that meet the set requirements, and that provide good safety management.

2.1.7 Safety competence must exist in organization at appropriate levels

The organization shall develop a Human Capital Plan for safety that addresses core competencies in the safety field.

2.1.8 Safety must have high visibility and transparency

Top management shall foster safety by establishing unambiguous policy, allocating adequate resources and promoting open communications.

2.1.9 Safety must be organized

To be effective, a safety program must be part of an integrated group of management policies and processes that form an overall governance structure.

2.1.9.1 Safety must be integrated into system changes and modernization programs

System safety management must ensure that system safety is effectively integrated into system changes and modernization programs in accordance with Safety Management System (SMS) guidance, and Acquisition Management System (AMS) policy. The main purpose is to identify, evaluate and eliminate or control system hazards during the lifecycle of a given program or system.

2.1.9.2 Safety R&D must be organized for efficiency and effectiveness

It has been estimated that about 50% to 60% of accidents appear to have their roots in the conceptualization, design and early development processes, across a range of industries including aviation. It is, therefore, imperative that safety
assessments and assurance accompany the early phases of development of operational and system views, thereby ensuring that safety and human factors best practices are integrated into the design and development processes themselves. This requires that lessons learnt from weaknesses as evidenced in aviation accidents and incidents are analyzed and fed back into design to ensure that vulnerabilities in the present aviation system can be rectified wherever possible. In fact, R&D to increase safety covers both the conduct of safety R&D and safety evaluation of R&D to enable full-scope assessment of the future aviation system. Safety R&D shall address the need to adopt, develop where needed and maintain appropriate safety assessment methods that help R&D to predict potential safety performance of proposed aviation enhancement.

2.1.9.2.1 Both the safety benefits and the weaknesses that new concepts might incur must be determined

The development of new aviation concepts carries with it a responsibility to determine both the safety benefits of those concepts and the potential weaknesses that these concepts might incur.

2.1.9.2.2 Safety information must be fed forward to industrial Stakeholders and ANSPs

This safety information must be fed forward to all Stakeholders including standardisation and regulatory bodies, industry, airspace users and ANSPs. In particular, safety R&D shall have a sound understanding of safety issues, shall lead to effective methods to analyze risk and assure safety via assessment and design practices, and shall then integrate such work to deliver to the above mentioned bodies the safety requirements for the future.

2.1.9.2.3 The SMS must be tailored to actual R&D activities

Whilst having an SMS is considered best practice, it is less common for a R&D organization to have an SMS that can have a real impact on the safety of its products. The SMS needs to be adapted to the validation of applied and innovative R & D activities; both to make sure that the SMS is tailored to the actual research activities and existing processes, and also to ensure the R&D body does not simply end up with more bureaucracy, which actually adds little safety value.

2.2 Safety Management must be adapted to the nature of aviation and aviation changes

Safety Management can only provide a means of controlling hazards that originate within the aviation system, or to which some element of the aviation system is a contributory factor. The evaluation of the overall safety of aviation must take into account any impact of safety that could arise from externally provided service.

2.2.1 Aviation must be interoperable

Interoperability and standards development in the aviation industry must be promoted to ensure that aviation systems of the future can communicate with each other.

2.2.1.1 Aviation must be internationally co-ordinated (standards and recommended practices) and must be viewed from a global perspective.

All elements of aviation system must interlock properly to enable aviation to remain a safe industry. A better understanding and handling of interfaces is required. In order to avoid ending up with wide variations in national standards and requirements satisfying the high level objectives set up in safety regulations – which ultimately will lead to a non-homogeneous, fragmented implementations of systems – there is a need to produce a global safety standard – referred to as safety interoperability standard - that will: (i) dictate the safety functions and performance that the system and sub-systems shall deliver; (ii) drive the design
and development of constituent parts (equipment, procedures, human operators) of the overall system; and (iii) ensure that national safety management standards and resources will not range from very good to inadequate. There must be a process that will lead to the elaboration of Safety Interoperability Standards. In particular, requirements for additional Standards and Recommended Practices (SARPs) in appropriate ICAO Annexes must be identified. The Safety Interoperability Standards shall cover: Air Traffic Control, aircraft operation, airport operations, manufacturing, rulemaking/certification/validation, maintenance activities, technicians/ATC Controllers/flight crew training, etc.

