FAA/EUROCONTROL
ATM Safety Techniques and Toolbox

Safety Action Plan-15

Issue 2

October 3rd, 2007

Table of Contents

Summary

This document contains some of the best safety assessment techniques currently available for Air Traffic Management applications, based on the joint experience of the FAA and EUROCONTROL[1] and based on a review of more than 500 safety techniques as used in nine different industries. The result is a set of twenty-seven techniques that can be used by safety practitioners and managers to evaluate and improve safety in Air Traffic Management.

The document begins by outlining a simplified eight-stage safety assessment approach and then provides the required safety assessment techniques in a consistent template format. This template format answers basic questions such as where the technique comes from, and its maturity and life cycle stage applicability, as well as more detailed insights into the technique's process and data requirements, and practical and theoretical advantages and disadvantages.

The overall approach in this document is biased towards concept design and development phases, since the significant and fast-evolving changes ongoing today in ATM represent the major driver for system safety assessment. Nevertheless, most of the techniques can be (and often are) just as easily applied to existing systems. A good number of the techniques themselves deal with Human Factors and human error aspects of safety, as the human element is a critical determinant of safety in current and future ATM, and cannot be ignored in safety assurance activities.

Some outline examples of actual safety assessment approaches using these techniques are provided to show how techniques may be selected from the toolbox. Lastly, some key web addresses and supporting information are given for those who require further information.

[1] These two organisations would also like to acknowledge the invaluable support of other organisations including NASA, NLR, CENA, and NATS (UK).

1.0 Objective

The globalization of ATM systems demands that common safety techniques or tools be identified to support a more efficient interoperability of safety analysis. The objective of this report is to summarize and discuss both common and unique FAA and EUROCONTROL safety techniques. These safety techniques are those judged to be the best currently available. The safety techniques identified in this report are enablers to develop safety material identified in the FAA's System Safety Management Program (SSMP) or EUROCONTROL Safety Assessment Methodology (SAM). Additionally, this report attempts to increase awareness of these techniques to assist safety practitioners in the air traffic community in conducting their respective safety analysis activities. Moreover, this report will attempt to provide guidance to analysis teams in the selection of effective and applicable techniques. The application of common safety techniques will allow ATM service providers to leverage their skills, knowledge, and experience with respect to global operations and systems. Safety management across ATM systems will therefore improve as safety practitioners implement common techniques, terms, and results. This report is the first major attempt to evolve a common inter-operable safety approach.

2.0 Organization of Report

The report begins with a brief safety assessment initiative history of both service providers (FAA & EUROCONTROL) ATM. Section 4.0 provides an overview of a generic system safety assessment methodology, introducing a eight stage safety process and techniques. Section 5.0 provides a matrix of techniques to assist in initial tool selection. Section 6.0 presents twenty-seven selected techniques, each in a consistent template format. Section 7.0 provides five case studies showing that techniques may be consolidated and used together in an integrated fashion to answer safety questions. Section 8.0 briefly considers future developments in the Toolbox, and Section 8.0 the References for the techniques in the Toolbox. Appendix A provides some further templates for tools used to support detailed analysis of flight data, radar-track data, and text data analysis. Appendix B contains a list of acronyms and abbreviations used in this report.

3.0 Review of Safety Initiatives (EUROCONTROL & FAA)

3.1 EUROCONTROL Safety Assessment Methodology Initiative

EUROCONTROL is an organization concerned with the safety of European ATM, and aims to support and harmonize approaches across different European Member States. EUROCONTROL has a vision of future ATM that includes many new airspace and advanced controller-tool concepts, and aims to ensure that this future vision is at least as

safe, and preferably safer, than current levels in Europe, even given projected significant increases in air traffic volume. In 2002-4 EUROCONTROL therefore undertook a major review of more than 500 safety assessment techniques from nine different industries [Review of techniques for SAM, 2004]. These techniques ranged from 'traditional' techniques examining hardware reliability to techniques focusing on human behavior and software safety. The purpose of the Safety Methods Survey project was to make an as complete inventory as possible and to identify from these the techniques and methods (including those developed in other domains and industries such as nuclear, chemical, telecommunication, railways, software design, but excluding commercially available tools) for its formal Safety Assessment Methodology (SAM) applications. From the inventory of more than 500 techniques, a selection was made that appeared most relevant to support the SAM in the short term (with minimal adaptation). In this report the selection of techniques for integration in the FAA tools has been based on broader criteria and this resulted into the selection of fifteen techniques from the ones selected for SAM on the short term, and a similar number of additional techniques.

EUROCONTROL aims to ensure a high degree of safety in the Agency's activities and a formal and systematic approach to safety management with the implementation of a Safety Management System (SMS). Local SMSs in the different Service Business Units (SBUs) and Operational Service Units (OSUs) of the Agency that adequately relate to the safety criticality of the activities and functions are being implemented. Additionally, a process is ongoing to adapt the Agency SMS to the activities at the Experimental Centre for the development of new ATM concepts.

3.2 FAA NAS Modernization System Safety Program Initiative

The FAA System Safety Management Program (SSMP) and System Safety Handbook (SSH) for the acquisition of new systems, establishes a plan to ensure system safety is effectively integrated into NAS (National Airspace Structure) Modernization. The SSMP and SSH identify various hazard identification techniques and provide specifics on how to apply these techniques to ATM systems.

The FAA's Air Traffic Organization (ATO) has been evolving towards a Safety Management System (SMS). The SMS provides guidance to the service provider to ensure hazards to the operation, system, and/or procedures are identified in a systematic, disciplined manner implementing defined hazard analysis tools. The SMS identifies various safety techniques (included in Table 1) to ensure that whoever performs the hazard analyses shall select the tool that is most appropriate for the type of system being evaluated.

3.3 FAA/EUROCONTROL Safety Assessment Methodology Joint Initiative

Both the FAA and EUROCONTROL have been working to maintain and improve the effectiveness of safety assessment. In April 2003, these two organizations identified the

roles, responsibilities, tasks and deliverables with respect to Coordinating Safety R&D, Understanding System Safety, and Assessing and Improving Safety as outlined in the FAA/EUROCONTROL R&D Committee Safety Action Plan (AP-15). This current report represents one of the first major outputs from this Action Plan. Its primary target audience is safety practitioners and safety managers in ATM, but it should also be useful for informing project and program managers developing future ATM concepts, and managers and safety personnel at operational facilities who need to manage the safety of existing operations.

3.4 Selection of techniques in this report

In order to obtain a techniques toolbox, which is the main aim of the current report, the EUROCONTROL inventory of over 500 techniques has been used again as a starting point. However, the current criteria for selection from these 500+ are slightly different than in [Review of techniques for SAM, 2004], namely:

- The technique should be currently in use;
- The technique is judged by the AP15 group as being of value;
- The technique is missing in the 500+ review, but satisfies the first two criteria.

This resulted in a list of 27 selected techniques. For these techniques this report provides explanatory material in the form of a template, and these 27 are listed below (in alphabetical order of their best known acronym):

1. Air-MIDAS
2. Air Safety Database
3. ASRS (Aviation Safety Reporting System)
4. Bias & Uncertainty Assessment
5. Bow-Tie Analysis
6. CCA (Common Cause Analysis)
7. Collision Risk Models
8. ETA (Event Tree Analysis)
9. External Events Analysis
10. FAST (Future Aviation Safety Team) Method
11. FMECA (Failure Modes Effects and Criticality Analysis)
12. FTA (Fault Tree Analysis)
13. Future Flight Central
14. HAZOP (Hazard and Operability study)
15. HEART (Human Error Assessment and Reduction Technique)
16. HERA (Human Error in ATM)
17. HTA (Hierarchical Task Analysis)
18. HTRR (Hazard Tracking and Risk Resolution)
19. Human Error Database
20. Human Factors Case
21. PDARS (Performance Data Analysis and Reporting System)
22. SADT (Structured Analysis and Design Technique)
23. SAFSIM (Safety in Simulations)

24. SIMMOD Pro
25. TOPAZ accident risk assessment methodology
26. TRACER-Lite
27. Use of Expert Judgment

As new techniques are developed or adapted for use in ATM, they will be added to this report in later versions of the Toolbox.

4.0 Overview of Safety Assessment

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 analyzes 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.

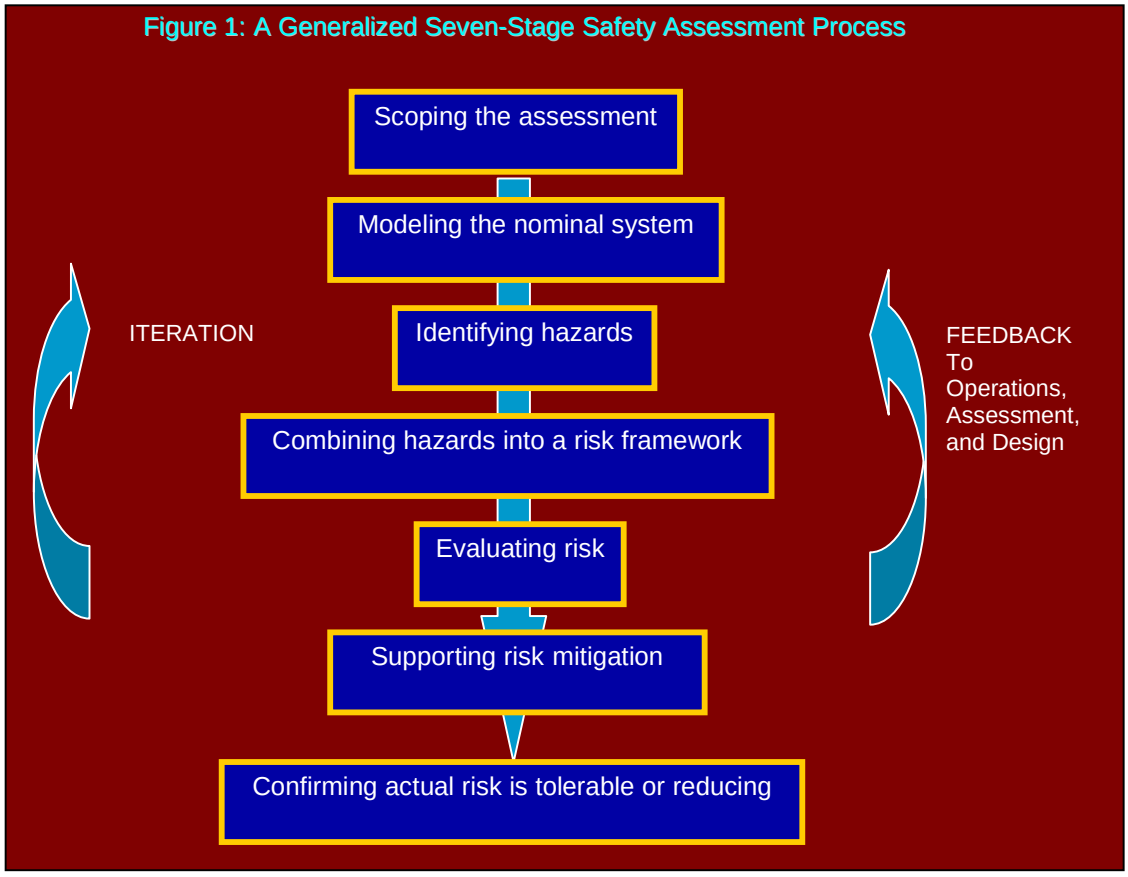
Usually at this point, this risk or safety assessment must be compared to a benchmark, such as existing system risk to see if it is an improvement or not . It is here that a ‘Target Level of Safety’ is often used. This will express for example, the tolerable (to society) frequency of an accident, in terms such as accidents per flight hour, or per approach/landing, or per surface movement. The TLS allows decision-making on whether or not to continue developing the concept, or to continue but with key safety requirements that need to be demonstrated in the new system for it to be adequately safe.

Once such a safety process is conducted, it is documented as a ‘safety case’, and used to justify to the regulatory authorities that the new proposed system or system change will not adversely affect safety. However, because the safety case will often contain safety requirements and assumptions that are key to ensuring that the system remains within its safe operational envelope, it should be seen as a living document, and be periodically updated. Ideally it contains information that is utilized initially by the system designers and then by the operations people for the remainder of the system’s lifecycle.

Once the new design itself is operational, there becomes a need to continually monitor safety performance so the responsibility for safety oversight then transfers to the management of the operational facility. Usually a safety activity will be created that will record safety-related events (e.g. loss of separation, TCAS events, etc.), for lessons

learned purposes. Trends may occur for example related to local factors (e.g. particular controller working practices and changes in local sector design) or more widespread factors (e.g. shifts in controller demography and availability). The detection of trends that could compromise safety requires archiving the relevant data and monitoring them continuously. The process cannot rely on human memory. When such a trend is detected and determined to be operationally significant, an appropriate reaction should occur to ensure that the system returns to its optimal safe performance. This amounts to safety or organizational learning (see the final 'step' in this section). This is still part of the system safety process, and indeed such information on the causes and contributors to incidents and accidents needs to be fed back to safety assessment practitioners, enabling them to refine their tools and techniques. The challenge to proactive management of safety is discovering the precursors of the next accident, identifying their causal factors, and implementing the most effective interventions before an accident occurs.

Safety Assessment of an air traffic operation can therefore be seen as a seven-stage process, as shown below (with feedback leading to Organizational learning as a potential 'eighth' step that could be developed for the industry).



The following paragraphs outline the key aspects of these seven steps, plus a key eighth step of organizational learning, and begin to identify what techniques can be used at each stage (several techniques can be useful in more than one stage (see Table 1).

- **Stage 1 - Scope the Assessment**

This stage for a development project entails the availability of an Operational Concept or System Specification. It is difficult to conduct system safety assessments without knowing the system operational concept. However, it is not uncommon in early assessments that the operational concept itself is a living document and 'ever-evolving'. The Project and the safety practitioner must develop a Safety Plan that specifies the scope of the safety assessment and outlines the approach. This can include such pertinent information as what Target Level of Safety(TLS) (or part of it) is relevant for the safety assessment, where the system boundaries are considered to be, and the relative focus on aspect such as hardware, software, and human elements of safety. This helps the safety assessor determine at an early stage the likely techniques to be used, and helps the Project Manager envision the likely safety-related resources such as access to operational personnel, the need for simulations and trials, etc. The Scoping stage is therefore partly technical (identifying the likely characteristics of the safety assessment based on an initial assessment of the nature of the proposed change), and partly administrative and regulatory. Nevertheless, the importance of the administrative/regulations component should not be under-estimated.

When a hazard arises in an existing system, the scoping of the required assessment will vary considerably depending on local factors and company procedures. Nevertheless, there will still be a need to consider the nature of the hazard, and this will depend critically on the tool or technique to be used. Many hazards that arise in existing systems may be Human Factors-related, yet tools for recording incidents, etc. often record too superficially the information required to scope a study (see however HERA-JANUS in the Toolbox section). Therefore, safety issues arising in existing Operational Units, often will require an initial scoping investigation; talking with operational personnel to better understand the issue. The TLS may still be used, but more often if it is a local issue, safety assessment and interventions may be more qualitative in approach. They may for example identify the hazard and move straight to developing mitigation measures, after a qualitative assessment of the risk.

Outputs: Safety plan; assignment of safety/risk criteria (e.g., TLS)
Techniques: Scoping does not always use defined techniques, and may be informed by assessor judgment and incident/accident experience, and prior practice in a related area; the TOPAZ accident risk assessment methodology may also be used. The approach will depend on local adaptation and the organization's Safety Management System (SMS) The FAST methodology helps scope the assessment by defining Areas of Change in the Concept of Operation.

- **Stage 2 - Modeling the nominal operation**

Safety Assessment is ‘transitive’ in nature – it requires an object, something to analyze. This is often not realized by non-safety practitioners. There is therefore a need to learn about the description of the operation and systems as it should work or function; this being the nominal ‘model’ (how the system should behave), from which the ‘risk’ model (how it can fail, and how it can be ‘recovered’) can be developed during and after the hazard identification phase.

There are various ways of modeling an operation for subsequent safety analysis, and indeed often this is done by the Project or Program in any case. Examples are Functional Block Diagrams or Use Case Modeling. In some cases, special modeling approaches might be required such as Task Analysis for modeling human interactions. Some of these are considered in the Toolbox section. These techniques are effectively abstractions of the system from a particular viewpoint, and so the exact safety modeling requirements are a function of the aspects on which the safety practitioner intends to focus on.

For existing systems, paradoxically, there may be no abstraction of the system available, particularly for the human (i.e. controller) tasks. Nevertheless, the safety practitioner will usually find it necessary to construct a representation of the system to properly assess it, and so techniques such as task analysis can be used for such purposes. The advantage for the safety assessor with existing systems is often that observation is feasible, and fewer assumptions have to be made, since the assessor can simply interview controllers or pilots or other operational experts.

Outputs: Description of operations and systems used.
Techniques: Hierarchical Task Analysis, *TOPAZ* accident risk assessment methodology, and SADT. Additionally a number of other system modeling techniques exist, but these vary in usage in ATM, and ATM is in fact still exploring best techniques to use. This area will therefore be redressed in later versions of this report.

- **Stage 3 - Identify hazards**

Probably the most critical stage in safety assessment is hazard identification and risk assessment. Such risks include those that may emanate from the Operational Concept itself; e.g., related to proposed hardware, software, procedures, and/or human elements. These may relate to ‘external events’ in the environment (e.g., bad weather), or to failures or events in other systems that can affect the system under consideration. One of the difficulties of hazard identification in ATM applications is that it is effectively a globally-interoperable system. This means firstly that it is difficult to know when a hazard identification exercise is complete. Secondly, it means that there is much to consider, especially in terms of interactions of system elements. Certain failures (e.g., power supply) will affect multiple systems, and loss of key data similarly can affect different systems in different (and sometimes unexpected) ways. These are called common cause failures (identified by Common Cause Analysis), and relate to what are called

'dependencies' between systems, and can lead either to new failure outcomes or elevated failure frequencies, so they need to be identified.

Most hazard identification techniques fall into two categories, namely single-assessor and group-based approaches. The single-assessor approach usually entails rigorous analysis of all aspects of a system according to a failure schedule or list of failure types. Some techniques are specifically aimed at certain hazard types (e.g., human error) whilst others are generic across different hazard categories. The group-based hazard identification approach involves doing this with a group of experts rather one or two assessors. The main challenge for both approaches involves shifting the boundary between imaginable hazards and unimaginable hazards.

In addition to hazard identification by experts, there is the option to use recorded observations, either from actual operations (e.g., using databases such as ASRS or radar track data) or from real-time and non real-time simulations. The former should ideally always be consulted when conducting hazard identification, to see if past experience can offer information about likely hazards and hazard interactions. The latter (real-time simulations and/or non-real-time simulations incorporating human performance models) can similarly be used to identify hazards in operability of a system, and can gather insights about potential errors that could contribute to hazards. They can also of course identify ways to mitigate or control hazards.

In current operations and systems, hazard identification is sometimes the starting point, since a series of hazard-related incidents may have occurred due to certain causes. The safety practitioner's job is then to investigate these incidents to find the complete set of causes, as well as possible alternative hazards that could arise, and derive mitigations to reduce incident rate or severity. Although such investigations will not usually follow a formal safety assessment pathway, some of the techniques can still be helpful to ensure that the specialist or practitioner has a complete understanding of the hazards, risks, causes, and contributory factors.

Output: Defined hazard set
Techniques: Air Safety Database, ASRS, Common Cause Analysis; External Events Analysis; FAST; FMECA; HAZOP; Human Factors Case; TOPAZ accident risk assessment methodology; TRACER-Lite, PDARS

- **Stage 4 - Combine hazards into a risk framework**

This stage means developing a way to aggregate the different identified hazards and their contributions to accident sequences into a risk model with which the total risk due to the proposed system or change can be evaluated. This stage is necessary in all but simple systems or narrowly-scoped analyses, because otherwise it becomes difficult to weigh up the different identified risks and their various accident sequences, and in particular to determine if the risks will be within the Target Level of Safety selected.

Typically, at the top level of a risk model there is a logic diagram such as a fault or event tree, which models respectively the causes of an event (usually a specific hazard), the resultant consequential pathways after an event and a collision risk model at the end of the pathways. These logic diagrams define according to strict rules how events can link together to cause a hazard, and how such hazards can either propagate to accidental consequences (such as mid-air collision, runway incursion or Controlled Flight into Terrain), or else safe states (via mitigations or safety nets). Such 'trees' can become quite complex, and usually they are analyzed by specially-designed computer tools.

Since levels of risk are influenced (possibly quite significantly) by dependencies and common cause failures that exist between different parts of the risk model, risk modeling should include a dependency analysis (e.g. going through the risk model identifying common elements and dependencies in particular concentrating on 'AND' gates if using fault trees, for example).

A complementary approach is to make use of a Monte Carlo simulation model which allows to evaluate multiple dynamical and dependent events, 'non-nominal' scenarios, and permutations of such events and scenarios, and to make effective use of a larger variety of qualitative and quantitative input data (e.g. human performance models). Such an approach is also more powerful in providing insight in the effectiveness and sensitivities of the interplay between multiple humans and systems involved in the operation (e.g. controller and pilot, aircraft systems, ATC system). If properly applied, it can make assumptions explicit and with this make the Monte Carlo simulation results open to scrutiny by operational experts.

The result is a risk model that encapsulates and relates the different hazardous and recovery events into a homogeneous model. This risk model can then be quantified (this process is called 'evaluation'), delivering not only the overall risk estimate, but also the ability to determine which elements in the operation are most safety critical. This then in turn points the way towards risk mitigation. The risk modeling is therefore one of the most critical parts of the overall safety assessment process.

Output: Risk Model
Techniques: *Bow-Tie; Collision Risk Models; Common Cause Analysis; Event trees; Fault trees; Human Performance Simulation; TOPAZ accident risk assessment methodology.*

- **Stage 5 - Evaluate Risk**

Having developed a risk model that is logic-based and/or simulation-based, the next stage is to determine the quantitative properties of the risk model – in particular how often the various events are likely to occur. In some cases, databases will exist which can give such information, e.g. the likely time before failure of a radar screen, or the probability of a communication error between controller and pilot. In other cases, there may be techniques to estimate such values.

When failure data are collected for a component, or for a particular human task, there will always be some uncertainty in the data derived, due to limits on data samples, and due to slight performance differences between the same components, and rather large potential differences between individual human 'components'. Therefore, having amassed the data required to 'evaluate' the risk model, considerations of residual bias in the data-set and uncertainties, and how they can interact, should occur. This requires expertise, but represents good practice for safety assessments. In particular, if there are too many uncertainties in the data, then comparison against a quantified Target Level of Safety will be unreliable. For those parts of the tree where a simulation model has been developed, large scale Monte Carlo simulations and sensitivity analyses are performed and documented. In addition, a formal bias and uncertainty assessment method can be applied.

Where no databases and no appropriate techniques exist, there can be recourse to expert judgment, using formal procedures and validated experts. However, because expertise is known to suffer from biases, and since by definition experts on the failure behavior of future systems have limited expertise, expert judgment protocols must include means for detecting biases and incoherent judgment, and hence rejecting the results should the expertise fail according to certain quality criteria.

On those places in the tree for which Monte Carlo simulations have been performed, it is also possible to compare the results of the simulation model with the experts judgment and, in case of differences, to discuss this with the experts. This often will lead both to better expert judgments and to a better simulation model.

The quantification of risk is unfortunately sometimes seen as a 'numbers game', relying on questionable data, crude modeling of scenarios and subsequent simplistic mathematical treatment. However, it is relevant to point out that a number of accidents have been predicted beforehand, but 'without the right numbers', hence underestimating their risk, and thus remaining unprepared for the accident. This could be seen as reinforcement of the position against quantification, however this would be short-sighted. Most accidents are complex and involve both related and unrelated factors and events, difficult to predict outside of complex risk modeling. Without quantification, such accidents tend to be assumed to be rare or negligible (due to a natural human bias called 'conservatism'). Therefore, the drive instead should be to derive better numbers by collecting and sharing event and incident data, so that when accident sequences are identified, their likelihood is accurately predicted.

Output: Evaluated Risk Model; identify and evaluate dependencies, evaluation of risk against target criteria; risk-informed decision-making becomes possible
Techniques: ASRS; Human Error Database; Bias and Uncertainty Assessment; Collision Risk Models; Common Cause Analysis, FAST; TOPAZ accident risk assessment methodology; HEART.

- **Stage 6 - Identify potential mitigating measures to reduce risk**

This stage involves four main steps. The first step is to consider whether risk reduction is required, i.e. whether the safety target criteria are met. This sets the initial obligation to reduce risk, and tells the assessor the size of the challenge ahead (particularly if the target level is not met). If the risk is in the broadly acceptable area the risk 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). If the risk is seen as being 'tolerable', no risk can be accepted unless reduced as far as reasonably practicable. Therefore this first step is concerned with what *must* be done, and then what *should* be done to reduce risk and increase safety.

The second step is to determine where the major element of risk is coming from, i.e. what part of the risk model is contributing most risk. This is the natural target for reduction. Some techniques (e.g. Fault Trees) can automatically generate a prioritized list of the events in terms of their contribution to risk. The third step is then to support design developers in identifying potential mitigations or changes that could reduce risk. Sometimes the major element of risk cannot be mitigated, so other lesser elements must be tackled, which together would lead to the required risk reduction. The fourth step is then to re-calculate risk, having adjusted either the model or the quantitative inputs according to the mitigations developed (called safety requirements) to verify that the system is acceptably safe. A word of caution here is that it is easy to over-estimate the impact of reduction measures and mitigations, and also it is easy to overlook unforeseen interactions and problems associated with the mitigations themselves. In fact in several industries after the identification of reduction measures or mitigations, it is a requirement to do further hazard identification to detect such unplanned interactions, followed by re-quantification of the risk model.

Another aspect of this stage concerns tracking safety requirements and assumptions. For design and development projects, these may occur over a long timescale. This means that either there will be several safety cases during the development life cycle, each becoming more detailed as design detail increases, or else the safety case work may be more of a continual and iterative process, gradually leading to a definitive safety case. In either of these situations, there is a need to track the key safety assumptions and requirements as they are made by the project, and ensure that they are enacted in the actual design of the system. This may mean that there are key training and procedural assumptions, or requirements concerning the Human Machine Interface (HMI), or key performance requirements of equipment that need to be assured and tested during equipment or system performance simulations or trials. Furthermore, the designers and developers may realize later in the process that they wish to change certain design parameters, and will want to know the impact on risk. A mechanism for enabling the impact of such changes to be rapidly seen is therefore desirable. Such a hazard and requirements tracking and impact evaluation technique has indeed been developed, and can therefore be used to keep track of all requirements, make sure they happen effectively, yet to allow some flexibility so that safety is not seen as a designers' 'strait-jacket'.

Output: Potential mitigating measures to reduce risk

Techniques: *HAZOP; Human Factors Case; TRACER-Lite; HTRR, Bow-Tie, TOPAZ accident risk assessment methodology.*

- **Stage 7 - Confirm actual risk is tolerable or reducing**

With respect to the existing systems, this stage refers to the need to continually monitor overall system safety performance and determine if the various safety requirements are performing their functions as expected. It requires a means of monitoring and analyzing resultant safety data, and then drawing lessons from those data in sufficient time to react and prevent accidents from occurring. This is not trivial, and requires pre-definition of safety parameters and events, automatic and manual recording mechanisms, analysis tools, and data storage and retrieval systems (knowledge bases). It also of course requires a good safety culture that will accept such monitoring and analysis and will act on its conclusions, and a legal framework (a so-called 'just culture') that will protect controllers and pilots offering up much-needed safety information on human errors and other events that occur. Actual collection, analysis and sharing of safety-related data allows the whole safety framework to become a learning system, leading to better safety data and safety evaluation techniques, and safer systems. Expectations and a system for monitoring should also be established prior to implementing an intervention in order to measure its effectiveness and identify any unexpected effects from system operations.

Output: Measurement of safety-related events & data against predictions
Techniques: ASRS, PDARS, Air Safety Database, FOQA, FDM (see also Appendix A)

- **Stage 8 – Organizational Learning through feedback**

In Figure 1 there are two feedback loops – the first refers to 'Iteration', meaning that safety assessment is usually iterative in nature and safety assessments themselves are not always 'once-through' processes. The right-hand feedback loop however refers to feedback at a more organizational level, involving three key parties. The first is clearly Operations, in that hazard and risk information can be of use to actual Operational Centers in their own safety management practices (including safety-related training for controllers). This may be of particular relevance when for example an assessment for a project uncovers new hazards that may apply to other projects or even existing systems. The second party that can benefit from structured feedback are safety assessors themselves, since then assessors working on new system assessments can see what hazards etc. were identified, with what risk levels, and with what mitigations. Assessors need not be constrained by prior assessments, but should be able to view them. Therefore a 'library' of safety assessments can be useful in this respect. The third party that can benefit from feedback are designers and developers of new concepts. Such people are not necessarily habitual readers of safety assessments, and yet if such information could be presented in a usable way to designers/developers, then they would be considering safety aspects from a very early stage in their concept formulation processes. Safety assessment

practice is therefore a potential source of organizational learning for the industry, which could enhance Safety Management efficiency and effectiveness. This step has yet to be properly developed for ATM, but is a logical addition to the ATM safety management approach.

A critical component of safety is the tracking and analysis of safety data to enhance awareness of potential hazardous situations. The collection, analysis, and sharing of safety data supports the continual improvement of safety in ATM. Various techniques exist to collect, prepare, and analyze data (quantitative and textual) to support feedback of information to stakeholders.

Output: Better knowledge in operations, safety assessment and design concerning how to manage safety effectively in ATM.
Relevant Techniques: ASRS, ASAP, PDARS, FOQA, FDM, Air Safety Database; HTRR. PLADS, GATE, Morning Report (see also Appendix A).

Table 1: Techniques in the Eight Stage Process

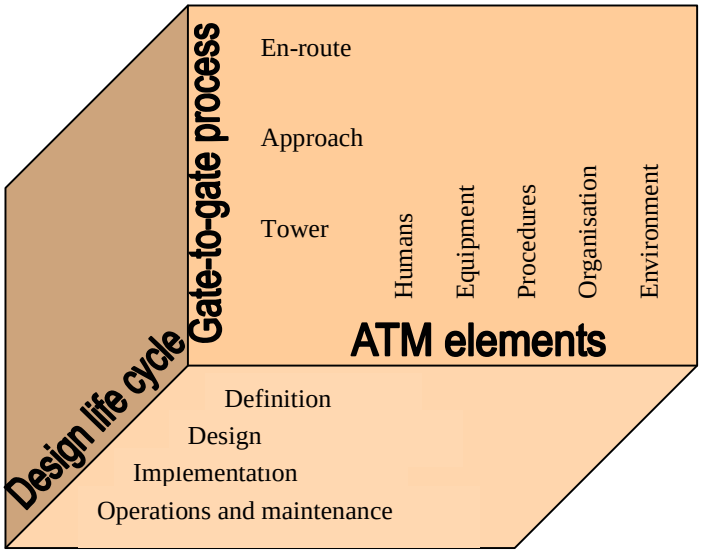
	Scoping	System Modeling	Hazard Identification	Risk Modeling	Risk Evaluation	Risk Reduction	Risk Monitoring	Feedback
Safety Management System	[Safety Plan]					Hazard tracking (HTRR)		Hazard Tracking (HTRR)
	[TLS]							
	TOPAZ							
General system safety techniques	FAST	System Modeling Techniques	HAZOP	Event Tree Analysis	Reliability Databases	HAZOP		
			FAST		FAST			
			FMECA	Fault Tree Analysis				
			External Events Analysis	Bow-Tie				
			Common Cause Analysis	Common Cause Analysis	Common Cause Analysis			
Operational Data Usage Specialised techniques			ASRS		ASRS		ASRS, ASAP	PLADS, GATE
			Air Safety Database		Bias & Uncertainty Assessment		Air Safety Database, FOQA, FDM, PDARS	Data Quality Filters, Data signatures, Morning Report
			Real-Time simulation					Data Signatures
		TOPAZ	TOPAZ	TOPAZ	TOPAZ	TOPAZ		
				Collision Risk Models	Collision Risk Models			
Human Factors		Hierarchical Task Analysis	Human Factors Case		Human Error Database	Human Factors Case		Future Flight Central
		SAFSIM			HEART		HERA	

		Reconfigurable flight simulator (RFS) SIMMOD-Pro	TRACER-Lite, Air-MIDAS + RFS		Air-MIDAS + RFS	TRACER-Lite		
		Human Performance Simulation	Human Performance Simulation	Human Performance Simulation	Human Performance Simulation	Human Performance Simulation		

5.0 Overview of Toolbox of techniques

Each of the 27 techniques selected for the toolbox attempts to support one or more of the eight stages in the system safety assessment process. Each one can also act on one or more aspect of a system; i.e., its procedures, the human element (individual or team performance), the hardware, software, or the environment, and can relate to one or more flight phases (ground, approach, en route) and lastly can occur during one or more of the system life cycle phases, as shown in Figure 2 below.

Figure 2: Contextual Dimensions for System Safety Assessment in ATM



In fact most techniques can relate to multiple aspects of the above three dimensions, but usually not all. Therefore, the following matrix (Table 2) is aimed at helping the user make an initial selection of techniques from the Toolbox. The matrix therefore lists the function of each technique and its applicability in the system life cycle. It also lists what resources are required in terms of expertise or data.

Table 2 - Matrix of Techniques

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
1	Air-MIDAS	Simulation of human-system interactions	Evaluating impacts of changes on human-system performance	Human-machine interaction	Design and Operations	Detailed analyses of tasks and interfaces; data input to Air-MIDAS model	Air-MIDAS expertise; domain knowledge
2	Air Safety Database	To provide world-wide statistical data for aviation safety studies	Maintaining a large / consistent set of multi-source data	Emphasis is on accidents and serious incidents	All Stages	Multiple data sources	Statistical and flight operational expertise
3	ASRS [Event data collection]	A database of confidential, voluntary reports of aviation incidents.	Provide a continuous indicator of system performance from the perspectives of all of its operators	Identify systemic issues deserving of further investigation for operational significance and causations	System design. Can capture information on system and equipment design and implementation. However, majority of reports relate to operations and maintenance.	Fill out an incident report form that can be downloaded from the ASRS web site	It is generally a standalone technique, easy to understand and use. Updated versions of the database are publicly available.
4	Bias and uncertainty assessment	Determination of confidence in risk estimates	Evaluation	All aspects quantified in risk model	All stages	Statistical properties and expert knowledge of	Statistical and reliability engineering expertise

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
						data used in evaluation	
5	Bow-Tie Analysis	A fault tree leading to a hazard, then leading to outcomes via event tree pathways	Combine hazards into a risk framework to guide risk mitigation	All aspects represented in the bow-tie	Late Concept design stage onwards	Identified hazard, causes and outcomes	Safety or risk assessment expertise
6	CCA (Common Cause Analysis)	Identify and evaluate hazards with a common or related (dependent) cause	Hazard identification	All system aspects	Usually detailed design stage onwards	Operational concept, design information, system definition and inter-relationships, use cases (scenarios)	Safety or risk analysis expertise
7	Collision Risk Models	Mathematical model evaluating risk of mid-air collision or flight into terrain	Evaluate collision risk in scenarios	Two passing or crossing aircraft	Concept onwards	Airspace design, traffic throughput and patterns, aircraft behavior, weather assumptions	Mathematical modeling expertise; collision modeling domain knowledge
8	(ETA) Event Tree Analysis	Determination of possible outcomes leading from an event or hazard	Hazard identification; risk evaluation	All system aspects	Late Concept stage onwards	Scenarios and system knowledge; event analysis	Safety and risk analysis expertise; domain knowledge

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
9	External Events Analysis	Determining how events external to the system can affect risk	Hazard identification	Mainly environment	Late Concept Design stage onwards	Operational Environment description; system knowledge; event analysis	Risk analysis expertise; domain knowledge
10	FAST Method (Future Aviation Safety Team)	Expert group hazard iidentification of changes	Hazard Identification	All system	Design	Concept of Operations changes (planned or *ad hoc*)	Domain and safety experience; expert group facilitation
11	FMECA (Failure Modes and Effects Criticality Analysis)	Identify failure modes, and controls to reduce risk	Hazard identification	Hardware	Late hardware design stage onwards	Detailed hardware knowledge	Risk and safety analysis expertise; domain knowledge
12	FTA (Fault Tree Analysis)	Determining the possible causes of a hazard, whether single or multiple, related or unrelated	Hazard identification; risk evaluation	All system aspects	Late Concept Design stage onwards	Detailed system knowledge; event analysis	Risk and safety analysis expertise; domain knowledge
13	Future Flight Central	High fidelity, human-in-the-loop Air Traffic Control Tower simulator	Study proposed changes for improved airport safety and capacity.	Validate airport design plans and procedures for human factors.	Operations and maintenance	Scenario descriptions for new designs and procedures.	FFC provides personnel experienced in high-fidelity simulations

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
14	HAZOP (Hazard & Operability Study)	Identifying hazards, their implications and mitigations using a structured brainstorming approach	Hazard identification; risk evaluation; risk mitigation	Usually all except software (unless specialized for this purpose)	Concept onwards	Group of experts (eg safety, aviation/ATM; designer; Human Factors); system description and operational concept	Risk analysis (HAZOP) expertise; domain knowledge
15	HEART (Human Error Assessment & Reduction Technique)	Quantifying the likelihood (probability) of human error	Risk evaluation	Human (individual or team)	Late Concept design stage onwards	Task analysis and appreciation of likely error forcing conditions	Human Reliability Assessment expertise (HEART)
16	HERA (Human Error in ATM)	Retrospective and prospective analysis of human error probabilities	Incident analysis method providing insights into the cognitive processes of controllers during incidents.	Human (individual or team)	Design concept and operational	Functional task analysis	Human Factors expertise
17	HTA (Hierarchical Task Analysis)	A systematic means of identifying the human roles in the system	Learning about the human tasks at the beginning of a safety analysis	Human (individual and team)	Late Concept Design stage onwards	Domain knowledge; operational concept; simulations; access to experts on how the	Human Factors expertise

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
						system will be operated	
18	HTRR – Hazard tracking & Risk Resolution	A means of tracking and managing all identified risks during the design life cycle	Risk evaluation and mitigation; safety monitoring also possible	All system aspects	Concept design stage onwards, though may stop at the end of the design phase (i.e. not in operations).	All hazards identified from whatever source.	Safety assessment and management expertise; project management expertise
19	Human Error Database	Quantifying human error probabilities for human-related events and recoveries identified	Risk evaluation	Human (individual and team)	Late Concept Design Stage onwards	Human error data collected either from actual events (e.g. incidents) or simulations, or formal expert judgment sessions.	Human Reliability Assessment expertise
20	Human Factors Case	Determination of Human Factors needs to achieve sufficiently safe performance	Hazard identification; risk mitigation	Human (individual and team)	Concept Design stage onwards	Group of experts; domain knowledge; operational concept	Human Factors expertise; expert group facilitation expertise

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
21	PDARS (Performance Data Analysis and Reporting System)	Collect, process, and archive operational data from each of the ATC facilities. Provide daily reports to each facility of previous day's performance.	Provides a variety of tabular and graphical reports on traffic counts and flows specified by, and customized to, the facility.	Primary focus is on procedures & organization.	Entails an iterative process. Starts with initial definition based on user-needs study, followed by design and implementation for evaluation, feedback, and redesign.	Access to raw data is automatic. Reports are designed and customized to user's requirements; easy to understand and manipulate	Training is part of the PDARS installation. Generally, capability with Microsoft Excel is sufficient.
22	SADT	System Functional Model	Provides a rigorous, disciplined approach to achieve understanding of user needs prior to providing a design solution.	All system aspects	Technique can be required as early as the scope and modeling phase of the life cycle.	Mission scenario based on Concept of Operations	System and Safety expertise
23	SAFSIM	Real-time Simulation of Human in the loop	To take measures during real-time human-in-the-loop simulations to derive safety insights	Human (Individual or Team)	Mid-way through Concept development	Hazard analysis or operational incident data	Human Factors expertise
24	SIMMOD	Validated	High-fidelity,	Model complex	Define scope of	Scenario	High level of

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
		simulation of airport and airspace operations	fast-time simulation of current and proposed airport and airspace operations.	interactions among ATM systems, disruptive events, and human resources and activities.	study, design solutions, implementation procedures, and optimization	definition of proposed changes	expertise in ATM systems
25	TOPAZ accident risk assessment methodology	Scenario and Monte Carlo simulation-based accident risk assessment of an ATM operation	ATM safety / capacity assessment	Holistic approach including organizational safety	All stages	Access to operational experts; domain knowledge, statistical data	Safety analysts and Operational experts. For an extension of a TOPAZ simulation toolset, Stochastic analysis and Cognitive psychology expertise is also required

	Tool	Short description	Function	System focus	Life cycle stage(s)	Input requirements	Expertise requirements
26	TRACER-Lite – Technique for Retrospective Analysis of Cognitive Error	Determining the human errors and recoveries possible in human-system interactions	Hazard identification; risk evaluation (via the Recovery Success Likelihood)	Human (mainly individual interactions) and procedural	Late Concept Design stage onwards	Task analysis, domain knowledge	Human Factors and safety expertise; domain expertise
27	Use of Expert Judgment	Application of expert judgment techniques to evaluate probabilities or frequencies of events	Risk evaluation	All system aspects possible – often focus is on human or environmental events	Concept Design stage onwards	Domain experts; detailed descriptions of the events or situations to be quantified	Expertise in aggregation of group expert knowledge and facilitation techniques; domain knowledge

6.0 Analysis of Toolbox of techniques

For each of the 27 techniques selected, a template has been produced so that the type of information contained is similar across the whole toolbox. A generic version of the template, showing what each category is meant to describe, is shown below in Figure 3.

The following pages then give the actual templates for the 27 techniques listed in Section 3.4. Fifteen of these templates are from [Review of techniques for SAM, 2004], and twelve additional templates have been produced by Action Plan 15 members during the research for the current report. Where references are used, these are to be found in full at the back of this report. In addition, Appendix A gives a comprehensive set of analytical tools, also in template form, that support analyses of digital databases (e.g. flight recorded data and radar track data) and of textual databases (e.g. ASRS and ASAP).

Figure 3 – Generic Techniques Template

'Name of the technique'	
References used:	References to books and papers used for the assessment of the technique
Alternate names:	Other names or specialty names
Primary objective:	Primary objective of the technique: the original purpose or function of the technique.
Description:	A description of the process which must be followed to apply the technique. This description is a digest of information drawn from the references, coupled with advice from those who have practiced the use of the technique
Process steps:	Steps required in the technique application process
Applicability range:	Does the technique assess humans (human error, human behavior), equipment (hardware, software, including HMI) or procedures/organization?
Life cycle stage:	Life cycle stage applicability: the earliest ANS life cycle stage at which the technique can probably be applied (definition; design; implementation; operations and maintenance; decommissioning).
Experience in application to air traffic:	Has the technique previously been applied in air traffic or air traffic management?
Related methods:	Alternative, overlapping or complementary techniques, e.g. techniques that can assist in the quantification of the results, if the technique itself is qualitative, or techniques that can be used preliminarily or successively to the technique.
Availability and tool support:	This criterion indicates that the technique is either available, or else it is unavailable because it has been discontinued, commercially related to one organization and not generally available, or still at the prototype stage and not yet generally available. The criterion also covers the availability of computer tools that can support application of the technique.
Maturity:	The extent to which the technique has been developed technically and has proven itself useful in applications.
Acceptability:	In some cases evaluation studies of techniques have been carried out by regulatory authorities (notably the US Nuclear Regulatory Commission) which indicate some degree of approval for techniques which have been given positive evaluations. Techniques that have achieved positive evaluations will receive a higher rating on this criterion. This criterion will also be influenced by the theoretical rigor of a technique and the extent to which it has been subjected to objective evaluations. Finally, it covers numerical accuracy of the results produced.
Ease of integration:	Does the technique easily or usually combine with particular other techniques (e.g. in the SAM)? This criterion also covers complexity: the technique is relatively easy to understand and use.
Documentability:	Documentability: the degree to which the technique lends itself to auditable documentation. The techniques are rated as low (meaning that the way the technique is utilized is difficult to document), moderate (meaning that the technique provides sufficient documentation to be repeatable), or high (indicating that all assumptions etc. are recorded, and that in addition the documentation will be usable for future system operations and will greatly facilitate future periodic assessments). This criterion also covers consistency of the technique, such that if used on two occasions by independent experts, reasonably similar results are derived.
Advantages:	Covers how it helps ATM safety assurance, qualitative usefulness (the degree to which the technique allows specific qualitative recommendations to be made concerning ways to improve safety), and other general advantages of the method, such as the extent to which the technique can provide useful results with limited information or data.
Disadvantages:	Any restrictions on applicability, e.g. problem scale, generality, accuracy, ease of use, cost, availability, maturity, use of resources, data requirements, etc.

1. Air MIDAS

Air Midas	
References used:	[Corker 03] [Corker,02] [Blom,Corker et al]] [Laughery,Archer, &Corker, K. 01] [Corker 00]
Alternate names:	None
Primary objective:	Used for impact analysis on the performance of single or multiple human operator(s) interacting with automation, complex procedures in Air Traffic Management, flight deck systems, process control systems and decision aiding systems. The model's primary purpose is to produce a prediction of the stream of behavior that will be observed in human interaction with complex dynamic systems and with other humans. In its Monte Carlo mode of operations (its most frequent use) the model produces distributions of behavioral sequences and performance times associated with those sequences. Risk or safety assessment with respect to that behavior is based on a post hoc analysis of the behavior sequences.
Description:	The Air MIDAS modeling framework provides interlinked human functional models which represent • Perception for auditory and visual stimuli (these model describe information seeking, and channel capacities of the human operator); • Attention (these models represent the processes of selection and limits of that selection after perception has taken place); • Memory functions (these models represent the encoding and retrieval process of working memory and the distinction in long term memory of procedural and declarative knowledge); • Cognition in the broad sense of decision making, action selection and knowledge application (Note that no learning processes are embodied in the Air MIDAS system); • An internal world representation is provided for each operator modeled. This representation includes the declarative facts about the simulation world known to that operator as well as the state of the procedures that make up that operators' intention. The internal world representation also hold "expectations" of the behavior of other agents in the simulation • Scheduling of behavior with an assumed concurrency of the activity scheduled as a default and then limitations in that concurrency imposed by consideration of channel capacity limits in visual, auditory, cognitive ,and motor constraints. • Queue management models are also used to guide activity and performance. These include task priority, interuptability and recommencement strategies, motor activity accuracy as a function of the speed accuracy tradeoff implicit in Fitts' law. These models work together with models of the operating environment (e.g. airspace) and other agents in that operating environment, (e.g., aircraft and other active assets like automation aiding systems) to stimulate activity in the human operator agents according to coded "goals" for performance in an active environment. The Air MIDAS human performance models also interact with other simulations systems for example simulations of airspace assets like the Simmod Pro or the reconfigurable flight simulator (RFS) to allow the more specialized external world simulations provide both faster overall simulation speed and higher fidelity to the Air MIDAS interaction with its environment.
Process steps:	The system under study must be identified in the following ways.

	1. A set of tasks and scenarios need to be defined. 2. The state of current or future equipment (at least in the most general sense of information required and control required) needs to be defined. This includes the active engagement of automation and aiding systems for the operator(s). 3. The human performance model depends on the development of a task decomposition of the procedures and the information requirements of a specific task. These are identified as supporting specific goals and these goals are then decomposed to sub goals and procedures to meet those goals. 4. The roles and responsibilities of the human(s) in the system are defined according to rules that are triggered by the appropriate stimuli in the world as represented in the external world models and in the "internal world" of the human agents. If there are no rules to map the state of the world to the operator's goals, then a knowledge based application of heuristics is undertaken. Then the model is run under the conditions specified and the human-system behavioral stream is produced. Deterministic Operation: As noted the model can be run in a deterministic model with no stochastic elements active in either the human operator(s)' behavior or in the simulated world. In this mode a "what-if" analysis can be performed with the model. That is to say, assuming all else remains the same, what would be the change to operator(s) behavior of introducing this change (in either procedure or equipment or in roles and responsibilities). Monte Carlo Operations: The modeled system can be run for a large number of repetitions (Monte Carlo mode) with parameters of the modeled performance varying within prescribed ranges. The result of these runs is a distribution of system performance and an exploration of options. This Monte Carlo process is supported by the fact that the model of human performance provides ranges of durations for action and provides variation in what action is selected to be performed based on environmental conditions and resource constraints. System Performance Results: Analysis of the resulting performance is undertaken to identify: • whether the objectives of the system are met, i.e. can the system as modeled perform the operations required (e.g approach and landing) successfully according to some criteria for success, • whether the human(s) in the system undergo high task load in the performance of the system, • Whether there are any conditions under which the system enters an unsafe or unstable condition. Operator performance results: The Air MIDAS system provides the analyst access to "internal processes" with the human operators represented such as: • Number of memory updates, • Number of activities begun and interrupted, • Specific decision alternatives considered, • Numeric estimates of workload and priority for task performance. The analysis of unsafe events is then usually undertaken by examining the state of the operator in the epoch surrounding that unsafe event (with special reference the "internal" variables) to attempt to get a causal chain associated with the unsafe action.
Applicability range:	The primary application of this system is to examine prototype systems, new operational concepts, new decision support tools, new aiding systems, display configurations etc-- for the full range of human-system integration. It has been used in air traffic management, flight deck design, nuclear power plant operation, helicopter design, and emergency operations response and more recently used to examine the interaction of teams of human

	operators in complex dynamic systems.
Life cycle stage:	Air MIDAS is usually used in the conceptual design stage
Experience in application to air traffic:	Air MIDAS has been used to examine: controller-pilot data link communications, CTAS operations, Free Flight safety zones, Cockpit alerts for turbulence detection, time-based and Miles-in-trail metering, stability on approach, advanced automated airspace management, European airspace analysis and URET interface analysis, dynamic re-sectorization based on controller load, automated handoff between sectors
Related methods:	There are several other cognitive process analysis tools that vary in the level of resolution at which they operate. ACT-R and EPIC, APEX, CPM-GOMS and Chi-Systems analysis tools have similar focus. They have not been used extensively for safety analyses however.
Availability and tool support:	Air MIDAS is a tool developed under sponsorship from the NASA, US Army, and FAA. As such it is available on a limited license basis. The functions of Air MIDAS are being developed for a web-based application that will provide access via internet to the Air MIDAS system.
Maturity:	Air MIDAS and earlier MIDAS have been under development since the late 80s and has been used successfully for analyses of aviation safety for 15 years. It is a mature and validated tool for human performance prediction. Recent development is making the system available for remote use of the world wide web.
Acceptability:	Air MIDAS has provided analytic solutions to principal investigators in Europe, and the US and most recently in Japan. The investigators have both used and validated the model's predictions, so the model output is acceptable. The model has not yet been made "general-user" acceptable.
Ease of integration:	Air Midas has been successfully integrated with RAMS, SIMMOD, RFS and other external world or human simulations. It has a clearly defined interface protocol.
Documentability:	Air MIDAS has an extensive web-based documentation archive as well as a web-accessible example program and the relevant research literature based on its use.
Advantages:	Air Midas can be used to simulate complex air traffic systems and scenarios with multiple human operators. Air MIDAS provides significant advantages in examining the human component of large scale systems. Its output has been used in risk and hazard analyses and its recent developments allow large numbers (millions) of runs to examine rare events.
Disadvantages:	Air MIDAS requires a high level of expertise in human performance and systems engineering to effectively model these systems. There is also a significant knowledge elicitation process that is needed as the model is applied to different operational concepts and as the analysis is applied to different problems.

2. Air Safety Database

References used:	Key references: • Airport Safety: A Study of Accidents and Available Approach-and-landing Aids, FLIGHT SAFETY DIGEST, Flight Safety Foundation, March 1996. • Air-ground communication safety study, EUROCONTROL, 2004. • Review of Air Traffic Management-related accidents world-wide, European Aviation Safety Seminar, 2003.
Alternate names:	NLR Air Safety Database
Primary objective:	To provide data for aviation safety analysis studies.
Description:	The NLR Air Safety Database contains detailed information on accidents and incidents of fixed wing aircraft from 1960 and onwards. The database contains information on more than 8,000 accidents and serious incidents that occurred worldwide. The data are obtained from a variety of accident / incident data sources: • ASRS • Airclaims CASE • ICAO ADREP • Robert E. Breiling Associates Business aircraft Accident Data • ALPA • NTSB accident/incident database • FAA Accident/Incident Data System database • Air Line Safety Reports • Accident data from accident investigation organizations worldwide • Accident/incident data from various mandatory occurrence reporting systems • Accident/incident data from aircraft manufacturers • Insurance claims Besides data on accidents/incidents the NLR Air Safety Database also collects and maintains non-accident related data: • Flight exposure data sources (EUROCONTROL, OAG, Airclaims CASE, ICAO, Aircraft manufacturers, Civil aviation authorities, ACI) • Airport data source (Jepessen airport data, ICAO, Airlines) • Weather data sources (Met offices worldwide) • Operator & aircraft fleet data sources (BACK aviation, Airclaims CASE, Aircraft manufacturers, IATA, ICAO) All data can be queried separately or in a relational way.
Applicability range:	The database covers a wide spectrum of aviation safety data. Although the main focus is on civil aviation, military transport aircraft are also covered by the database.
Life cycle stage:	The NLR Air Safety Database is updated frequently using reliable sources.
Experience in application to air traffic:	The NLR Air Safety Database has been used in many studies related to air traffic. Examples are: • Air-ground communication safety study (EUROCONTROL) • Model to assess the runway incursion vulnerability of an airport • Review of Air Traffic Management-related accidents world-wide • Safety aspects of air cargo operations • Safety aspects of crosswind operations • Airport Safety: A Study of Accidents and Available Approach-and-landing Aids (FSF) • Safety aspects of aircraft performance on wet and contaminated runways.
Related methods:	ASRS; PDARS
Availability and tool support:	NLR safety experts within the safety & Flight Operations department run the NLR Air Safety Database. Standard software tools are used to operate the database (e.g. SQL, DBASE, MS ACCESS, EXCEL etc).

Maturity:	The NLR Air Safety Database is the standard supporting tool for many safety studies conducted by NLR for many years.
Acceptability:	The NLR is widely recognised by the aviation community as a valuable source of aviation safety data.
Ease of integration:	-
Documentability:	-
Advantages:	The NLR Air Safety Database has been used in numerous safety studies directly related to ATM. Examples are the air-ground communication safety study conducted for EUROCONTROL, the review of ATM related accidents, and the development of a runway incursion vulnerability assessment model. The database is also used to obtain data to be used as input into different mathematical safety models.
Disadvantages:	Usage of the NLR Air Safety Database requires significant experience in aviation. Detailed knowledge of aircraft operations, aircraft design, basic flying techniques and experience in the field of accident/incident investigation are necessary to use the database effectively.

3. ASRS (Aviation Safety Reporting System)

References used:	ASRS: The Case for Confidential Incident Reporting Systems (white paper)
Alternate names:	None
Primary objective:	The program was designed primarily to support the FAA in its mission to eliminate unsafe conditions in the national aviation system, and prevent avoidable accidents.
Description:	When organizations and industries want to learn more about safety incidents and why people did what they did, the best approach seems to be to simply ask the participants. People are generally willing to share their knowledge if they are assured their identities will remain anonymous and the information they provide will be protected from disciplinary and legal consequences. A properly structured *confidential*, *voluntary*, *non-punitive* incident reporting system can be used by any person to share this information. Such a system has the strength and means to ask, and frequently answer, the question of *why*. There is no substitute for knowing why a system failed or why a human erred.
Process steps:	Fill out an incident report form, including fixed field and narrative information; submit the form to ASRS within 10 calendar days of incident occurrence; receive ID strip from reporting form as proof of submission.
Applicability range:	The technique can assess humans (human error, human behaviour), equipment (hardware, software, including HMI), and/or procedures/organization.
Life cycle stage:	Design. The technique can capture information on system and equipment design and implementation. However, the majority of ASRS reports apply to the operations and maintenance stages.
Experience in application to air traffic:	The ASRS program has been available to ATM facilities in the U.S. for 28 years and has been used for this length of time.
Related methods:	"Structured callback" or survey methodology can assist in successive quantification of the results. Reporters are contacted by telephone to answer a questionnaire based on incident occurrence. The questionnaire probes areas of operations that may not be reported fully in the incident report form. The survey may gather both quantitative and qualitative information.
Availability and tool support:	The technique is widely available; incident reporting forms can be obtained by downloading forms from the ASRS web site at http://asrs.arc.nasa.gov; from FAA Flight Service Stations; from FAA Flight Standard District Offices; from air carrier flight operations offices; from professional aviation organizations; and by directly contacting the ASRS.
Maturity:	The ASRS program is entering its 28th year of operation. It has received more than 600,000 incident reports without violating reporter confidentiality. It is a proven national resource and is the world's largest aviation incident reporting system.
Acceptability:	The ASRS program has undergone formal evaluation by the National Academy of Public Administrators (NAPA) and a NASA Task Force in 1994-95; and again in 2001 by a NASA task force. In each case the ASRS received positive overall evaluations. The main weaknesses noted were system limitations due to funding constraints (inability to full-form process more than a certain percentage of reports received).
Ease of integration:	The technique is generally a standalone technique, and is easy to understand and use.
Documentability:	The ASRS system has a high degree of documentability, in that a record of each incident report is produced, and the documentation is usable for future system operations. The ASRS database currently holds more than 112,000 full-form records covering the time period from 1988 to 2004. Reports are processed using the Analyst Workbench computerized software application, which fully documents each incident record, and tracks it from date of receipt to date of final processing.
Advantages:	ASRS reporters are forthcoming about their mistakes and those of others. Through its Alert Message process, the ASRS program gathers useful safety information from

	organizations and individuals and disseminates this information system-wide. This information includes problems with ATM procedures and facilities. Reporters' recommendation for improving safety are included in the Alert Messages. Often a single incident report can provide useful results when used as the basis of an Alerting Message.
Disadvantages:	Information collected through the ASRS is subjective and not verifiable. It cannot be used as the basis for statistical conclusions because it is submitted voluntarily, and cannot be considered a random, representative sample. Data collected may also be subject to self-reporting biases. Although mature, the ASRS system is labor-intensive and requires expert analyst support for report processing. Any restrictions on applicability, e.g. problem scale, generality, accuracy, ease of use, cost, availability, maturity, use of resources, data requirements, etc.

4. Bias and Uncertainty Assessment

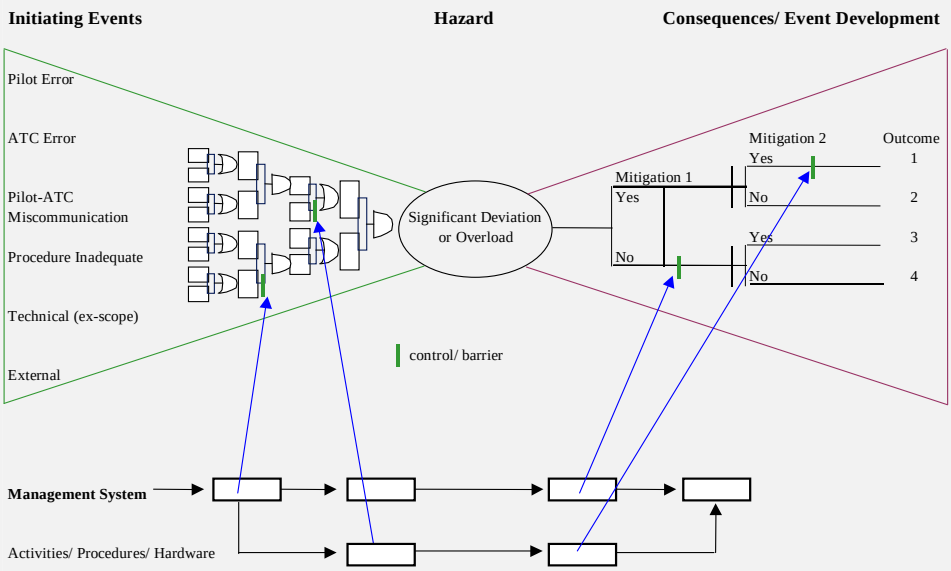
References used:	Key references: • [Everdij&Blom02] • [Everdij and Blom04] Other references: • [FT handbook02] • [Henley&Kumamoto92] • [Kumamoto&Henley96] • [Nurdin02]
Alternate names:	None
Primary objective:	When risk (e.g. accident risk) is assessed using a simulation model of reality, there is always an uncertainty as to whether the model-based risk result is a good representation of realistic risk. This is due to the fact that during the modeling, assumptions need to be adopted, and values need to be given to parameters for which sometimes no reliable data is available. In this template, the terms 'assumption' and 'parameter' are used with the following interpretation: • An assumption describes a particular issue that (for some reason) has not been covered by the model of reality considered, but that may be a relevant aspect of reality itself. Example: 'In the model, the pilot is assumed not to disconnect the autopilot deliberately'. • A parameter is a model entity that can have a particular numerical value. Example: 'The reaction time of a pilot in response to a TCAS alert is denoted by a parameter R_{TCAS}. In the model, R_{TCAS} has a value of 5 seconds'. Due to choices of model assumptions and parameter values, the model differs from reality, hence the accident risk that comes out of the model may also differ from realistic accident risk. Some assumptions (pessimistic assumptions) have increased model-based risk with respect to realistic risk. Other assumptions (optimistic assumptions) have decreased model-based risk with respect to realistic risk. The effect of uncertainties in parameter values also has an effect on the gap between model-based risk and realistic risk. This effect is influenced by the size of the uncertainty in the parameter value used (e.g., major uncertainty, or only minor uncertainty), but also by the sensitivity to risk of the parameter (if accident risk is less sensitive to changes in a parameter, then a particular uncertainty in the parameter value has a smaller effect on the uncertainty of model-based risk). A Bias and Uncertainty Assessment gives insight into the gap between model-based risk and realistic risk.
Description:	Bias, uncertainty and sensitivity assessment as a generic term is often applied at a low level, e.g. only the most obvious assumptions are assessed individually (e.g., 'the effect of this assumption is less than 2%'), and for the parameters that seem most critical two other values are used to obtain an optimistic and a pessimistic result. For particular modelling techniques such as Fault Tree Analysis, more advanced uncertainty assessment techniques have been developed, see e.g. [Kumamoto&Henley96], [Henley&Kumamoto92], [FT handbook02]. These uncertainty assessments deal with parameter values only. A technique that evaluates the combined effect of bias and uncertainty of all model assumptions and all model parameter values has been developed in [Everdij&Blom02]. This technique assesses the bias and uncertainty in model-based accident risk, with respect to realistic accident risk. It follows several steps: 1. Identify all model assumptions adopted and identify all parameter values used in the model. Usually, assumptions exist of various types, such as numerical approximation

	assumptions, model structure assumptions, assumptions due to non-coverage of identified hazards, etc. 2. Assess each model assumption separately on two aspects: • Did its introduction increase model-based risk with respect to realistic risk (i.e. is it a pessimistic model assumption) or did it decrease risk (i.e. is it an optimistic model assumption) • By what factor did it increase or decrease risk. This factor is to be taken relative to all factors for assumptions already assessed. Both aspects are generally to be judged by operational experts. Next, model-based accident risk is compensated for all model assumptions adopted, by using the assessed factors one by one to increase or decrease model-based accident risk. For example, if the first assumption was judged to be pessimistic by a factor 2, then model-based risk is divided by a factor 2 to compensate for this assumption (so that it comes closer to realistic risk). If the second assumption was judged to be pessimistic by a factor 1.5, taking account of the factor for the first assumption, then model-based risk is divided by an additional factor 1.5 to compensate for this second assumption. 3. Assess each model parameter value on two aspects: 95% credibility interval for the parameter value; and Risk sensitivity, expressed by the factor by which risk changes if the parameter value is changed by some normalised factor. From these assessments, a particular mathematical formula (see [Everdij&Blom02]) is used to find a 95% credibility interval around model-based risk, due to biases and uncertainties in the model parameter values. 4. The output of steps 2 and 3 are combined to obtain a 95% credibility interval for realistic accident risk, based on the model-based risk value, the model assumption assessments and the parameter value assessments. To save expensive computational time, steps 2 and 3 can be performed through qualitative assessments first (i.e. in terms of e.g. negligible, minor, significant, considerable, major), after which the most influential assumptions and parameter values are re-assessed quantitatively.
Applicability range:	The method is applicable to all types of mathematical models, hence applicability restrictions are based on applicability range of the model the technique is applied to.
Life cycle stage:	Any lifecycle stage in which model-based assessments are used.
Experience in application to air traffic:	The technique has been applied several times to complex ATM situations.
Related methods:	No specific related techniques identified.
Availability and tool support:	The technique is publicly available. Tool support is dependent on tool support for the model assessed: These tools should be able to re-run the model with another parameter value setting. In addition, a spreadsheet could come in handy to keep track of and to combine the results numerically.
Maturity:	The technique has only been developed recently (2001) but has been applied several times to various complex real ATM accident risk assessments. The technique is being further developed.
Acceptability:	The theoretical background of the technique has been reviewed by independent reviewers, but not by regulatory authorities. A study has tested the parameter value-part of the technique on numerical accuracy, with positive results, albeit that the test case was a simple one [Nurdin02].
Ease of integration:	The technique is easy to understand, however, it requires the input of various resources and operational expertise. It can be applied to any model-based result, including fault trees. All assumptions on which the technique is based are listed in [Everdij&Blom02]; these assumptions are of rather technical nature and may not be easily understood by non-experts.
Documentability:	Since assessments of assumptions through expert judgement are often subjective,

	assessment by other experts may lead to different results. However, since documentability is reasonably high, all steps and sub-steps made during application of the technique can be reviewed (and modified, if necessary) by independent experts. Particular assessments that involve running the model require an expert who knows how to do that; however, since this type of assessment is not subjective, a similar result should be obtained by another expert.
Relevance to ATM:	A Bias and Uncertainty Assessment is an essential step in any model-based assessment, since otherwise there is no telling how far the model-based results could deviate from reality. General strengths of the technique described are: 1. It assesses and compensates for the effects of all model assumptions (including parameters) adopted, not just a few of them. 2. The effects of combinations of assumptions on the risk result are taken into account. 3. It generates both an expected risk result, and a 95% credibility interval for realistic risk. 4. The results of application of the technique are well documented, hence any subjectivity in the results can be reviewed and modified by independent experts. 5. The technique can be applied at a qualitative level first, which saves use of valuable resources.
Con's and resources:	The technique relies heavily on the following resources: • Operational experts who must have a feeling for (changes in) accident risks • An expert who is able to run the underlying accident risk model with different parameter settings • Statistical data (or expert judgement-based data) on suitable parameter values, including credibility intervals for these data General weaknesses are: 1. The resources required heavily depend on the complexity of the model to be assessed. 2. The assumptions on which the technique is based are rather technical, hence hard to verify by non-experts. 3. The technique relies partly on expert judgement, hence these results may be subjective.

5. Bow-Tie Analysis

References used:	Key references: • [Edwards99] • [Zuijderduijn99] Other references: • [Bishop90] • [Blom&Everdij&Daams99] • [DNV-HSE01] • [EHQ-PSSA] • [EN 50128] • [GenericBT] • [MHF-RGN10] • [Rademakers&al92] • [SGS-FSR] • [Trbojevic&Carr99] • [Villemeur91-1] Additional reading: • [Petrolekas&Haritopoulos01]
Alternate names:	Butterfly model, according to [SGS-FSR]
Primary objective:	Bow-Tie Analysis is executed as part of a Hazards and Effects Management Process (HEMP). The primary objective of Bow-Tie Analysis is to give safety experts a means to communicate with operational experts regarding safety findings, so that these operational experts can identify preventive and recovery measures for hazards, while the safety experts keep a neutral position. A Bow-Tie itself is a pictorial representation of how a threat can be hypothetically released and further developed into a number of consequences.
Description:	For each step in the Bow-Tie, Safety analysts can use Operational experts to systematically generate ideas to improve safety. All safeguards relating to the hazard are shown explicitly and colour coding can be used to differentiate technical and procedural safeguards, and potentially the role of specific individuals or groups. The link to the safety management system depends on the safeguard type. If it is technical then it might link to the preventive maintenance portion; if it is procedural it might link to the training and qualification system, and both to the ongoing monitoring and audit program. Bow-Tie Analysis is a tool that has both proactive and reactive elements and that systematically works through the hazard and its management. It uses a methodology known as the Hazards and Effects Management Process (HEMP) ([Edwards99], [Zuijderduijn99], [Blom&Everdij&Daams99]), which requires threats to be identified, assessed, controlled and if subsequently they are released, to identify recovery measures to be in place to return the situation to normal if possible. The pictorial representation of the Bow-Tie exists in several versions, depending on the application and preferences of the users. Still, in most representations, the knot of the Bow-Tie represents a Hazard, the left-hand side wing includes contributors leading to threats that can cause the hazard, the right-hand side wing includes consequences of the hazard. To mitigate a hazard, barriers are incorporated on the left-side and controls are added to the right-side of the Bow-Tie.

	In one version, the Bow-Tie is produced as a combination of Fault Tree (which shows how initiating events and combinations of failures lead to a hazard) and Event Tree (which shows consequences of the hazard).  The Bow-Tie diagram size is preferably limited to a single page and ideally should be kept simple, as their main function is to demonstrate mechanisms and to allow staff and managers to understand how major hazard events can occur and what safeguards exist to prevent them. One qualitative decision tool is to judge the qualitative risk and based on whether this is high, medium or low, then more or fewer safeguards are required. To ensure good balance, the approach demands equivalent safeguards on both sides of the Bow-Tie. This ensures that preventive barriers as well as mitigation barriers both exist. A good check is to list methodically every safeguard identified in the hazard identification and confirm that these appear on the Bow-Tie relating to that major hazard. This helps linking the hazard identification to the subsequent risk analysis. Once the diagram is completed it becomes visually obvious where there is insufficient safeguarding and conversely where there might be excess safeguarding.
Steps:	The stages worked through in a Bow-Tie are [Edwards99] Proactive measures: • Identification of the hazard contributors • Identification of the hazard initiators that could release the hazard contributor • Assessment of the hazard controls already in place and the identification of additional controls that may be necessary to manage the hazard effectively • Identification of the Hazard that can lead to an accident Reactive measures: • Assessment of the Recovery measures that would be appropriate to return the situation to as near to normal as possible • Assessment of the Consequences that may be incurred if controls fail and the hazard completes its cycle from release to result • Identification of the Mitigating measures that must be taken to reduce to a minimum the effect of the consequences upon the company and the people involved.

	A representation of these steps is provided by the figure above, which is from [Edwards99], [Blom&Everdij&Daams99], and which has the shape of a Bow-Tie.
Applicability range:	The technique can incorporate technical system failure, as well as human error. Also inadequate procedures can be incorporated in the analysis.
Life cycle stage:	Bow-Tie analysis can be used in the definition or design stages, in order to link hazard causes to their consequences. During later stages it can be used to assess whether preventive or mitigating measures have been put properly into place. In the definition phase, the Bow-Tie is used from the left to the right (the left part being limited) to identify the consequences of a hazard; however, it can also be used from the right to the left to identify the worst credible case and consequently allocate a safety objective to the hazard knowing its effect's maximum tolerable frequency of occurrence and the success/fail rate of each barrier. Then in the design phase (understanding what can cause the hazard) it is used from the right to the left to apportion Safety Objectives to Safety Requirements. It is also used from the left to the right to validate that the design and its implementation meet the Safety Objectives.
Experience in application to air traffic:	Most applications of Bow-Tie analysis have been in the chemical and petro-chemical industries. [Edwards99] describes its use for Shell Aircraft, while developing a Safety Case for an aircraft operator. The more specific version that links FTA and ETA into a Bow-Tie has been used for ATM applications.
Related methods:	Link to PRA (Probabilistic Risk Assessment based on FTA/ETA) or PSA (Probabilistic Safety Assessment). In [EN 50128], [Rademakers&al92], [Villemeur91-1], [Bishop90], a diagram where Fault Trees are linked to Event Trees through one critical event are named Cause Consequence Diagrams. According to [GenericBT], the Bow-Tie Diagram combines Cause Consequence Diagrams, Barrier and Recovery Diagrams, Swiss Cheese Model (J. Reason), Fault and Event Trees, Error Likely Situations (ELS), Accident Prone Situations (APS), and Influence of Human Factors and effects of Human Errors.
Availability and tool support:	At least one supporting tool is available. See the Global Aviation Information Network (GAIN) Working Group B (Analytical Methods and Tools).
Maturity:	The Bow-Tie Diagram has evolved over the past decades from the Cause Consequence Diagram of the 1970s and the Barrier Diagram of the mid 1980s. It has been most often used in chemical and petro-chemical industries. The approach has been popularised only recently (EU Safety Case Conference, 1999) as a structured approach for risk analysis within safety cases where quantification is not possible or desirable.
Acceptability:	Occupational Health and Safety (Major Hazard Facilities) Regulations state in their Regulatory Requirements (Reg 303): [MHF-RGN10] • The operator needs to be able to identify and understand the links between identified hazards and the control measures intended to address those hazards; • The operator must understand and have documented the various types of control measure on the facility, the means by which the control measures eliminate hazards or reduce risk, and the effect the control measures have on that hazard or risk, and refer to Bow-Tie diagrams as a simple method of linking and communicating the information together.
Ease of integration:	When a Bow-Tie is used by combining Fault Trees and Event Trees, the ease of construction of a Bow-Tie diagram is directly related to the ease of constructing a fault tree and an event tree. However, since only simple fault trees and event trees are commonly used for a Bow-Tie, this task is relatively less complex than for full FTA and ETA.
Documentability:	As with fault trees and event trees, the end-result of a Bow-Tie analysis can be well documented, however, in practice, the assumptions adopted and the steps leading to the end-results are often not described and are not easily audited by independent experts.

	This approach lends itself well to risk communication. The format is not overly complex and non-specialists can understand the approach. All safeguards relating to the hazard are shown explicitly and color coding can be used to differentiate technical and procedural safeguards, and potentially the role of specific individuals or groups. [DNV-HSE01]
Advantages:	The Bow-Tie approach has become an increasingly common technique to identify under-controlled areas of the overall system. A key benefit is the ability to link the assessment to the activities required to control risks and the broader safety management system [EHQ-PSSA]. Other general advantages are [DNV-HSE01]: 1. It is good for awareness, education and communication 2. The full range of initiating events is shown 3. The intervening safeguards are clearly shown 4. The actual way in which these combine and escalate is clearly shown 5. The consequences side shows barriers in an equivalent manner 6. The many possible consequence outcomes are defined 7. The linkage of the barriers to the safety management system can be made explicit 8. Once a good Bow-Tie is produced, the resources required to use it in communication with operational experts are rather limited
Disadvantages:	Some weaknesses are: 1. In ATM it is not always possible to think in a fixed sequence of events to define a Bow-Tie. 2. Semi-quantitative approaches to risks, such as Bow-Tie Analysis, are not normally suitable to evaluate the acceptability of the risks. They are optimised to highlight the safeguards that are in place, and to ensure that suitable safeguards are considered for each hazard. By themselves, they do not provide a framework to evaluate whether the selected safeguards are sufficient. [DNV-HSE01] 3. The technique does not help identify common causes of failures or links between barriers or design elements. 4. The “distance” between the hazard (at the boundary of the operation being assessed) and the end effects has an impact on the effectiveness of the technique when trying to allocate a safety objective to the hazard (in the knot).

6. CCA (Common Cause Analysis)

References used:	Key references: • [ARP 4754] • [SAE2001] Other references: • [DS-00-56] • [Dvorak00] • [EN 50128] • [FAA00] • [Lawrence99] • [MUFTIS3.2-I] • [OSTI] • [ΣΣ93, ΣΣ97] • [Sparkman92] • [SQUALE99] • [Zio02]
Alternate names:	Sometimes referred to as another name for Zonal Analysis.
Primary objective:	The purpose of CCA is to identify any accident sequences in which two or more events could occur as the result of one common event. These common causes or events may result from a common process, manufacturing defect, a common human operator error, or some common external event. Common causes are present in almost any system where there is any commonality, such as human interface, common task, and common designs, anything that has a redundancy, from a part, component, sub-system or system. In hardware systems, common causes typically deal with physical location and manufacturing characteristics such as common subjected environments, wire routing through a common connector, common design processes that introduce a generic design defect, or susceptibility to common calibration errors because a defective instrument (or procedure) was used during installation or maintenance. If the probability of a common cause is significantly greater than the probability of the two or more resulting events occurring independently, then the common cause could be an important risk contributor.
Description:	Common Cause Analysis exists in different versions. In [ARP 4754] (frequently referenced by other documents), CCA is said to be a generic term, subdivided into the following three areas of study to aid in the assessment: • Zonal Analysis (generally named Zonal Safety Analysis in avionics), which should examine each physical zone of the aircraft to ensure that equipment installation and potential physical interference with adjacent systems do not violate the independence requirements of the systems. An important aspect is the identification of interfaces and interference with other parts of the system. Zonal Analysis is used to identify sources of common cause failures and effects of components on their neighbours. It is an analysis of the physical disposition of the system and its components in its installed or operating domain. It should be used to determine: a) The consequences of effects of interactions with adjacent systems in the same domain. b) The safety of the installation and its compliance with relevant standards and guidelines. c) Areas where maintenance errors affecting the installation may cause or contribute to a hazard. d) The identification of sources of common cause failure; e.g. environmental factors. e) Transportation and storage effects. [DS-00-56], [MUFTIS3.2-I] • Particular Risks Assessment (sometimes referred to as Environment-related Common Cause Analysis), which should examine those common events or influences that are outside the system(s) concerned but which may violate independence requirements. These particular risks may also influence several zones at the same time, whereas Zonal Safety Analysis is restricted to each specific zone. Some of these risks may also

	be the subject of specific airworthiness requirements. Examples of the risks considered are fire, leaking fluids, loss of power supply, loss of network connections, tire burst, High Intensity Radiated Fields (HIRF), exposure, lightning, uncontained failure of high energy rotating fields, etc. Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects, or influences, that may violate independence [Dvorak00] • Common Mode Analysis (or Process-related Common Mode Analysis), which provides evidence that the failures assumed to be independent in the system design are truly independent. It considers the effects of specification, design, implementation, installation, maintenance errors, manufacturing errors, environmental errors other than those already considered in the particular risk analysis, e.g. hardware errors, common type of equipment or technologies, common development, software errors, manufacturing or installation errors, common maintenance procedures or personnel, common assessment activities or procedures, environmental issues such as temperature. [Dvorak00]. In [Lawrence99], the following steps constitute the CMA phase: 1) Establish specific checklists; 2) Identify the CMA requirement (through analysis of FTA And gates or by review of specific product checklists); 3) Analyse the design to ensure compliance with requirements; 4) Document the results in a CMA report. The output of a Common Cause Analysis therefore includes [SQUALE99]: • From the Zonal Analysis: 1) a List of widely independent parts (zones) of the system; 2) A list of interfaces and remaining dependencies between the parts; 3) A list of failures of the individual parts that may have impacts on other parts of the system. The failure modes and effects are also described. • From the Particular Risks Assessment: 1) A description of the analysed environment related hazards; 2) A list of the parts of the system affected by these hazards; 3) A description of the failure modes caused by these hazards as well as a description of its effect; 4) A description of the deviation to the initial assumptions and the implication of this deviation. • From the Common Mode Analysis: A list of common mode failures and their effects. In [ΣΣ93, ΣΣ97] and in [SAE2001], the basic steps to common cause analysis are: 1. Identify and group the critical components to be evaluated. These components and their relationships can be identified using other analysis techniques, such as FMEA and FTA. 2. Within the groups, check for commonalities such as physical location and manufacturing characteristics, common manufacturers, a common design process that could introduce a generic design defect, etc. 3. Within each identified commonality, check for credible failure modes such as, electrical shorts or opens, maintenance errors, etc. 4. Identify generic causes or trigger events that could lead to the credible failure modes, such as, corrosion, overheating, fire, flood, etc. 5. Based on the above, draw conclusions and make recommendations for corrective action. Corrective actions include requirements redesign, invoking emergency procedures, and function degradation. Reference [OSTI] explains how common causes can be identified from the minimal cut sets of fault trees (see the FTA section for a definition of minimal cut sets): Minimal cut sets containing events from components sharing a common location or a common link are called common cause candidates. Components share a common location if no barrier insulates any one of them from the secondary cause. A common link is a dependency among components that cannot be removed by a physical barrier (e.g., a common energy source or common maintenance instructions). The fault tree minimal cut sets are searched for shared susceptibility to various secondary events (common causes) and common links

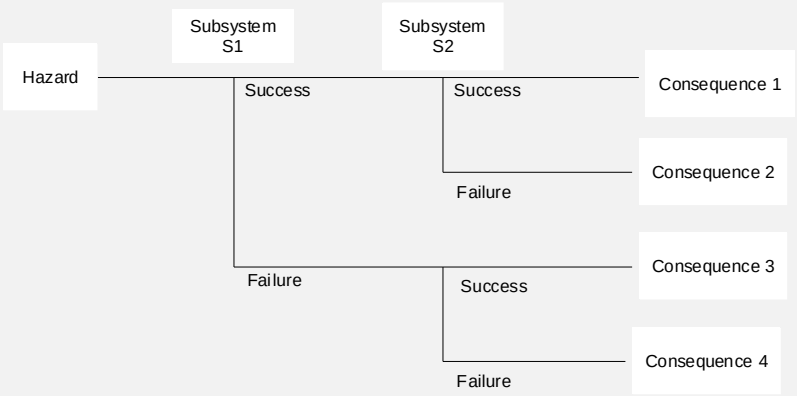
	between components. In the case of common causes, a location check may also be performed to determine whether barriers to the common cause exist between components. Common manufacturers of components having events in the same minimal cut set can be located. A relative ranking scheme for secondary event susceptibility can be included. In [FAA00] this technique is named Common Cause Failure Analysis (CCFA). Tools available. See also [Zio02].
Applicability range:	Mostly used for hardware, but can also be used to incorporate human error or software problems. For software, the technique is named Common Cause Failure Analysis in [EN 50128], but the description in [EN 50128] does not mention Fault trees, while [FAA00] does when referring to CCFA. [Sparkman92] refers to CCFA as an extension of FMEA to include common mode failures of redundant components.
Life cycle stage:	May be performed at any lifecycle stage, from definition to decommissioning. Obviously, the most cost-effective time is early in the design process because of the potential influence on system architecture. However, confirmation may not always be feasible until implementation is complete [ARP 4754].
Experience in application to air traffic:	CCA has been applied and recommended by the Society of Automotive Engineers (SAE), in their Aerospace Recommended Practice documents, although mainly in aircraft hardware and software assessments. NASA uses CCA since 1987.
Related methods:	Link to Zonal Analysis (ZA), Zonal Safety Analysis (ZSA), Common Mode Failure Analysis (CMFA), Beta-Factor Method, Shock Method, Common Mode Analysis (CMA), Multi-Level HAZOP (HzM), Human Performance Limiting Values (HPLV), Emergency Exercises, Re-try Fault Recovery, Return to Manual Operation. Related to Root Cause Analysis, Contingency Analysis.
Availability and tool support:	Supporting tools are available. The analysis can also be supported by checklists.
Maturity:	CCA has been used at NASA since 1987. The CCA term itself is probably older (older than 1975).
Acceptability:	CCA is recommended by the SAE (Society of Automotive Engineers) for assessment of Airborne Systems and Equipment.
Ease of integration:	CCA can be integrated with and uses input from other hazard analysis techniques such as FMECA, FTA and ETA. CCA requires a deep knowledge of the development, operation, maintenance, installation and system disposal processes.
Documentability:	The use of checklists ensures a systematic analysis of the zones of the system, the interfaces between these zones, external events and common mode failures. Justification of completeness of these lists and on independence assumptions between the different parts should be given. This ensures good documentability of the results.
Relevance to ATM:	Common causes are often very important sources of safety critical situations, hence their identification is important for ATM safety assessments. General advantages of CCA are: 1. Potential common cause failures are most easily identified 2. As Common Cause Failures are addressed, one learns about how common cause failures will take place. CCA will enable a focus on recovery from such failures, leading to a more resilient and robust system.
Con's and resources:	In terms of resources to be used, a CCA is generally quite demanding. General weaknesses are: 1. It is a problem to be complete when addressing operations in ATM (due to unimaginable common causes and a high degree of interactions between elements in the ATM operation). 2. The method is relatively unstructured. 3. It is difficult to be used when the system analyzed includes COTS (Commercial Off The Shelf) equipment or software. 4. It is difficult to know where to stop the analysis.