2.2.1.2 Integrative safety approach must be applied

The safety approach must be holistic. It shall cover the entire aviation system. It shall cover both the aircraft design and the operations of the customers of ATM as well as the ATM layers. Those layers shall cover the entire ATM service, i.e. everything ATM supplies to the pilot. This includes:

- Strategic conflict management:
  - Airspace organisation and management
  - Demand and capacity balancing
  - Traffic synchronisation

- Tactical conflict management
  - Tactical separation provision (preventive)
  - Collision avoidance (recovery)

- Information services (AIS, MET etc)

The safety work shall cover all aviation systems, i.e. everything that contributes to safe movement of air traffic, including space-based, ground-based and air-based Communications, Navigation and Surveillance (CNS) equipment.

The safety work shall cover equipment, procedural and human-related issues. General ATM safety management, including safety culture and the organisational contribution to accidents, are also covered in outline.

The safety work shall cover the gate-to-gate aviation cycle. It is considered to start at the moment the user first interacts with ATM and ends with the switch-off of the engines.

2.2.2 Changing requirements have to be understood and monitored

Safety requirements must be implemented in the design of the aviation system. Since the development process is iterative in nature – as the design evolves, changes are made - the safety significance of those changes must be reassessed continuously.

2.2.3 Traceability and Connectivity (high level vs. lower levels requirements) must be provided and proved

The concept of traceability involves providing (or proving) the connectivity between the higher-level through lower-level requirements. This system engineering or management process should also be documented within the program.

2.3 Safety Management shall seek independent scrutiny

In those States where the Civil Aviation Authority (CAA) acts as both the regulator and air traffic service provider, it is important that a clear separation between the
air traffic service provision function and the air traffic safety regulatory function be maintained. The safety regulation of the service provision should be conducted as though the service provider was an external entity in order to maintain the independence of the regulatory function. This also covers multi-States Agency that a) draws-up common standards to ensure the highest level of safety; b) oversees their uniform application across those states and; c) promotes them at world level. Moreover, with the need for the safety culture to rely on a voluntary reporting in the required non-punitive environment, the separation must be maintained of such a safety culture from the responsibilities of the regulatory agency.

2.3.1 Safety documentation must be accessible and transparent

Arrangements must be in place for all necessary staff to have access to relevant safety management and safety technical information.

2.3.2 Independent third party peer review of safety documentation must be conducted

To insure that the safety document is based on the best scientific information and judgments, a non-profit organization shall conduct an independent peer review.

2.3.3 Appropriate regulatory bodies must review safety documentation and conduct safety audits

National authorities must take up the duty of safety oversight (including safety audits). *i.e.* safety validation. This is usually an audit against documented procedures.

2.3.3.1 Internal Regulatory Body

Internal to the organization, but separated from the service provision side, an internal independent body must provide advice in order to ensure consistent high levels of safety with other aviation bodies. The internal regulatory body must undertake work in the field of setting and implementation of harmonised safety regulatory objectives and requirements for aviation.

2.3.3.2 External Regulatory Body

Each State shall establish an appropriate state organ/agency referred to as the Civil Aviation Authority with the necessary empowerment to ensure compliance with the air navigation’s operating safety regulations promulgated.

2.4 Safety Management must make efficient use of resources through co-ordination of efforts

Standards and procedures across aviation must be harmonised thereby minimizing development effort and ensuring transferable resources and knowledge.

2.5 Aviation Safety must remain open to experience in other industry

Safety learning must be shared with the overall aviation industry and other industries.
3. Boundary aspects and inter-dependencies between ATM and aircraft operations must be and continue to be safe

The interdependent nature of aviation means that it is necessary for the system and operational views as well as for the risk model to cover aviation as a whole.