7. Collision Risk Models

References used:	• [Bakker&Blom93] • [Blom&Bakker02] • [Brooker02] • [ICAO CRM80] • [Mizumachi&Ohmura77] • [MUFTIS1.2] • [MUFTIS3.2-II] • [Reich64]
Alternate names:	
Primary objective:	Mathematical models used in predicting risk of mid-air collision or collision with obstacles.
Description:	Several collision risk models exist, amongst which: • Collision Risk Model (CRM) of ICAO Obstacle Clearance Panel. This is a statistical model of the vertical and lateral behavior by aircraft on ILS arrival path. [ICAO CRM80] • Gas model: Analytical accident risk model to determine probability of collision between aircraft or to assess air traffic controller workload. Based on the physical model of gas molecules. [MUFTIS1.2] • Generalized gas model: Analytical model. Based on the gas model, but the aircraft do not always fly in random directions. Aim is to determine probability of collision between aircraft or to assess air traffic controller workload. [MUFTIS1.2] • Absorbing boundary model: Collision risk model; Reich-based collision risk models assume that after a collision, both aircraft keep on flying. This one does not. • Reich Collision risk model, adopted by ICAO. Estimates of the level of risk of a mid-air collision between two en route level flying aircraft under procedural control. Under several assumptions, two of which are rather restrictive, the model allows to calculate collision risk from traffic factors, aircraft parameters and navigational performance. Mainly applies to largely strategic procedures only. No dynamic role for ATCos and pilots; basic logic is "navigational errors -> mid-air collisions". [Bakker&Blom93], [Brooker02], [MUFTIS3.2-II], [Reich64] • Refined Reich collision risk model: Refinement of Reich collision risk model (CRM) to evaluate risk of collision between aircraft. Replaces the two restrictive Reich assumptions by one less restrictive one. [Bakker&Blom93], [Mizumachi&Ohmura77], [MUFTIS3.2-II] • Generalized Reich collision risk model: Generalization of Reich collision risk model. For the determination of collision risk between aircraft. Does not need two restrictive assumptions that Reich's CRM needs. Used within TOPAZ. Bakker&Blom93], [Blom&Bakker02], [MUFTIS3.2-II]
Applicability range:	For each of the mathematical collision risk models certain restrictions of their applicability apply. Appropriate application of the model within its restrictions requires expert knowledge.
Life cycle stage:	Concept onwards
Experience in application to air traffic:	Ample experience in applications to air traffic applies to all these models
Related methods:	TOPAZ, ETA
Availability and tool support:	All are publicly available in literature.
Maturity:	All models are mature
Acceptability:	All models are well accepted

Ease of integration:	Significant level of mathematical expertise is required to judge the precise integration of a model within a collision risk assessment.
Documentability:	
Advantages:	ICAO supported modeling approach
Disadvantages:	Level of expertise required for an appropriate integration

8. ETA (Event Tree Analysis)

References used:	Key references: • [Leveson95] Other references: • [Baybutt89] • [DNV-HSE01] • [MUFTIS3.2-I] • [Rademakers&al92] • [Rakowsky] • [Reason90] • [ΣΣ93, ΣΣ97] • [Siu94] • [Smith9697] • [Storey96] • [Terpstra84] • [Villemeur91-1] Additional reading: • [Apthorpe01], [Bishop90], [EN 50128], [FAA00], [Fota93], [Kirwan&Ainsworth92], [Kirwan94], [Moek84], [Parry92], [Roberts&al81], [Toola93]
Alternate names:	Former name is Consequence Tree Method [Villemeur91-1].
Primary objective:	An Event Tree models the sequence of events that results from a single hazard or initiating event and thereby describes how serious consequences can occur. ETA can be used for developing counter measures to reduce the consequences.
Description:	An ETA reasons forwards, starting from the hazard or initiating event. From here on, two branches are introduced which represent the functioning and disfunctioning of the first (sub)system which is designed to reduce the effect of the hazard. Each of these branches splits into two branches that represent the functioning or failure of the second (sub)system, etc. With each branch of the thus constructed tree a particular consequence is associated, e.g. safe situation, minor loss, major loss, disaster. If for a branch the functioning or failure of a (sub)system does not influence the further consequences anymore, the branch is not split at that point, so that the tree is reduced. An example event tree is given in the figure below. Here, consequence 2 is the result of success of subsystem S1, followed by failure of subsystem S2.  The technique is easily extended to include non-binary outcomes of branches, i.e. branches splitting up in three or more branches. Large event trees can be reduced by eliminating

	sequences whose functional and operational relationships are illogical or meaningless, e.g. branches that cannot occur given the sequence of branches that precedes it. Quantification of an event tree is relatively simple, and is readily performed by hand, although spreadsheets or computer models are increasingly used to automate the multiplication task. A probability is associated with each branch, being the conditional probability of the branch, given the answers (success/failure) of all branches leading up to it. Fault trees for the subsystems above the tree and for the hazard or initiating event are often used to determine these probabilities. In each case, the sum of the probabilities of each branch must be unity. The probabilities of each outcome are the products of the probabilities at each branch leading to them. The sum of the probabilities for all outcomes must be unity as well. This provides a useful check on the analysis. [DNV-HSE01] There have been cases in which a continuous random variable (instead of a binary event outcome) has been introduced in an event tree [Leveson95]. This analysis uses a continuous conditional probability density and provides continuous joint distributions. In [ΣΣ93, ΣΣ97], the basic steps to constructing an event tree are: 1. List all possible hazards or initiating events, e.g. based on review of the system design and operation, the results of another analysis such as FMEA, Hazardous Operations Analysis, etc., or personal operating experience acquired for a similar system 2. Identify functional system responses 3. Identify support system responses 4. Group hazards or initiating events with all responses 5. Define accident sequences, using the structure as in the figure above. At the end of each sequence is an indication of the consequences that can be expected 6. Probabilities can be assigned to each step in the event tree to arrive at total probability of occurrence for each accident sequence. First a Functional event tree can be built, then a System event tree. In large scale risk studies often the terms Small Event tree/Large Fault tree (SELF, also called Fault tree linking) and Large Event tree/Small Fault tree (LESF, also called Boundary conditions approach) are used [Siu94].
Applicability range:	The technique is universally applicable to technical systems of all kinds, with the limitation that unwanted hazards (as well as wanted events) must be anticipated to produce meaningful analytical results. In some applications, human error is also incorporated. [Rakowsky] claims ETA can also handle software.
Life cycle stage:	Like FTA, ETA is most appropriate after most of the design is complete. However, it can also be used during definition phase to define some interactions between the system and barriers, or between barriers, and to decide to set objectives onto some barriers such that they have a certain efficiency (success/failure rate).
Experience in application to air traffic:	ETA has been widely studied in various industries, such as nuclear industry (its main area of use), offshore business, aviation. Simple event trees have been used in [Smith9697] for an application to ATM route structures.
Related methods:	Link to DFMM (Double Failure Matrix Method), HRAET (Human Reliability Analysis Event Tree), COMET (COMmission Event Trees), PRA (Probabilistic Risk Assessment based on FTA/ETA) or PSA (Probabilistic Safety Assessment). Sometimes, the combined use of event trees and fault trees, after a Preliminary Hazard Analysis (PHA) is named PSA (Probabilistic Safety Assessment) or PRA (Probabilistic Risk Assessment), [Baybutt89], [Reason90]. PSA is a very largely spread technique in safety analysis of nuclear and chemical plants. In addition, ETA can be used with FTA in the Bow-Tie Analysis approach. Event Sequence Diagrams (ESD) form another generalization of ETA, which are not

	necessarily restricted in their representation of event sequences. ESDs are developed for each group of initiating events. Alternative success paths are allowed, repairable systems can be modeled. They can be extended to include accident scenarios in which the operating crew is treated in a behavioral manner. The term ESD is sometimes used as a label for the class of methods between ETA and dynamic methods, which are discussed later. An example of an ESD is given in Appendix A.7 of [Rademakers&al92]. One method to quantify event trees (and, additionally, fault trees) is Phased Mission Analysis [Terpstra84], which is reviewed in Appendix D.2 of [MUFTIS3.2-I].
Availability and tool support:	The technique is widely available. Supporting tools exist.
Maturity:	ETA was developed in 1980 and has been used widely since, especially in the nuclear power industry.
Acceptability:	ETA is widely used and well accepted.
Ease of integration:	In [ΣΣ93, ΣΣ97], ETA is referred to as a technique among the more difficult. Successful application to complex systems cannot be undertaken without formal study over a period of several days to several weeks, combined with some practical experience. Once mastery is achieved, the technique is not particularly difficult to apply. ETA can be easily combined with FTA in various ways.
Documentability:	In principle Moderate, but in practice, the assumptions made during the event tree construction process are not commonly documented. The choice of events (primary or otherwise) is often subjective, so event trees by different teams vary.
Relevance to ATM:	ETA can be very useful to ATM applications in combination with fault trees. Other general strengths of ETA are: 1. It is widely used and well accepted. [DNV-HSE01] 2. It is suitable for many hazards in QRA that arise from sequences of successive failures. [DNV-HSE01] 3. It a clear and logical form of presentation. [DNV-HSE01] 4. It is simple and readily understood. [DNV-HSE01] 5. ETA makes it possible to analyse event sequences. 6. Sequences of conditionally independent events can be handled systematically. 7. ETA can identify alternative consequences (system damage states) of failure. 8. Complex systems, made of subsystems in interaction, can be described. 9. It is one of the most exhaustive techniques, if properly applied. 10. Event trees are better at handling notions of time and logic than fault trees. 11. Event trees can be helpful in identifying the protection system features that contribute most to the probability of an accident, so that steps can be taken to reduce their failure probability 12. Event trees can be helpful in identifying top events for fault trees. They can also be helpful for displaying various accident scenarios that may result from a single initiating event.
Con's and resources:	ETA can be time-consuming. A potential disadvantage is that event trees can appear very impressive but contain serious errors. Care must be taken to thoroughly review the resulting tree against the system descriptions, assumptions and judgement factors. Due to the high need for resources, ETA use is reserved for systems wherein risks are thought to be high and well concealed. Other general weaknesses of ETA are: 1. An event tree can become very complex, especially when a number of time-ordered system interactions are involved. 2. Defining the subsystems at the top of the event tree, and their order, is sometimes difficult. 3. Static systems are also difficult to handle, since their state depends primarily on environmental events or event combinations rather than on the component state itself. 4. A separate tree is required for each initiating event, making it difficult to represent

	interactions between event states in the separate trees or to consider the effects of multiple initiating events. 5. The ETA offers no help in determining whether a sequence of successes or failures of branches leads to system failure. 6. Event trees are only practical when the chronology of events is stable. 7. ETA is inflexible in the sense that only non-recoverable subsystem event sequences with non-recoverable initiating events are described. Dynamic behaviour of the system in the presence of failures can not really be taken into account. 8. The model only consists of intended actions. No direct attention is paid to the possible extra actions or incomplete actions, including those taken too early or too late. 9. Timing issues can cause problems in event tree construction. In some cases, failure logic changes depending on when the events take place. 10. It loses its clarity when applied to systems that do not fall into simple failed or working states. [DNV-HSE01] 11. All system events must be anticipated. 12. Thoroughness is based on the presumption that all consequences of events have been explored 13. For some systems (other than maybe nuclear power plants), there can be many initiating events, and an exhaustive set may be difficult to determine. 14. Since ETA starts with all possible events and works forward to determine their outcomes, much of the analysis is concerned with operations that have no safety implications. [Storey96] 15. It is not efficient where many events must occur in combination, as it results in many redundant branches. [DNV-HSE01] 16. Event trees can only address dependence in a limited fashion. 17. Establishing branch probabilities can be very time-consuming. 18. The use of fault trees to determine the probabilities for many of the event tree branches may make it more difficult to identify common causes of failures.

9. External Events Analysis

References used:	Key references: • [Region I LEPC] • [RSC slides] Other references: • [DOE 1023-95] • [NEA98] Additional reading: • [FAA00], [ΣΣ93, ΣΣ97]
Alternate names:	Natural Phenomena Hazards Mitigation, Cross boundary hazard identification
Primary objective:	The purpose of External Events Analysis is to focus attention on those adverse events that are outside of the system, operation or process under study. These are events that might occur outside the boundaries of the process, and/or that may be the result of a malicious or intentional act, which could have a deleterious impact on the process, perhaps resulting in an accidental release of a regulated substance. It also includes internal hazards such as internal floods and fires. It is to further hypothesise the range of events that may have an effect on the system being examined.

Description:	The occurrence of an external event such as an earthquake is evaluated and effects on structures, systems, and components in a facility are analyzed. Hence it is possible to have multiple external event-induced failures of structures, systems and components. It should be noted that current design codes for chemical processing plants have safety factors to allow plant equipment to withstand major external events (such as earthquake, flood, tornado or extreme wind) without a catastrophic failure. Thus, the major emphasis in hazard assessments related to external events should be placed on mitigating the risk of an accidental release by ensuring that there are safe shutdown systems and procedures or by evaluating substitution of an inherently safer technology for the process.
	
	External events usually have the potential to be sources of common cause failure. Moreover, they are generally less straight forward to assess due to
	• Limited data on occurrence rates due to rare nature
	• Potential for complex interactions leading to difficulty of modeling the effects on systems
	• They usually reflect larger degree of subjective input on results
	• They may be seen as outside, or at the edges of the scope or the safety case, and therefore viewed as somebody else's problem.
	
	An External Events Analysis comprises five basic analysis steps [RSC slides]:
	1. Selection of events for analysis, e.g. [Region I LEPC] provides a list of external events. These should first be screened such that a relevant list remains. The screening could involve checking whether:
	  • Event is conceivable for the site of interest (e.g. the site is not located near any volcano or ocean)
	  • Design features preclude the event (e.g. an assured source of cooling water is available near the site in the event of an extended drought)
	  • Preliminary estimate of event frequency is low relative to other events with comparable consequences
	2. Characterisation of event hazards; this involves determining the relationship between the frequency and the severity of the event. The nature of hazard characterisation is different for each type of external event. This step often requires use of specialised expertise.
	3. Assessment of equipment response to event. Objective is to assess the conditional probability of equipment failure as a function of event severity. This step often

	requires use of specialised expertise. 4. Identification of event sequences, integrating information about events into plant models. Objective is to assess how equipment failures relate to system effects. Event trees and fault trees can be constructed to reflect these effects. The sub-steps are: • Include events for unique effects of initiator; • Simplify models by eliminating low-probability 'random' failures where appropriate; • Include special operator actions taken to reduce effects of initiator. This analysis is much more efficient if an internal events analysis is already complete or well underway, since this gives insight into important aspects of plant design and operation, is gives an understanding of available recovery actions, and there is no need to generate entirely new models. 5. Estimation of sequence frequencies, by integrating the results of the previous steps. The treatment of uncertainties is a key element in External Events Analysis [RSC slides]: • Due to the rare nature of events, uncertainties in hazard and fragility analyses are often very large. • Simplifications must usually be made in assessing system and plant responses due to complexity of interactions. • Sensitivity studies can sometimes be more useful than uncertainty analyses in providing insights into the analysis (see Bias and Uncertainty Analysis template). • Any quantitative uncertainty calculations should be supplemented by qualitative discussion • Identification of areas in which subjective judgement was a primary input to the analysis • Areas in which available models and data are believed to be especially weak • Judgement regarding validity of analyses and result for decision making [NEA98] notes that the type of human actions that need to be undertaken as a response to an external event may be event specific. Thus, in the case of an internal fire the plant staff may need to: (a) undertake actions to mitigate the fire itself, and (b) to respond to the internal initiating event caused by the fire. On the other hand, seismic events as such can not be mitigated and only the second type of response (b) applies in this case. Moreover, the operator response to external events may be subject to specific difficulties, related to the characteristic features of such events: 1. External events constitute Common Cause Initiators (CCIs), i.e. the redundant equipment needed for the mitigation of the event might have been disabled by the occurrence of this event. 2. The information normally available to the operators may be distorted due to the impact of external events on instrumentation and signal processing. 3. The staff can be physically affected by the external event (e.g. by smoke). Consequently, appropriate modelling of human behaviour under conditions associated with external events is a complex task. Scarceness of relevant data, in most cases practically non-existent operational experience of situations characteristic for conditions that may appear upon occurrence of an external event, and limitations in simulator training to represent such situations, are additional factors contributing to the large uncertainties in human reliability assessments.
Applicability range:	The technique is applicable to process plants.
Life cycle stage:	An External Events Analysis can be done during design.
Experience in application to air traffic:	External Events Analysis has been done for Nuclear and Chemical industry, but applications to ATM or air traffic situations have not been found by this study.
Related methods:	Link to Data Security, SHA (System Hazard Analysis), Interface Analysis,

	Interdependence Analysis, Change Analysis, Maximum Credible Accident/ Worst Case, ETBA (Energy Trace and Barrier Analysis for Hazard Discovery and Analysis), Scenario Analysis, O&SHA (Operating and Support Hazard Analysis), Systematic Occupational Safety Analysis, ERA (Environmental Risk Analysis), WSA (Work Safety Analysis), Barrier Analysis, CSSM (Continuous Safety Sampling Methodology)
Availability and tool support:	Supporting tools are available.
Maturity:	The technique was developed in 1992 or earlier. The related Natural Phenomena Hazards Mitigation was jointly developed by staff from EH's Natural Phenomena Hazards Safety Program and the Office of Nuclear Energy's Office of Nuclear Safety Policy and Standards.
Acceptability:	The Department of Energy (DOE) has issued an Order (DOE 5480.28) which establishes policy and requirements for Natural Phenomena Hazard (NPH) mitigation for DOE sites and facilities [DOE 1023-95].
Ease of integration:	Techniques like FTA and ETA can be used in the analysis. An External Events Analysis often requires specialised expertise. HAZOP can also be a useful aid, as it allows structured brainstorming, and thinking 'outside of the box', i.e. beyond the usual barriers and pre-conceived failure events.
Documentability:	Documentability is moderate. The use of checklists of possible external events can guide the analysis.
Relevance to ATM:	In other industries systems are often well-bounded – e.g. nuclear power plants of offshore or onshore petrochemical installations are geographically bounded, and there are limited interactions with the environment. ATM is fundamentally different. Each ATM system is linked with many others, and the system is in effect a global one. This presents a problem when developing a new tool, for example. Where should the assessment stop? What could it interact with, even if no such interaction was intended? What aspects of the airborne system should be included in the assessment scope? Should the assessment scope include other future concepts under development? Questions such as these are not idle ones, as often accidents can be the result of unintended and unanticipated interactions between systems at their boundaries, i.e. where no interaction is expected, or where the assessment assumes such considerations are outside its scope or remit. There is therefore a danger of a 'compartmentalised' safety approach in ATM, which may miss critical interactions with other elements of the ATM environment. What can be seen at the time as 'someone else's problem', can then be addressed by no-one, until an accident occurs and it becomes everyone's problem. There is therefore a need to consider safety issues at the 'edge' or boundary of the assessment scope. This would effectively be a check on the assessment scope, and perhaps the need to either draw more into the scope, or to co-ordinate with other design and development projects undergoing assessment to ensure that potential boundary interactions are being addressed. HAZOP is one of the approaches that can be used for this type of issue, due to its structured creative approach. This is therefore an area for development of a practicable method that can fit with current and developing safety assessment methodologies. Although some external events the technique was designed to analyse, such as earthquakes and floods, are probably more relevant for ATC systems and ATC control rooms than for ATM as a whole, the basic steps of the technique could be applicable to external events influencing ATM, such as weather, satellite systems, aircraft operators, fire, aircraft emergency descents, etc. Hazard brainstorming sessions with experts could prove useful for this.
Con's and resources:	Analysis of external events often requires specialized expertise.

10. Future Aviation Safety Team (FAST)

Future Aviation Safety Team (FAST) Method	
References used:	EUROCONTROL Safety Regulation Commission, ESARR 3 Use of Safety Management Systems by ATM Service Providers. http://www.eurocontrol.int/src/public/standard_page/esarr3.html EUROCONTROL Safety Regulation Commission, ESARR 4 Risk Assessment and Mitigation in ATM. http://www.eurocontrol.int/src/public/standard_page/esarr4.html FAA System Safety Handbook, Chapter 9: Analysis Techniques, http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook FAST Handbook. *Website address to be inserted here as soon as available* JAA Safety Strategy Initiative and EASA Strategic Safety initiative. http://www.jaa.nl/jssi/profile.html
Alternate names:	Areas of Change Analysis Method for Identification of Future Hazards
Primary objective:	A "Prognostic" or "Predictive" approach that is aimed at discovering future hazards arising as a consequence of future changes introduced inside or outside the global aviation system.
Description:	Evaluate proposed changes to the aviation system, identify hazards that may be created by such changes and by interaction effects, and subsequently develop and implement mitigating actions. Definitions: FAST **Customers** are those individuals or organizations that have the authority to either recommend or implement changes to the global aviation system, or are curious regarding changes and the possible introduction of hazards. The FAST Customer can be a person, an organization, or a consortium of organizations such as companies, regulatory agencies, or interest groups. FAST **Stakeholders** are those individuals or organizations that may be impacted by an envisioned change to the global aviation system, but that do not have primary responsibility for the implementation of that envisioned change.
Process steps:	***Step 1:*** *Responsible Party Proposes Implementation of Change(s) to the Global Aviation System* *For the Customer* Customer accepts responsibility for the consequences of implementation of global aviation system changes they are proposing . They recognize the need for systematic prediction of hazards associated with changes and to design those hazards out of the system or avoid or mitigate the hazard. Consider who the Stakeholders might be, then contact them. Contact FAST for assistance. **Step 2:** Clearly Define Scope of Expert Team Hazard Identification Study *For FAST and the Customers and Stakeholders* Clearly define the scope of the Expert Team study. The Customer should document their: • approximate future of interest; hereinafter referred to as the Future • desired deliverables, including desired report structure • schedule • resources **Step 3:** Assemble an Expert Team *For FAST, assisted by Customers as necessary* Assemble an Expert Team: • 8 to 10 individuals at most • Individuals representing diverse perspectives • Combination of visionary and operational experience • Include at least one individual from each Customer and each Stakeholder organization

	• Combination of engineering, operational, and human factors experience **Step 4:** Understand Customer Requirements and Future of Interest *For the Customer and FAST Core Team* The Customer should thoroughly brief the Expert Team and FAST to communicate the identified Future – the full scope of what they plan to introduce in the future. Refine and describe in detail the intended vision of Future. See Annex II of the FAST Methodology Handbook for guidelines for drafting a future scenario and an example "vision of the Future." The following items should be agreed upon at this stage: • Desired deliverables for the hazard analysis, including suggested report structure • Schedule • Resources **Step 5:** Identify Hazards Intrinsic to Future (optional) *For the Expert Team* Identify the Hazards intrinsic to the Future. Based on the judgment of the Expert Team and the Future, select an appropriate hazard identification method (See Annex IV for hazard identification techniques). Identify "what could possibly go wrong?" when implementing a future technology system, a novel operational concept or new business model. Hazards identified must be associated with a clear and specific vision of the Future to be credible and be set in proper context. General and specific hazards may be related to: • Systems integration gaps and overlaps • Concept development, design, and production • Human-human, human-systems, and organizational interactions • Procedures and training • Intersecting futures • Operations including maintenance • Decommissioning **Step 6:** Identify Areas of Change (AoC) Pertinent to Future *For the Expert Team* The Expert Team (which has Customer representatives) should review the full Areas of Change list and make an initial assessment of which AoC's are most likely to be relevant to the generation of hazards within their Future. This is a critically important step because the change phenomena that are either ongoing or that lie ahead may be important catalysts for future hazards. The FAST should be available for consultation with the Expert Team at this stage in the event clarification of specific AoC's is required. **Step 7:** Enrich Hazards by Evaluation of Interactions with AoC's *For the Expert Team* Identify hazards generated by interactions between and among Areas of Change that could adversely impact the safety characteristics of the Future. The Expert Team should also attempt to identify and synthesize unusual patterns of AoC interactions that might not have detected if the hazard analysis had not been broadened by examination of the AoC's. A fundamental premise of the FAST method is that interactions and overlaps/gaps among the vision of the Future and the FAST AoC's are the most likely catalysts for revealing and understanding future hazards. Enrich the hazards identified during Step 5 (or during a Customer PHA) by postulating key interactions between: • The AoC's and the Future • The AoC's and the identified hazards associated with that Future Interactions are those reciprocal actions or influences between the future and the Areas of Change in which the future of interest is immersed that may generate hazards not otherwise identified by narrow safety analysis methods. The objective of this step is to use domain expertise to identify phenomena that would amplify or diminish the interaction effects. Communicate with FAST and the Customer as necessary to accomplish this step. **Step 8:** Identify Hazard Mitigations & AoC Effects on Mitigations (optional) *For the Expert Team* Identify potential mitigations for identified hazards and how efficacy of those mitigations

	might be modified when interacting with future AoC's. The mitigations may be those developed previously by a Customer or those proposed by the Expert Team in response to the identified hazards.A key aspect of this step is evaluating potential effect of the FAST Areas of Change on the efficacy of proposed mitigations. Note: Step 8 is optional and is to be performed at the discretion of the Customer. Mitigations for existing or potential future hazards are generally the responsibility of the customer or regulatory entity. Expert Team analysis of the effects of AoC's on mitigations for future hazards should be conducted only if the customer sees substantial value in this activity. Such might be the case if the Customer has not yet performed a preliminary hazard assessment. In this case, the Expert Team may be requested to undertake this work and provide possible mitigation recommendations that reflect interaction effects with the AoC's. If the Customer does not desire recommendations for mitigations, simply skip Step 8 and move directly to Step 9 of the methodology. **Step 9:** Formulate Recommendations & Identify Watch Items *For the Expert Team* As requested by the Customer, formulate general recommendations. Consider hazard elimination, avoidance, and mitigation strategies. If the Expert Team discovers hazards that currently exist, but are not widely recognized, forward that information to FAST for transmission to the Customer and others as appropriate. Recommendations should identify Stakeholders that may be affected by the hazard and actions that may be needed by the Stakeholder community. If hazard prioritization is seen as beneficial, see Annex V for suggestions for ranking the future hazards. **Step 10:** Inform FAST and Customers Regarding Results *For the Expert Team* Inform FAST regarding results: • Report the following to FAST: • Future of interest and associated AoC's • Future hazards and newly-discovered present hazards • Watch Items • Recommendations Inform the Customer regarding results: • Future of interest and associated AoCs • Future hazards and newly-discovered present hazards • Watch Items • Recommendations for enhancements or modifications to the change(s) being proposed by the Customer Report the following to FAST: • Observations and suggestions regarding the FAST method
Applicability range:	The primary application of this methodology is to identify potential hazards resulting from implementation of prototype systems, new operational concepts, new decision support tools, new aiding systems, display configurations, covering the full range of human-system integration, procedures and organizational factors.
Life cycle stage:	Life cycle stage applicability: primarily design. Prior to a hazard being introduced to the global aviation system, the FAST hazard discovery process attempts to identify those hazards. FAST prognostic hazard discovery processes inform design processes so that the hazards can be eliminated from the future. Outputs of a FAST analysis are intended to prevent potential future hazards from even materializing or at a minimum recommend strategies to prepare the mitigations for the identified hazards.
Experience in application to air traffic:	The FAST Method has been used to perform a Preliminary Hazard Analysis of the EUROCONTROL Concept of Operations for European ATM in 2011. It has also been used to understand future hazards associated with increasing flight crew reliance on cockpit automation, a topic related to future ATM systems development.
Related methods:	PHA, Brainstorming, Zonal Analysis, Event Tree Analysis, Action Error Analysis (AEA),
Availability and tool support:	The technique is available for use by the broad aviation community. The FAST Methodology Handbook and Areas of Change repository can be obtained from the co-chair

	of the FAST, Rudi den Hertog at rudi.denhertog@stork.com or via the FAST web site that will go live at the European Commission Joint Research Center in January of 2007. http://fast.jrc.it/
Maturity:	Assessment of applicability of the FAST Method to ATM from ECTL ConOps 2011 hazard assessment: • Objectives of FAST analysis largely met - benefits of safety assessment of operational concepts demonstrated • Involvement of all ATM actors is essential: allowing for synergies and shared knowledge of the system components and their interactions • Use of operational ATM scenarios considered essential: helps experts understand the concept and improves process efficiency • FAST method can be used for safety analysis of future ATM concepts, although further improvement and fine tuning are still needed • FAST method can be used as part of Risk Assessment (e.g., ESARR 4 Risk Assessment and Mitigation in ATM) and Risk Management (e.g., ESARR 3 Use of Safety Management Systems by ATM Service Providers)
Acceptability:	The FAST Method is being recommended for use as preliminary hazard analysis method within the Single European Sky ATM Research program (SESAR).
Ease of integration:	The FAST Method is relatively easy to understand and use but the validity and applicability of the outputs depend to a large extent on the proper breadth and depth of safety experience of the Expert Team that will perform a given analysis.
Documentability:	Documentability: moderate (the technique provides sufficient documentation to be largely repeatable) Consistency: moderate. Because the domain experts on the analysis team have no operational experience with the future, the FAST method, if used on two occasions by independent experts, may yield some variation in the results.
Advantages:	The FAST Method enables: Anticipation of major safety issues right from the concept definition phase Validation of new concepts from safety perspective Generation of recommendations for further analysis and research on specific concept elements and implementation solutions decision making in the planning and development phases
Disadvantages:	Limitations: Non-linear increase of hazard prediction uncertainties with time High level of abstraction required among the Expert Team

11. FMECA (Failure Modes Effects and Criticality Analysis)

References used:	Key references: • [Leveson95] • [Pentti&Atte02] Other references: • [Bishop90] • [DNV-HSE01] • [ECSS-HSIA96] • [Hoegen97] • [Kumamoto&Henley96] • [Matra-HSIA99] • [Page&al92] • [Parker&al91], • [Rademakers&al92] • [Richardson92] • [SAE2001] • [Storey96] • [Villemeur91-1] Additional reading: [Andow89], [CAA-RMC93-1], [CAA-RMC93-2], [DEFSTAN00-56], [FAA00], [Garrick88], [Henley&Kumamoto92], [MAS611-2], [Moek84], [MUFTIS3.2-I], [Roberts&al81], [ΣΣ93, ΣΣ97], [Toola93].
Alternate names:	In [Richardson92] FMEA is called SFMEA, with the S of System.
Primary objective:	FMEA (Failure Modes and Effects Analysis) and FMECA (Failure Modes, Effects and Criticality Analysis) are traditionally considered inductive (i.e. bottom-up) techniques that [SAE2001]: • Identify and evaluate potential failure modes of a product design and their effects • Determine actions or controls which eliminate or reduce the risk of the potential failure • Document the process. FMEAs are widely used in the automotive industry, where they have served as a general purpose tool for enhancing reliability, trouble-shooting product and process issues, and as a standalone tool for hazard analysis.
Description:	The primary difference between FMEA and FMECA is that the latter explicitly includes criticality analysis for both the original design and the final design The results of the FMEA or FMECA are documented in a table with column headings such as item, potential failure mode, potential effects of the failure, severity of the failure, potential causes of the failure, the likelihood that a potential cause will occur (in qualitative or quantitative terms), current design controls, risk priority number, and recommended actions. Checklists can be used to support the analysis. When system definitions and functional descriptions are not available to the specified component level, the initial analyses are performed to the lowest component level to provide optimum results. When system definitions and functional definitions are complete, the analysis is extended to the specified component level. In [Page&al92], [Richardson92], [Kumamoto&Henley96], [Villemeur91-1] examples of FMEA tables are presented. In a FMECA, for each failure mode the probability of occurrence and the criticality of consequences is assessed (so a rough quantitative analysis is possible). There often are four criticality rankings: safe (or negligible), marginal, critical and catastrophic. In [Rademakers&al92] an example of a FMECA table is presented.

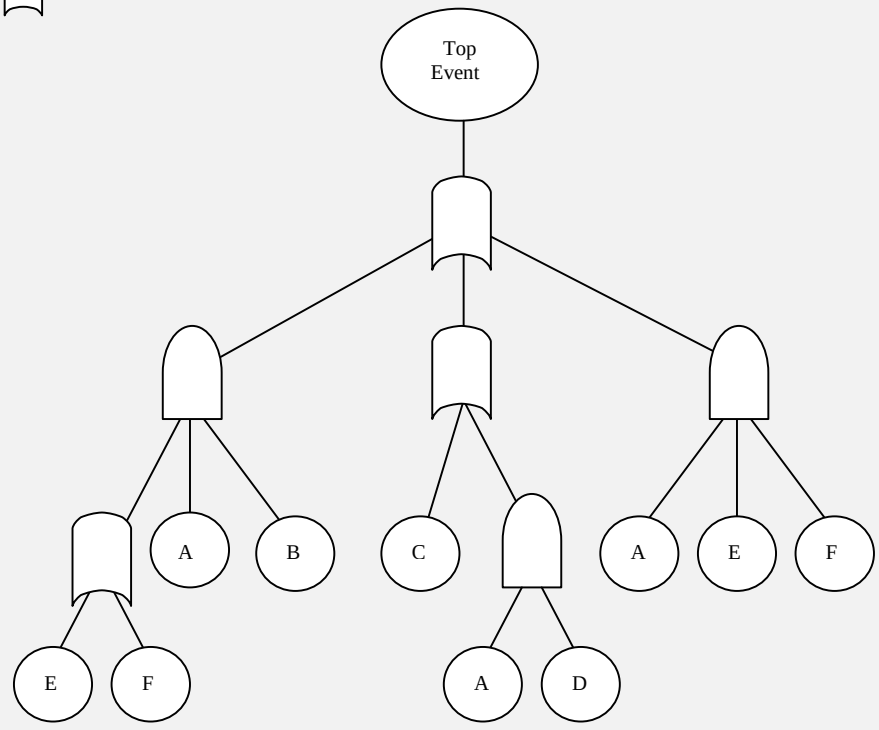
	[Bishop90] quotes ARP 926 when saying that the FMECA criticality number for each component is indicated by the number of failures of a specific type expected during each million operations occurring in a critical mode. The criticality number is a function of nine parameters, most of these have to be measured. In [Kumamoto&Henley96], the ARP 926 criticality number is given explicitly. A very simple method for criticality determination is to multiply the probability of component failure by the damage that could be generated; this method is similar to simple factor assessment. According to [Matra-HSIA99], the FMECA shall contain software failure modes, effects, and criticalities and shall use for their establishment the HSIA (Hardware/Software Interaction Analysis). HSIA, see e.g. [Parker&al91], is obligatory on ESA (European Space Agency) programs and is performed for all functions interfacing the spacecraft and / or other units. The objective of the HSIA (according to [Hoegen97]) is to systematically examine the hardware/software interface of a design to ensure that hardware failure modes are being taken into account in the software requirements. Further, it is to ensure that the hardware characteristics of the design will not cause the software to over-stress the hardware, or adversely change failure severity when hardware failures occur. The analysis findings are resolved by changing the hardware and/or software requirements, or by seeking ESA approval for the retention of the existing design. It can be performed for flight hardware which will be controlled via on-board software. The HSIA shall identify: • The effect of each hardware failure mode on the software operation: • all disruptions to software functions for each failure mode • fault which originate in hardware and are propagated by the software whether or not the fault affects the software operation • method of detection of faults by software • methods of correction/containment of faults by software • The effects of software on hardware elements including: • potential damage resulting to hardware from incorrect methods of prevention of these harmful effects • prior fault detection methods applied to the software functions. • methods of controlling/containing the harmful effects of faults • recovery/rollback method applied According to [ECSS-HSIA96], HSIA shall be performed to ensure that the software is designed to react in an acceptable way to hardware failure. This shall be performed at the level of the Software Requirements Document.
Steps:	In [SAE2001], a FMEA or FMECA consists of the following basic steps: 1. Identify and list individual components, the function they provide, and their failure modes. Consider all possible operating modes. 2. For each failure mode, determine the effects of the failure on all other system components and on the overall system. 3. Determine the severity of the failure, the potential causes of the failure, and the likelihood that a potential cause will occur. 4. Identify the current design controls that will assure the design adequacy for the failure controls. Determine the ability of the proposed design controls to detect a potential cause, or the ability of the proposed controls to detect the subsequent failure mode before the component is released for production. 5. Determine the Risk Prioritisation Number (RPN) based on the severity, occurrence, and detection rankings. 6. For the highest ranking RPN's, recommend actions to take that will reduce the severity, occurrence, and/or detection rankings. Re-evaluate the RPN based on the new estimates of the severity, occurrence, and detection

	rankings.
Applicability range:	FMECA is most appropriate for standard parts with few and well-known failure modes, since all failure modes must be known in advance. Although the FMECA is an essential reliability task, it also provides information for other purposes. The use of FMECA is called for in maintainability, safety analysis, survivability and vulnerability, logistics support analysis, maintenance plan analysis, and failure detection and isolation subsystem design. These all concern hardware systems. FMECA is not suitable for human reliability analysis. The references disagree on its suitability for software analysis (however, see the SFMEA template for FMEA-based software assessments).
Life cycle stage:	The references give various statements on life cycle stage applicability. According to [Bishop90], a FMEA is carried out after design. In [Leveson95], FMEAs are considered appropriate when a design has progressed to the point where hardware items may be easily identified on engineering drawings and functional diagrams. According to [Storey96], FMEA may be applied at various stages of a development project. It is often used at a functional level early in the lifecycle, when it can be useful in the determination of the required safety integrity level. It can also be applied at a fairly late stage, after much of the design work has been done. Here it may be applied at either a component or a functional level. [Pentti&Atte02] state that FMEA can be used in all phases of the system lifecycle, from requirements specification to operation and maintenance, although most benefit from use of FMEA can be achieved at the early phases of design, where it can reveal weak points in the system structure.
Experience in application to air traffic:	FMEA has been widely adopted and has become standard practice in Japanese, American, and European manufacturing companies. It is also being used in the areas of electronics, automobiles, consumer products, electrical generating power plants, building and road construction, telecommunications, electromechanical industries, semi-conductor and medical device industries, computer hardware and software industries. The three big US car manufacturers request that their suppliers use FMEA. FMEA applications in the aerospace and nuclear industries have seen an exponential increase in product software content and complexity. Since FMECA is focused on hardware problems, and does not incorporate human reliability, it is less relevant for ATM applications, especially in comparison with HAZOP.
Related methods:	Link to FMEA (Failure Mode and Effects Analysis) or SFMEA (Systems Failure Mode and Effect Analysis), GFCM (Gathered Fault Combination Method), FMES (Failure Modes and Effects Summary), HMEA (Hazard Mode Effects Analysis), Criticality Analysis, HSIA (Hardware/Software Interaction Analysis). A very rigorous generalization of FMEA is the Truth Table Method, see [Villemeur91-1]. Another extension and generalization is Gathered Fault Combination Method (GFCM), see [Villemeur91-1].
Availability and tool support:	The technique is widely available. Supporting tools exist; see the Global Aviation Information Network (GAIN) Working Group B (Analytical Methods and Tools).
Maturity:	FMECA was developed in 1967 by Society of Automotive Engineers (SAE); Aerospace Recommended Practice (ARP) 926. It is widely used since and well-understood. FMEA even dates from 1949 and was originally developed in the US Military. Outside the military, the formal application of FMEA was first adopted to the aerospace industry, where FMEA was already used during the Apollo missions in the 1960s [Pentti&Atte02].
Acceptability:	Recommended in all system reliability analyses, in particular for safety critical hardware systems where reliability data of the components is available. The final document of a FMEA analysis is often used in a formal way to certificate the system, if no other dependability study is available. Aerospace and defence companies usually referred to MIL-STD-1629A as a standard for FMEA or FMECA (dated 1980), but this standard was cancelled by the action of the standard authority on 4 August 1998. Users are now referred to other standards and documents [Pentti&Atte02]
Ease of	The output of FMECA can be used for FTA. The level of mastery needed to perform the

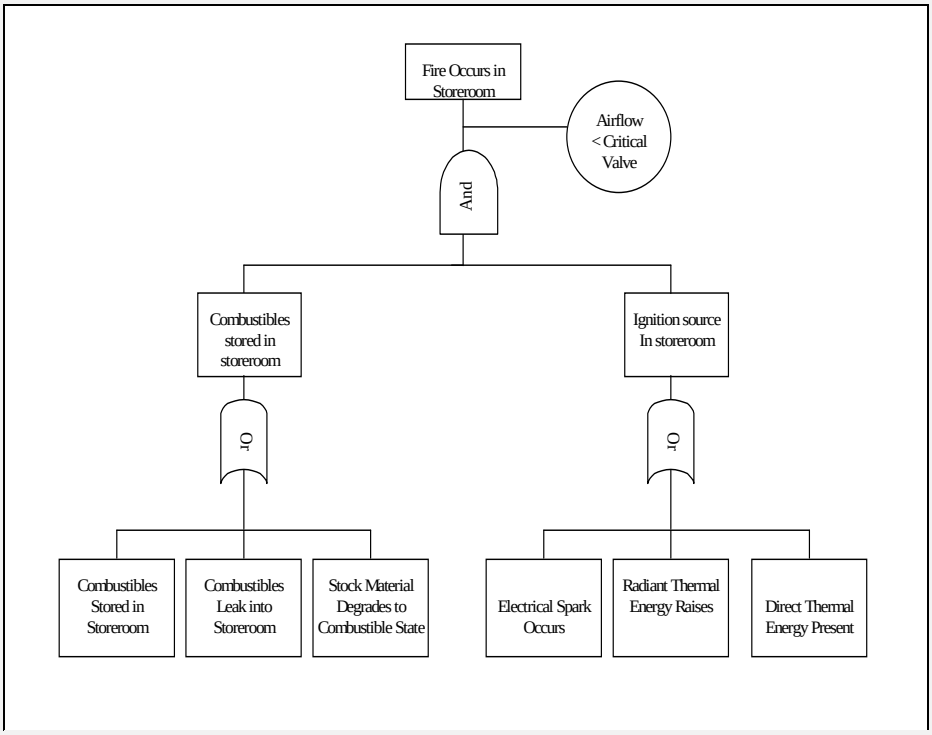
integration:	FMECA is not that extensive. An entry level engineer under the supervision and tutelage of a system safety engineer who is familiar with the process is normally sufficient to produce an acceptable product. Since the FMECA process is usually a qualitative one, the level of difficulty is not as challenging as one that is quantitative.
Documentability:	The method is supported by standardised forms to complete, hence documentability is high.
Advantages:	General advantages are: 1. Information on single failure modes and their effects are well structured. 2. The results constitute an essential input to FTA and similar numerical methods [Bishop90] 3. The method is systematic and comprehensive [Bishop90] 4. The method is supported by standardised forms to complete [Bishop90] 5. The method permits an analysis of the capability for detecting component failures [Bishop90] 6. It is widely-used and well-understood [DNV-HSE01] 7. It can be performed by a single analyst [DNV-HSE01] 8. It identifies safety-critical equipment where a single failure would be critical for the system [DNV-HSE01]
Disadvantages:	For larger systems, the FMECA process can be very extensive and time consuming and the use of some form of computer assistance is nearly always mandatory. Other general weaknesses are: 1. It does not study multiple, simultaneous failures without tremendous increase of required labor for studying all the different failure combinations. 2. It does not study the effects of human mistakes on the functioning of the system. 3. It is optimized for mechanical and electrical equipment, and does not apply to procedures or process equipment. 4. The technique does not provide any systematic approach for identifying failure modes or for determining their effects and no real means for discriminating between alternate courses of improvement or mitigation. 5. The table can get more extensive than necessary because not all component failure modes affect safety on system level. 6. Since the number of entries in a FMEA table tends to be very extensive, the descriptions of these entries tend to be very brief, which may lead to ambiguities, difficulties in understanding, and difficulties in maintenance. 7. Although some FMEA effects arise repeatedly, FMEA does not group together the items causing the effects. 8. FMEA often suffers from duplication of effort and large amounts of redundant documentation. 9. The information overload from repetitive, redundant, and scattered data obscures the relationships among the rows and columns of the FMEA, adding to confusion. 10. FMEA is not very suitable for complex systems, it must be combined with additional techniques. 11. The technique is static, there are no temporal aspects. 12. A comprehensive FMEA may be very time consuming and expensive [Bishop90] 13. It is carried out after design, and so is too late to influence design changes [Bishop90] 14. It assumes extreme failures [Bishop90] 15. It is not good at identifying failures caused by items that are not part of the system under study. 16. Its benefit depends on the experience of the analyst. [DNV-HSE01] 17. It requires a hierarchical system drawing as the basis for the analysis, which the analyst usually has to develop before the analysis can start. [DNV-HSE01] 18. It does not produce a simple list of failure cases. [DNV-HSE01] 19. It only looks at hazards associated with failures, not those associated with normal operations.

	20. It does not identify all hazards associated with a system, even if it identifies all single-point failures. A failure does not have to occur for a hazard to be present in the system. 21. It only looks at the hardware failures, not the interaction between personnel, equipment or environment. Overall, FMECA is useful for safety-critical mechanical and electrical equipment, but should not be the only hazard identification method. Most accidents have a significant human contribution, and FMECA is not well suited to identifying these. As FMECA can be conducted at various levels, it is important to decide before commencing what level will be adopted as otherwise some areas may be examined in great detail while others are examined at the system level without examining the components. If conducted at too deep a level, FMECA can be time consuming and tedious, but it leads to great understanding of the system. [DNV-HSE01]

12. FTA (Fault Tree Analysis)

References used:	Key references: • [FT handbook02] • [Henley&Kumamoto92] Other references: • [DNV-HSE01] • [Howat02] • [Kumamoto&Henley96] • [Leveson95] • [Smith9697] • [Villemeur91-1] Additional reading: • [Apthorpe01], [Bishop90], [Holloway89], [MAS611-2], [MUFTIS3.2-I], [ΣΣ93]
Alternate names:	Former name is Cause Tree Method [Villemeur91-1].
Primary objective:	To aid in the analysis of events, or combination of events, that will lead to a hazard or serious consequence
Description:	Starting at an event which would be the immediate cause of a hazard or serious consequence (the 'top event'), the analysis is carried out along a tree path. Combinations of causes are described with logical operators (And, Or, etc). Intermediate causes are analysed in the same way, and so on back to basic events where analysis stops. The method is graphical, and a set of standardised symbols are used to draw the fault tree. An example is given in the figure below. Here,  denotes an 'And' gate;  denotes an 'Or' gate.  Besides 'And' and 'Or' gates, other symbols have been introduced for gates to represent 'exclusive or', 'priority and', 'external event', 'conditioning event', 'undeveloped event',

	'inhibit gate', etc. Also for the events, there are different symbols available, such as 'basic event', 'undeveloped event', 'event represented by a gate', 'conditional event used within inhibit gate', 'house event; either occurring or not occurring', 'transfer symbol'. See e.g. [Kumamoto&Henley96] for many examples. In practice, predominantly And and Or gates are used. A common approach to analyze a fault tree is to determine its minimal cut sets, i.e. minimal sets of primary failures, such that if all these simultaneously exist, the top event exists. For the example fault tree above, the minimal cut sets are: {C}, {A,D}, {A,B,F}, {A,B,E}, {A,E,F}. The top event occurs if one of the minimal cut sets occurs, and with this the fault tree can be reduced to one with a simpler structure: a top event, with an 'Or' gate, and below it as many 'And' gates as there are minimal cut sets. Each 'And' gate connects the elements in its corresponding minimal cut set. Tools exist that support the identification of these minimal cut sets. One-event cut sets are significant contributors to the top event, unless their probability of occurrence is very small. Two-or-more-event cut sets can often be neglected if one-event sets are present, because co-occurrence of rare events have low probabilities. However, when a common cause is involved, it may cause multiple basic event failures, so some two-or-more-event cut sets behave like one-event cut sets. A path set is a dual concept to the cut set. A minimal path set is a minimal collection of basic events, and if none of the events in the set occur, the top event is guaranteed to not occur. Quantification of the fault tree is usually done through as minimal cut sets. The probability of occurrence of a minimal cut set is taken equal to the product of the probabilities of occurrence of its basic events, provided there are no dependent events in a minimal cut set. The probability of the top event is equal to the sum of the probabilities of the minimal cut sets, provided there are no dependencies between minimal cut sets. If probabilities of basic events are given by density functions, then the probability of the top event should also be given by a density function. Monte Carlo simulation can be used to determine these functions. FTA is generally regarded as a top-down method; however it can also be used in combination with bottom-up: The top-down phase is to support the system definition and first part of the design phase when trying to understand how sub-functions contribute to functions. Next, a bottom-up phase is to collect data on system elements and to support the verification of the ability of the architecture to meet safety objectives.
Steps	A Fault Tree Analysis follows the following steps: [Leveson95] 1. System definition; often the most difficult part of the FTA. It requires determining the top event, initial conditions, existing events, and impermissible events. 2. Fault Tree construction for each identified top event. 3. Qualitative analysis, which comes down to determining the minimal cut sets. 4. (Optional) quantitative analysis, which uses the minimal cut sets to calculate the probability of occurrence of the top event from the probability of occurrence of the basic events. The quantitative part is not very useful if only limited quantitative data are known. It is more useful to identify more sources of hazard than to quantify with greater precision those already found.

Example:	**EXAMPLE:** Below is a brief example of a Fault Tree that illustrates how an event may be traced to specific causes that can be very precisely identified at the lowest levels.. 
Applicability range:	Fault Tree Analysis is mainly intended for the analysis of hardware systems, but there have also been attempts to apply this approach to software failure analysis and human error. Conditions are that the undesirable system events that are to be analyzed, and their contributors, must be foreseen, and each of the undesirable system events must be analyzed individually. Because of its relative complexity and detail, it is normally not cost effective to use the FTA against risks assessed below the level of high. The method is used extensively in the acquisition of new systems
Life cycle stage:	FTA can best be used from the design stages on, since it requires a completed system design and a thorough understanding of the system and its behaviour in all operating modes to be most effective. FTA could also assist during the definition phase, however building fault trees during definition is usually not very cost efficient, since they will only provide information that is well known and already part of the project standards and design criteria. However, it can be used during definition phase by using FTA as a top-down method to understand how functions interact/overlap or recover one another.
Experience in application to air traffic:	The technique has been frequently used for the assessment of safe aircraft equipment, and is regarded as one of the main techniques for this purpose. FTA has also been applied to ATC computer systems, in combination with Event Tree Analysis. In combination with collision risk modeling techniques, simple fault trees have also been used in some ATM applications, e.g. to assess the probability that an aircraft deviates from its planned route in cruise phase [Smith9697].

Related methods:	Dependence Diagrams are similar to Fault Trees. FTA is also related to Cause Consequence Diagrams, Cause Consequence Analysis, GO charts, Master Logic Diagrams, Reliability Block Diagrams, and is often used in combination with Event Tree Analysis, e.g. in Bow-Tie. A variant designed for software safety is called Software Fault Tree Analysis. Techniques to help quantify the top event of a Fault Tree are Kinetic Tree Theory and Phased Mission Analysis. Link to Functional Flow Diagram, Fault Schedule and Bounding Faults, PRA (Probabilistic Risk Assessment based on FTA/ETA) or PSA (Probabilistic Safety Assessment), GO charts, Reliability Block Diagrams, Software Fault Tree Analysis
Availability and tool support:	The technique is widely available. A medium-sized fault tree can have millions of minimal cut sets, so computer programs have been developed to determine them. Numerous supporting tools exist; see the Global Aviation Information Network (GAIN) Working Group B (Analytical Methods and Tools).
Maturity:	FTA has been developed in 1961, by H.A. Watson of Bell Telephone Laboratories as a plan to evaluate the safety of the Minuteman Launch Control System. Later, the Boeing company modified the concept for computer utilization. In 1965, D.F. Haasl further developed the technique of fault tree construction and its application to a wide variety of industrial safety and reliability problems. A guide was published in 1981. Since then, the technique has been used in many domains and is often regarded as a standard technique.
Acceptability:	FTA has been used and recommended by JAR, FAA, SAE.
Ease of integration:	For systems of low complexity, a qualitative Fault Tree is relatively easy to construct and understand. If there are many dependent events then quantification is more difficult and sometimes impossible. FTA is easily combined with other techniques such as Event Tree Analysis (e.g. in a Bow-Tie), Failure Modes and Effects Analysis, Cause Consequence Analysis.
Documentability:	In principle Moderate, but in practice, the assumptions made during the Fault Tree construction process are not commonly documented. The choice of events (primary or otherwise) is often subjective, so fault trees by different teams vary.
Advantages:	The technique is very useful for technical system failure analysis and reliability analysis, including human error analysis; when human behaviour and dynamic aspects are involved, other techniques should be used. Other general advantages are: 1. A fault tree (if not too large) is generally easy to read and understand, reviewed by experts, and used by designers. 2. FTA can handle multiple failures or combinations of failures. 3. It can expose the needs for control or protective actions to diminish the risk. 4. It quickly exposes critical paths. 5. The technique is well accepted and lends itself for quantification. 6. Other faults than hardware failures can be included very easily. 7. The results can provide either qualitative or quantitative data for the risk assessment process.

Disadvantages:	A lot of effort is required to produce the fault trees in a full FTA since all the relevant undesirable events must be identified and all contributing factors must be adequately identified and explored in sufficient depth. Also, there is the potential for failure paths to be missed. Other weaknesses of the technique are: 1. FTA is deductive in its approach to hazard evaluation. The analyst must see the whole picture [Howat02] 2. A fault tree may get very large and complex. Many standardized computer packages exist to support this complexity. 3. Significant training and experience is necessary to use this technique properly. Once the technique has been mastered, application stays time-consuming. 4. For safety-critical operations the quality and use of an FTA depends to a large extent on the ingenuity of the expert who makes the fault tree. This is rather an art than a science. As such, one should be aware that for a safety critical operation, the analysis part of FTA starts as soon as the fault tree is given. 5. Common cause failures that occur by fault propagation (domino effects) cannot be handled. [Leveson95] 6. Dynamic aspects, temporal aspects and time are not addressed particularly well. A fault tree with only And and Or gates is merely a snapshot of the state of a system at one point in time. A fault tree with e.g. Delay and Inhibit gates reduce part of this problem, but are rather difficult to understand and have to be reviewed by experts. 7. Static systems are also difficult to handle, since their state depends primarily on environmental events or event combinations rather than on the component state itself. 8. Process variables and human behavior (except for human error) are not addressed particularly well. 9. FTA can account for some dependencies only, by using additional approximate techniques. Dependent events can only be handled in a rather heuristic way and there is no sequential dependency (i.e. no chronological order of failures occurrence). 10. Problems occur in the analysis of systems in which the same equipment is used at different times and in different configurations for different tasks. [Leveson95] 11. The method concentrates its attention to specific top events, and is therefore not well suited to reveal other serious consequences. 12. While the tree on its own can be useful for defining safeguards, on more complex trees this can be difficult to visualise or it may conceal common cause failures [DNV-HSE01] 13. The method's capability for producing numerical results is often abused: much effort can be spent in producing refined numerical statements of probability, based on contributory factors whose individual probabilities are poorly known and to which broad confidence limits should be attached. Common cause failures cause problems and can lead to orders-of-magnitude errors in the calculated failure probability. Also, often frequencies are multiplied instead of probabilities, with meaningless results. 14. The most useful fault trees require detailed knowledge of design, construction and operation of the system, hence can only be constructed after the product has been designed. [Leveson95] 15. Fault tree analysis shows cause and effect relationships but little more. Additional analysis and information is usually required for an effective safety program [Leveson95]

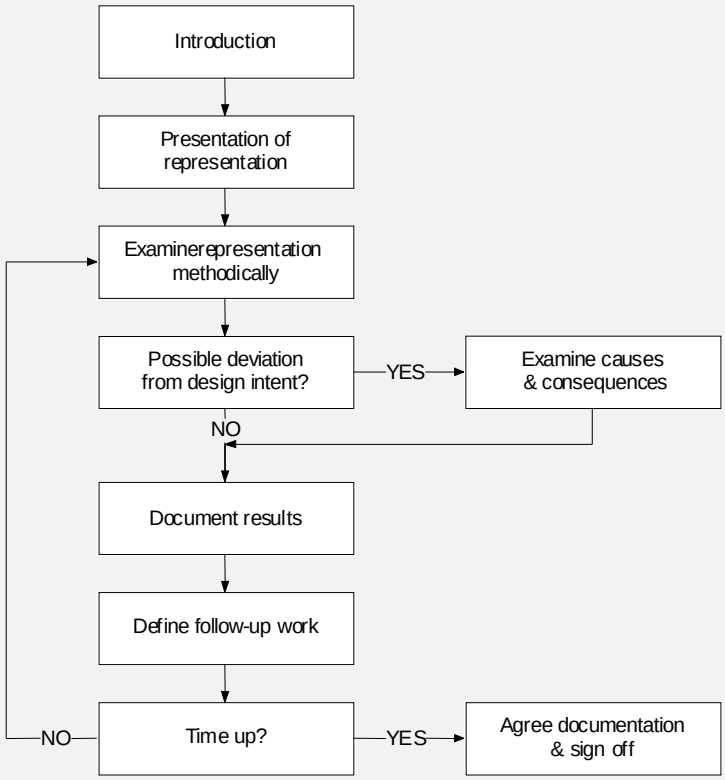
13. Future Flight Central (FFC)

Future Flight Central	
References used:	• FutureFlight Central Customer Guide (July 6, 2004) • FutureFlight Central Website: www.ffc.arc.nasa.gov
Alternate names:	
Primary objective:	Use human-in-the-loop simulation to study improvements to airport safety and capacity.
Description:	Full-scale high fidelity Air Traffic Control Tower simulator. The simulator features a 360 degree out-of-the-window visual scene, 12 tower cab stations, radar displays, controller-pilot communications, hub traffic levels, large aircraft and ground vehicle model library, and extensive data collection.
Process steps:	1. Contact FFC manager 2. Submit Simulation Requirements form 3. Prepare project agreement 4. Develop and validate simulation 5. Run simulation 6. Deliver data and/or report
Applicability range:	• Validate airport design plans using human factors • Evaluate new technologies for tower air traffic controllers • Evaluate and optimize ATC procedures • Train Air Traffic Controllers on new, routine, and/or emergency procedures • Provide remote science environment for mission planning/operations (e.g. Mars)
Life cycle stage:	Operations and maintenance.
Experience in application to air traffic:	• Runway Incursion Studies (LAX) • Surface Management System (DFW) technology assessment • Perimeter Taxiways Simulation (DFW) • Center Taxiway Study (LAX) • Tower Siting for runway reconfiguration (SFO) • Ramp Tower Controller Training (SFO) • Shuttle Landing Facility Virtual Training (Kennedy Space Center) • Extreme Short Take-Off and Landing (ESTOL) Aircraft: conceptualization of airport operations
Related methods:	Interoperability through High Level Architecture (HLA) protocol with: 1. Ames Flight Simulators (B747-400, Advanced Cab, and Vertical Motion Simulator) 2. Ames Airspace Operations Lab (TRACON and Center) 3. External software tools and displays (SMS, ASR-9/D-BRITE emulation) 4. External simulators (future) (See SAFSIM)
Availability and tool support:	Available airport databases: SFO, LAX, DFW, SLF, ORD. Future: SDF, SJC Available tools: Airport Surface Data Collection, High Level Architecture (HLA), Noise Modeling (INM)
Maturity:	The facility has been operational for five years.
Acceptability:	NASA ARC partnered with the FAA to design and fund the facility, develop the requirements and validate the capabilities.
Ease of integration:	• FFC has experience in integrating new technologies/software (e.g. SMS, ASR-9). • FFC has experience in integrating external simulators and external targets into the scenarios.
Documentability:	High • Simulation run out-the-window scene can be recorded and replayed. • Controllers-Sim Pilot communication is recordable. • Airport surface operation data (e.g. taxi times, departures rates, incursions) are recordable. • Tower ambient sound is recordable.

	• Digital video of tower activities is recordable. • Controller surveys can be administered.
Advantages:	• Mitigates risk of unworkable or unsafe airport changes • Ideal environment for obtaining controller feedback by eliminating concern for safety • Cost-effective way to evaluate new airport design before major investment • More thorough testing by flexibility to alter test conditions (e.g. weather) • NASA as neutral party promotes pilot and controller cooperation, buy-in
Disadvantages:	• 3-4 month lead-time is required to develop a new airport database and traffic exercises. • Large number of Sim-Pilots is required for high traffic volume scenarios.

14. HAZOP (Hazard and Operability study)

References used:	Key references: • [Kennedy slides] • [Kirwan&Ainsworth92] Other references: • [CAA-RMC93-1] • [CAA-RMC93-2] • [Foot94] • [Kennedy&Kirwan98] • [Kirwan98-1] • [Kirwan-sages] • [Kletz74] • [Leveson95] • [Reese&Leveson97] • [ΣΣ93, ΣΣ97] • [Storey96] • [Villemeur91-1] Additional reading: • [Bishop90], [EN 50128], [Garrick88], [Kirwan94], [MUFTIS3.2-I], [Rademakers&al92], [Rakowsky], [Toola93]
Alternate names:	None
Primary objective:	Aim is to discover potential hazards, operability problems and potential deviations from intended operation conditions. Also establishes approximate likelihood and consequence of event. HAZOP is a qualitative method; it does not attempt to quantify hazards. In Chemical process industry, the term HAZAN (HAZard ANalysis) denotes numerical methods.
Description:	HAZOP is based on a group review, and is essentially a structured brainstorming using specific guidewords. Sometimes regarded as adaptation of FMEA [Villemeur91-1]. The basic notion is that the system is a collection of connected nodes. A HAZOP study considers various aspects (or parameters) of the operation of nodes and flows between them. In particular, it considers deviations from the expected behavior, prompted by guidewords. The consequences of deviations from the intended functioning of the system are also considered. The five HAZOP requirements are: 1. A team of multi-disciplinary 'experts', including chairperson, secretary, system designer, engineer, operator/controller, human factors expert 2. A system representation, in terms of nodes/parameters and flows between them. For a human HAZOP this can be in the form of a task analysis diagram, a decision flow diagram, or a human machine interface diagram 3. A list of guide words, e.g. • NO or NONE, meaning a complete negation of the intention • REVERSE, meaning the clear opposite of the intention • LESS OF / MORE OF, meaning a quantitative decrease / increase • AS WELL AS / PART OF, meaning a qualitative increase / decrease • SOONER THAN / LATER THAN, meaning intention done sooner / later than required • Some other references in addition use guidewords like OTHER THAN, REPEATED, MIS-ORDERED, EARLY, LATE 4. A list of property words. For an engineering system these may be e.g. flow,

	temperature, pressure, concentration, reaction, transfer, contamination, corrosion/erosion, testing. For a human HAZOP these property words could include e.g. Information, Management, Selection, Communication, Input 5. A recording form to capture information, i.e. a table with the following column headings: Step, Deviation, Cause, Consequence, Indication, System defence, Recommendations Note that in practice, the name HAZOP is often (ab)used for any "brainstorming with experts to fill a table with hazards and their effects".
Steps:	In [Storey96], a HAZOP is typically conducted by a team of 4 to 8 engineers, including experts in the application area as well as those directly concerned with the design of the system. A summary of the HAZOP study process is given by the figure below .  [Storey96] provides a more detailed flowchart of the HAZOP study process. In addition, he notes that various guidewords will be given varied interpretations depending on the industry concerned and where they are applied. For this reason the meaning of each guideword must be defined as part of the study.
Applicability range:	HAZOP is a hazard identification and criticality evaluation approach, which applies to complex systems with human operations in the loop. HAZOP can also be applied to a software requirements specification, [Leveson95], [Storey96]. In that case, suitable attributes might include 'data value', 'pointer value', 'algorithm', 'timing', and suitable guidewords might include 'incorrect', 'too fast', and 'too slow'. [Leveson95] and [Reese&Leveson97] refer to Software Deviation Analysis (SDA) as an automated variant of HAZOP, suitable for software.
Life cycle stage:	Since HAZOP uses all types of process descriptions as input, it is best used late in design. However, a preliminary HAZOP can be applied on conceptual process descriptions early in the design stage to avoid later costly problems. A full HAZOP can then be done later in

	the design process, even if a preliminary HAZOP has already been done.
Experience in application to air traffic:	Although HAZOP is most often used as a method of analyzing hazards within chemical and process control plants, in recent years it has also come to be accepted as a powerful technique within other sectors, and is now used in a range of applications, including those based on the use of computers. NATS has been applying HAZOP to ATM, for example.
Related methods:	Link to Brainstorming, Change Analysis, Maximum Credible Accident/ Worst Case, Human (Error) HAZOP (Human (Error) Hazard and Operability study), SCHAZOP (Safety Culture Hazard and Operability), HAZid (Hazard Identification), CIT (Critical Incident Technique), Job Safety Analysis, Talk-Through, Walk-Through Task Analysis. HAZid (Hazard Identification) is a modification of HAZOP especially to be used for the identification of human failures, see [CAA-RMC93-1], [CAA-RMC93-2], [Foot94]. It has an additional first column with some keywords to lead the guidewords. In [ΣΣ93, ΣΣ97], HAZOP is referred to as an integration of Brainstorming and the Delphi method.
Availability and tool support:	HAZOP is widely available. Spreadsheets can be useful as supporting tools. Numerous supporting tools exist; see the Global Aviation Information Network (GAIN) Working Group B (Analytical Methods and Tools).
Maturity:	HAZOP was initially developed by Imperial Chemical Industries in the early 1970s and later improved upon and published by the Chemical Industries Association in London [Kletz74]. HAZOP is applied most often to thermal-hydraulic systems, and is essentially used by the British chemical industry; about half of the chemical process industry now uses HAZOP for all new facilities. It has also been found to be a good safety tool in the offshore and onshore petrochemical industries, and with some application in the nuclear power industry. It has proven itself on many occasions, and has recently been used by NATS on their FAST and FACTS design projects, with success.
Acceptability:	[Kennedy&Kirwan98]: HAZOP has received wide acceptance by both the process industries and the regulatory authorities (Andrews and Moss, 1993).
Ease of integration:	HAZOP can provide input to e.g. FTA, ETA.
Documentability:	[Kirwan98-1] rates documentability as High. However, the documentation is lengthy (for complete recording).
Advantages:	In comparison with some other hazard identification techniques like checklists, HAZOP is able to elicit hazards in new designs and hazards that have not been considered previously. Other general strengths are: 1. HAZOP is effective for both technical faults and human errors; it covers human operators in the loop. 2. HAZOP can rapidly spot those functionalities whose failure mode effects can be remedied. It recognizes existing safeguards and develops recommendations for additional ones. 3. Unlike FMEA it does not require the systematic study of the failure modes of each part of the functionality and of their effects. 4. It does not concentrate only on failures, but has the potential to find more complex types of hazardous events and causes. 5. It provides a systematic and exhaustive coverage and can lead to the discovery of new hazards. It can provide a very comprehensive hardware review 6. It encourages creative thinking about all the possible ways in which hazards or operating problems may arise. 7. HAZOP is very useful in the analysis of complex systems or plants, with which there is yet little experience, and procedures that occur infrequently. 8. It can identify design problems at an early stage. 9. Only limited training required; HAZOP is an ‘intuitive’ method

	10. It uses the experience of operating personnel as part of the team. The use of a team gives a range of viewpoints and the interaction of several disciplines or organizations provides results that are often overlooked by groups working in isolation. 11. HAZOP has a good track record in certain industries; it is widely used and its disadvantages are well-understood 12. The technique is versatile.
Disadvantages:	According to some references, a HAZOP can be very time consuming and labor intensive. Six to eight people required, including the services of an experienced HAZOP team leader. Some other general weaknesses are: 1. A main weakness of the method is that the same group of experts identify both hazards and mitigating measures, whereas the latter function may be better served by other experts. 2. It is difficult to assign to each guideword a well-delineated portion of the system and failure causes. 3. Errors can be made in the analysis – in particular if the group becomes fatigued, hazards may be overlooked. 4. Due to the systematic approach used and the number of people involved, the method is often time-consuming, and therefore expensive. 5. Its success heavily depends on the facilitation of the leader and the knowledge, experience, degree of co-operation and commitment of the team. GIGO (garbage in, garbage out) applies. 6. HAZOP may not pick up on multiple failures. 7. HAZOP cannot easily model dependency between failures. 8. It concentrates on single deviations. 9. It is optimized for process hazards, and needs modification to cover other types of hazards. 10. It requires development of procedural descriptions, which are often not available in appropriate detail. However, the existence of these documents may benefit the operation. 11. Documentation is lengthy (for complete recording). 12. It analyses causes and effects with respect to deviations from expected behavior, but it does not analyze whether the design, under normal operating conditions, yields expected behavior or if the expected behavior is what is desired. 13. Deviations from within components or processes are not inspected directly; instead, a deviation within a component is assumed to be manifested as a disturbed flow. Process-related malfunctions and hazards may be neglected in favor of component-related causes and effects. Overall, HAZOP has become a common approach for process plant design offshore, and has become procedural. HAZOP is widely used for simultaneous operations and assessment of evacuation systems. However, other hazard identification techniques may be more efficient for some other applications.

15. HEART (Human Error Assessment and Reduction Technique)

References used:	Key references: • [Williams88] Other references: • [CAA-RMC93-1] • [CAA-RMC93-2] • [Foot94] • [Humphreys88] • [Kennedy] • [Kirwan&Kennedy&Hamblen] • [Kirwan96-I] • [Kirwan&al97-II] • [Kirwan97-III] Additional reading: • [Kirwan94], [MUFTIS3.2-I]
Alternate names:	None
Primary objective:	HEART quantifies human errors in operator tasks. It considers particular ergonomic and other task and environmental factors that can negatively affect performance. The extent to which each factor independently affects performance is quantified, and the human error probability is then calculated as a function of the product of those factors identified for a particular task.
Description:	The method is based on the following premises: 1. Basic human reliability is dependent upon the generic nature of the task to be performed. 2. Given perfect conditions, this level of reliability will tend to be achieved consistently with a given nominal likelihood within probabilistic limits. 3. Given these perfect conditions do not exist in all circumstances, the human reliability predicted may be expected to degrade as a function of the extent to which identified Error Producing Conditions (EPCs) might apply. [Kennedy] gives the following overview of the HEART process. This process follows six steps: **Step 1.** Classify generic task type • The analyst has a choice of eight different generic task types (GTTs), A through H. These are listed in the first column of the table below. The GTTs are differentiated in terms of the characteristics or attributes that describe the task being assessed. Category M is available when the characteristics of the task fit none of the eight categories. **Step 2.** Assign Nominal Human Error Probability. • The Nominal HEP (or unreliability) for the task is obtained for the GTT, according to the last column of the table below.

GTT description	Nominal Unreliability
A - Totally familiar, performed at speed with no idea of likely consequences	0.55
B - Shift or restore system to new or original state on a single attempt without supervision or procedures	0.26
C - Complex task requiring high level of comprehension and skill	0.16
D - Fairly routine task performed rapidly or given scant attention	0.09
E - Routine highly-practised, rapid task involving relatively low level of skill	0.02
F - Restore or shift a system to original or new state following procedures with some checking	0.003
G - Completely familiar, well designed, highly practised routine task occurring several times per hour	0.0004
H - Respond correctly to system command even when there is an augmented or automated supervisory system	0.00002
M - None of the above	

Note that [Humphreys88] also lists 5-95% percentile bounds for the unreliabilities.

Step 3. Identify error producing conditions.

- The analyst is then required to select Error Producing Conditions (EPCs) that have a negative impact on the task. EPCs should be separate to those already covered in the GTT, and should be of an obvious nature and defendable by the analyst. The EPCs are given in the table below, together with their associated total effect factors. These factors denote the maximum predicted nominal amount by which unreliability might change going from good conditions to bad. This means that conditions not affecting the reliability will not be taken into account (factor is 1) and conditions which affect the reliability will be taken into account with a factor larger than 1.

Error Producing Conditions (EPC)	Total effect
1 - Unfamiliarity	x 17
2 - Shortage of Time	x 11
3 - Low signal to noise ratio	x 10
4 - Ease of information suppression	x 9
5 - Ease of information assimilation	x 8
6 - Model mismatch (operator / designer)	x 8
7 - Reversing unintended actions	x 8
8 - Channel capacity overload	x 6
9 - Technique unlearning	x 6
10 - Transfer of knowledge	x 5.5
11 - Performance standard ambiguity	x 5
12 - Mismatch between perceived / real risk	x 4

Step 4. Determine the Assessed Proportion of Affect (APOA).

- For each EPC identified in Step 3, the analyst makes a judgement on how much it

	influences the overall unreliability of the task. This is known as the Assessed Proportion of Affect (APOA) for the EPC. **Step 5.** Calculate Final HEP • The Final Human Error Probability is calculated as follows: Suppose an assessor wants to determine the unreliability of an operator task. First he determines which of the generic tasks of the first table applies to this problem. The associated factor r in the first table determines the nominal unreliability. Next, he determines which of the EPCs of the second table apply to the task, looks up their associated factors f_i and estimates for each EPC, using his own judgment, the APOA, i.e. what proportion p_i of these error producing conditions might affect the operator in this special case. The nominal likelihood of human failure then becomes $r \times \prod_i p_i (f_i - 1) + 1$, if this is less than or equal to one, where Π_i denotes product over all i. **Step 6.** Consider Error Reduction Measures (ERM) • For each EPC identified in Step 3, the analyst may attempt to apply the associated HEART ERMs. Here, a tactical or a strategic approach could be adopted. Note that the derivation of appropriate ERMs is a specialist task that involves more than just choosing items from a table. In [Humphreys88], [Williams88] some case studies in which HEART was used are presented.
Applicability range:	HEART quantifies human errors in operator tasks.
Life cycle stage:	It can be used both in design stage and in operational stage.
Experience in application to air traffic:	HEART has been used by NATS. In reference [CAA-RMC93-1], [CAA-RMC93-2], [Foot94], they used it for human failures quantification of events in Fault Trees modeling the occurrence of top events in ATC operations for two airspace sectors in the UK.
Related methods:	NE-HEART (Nuclear Electric HEART); CORE-DATA; Use of Expert Judgment; Hierarchical Task Analysis; TRACER-Lite; various Human Reliability Assessment Methods; THERP; JHEDI
Availability and tool support:	HEART is publicly available. Tool support is not really necessary.
Maturity:	HEART was developed by Jeremy Williams, a British ergonomist, in 1985. Presently, it is the most popular human error quantification technique used in the UK, especially for nuclear power and reprocessing, and chemical industry, and is used in various European and Scandinavian industry sectors (petrochemical and chemical), as well as for railway and defence industries.
Acceptability:	Quantification of HEPs is usually by HEART in UK nuclear power plant (NPP) PSAs/HRAs, and may include the usage of the extended HEART approach called NE-HEART (Nuclear Electric HEART), which added several new generic error probabilities specific to NPP tasks and systems (e.g. 'NE1' and 'NE2' for errors in emergency diagnosis). Some guidance on HEART usage exists from other projects on Consistency in Usage of HEART. Generally category 'F' is most used in Human Reliability Assessments (HRAs), with usage of a relatively small set of EPCs by analysts. Analysts are encouraged to use EPCs, however, to create meaningful links (if only qualitative ones) between the HEPs and error reduction that may occur later in the PSA. [Kirwan&Kennedy&Hamblen] In [Humphreys88], several human reliability assessment techniques, among which HEART, are compared on various criteria, which are: Accuracy, Validity, Usefulness, Effective use of resources, Acceptability and Maturity. All techniques are evaluated on these criteria by a panel of experts, in the form of marks from 1 to 5, where 5 means evaluated high (positive) and 1 means evaluated low (negative). These criteria evaluations

	are next weighted and added for each technique. The results are presented in the table below. According to this table, HEART receives the highest Preference Index of the techniques evaluated.

Criteria (weight)	APJ	PC	TESEO	THERP	HEART	IDA	SLIM	HCR
Accuracy (0.30)	3	3	1	3	3	1	3	1
Validity (0.22)	4	3	1	3	3	3	3	1
Usefulness (0.15)	4	2	4	3	5	4	5	2
Resources (0.15)	3	2	5	2	5	2	2	3
Acceptability (0.11)	3	4	1	5	3	3	4	2
Maturity (0.07)	5	3	1	5	2	2	4	1
Preference Index	3.51	2.81	2.05	3.21	3.53	2.33	3.33	1.56

	Note that the rather low maturity rating for HEART may be due to the fact that this evaluation was done in 1988, only a few years after HEART was developed. The ratings for accuracy of THERP and HEART are confirmed by [Kirwan96-I], [Kirwan&al97-II], [Kirwan97-III] who experimentally found the accuracy of THERP and HEART reasonable and similar to each other. HEART has been positively validated three times in three separate studies in the nuclear power industry. A project is underway in the nuclear power industry to 'revamp' HEART with human error data from CORE-DATA (see the Human Error Data Collection template), increasing its acceptability and validity.
Ease of integration:	HEART is a quantitative human error probability assessment technique only. It can be used in combination with qualitative Human task analysis techniques that identify operator tasks to be assessed. According to [Kennedy], HEART is relatively simple to use when compared with other human reliability quantification methods and also it is easily understood by practitioners from both engineering and social science backgrounds.
Documentability:	According to [Kirwan96-I], [Kirwan&al97-II], [Kirwan97-III], HEART consistency is reasonable, but worth attempting to improve. In practice, different assessors are not always consistent in their choice of generic task types (GTT), since the categories overlap. However, this does not necessarily mean that the final human error probabilities are much different. The HEART steps are straightforward and repeatable. [Humphreys88] rates HEART's auditability as potentially high, depending upon how well the individual analyst has documented a study.
Relevance to ATM:	Since probabilities of human operator tasks have a big influence in ATM safety assessments, a technique like HEART is very relevant for SAM. General strengths of HEART are: 1. HEART has a very low demand on assessor resources. 2. The method is a flexible assessment tool. 3. It identifies the major influences on human performance in a systematic, repeatable fashion. 4. It has been developed primarily for use in design assessments and appears to be most powerful and useful in this context. 5. It can be incorporated by an FTA. 6. Limited training is required 7. It is conservative (tending towards pessimism rather than optimism) 8. It is capable of sensitivity analysis 9. A range of EPCs is used

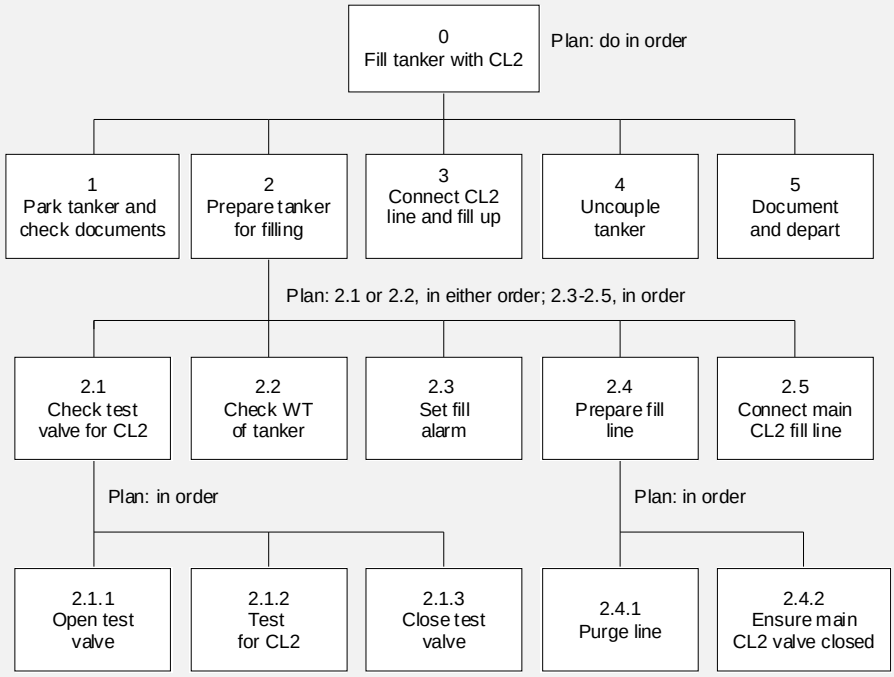
	10. It identifies areas for error reduction, albeit simplistic ones 11. It is versatile – HEART has a track record in various industries
Con's and resources:	HEART is very resource efficient (see also the table under "Acceptability"). General weaknesses are: 1. Only tasks in isolation can be assessed. 2. The assessment part of HEART will tend to be pessimistic. 3. The technique is not exhaustive. 4. The empirical justifications of the HEART multipliers are currently obscure. 5. Dependence between different factors is not modeled within the technique. 6. When applying HEART to ATM, one has to take into account that Air Traffic Controller tasks and their contexts are likely to differ considerably from those of operators in the process industries on which much previous research has concentrated. 7. Errors of commission (see Section 7) are not assessed. 8. Assessor judgement is required, especially in step 4 of the technique, hence the technique may be open to abuse 9. Double counting effects between task types and error producing conditions may lead to biases 10. Guidance to determine APOA (Assessed Proportion of Affect) may be necessary 11. There is no modeling of task / error dependence

16. HERA (Human Error in ATM)

References used:	**EUROCONTROL (2003)** The Human error in ATM Technique (HERA JANUS). HRS/HSP-002-REP-03. Eurocontrol. Brussels. **EUROCONTROL (2003)** Technical Review of Human Performance Models and Taxonomies of Human Error in ATM (HERA). Eurocontrol. Brussels. **EUROCONTROL (2003)** A method for predicting Human Error in ATM (HERA Predict). HRS/HSP-002-REP-07. Eurocontrol. Brussels.
Alternate names:	./.
Primary objective:	HERA is a retrospective incident analysis method providing insights into the cognitive processes of controllers during incidents.
Process steps:	HERA is subdivided into a retrospective part for incident analysis and a prospective part for using the information collected for the assessment of human error probabilities in safety cases.
Description:	**A) HERA Observe:** The classification system was developed in two formats - a tabular format and a series of decision-flow chart diagrams. Tabular format: A tabular hierarchical format was used to represent the following: • Task • Information and Equipment • Error / Violation Types (ETs) • Contextual Conditions (CCs) This format allows for the quick identification of relatively clear categories. Decision-flowcahrt diagrams: A series of decision-flowchart diagrams were developed to enable the HERA analyst to identify errors by answering a series of 'Yes/No'-type questions. There are separate decision-flow diagrams for: • Error Detail (ED) • Error Mechanisms (EMs) for each Error Detail • Information Processing levels (IPs) for each Error Detail • Contextual Conditions (CCs) sub-categories. **B) HERA Predict:** HERA Predict consist of nine steps as follows: • Undertake a Functional Task Analysis (FTA) on the system. • Verify the FTA within the operational environment with air traffic controllers and other technical experts depending on the system under analysis. • For each identified task, identify the associated HERA-JANUS Contextual Conditions. • Undertake an FTA on the changing or changed system. • Verify the FTA within the operational environment with air traffic controllers and other technical experts depending on the system under analysis. • For each identified task, identify the associated HERA-JANUS Contextual Conditions. • Compare the current operational tasks to the changed operational tasks, and list the changes in a change matrix. • Undertake a HERA-JANUS Error Detail, Error Mechanism, Information Processing level and Contextual Conditions identification process on all task

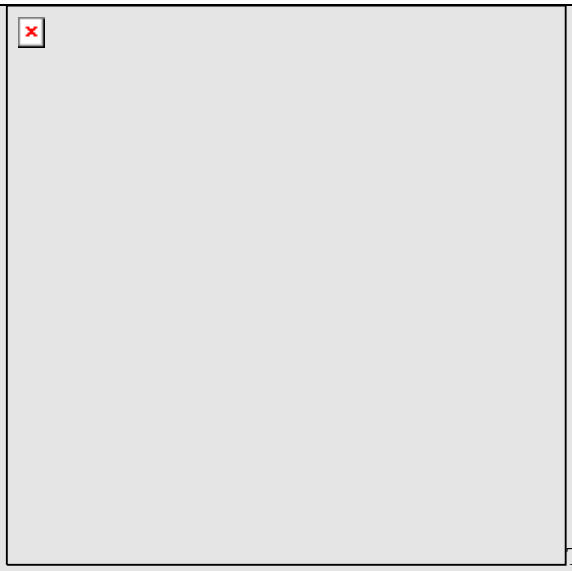
	changes. • Establish the risks involved by assessing frequency of task and the severity of occurrence, if known.
Applicability range:	The method is focused on the controllers' cognitive performance and related influencing factors.
Life cycle stage:	The retrospective part of the technique can be applied in the analysis of incidents mainly (operational phase). The prospective part is applicable for early design of systems up to the operational improvement.
Experience in application to air traffic:	HERA is applied in ATM operational safety management. Courses are available at the EUROCONTROL Training Institute IANS. A HERA User Group (HUGS) was established where the method is validated, continuously improved and aligned to needs of operational safety managers. The group also shares data collected with the method in order to provide cross-service provider insights. Data collected was prospectively used for a systematic comparison of the assessment of human errors in safety cases with operational experience in the EUROCONTROL Upper Area Control Centre in Maastricht (MUAC).
Related methods:	TraceR is a similar approach developed in the UK ATM environment, which also combined prospective and retrospective features. TraceR and HERA use almost equivalent steps but differ in detail. HERA was more applied in the retrospective analysis of incidents while TraceR was more used for error assessment. A further exploitation of HERA data for design is possible by linking it to the SHAPE (Solutions for Human Automaiton Partnership for European ATM) and SAFbuild projects. A similar approach for exploiting retrospective data for prospective assessment was developed in nuclear CAHR (Connectionism Assessment of Human Reliability).
Availability and tool support:	The retrospective part of the technique is supported by a web based incident analysis tool.
Maturity:	The retrospective part of the technique is - related to the rather recent introduction into the safety management of ANSPs - already in a mature state and receives considerable stakeholder support. The prospective part of the technique has received first applications in NATS and MUAC.
Acceptability:	The technique was recently officially accepted as an important tool for the implementation of safety management within EUROCONTROL.
Ease of integration:	The technique and underlying logic is easy to understand. However, recommended as a minimum, practitioners take formal training.
Documentability:	High.
Advantages:	HERA provides insights into the cognitive processes of controllers and their working practices. Herewith it allows better understanding of the constraints and conditions under which controllers work. These conditions are known as relevant for understanding controllers' incompliance with existing procedures as well as skill-based errors.
Disadvantages:	HERA does only provide limited insights into other operational levels (e.g., maintenance, management, regulation) and into safety net interactions (only via contextual conditions). A further development into this direction is envisaged by EUROCONTROL Safety and Security Management in cooperation with Safety R&D EEC.

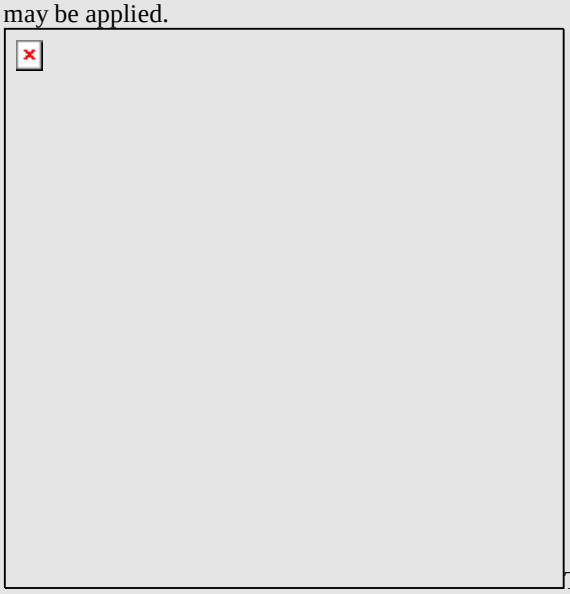
17. HTA (Hierarchical Task Analysis)

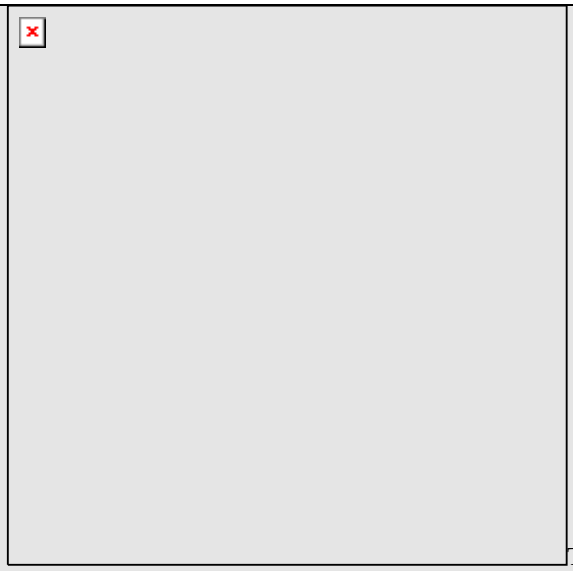
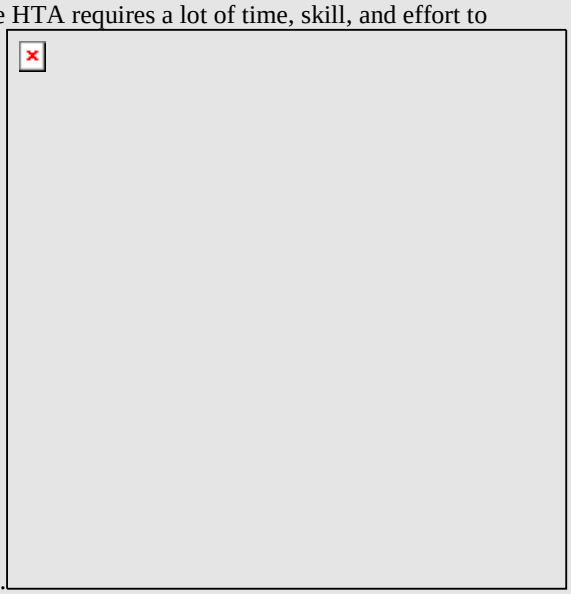
References used:	Key references: • [Shepherd01] • [Kirwan&Ainsworth92] • [Kirwan94] Other references: • [Kirwan&al97] Additional reading: • [Stanton&Wilson00]
Alternate names:	None
Primary objective:	HTA is a method of task analysis that describes tasks in terms of operations that people do to satisfy goals and the conditions under which the operations are performed. The focus is on the actions of the user with the product. This top down decomposition method looks at how a task is split into subtasks and the order in which the subtasks are performed. The task is described in terms of a hierarchy of plans of action.
Description:	The method involves defining an overall goal, breaking this down into tasks, sub-tasks, and at the lowest level of description, operations. These are usually represented diagrammatically in a hierarchical 'tree' fashion. The relationship between a set of sub-ordinate tasks (or operations or sub-tasks) and their parent goal (or task or sub-task) is defined by a plan. The 'plan' at each node in the HTA states 'when' each of the tasks or operations below it are to occur. There are a number of plan types available, which can describe most types of relationships. The HTA is usually also numbered for easy and reliable reference to the various tasks/operations and levels in the task analysis representation. Transfer from one page of HTA to another is achieved via transfer boxes as in fault tree analysis. The figure below shows an example HTA, which is from [Kirwan94].  The same analysis can also be represented in table format, see e.g. [Kirwan&Ainsworth92] for an example. Although diagrams as in the figure above are more easily assimilated by

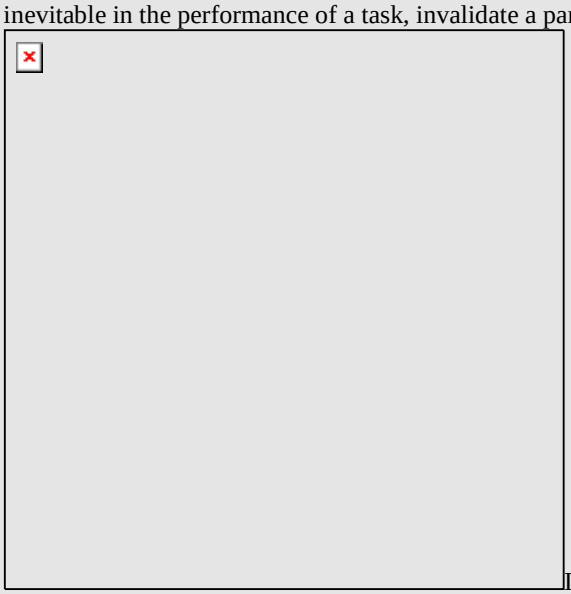
	people, tables are more thorough, because detailed design notes can be added. The technique itself at first sight resembles a flowchart, but the boxes are laid out hierarchically in a top-down fashion, going from a top level goal, to the various tasks which together fulfil that goal, to the actual physical and mental operations that are required to carry out the task. Three 'levels' in the HTA is usually the minimum, with seven as a practically-recommended maximum: the required depth of the HTA depends on the depth of analysis and the complexity of the task. The general HTA steps are: 1. Identify main task goal. 2. Describe the main goal as a set of sub-operations with a plan specifying under what conditions and order the operations are performed. Descriptions may be graphical and/or textual. Remember to use verbs. 3. Decide if further breakdown of operations is needed. 4. If answer to #3 is yes, go to #2. 5. Analyse the decomposition for inefficiencies of task operations to achieve goal. 6. Recommend changes to task operations and plans to improve system performance. Look at redesign of the task, interactions, tools, products or the system. An important aspect of HTA is known as the 'stopping rule', or the decision of when to stop re-describing the task in terms of sub-tasks and operations. The main stopping rule is to stop re-describing when further re-description will add no further useful information for the analysis. The analyst must use judgment to decide on the level of re-description required for a particular analysis, and in the HRA context, this will depend on the scope of the analysis as defined in the problem definition, and the risk of missing potential errors in a task by failing to re-describe to a particular level. Wherever the analyst does stop, (s)he would then simply stop re-describing at those points, and this is represented in the HTA by drawing a line under the description boxes for those tasks. Another frequently used HTA stopping rule is P x C: Stop when the product of probability of unsatisfactory performance (P) times the cost of unsatisfactory performance (C) approaches zero (usually P or C will tend to zero first). The cost should be interpreted broadly, for example time to correct the results of a wrong keystroke in software, personal injury due to lifting etc. [Kirwan94] provides some detailed guidance questions and rules on HTA generation for safety assessment, with more recent and more comprehensive guidance being given by [Shepherd01].
Applicability range:	HTA is best suited for analysing relatively simple cognitive and physical tasks where a clear goal, tasks and subtasks required to accomplish the goal can be determined. It is helpful for a redesign when the steps involved in the process are known based on the existing product. A HTA can be used in many types of human factors assessments, e.g. Function allocation, Interface and display design, Work organization, Job design, Training and procedures, The development of operator manuals and job aids, Error identification and quantification, [Kirwan&Ainsworth92], [Kirwan94].
Life cycle stage:	HTA can be applied in all lifecycle stages to help designers articulate how tasks should be carried out [Kirwan&Ainsworth92].
Experience in application to air traffic:	According to [Kirwan&al97], HTA's were completed for all NATS' ATC domains in the UK, including Area Control, Terminal Control, Airfield Operations, Distress & Diversion, and Oceanic Operations.
Related methods:	Link to TRACER, HEART, Link Analysis, Task Decomposition, OSD (Operational

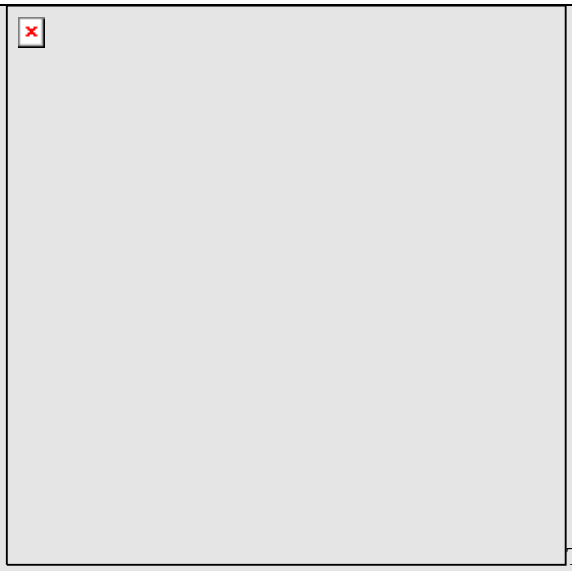
	Sequence Diagram), Task Description Analysis, Timeline Analysis, HTLA (Horizontal Timeline Analysis), VTLA (Vertical Timeline Analysis), Operator Task Analysis, DADs (Decision Action Diagrams), OFM (Operation Function Model), SDA (Sequence Dependency Analysis). FAST (Functional Analysis System technique) is a quick variant of the HTA concept, probably most pertinent in the early stages of design [Kirwan&Ainsworth92]
Availability and tool support:	HTA is available. Although it can be done with paper and pencil, computer support can be helpful, especially in preparing tables and hierarchical diagrams.
Maturity:	HTA was developed in 1971. It is the most often-used task analysis technique [Kirwan94]
Acceptability:	HTA is the most popular and flexible of the task analysis techniques.
Ease of integration:	HTA can be supported and integrated with many other task analysis techniques and approaches of data collection. It is relatively straightforward to apply and is much simpler than many other task analysis approaches.
Documentability:	There does not seem to be a structured method for gathering the input information required, hence carefully documenting the gathering process may sometimes be forgotten. It is often best to use a tabular format as well as the diagram format, both to record and to communicate the analysis.
Relevance to ATM:	A technique like HTA is relevant to ATM applications since human tasks can greatly affect ATM safety; however, for complex human tasks, the technique has its weaknesses. Some general strengths are: 1. HTA is easy to learn and to use; It is easy with an HTA to assimilate a large amount of information relatively quickly, whereas certain other techniques require more intensive scrutiny. 2. Is relatively straightforward to apply. 3. It can be used as a basis for addressing a large range of problems. 4. HTA is an economical method of gathering and organizing information since the analyst needs only to develop the parts of the hierarchy where it is justified. 5. The hierarchical structure of HTA enables the analyst to focus on crucial aspects of the task within the context of the overall task. 6. HTA provides a context on which other specific approaches to task analysis (e.g. for data collection of for modeling design possibilities) may be applied to greater effect. 7. HTA is best developed as a collaboration between the task analyst and people involved in operations. Thus, the analyst should operate in accordance with the perceived needs of line personnel who are responsible for effective operation of the system. 8. HTA offers two distinct training benefits to people engaged in the analysis. First, analysts can use the technique rapidly to gain insight into processes and procedures entailed in plants and organizations generally. Second, it has training benefits for people collaborating with the analyst, since they are required to express how they think tasks should be carried out, thereby articulating their understanding of systems. 9. HTA forms the basis of many other assessments, e.g. communications analysis. 10. Because each task element is only broken down into a limited number of sub-elements, the analyst is provided with a convenient check that no task elements have been omitted at each stage. 11. Separating the task into subtasks allows the design of supporting systems to offer new ways of performing parts of the task. 12. Subtasks can be expanded further to show more details. In some circumstances, subtasks can be broken down into individual keystrokes. A detailed model of this kind would enable precise performance analysis. 13. Helpful in the redesign of an existing product or process where tasks should follow a logical sequence.