3.1 Highly integrated ATM and aircraft operations systems must be co-ordinated

The overall approach to safety and how the various safety activities integrate shall support the delivery of the future safe aviation system. This implies a holistic approach to aviation system safety. Moreover, studies have shown that major contributing elements to accidents and incidents are failures at the interfaces within the aviation system. This covers intra-organizational and communication interface problems that had a direct and immediate impact on flight safety, which were identified within flight operations and within ATC. The degree of interdependence between ground-based and airborne components becomes more significant in the development of the future operational concept, thereby creating more technical and operational interfaces. Consequently, there is a need to federate all the air transport stakeholders to enable:

3.1.1 Consensus-based operational concepts and transition strategies

The new vision of aviation will not happen overnight, but will inevitably occur in phases. A risk-informed transition strategy shall therefore be developed to ensure a safe sequence of implementation. This shall lead to a ‘roadmap’ (Master Plan) for achieving safety in future aviation.

3.1.2 A comprehensive and consistent set of performance standards

Aviation safety targets must be consistent. Consistency ensures that resources can be allocated in areas where they will be most beneficial in reducing the aviation risk. A top-down methodology for the definition of safety performance requirements for the various elements of the future aviation system is required. A piecemeal approach shall be avoided.

3.1.2.1 ATM service-based requirements

The top-down methodology shall lead to safety minima for ATM-related events that (1) are fully co-ordinated with aircraft operations safety performance requirements; and (2) enable safety improvement across the whole range of aviation.

3.1.2.2 Aircraft operations performance requirements

The top-down methodology shall lead to safety minima for aircraft operations-related events that (1) are fully co-ordinated with ATM safety performance requirements; and (2) enable safety improvement across the whole range of aviation.

3.1.3 End-to-end certification plans and operational safety assessments

Certification processes for ground and air systems must account for interactions between air and ground systems. This means, for example, that systems destined for the cockpit or aircraft must consider potential impact on the controller working methods and ground system performance. Overall there is a need for more unified air-ground operational safety assurance / certification approach, one focusing on
the whole system as embodied currently by ATM and aircraft airworthiness/operational validation.

3.1.4 System element certification/acceptance

To date, mechanisms for safety certification, validation, monitoring through occurrence reporting systems are fragmented in the various aviation arenas. The successful implementation of a high performance aviation system requires a change in the existing regulatory environment – that should be global in nature – to ensure that safety requirements are implemented harmoniously. This work shall lead to recommendations for an integrated approach to safety regulation (EUROCONTROL, FAA, EU, EASA, national regulatory bodies). In particular, requirements for additional SARPs in appropriate ICAO Annexes will be identified.

3.1.5 Operational approvals

The safety question is reduced to its essentials: can an overall system be approved for the purpose for which it was intended? This is referred to as Operational approval, i.e. the process through which a desired level of confidence in the ability of a system to operate in real-life environment may be demonstrated against a pre-defined level of functionality, operability and performance. The interdependent nature of aviation means that it will be necessary for both certification/validation and regulation to cover aviation as a whole. There is, in particular, the need for a more unified safety validation approach, i.e. one focusing on the whole system.

3.2 There exists a comprehensive understanding of all risks and their relative importance and interdependencies

There must be a risk model representing the risk of aviation. Aviation relies on the effective integration of, and communication among, multiple human and non-human agents. Consequently, the key challenge for the risk model is to construct a quantitative link between hazard risks and underlying causes, distinguishing ATM from other contributors, so that areas for risk reduction can be identified.

3.2.1 There exists a formal avenue for addressing safety issues of the integrated, end-to-end system

There must be a co-ordinated aviation attempt to address the challenges in developing an overall aviation risk model. The following challenges must be addressed:

- The complex system of safeguards intended to prevent aviation accidents means that most accidents are complex, involving a combination of failures. These are sometimes independent, and can appear extraordinary and unpredictable. In other cases, the failures are interlinked, with subtle connections to the underlying safety culture.

- Behind the proximate technical and operational causes of accidents, there are often common latent problems, including safety management, safety regulation, procedures, or training. However, these are rarely made explicit in accident investigations, and hence are difficult to substantiate. Similarly, the contribution of airspace management to failures in air traffic control is rarely identified.

- While technical systems can be modelled, with some simplification, as either working or not working, and human operators can be modelled as occasionally committing distinct errors, the underlying problems of safety management and regulation cannot be represented as simple success or failure. They do not directly cause accidents and, although they have a
strong influence on the accident risks, this influence is diffuse and difficult to define.