14.  The hierarchical structure of this task analysis approach allows the analyst to concentrate on crucial aspects of the task within the context of the overall task. Also other specific techniques of task analysis may be applied.

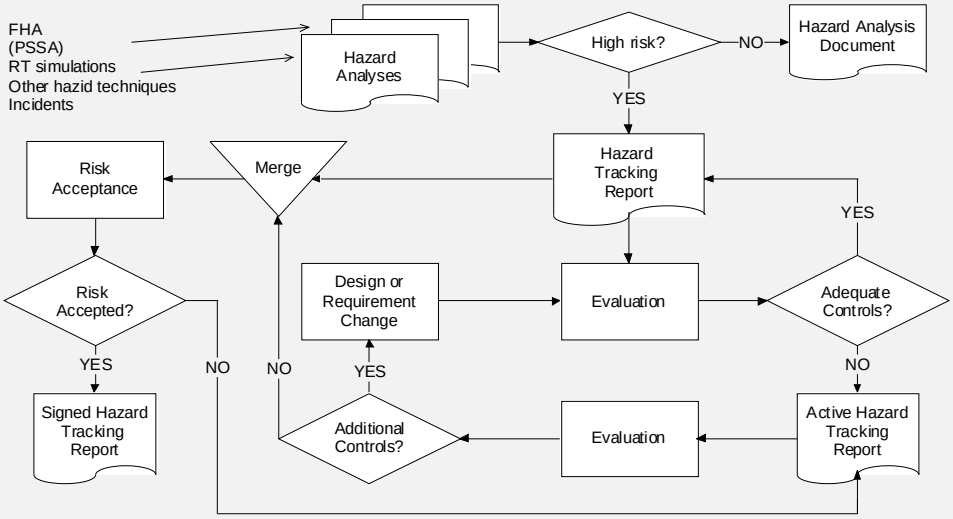
15.  This method is best developed as a collaboration between the task analyst and user involved in operations. Thus the analyst should operate in accordance with the perceived needs of people who are users of the system.

	16.  The HTA is commonly used and widely accepted in cognitive task analysis. 17. The HTA is very powerful because it can be applied to different types of physical and mental activities and different domains of applications.
Con's and resources:	The HTA requires a lot of time, skill, and effort to use.  An HTA can be undertaken by one analyst; more than one for larger tasks. In addition, the method must be carried out with the collaboration of managers, engineers and operating staff, and this collaboration involves agreement, time and effort from a lot of people. Some general weaknesses of HTA are: 1. The major weakness is that HTA tends to focus on the "what", rather than the "why" of tasks and subtasks. 2. The analyst needs to develop a measure of skill in order to analyze a task effectively – the technique is not a simple procedure that can be applied immediately. However, the necessary skills can be acquired reasonably quickly through practice. 3. HTA has to be carried out with a measure of collaboration from managers, engineers and other operating staff. This is necessary in order to ensure adequacy of information and to confirm that the HTA complies with managerial requirements. While this collaboration is in most respects a strength, it entails commitment of time and effort from busy people.

	4. HTA focuses on processes, meaning that it may not pick up problems with the look, layout, or content of the interface. 5. While a top-down decomposition and the plans can give a general sense of sequential actions, an HTA does not give a good sense of the length of time of various activities. As a result, inefficiencies due to "waiting" may be missed. Other techniques (e.g. timeline analysis) must be used to achieve such objectives. 6.  Errors and “unforeseens”, inevitable in the performance of a task, invalidate a part of the plans. 7.  It is difficult to represent in the plan goals which apply to every activity, interrupted activities or 'ad hoc' activities

	8.  The HTA applies only to procedural activities and not to heavily parallel activities. 9. Real tasks may be very complex. HTA does not scale very well; the notation soon becomes unwieldy, making it difficult to follow. In practice no more than seven 'levels' must be used, with 4-5 as an ideal HTA 'depth'. 10. Some cognitive activities can be difficult to represent in HTA.	

18. HTRR (Hazard Tracking and Risk Resolution)

References used:	Key references: • [FAA00] • [FAA SSMP] Other references: • [NEC02] • [Stroup]
Alternate names:	None identified
Primary objective:	HTRR is a method of documenting and tracking hazards and identifying safety issues, and verifying their controls after the hazards have been identified by analysis or incident. The purpose is to ensure a closed loop process of managing (i.e. identifying and controlling) safety hazards and risks. Each program must implement a Hazard Tracking System (HTS) to accomplish HTRR.
Description:	A key part of the HTRR process, management risk acceptance, ensures that the management activity responsible for system development and fielding is aware of the hazards and makes a considered decision concerning the implementation of hazard controls. This process is shown in the figure below, which is from [FAA00], although slightly adapted to match SAM recommendations.  The hazard analyses are fed by e.g. FHA (Functional Hazard Analysis), Real-time simulations, incident reports and other hazard identification techniques. Also, output of PSSA (Preliminary System Safety Assessment) might be used. When a safety analysis is completed or an incident analysis identifies the hazard, the Medium and High-risk hazards are copied into the HTS (Hazard Tracking System). In the HTS, each hazard is recorded in a unique record, named a Safety Action Record (SAR). Each SAR includes (see [FAA SSMP]): 1. A description of the hazard, status 2. An updated narrative history, including origin and context of hazard identification 3. A current risk assessment 4. Justification for the risk severity and probability to include existing controls, and requirements for the SRVT (Safety Requirements Verification Table) 5. A mitigation and verification plan 6. Potential effects if the hazard is realized (Note that Section 2.2.3 of [FAA00] gives a more detailed list of what SARs must

	include). Each SAR must be classified according to status (Proposed, Open, Monitor, Recommend closure, Closed). All program SARs are reviewed with (1) Proposed status, (2) Open status, and (3) current high risk. This review is to occur at least biannually per program. The key is the maintenance and accessibility of a SAR. In [NEC02], in a HTRR, a single closed-loop hazard tracking system is established to document and track hazards and their controls, providing an auditable trail of hazard resolutions. A centralized file, computer database or hazard log must be maintained. The hazard log will contain: • The name of the safety engineer who generated the hazard report • Descriptions of each hazard, including an associated hazard risk index • The system/subsystem involved • Events/mission phases associated with the identified hazard • Hazard effects on personnel, equipment, platform and environment • Controls recommended to reduce the hazard to a level of risk acceptable to the Managing Activity • Initial, target and final risk assessment • Status of each hazard and its control • Traceability of the process on each hazard log item from initial identification to resolution at a level acceptable to the Managing Activity • Identification of residual risk • Action person(s) and organizational elements • Final disposition/verification • The signature of the Managing Activity person accepting the risk, which affects closure of the hazard log.
Applicability range:	The HTRR technique as described above applies mainly to hardware and software-related hazards. However, it should be possible to extend the method to also include human and procedures related hazards, by feeding these hazards from suitable hazard identification techniques.
Life cycle stage:	According to [Stroup], [FAA SSMP], HTRR is performed during Operations and maintenance.
Experience in application to air traffic:	[Stroup] mentions that FAA are establishing a National Airspace System (NAS) Wide Hazard Tracking and Risk Resolution database to monitor high and medium risks identified by the analyses.
Related methods:	Link to Failure Tracking. The hazard analyses are fed by FHA (Functional Hazard Analysis), Real-time simulations, incident reports and other hazard identification techniques. Also, output of PSSA (Preliminary System Safety Assessment) might be used. The TOPAZ methodology, for example, includes a hazard coverage analysis.
Availability and tool support:	Tool being developed [Stroup]
Maturity:	2000 or older
Acceptability:	HTRR is recommended by the FAA.
Ease of integration:	Hazard identification techniques other than those already mentioned can be easily integrated in the process.
Documentability:	The level of documentability of this technique is essential for a good outcome, and appears to be high.
Relevance to ATM:	ATM needs a systematic list of how each hazard is handled, hence a technique like HTRR is relevant for ATM safety applications. However, other techniques could also be appropriate (see Related methods).
Con's and resources:	Resources are required to properly take the origin of the hazard identification into account.

19. Human Error Database

References used:	Key references: • [Kirwan&Basra&Taylor.doc] Other references: • [Kirwan96-I] • [Kirwan&al97-II] • [Kirwan97-III] Additional reading: • [Kirwan&Basra&Taylor.ppt], [Kirwan&Kennedy&Hamblen]
Alternate names:	None
Primary objective:	To collect data on human error, in order to support credibility and validation of human reliability analysis and quantification techniques.
Description:	There is often significant uncertainty or lack of real confidence in human error probabilities derived through the use of Human Reliability Analysis (HRA) techniques, due to paucity of real data or to uncertainty over the accuracy of HRA techniques themselves. HRA has come to live with this; however, the potential advantages of 'real' data still outweigh the difficulties of collecting and structuring a database. An example of a human error data collection initiative is CORE-DATA (Computerized Operator Reliability and Error Database), funded by various industrial domains (especially nuclear power). CORE-DATA has been generated via a human reliability assessment user needs analysis, and is based on valid human error taxonomies by which qualitative and quantitative data can be identified and categorized. The database contains human error data that have been collected from a variety of sources. A similar initiative could be started for ATM, therefore CORE-DATA is described here. CORE-DATA currently contains over 400 data points. Data were originally (1992-1995) collated from the nuclear power industry, but recent activities (1995-2000) have extended into other industry sectors, such as offshore lifeboat evacuation, manufacturing, offshore drilling, permit-to-work, electricity transmission, nuclear power plant emergency scenarios, calculator errors, and a small number of ATM-related human error probabilities have been developed. Development of CORE-DATA is ongoing. The ultimate intention of the program is to learn generic insights into error irrespective of the industrial domain. Data can be searched within the system using the five search parameters of Industry type; Level of operations; Equipment/task; Human action, and External error mode. A search can be made as wide or as specific as required by manipulating these search parameters. Aviation is among the diverse data points currently within the system.
Applicability range:	Human error data collection can be used to provide input for human reliability analysis techniques, or to provide input to risk assessments (e.g. for human errors needed for fault or event trees).
Life cycle stage:	Databases with quantitative human error probabilities are most applicable during design. However, they may also be used as qualitative sources of hazards during earlier phases. Such databases can be extended with more data during operations and maintenance.
Experience in application to air traffic:	Some preliminary work has been carried out to generate a small number of human error probabilities as part of the ongoing CORE-DATA work program.
Related methods:	Link to HEART, TRACER, Fault Tree Analysis, Event Tree Analysis, Errors of Commission.
Availability and tool support:	CORE-DATA is a computerised system but also exists in hard copy format.

Maturity:	CORE-DATA was initiated in 1992, following a recommendation by an advisory committee for the safety of nuclear installations. CORE-DATA currently contains approximately 400 data points in the computerized format, and a further 1100 in hard copy format. After a recent study the database is being extended. Three main areas of further development are: 1) Consolidation of the CORE-DATA system; 2) Extending the database into key areas; 3) Development of CORE-DATA as an industry resource and service.
Acceptability:	CORE-DATA is currently being managed and developed by the UK Health & Safety Executive, the UK regulator.
Ease of integration:	Any human reliability analysis technique can profit from databases with human error probability data.
Documentability:	At the moment full documentation is not available, though the database itself can be queried.
Relevance to ATM:	Databases on human error probabilities are highly relevant for ATM human factors assessments. CORE-DATA contains real data on human error, rather than collections of data based on expert judgement (as its USA counterpart NUCLARR does). General advantages of using real data are: 1. They can be directly used in assessments (although for this purpose the database must be very large and specific to the application area) 2. They can be used as calibration data for certain HRA techniques (for example, Paired Comparisons needs two or three real human error probabilities in order to produce new probabilities – see the Use of Expert Judgement template) 3. They can be used as validation data when comparatively testing techniques (see e.g. [Kirwan96-I], [Kirwan&al97-II], [Kirwan97-III]) 4. They can be used as guidance data for assessors and regulators to know the approximate general failure rates for different tasks.
Con's and resources:	Resources – the computerised version can be used quickly to search for relevant human error data. Some general weaknesses are: 1. There is a danger in over-reliance in the 'real' data. The circumstances under which the data was collected should always be taken into account. 2. The database at the moment contains very little in the way of ATM-related data, therefore some effort is needed to populate the database, either from incident studies or from real-time simulations. 3. The international availability of the database remains unclear at this time, although the workings of the database, some sections of data, and its recording formats have been published.

20. Human Factors Case

References used:	Key references: • [Eurocontrol strategy] • [HFC] Additional reading: • [Barbarino01], [Barbarino02]
Alternate names:	Human Factors Integration in the development of new systems
Primary objective:	The Human Factors Case approach has been developed to provide a comprehensive and integrated approach that the human factors aspects are taken into account in order to ensure that the system can safely deliver desired performance. A Human Factors Case is a framework for human factors integration, similar to a Safety Case for Safety Management. EATMP will apply human factors expertise, methods, tools and products to concept formulation, design, implementation and operation of projects, in order to provide a regulatory framework for human factors integration through the application of mandatory EATMP human factors cases. [Eurocontrol strategy]
Description:	The Human Factors Case is designed to be simple, practical and effective, with four key stages: • Stage 1 – Fact Finding and Human Factors Issue Analysis (HFIA). Recording of factual information about the project background, system and system environment, as well as key stakeholders and documentation. Identification of the project-specific human factors issues at the early, middle and late phases of the project lifecycle, as well as the importance and urgency with which these issues need to be addressed, the safeguards and arrangements already in place and a description of the further actions required to address the issues in a suitable and sufficient manner. • Stage 2 – Human Factors Integration. Integration of human factors approaches to optimise system performance, and assessment of the human factors work carried out within the project to demonstrate that the main human factors issues have been addressed adequately. Statements of key conclusions from human factors studies with references to the relevant sources of evidence so that they can be challenged if it emerges that they are critical to the outcome. • Stage 3 – Monitoring. Description of the monitoring arrangements (planned or implemented) for the operational phase of the project in order to provide feedback on the performance of the system with respect to the human factors issues identified within the human factors case. • Stage 4 – Human Factors Case Assessment. Independent assessment of the Human Factors Case. The approach utilises team-based issue identification and analysis, and assists in integrating Human Factors by suggesting methods and tools that can be used within a 'ladder' approach, where different levels of human factors integration are stipulated to help plan the required human factors activities and record the key conclusions. Six 'Human Factors Issues' underlie the whole approach to help identify, assess, and monitor issues relevant to a project: • Human-Computer Interaction. • Organization and Staffing. • Team work and Communication. • Training and Development. • Procedures, Roles and Responsibilities. • Recovery from Failure.
Applicability range:	A Human Factors Case should be prepared for all: • Bespoke systems – new, tailor-made systems.

	• Commercially available systems – "Commercial Off The Shelf" (COTS) systems and products.
	• Systems implemented elsewhere – main emphasis on local implementation issues.
	• Modified systems that are:
	  • extended by new system level functionality.
	  • changed to have a new or modified fit, including technology updates.
	  • proposed for a change of role or operational use, which was not envisaged in the previous Human Factors Case, even where there is to be no change in system configuration.

Life cycle stage:	The Human Factors Case should be initiated at the earliest possible stage in the Project or Program so that human factors issues are identified and dealt with while opportunities exist to resolve them satisfactorily. The Human Factors Case Guidance divides the EATMP Phases into three summary phases: • Early: Initiation, Planning and Feasibility • Middle: Development and Pre-operational • Late: Implementation, Local Implementation and Operations
Experience in application to air traffic:	1. 2002-2003: First application was in the feasibility study for Airborne Traffic Situational Awareness (ATSAW). The purpose of the ATSAW Service is to provide the Aircrew with an improved awareness of the surrounding traffic situation. By improving such awareness, the ATSAW Service is expected to contribute to the strategic objectives of the Target concept contained in the EATMP Operational Concept Document and the ATM 2000+ Strategy. 2. 2002: A Human Factor Issue Analysis has been performed for a phraseology issue for the safety group of the EUROCONTROL MUAC (Maastricht Upper Area Center).
Related methods:	Link to Ergonomics Checklists, Interface Surveys. Safety Case: A Human Factors Case has a different focus to a Safety Case. The Human Factors Case is more focused on performance optimisation - augmenting human strengths and compensating for human limitations to improve total system performance. However, the Human Factors Case may also highlight some new safety-relevant issues, provide more detail or identify better control measures, via a more detailed examination of human factors issues such as 'human error' human recovery from system failures, reduce the potential for fatigue problems, workload problems, etc. Such issues will normally be addressed at some level in a safety case. However, other important human factors issues are often not addressed at all in a Safety Case. These include workstation ergonomics, Human-Machine Interface (HMI) usability, trust in and acceptance of in the system, longer-term planning and staffing, skill changes. Quality Management: Project Risk Management enables the management of risk as an integrated part of project management through all project phases. With increasing project complexity, tighter schedules, demanding budget constraints and the need to comprehend an escalating volume of information, it becomes increasingly difficult to maintain focus and stay in continuous control of a project. Traditional project management techniques often fail to address the uncertainty in the decision-making processes. This leads to a reactive approach to risk management, where 'fire-fighting' becomes the norm. Risk-based Project Management: Risk-based project management provides a more transparent and structured approach to understand, communicate and manage project risk. Proactive risk management provides continuous focus on the most important threats and opportunities, allowing the project to make more informed decisions, seize opportunities and avoid pitfalls, thus increasing the chance of project success. Insights can be gained from such approaches, which help to predict and manage threats and opportunities. However, they will not necessarily ensure

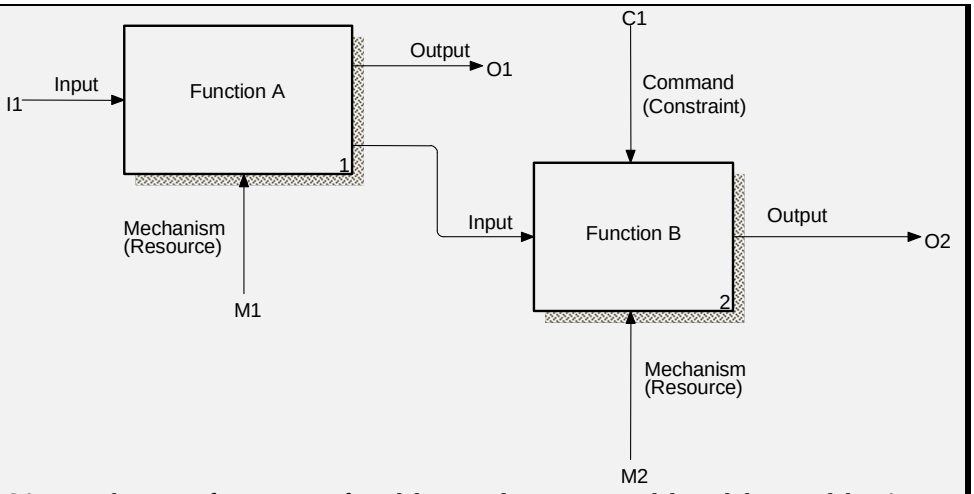
	that the pertinent HF issues are addressed.
Availability and tool support:	The first draft of Human Factors Case Guidance Material is available from April 2003. The guidance is available in document format with support from a Web-based tool. See www.eurocontrol.int/eatmp/hifa
Maturity:	Human Factors Case was recently (2002-2003) developed by EATMP HUM (EUROCONTROL).
Acceptability:	In due course, Human Factors Cases will be mandatory by EATMP. First applications in the ATSAW project and the MUAC phraseology issue have shown high acceptability by all parties involved.
Ease of integration:	The overall approach of the Human Factors Case aims to be simple, practical, and effective. Human Factors is a broad discipline, which considers many other factors that influence human- and system performance, such as job or role, procedures and task design, team issues, human-machine interface design. In addition, the impact of human resources practices are also incorporated, such as selection, training, planning and staffing, competency checking and licensing.
Documentability:	The Human Factors Case offers all techniques, tools and templates to gather and input all information required, hence careful documentation of all four phases of the Human Factors Case for comprehensive human factors integration.
Relevance to ATM:	The Human Factors Case proposes a standardised and straightforward process to enable Project Managers to 'make a case for human factors'. The Human Factors Case has three key functions. First, it helps to confirm and support the realisation of intended system performance objectives and criteria. In this sense, the Human Factors Case offers predicted performance assurance, which may be in terms of increased landing rate, sector flow throughput, improved conflict resolution, etc. Second, it helps to guide and manage the human factors aspects in the design cycle so that negative aspects do not arise and prevent the system reaching its performance level. Third, it helps to identify and evaluate any additional detailed human factors safety aspects not already found in the safety case. A unique aspect of the Human Factors Case is that it prompts attention at the earliest possible stage of the project lifecycle to planning, training and staffing issues, to help ensure that competencies and resources are available for the timely implementation of new systems.
Con's and resources:	The Human Factors Case requires time and facilitation skills. A variety of personnel or system users may be considered, these include ATCos, engineers and maintenance personnel, control and monitoring personnel, trainers, supervisors, management and support personnel. A Human Factors Case should consider anyone who is affected by system changes and whose performance contributes to the total system performance. Key roles identified: 1. Project Manager 2. Human Factors Coach 3. Facilitator 4. Human Factors Case Key Stakeholder Team 5. Independent Human Factors Assessor The application of human factors methods is a key part of the system design, evaluation, and timely implementation, but the process can be complex and difficult to understand.

21. PDARS (Performance Data Analysis & Reporting System)

References used:	[Braven&Schade03]
Alternate names:	GRADE (Graphical Airspace Design Environment)
Primary objective:	Provide Performance Measurement Metrics for the Federal Aviation Administration (FAA) at the national, as well as field level (individual en route and terminal facilities)
Description:	The FAA and NASA are jointly sponsoring a program to develop PDARS, the objective of which is to collect and process operational data (including aircraft tracks) and provide information to the users relevant to the air traffic system performance on a daily basis.
Process steps:	'Tap clients' are maintained at each facility site to continuously collect selective radar data, the data is processed and daily reports are generated, daily data is then sent to a central site for storage where the user can retrieve historical data, as well as conduct trend analyses.
Applicability range:	Primary focus is on procedures/organization and provides a variety of text and graphical outputs for use in analyses or a wide variety of user-specified graphics.`
Life cycle stage:	PDARS involves an iterative process with the first step being definition, followed by design and then implementation. Based on feedback and the dynamic nature of air traffic operations this process is repeated with accompanying maintenance.
Experience in application to air traffic:	Ultimate development of PDARS has evolved from experience in applications, including: accident/incident investigation, airport/airspace design, visualization of complex traffic operations, flight path/profile analysis, traffic flow/sector loading analysis, operational performance assessment, environmental assessment and public relations.
Related methods:	Radar data can be processed from en route SAR tapes, terminal optical discs, and oceanic DOTS data to provide the same aircraft tracking information available through the site-specific tap clients installed at the ARTCCs and TRACONs.
Availability and tool support:	PDARS will soon be installed and operational at all the en route centers in the contiguous U.S. All facilities with PDARS installation are monitored daily and problems addressed immediately. Processing and tool software are updated periodically and retraining is provided to the users as needed. Contractor support via telephone is also available to assist and correct any problems encountered.
Maturity:	PDARS has evolved from the prototype stage to being implemented nationwide. PDARS Quarterly Users' meetings have provided technical guidance to maturing the system and numerous useful applications have been presented by the attendees.
Acceptability:	PDARS has been fully accepted in all facilities where it has been installed. PDARS has been adopted as the measuring tool to evaluate the transition to RVSM in the US. Numeric accuracy is well within the FAA standards for traffic operations analysis and provides the most accurate measurement tool available to the FAA to date.
Ease of integration:	PDARS provides data that can be easily included in other techniques. PDARS reports can be formatted to match requirements of other techniques. Essential PDARS skills are taught in a three-day hands-on training class. No advanced statistics are required.
Documentability:	PDARS supports it user with a suit of documentation manuals which include: the File Manager Analyst and Operations Guide, a current version of the Training Workbook, the Quick-Start Guide, the User's Manual, and the PDARS Deployment Notes (assist in the deployment of hardware at the site locations.
Advantages:	PDARS is extremely versatile. It can analyze operations of a single flight, operations within one airspace volume, facility, airport, or larger airspace system. It can look at single days or multiple days, limited only by the available data. PDARS has many applications for ATM safety assurance, including airspace optimization, incident analysis, impact analysis of temporary airspace modifications, etc. Visualization tools in PDARS are extremely suitable to support qualitative analysis. PDARS does not require any set level of data, provides results with little available data and better results for large data sets.
Disadvantages:	PDARS does not integrate airborne data or ATC flight plan and ATC instructions data.

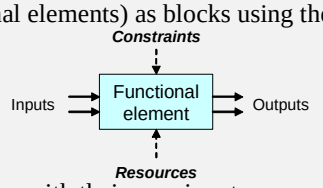
22. SADT (Structured Analysis and Design Technique)

References used:	Perrin, and Spouge. (2004) 2004 Baseline Integrated Risk Picture for Air Traffic Management in Europe Perrin, and Damidau. (2004) ATM SADT model at the horizon 2012 Hale, A.R., Heming, B., Carthey, J. and Kirwan, B. (1997) Problem solving cycle model and safety culture. Safety Science, 26, 121 -140. Hale, A.R. , Kirwan, B., Guldenmund, F., and Heming, B. (1998) Capturing the river: multi-level modelling of safety management. In Misumi, J., Wilpert, B., and Miller, R. (1998) Nuclear Safety - a Human Factors Perspective. London: Taylor and Francis, pp. 161 - 182. Marca, D.A. and C.M. McGowan. (1988) SADT Structured Analysis and Design Technique.
Alternate names:	Top-down modular and hierarchical functional decomposition (System Functional Model)
Primary objective:	SADT™ is a technique that is useful for system planning, requirements analysis and system design. It was developed to provide a rigorous, disciplined approach to achieve understanding of user needs prior to providing a design solution. It is generally used in the planning, analysis and general design phases for software module, although other techniques are used to specific program design since the constructs necessary for program design of sequence and interaction are not found within SADT. The usefulness of SADT modeling technique to support ATM safety assessments is to use the ATM model as a preliminary identification of the causes of accidents, for use in a risk model. Accidents are considered to arise from a failure of one or more activities to deliver their intended outputs.
Process steps:	1) Define Top-Level Functions (from Inputs) 2) Organize Functions Into Logical Relationships 3) Decompose Higher-Level Functions Into Lower-Level Functions 4) Evaluate Alternative Decompositions 5) Document Functional Analysis Baseline 6) Relate SADT model to risk model (this step is added on top of the 'normal SADT process)
Description:	Step 1 serves as an input to Step 2. Here the functions include the central functions required for the system to accomplish its mission as specified by the concept of operations (e.g. EUROCONTROL OCD). In Step 3, higher-level functions are decomposed into sub-functions with specificity increasing at each level of decomposition. Basically, the decomposition of a system is a top-down approach to problem-solving. Shown graphically (below), the decomposition is taken to a level at which the functions have been totally decomposed into basic sub-functions and each sub-function at the lowest level is completely, simply, and uniquely defined by its own set Requirements. This means that functional decomposition continues as long as there is a further need to define lower-level Requirements. When the requirements development process ceases, the SADT modeling may cease.



SADT makes use of two types of models, namely activity models and data models. A SADT activity model describes the decomposition of activities. A SADT data model describes the decomposition of data.

The SADT activity model represents activities (or functional elements) as blocks using the following notation:



- Outputs from the activity - shown to the right.
- Inputs required – shown to the left.
- Necessary resources – shown from below.
- Constraints limiting the activity – shown from above.

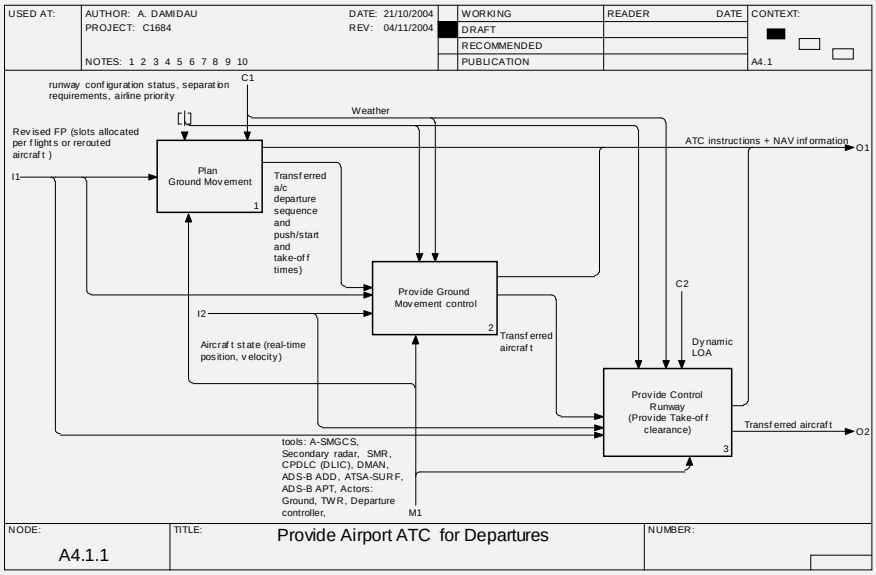
Each activity may be decomposed into component activities, with their own inputs, outputs, resources and constraints.

An inadequate output may result from either:

- Inadequate inputs or a failure of the activity to compensate for this.
- Inadequate performance of the activity by the specified resources, under the influence of relevant constraints.
- Inputs are specific flows of information required for the activity. Inadequacies in these information flows will prevent the activity functioning as intended (although it may function in a degraded state). They will appear explicitly as failure events in the risk model. For example, the surveillance picture is an input to ATC, and output in the form of inadequate ATC instructions may result from an inadequate surveillance picture.
- Constraints are conditions that can influence the activity or its effectiveness (defined as the probability of the output being adequate). Constraints do not immediately prevent the activity functioning as intended, but may erode safety margins (sometimes described as “latent” faults). The SADT model attempt to identify the major topic areas within which such faults may occur.
- Resources are the people or systems required to perform the activity. They will appear as actors in a risk model. Inadequacies in their performance are in effect another type of constraint, influencing the effectiveness of the activity.

In Step 4, alternative decompositions of functions (Functional Architectures) and Requirements at all levels are evaluated. These evaluations are necessary since there is no single “correct” decomposition; however not all decompositions are of equal merit. It is necessary to evaluate alternative decompositions in order to select the decomposition best suited to support the forthcoming risk modeling.

A detailed SADT diagram for airport ATC departure service provision is provided below:

	 Step 5 is documenting the process with the hierarchy of SADT models, assumptions made and rationale behind the functions decomposition. Step 6 is to create a transparent link between the SADT-based ATM model and the risk model. The approach to this is briefly considered as follows: In general, a risk model can be formed from a functional model by turning each element into a corresponding failure, which can usually be achieved by a prefix such as “inadequate”, “ineffective” or “inappropriate”. All aircraft accidents can be loosely considered to result from an “inappropriate flight trajectory”. Working backwards through the SADT model, the causes of this can be seen as “ineffective avoidance action”, “inadequate flight management” etc. Each of these may be the result of either: ▪ Inadequate inputs, such as ATC instructions, flight plans, position information etc. The causes of these may also be traced back through the SADT model to their own inputs. Further decomposition of the SADT model will give a more detailed breakdown of these causal factors. ▪ Inadequate performance of the resources under relevant constraints. For example, this might be poor flight crew performance in combination with adverse weather, poor aircraft ergonomics etc. Inadequate performance in an activity is not usually a simple result of inadequacies in the information received, but is more commonly the second type of cause above, resulting from inadequacies in the processing of the available information. This occurs “within the box” of each activity in the SADT model. A human operator may fail to identify the critical information among a large quantity of less important alarms and indications, or fail to make proper use of the information. An automated system may also make incorrect decisions, due to inadequacies in design, maintenance or operation. These errors originating within an activity can be represented as failures of the resources or constraints within the SADT model. Hence developing a systematic analysis of the resources and constraints may be as important as tracing the inputs to each functional block.
Applicability range:	This technique is applied to the functional modeling that is needed to identify specific information flows between the main actors and systems involved in ATM, so that interdependencies can be identified and so that it is clear whether or not they are represented in the risk model. The model is necessarily a simplified representation of the complex reality.
Life cycle stage:	Technique can be required as early as the scope and modeling phase of the life cycle.
Experience in application to air	This technique has been extensively applied to the functional specifications and design of ATM systems in the industry; specifically ATM/CNS systems and services. This

traffic:	technique is being applied to the Integrated Risk Picture to support gate-to-gate risk assessment.
Related methods:	Petri Net modeling techniques are also used for the safety modeling of complex safety critical systems and operations (e.g. by TOPAZ)
Availability and tool support:	This technique has been available since early 80's and different computer programming tools can be purchased (e.g. BPWin/IDEF0 tool commercialized by Computer Associates) to support the SADT-modeling.
Maturity:	- SADT™ is mature (more than 20 years application to support design activities) in its development and has been widely used in industry (not only aeronautics) in particular supporting software engineering. - Application of the SADT modeling to support risk modeling and subsequent safety assessment is on the other hand fairly new and is being demonstrated.
Acceptability:	- SADT™ use to describe complex systems and control the development of complex software is widely accepted. - To support risk modeling and more generally safety assessment, this technique is currently in evaluation for acceptability in the EUROCONTROL Safety Assessment Methodology (SAM) and SAND (Safety Assessment for New Designs) processes. To date, results are under review and appear reasonable.
Ease of integration:	The technique and underlying logic is easy to understand. However, recommend as a minimum, practitioners take formal training.
Documentability:	High.
Advantages:	The SADT modeling technique enables to form a complete, albeit very simplified, model of ATM. It identifies the main activities, actors and information flows in ATM at present, and provides a suitable framework for representing the changes in these in the future. The model could be broken down to provide a more detailed description of ATM. An important aspect of the SADT model is that it highlights interdependencies between functional blocks, so that it is clear whether these are represented in the risk model. One type of interdependency may be common origins of apparently independent information that is input to an activity. The SADT model allows these common sources to be identified. Another type of interdependency may be common resources or constraints between different elements of the SADT model.
Disadvantages:	▪ Applied to wide system (e.g. ATM overall model and layers), the SADT model may get very large and complex. ▪ The selection of inputs, outputs, resources and constraints is to some extent arbitrary. For example, most real activities make use of inputs ranging from always essential to occasionally useful. Similarly, there are innumerable constraints ranging from the obvious to the indistinct. The models presented here make a preliminary identification of the key inputs, outputs, resources and constraints. More systematic treatment may result from hazard identification exercises and the risk modeling, and hence an iterative approach to SADT model development is desirable. ▪ Temporal relationships are not always clear - When are inputs produced? - When are outputs produced? - When do boxes perform actions? (sequentially, concurrently throughout, partially overlapping)

23. SAFSIM Template

SAFSIM	
References used:	• 'Interim SAFSIM Guidance' that is about to go on our website which can be referenced as Kermarquer, Y. and Antonini, A. 2004, Interim SAFSIM Guidance, Eurocontrol with the wesite address. http://www.eurocontrol.int/eec • Scaife, R., Fearnside, P., Shorrock, S.T., and Kirwan, B. (2000) Reduction of separation minima outside controlled airspace. Aviation Safety Management conference, Copthorne Tara Hotel, London, 22-23 May. • Rachael Gordon[1], Steven T. Shorrock[2], Simone Pozzi[3], Alessandro Boschiero[4] (2004) Using human error analysis to help to focus safety analysis in ATM simulations: ASAS Separation. Paper presented at the Human Factors and Ergonomics Society 2004 Conference, Cairns, Australia, 22nd - 25th August, 2004. • Shorrock, S. Kirwan, B. and Smith, E. (2005: in press) Performance Prediction in Air Traffic Management: Applying Human Error Analysis Approaches to New Concepts. In Kirwan, B., Rodgers, M., and Schaefer, D. (Eds) Human Factors Impacts in Air Traffic Management. Ashgate, Aldershot, UK • Adrian Gizdavu; EEC Report N°374/2000, Spata 2000 R eal-time Simulation http://www.eurocontrol.int/eec/publications/eecreports/2002/374.htm
Alternate names:	Safety Measures for Real Time (Human-in-the-Loop) Simulations
Primary objective:	To take measures during real-time human-in-the-loop simulations to derive safety insights
Description:	SAFSIM is a process and a toolbox of measures. The process involves either the measurement of the safety of controller performance when faced with specific safety safety-related events (e.g. hazards) in a simulation, or else general safety monitoring using less intrusive procedures to see if any safety-relevant information arises during a real time simulation.
Process steps:	1. Determine whether there are specific safety objectives for a simulation – these may arise from a hazard analysis (e.g. particular hazards that are of concern and may be seen during a simulation) or from other sources (e.g. review of operational incident data or controllers' opinion about pertinent safety issues). 2. If there are specific safety-related events of interest for the simulation these must be related to the simulation environment and objectives, to see how they can be integrated into the overall simulation plan and its execution. This will lead to the definition of specific safety events or scenarios that must occur during the simulation in a planned and measurable fashion. Examples of such events could be failure or 'bad data' resulting from a proposed controller tool, or adverse weather events, or pilot error. If there are no specific safety events of interest then a standard set of general measures can be applied to the simulation (see [3] below). 3. Measures must be chosen for the simulation that will allow safety conclusions or at least insights to be drawn. General measures include automatic monitoring of reductions in standard ATM-relevant safety criteria (e.g. losses of separation; runway incursions; ACAS/TCAS activation, etc.) via automatic event logging systems or more specialized safety monitoring systems. Such approaches may also be facilitated by controller self-report and simulation observer report. Standard debriefs and questionnaires after each exercise and at the end of the simulation should also include general safety questions. For more safety-related-event oriented simulations, e.g. considering the potential impacts of a hazard on

situation awareness, workload or teamwork, more specific measurements will be used (see Table below). For all measures, it must be decided how the measure will be administered, the expected direction of the effect, and how to analyze the measure, and the safety criterion (qualitative or quantitative) from which to judge the extent of the impact. In a number of cases this will include the need for a severity classification scheme (e.g. for losses of separation), but in other cases may be more subjective or interpretative by the simulation 'experimenters' e.g. interpretations of workload or situation awareness impacts.

4. The simulation is then run. For general safety measurement, there may be a need for debrief and clarification sessions with the controller subjects. For more focused measures these debrief sessions (with single controllers or multiple controllers) may be expected to be more intensive. Some measures (e.g. situation awareness or physiological measures) may also be more 'intrusive' in that they may actually require a short temporary interruption of the simulation itself whilst key questions or measurements are taken, or in the case of psycho-physiological measurements (e.g. heart rate, eye movement tracking, electro-dermal activity, etc.) the measures may not actually interrupt the simulation but the controller will be required to wear monitoring equipment. In all such cases the impacts of the measurements and measurement methods themselves on behavior must be assessed to determine how they affect the validity of results on safety and other simulation objectives.
5. Analysis and determination of safety insights then occurs. In simulations exploring reactions to safety-related events, this should usually lead to a conclusion that safety *as evidenced in the simulation* was either enhanced, degraded, no change occurred, or the measure/simulation/scenario was insufficiently sensitive to the intended safety aspect being investigated, or finally that the observed change was an artifact from the measure itself (and therefore may not appear in a real situation). Interpreting such safety insights or evidence requires careful interpretation however. Firstly, for hazards that are 'fed into' the simulation, these will often have a far higher occurrence rate in the simulation than in reality – therefore the controller reactions may differ from reality, particularly when considering rare hazards or events. Secondly, in terms of errors or events that 'arise' during a simulation (i.e. they were not pre-planned into the simulation), it must be remembered that these safety-related events may sometimes occur more easily in simulations than in reality, due to lack of familiarity of controllers with the simulation and scenarios (e.g. HMI, new concept and airspace unfamiliarity), and also simply because it is 'just a simulation' and so controllers may act less safely than when handling real traffic in the controllers' normal working environment. This does not mean that observed events (e.g. controller errors) are artificial, but rather the 'rate' may be significantly higher than in normal activities. As an important counterpoint to this potential 'bias' however, if an event predicted as possible (e.g. a human error) does not appear during a simulation, it does not mean it will never appear in reality. A typical simulation may last two weeks with thirty controllers facing five exercises per day. Whilst this is always a substantial test of a system, in safety and risk terms it will not be a reliable measure of rare events (e.g. less than one in a thousand in terms of anticipated likelihood). Care is therefore needed in drawing conclusions from simulations to inform project safety case conclusions. Real time simulations can provide important insights for safety cases, but will not always be definitive. This is why the project was called 'Safety insights in simulations' – because a simulation can rarely be exhaustive due to practical limitations (simulation costs and availability of controllers), and so it is insufficient as a means to judge safety conclusively when considering rare events. Nevertheless, the controller reactions and experiences associated with such simulations can lead to important insights about safety of the concept being simulated, and associated errors and failure-recovery paths. These experiences

can still inform the safety of a project or system, and lead to the derivation of safety requirements, as well as training and procedural improvements.