The risk model implementing the integrative risk approach shall provide the primary means for presenting the risk results but also the assumptions on which they depend. This is of the utmost importance when there are not sufficient data to prove whether those assumptions are valid.

3.2.2 Commitment by stakeholders to accomplish safety activities

Considering the above challenges, an aviation Safety Policy must convey the commitment of all air transport stakeholders (the Users – Commercial Air Transport, Military and General Aviation – Air Navigation Service Providers (ANSPs), Airport Authorities, FAA, EUROCONTROL, the European Aviation Safety Agency (EASA), ICAO, and Industry) to achieving tolerable safety performance.

3.3 Hazards at edges of system boundaries must be identified

An integrated risk picture is primarily one that shows the sum of the effects of all causal factors within the gate-to-gate cycle. However this is not a simple matter of adding up independently estimated parts of the risk picture because of interdependencies between them. These effects are described as cross-boundary hazards and are classified as Common-Cause Failures and Interactions.

3.3.1 Common-cause failures affecting different parts of the system must be identified

Common-cause failures are failures affecting different parts of the risk picture at once. These include:

3.3.1.1 External Events
For example, earthquakes, flooding etc. may affect nominally independent aviation sub-systems.

3.3.1.2 Human/procedural hazards
For example, deviations from standard operating procedures may invalidate several safeguards simultaneously.

3.3.1.3 Management/Organisational failures
For example, a poor safety culture in an Air Traffic Service Unit (ATSU) may create a potential for simultaneous deficiencies in diverse areas such as training, maintenance, incident reporting etc.

3.3.1.4 Common information sources
For example, future aviation concepts may involve the automated transfer of information which, if corrupted, could affect several systems simultaneously.

3.3.1.5 System design defects
Although safety is usually thought of as a property of an existing system and how it is operated, the roots of safety, and the roots of disaster, are often in the early design phases. Design and development defects may propagate up through the fault tree, and hence the (unseen) influences on intermediate events are often the combination of influences of those bottom events. Therefore there shall be positive safety features built into the design of future systems.
3.3.1.6 Manufacturing defects
This requires a structured process that fits into a design and development culture in terms of methods, data and understanding that can lead to more robust design, development and industrialization stages. Design, development and industrialization processes shall aim to be ‘resilient’ against aviation accidents.

3.3.2 Interactions between sub-systems must be captured
Those are interactions between ATM and aircraft operations sub-systems, occurring as the aviation system develops or changes.

3.3.2.1 Boundaries must be explicitly defined
The boundaries of the system under study must be unambiguously defined so that interaction and interface aspects are adequately covered. The human factors, functional and component failures, and functional relationships between components comprising the subsystems (including software) must be factored in. Ultimately, a global approach to air transport safety must consider interactions with and risks export to other modes of transport.

3.3.2.2 Positive interactions (synergies) must be identified
For example, improved information services may allow increased efficiency of several different safeguards.

3.3.2.3 Negative interactions must be identified
These are safety gains in one area that are accompanied by losses in another. For example, a new safety net may provide extra redundancy in the warning about imminent accidents, but this may induce passivity in the pilots or controllers, which may offset or even reverse the expected safety benefits. This category can also include positive interactions (net safety gains) that are not realised during the design and transition process.

3.3.2.4 Recovery potential must be evaluated
Not only hazards but recovery potential must be evaluated including trade-offs between the positive and negative interactions.

3.3.2.5 Migration of risks and risks export must be captured
Those are related to new ATM concepts implying changes in responsibility for managing hazards. Whereas migration of risks is not intended and can only be captured by monitoring safety performance, risks export is predictable in a safety case. For example, responsibility for separation may be transferred from controllers to pilots, with associated transfer of the risk of failures. Increased automation in ATM may reduce human errors by controllers but increase the importance of errors in equipment specification and design.