6. Safety insights are fed into the project safety documentation.

Table – Typical Measures for Gaining insights from Real Time Simulations

Event Logging (automatic recording)	Safety-related measures & techniques	Human Factors-related measures	Psycho-physiological measures
Loss of standard separation	'Seeding' hazards and safety-related scenarios into simulations	Workload (various measures such as NASA-TLX; ISA; SWAT; etc.	**Heart Rate Variability**
Automatic Safety Monitoring Tool (ASMT) – measures various safety-related parameters	Severity classification schemes	Situation Awareness (e.g. SASHA; SAGAT)	**Eye movement tracking and pupil diameter measurement**
Safety net activations (e.g. ACAS/TCAS; short-term conflict alert occurrence; other)	Time to recover from hazards	Teamwork impacts (various – see SAFSIM manual)	**Electro-dermal activity**
Video recording; radar screen and strips recording; voice recording; other event logging	Subjective questions and debriefs on perceived safety impacts	Skill degradation (SHAPE toolkit)	**Brainwave measures (e.g. P300)**
Time (for various measures – e.g. time to detect or respond to events)	HERA – Human Error in ATM – used to classify and understand human error events	Trust (e.g. in automation or fellow controllers – SHAPE toolkit)	
Communications and communications time	**TRACER – used to predict possible errors that can then be observed in the RTS**	**Usability metrics (for HMI aspects – see SAFSIM Manual)**	

Applicability range:

Real time simulations are a flexible approach, able to address airspace design, new automation tools and concepts, controller working methods and Human-Machine Interface (HMI) design for example. Real time simulations are also particularly useful in examining impacts on controller performance. Real time simulations are less used for software and hardware evaluation, because firstly other methods are available and more efficient, and also simulation 'platforms' are themselves usually a simplified abstraction of the real system, so can only test hardware and software aspects in principle or functionally. Nevertheless, they are good overall tests of a system, able to find problems in the intended system architecture and implementation. For this reason often large-scale tests may be carried out on site, in a simulation facility at or adjacent to an air traffic control centre. If a system is tested in the center itself, this constitutes either a 'shadow-mode trial' (controllers using the system are not in control but are 'following' live traffic), or else it can be an actual 'live trial' in which the new system is actively used to control/monitor traffic. In both of these cases, there must be an assessment of the safety of the trial itself, so that the trial cannot induce actual incidents or reduce the real system's ability to respond to actual incidents during or after the trial (this can be done using a HAZOP of the live trial itself – called 'Live Trial HAZOP' – see HAZOP in the toolbox).

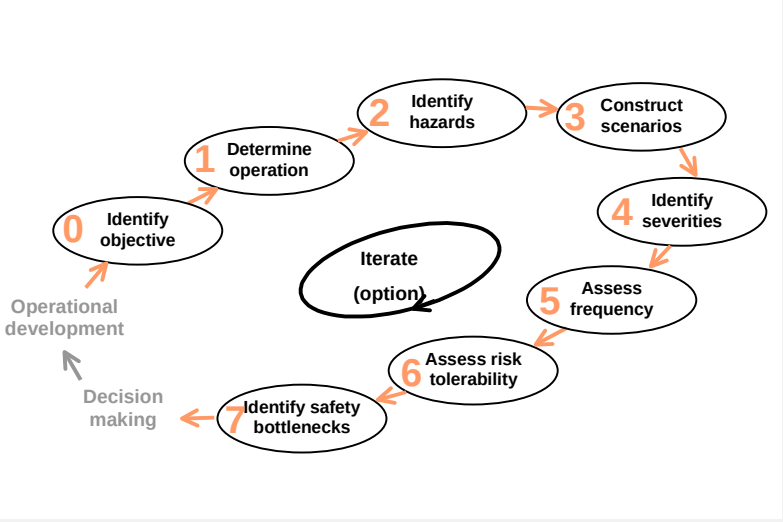
Life cycle stage:	Usually real-time simulations occur mid-way until late in the concept development life cycle (i.e. a detailed stage of design at which at least provisional controller procedures and working methods have been developed, and at least a preliminary working HMI exists). However, a real time simulation can be used with a preliminary platform to explore the concept more fully – such simulations even if operating in real time, may be called prototyping simulations. Simulations can also occur until Implementation and Operation stages of the life cycle, and for operational systems about to receive an airspace design stage, new controller tool, new procedures, etc.
Experience in application to air traffic:	The general approach of gaining safety insights from simulations has been in existence since ATM real time simulations began several decades ago, since many simulations have looked for and/or found safety insights. In this sense SAFSIM is mainly a collection of good practices and an attempt to render the approach more explicit and structured. .Some explicit applications have occurred however. For example, [Scaife, 00] used two military simulations to contribute to the determination of whether it was safe to reduce vertical and lateral separation to aircraft receiving a Radar Advisory Service in the Open Flight Information Region in the UK. The simulation measures of losses of separation, situation awareness, workload, and subjective measures led to the conclusion that vertical reduction of minimum separation was safe whilst lateral reduction was not. A more recent example [Gordon, 04] is the work supporting exploration of the Mediterranean Free Flight (MFF) concept. This work examined a number of hazards from a safety case (an Operational Hazard Analysis) during the simulation, to see how controllers would handle the hazards, and if other hazards might arise. Interestingly, the simulation identified a new hazard not originally considered in the simulation itself nor the Operational Hazard Assessment. Other examples include work in UK NATS (National Air Traffic Services) in the '90s evaluating a range of future tools for ATM and using human error identification associated with simulations [Shorrock, 05], leading to insights on hazards, human errors and how to improve recovery from errors with the HMI. A fourth example concerns the simulation [Gizdayu, 00] at Eurocontrol Experimental Centre of the planned airspace for the Athens Olympic Games, during which a hazardous situation was identified – the information was reported and forwarded to the relevant authorities. This simulation is of interest because this was an example of a general insight from a real time simulation.
Related methods:	Several techniques are related in the toolkit. These techniques can either help to identify scenarios or hazards or issues that should become safety objectives in the simulation (External Events Analysis, Common Cause Analysis, Fault Tree Analysis, FMEA, Event Tree Analysis, HAZOP, Human Factors Case, TRACER), or else simulations can help to generate or corroborate data for certain techniques (e.g. Reliability Databases, Human Error Data, Future Flight Central), or else the outputs in terms of safety insights or conclusions can feed into them directly (Hazard Tracking systems).
Availability and tool support:	The techniques listed in the SAFSIM manual and referred to in the table above are publicly available. However, there is not an integrated SAFSIM approach – SAFSIM is in effect a separate toolbox for safety investigation in simulations. Many of the tools do not require sophisticated analysis (e.g. observations and questionnaire/interview measurements, though time-consuming and requiring data representation and storage, can usually be applied with the support of conventional office-based tools). Automatic logging depends on the simulation set-up, and ASMT must be acquired through Eurocontrol for safety-related experimental purposes. Eye Movement Tracking and other psycho-physiological measurement methods are very specialized requiring specific equipment, analysis support software, and training in their usage. There are a number of such suppliers available.
Maturity:	Whilst the principle of investigating safety in real time simulations has been in existence for some time, the formal measurement of explicit safety objectives and their direct linkage to safety case conclusions has been less common. Nevertheless the approach has been used and is not overly complex. Additionally the approach is coherent with the idea and practice of Validation (an often-stated objective of a simulation), in that since all future concepts are supposed to at least maintain the target level of safety, such safety

	should therefore be explicitly measured where possible. The sub-approaches themselves listed above in the table are variable in their maturity, but all have been applied in various simulations (with the possible exception of the teamwork measure). Some of the measures require domain expertise (e.g. Human Factors or Psycho-physiology expertise).
Acceptability:	Developers of the SAFSIM manual have attended workshops and visited simulation laboratories to develop the SAFSIM guide on best practice for safety investigation in simulations. There has however been no formal evaluation of the guidance.
Ease of integration:	The aim of SAFSIM is twofold: first, to inform the project that is the subject of simulation (e.g. a new controller tool), so that the project team understand the safety issues. The second aim is to inform the safety case. Whilst this has happened in a few cases (e.g. the vertical separation reduction case cited above), the exact ways in which simulations can inform safety cases have not been fully explored. This is at least in part because simulations themselves vary so much in their nature and objectives. It is hoped that as formal safety investigations in simulations progress, a comprehensive set of formal relationships will be established. SAFSIM has been developed for real-time simulations of Air Traffic Control, but can be linked with cockpit simulators, e.g. to study handing over of separation responsibility to aircraft. Some examples of this approach of coupling ground and air simulations have occurred in the ATM world in Europe and the US.
Documentability:	Simulation documentability varies but is often extensive. This means that safety-related measures will similarly be exhaustively documented. Information on safety issues should be stored in project safety documentation via Hazard Tracking & Resolution Systems.
Advantages:	• Real time simulations represent a relatively realistic environment in which to test safety of a system that is nearly real, but with no actual risk. • The results from a real time simulation usually have a relatively high degree of authority, due to the realism and the use of real valid controllers in such simulations. • Although controlled and planned in great detail, real time simulations are a sufficiently rich environment that they can allow the emergence of realistic new errors or hazards that were not previously predicted.
Disadvantages:	• Whilst the controllers are real controllers in a realistic environment, the pilot representation is less realistic in most real time simulations, using 'pseudo-pilots' who are sometimes actual pilots but sometimes not, who follow a script and sit in an adjacent room acting as one or more pilots for the controllers.

24. SIMMOD Pro

SIMMOD Pro	
References used:	Simmod *PRO!* Reference Manual
Alternate names:	None.
Primary objective:	Used for conducting high-fidelity fast-time simulations of current and proposed airport and airspace operations.
Description:	The Airport and Airspace Simulation Model, SIMMOD, is an FAA-validated model used by airport planners and operators, airlines and air traffic authorities. Simmod *PRO!* adds advanced modeling capabilities, incorporating rules-based dynamic decision making. The rules-based decision making can be used to model complex interactions between ATM systems, disruptive events and human resources and activities (e.g., controllers, pilots, etc.)
Process steps:	Appropriate data needs to be obtained that covers the scope of the analysis. Airport based studies would require airfield layouts, flight schedules, ground operating procedures, runway operating procedures and at least a limited amount of airspace. This data is input to the model and a period of activity is simulated. Using the tools reporting capability, various operating statistics can be generated including an animation replay of the simulated traffic.
Applicability range:	Primary focus is on procedures/organizations and provides a variety of text and graphical outputs for use in analyses.
Life cycle stage:	Simmod *PRO!* can be utilized in several stages of the life cycles. It can be used as a tool to help define the scope of the study; during the design of the solution; how best to implement the design; and how to optimize the impacted operations.
Experience in application to air traffic:	SIMMOD was one of the first computer simulation applications for analyzing air traffic management. Simmod *PRO!* has been used extensively for numerous airport and airspace analysis applications, including runway incursions.
Related methods:	Simmod *PRO!* provides quantitative results. PDARS data can be used to develop the airspace structure and inputs to a Simmod *PRO!* simulation model. Once the analysis has been completed and the changes incorporated into the air traffic system, PDARS can again be used to assess the benefits and compare actual to predicted results.
Availability and tool support:	Until recently, Simmod *PRO!* was an ATAC Corporation proprietary tool. It is now available to be licensed for general use through ATAC.
Maturity:	SIMMOD has been in use since the mid-80s and has undergone an extensive validation process by the FAA. Simmod *PRO!* was developed in 1999 and has been used extensively since that time in both civilian and military applications. SIMMOD is continually being enhanced based on feedback from clients and user groups.
Acceptability:	SIMMOD went through an exhaustive validation by the FAA in the 80s. Clients continue to rely on it to provide defensible, quantitative results of new operational concepts and procedures.
Ease of integration:	Simmod *PRO!* can be used to develop simple models of basic airports to complex, multi-airport systems that involve probabilistic decisions, disruptive events, human resources and advance operating concepts. The resulting output and statistics can easily be used by other software and methodologies for additional analysis..
Documentability:	Simmod *PRO!* has detailed documentation covering its methodologies and algorithms. The input database and output results allow for analysis transparency, validation, verification and repeatability.
Advantages:	Simmod *PRO!* can be used to simulate complex air traffic systems and scenarios, providing a method to capture the dynamics of operations that depend on the state of the system and probabilistic behavior of system elements.
Disadvantages:	Simmod *PRO!* requires a high level of expertise in ATM systems to effectively model these systems.

25. TOPAZ accident risk assessment methodology

References used:	Key references: • [Blom&al98,01], • [DeJong04] • [Everdij&Blom02] Other references: • [Air safety database], [Baren&al02], [Blom&al03a], [Blom&al03b], [Blom&al03c], [Blom&Corker&al03], [ESARR4], [Everdij&al02], [Everdij&Blom03], [JAR25.1309], [Klein Obbink & Scholte03], [Kos&al00/01], [Laughery&Corker, 1997], [Scholte&al04], [Stroeve&al03a], [TOPAZ hazard database]. Additional reading: • [Blom&Bakker93], [Blom&Daams&Nijhuis00], [Blom&Stroeve&Daams&Nijhuis01], [Blom&Stroeve&Everdij&Park02], [Daams&Blom&Nijhuis00], [DeJong&al01a], [DeJong&al01b], [DeJong&al03], [DeJong&al04], [ESARR2], [MUFTIS3.2-II], [Stroeve&al03b]
Alternate names:	Traffic Organization and Perturbation AnalyZer
Primary objective:	Scenario and Monte Carlo simulation-based accident risk assessment of an ATM operation, which addresses all types of safety issues, including organisational, environmental, human-related and other hazards, and any of their combinations.
Description:	An overview of the steps in a TOPAZ safety assessment is given in the figure below. During step 5 use is made of Monte Carlo-simulations for selected safety aspects.  In step 0 the objective of the study is determined, as well as the safety context, the scope and the level of detail of the assessment. The actual safety assessment starts by determining the operation that is assessed (step 1). Next, hazards associated with the operation are identified (step 2), and clustered into conflict scenarios (step 3). Using severity and frequency assessments (steps 4 and 5), the risk associated with each conflict scenario is classified (step 6). For each conflict scenario with a (possibly) unacceptable risk, safety bottlenecks are identified (step 7), which can help operational concept developers to find improvements for the operation. Should such an improvement be made, a new cycle of the safety assessment should be performed to investigate whether all risks have decreased to a negligible or tolerable level. ***Step 0: Identify objective*** Before starting the actual safety assessment, the objective and scope of the assessment are

set. This should be done in close co-operation with the stakeholder(s). Also, the safety context must be made clear, such that the assessment is performed in line with the safety management framework of the stakeholder(s).

Objective and scope
Generally, the objective of the safety assessment is to obtain an indication how safe the developed operation is, in order to decide about implementation of the operation, or redevelopment. The scope of the assessment concerns for instance the boundaries of the operation under consideration. These can be physical boundaries as well as boundaries of the procedures or systems under consideration.

Safety criteria
An important issue for the safety context is the choice of safety criteria with respect to which the assessment is performed. Example criteria are by ICAO, EUROCONTROL ([ESARR4]), JAA ([JAR25.1309]) or others (e.g. LVNL, DFS). Such criteria are defined for particular flight condition categories (this may vary from flight phases to detailed conflict scenarios and anything in between) and for particular severity categories (e.g. accident, serious incident). Typically, within the chosen context, these criteria define which flight condition / severity categories have to be evaluated and which frequency level forms the threshold between tolerable and unacceptable risk per flight condition / severity category. In line with ICAO terminology, we refer to such a threshold value as a TLS (Target Level of Safety).

Step 1: Determine operation

Step 1 just serves for the safety assessors to obtain a complete and concise overview of the operation, and to freeze this description during each safety assessment cycle.
Main input to step 1 is a description of the operation from concept developers, while the output is a sufficiently complete, structured, consistent and concise description of the operation considered. The operational context of the operation should be described in generic terms if possible in order to promote universality of application. On the other hand, the description should provide any particular operational assumption to be used in the safety assessment, and the description has to be verified by the operational concept experts/designer(s). Note that it is not part of the safety assessment to develop the operation; this is a task outside the scope of the assessment, which definitely should be performed by operational concept designers.

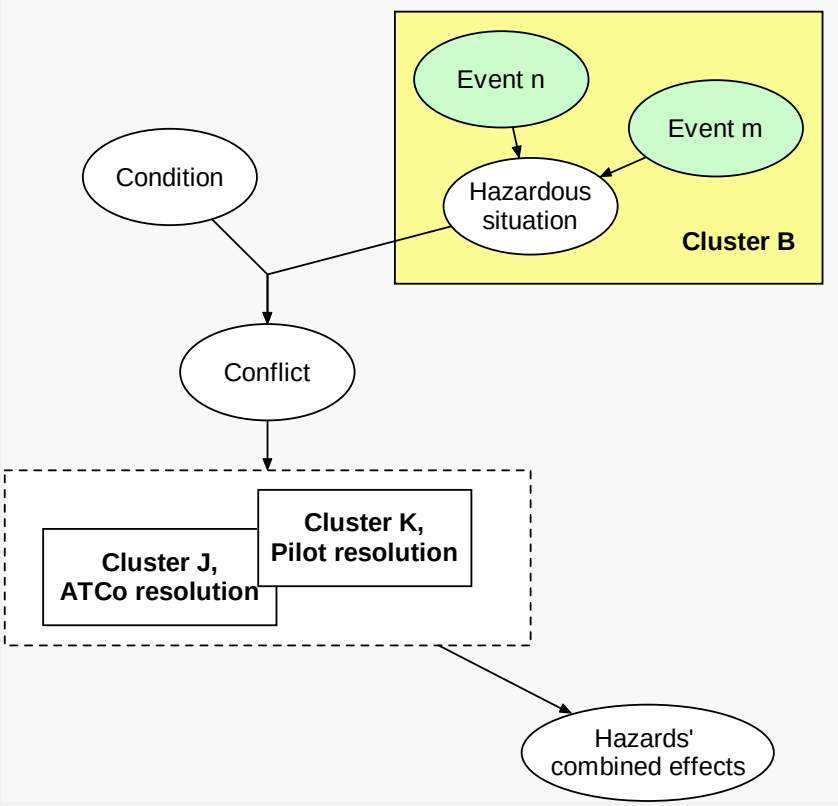
Important aspects that need to be covered in the operational concept description are:

- The *objective* of the operation and the *traffic flows* to be accommodated;
- The *operational context* of the operation, describing e.g. the geometry of the airport or the air route structure, the timeframe, and the traffic characteristics;
- The roles and responsibilities of the *humans* involved in the operation, especially air traffic controllers and pilots;
- The operational *procedures*, both from an ATC and from a pilot point of view; and
- The *technical systems* used in the operation. These systems are usually divided according to communication, navigation and surveillance functions. Questions like how the systems serve the human, what is their performance, and how are they used need to be answered.

Step 2: Identify hazards

Similar to [ESARR4] the term hazard is used in the wide sense; i.e. an event or situation with possibly harmful effects. Such a non-nominal event or situation may evolve into

	danger, or may hamper the resolution of the danger, possibly in combination with other hazards or under certain conditions. Goal of step 2 is to identify as diverse and many hazards as possible. Hazard identification brainstorming sessions are used as primary means to identify novel hazards. Necessary participants in these sessions are an air traffic controller, a pilot, a moderator, somebody taking notes, and preferably an expert on the operational concept. The participants should all have a sufficient level of understanding of the operation under consideration. The moderator should prepare by explaining the operation and by identifying some hazards to trigger the brainstorm when necessary, and by making an initial list of conflict types that should be covered. Emphasis is on shifting the boundary between imaginable and unimaginable hazards [DeJong04]. These hazard identification brainstorming sessions should be used to identify potential hazards only, and not to analyze them. Hazards seemingly unimportant during the brainstorming may turn out to be very important in the later steps, and may also trigger the identification of other hazards. Another important source is formed by hazards identified in previous studies on similar subjects. For this purpose, hazards identified in previous studies are maintained in [TOPAZ hazard database]. ***Step 3: Construct scenarios*** When the list of hazards is as complete as reasonably practicable, it is processed to deal with duplicate, overlapping, similar and ambiguously described hazards. First, per flight condition selected in Step 0, the relevant conflict types which may result from the hazards are to be identified using a full list of potential conflict types, such as for instance 'conflict between two aircraft merging onto one route' or 'aircraft encounters wake vortex of parallel departure'. Per flight condition, each conflict type is subsequently used as crystallization point upon which all applicable hazards and their combined effects are fitted. The output of such crystallization process is a bundle of events and condition sequences and effects per crystallization point, and these are referred to as a *conflict scenario*. This way of constructing conflict scenarios aims to bring into account all relevant ways in which a hazard can play a role in each flight condition / severity category. In order to cope with the complexity of the various possible causes and results to be considered, *clusters* of generic hazards are formed. Such a cluster may cause, or may result from, the same generic hazardous situation. A cluster of events could for instance be the set of 'events causing a missed approach to deviate from the normal path'. An example is given in the figure below. It should also be noticed that one cluster of hazards may play a role in one or more *conflict scenarios*. Often, a conflict is caused by a hazard in combination with a specific condition. Each of the identified hazards can be of the following types: • a root hazard, which may cause a conflict; or • a resolution hazard, which may complicate the resolution of a conflict. Usually, both clusters with root hazards and with resolution hazards play a role in conflict scenario resolution.



Step 4: Severities of hazards' combined effects

For each of the in Step 3 identified conflict scenarios it is determined which of the severity categories selected in step 0 are applicable to the hazards' combined effects. Safety experts should assess which of the severities are applicable for each conflict scenario, by consultation of and review by operational experts. For each conflict scenario the hazards' combined effects and their severities depend on many factors, such as the conditions under which the conflict occurs, the geometry of the conflict, and on whether (timely) resolution of the conflict takes place. Therefore, a range of severities may apply to a conflict scenario. If necessary, the structuring of the events in the conflict scenarios of step 3 are updated such that each applicable severity category is linked to the occurrence of specific event sequences.

Step 5: Assess frequency per severity category

Next, for each possible severity outcome of each conflict scenario the occurrence frequency is evaluated by making use of appropriate trees per scenario. The probability of the top event in the tree is expressed as a sum of a product of probabilities of applicable conditional events. For assessing the factors in these trees, primary sources of data are formed by available statistical databases, such as data collected through the Aviation Safety Reporting System (ASRS), NLR's Air Safety Database [Air safety database], local controller reporting system(s), etc. For an appropriate use of such data dedicated operational expertise is taken into account. Of those particular areas of the tree for which a dedicated TOPAZ simulation tool exists, such tool will be used for risk estimation including bias and uncertainty assessment. Important additional data for the frequency assessments is formed by interviews with operational experts, who are familiar with the local ATM systems and procedures of the operation under consideration. Qualitative expressions are to be translated in quantitative numbers when the selected safety criteria of

Step 0 also are expressed in numbers. Complicating factors in assessing the frequency of a conflict ending in a given severity at once can be that there is often little or no experience with the new operation, and that the situation may involve several variables. This holds especially for the more severe outcomes of the conflict, since these situations occur rarely, and accordingly less information is at hands about the behavior of air traffic controllers and pilots in such situations. Using a suitable TOPAZ simulation tool for such assessments has then significant advantages: 1) the risk estimate quality improves, and 2) it is possible to estimate a 95% uncertainty area. Whenever a suitable TOPAZ simulation tool is not available for the application considered, then it is a realistic option to extend an existing or to develop a TOPAZ simulation toolset for this.

Methodology to extend or develop a TOPAZ simulation tool set

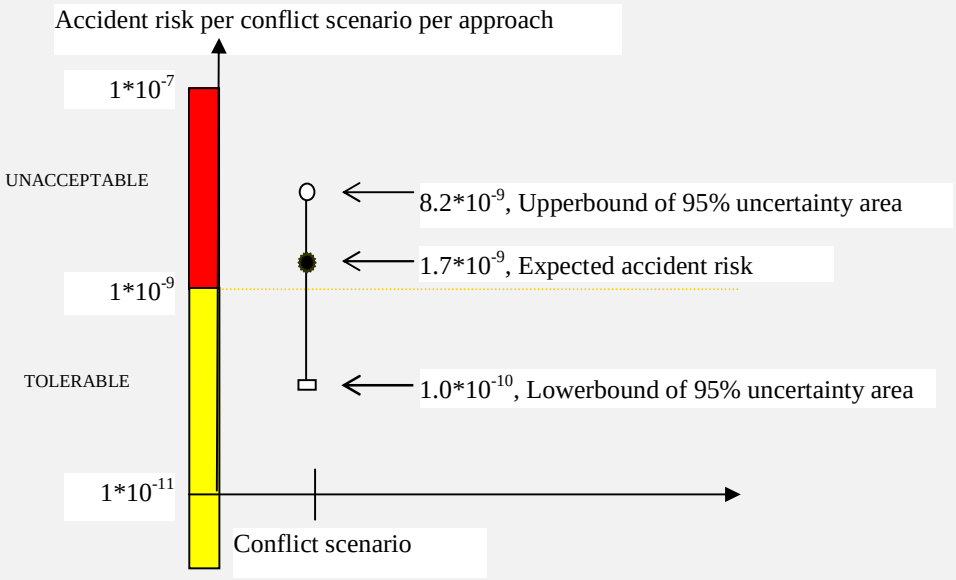
The underlying idea of the TOPAZ methodology is to run Monte Carlo simulations of the operation to count the number of risk related events over very large periods of time, e.g. 10^{10} flight hours or more. Although the idea is simple, making this work in practice is not. The key problems and how each is managed within the TOPAZ methodology are described next:

a) In order to simulate 10^{10} or more flight hours in a straightforward manner, even with a supercomputer, one needs a lifetime to accomplish this. Within TOPAZ, use is made of various techniques to speed up the Monte Carlo simulations. Basically, these techniques allow to "factorize" the accident risk in a suitable form. Subsequently, for each factor in this product, a conditional Monte Carlo simulation is performed and at the end all factors are combined into the desired result, e.g. [Blom&al03c].
b) How to compare the Monte Carlo simulation model and results with reality? A systematic approach in identifying differences between the Monte Carlo simulations model and reality and in assessing the effects of these differences in terms of bias and uncertainty. The operational concept designers are actively involved with the evaluation of these differences. [Everdij&Blom02] and [Stroeve&al03a].
c) How to model human behavior and interactions with other humans and systems? The psychological knowledge and sub-models that are used for this have a lot in common with those used in Air-MIDAS and IPME [Laughery & Corker, 1997]. The main difference is that more attention goes to modeling the non-nominal [Blom&al98,01], [Stroeve&al03a] and less to modeling various human performance metrics [Blom&Corker&al03].
d) How to build in a controlled way a Monte Carlo simulator for a complex operation in ATM? For building a Monte Carlo simulator use is made of formal mathematical specification methods such as Petri Nets, stochastic differential equations, Markov processes and similarity transformations. Once such a formal specification is completed, it is used to generate the Monte Carlo simulation code in a semi-automated way [Everdij&Blom03],

Step 6: Assess risk tolerability per severity category

The aim of this step is to assess the tolerability of the risk for each of the flight condition / severity categories selected in step 0. First the total risk per flight condition / severity category is determined by summing over the assessed risk contributions per conflict scenario for that flight condition / severity category. This summation takes into account both the expected value and the 95% area of the risk summation. Next for each severity category the total risk expected value and the 95% area are compared against the in Step 0 selected TLS. If either the expected value arises above the TLS, or the 95% area peaks over the 10xTLS, then the operation is qualified as being UNACCEPTABLE regarding the safety of this severity category. Otherwise the safety of the severity category is qualified as being TOLERABLE.

The figure below presents an example of such a comparison.



*Accident risk per approach for one particular conflict scenario. The * denotes expected accident risk, the area between the small square and small circle is the 95% uncertainty area.*

During step 0 in [Scholte&al04] each conflict scenario is selected as a flight condition category and four severity categories have been adopted (ACCIDENT, SERIOUS INCIDENT, MAJOR INCIDENT, SIGNIFICANT INCIDENT). For ACCIDENT a TLS of 10^{-9} per conflict scenario has been adopted. During step 5, for one of the conflict scenarios (at least one aircraft is turning to intercept its localizer) the ACCIDENT risk level has been assessed in terms of expected value and 95% uncertainty area. In this example, the 95% uncertainty area stays below 10xTLS, however the expected risk level falls above the TLS. Hence the ACCIDENT risk due to an aircraft turning to intercept its localizer for the operation considered within this Sourdine example has been qualified as being UNACCEPTABLE.

Step 7: Identify safety bottlenecks

From the risk tolerability assessment, it follows which conflict scenario(s) contribute(s) most to the expected value and the 95% area of the risks that has been qualified as being UNACCEPTABLE. For these conflict scenarios the hazards or conditions that contribute most to these high risk level or uncertainty are identified during step 7. If desired, this may also be done for TOLERABLE risks levels that are near the TLS level. Knowledge about these bottlenecks can be used to support further development of the operation.
A systematic way to identify hazard or uncertainty safety bottlenecks for a conflict scenario with UNACCEPTABLE risk is through a sensitivity study. For each hazard/condition one evaluates how much the total risk would improve if its estimated frequency (or uncertainty) is reduced by a factor ten. For some of the hazards and conditions the risk such a factor ten improvement may even reduce the total risk to a TOLERABLE level. These hazards and conditions apparently play a large role in causing the large risk of the conflict scenario, and hence are referred to as safety bottlenecks. The identification of safety bottlenecks is important as it gives operational concept designers directions in searching for potential risk mitigating measures for the operation, and for the safety assessment experts to be aware of the hazards/conditions for which the reduction of

<table>
<tr><td></td><td>uncertainty has high priority.

Optional Step: Support mitigating measure brainstorm
Following the above assessment steps, decision-makers can consider whether the operation will be implemented as such, or that the operation will not be implemented at all, or that the operation will be adapted with mitigating measures to be developed by operational experts. This mitigation measures development process can very well be supported by a mitigation measure brainstorm with concept designers and operational experts as participants and a safety analyst as moderator. The safety analyst moderator can structure the brainstorm on the basis of the outcomes of the safety analysis performed.

Iteration of safety assessment cycle
In case adaptation or redevelopment of the operation takes place, a new safety assessment should be performed that adopts the same wide view as the first cycle, not limiting to the adapted operational details. The reason for this is that adaptations of the air traffic operation may improve safety in one respect, but may imply additional hazards also. And in combination with earlier hazards the additional hazards may deteriorate safety even more than the aimed safety improvement.</td></tr>
<tr><td>Applicability range:</td><td>The TOPAZ methodology incorporates operational hazards of all types, e.g. related to technical systems, humans, procedures, environment, organisation and their interactions. Moreover, it includes a method to systematically identify and assess all these types of hazards.</td></tr>
<tr><td>Life cycle stage:</td><td>Any lifecycle stage, from system definition until and including operations and maintenance and decommissioning.</td></tr>
<tr><td>Experience in application to air traffic:</td><td>TOPAZ has been applied to existing and advanced ATM applications; examples with references are:
<table><tr><td>Active runway crossings</td><td>[Stroeve&al03a], [Klein Obbink&Scholte03]</td></tr><tr><td>Converging runways</td><td>[Blom&al03b]</td></tr><tr><td>Parallel route ASAS equipped a/c</td><td>[Everdij&al02]</td></tr><tr><td>Wake vortex induced risk</td><td>[Kos&al00/01], [Baren&al02]</td></tr><tr><td>Parallel en route lanes</td><td>[Blom&al03a]</td></tr><tr><td>Continuous Descent Approach</td><td>[Scholte&al04]</td></tr></table></td></tr>
<tr><td>Related methods:</td><td>The methodology uses, in an integrated way, many individual techniques, such as Bias and Uncertainty Assessment, DCPN (Dynamically Colored Petri Nets), Generalized Reich collision risk model, HSMP (Hybrid-State Markov Processes), TOPAZ-based hazard brainstorm, Monte Carlo Simulations, Markov Chains, Multiple Agent based modeling, PDP (Piecewise Deterministic Markov Processes), Risk decomposition, TOPAZ hazard database, Situational Awareness Error Evolution, Stochastic Differential Equations in ATM, Human performance simulations in Air-MIDAS and IPME. [Laughery&Corker, 1997].</td></tr>
<tr><td>Availability and tool support:</td><td>The methodology is publicly available, and is supported by dedicated courses at different usage levels (from applying an existing TOPAZ simulation toolset to extending / developing a TOPAZ simulation toolset). The methodology is supported by a database with hazards from previous studies, previous sub-models, simulation toolsets and environments.</td></tr>
<tr><td>Maturity:</td><td>TOPAZ methodology is applied on a routine basis to air traffic operations at or around Schiphol airport.</td></tr>
<tr><td>Acceptability:</td><td>TOPAZ methodology is well accepted by LVNL for assessing its operations.</td></tr>
<tr><td>Ease of integration:</td><td>TOPAZ is an integrated methodology of methods itself, and can be integrated with other human performance simulation approaches, e.g. Air-MIDAS, IPME.</td></tr>
<tr><td>Documentability:</td><td>For each step of the TOPAZ methodology the documentation process is well defined.</td></tr>
<tr><td>Advantages:</td><td>Advantages are:
1. Large variety of hazard types are covered.</td></tr>
</table>

	2. Combinations of hazards are covered. 3. The methodology is scenario-based. 4. It has a broad coverage of hazards, both in identification and in analysis. 5. Once an appropriate simulation toolset is available, there is no need anymore for involvement of stochastic analysts and cognitive psychologists 6. Relative easy method to assess safety and provide safety feedback even in early stages of concept development.
Disadvantages:	1. The development or extension of a TOPAZ simulation toolset needs dedicated expertise also from stochastic analysts and cognitive psychologists. 2. Persons from these different scientific disciplines need to be able to communicate well over disciplinary boundaries; this requires a learning process. 3. A completely novel development and assessment requires significant effort (about two person years) and throughput time (about one year).

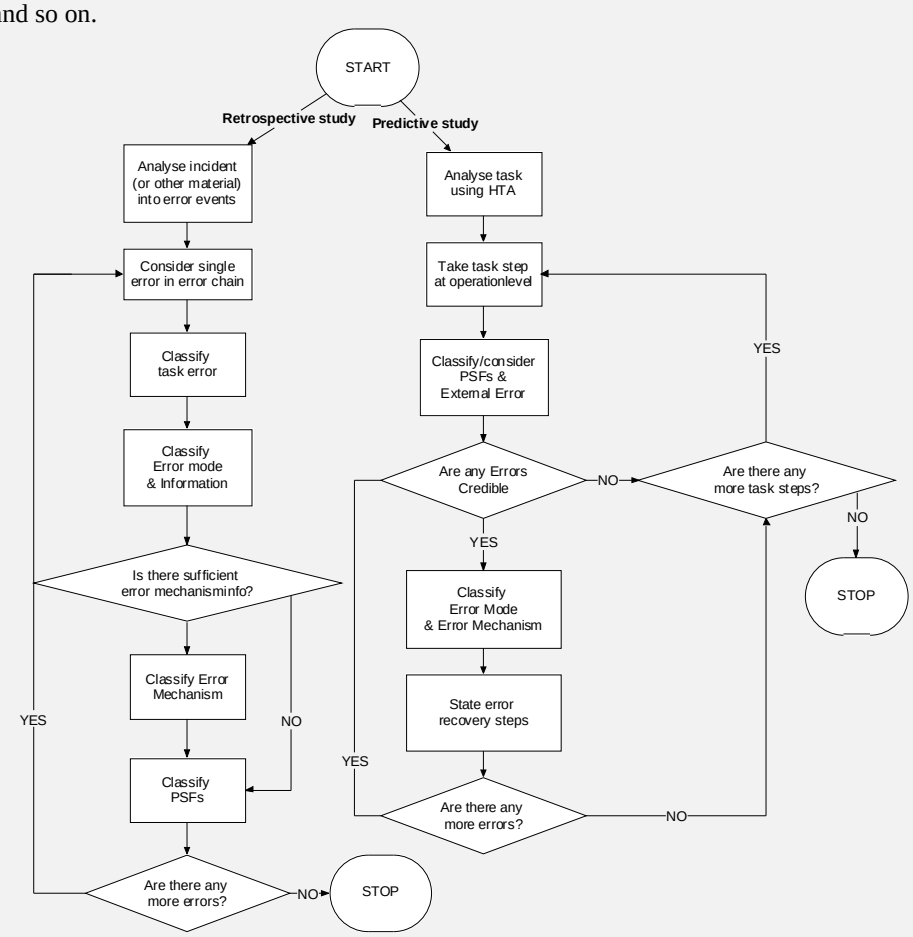
26. TRACER-Lite (Technique for the Retrospective Analysis of Cognitive Errors)

<table>
<tr><td>References used:</td><td>Key references:
• [Shorrock01]
Other references:
• [HIFA_human]
Additional reading:
• [Shorrock&Kirwan98], [TRACEr lite_xls]</td></tr>
<tr><td>Alternate names:</td><td>None</td></tr>
<tr><td>Primary objective:</td><td>To predict human errors that can occur in ATM systems, and to derive error reduction measures for ATM. Aim is to aid the design process by predicting what errors could occur, thus helping to focus design effort. It is designed to be used by ATM system designers and other operational personnel. The tool helps to identify and classify the ‘mental’ aspects of the error, the recovery opportunities, and the general context of the error, including those factors that aggravated the situation, or made the situation more prone to error.</td></tr>
<tr><td>Description:</td><td>TRACER-Lite provides a human error identification technique specifically for use in the air traffic control domain. It builds on error models in other fields and integrates Wickens' (1992) model of information processing in ATC. TRACER is represented in a series of decision flow diagrams.

The original version of TRACER was retrospective, used for classifying errors that contributed to incidents. This was the fore-runner to the EUROCONTROL HERA technique. TRACER originally comprised a modular structure of taxonomies describing the context, error and error recovery (see table below) represented as a series of colour-coded decision-flow diagrams and tables [Shorrock01].

<table>
<tr><th>Taxonomy</th><th>Description</th></tr>
<tr><td colspan="2">CONTEXT</td></tr>
<tr><td>Task Error</td><td>What task(s) failed or led to an unwanted outcome?</td></tr>
<tr><td>Information</td><td>What information was the subject of the error?</td></tr>
<tr><td>Performance Shaping Factors</td><td>What other factors associated with the task, the working environment or the controller affected performance?</td></tr>
<tr><td colspan="2">ERROR PRODUCTION</td></tr>
<tr><td>Cognitive Domains</td><td>What information processing domain was implicated in the error?</td></tr>
<tr><td>External Error Modes</td><td>What was the external manifestation of the error?</td></tr>
<tr><td>Internal Error Modes</td><td>What cognitive function failed, and in what way did it fail?</td></tr>
<tr><td>Psychological Error Mechanisms</td><td>What was the psychological mechanism involved</td></tr>
<tr><td colspan="2">ERROR RECOVERY</td></tr>
<tr><td>Error Detection</td><td>How did the controller become aware of the error?</td></tr>
<tr><td>Error Correction</td><td>How did the controller correct the error?</td></tr>
</table>

The process of developing TRACER was iterative. The main inputs included:
• A literature review (covering over 70 sources).
• A controlled study of error classification.
• Analysis of numerous controller interviews regarding unreported human errors.
• Analysis of many ATM incident reports</td></tr>
</table>

	• Controller reviews of TRACER taxonomies. • Application to several equipment design and airspace design studies on paper, in real-time simulations, and in live trials. Initially, TRACER was designed to be used primarily by HF specialists. However, it became clear that TRACER could be beneficial to other ATC specialists, such as incident investigators and designers. Operational feedback revealed that TRACER appeared too complex or time-consuming to apply in an operational environment by non-HF specialists, as with other error classification systems. If such a technique was to be used in practice, a reduced-scope version, was needed. This idea was called 'TRACER-Lite' - an error analysis and classification tool for operational ATC personnel. The figure below gives a TRACER-Lite method flowchart. The right hand side part of this flowchart refers to the TRACER-Lite prediction technique. The left hand side refers to TRACER-Lite incident error classification technique. Classifying errors using TRACER-Lite first requires a task analysis of the process of using the ATM system. Various methods could be used, though Hierarchical Task Analysis (HTA) is often used. Depending on the scope of the study, it may be necessary to select and analyse only the critical tasks on order to limit the analysis. Such tasks may be critical to safety, acceptance, and so on.  See [Shorrock01] for more details on TRACER-Lite.
Applicability range:	TRACER has been applied to the following areas [Shorrock01]: • Analysis of UK Aircraft Proximity (Airprox) incidents (a mandatory reporting system) occurring within both controlled and unregulated airspace between 1996 and 1999.

	• Analysis of confidential incident/error reports (voluntary reporting system) from the Confidential Human Factors Incident Reporting Programme (CHIRP). • Prediction and analysis of errors occurring in large-scale real-time simulations as part of the New Scottish Centre (NSC) program. • Prediction and analysis of errors occurring in small-scale military simulations of reduced separation standards outside controlled airspace. • Human error prediction for the Final Approach Spacing Tool (FAST).
Life cycle stage:	The Predictive version can be applied in all lifecycle stages. The Retrospective version can be used during operational stages.
Experience in application to air traffic:	TRACER was originally developed by NATS to gain a better understanding of air traffic controller error. It was used in an analysis of UK Airprox incidents occurring within both controlled and unregulated airspace between 1996 and 1999. TRACER has recently been tested (positively) in a study in which the technique was applied to three EUROCONTROL projects (Conflict Resolution Assistant, Time-Based Separation (Approach phase) and an ASAS (Airborne Separation Assurance System) concept.
Related methods:	Link to HTA, HAZOP, and human error analysis techniques such as AEA (Action Error Analysis), CMA (Confusion Matrix Analysis), SRK (Skill, Rule and Knowledge-based behavior model), THERP (Technique for Human Error Rate Prediction), Human error recovery, APRECIH (Analyse PREliminaire des Conséquences de l'Infiabilité Humaine), AEMA (Action Error Mode Analysis), SHERPA (Systematic Human Error Reduction and Prediction Approach), PHEA (Predictive Human Error Analysis technique). In a EUROCONTROL project, TRACER was the prototype for the HERA incident-error classification technique, and the subsequent JANUS version also developed in the US.
Availability and tool support:	TRACER-Lite is available in a partner version for retrospective use in incident investigation and analysis. It is available as a paper version, but also supported by a Microsoft Excel tool package.
Maturity:	TRACER was developed within NATS only recently (1999), however, it has been applied several times to ATM situations.
Acceptability:	As a relatively new technique, this is as yet unknown. However, a recent testing of the approach in EUROCONTROL on three projects produced favorable evaluation by the project personnel.
Ease of integration:	TRACER can be used with human task analysis techniques.
Documentability:	Use of the TRACER-Lite Excel worksheet ensures a high documentability.
Relevance to ATM:	The method marks a shift away from knowledge based errors in other error analysis tools to better reflect the visual and auditory nature of ATM. It has proved successful in analysing errors in AIRPROX reports to derive measures for reducing errors and their adverse effects [HIFA_human], and has successfully predicted errors that have been found to occur in subsequent real-time simulations. Other general advantages are: 1. TRACER-Lite is a comprehensive Human Error Identification technique, contextual to ATM 2. It is a robust and usable system, based on structured decision flow diagrams 3. It is also used to derive error reduction measures for ATM 4. TRACER-Lite's modular structure allows the user to describe the error at a level for which there is supporting evidence. 5. TRACER-Lite is compatible with TRACER, such that more complex cognitive errors can, if required, be initially classified using TRACER-Lite, then revisited using TRACER by a human factors specialist and incident investigator. 6. By using a common framework and shared taxonomies for prospective and retrospective use, maximum use is made of the feed forward and feedback loops that are available.
Con's and	The TRACER method itself can be primarily used by human factors specialists only. The

resources:	expertise required for TRACER-Lite is lower, however. The resources required for TRACER-Lite are moderate. General weaknesses are: 1. Operational feedback revealed that TRACER appeared too complex or time-consuming to apply in an operational environment by non-human factors specialists, as with other error classification systems. TRACER-Lite was developed to reduce this weakness. 2. TRACER relies on having a prior task analysis – for early system design evaluation, other methods (e.g. a HAZOP focusing on human error) may be more useful.