4. Conclusions
This Safety Principles structure provides a top-down approach from the highest proposition of ‘Aviation is safe’ down to termination points that are the foundations of the safety argument. The main high level safety principles that can stand out from the overall architecture are:

1. Aviation safety incidents are preventable
2. Safety must be built in at the early stages of aviation system design, right through to implementation, operation, maintenance and dismantling
3. Aviation must become a learning organization
4. Safety supports the quality of operations
5. Safety is a culture but relies on an organized process that clearly defines responsibilities at all levels
6. Safety is for the benefit of the aviation system
7. Aviation must be sure that the systems it is developing will deliver the required safety levels in a timely and cost-efficiently way

The use that can be made of the Aviation System Safety Principles is threefold:

1) The proposed architecture therefore enables to answer the questions: “How to ensure that the proposed changes to the aviation landscape will fulfil the future safety expectations and objectives” and “How do we know that the safety activities and initiatives will ensure safety of operation”.

2) Moreover the architecture sets out aims and expectations of the aviation industry in terms of safety management. Consequently, the tree lays out a Safety Management framework that describes the main key activities and elements to appropriately safety manage the aviation business. As such, it may be used to guide the implementation of Safety Management Systems within a range of organizations covering the research and development, industrialization, implementation and operation phases.

3) Finally, the Safety Principles can be used to derive Safety R&D work programs by comparing the present situation in terms of knowledge, tools, and practices with the ultimate situation that will enable to substantiate with factual evidences that the top proposition is true. Within the framework of the Action Plan 15 between the FAA and EUROCONTROL, this document will feed forward in a Gap Analysis yet to be conducted.

5. References
[Ref. 2] Eurocontrol Safety R&D Agreement, Eric Perrin, Barry Kirwan, Eurocontrol, 2004
[Ref. 6] ICAO Annex 11
[Ref. 7] ICAO Annex 13
[Ref. 8] ICAO Doc 4444, PANS-ATM
[Ref. 9] Proposed paper on the development of a global gate-to-gate safety assessment methodology, Presented by the Netherlands, 121st meeting of Directors General of Civil Aviation, ECAC, 2004

### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFARP</td>
<td>As Far As Reasonably Practicable</td>
</tr>
<tr>
<td>AIS</td>
<td>Aeronautical Information Service</td>
</tr>
<tr>
<td>ALS</td>
<td>Achieved Level of Safety</td>
</tr>
<tr>
<td>ANSP</td>
<td>Air Navigation Service Provider</td>
</tr>
<tr>
<td>AP15</td>
<td>FAA/EUROCONTROL Action Plan 15 (Safety)</td>
</tr>
<tr>
<td>ASMT</td>
<td>Automatic Safety Monitoring Tool</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATCO</td>
<td>Air Traffic Controller</td>
</tr>
<tr>
<td>ATM</td>
<td>Air Traffic Management</td>
</tr>
<tr>
<td>ATSU</td>
<td>Air Traffic Service Unit</td>
</tr>
<tr>
<td>CAA</td>
<td>Civil Aviation Authority</td>
</tr>
<tr>
<td>CNS</td>
<td>Communication, Navigation, Surveillance</td>
</tr>
<tr>
<td>DSNA</td>
<td>Direction des Services de la Navigation Aérienne</td>
</tr>
<tr>
<td>EASA</td>
<td>European Aviation Safety Agency</td>
</tr>
<tr>
<td>ESARR</td>
<td>EUROCONTROL Safety Regulatory Requirements</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>HEP</td>
<td>Human Error Probability</td>
</tr>
<tr>
<td>HRO</td>
<td>High Reliability Organization</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical &amp; Electronics Engineers</td>
</tr>
<tr>
<td>LoR</td>
<td>Level of Risk</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NATS</td>
<td>UK National Air Traffic Services</td>
</tr>
<tr>
<td>NLR</td>
<td>Dutch National Aerospace Laboratory</td>
</tr>
<tr>
<td>R &amp; D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>SARPs</td>
<td>Standards and Recommended Practices (ICAO)</td>
</tr>
<tr>
<td>SMS</td>
<td>Safety Management System</td>
</tr>
<tr>
<td>TCAS</td>
<td>Traffic Alert &amp; Collision Avoidance System</td>
</tr>
<tr>
<td>TLS</td>
<td>Target Level of Safety</td>
</tr>
</tbody>
</table>
FINAL PAGE (BLANK)