27. Use of Expert Judgement

References used:	Key references: • [Ayyub01] • [Humphreys88] Other references: • [Kirwan94] • [Kirwan&Kennedy&Hamblen] • [Nijstad01] • [Williams85] Additional reading: • [Basra&Kirwan98], [Foot94], [MUFTIS3.2-I]
Alternate names:	Engineering judgement; Delphi technique; Brainstorming; Consensus Groups; Absolute Probability Judgement; Direct Numerical Estimation; Nominal Groups Technique; and Paired Comparisons.
Primary objective:	Use of expertise when no suitable data or methods exist to provide a quantitative estimate or a qualitative input, or a decision result to a particular problem. Some examples might be the following: estimation of external events (e.g earthquake likelihood, fire, etc.), failure or recovery likelihood (e.g. probability of TCAS risk alert leading to recovery in a particular collision scenario, or probabilities of human errors or recoveries), identification of hazards in a new system (e.g. data-link errors or errors with ASAS applications), or partitioning of known data into failure sub-sets (e.g. deciding what proportion of a historical event frequency was human-caused, and what was equipment-caused). In practice, safety assessments are often data or technique-limited, and recourse will be made to expert judgment approaches.
Description:	Expert judgment approaches all have two principal components or requirements: 1. Expertise 2. Ways of combining expertise accurately Expertise, or to be precise, *substantive* expertise, means that the experts have detailed knowledge and experience of the issue in question. Typically an 'expert' should have a minimum of 10 years of expertise in an area. During such time, the 'expert' will have seen not only how things work, but how they fail, and will have gained sufficiently broad experience to be able to inform the expert judgment process. Technically, if substantive experts are not available, then the derivation of judgments is called '*engineering judgment'* rather than expert judgment. The former may be used when no experts are available for example, but obviously such judgments carry less 'weight' than if experts had been used. Ways of combining expertise accurately means that the expertise is elicited and combined in a way that maximizes the validity of the actual expertise of the expert(s). In particular, expert judgment techniques, whether qualitative or quantitative in nature, seek to avoid *biases* in expert judgment. There are a number of well-documented biases such as availability (giving more weight to recent or otherwise memorable events), conservatism (underestimating extremes such as very high and very low probabilities or frequencies), and anchoring (inadvertently giving the expert a 'clue' as to the 'desired' number, hence making it difficult for them to come up with a highly different number, despite what they originally thought), etc. Additionally, there are *motivational* biases, meaning that one or more experts have some vested interest (known or unknown to themselves) in deriving a particular answer – e.g. a designer quantifying the failure likelihood of his or her own design. Lastly in terms of biases, since many expert judgment techniques use group processes, allowing the experts to share their expertise and resolve different opinions, other biases can occur relating to

group dynamics – e.g. one or more experts may dominate the discussion, etc. This is why in expert judgment sessions involving groups, a trained 'facilitator' should be used to lead the session, someone who understands the biases and how to avoid them in the first place, or combat them should they arise – see [Kirwan94].

Formal methods are available, and for the sake of exemplifying the approaches first on the quantification side, the subject of human error quantification is used.

It is assumed that a list of human errors is available e.g. events of a fault tree), for which a probability of occurrence has to be estimated. Next, two human error probability estimation techniques are applied, APJ (Absolute Probability Judgment) and PC (Paired Comparisons). These techniques can be used in combination, e.g. by applying them both, and then taking the most conservative human error probability as the final estimate. Another option is to use APJ to get the probabilities, and to use PC to test which judges were consistent (see further below). APJ and PC are described next.

There are two forms of APJ, namely Groups APJ method, and Single Expert Method. In the latter case, a single expert makes the estimates. For Group APJ there are four major methods:

- Aggregated Individual Method. The experts make their estimates (i.e. estimates of the HEPs) individually. The resulting, say, n probabilities are multiplied and the n^{th} root of the product is the final result (this is called the geometric mean, and is generally the average used for probabilities, although the median can also be considered).
- Delphi Method. The experts make their estimates individually, and next review each others' assessments. Then they reassess their judgments, after which the results are statistically aggregated as above.
- Nominal Group Technique. Is like the Delphi Method, except that the allowed discussion between experts is limited to clarification comments.
- Consensus Group Method. The group discusses together to find an estimate upon which all group members agree.

The first method has the advantage of avoiding inter-personal (group dynamics) problems and the advantage that the experts do not have to be together at the same time and place, but has the disadvantage that the group does not share expertise. For the last method the opposite holds. [Kirwan94] rates the last technique preferable to the third, and so on, with the first technique least preferable, but leaves it up to the practitioner to decide.

All experts have to be instructed sufficiently in advance, such that the probability of differences in the interpretation of the evaluation to be performed is negligible. This aspect must not be under-estimated – the issues for quantification must be fully specified, with full contextual detail.

APJ needs to be run by an experienced facilitator. The overall APJ procedure is as follows, see [Humphreys88] or [Kirwan94] for details:

1. Select subject-matter experts
2. Prepare the task statements
3. Prepare the response booklets
4. Develop instructions for subjects
5. Obtain judgements
6. Calculate inter-judge consistency
7. Aggregate the individual estimates
8. Estimate uncertainty bounds.

The inter-judge consistency (step 6) can be calculated using e.g. the analysis of variance (ANOVA) technique. [Kirwan94] gives formulas for calculating the upper and lower uncertainty bounds (step 8).

PC estimates human error probabilities by asking experts which pair of error descriptions

is more probable. The result is a ranked list of human errors and their probabilities. The relative likelihoods of human error are converted to absolute human error probabilities assuming logarithmic calibration equation and two empirically known error probabilities. For n tasks, each expert makes n(n-1)/2 comparisons (although there are techniques to reduce this number, see [Kirwan94]). When comparisons made by different experts are combined, a relative scaling or error likelihood can then be constructed. This is then calibrated using a logarithmic calibration equation, which requires that the human error probabilities be known for at least two of the errors within each task set. The method usefully determines whether each expert has been consistent in the judgements he has made.

The complete PC procedure is as follows; see [Humphreys88] or [Kirwan94] for details:

1. Define the tasks involved
2. Incorporate the calibration tasks
3. Select the expert judges
4. Prepare the exercise
5. Brief the experts
6. Carry our paired comparisons
7. Derive the raw frequency matrix
8. Derive the proportion matrix
9. Derive the transformation X-matrix
10. Derive the column-difference Z-matrix
11. Calculate the scale values
12. Estimate the calibration points
13. Transform the scale values into probabilities
14. Determine the within-judge level of consistency
15. Determine the inter-judge level of consistency
16. Estimate the uncertainty bounds.

The within-judge consistency (step 14) can be determined through the number *c* of 'circular triads', i.e. the number of times the same judge says e.g. 'A is greater than B, B is greater than C, C is greater than A'. This number equals:

$c = \left(\frac{n \times (n^2 - 1)}{24} \right) - \frac{T}{2}$, where *n* is the number of events, $T = \sum_{i=1}^{n} (a_i - a)^2$,

$a = (n-1)/2$ and a_i is the number of times that an event a_i was judged to be more likely than any other event. The coefficient of consistency *K* can now be found by:

$K = 1 - (24c / n(n^2 - 1))$ if *n* is odd and $K = 1 - (24c / n(n^2 - 4))$ if *n* is even. If *K* is too small, then the results for this judge should be rejected.

In advanced forms of expert judgement using these methods, expertise may be 'weighted' according to its assessed quality, so that some experts' judgements contribute more to the final result than others.

On the qualitative side, expert judgement is used for hazard identification, for example, or for brainstorming solutions to problems, new hazards, etc. HAZOP is therefore an expert judgement technique. More generally, brainstorming should also follow certain rules. For example, for a hazard brainstorm with operational experts that has the aim to get as many hazards and bottlenecks as possible out in the open, such rules are:

- The brainstorm should be organised at an early stage of the design lifecycle to get as many "unimaginable" hazards as possible.
- The brainstorm should start with a short introduction into the problem or operation to be analysed, so that everyone is up-to-date and looking into the same direction. This introduction should not include too many technical details.
- Before the brainstorm, the organisers should have made a list with points of attention

	and issues that cover the subject to be analysed. This list should be used as a guideline both for the subjects to be dealt with and for the planning to be kept.
	• The brainstorm itself could be very simple:
	  • One of the operational experts mentions a bottleneck or hazard.
	  • The chairman writes it down on e.g. a flip-over
	  • A secretary makes more detailed notes on paper
	  • Repeat.
	• The operational experts should not be afraid to mention hazards and bottlenecks for which it is not immediately clear in advance if they are really bottlenecks. The analysis should be done after the session. The brainstorm chairman should therefore immediately intervene if hazards are being analysed or criticised. The 'brainstormers' should be kept in a creative state, not in an analysis state, and should play the devil's advocate.
	• The brainstorm chairman has another important role: he should be able to stimulate the brainstormers' imagination, and should be able to look at a bottleneck from another viewpoint or in another state, etc.
	• Recent study [Nijstad01] has shown that it is not necessary to have a large group of experts assembled for a brainstorm. In fact, the quality of the output generally decreases with the size of the group. This has to do with 'blocking' (when person A speaks, persons B, C, D, ... cannot speak, and may even forget what they wanted to say) and 'responsibility' (in a large group half of the people can afford to not speak at all). This problem can be reduced by, during the brainstorm or before the brainstorm, taking a break by letting every participant writing down hazards and bottlenecks on a piece of paper for, say, 15 minutes. In practice, a group of three to six experts, with at least an air traffic controller and a pilot, appears to be most effective for a hazard identification brainstorm.
	
	See [Ayyub01] for a very complete overview of expert judgement issues.

Applicability range:	APJ and PC are used to estimate human error probabilities, but neither necessarily restricts to human error only. APJ may be particularly helpful for diagnosis and errors of commission or rule violations, [Kirwan&Kennedy&Hamblen]. Hazard brainstorming can be used for hardware, software, humans, procedures and organization.
Life cycle stage:	Expert judgment can be used in all lifecycle stages, although human error quantification is mostly applied from the design stages on. Hazard identification should be done as early in the lifecycle as possible.
Experience in application to air traffic:	The approach of using APJ in combination with PC has been applied in NATS to develop a small number of human error probabilities. More generally, expert judgment (and more often, engineering judgment) is used frequently in ATM as in other domains.
Related methods:	Link to PC (Paired Comparisons), APJ (Absolute Probability Judgment), Questionnaires, Delphi Knowledge Elicitation Method or Delphi Method, TOPAZ-based hazard brainstorm.
Availability and tool support:	Both APJ and PC are available. Spreadsheets can be used to support the calculations.
Maturity:	Expert judgment as a technique dates back to the 1950s and the beginnings of reliability and later, risk assessment approaches. There was a resurgence in interest after the Three Mile Island accident in 1979, leading to a number of good works on the area applicable to a range of expert judgment scenarios. Expert judgment is used routinely in many cases in nuclear power, offshore, and chemical risk assessments, for example. APJ was developed in 1981 or earlier; PC was developed in 1966, but is based on theories dating back to 1927. According to [Humphreys88], APJ is the oldest technique for probability estimation and has been used and developed in a number of areas. Given its many actual applications in human reliability assessment, it is, overall, a highly mature technique. PC is borrowed from the domain of psychophysics (a branch of psychology). It has been used by psychologists for several decades. It has also been used in human

<table>
<tr><td></td><td>reliability applications for some years, although the actual number of studies has remained small. Its potential for further development is small. Overall, it can be regarded as a moderately mature technique. The principal advantage of PC is that it can sort out experts from non-experts, although professional ethics dictate that such discriminations should not be disclosed to third parties – individuals may however be given feedback, as this is called ‘calibration of expertise’, and helps develop expertise itself.</td></tr>
<tr><td>Acceptability:</td><td>In [Humphreys88], several human reliability assessment techniques, among which APJ and PC, are compared on various criteria, which are: Accuracy, Validity, Usefulness, Effective use of resources, Acceptability and Maturity. All techniques are evaluated on these criteria by a panel of experts, in the form of marks from 1 to 5, where 5 means evaluated high (positive) and 1 means evaluated low (negative). These criteria evaluations are next weighted and added for each technique. The results are presented in the table below. According to this table, HEART receives the highest Preference Index of the techniques evaluated, closely followed by APJ.
<table>
<tr><td>Criteria (weight)</td><td>APJ</td><td>PC</td><td>TESEO</td><td>THERP</td><td>HEART</td><td>IDA</td><td>SLIM</td><td>HCR</td></tr>
<tr><td>Accuracy (0.30)</td><td>3</td><td>3</td><td>1</td><td>3</td><td>3</td><td>1</td><td>3</td><td>1</td></tr>
<tr><td>Validity (0.22)</td><td>4</td><td>3</td><td>1</td><td>3</td><td>3</td><td>3</td><td>3</td><td>1</td></tr>
<tr><td>Usefulness (0.15)</td><td>4</td><td>2</td><td>4</td><td>3</td><td>5</td><td>4</td><td>5</td><td>2</td></tr>
<tr><td>Resources (0.15)</td><td>3</td><td>2</td><td>5</td><td>2</td><td>5</td><td>2</td><td>2</td><td>3</td></tr>
<tr><td>Acceptability (0.11)</td><td>3</td><td>4</td><td>1</td><td>5</td><td>3</td><td>3</td><td>4</td><td>2</td></tr>
<tr><td>Maturity (0.07)</td><td>5</td><td>3</td><td>1</td><td>5</td><td>2</td><td>2</td><td>4</td><td>1</td></tr>
<tr><td>Preference Index</td><td>3.51</td><td>2.81</td><td>2.05</td><td>3.21</td><td>3.53</td><td>2.33</td><td>3.33</td><td>1.56</td></tr>
</table>
[Humphreys88] rates the acceptability of APJ to assessors as relatively low, probably because it is often equated as “guessing”. However, the systematic use of multiple experts, together with statistical measures of agreement may be regarded as an acceptably scientific and systematic for of APJ. PC is a well-established technique based on a good deal of scientific research, and this enhances acceptability.
The ratings for accuracy of APJ, PC and HEART are confirmed by [Kirwan94], who experimentally found their accuracy reasonable and similar to each other, with a slight favor for APJ.</td></tr>
<tr><td>Ease of integration:</td><td>It can be used to provide input to any technique that needs data where no suitable statistical data exist, such as human error probability data, external event likelihood data, other rare event data, etc. APJ is relatively quick to use, and PC is relatively easy for the experts to carry out, since they do not need to provide numerical values. Since neither APJ nor PC restrict to human error alone, they can be incorporated by an FTA.</td></tr>
<tr><td>Documentability:</td><td>Documentability is high, provided all steps and the rationale underlying judgments are recorded during the sessions.</td></tr>
<tr><td>Relevance to ATM:</td><td>The approach is particularly relevant to ATM, since the industry has relied on implicit safety for many years, and does not have a tradition of failure rate assessment, and nor does it have well-established databases of failures or events or errors. Therefore, until such data limitations are redressed, or other analytical methods are used (e.g. mathematical models etc.), there is likely to be a frequent need to utilise expert judgement.

The general strengths of expert judgement are:
1. Expert judgement can provide needed answers
2. It can be used to consider new hazards and solutions, i.e. for novel scenarios where</td></tr>
</table>

	there would be no data available in any case. 3. Expert judgement taps into a valuable experience base, e.g. of controllers, who can often answer questions based on experience that would take mathematical models a long time to model and compute, often with similar levels of uncertainty General strengths of APJ are: 1. In terms of predictive accuracy to general reliability assessments, APJ is probably the best quantifying technique, [Williams85]. 2. APJ is the most direct approach to the quantification of Human Error Probabilities (HEPs) 3. The method is relatively quick to use, yet it allows as much detailed discussion as the experts think fit, and this detail, if documented, can often be qualitatively useful. 4. It can be incorporated by an FTA. 5. APJ has also been shown to provide accurate estimates in other fields than human error probability estimations. 6. Discussions between experts can also be used for consideration of how to achieve error reductions. General strengths of PC are: 1. Comparative judgments are often easier to give than quantitative judgments. 2. The technique makes it possible to determine if individual judges are poorly qualified to assess a particular data set. 3. A minimum of two empirically known error probabilities is necessary, so most effective use is made of scarce empirical data. 4. Even without the calibration part the results are useful. 5. PC can be applied fairly quickly. 6. The experts do not have to be together at the same time and place. 7. Can be incorporated by an FTA. General strengths of the combined use of APJ and PC is that two independent techniques are used, which may remove bias in the results.
Con's and resources:	The resources required are the operational experts, and the analysis if using formal techniques. However, since the methods can be performed fairly quickly, these experts are not asked for much of their time. Consensus, Delphi, and Nominal Group techniques produce the results on the same day of the expert judgment exercise. For APJ and PC specifically, a combined use of APJ and PC is of course costlier than the use of only one of these techniques. An experimental assessment described in [Kirwan94] found that PC for human error assessment took about 2 to 3 times more from experts as for HEART, and APJ took about 3 to 5 times more than HEART. General weaknesses of expert judgment are: 1. Availability and ease of co-location of real experts 2. Garbage in, garbage out 3. Biases can sometimes be difficult to avoid 4. Sometimes no-one, not even the experts, know the answer – a distinction must be made between combining expertise (where they know the problem and have experience of it), and where the experts are extrapolating and 'best guessing'. 5. Formal methods can be time-consuming, although computer tools now make paired comparisons, for example, much faster. 6. A poorly prepared set of questions will result in wrong answers, or no answers at all. General weaknesses of APJ are: 1. APJ may give biased results, and be influenced by personality/group conflicts, which may affect the validity of the technique. 2. Since the technique is often compared with 'guessing' it is somewhat low in terms of validity.

	3. The technique is critically dependent on the selection of appropriate experts. General weaknesses of PC are: 1. Tasks being considered may be too complex for easy comparisons. 2. Tasks may not be homogeneous (i.e. comparing like with like), which they have to be if they are to be compared. 3. (Consecutive) comparisons may not be independent of each other. 4. If the number of comparisons is large, the judges may become tired and therefore carry out later comparisons differently from earlier ones.

7.0 Examples of Applications

A few brief case studies are shown below which have utilized a number of the techniques in the Toolbox, to demonstrate how the techniques may work together.

Case Study #1 – Reduction of Vertical Separation Minima in UK Flight Information Region (FIR)

Outside of normal civil air traffic 'lanes' in the UK, aircraft may receive a Radar Advisory Service (RAS) from military controllers, if they wish. Until recently, such regions of airspace used similar separation minima as in conventionally-controlled airspace, namely 5000 feet vertical separation or 5nm lateral separation. However, for a variety of reasons, this could create considerable workload for the military controllers, and it was desired to reduce the separation minima to 3000 feet and 3nm respectively. This objective required a safety evaluation and a formal safety case.

The approach involved two main streams of work – collision-risk (mathematical) modeling and a human reliability evaluation, since the main impact would be on controllers and their possibly reduced reaction times given the reduction in separation minima.

In fact the following techniques were used, in the following sequence:

- Event analysis (of military and civil incidents and losses of separation)
- Hierarchical Task Analysis of operations
- TRACER analysis to identify errors and recoveries
- Fault Tree Analysis of vents that could lead to loss of separations
- Event tree Analysis of outcome pathways from such hazards
- Simulations (two) to evaluate key Human Factors parameters (principally workload and situation awareness) in reduced and normal separation minima conditions
- Collision risk modeling with the new criteria

The above led to the conclusion that reduction of the vertical minima was safe, but not the proposed lateral separation minima reduction. The safety case therefore dropped the objective of reducing lateral separation minima. A live trial was proposed. The safety of the trial itself, since it would involve six military Air traffic Service Units and real airspace, was assessed using the HAZOP technique.

After an initial six-month trial, and a further six months trial with no adverse events, the reduction of vertical separation was accepted and the scheme went national.

Case study # 2 - Category-I (CAT-I) Ground-Based Augmentation System (GBAS)

CAT-I/II/III operations at European airports are presently supported by Instrument Landing Systems (ILS). The continued use of ILS-based operations as long as operationally acceptable and economically beneficial is promoted by the European Strategy for the planning of All Weather Operations (AWO). However, in ECAC (European Civil Aviation Conference), the forecast traffic increase will create major operational constraints at all airports, in particular in Low Visibility Conditions (LVC) with the decreased capacity of runways. Consequently, the technical limitations of ILS such as Very High Frequency (VHF) interference, multi-path effects due to, for example, new building works at and around airports, and ILS channel limitations will be a major constraint to its continued use. Within this context GBAS is expected to maintain existing all weather operations capability at CATI/II and III airports. GBAS CAT-I (ILS look-alike operations) is seen as a necessary step in order to extend its use to the more stringent operations of CAT-II/III precision approach and landing. Initial implementation of GBAS could be achieved in ECAC as early as 2006.

The process of GBAS ground station Type Approval is already ongoing in some ECAC states and in the US. It has been recognized that there is also a need for an Operational Safety Assessment of GBAS CAT-I approaches. EUROCONTROL has been working with stakeholders to define the requirements for an Operational Safety Assessment. The combination of Type Approval plus the Operational Safety Assessment plus aircraft certification activities will cover the equipment, human, and procedural aspects of GBAS as well as its operational environment, and will ensure that there has been a total aviation assessment of the safety of GBAS. The Functional Hazard Assessment (FHA) (hazard identification) has been completed and the Preliminary System Safety Assessment (PSSA) (risk assessment) is being finalized.

The following techniques were/are being used, in the following sequence:

- ✓ structured hazard identification brainstorming sessions (HAZIDs)
  Note: the hazard identification and analysis has been iterative and linked into the development of a Concept of Operations for GBAS CAT-I (3 stages: Pre-Concept, Interim and Post-Concept FHAs)
- ✓ Event Data Collection and Analyses) (data sources included Airclaims World Aircraft Accident Summary (WAAS), NASA's Aviation Safety Reporting System (ASRS), Flight Safety Foundation articles, British Airways' BASIS data and others)
- ✓ Fault Trees (related to four main functions that are: (i) Select the correct approach; (ii) Capture the correct approach; (iii) Maintain this approach from FAF to DA/DH; and Conduct a missed approach if required) and Event Trees Analyses (CFIT, mid-air collisions and collision with obstacles on the ground)
- ✓ Hierarchical Task Analyses (HTA) for Maintenance Tasks and Switching approaches Tasks (potential use of TRACEr-lite as a trial to see if technique identifies extra failure modes we have so far missed)
- ✓ Bow-Tie Modeling
- ✓ Common Cause Analysis (CCA) (ongoing)

- ✓ Use of Experts Judgment (Absolute Probability Judgments & Paired Comparisons) & historical data sources (quantification) (ongoing)
- ✓ THERP and other techniques (e.g. Beta factors) for conditional probabilities to be calculated (ongoing)
- ✓ appropriate mix of qualitative and quantitative risk analysis to the fault and event trees based on see-saw modeling (relative approach to risk assessment)
- ✓ Claim trees using the GSN (Goal Structured Notation) to support the safety cases development (Pre- and Post-Implementation)
- ✓ Use of operational trials and GBAS Modular Analysis and Research System (EUROCONTROL tool) for critical reviews (System Safety Assessment – SSA – stage and validation of the GBAS Collision Risk Model (CRM)) and monitoring (Post-Implementation Safety Case) (not before 2006)

Following generation of risk results, sensitivity testing and review of risk reduction measures, a comparison will be made to the GBAS Safety Targets. If the targets are met and if risks can be shown to have been reduced as far as reasonably practicable, then GBAS CAT I "ILS look-alike" approaches can be judged to be tolerably safe. If this is the case, then safety objectives and requirements can be based on the quantification in the model. If the Safety Targets are not met, then safety objectives will need to be developed which are effectively more stringent than the base case estimates in the model. Subsequent stages of the safety assessment (SSA) will then need to provide evidence that these more stringent objectives can be met in reality.

Case study # 3 – Simultaneous use of converging runways at Schiphol

The following techniques were used:

- Real time pilot in the loop flight simulation
- Air Safety Data base exploration on related incidents and accidents
- Investigation of safety criteria used by other large airports (Europe and US)
- TOPAZ accident risk assessment methodology, including:
- ✓ Collecting information from controllers and pilots
- ✓ Controller Missed Approach report analysis
- ✓ Hazard identification (to shift boundary between imaginable and unimaginable hazards)
- ✓ Development of conflict scenarios
- ✓ Petri Net based modeling of the operation
- ✓ Monte Carlo simulation of the Petri Net model
- ✓ Assessment of the Bias and uncertainty in risk due to difference between model and reality
- ✓ Safety criteria and risk comparison
- ✓ Safety criticality feedback to the operation design

The accident risk assessment cycle has been cycled through several times, e.g to assess effects of operation design cycle, improvement of model, collection and analysis of novel data.

Reference: [Blom&al03b]

Case study # 4 – Active Runway crossing at Schiphol

The following techniques were/are being used:

- Real time pilot in the loop flight simulation
- Air Safety Data base exploration on related incidents and accidents
- TOPAZ accident risk assessment methodology, including:

✓ Scoping of the safety assessment objective and study
✓ Collecting information from controllers and pilots
✓ Controller runway incident report analysis
✓ Hazard identification (to shift boundary between imaginable and unimaginable hazards)
✓ Development of conflict scenarios
✓ Petri Net based modeling of the operation
✓ Monte Carlo simulation of the Petri Net model
✓ Assessment of the Bias and uncertainty in risk due to difference between model and reality
✓ Safety criteria and risk comparison
✓ Safety criticality feedback to the operation design

The accident risk assessment cycle has been cycled trhough several times, e.g to assess effects of operation design cycle, improvement of model, collection and analysis of novel data.

Reference [Stroeve&al03b]

Case study # 5 – Use of PDARS

Various ATC facilities have used PDARS for example in the following safety-related studies:

1. Optimization of Airspace (e.g. splitting a High Volume Sector into Two)
2. Quality Control of Airspace Definitions (e.g., detecting Gaps/Overlaps in new Sector Designs)
3. Analysis of Airspace/Procedural Changes (e.g., determine viability of Special Use Airspace/Letters of Agreement)
4. Enhancement of Training (e.g., development of Training Scenarios)
5. Analysis of Temporary Flight Restrictions
6. Analysis of VFR/IFR flow interaction
7. Analysis of TCAS Resolution Advisories

These brief case studies and the supporting references in the technique templates show that these techniques are indeed being used in ATM system safety assessment. Some useful sources of further information are cited below.

8. Additional Information

8.1 Further Developments

For most of the selected techniques this report provides an explanation template. For three selected techniques, however, such a template will be produced and incorporated in a future version of this report. These three techniques are: Event Data Collection and Analysis, Flight Data Analysis (see appendix A) and Reliability Databases. In addition it will then be considered if it is useful to further extend the tool set with other techniques that are currently being evaluated for their use as safety technique in ATM.

8.2 Limitations

The toolbox provides currently used and accepted methods for the assessment of system safety. They provide valuable and necessary tools and methods in order to achieve a high level of safety of the ATM system. As the ATM system is likely to change considerably in the coming years, also the safety assessment methods have to be adapted to these changes, on the American, European as well on the global level. ATM system changes will also have an impact on the usability of current safety methods.

To reflect future requirements for safety was not an objective of this toolbox. It should be noted that the methods represented here would need to be further improved regarding future developments of ATM. The current safety strategy indicates the following potential impacts on safety assessment methods:

- Risk monitoring in particular for managing the safety during transition periods (technological or organizational) and throughout the entire lifecycle of the system
- Assessment of unexplored risk contributions (e.g., software, new navigation systems) and combined risk contributions (air/ground; operation/regulation).
- The inclusion of organizational aspects and decision making into risk assessment (e.g., decision errors due to cost/benefit considerations).
- Dynamic risk modeling for enabling scenario based risk assessments and better representation of dependencies in the entire system

Nevertheless, the toolbox document provides an excellent reference for further developments required, because advanced methodologies need to be based on the established tools and methods.

9. TOOLBOX REFERENCES

[ΣΣ93, ΣΣ97]	R.A. Stephens, W. Talso, System Safety Analysis handbook: A Source Book for Safety Practitioners, System Safety Society, 1st edition in 1993, 2nd edition in 1997 (1997 edition partly at http://www.nm-esh.org/sss/handorder.html.)
[Air safety database]	NLR, Air Safety Database, Database maintained at NLR containing world-wide data on air safety (contact: vanes@nlr.nl).
[Amalberti&Wioland97]	R. Amalberti and L. Wioland, Human error in aviation, Proc. Int. Aviation Safety Conf., VSP, Utrecht, 1997, pp. 91-108.
[Andow89]	P. Andow, Estimation of event frequencies: system reliability, component reliability data, fault tree analysis. In R.A. Cox, editor, Mathematics in major accident risk assessment, pp. 59-70, Oxford, 1989.
[Apthorpe01]	R. Apthorpe, A probabilistic approach to estimating computer system reliability, 4 June 2001, http://www.jump.net/~arclight/reliability/lisa/2001/reliability_analysis.ps
[ARP 4754]	SAE ARP 4754, Certification considerations for highly-integrated or complex aircraft systems, Systems Integration Requirements Task Group AS-1C, Avionics Systems Division (ASD), Society of Automotive Engineers, Inc. (SAE), September 1995.
[Ayyub01]	B.M. Ayyub, Elicitation of expert opinions for uncertainty and risks, CRC Press, Boca Raton, Florida, 2001.
[Barbarino01]	M. Barbarino, EATMP Human Resources R&D, 2nd ATM R&D Symposium, 18-20 June 2001, Toulouse, http://www.cena.dgac.fr/actualites/atmrd/barbarino-hum-r&d-symposium.ppt
[Barbarino02]	M. Barbarino, EATMP Human Factors, ATM 2000+ Strategy Update Workshop, 5-7 March 2002, http://www.eurocontrol.int/eatmp/events/docs/ATM_hum.pdf
[Baren&al02]	G.B. Van Baren, L.J.P. Speijker, A.C. de Bruin, Wake vortex evaluation of single runway approaches under different weather and operational conditions, Proc. 6th Conf. Probabilistic Safety Assessment and Management, July 2002.
[Basra&Kirwan98]	G. Basra and B. Kirwan, Collection of offshore human error probability data, Reliability Engineering and System Safety, Vol 61, pp. 77-93, 1998
[Baybutt89]	P. Baybutt, Uncertainty in risk analysis, Mathematics in major accident risk assessment. In R.A. Cox, editor, Mathematics in major accident risk assessment, pp. 247-261, Oxford, 1989.
[Bishop90]	Dependability of critical computer systems - Part 3: Techniques Directory; Guidelines produced by the European Workshop on Industrial Computer Systems Technical Committee 7 (EWICS TC7). London Elsevier Applied Science 1990 (249 pages), P.G. Bishop (editor), Elsevier, 1990
[Blom&al03a]	H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij & M.N.J. van der Park, Human cognition performance model to evaluate safe spacing in air traffic, Human Factors and Aerospace Safety, Vol. 3 (2003), pp. 59-82
[Blom&al03b]	H.A.P. Blom, M.B. Klompstra and G.J. Bakker, Accident risk assessment of simultaneous converging instrument approaches, Air Traffic Control Quarterly, Vol. 11 (2003), pp. 123-155.
[Blom&al03c]	H.A.P. Blom, G.J. Bakker, M.H.C. Everdij, M.N.J. Van der Park, Collision risk modelling of air traffic, Proceedings European Control Conference, Cambridge, UK, September 2003.
[Blom&al98,01]	H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij, and M.B. Klompstra, Accident risk assessment for advanced ATM, 2nd USA/Europe Air Traffic Management R&D Seminar, FAA/Eurocontrol, 1998, http://atm-seminar-98.eurocontrol.fr/finalpapers/track3/blom.pdf, also in Eds G.L. Donohue, A.G. Zellweger, Air Transportation Systems Engineering, AIAA, pp. 463-480, 2001.
[Blom&Bakker93]	H.A.P. Blom, G.J. Bakker, A macroscopic assessment of the target safety gain

	for different en route airspace structures within SUATMS, Working paper for the ATLAS study of the commission of European Communities, NLR report CR 93364 L, 1993.
[Blom&Corker&al03]	H.A.P. Blom, K.M. Corker, S.H. Stroeve and M.N.J. van der Park, Study on the integration of Air-MIDAS and TOPAZ, Phase 3 final report, NLR contract report CR-2003-584, 2003.
[Blom&Daams&Nijhuis00]	H.A.P. Blom, J. Daams, H.B. Nijhuis, Human cognition modelling in ATM safety assessment, 3rd USA/Europe Air Traffic management R&D seminar, Napoli, 13-16 June 2000, http://atm-seminar-2000.eurocontrol.fr/acceptedpapers/pdf/paper92.pdf, also in Eds G.L. Donohue, A.G. Zellweger, Air Transportation Systems Engineering, AIAA, pp. 481-511, 2001.
[Blom&Everdij&Daams99]	H.A.P. Blom, M.H.C. Everdij, J. Daams, ARIBA Final Report Part II: Safety Cases for a new ATM operation, NLR report TR-99587, Amsterdam, 1999, http://www.nlr.nl/public/hosted-sites/ariba/rapport6/part2/.
[Blom&Stroeve&Daams &Nijhuis01]	H.A.P. Blom, S. Stroeve, J. Daams and H.B. Nijhuis, Human cognition performance model based evaluation of air traffic safety, 4th International Workshop on Human Error, Safety and Systems Development, 11-12 June 2001, Linköping, Sweden
[Blom&Stroeve&Everdij &Park02]	H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij, M.N.J. van der Park, Human cognition performance model based evaluation of safe spacing in air traffic, ICAS 2002 Congress
[Braven&Schade03]	W. Den Braven, J. Schade, "Concept and Operation of the Performance Data Analysis and Reporting System", SAE conference, Montreal, September 3-7, 2003
[CAA-RMC93-1]	Hazard analysis of an en-route sector, Volume 1 (main report), Civil Aviation Authority, RMC Report R93-81(S), October 1993.
[CAA-RMC93-2]	Hazard analysis of an en-route sector, Volume 2, Civil Aviation Authority, RMC Report R93-81(S), October 1993.
[Cacciabue98]	P.C. Cacciabue, Modelling and human behaviour in system control, Advances in industrial control, Springer, 1998
[Corker 03]	Corker, K (2003) Requirement for a Cognitive Framework for Operation in Advanced Aerospace Technologies . In E. Hollnagel (ed.). The Handbook of Cognitive Task Design , Lawrence Earlbaum Associates, 2003.
[Corker 02]	Corker, K. (2002). Hazard, Risk and Performance Prediction in Large-Scale Airspace Simulations: Human Performance Compared to Human Model Prediction. Proceedings of the International Symposium on Air Traffic Management 2002. Capri, Italy
[Corker 00]	Corker, K. (2000). Cognitive Models & Control: Human & System Dynamics in Advanced Airspace Operations. (2000) in N. Sarter and R. Amalberti (Eds.) Cognitive Engineering in the Aviation Domain. Lawrence Earlbaum Associates, New Jersey.
[Cotaina&al00]	N. Cotaina, F. Matos, J. Chabrol, D. Djeapragache, P. Prete, J. Carretero, F. García, M. Pérez, J.M. Peña, J.M. Pérez, Study of existing Reliability Centered Maintenance (RCM) approaches used in different industries, Universidad Politécnica de Madrid, Facultad de informática, TR Number FIM/110.1/DATSI/00, 2000, http://laurel.datsi.fi.upm.es/~rail/bibliography/documents/RAIL-soa-FIMREPORT-00.pdf
[Daams&Blom&Nijhuis00]	J. Daams, H.A.P. Blom, and H.B. Nijhuis, Modelling Human Reliability in Air Traffic Management, PSAM5 - Probabilistic Safety Assessment and Management, S. Kondo, and K. Furata (Eds.), Vol. 2/4, Universal Academy Press, Inc., Tokyo, Japan, 2000, pp. 1193-1200.
[DEFSTAN00-56]	Hazard analysis and safety classification of the computer and programmable

	electronic system elements of defence equipment, Int. Defence standard 00-56/1, April 1991.
[DeJong&al01a]	H.H. De Jong, R.S. Tump, H.A.P. Blom, B.A. van Doorn, A.K. Karwal, E.A. Bloem, Qualitative Safety Assessment of a RIASS based operation at Schiphol airport including a quantitative model, Crossing departures on 01L/19R under good visibility conditions, NLR memorandum LL-2001-017, May 2001
[DeJong&al01b]:	H.H. De Jong, H.A.P. Blom, B.A. Van Doorn, E.A. Bloem, Overview of a Qualitative Safety Assessment methodology for air traffic operations, NLR-Memorandum LL-2001-046, December 2001.
[DeJong&al03]	H.H. De Jong, J.J. Scholte, G.B. Van Baren, Safety evaluation for the dependent operation of the southern taxiway and runway 18C/36C, Part 4: Inbound Mode 4 Argumentation based evaluation, Contract Report NLR-CR-2003-516, National Aerospace Laboratory NLR, LVNL Company confidential, 2003
[DeJong&al04]:	H.H. De Jong, H.A.P. Blom, B.A. Van Doorn, E.A. Bloem, Overview of Qualitative Safety Assessment methodology for air traffic operations, NLR-Memorandum ATSF-2004, 2004.
[DeJong04]	H.H. De Jong, Guidelines for the identification of hazards; How to make unimaginable hazards imaginable, Contract Report NLR-CR-2004-094, National Aerospace Laboratory NLR, 2004
[DNV-HSE01]	Det Norske Veritas, for the Health and Safety Executive, Marine risk assessment, Offshore technology Report 2001/063, http://www.hse.gov.uk/research/otopdf/2001/oto01063.pdf
[DOE 1023-95]	Department Of Energy (DOE) Standard, Natural Phenomena Hazards Assessment Criteria, DOE-STD-1023-95, July 1995, http://www.deprep.org/1995/tb95g31a.PDF
[DOE-3006]	Department Of Energy (DOE) Standard, Planning and Conduct of Operational Readiness Reviews (ORR), DOE-STD-3006-2000, June 2000, http://tis.eh.doe.gov/techstds/standard/std3006/std_3006_2000.pdf
[Dryden-ORR]	NASA, Dryden Centerwide Procedure, Code SH, Facility Operational Readiness Review (ORR), DCP-S-031, http://www.dfrc.nasa.gov/Business/DMS/PDF/DCP-S-031.pdf
[DS-00-56]	Defence Standard 00-56, Safety Management Requirements for defence systems containing programmable electronics, 21 September 1999, http://wheelie.tees.ac.uk/hazop/standards/56/lifecyc/zanal.htm
[Dvorak00]	E. Dvorak, Safety assessments for part 23 aeroplanes, Small Airplane Directorate, Regulations and policy branch, FAA, 3 May 2000, av-info.faa.gov/dst/Bostonrec/C1-Dvorak.ppt
[EATMS-CSD]	EATMS Concept and Scope Document (CSD), EATCHIP doc: FCO.ET1.ST02.DEL01, Edition 1.0, 15 September 1995
[ECSS-HSIA96]	ECSS, European Cooperation for Space Standardization, Space Product Assurance, Dependability, ECSS–Q–30A, 19 April 1996, http://dutlsisa.lr.tudelft.nl/seinternet/LIBRARY/ecss-q-30a.pdf
[ED 78A]	ED78A/DO264 -"Guidelines for approval of the provision and use of Air Traffic Services supported by data communications") (12/00)
[Edwards99]	C.J. Edwards, Developing a safety case with an aircraft operator, Proc Second Annual Two-Day Conference on Aviation Safety Management, May 1999
[EEC SRDP]	EUROCONTROL Experimental Centre Safety Research and Development plan 2002-2006+, Edition 1, 1 July 2002, http://www.eurocontrol.fr/ba_saf/EEC_Safety_RD_Plan_1.pdf
[EHQ-MOD97]	EUROCONTROL, Model of the cognitive aspects of air traffic control, Brussels, 1997.
[EHQ-PSSA]	PSSA part of [EHQ-SAM]
[EHQ-SAM]	Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, including Safety Awareness Document edition 0.5 (30 April 1999), Functional Hazard Assessment edition 1.0 (28 March 2000), Preliminary

	System Safety Assessment edition 0.2 (8 August 2002) and System Safety Assessment edition 0.1 (14 August 2002)
[EHQ-TASK98]	EUROCONTROL, Integrated Task and Job Analysis of air traffic controllers, Phase 1, Development of methods, Brussels, 1998.
[EN 50128]	CENELEC (Comité Européen de Normalisation Electrotecnique), European standard Pr EN 50128: Railway applications, Software for railway control and protection systems, January 1996; From the internet: Annex B: Bibliography of techniques, http://www.dsi.unifi.it/~fantechi/INFIND/50128a2.ps
[Endsley95]	M.R. Endsley, Towards a theory of situation awareness in dynamic systems, Human Factors, Vol. 37, 1995, pp. 32-64.
[Enterprise-ORR]	Cotran Technologies, Enterprise Application Software Systems - Operational Readiness Review (ORR) Procedures & Checklists, http://www.cotrantech.com/id127.html, http://www.cotrantech.com/orr_check_process.htm
[ESARR 4]	EUROCONTROL Safety Regulatory Requirement (ESARR), ESARR 4, Risk assessment and mitigation in ATM, Edition 1.0, 5 April 2001, http://www.eurocontrol.be/src/index.html (SRC deliverables).
[ESARR2]	EUROCONTROL Safety Regulatory Requirement, ESARR 2, Reporting and assessment of safety occurrences in ATM, Edition 2.0, Released issue, 3 November 2000.
[ESH-ORR]	ESH 1.3.2 Operational Readiness Review, https://sbms-authqa.bnl.gov/ld/ld08/ld08d071.htm
[Eurocontrol strategy]	EUROCONTROL, ATM Strategy for the Years 2000+, Draft Proposal for an update of Volume 2, Version 1.0a, 02/02/2002, http://www.eurocontrol.int/eatmp/library/documents/ATM2000-Vol2en-10a.pdf
[Everdij&al02]	M.H.C. Everdij, G.J. Bakker & H.A.P. Blom, Estimating safe separation criteria, CARE/ASAS Activity 3: Airborne separation minima, WP3 report, January 2002
[Everdij&Blom02]	M.H.C. Everdij and H.A.P. Blom, Bias and Uncertainty in accident risk assessment, TOSCA-II WP4 final report, 2 April 2002, NLR TR-2002-137, TOSCA/NLR/WPR/04/05/10
[Everdij&Blom03]	M.H.C. Everdij, H.A.P. Blom, Petri nets and hybrid-state Markov processes in a power-hierarchy of dependability models. In: Engel, Gueguen, Zaytoon (eds.), Analysis and design of hybrid systems, Elsevier, pp. 313-318.
[Everdij&Blom04]	M.H.C. Everdij and H.A.P. Blom, Bias and Uncertainty Modelling in accident risk assessment, HYBRIDGE WP8.4, 2004
[FAA SMSM]	US Department of Transportation, Federal Aviation Administration, Safety Management System Manual, Version 1.1, May 21, 2004
[FAA SSMP]	US Department of Transportation, Federal Aviation Administration, NAS Modernization, System Safety Management Program, FAA Acquisition Management System, ADS-100-SSE-1, Rev 3.0, 1 May 2001, http://faculty.erau.edu/fitzg3f9/MAS611/NASModSSMP.pdf; section on HTRR also on FAA Acquisition System Toolset web page, http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10
[FAA SEM]	NAS System Engineering Manual (SEM) Version 2.1, 19 Nov 03
[FAA00]	FAA System Safety Handbook, December 2000, www.asy.faa.gov/RISK/SSHandbook/contents.htm
[Foot94]	P.B. Foot, A review of the results of a trial hazard analysis of airspace sectors 24 and 26S, Civil Aviation Authority CS report 9427, April 1994.
[Fota93]	O.N. Fota, Étude de faisabilité d'analyse globale de la sécurité d'un CCR à l'aide de l'EPS (Evaluation Probabiliste de la Sécurité. Sofréavia, CENA/R93-022, 1993.
[FT handbook02]	W. Vesely et al, Fault Tree Handbook with Aerospace Applications, NASA office of safety and mission assurance, Version 1.1, August 2002, http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

[Garrick88]	B.J. Garrick, The approach to risk analysis in three industries: nuclear power, space systems and chemical process, Reliability engineering and system safety, Vol. 23, pp. 195-205, 1988.
[GenericBT]	http://www.bowtiesystems.snap.net.nz/page7.html
[Gizdayu00]	Adrian Gizdavu; EEC Report N°374/2000, Spata 2000 Real-time Simulation http://www.eurocontrol.int/eec/publications/eecreports/2002/374.htm
[Gordon04]	Rachael Gordon[1], Steven T. Shorrock[2], Simone Pozzi[3], Alessandro Boschiero[4] (2004) Using human error analysis to help to focus safety analysis in ATM simulations: ASAS Separation. Paper presented at the Human Factors and Ergonomics Society 2004 Conference, Cairns, Australia, 22nd - 25th August, 2004.
[Hale97]	Hale, A.R., Heming, B., Carthey, J. and Kirwan, B. (1997) Problem solving cycle model and safety culture. Safety Science, 26, 121 -140.
[Hale98]	Hale, A.R. , Kirwan, B., Guldenmund, F., and Heming, B. (1998) Capturing the river: multi-level modelling of safety management. In Misumi, J., Wilpert, B., and Miller, R. (1998) Nuclear Safety - a Human Factors Perspective. London: Taylor and Francis, pp. 161 - 182.
[Henley&Kumamoto92]	E.J. Henley and H. Kumamoto, Probabilistic Risk Assessment; Reliability engineering, design, and analysis, IEEE Press, 1992
[HFC]	The Human Factors Case: Guidance for HF Integration, Edition No 1, 21 February 2003, Draft; Intended for General Public, www.eurocontrol.int/eatmp/hifa
[HIFA_human]	EUROCONTROL EATMP HIFA data tools: human error, http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_humanerror.html
[Hoegen97]	M. Von Hoegen, Product assurance requirements for first/Planck scientific instruments, PT-RQ-04410 (Issue 1), September 1997, ESA/ESTEC, Noordwijk, The Netherlands, http://www.estec.esa.nl/spdwww/first/docs/pt-04410.pdf
[Holloway89]	N.J. Holloway, Pilot study methods based on generic failure rate estimates, Mathematics in major accident risk assessment. In R.A. Cox, editor, pp. 71-93. Oxford, 1989.
[Houmb02]	S.H. Houmb, Stochastic models and mobile e-commerce: Are stochastic models usable in the analysis of risk in mobile e-commerce?, University College of Østfold, 15 February 2002, http://www.idi.ntnu.no/~sivhoumb/msc_siv_2002.pdf
[Howat02]	C.S. Howat, Hazard identification and Evaluation; Introduction to Fault Tree Analysis in Risk assessment, Plant and Environmental Safety, 2002, http://www.engr.ukans.edu/~ktl/lecture/cpe624/Fault.pdf
[HPMW03]	Proceedings Human Performance Modeling Workshop [Specific focus on controller workload and en route capacity modeling], October 21-23, 2003, NASA Ames Research Center
[Humphreys88]	P. Humphreys, Human reliability assessors guide, Safety and Reliability Directorate UKAEA (SRD) Report No TRS 88/95Q, October 1988.
[ICAO CRM80]	ICAO Manual on the use of the collision risk model (CRM) for ILS operations, 1980, ICAO Doc. 9274-AN/904
[Ippolito&Wallace95]	L.M. Ippolito, D.R. Wallace, A Study on Hazard Analysis in High Integrity Software Standards and Guidelines, National Institute of Standards and Technology, January 1995, http://hissa.nist.gov/HHRFdata/Artifacts/ITLdoc/5589/hazard.html#33_SEC
[JAR25.1309]	Joint Aviation Requirements JAR - 25, Large Aeroplanes, Change 14, 27 May 1994, and Amendment 25/96/1 of 19 April 1996, including AMJ 25-1309: System design and analysis, Advisory Material Joint, Change 14, 1994.
[Kennedy slides]	R. Kennedy, Human Error assessment – HAZOP studies, "hazop.ppt"
[Kennedy&Kirwan98]	R. Kennedy and B. Kirwan, Development of a hazard and operability-based method for identifying safety management vulnerabilities in high risk systems,

	Safety Science 30 (1998) 249-274
[Kennedy]	R. Kennedy, Human error assessment and reduction technique (HEART), "heart.ppt"
[Kirwan&Ainsworth92]	A guide to task analysis, edited by B. Kirwan and L.K. Ainsworth, Taylor and Francis, 1992
[Kirwan&al97]	B. Kirwan, A. Evans, L. Donohoe, A. Kilner, T. Lamoureux, T. Atkinson, and H. MacKendrick, Human Factors in the ATM System Design Life Cycle, FAA/EUROCONTROL ATM R&D Seminar, 16 - 20 June, 1997, Paris, France, http://atm-seminar-97.eurocontrol.fr/kirwan.htm
[Kirwan&al97-II]	B. Kirwan, R. Kennedy, S. Taylor-Adams, B. Lambert, The validation of three human reliability quantifiction techniques – THERP, HEART and JHEDI: Part II – Results of validation exercise, Applied Ergonomics, Vol 28, No 1, pp. 17-25, 1997, http://www.class.uidaho.edu/psy562/Readings/Kirwin%20(1997)%20A%20II.pdf
[Kirwan&Basra&Taylor.doc]	B. Kirwan, G. Basra and S.E. Taylor-Adams, CORE-DATA: A computerised Human Error Database for Human reliability support, Industrial Ergonomics Group, University of Birmingham, UK, "IEEE2.doc"
[Kirwan&Basra&Taylor.ppt]	B. Kirwan, G. Basra and S.E. Taylor-Adams, CORE-DATA: A computerised Human Error Database for Human reliability support, Industrial Ergonomics Group, University of Birmingham, UK, "core-data.ppt"
[Kirwan&Kennedy&Hamblen]	B. Kirwan, R. Kennedy and D. Hamblen, Human reliability assessment in probabilistic safety assessment - guidelines on best practice for existing gas-cooled reactors, "Magnox-IBC-final.doc"
[Kirwan00]	B. Kirwan, SHAPE human error interviews: Malmo and Stockholm, 14-16 November 2000-11-28, "SHAPE Human Error Interviews 1.doc"
[Kirwan94]	B. Kirwan, A guide to practical human reliability assessment, Taylor and Francis, 1994
[Kirwan96-I]	B. Kirwan, The validation of three human reliability quantifiction techniques – THERP, HEART and JHEDI: Part I – technique descriptions and validation issues, Applied Ergonomics, Vol 27, No 6, pp. 359-373, 1996, http://www.class.uidaho.edu/psy562/Readings/Kirwan%20(1996).pdf
[Kirwan97-III]	B. Kirwan, The validation of three human reliability quantifiction techniques – THERP, HEART and JHEDI: Part III – Practical aspects of the usage of the techniques, Applied Ergonomics, Vol 28, No 1, pp. 27-39, 1997, http://www.class.uidaho.edu/psy562/Readings/Kirwin%20(1997)%20A%20III.pdf
[Kirwan98-1]	B. Kirwan, Human error identification techniques for risk assessment of high risk systems – Part 1: Review and evaluation of techniques, Applied Ergonomics, Vol 29, No 3, pp. 157-177, 1998, “HEAJNL6.doc”, http://www.class.uidaho.edu/psy562/Readings/Kirwan%20(1998)%20A%201.pdf
[Kirwan-sages]	B. Kirwan, "bk-sages-template.doc"
[Klein Obbink &Scholte03]	B. Klein Obbink and J.J. Scholte, Safety evaluation for the dependent operation of the southern taxiway and runway 18C/36C, Part 1: Top-level document, NLR contract report CR-2003-513, 2003.
[Kletz74]	T. Kletz, HAZOP and HAZAN – Notes on the identification and assessment of hazards, Rugby: Institute of Chemical Engineers, 1974.
[Kos&al00/01]	J. Kos, H.A.P. Blom, L.J.P. Speijker, M.B. Klompstra, and G.J. Bakker, Probabilistic wake vortex induced accident risk assessment, 3rd USA/Europe Air Traffic Management R&D Seminar, FAA/Eurocontrol, 2000, also in Eds G.L. Donohue, A.G. Zellweger, Air Transportation Systems Engineering, AIAA, 2001. pp. 513-531 http://atm-seminar-2000.eurocontrol.fr/acceptedpapers/pdf/paper56.pdf.
[Kumamoto&Henley96]	H. Kumamoto and E.J. Henley, Probabilistic risk assessment and management

	for engineers and scientists, IEEE, New York, NY, 1996.
[Laughery & Corker, 1997]	R. Laughery and K. Corker, Computer modeling and simulation of human / system performance, In: G. Salvedy, Congnitive engineering handbook, Wiley Interscience, 1997
Laughery, Archer & Corker 2001]	Laughery, R., Archer, S. and Corker, K. (2001). Modeling Human Performance in Complex Systems.In G. Salvendy (Ed.) Handbook of Industrial Engineering. Wiley Interscience.Human Performance Modeling:
[Lawrence99]	B.M. Lawrence, Managing safety through the Aircraft lifecycle – An aircraft manufacturer's perspective, Proc Second Annual Two-Day Conference on Aviation Safety Management, May 1999
[Leveson95]	N.G. Leveson, Safeware, system safety and computers, a guide to preventing accidents and losses caused by technology, Addison-Wesley, 1995
[Lutz&Woodhouse96]	R.R. Lutz and R.M. Woodhouse, Experience report: Contributions of SFMEA to requirements analysis, ICRE 96, April 15-18, 1996, Colorado Springs, CO, http://www.cs.iastate.edu/~rlutz/publications/icre96.ps
[Malhotra96]	Y. Malhotra, Organizational Learning and Learning Organizations: An Overview, 1996, http://www.brint.com/papers/orglrng.htm
[Mana02]	P. Mana, EATMP Safety Management Software Task Force, slides for FAA National Software Conference, May 2002, http://av-info.faa.gov/software/Conf02/Eurocontrol.pdf
[MAS611-2]	Powerpoint slides, www.ec.erau.edu/cce/faculty/mas611-2.ppt
[Matra-HSIA99]	Matra Marconi Space, PID-ANNEX (draft), Documentation requirements description, 11 March 1999, http://www.irf.se/rpg/aspera3/PDF/Doc_Req_Descr_990313.PDF
[MDA press release97]	MDA press release, 27 November 1997, http://www.mda.ca/news/pr/pr71127A.html
[MHF-RGN10]	Major Hazard Facilities Regulations Guidance Note, MHD-GN10, September 2001, http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN10.pdf
[MIL-HDBK-764]	U.S. Military Handbook 764, System Safety Engineering Design Guide for Army Materiel, 12 January 1990
[Minutes SMS]	M.H.C. Everdij, Minutes of 9 July 2002 kick-off meeting Safety Methods Survey project, 16 July 2002, Final.
[Moek84]	G. Moek, "Methoden voor risicobepaling en risico evaluatie", NLR Memorandum MP 84019 U, 1984. (In Dutch)
[Moubray00]	J. Moubray, Reliability-Centered Maintenance, 1999, 2000, http://www.maintenanceresources.com/ReferenceLibrary/RCM/RCM1.htm, http://www.plant-maintenance.com/RCM-intro.shtml, http://www.aladon.co.uk/08ap.html, http://www.aladon.co.uk/02rcm.html
[MUFTIS3.2-I]	M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom, O.N. Fota, MUFTIS work package report 3.2, final report on safety model, Part I: Evaluation of hazard analysis techniques for application to en-route ATM, NLR TR 96196 L, 1996
[MUFTIS3.2-II]	M.H.C. Everdij, M.B. Klompstra and H.A.P. Blom, MUFTIS workpackage report 3.2 Final report on Safety Model Part II: Development of mathematical techniques for ATM safety analysis, NLR TR 96197 L, 1996
[NASA-RCM]	NASA Reliability Centered Maintenance Guide for Facilities and Collateral Equipment, http://www.hq.nasa.gov/office/codej/codejx/rcm-iig.pdf
[NEA98]	Nuclear Energy Agency, Committee on the safety of nuclear installations, Critical operator actions: human reliability modelling and data issues, 18 February 1998, http://www.nea.fr/html/nsd/docs/1998/csni-r98-1.pdf
[NEC02]	The New England Chapter of the System Safety Society, System Safety: A Science and Technology Primer, April 2002, http://ax.losangeles.af.mil/se_revitalization/aa_functions/safety/Attachment/Sys

	tem-Safety-Primer.pdf
[Nijstad01]	B.A. Nijstad, How the group affects the mind: effects of communication in idea generating groups, PhD Thesis Interuniversity Center for Social Science Theory and Methodology (ICS) of Utrecht University, The Netherlands, 2001
[NNSA-ORR]	National Nuclear Security Administration (NNSA) homepage, http://tis.eh.doe.gov/orr/
[Nurdin02]	H. Nurdin, Mathematical modelling of bias and uncertainty in accident risk assessment, MSc Thesis, Twente University, The Netherlands, June 2002, http://www.nlr.nl/public/hosted-sites/hybridge/
[OL glossary]	University of Mannheim Glossary, Organisational Learning entry, 10 November 1997, http://www.sfb504.uni-mannheim.de/glossary/orglearn.htm
[OSTI]	http://www.osti.gov/estsc/PDFs/comcan3.pdf
[Page&al92]	M.A. Page, D.E. Gilette, J. Hodgkinson, J.D. Preston, Quantifying the pilot's contribution to flight safety, FSF 45th IASS & IFA 22nd international conference, pp. 95-110, Long Beach, California, 1992.
[Parker&al91]	R.G. Parker, N.H.W. Stobbs, D.Sterling, A.Azarian, T. Boucon, Working paper for a preliminary study of expert systems for reliability, availability, maintainability and safety (RAMS), Workpackage 5000 final report, 19 July 1991
[Parry92]	G.W. Parry, Critique of current practice in the treatment of human interactions in probabilistic safety assessments. In Aldemir, T., N.O. Siu, A. Mosleh, P.C. Cacciabue, and B.G. Göktepe, editors, Reliability and Safety Assessment of dynamic process systems, volume 120 of Series F: Computer and Systems Sciences, pp. 156-165. Springer Verlag, 1994.
[Pentti&Atte02]	H. Pentti, H. Atte, Failure Mode and Effects Analysis of software-based automation systems, VTT Industrial Systems, STUK-YTO-TR 190, August 2002, www.stuk.fi/julkaisut/tr/stuk-yto-tr190.pdf
[Petrolekas&Haritopoulos 01]	P. D. Petrolekas and P. Haritopoulos, A Risk Management Approach For SEVESO Sites, ABS Group and Shell Gas, Greece, 2001, http://www.microrisk2001.gr/Petrolekas.doc
[Polat96]	M.H. Polat, A Comprehensive Reference List on Organisational Learning and Related Literatures (with special focus on Team Learning), Version: 1.0 – 2, 25 March, 1996, University of Wollongong, Australia, http://engineering.uow.edu.au/Resources/Murat/olref.html
[Rademakers&al92]	L.W.M.M. Rademakers, B.M. Blok, B.A. Van den Horn, J.N.T. Jehee, A.J. Seebregts, R.W. Van Otterlo, Reliability analysis methods for wind turbines, task 1 of the project: Probabilistic safety assessment for wind turbines, Netherlands energy research foundation, ECN Memorandum, 1992.
[Rakowsky]	U.K. Rakowsky, Collection of Safety and Reliability Engineering Methods, http://www.uk-rakowsky.de/ry-mbib.html
[Rausand&Vatn98]	M. Rausand and J. Vatn, Reliability Centered Maintenance. In C. G. Soares, editor, Risk and Reliability in Marine Technology. Balkema, Holland, 1998, http://www.ipk.ntnu.no/fag/SIO3050/notater/Introduction_to_RCM.pdf
[Reason90]	Reason, J.T., Human error, Cambridge University press, 1990.
[Reese&Leveson97]	J.D. Reese and N.G. Leveson, Software Deviation Analysis: A "Safeware" Technique, AIChe 31st Annual Loss Prevention Symposium, Houston, TX March 1997, http://www.safeware-eng.com/pubs/SofDev.shtml.
[Ref. 1].	EUROCONTROL: *"Risk Assessment and Mitigation in ATM"*, EUROCONTROL Safety Regulatory Requirement (ESARR) 4, Edition 1.0, Released Issue.
[Ref. 2].	EUROCONTROL: *"EATMP Safety Policy"*, SAF.ET1.ST01.1000-POL.-01-00, Edition 1.1, August 1999 (supplemented by SAF.ET1.ST.1000-GUI-01-00, Edition 1.2, August 1999)

[Ref. 3].	ICAO RGCSP [Review of the General Concept of Separation Panel] (1995). Working Group A Meeting: Summary of Discussions and Conclusions. ICAO.
[Ref. 4].	EUROCONTROL: *"TLS Apportionment Method"*, Edition 1.0, March 2003.
[Ref. 5].	ICAO, Annex 13 / Doc 9713
[Ref. 6].	Cranfield University: *"Consistent and up-to-date aviation safety targets"*, Draft, Peter Brooker, October 2003
[Ref. 7].	NASA: *"Comments on Principles"*, Irving Statler in his mail to Eurocontrol and FAA dated 2 December 2003.
[Ref. 8].	EUROCONTROL: *"Reporting and assessment of safety occurrences in* ATM*"*, EUROCONTROL Safety Regulatory Requirement (ESARR) 2, Edition 2.0, Released Issue.
[Region I LEPC]	Region I LEPC, California Accidental Release Prevention Program (CalARP), Implementation guidance document, January 1999, http://www.acusafe.com/Laws-Regs/US-State/CalARP-Implementation-Guidance-LEPC-Region-1.pdf
[Relex-RCM]	Relex software website on Reliability Centered Maintenance, http://www.reliability-centered-maintenance.com/
[Review of techniques for SAM, 2004]	EEC, Review of techniques to support the EATMP Safety Assessment Methodology, Volume I and II, EEC Note No. 01 / 04, Project SRD-3-E1, M.H.C. Everdij, January 2004
[Richardson92]	J.E. Richardson, The design safety process, FSF 45th IASS & IFA 22nd international conference, pp. 95-110, Long Beach, California, 1992.
[Roberts&al81]	N.H. Roberts, W.E. Vesely, D.F. Haasl, F.F. Goldberg, Fault tree handbook, U.S. Nuclear Regulatory Commission, NUREG-0492-1981.
[RSC slides]	RSC site, powerpoint slides, Session 3: Solving the plant model & External Events Overview, http://www.rscsite.com/RSC%20Secure%20Site/rsc%20training%20files/RSC%20Training/Session%203%20Overview%20of%20External%20events%20analyses/sld001.htm
[SAE2001]	S. Amberkar, B.J. Czerny, J.G. D'Ambrosio, J.D. Demerly and B.T. Murray, A Comprehensive Hazard Analysis Technique for Safety-Critical Automotive Systems, SAE technical paper series, 2001-01-0674, 2001, http://www.delphi.com/pdf/techpapers/2001-01-0674.pdf
[SAFBUILD web]	EUROCONTROL Experimental Centre, Project SAFBUILD web page http://projects.eurocontrol.fr/consultproject?LOID=6.0.164056, 9 April 2002
[Scaife00]	Scaife, R., Fearnside, P., Shorrock, S.T., and Kirwan, B. (2000) Reduction of separation minima outside controlled airspace. Aviation Safety Management conference, Copthorne Tara Hotel, London, 22-23 May.
[Scholte&al04]	J.J. Scholte, M.H.C. Everdij, M.N.J. Van der Park, J.W. Smeltink, Sourdine II, Safety assessment for approach procedure II-A, Part 1: Main document, Draft version, July 2004
[Seamster&al93]	T.L. Seamster, R.E. Redding, J.R. Cannon, J.M. Ryder, J.A. Purcell, Cognitive Task Analysis of Expertise in Air Traffic Control. The International Journal of Aviation Psychology, 3, 257-283, 1993.
[Seamster&al97]	T.L. Seamster, R.E. Redding and G.L. Kaempf, Applied cognitive task analysis in aviation, 1997.
[SGS-FSR]	SGS Environmental services website, http://www.sgsenvironment.be/sgs/sgsenvir.nsf/pages/swa_vr.html
[SHAPE web]	http://www.eurocontrol.int/humanfactors/shape.html
[Shorrock&Kirwan98]	S. Shorrock and B. Kirwan, The development of TRACEr: Technique for the retrospective analysis of cognitive errors in Air Traffic Management, Powerpoint Slides, Human Factors Unit, NATS, Presented at the Second International Conference on Engineering Psychology and Cognitive

	Ergonomics, 1998, "tracer7.ppt"
[Shorrock01]	S.T. Shorrock, Error classification for Safety Management: Finding the right approach, DNV Ltd, 2001, “error-classification.doc”
[Shorrock05]	Shorrock, S. Kirwan, B. and Smith, E. (2005: in press) Performance Prediction in Air Traffic Management: Applying Human Error Analysis Approaches to New Concepts. In Kirwan, B., Rodgers, M., and Schaefer, D. (Eds) Human Factors Impacts in Air Traffic Management. Ashgate, Aldershot, UK
[SINTEF-RCM]	SINTEF website on Reliability Centered Maintenance, http://www.sintef.no/units/indman/sipaa/prosjekt/rcm.html
[Siu94]	N. Siu, Risk assessment for dynamic systems: An overview, Reliability Engineering and System Safety, Vol. 43, pp. 43-73, 1994.
[Smith9697]	E. Smith, Hazard analysis of route separation standards for EUROCONTROL, DNV Technica, 1996 and 1997
[Sparkman92]	D. Sparkman, Techniques, Processes, and Measures for Software Safety and Reliability, Version 3.0, 30 May 1992, http://fessp.llnl.gov/csrc/files/108725.pdf
[SQUALE99]	SQUALE Evaluation Criteria, January 1999, http://www.newcastle.research.ec.org/squale4.pdf
[Stanton&Wilson00]	N.A. Stanton, J.A. Wilson, Human factors: Step change improvements in effectiveness and safety, Drilling Contractor, Jan/Feb 2000, http://www.iadc.org/dcpi/dc-janfeb00/j-step%20change%20psych.pdf
[Storey96]	N. Storey, Safety-Critical Computer Systems, Addison-Wesley, Edinburgh Gate, Harlow, England, 1996
[Stroeve&al03a]	S. Stroeve, H. Blom, M. Van der Park, Multi-agent situation awareness evolution in accident risk modelling, 5th USA/Europe Air Traffic Management R&D Seminar, Budapest, Hungary, 23-27 June 2003, http://atm2003.eurocontrol.fr/
[Stroeve&al03b]	S.H. Stroeve, H.A.P. Blom, M.N.J. Van der Park, M.H.C. Everdij, Improved bias and uncertainty assessment in accident risk assessment, NLR memorandum LL-2003-013, October 2003.
[Stroup]	R. Stroup, An approach to the software aspects of safety management, FAA, http://www2.faa.gov/aio/common/documents/Safety/SofSafMgmt.pdf
[Technical Annex]	M.H.C. Everdij, Review of techniques to support the EATMP Safety Assessment Methodology, Technical Annex, Safety methods Survey Final report D5, 31 March 2003.
[Terpstra84]	K. Terpstra, Phased mission analysis of maintained systems. A study in reliability and risk analysis, Netherlands energy research foundation, ECN Memorandum, 1984.
[Toola93]	A. Toola, The safety of process automation, Automatica, Vol. 29, No. 2, pp. 541-548, 1993.
[TOPAZ hazard database]	TOPAZ ATM Hazard Database, Database maintained within NLR’s TOPAZ Information Management System (TIMS) containing the hazards identified during ATM safety assessments (contact klomsptr@nlr.nl).
[TRACEr lite_xls]	Excel files "TRACEr lite Excel Predict v0.1 Protected!.xls" and "TRACEr lite v0[1].1 Protected.xls"
[Trbojevic&Carr99]	V.M. Trbojevic and B.J. Carr, Risk based safety management system for navigation in ports, 1999, http://www.eqe.com/revamp/porttechnology.html
[Villemeur91-1]	A. Villemeur, Reliability, availability, maintainability and safety assessment, Volume 1: Methods and Techniques, John Wiley and Sons, Inc., 1991.
[Williams85]	J.C. Williams, Validation of human reliability assessment techniques, Reliability Engineering, Vol. 11, pp. 149-162, 1985.
[Williams88]	J.C. Williams, A data-based method for assessing and reducing human error to improve operational performance, 4th IEEE conference on Human factors in Nuclear Power plants, Monterey, California, pp. 436-450, 6-9 June 1988.
[Zio02]	E. Zio, Common Cause Failures, and analysis methodology and examples, April

	2002, http://www.cesnef.polimi.it/corsi/sicura%5Ccomcaufa.doc
[Zuijderduijn99]	C. Zuijderduijn, Risk management by Shell refinery/chemicals at Pernis, The Netherlands; Implementation of SEVESO-II based on build up experiences, using a Hazards & Effects Management Process, 1999, http://mahbsrv.jrc.it/Proceedings/Greece-Nov-1999/B4-ZUIJDERDUIJN-SHELL-z.pdf.

Appendix A: Analytical Techniques Supporting Analyses of flight recorded data (FOQA, APMS), radar-track data (PDARS), and textual data (e.g., ASRS and ASAP)

There are several systems in place for continuously monitoring system performance that are developing very large databases. These are rich sources of information on safety risks and tools and methodologies have been, and are being, developed to mine these sources. These entail databases of both numerical and textual data. The following tables include descriptions of examples of these databases and some of the tools for their automated analyses.

Air carriers are using systems to monitor, process, and analyze flight-recorded data routinely. In the US, the current techniques are called Flight Operational Quality Assurance (FOQA) programs. In Europe, the same methodologies are called Flight Data Monitoring (FDM). These are based, largely, on the identification of prescribed exceedances (e.g., high rate of rotation during take off, high rate of descent at 1000 feet during landing, or flap positions at high speeds). These are generally referenced in the report from the GAIN Working Group B titled "Guide to methods and tools for Airline Flight Safety Analysis", 2nd edition, June 2003, www.gainweb.org

The Aviation Performance Management System (APMS) is an example of the next-generation of tools for analyzing digital data. The APMS is a suite of tools for assisting the Flight Operational Quality Assurance (FOQA) management teams at the air carriers with the analyses of flight-recorded data to identify unexpected events or trends that could compromise safety of operations. Most of the APMS tools described in Tables A 1 through A-11 have been adapted to radar-track data as well in support of the Performance Data Analysis and Reporting System (PDARS).

A-1. The Morning Report of Atypical Flights

References used:	Key references: • Methods of Multivariate Analysis by Alvin C. Rencher; • APMS SVD Methodology and Implementation by Brett G. Amidan & Thomas A. Ferryman, PNNL Technical Paper. • Clustering Analysis of Digital Flight Data for the Aviation Performance Management System by A.R. Willse et al, PNNL Technical Paper. • Lowest Practical Value (LPV) Methodology by Brett G. Amidan and Thomas A. Ferryman, White Paper. • Applied Regression Analysis, by Draper and Smith. • Performance Envelope Related Data Compression Methodology, by Cooley, Amidan, and Scherrer, PNNL White Paper.
Alternate names:	Aviation Performance Measurement System (APMS)
Primary objective:	Flight Data Analysis tools assist in the routine analysis of flight data generated during line operations in order to reveal situations that require corrective action, enable early corrective action before problems occur, and identify operational trends.
Description:	APMS consists of a suite of Flight Data Analysis tools for data processing and analysis. The statistical analysis tools underlying the display of the Morning Report include:

	- Data Quality Filters: This technique removes bad data, i.e. flight data that are physically impossible. See Table A-2 - Continuous Data Signatures:. This technique summarizes a potentially long string of time series data for a given parameter with a vector with 18 elements by using a regression based moving window. The calculated values are summarized in a matrix that is then available for analyses like clustering and calculating atypicality scores. See Table A-3. - Discrete Data Signatures: This technique produces a summary of the data, which is used in all analysis steps. See Table A-4. - Data Compression Signatures: This technique creates a reduced set of data that is stored in order to perform plots and performance envelopes. It saves the most important data points, such that the amount of error is minimized. See Table A-5. - Clustering: This technique allows for the grouping of similar flights. This allows the flight analyst to focus on studying patterns of flights and not having to study each individual flight. This allows him/her to find and understand the common patterns, as well as identifying the uncommon flight patterns. See Table A-6. - Atypicality scores: This technique identifies flights that are mathematically unusual. It allows the flight analyst to focus on these flights, increasing his/her ability to find concerns in equipment, flight practices, or other unsafe events. Mathematical multivariate methods are used to reduce the size of the data and then measure the distance each flight is from the center of the data, in multi-dimensional data spaces. See Table A-7. - Performance Envelopes: This technique allows the flight analyst to compare atypical flights to typical flights. Individual flights can be overlaid on this plot to show how it differs from the group. See Table A-8. - Least Practical Value: Original analyses showed some atypical flights that had mathematically significant reasons for being atypical, but these reasons were not operationally significant. The Least Practical Value technique aims to minimize these types of findings, allowing the safety analyst to focus on flights atypical for more practical reasons. As such, it removes the effects of non-practical differences between flights within clustering and atypicality score calculations. See Table A-9. - Storymeister: Explains in a written paragraph why a certain flight or cluster has been deemed significantly different from some standard, like the most common 80% of flights, or the most common cluster. See Table A-10.
Applicability range:	The flight data analysis tools of APMS enable users to interpret the safety and efficiency of operations. APMS offers to the air-transport community an open, voluntary standard for flight-data-analysis – a standard that helps to ensure suitable functionality and interchangeability among competing software programs. APMS has the ability to retain de-identified data from all the flights from which the full population can be determined for recorded flight parameters and link this data with other sources of information, such as weather at the time and location of flight events.
Life cycle stage:	Operational
Experience in application to air traffic:	These tools are, for the most part, designed for and are widely used by aviation operators.
Related methods:	There are many commercial Flight Safety Analysis software packages available, such as: - AirFASE (Aircraft Flight Analysis and Safety Explorer) - AGS (Analysis Ground Station) - AVSCAN.flight - British Airways Flight Data Tools - CEFA (Cockpit Emulator for Flight Analysis) - EMS (Event Measurement System) - Flight.Analyst - FlightTracer - FlightViz

	- FltMaster - GRAF (Ground Recovery and Analysis Facility) - GRAF-VISION Flight Data Animator - LOMS (Line Operations Monitoring Systems) - RAPS (Recovery, Analysis & Presentation System) - SAFE (Software for Flight Exceedance) For more details of these packages see GAIN.
Availability and tool support:	APMS is suite of tools developed within a National Aeronautics and Space Administration (NASA) funded program to develop advanced software analysis tools to ease the large-scale implementation of flight-data analyses within each of the air transport users. As a government R&D project, APMS is not a commercially-available package, but a developer of technologies implemented at carriers participating in Space Act Agreements, and transferred to the FOQA software vendor community. This partnering relationship is made available by the Space Act of 1958, and serves to protect the confidentiality of data accessed through this research.
Maturity:	Mature are: Clustering, Discrete Data Signatures Fairly mature are: Atypicality Scores, Performance Envelopes, Continuous Data Signatures, Data Compression Signatures, Data Quality Filters Young are: Storymeister, Least Practical Value
Acceptability:	The mature techniques are largely accepted and commonly used. The other techniques are currently in evaluation of acceptability in an operational environment.
Ease of integration:	All techniques are relatively easy to use
Documentability:	The documentability of all techniques ranges from moderate to high.
Advantages:	Flight Data Analysis tools allow to systematically evaluate large flight data sets
Disadvantages:	In general, there is a need for many flights in order to make Flight Data Analysis more useful

A-2. Data Quality Filters

References used:	References to books and papers used for the assessment of the technique
Alternate names:	None
Primary objective:	Remove bad data
Description:	This technique removes flight data that are physically impossible.
Process steps:	1) Create a data quality limits table that contains the largest possible value, smallest possible value, and the largest possible rate of increase or decrease in the value; 2) Remove data that are smaller than the smallest value and the data that are larger than the largest value; 3) Identify when there is a difference of, say, delta between consecutive data points that is larger than the largest possible delta.
Applicability range:	This technique assesses equipment operations.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has been applied to air traffic radar-track data.
Related methods:	None
Availability and tool support:	This technique is currently incorporated within the APMS Morning Report Tool.
Maturity:	This technique is fairly mature in its development and has been useful in creating performance envelopes within the APMS Morning Report Tool.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to use and understand.
Documentability:	Documentability is moderate. The results are consistent.
Advantages:	This technique removes bad data, so that atypical flights will not be atypical due to bad data.
Disadvantages:	This technique requires a flight analyst's knowledge in order to produce the data quality limits table.

A-3. Continuous Data Signatures

References used:	Applied Regression Analysis, by Draper and Smith. APMS SVD Methodology and Implementation by Brett G. Amidan & Thomas A. Ferryman, PNNL Technical Paper.
Alternate names:	None.
Primary objective:	This technique summarizes a potentially long string of time series data for a given parameter with a vector with 18 elements.
Description:	Using a regression based moving window, this technique creates a summary of time series data from many flight parameters. The calculated values are summarized in a matrix that is then available for analyses like clustering and calculating atypicality scores.
Process steps:	1) Loop through each flight parameter (with continuous data) and do the following: 2) At each second calculate a 2^{nd} order regression equation and store the a, b, c, d values; 3) Within each flight phase, summarize the a, b, c, d values by finding the min, max, mean, and standard deviation, as well as the start and end parameter values for the phase.
Applicability range:	This technique assesses equipment.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has been applied to air traffic radar-track data.
Related methods:	None
Availability and tool support:	This technique is currently incorporated within the APMS Morning Report Tool.
Maturity:	This technique is fairly mature in its development and has been useful in finding atypical flights within the APMS Morning Report Tool.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to use, but a little more difficult to understand.
Documentability:	Documentability is moderate. The results are consistent.
Advantages:	This technique produces a summary of the data, which is used in all of the analyses.
Disadvantages:	Creates a summary of the data, instead of something that could reproduce the data.

A-4. Discrete Data Signatures

References used:	None
Alternate names:	None
Primary objective:	This technique summarizes a potentially long string of time series data for a given discrete parameter with a vector. A discrete parameter is a parameter with a result that is a state or level.
Description:	This technique summarizes the characteristics of each discrete parameter over time.
Process steps:	1) Loop through each discrete parameter and do the following: 2) Calculate the proportion of time spent in each state; 3) count the number of times one state transitioned to another step, keeping track of which transition went to which. 4) Record these findings in a vector to be combined with the continuous data signatures.
Applicability range:	This technique assesses equipment.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has not previously been applied to air traffic data because discrete data have not yet existed in the database.
Related methods:	None
Availability and tool support:	This technique is currently within the APMS Morning Report Tool.
Maturity:	This technique is fairly mature in its development and has been useful in finding atypical flights within the APMS Morning Report Tool.
Acceptability:	This technique has not gone through any outside evaluation of acceptability. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to use, but a little more difficult to understand.
Documentability:	Documentability is moderate. The results are consistent.
Advantages:	This technique produces a summary of the data, which is used in all of the analyses.
Disadvantages:	Creates a summary of the data, instead of something that could reproduce the data.

A-5. Data Compression Signatures

References used:	Performance Envelope Related Data Compression Methodology, by Cooley, Amidan, and Scherrer, PNNL White Paper.
Alternate names:	PLI (Progressive Linear Interpolation); LI Comp (Linear Interpolating Leader)
Primary objective:	This technique creates a reduced set of data that is stored in order to perform plots and performance envelopes.
Description:	This technique reduces the amount of data points per parameter from thousands to only around 200. It saves the most important data points, such that the amount of error is minimized.
Process steps:	1) Perform a regression fit between the start and end values (same thing as drawing a straight line between the two points); 2) Find the data point that is furthest from the line; 3) Establish that as a data compression point and perform a regression between each pair of consecutive points; 4) Repeat steps 2 and 3 until your total error is below a desirable point, or until you've iterated it a specified amount.
Applicability range:	This technique assesses equipment.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	The application of this technique to air traffic data has not been warranted because radar-track data are only recorded every 5 to 60 seconds.
Related methods:	None
Availability and tool support:	This technique is currently within the APMS Morning Report Tool.
Maturity:	This technique is fairly mature in its development and has been useful in creating performance envelopes within the APMS Morning Report Tool.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to use and understand.
Documentability:	Documentability is moderate. The results are consistent.
Advantages:	This allows for less data storage and less data to process for plots.
Disadvantages:	This is not meant to reproduce the actual raw data, but instead to generalize it for plotting.

A-6. Clustering

References used:	Methods of Multivariate Analysis by Alvin C. Rencher; Clustering Analysis of Digital Flight Data for the Aviation Performance Management System by A.R. Willse et al, PNNL Technical Paper.
Alternate names:	Kmeans; Hierarchal clustering
Primary objective:	To mathematically assign flights to similar groups.
Description:	This technique collects similar flights into groups according to the data recorded for each flight. Most clustering algorithms need to be told how many groups to have. There are many methods for determining the number of clusters needed, however, they each have their problems. This method uses the square root of the number of flights for a general rule.
Process steps:	1) Perform Principal Component Analysis on original data matrix; 2) Identify initial centroids for each cluster; 3) Assign each flight to the cluster that it is closest to; 4) Iterate the process as wanted.
Applicability range:	This technique assesses equipment operations, although it could be extended to other subject areas.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has been applied to air traffic radar-track data.
Related methods:	None.
Availability and tool support:	Clustering techniques are widely available in many analytical softwares, including Matlab, SAS, and S-Plus. C++ and other computer language clustering routines commonly exist.
Maturity:	This technique is mature.
Acceptability:	This technique is largely accepted and is commonly used.
Ease of integration:	The technique is generally easy to use and understand, although the underlying mathematics may be difficult to understand.
Documentability:	Documentability is high. Results are consistent, as long as the same method is used. There are many different clustering methods and they commonly give results that contain some differences.
Advantages:	This technique allows for the grouping of similar flights. This allows the flight analyst to focus on studying patterns of flights and not having to study each individual flight. This allows him/her to find and understand the common patterns, as well as identifying the uncommon flight patterns.
Disadvantages:	There is a need for many flights, in order to make this technique more useful.

A-7. Atypicality Scores

References used:	Methods of Multivariate Analysis by Alvin C. Rencher; APMS SVD Methodology and Implementation by Brett G. Amidan & Thomas A. Ferryman, PNNL Technical Paper.
Alternate names:	Anomalator; Mahalanobis Distance
Primary objective:	To mathematically find atypical flights using multivariate data
Description:	Mathematical multivariate methods are used to reduce the size of the data and then measure the distance each flight is from the center of the data, in multi-dimensional data spaces. Flights with the largest distances are considered most atypical.
Process steps:	1) Perform Principal Component Analysis on original data matrix; 2) Calculate atypical scores by finding the Mahalanobis Distances for each flight; 3) Order flights according to the atypicality scores.
Applicability range:	This technique assesses equipment operations, although it could be extended to other subject areas.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has been applied to air traffic radar-track data.
Related methods:	None.
Availability and tool support:	This technique is currently incorporated within the APMS Morning Report Tool for flight-recorded data.
Maturity:	This technique is fairly mature in its development and has been useful in finding atypical flights within the APMS Morning Report Tool.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to understand and use.
Documentability:	Documentability is moderate. The results are consistent.
Advantages:	This technique identifies flights that are mathematically unusual. It allows the flight analyst to focus on these flights, increasing his/her ability to find concerns in equipment, flight practices, or other unsafe events.
Disadvantages:	There is a need for many flights, in order to make this technique more useful.

A-8. Performance Envelopes

References used:	None
Alternate names:	Cluster Trend plots
Primary objective:	Graphically show the trends of a group of flights over time for a given flight parameter. Individual flights can be overlaid on this plot to show how it differs from the group.
Description:	A description of the process which must be followed to apply the technique. This description is a digest of information drawn from the references, coupled with advice from those who have practiced the use of the technique
Process steps:	1) Create a contouring image plot over time summarizing the location of the group of flights in a given flight phase, this creates the performance envelope for the group; 2) Plot any flights of interest against this performance envelope plot.
Applicability range:	This technique assesses equipment operations.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has been applied to air traffic radar-track data.
Related methods:	Contour plots; time series plots.
Availability and tool support:	This technique is currently incorporated within the APMS Morning Report Tool.
Maturity:	This technique is fairly mature in its development and has been useful in graphically displaying atypical flights within the APMS Morning Report Tool.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to understand and use.
Documentability:	Documentability is moderate. The results are consistent.
Advantages:	This technique graphically displays flights that are mathematically unusual. It allows the flight analyst to focus on these flights as compared to typical flights, increasing his/her ability to find concerns in equipment, flight practices, or other unsafe events.
Disadvantages:	There is a need for many flights, in order to make this technique more useful.

A-9. Least Practical Value

References used:	Lowest Practical Value (LPV) Methodology by Brett G. Amidan and Thomas A. Ferryman, White Paper.
Alternate names:	LPV
Primary objective:	This technique removes the effects of non-practical differences between flights within clustering and atypicality score calculations.
Description:	Whenever flight data are scaled and centered, there is a possibility that the scaled values may be large, but with an actual value difference that is small and not practically significant. This technique reduces the mathematical significance so that non-practical differences have minimal influence on the analysis.
Process steps:	1) With help from a flight analyst, record the smallest value (referred to as least significant differences) for each parameter that would be considered a significant difference (for example an airspeed difference of 1 knot would not be important, however an airspeed difference of 5 knots would); 2) During any statistical method that requires centering and scaling (i.e. PCA or Z-scores), perform the LPV method instead of the usual centering to 0 and scaling to 1 standard deviation.
Applicability range:	This technique assesses equipment operations.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has been applied to air traffic radar-track data.
Related methods:	None
Availability and tool support:	This technique is currently incorporated within the APMS Morning Report Tool.
Maturity:	The technique is young in its maturity.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to understand and use.
Documentability:	Documentability is high. The technique produces consistent results as long as the least significant differences do not change.
Advantages:	Original APMS atypicality analyses showed some atypical flights that had mathematically significant reasons for being atypical, but these reasons were not significant to the flight analyst. This technique has helped to minimize these types of findings, allowing the safety analyst to focus on flights atypical for more practical reasons. Technique is quick and transparent to the user.
Disadvantages:	Technique requires least significant differences to be recorded for each flight parameter to be effective. If none are given, then method defaults to using traditional centering and scaling.

A-10. Storymeister

References used:	None
Alternate names:	Rationale
Primary objective:	This technique results in a written paragraph explaining why a certain flight or cluster has been deemed significantly different from some standard, like the most common 80% of flights, or the most common cluster.
Description:	This technique requires a vocabulary look-up table containing the proper wording to be included in the resulting sentences.
Process steps:	1) Identify the population to be compared to the flight or cluster of interest; 2) Determine which flight parameters the flight or cluster of interest have been found to be significantly different than the population; 3) Use a vocabulary look up table to form sentences explaining the differences and assemble these in a paragraph.
Applicability range:	This technique assesses equipment operations, although it could be extended to other subject areas.
Life cycle stage:	Doesn't apply.
Experience in application to air traffic:	This technique has not been applied to air traffic radar-track data, although it is planned to have this capability available by the end of the FY 2004.
Related methods:	None.
Availability and tool support:	This technique is currently incorporated within the APMS Morning Report Tool for comparisons of individual flights to the most common 80% of flights.
Maturity:	The technique is young in its maturity.
Acceptability:	This technique is currently in evaluation of acceptability in an operational environment. Code and results have been internally reviewed and results have appeared reasonable.
Ease of integration:	This technique is relatively easy to understand and use.
Documentability:	Documentability is moderate. Results are consistent, however, as flight parameters change, the vocabulary needs to be updated.
Advantages:	This technique allows for the flight analyst to have a written paragraph explaining what makes a flight or cluster different, instead of having to rely on reading statistical output and graphs.
Disadvantages:	Difficult to make sentences that are grammatically correct.

A-11. Automated Search for Prescribed Parameter Patterns

References used:	Not applicable
Alternate names:	Pattern Search
Primary objective:	Enable search of any portion of a database of flight parameters for any pattern or time sequence of patterns.
Description:	The tool provides a method of constructing user-defined "modules" that include prescribed flight-performance criteria for sets of parameters. Each of these modules can be assigned a value by airline subject-matter experts that relate to the severity of the risk associated with specified criterion. One or more of these modules may constitute a search pattern. A search produces a list of flights that match the prescribed search pattern. Once matching flights are located, a parameter viewer can be used to examine flight parameters in detail. There are numerous situations in which this type of flight search capability may prove invaluable. For example, using the Pattern Search Tool, it is possible to locate flights exhibiting similar characteristics to a selected flight under analysis. By examining similar flights it may be possible to generalize and understand causal factors leading to observed unsafe operating conditions. This capability can also be used to help airline personnel investigate specific hypotheses about safety and operations by querying the flight database. These hypotheses may be formulated based on anecdotal evidence and require hard data to confirm or refute.
Process steps:	The user specifies an event frame (time, event, altitude, or flight phase range), and a series of constraints (such as a parameter value exceeding some procedural criterion) into modules. Each module is assigned a risk index. Several modules are then combined to form a pattern. For example, for an unstable approach, modules examine each flight from 1000 feet above the runway to touchdown for airspeed greater than Vref +25, vertical speed greater than 1500 fpm down, flaps or gear not at their landing setting, engine power below approach setting, and localizer or glide slope deviations greater than one dot. Pattern Search identifies each flight triggering one or more modules.
Applicability range:	Applicability of Pattern Search is fairly broad, as it searches for potential precursor events that may stem from human actions, equipment deficiencies, or organizational characteristics.
Life cycle stage:	Pattern Search may be applied whenever data is collected in testing or operations.
Experience in application to air traffic:	No.
Related methods:	
Availability and tool support:	This criterion indicates that the technique is either available, or else it is unavailable because it has been discontinued, commercially related to one organisation and not generally available, or still at the prototype stage and not yet generally available. The criterion also covers the availability of computer tools that can support application of the technique.
Maturity:	Though NASA pioneered this tool, nearly all COTS vendors now have a similar function.
Acceptability:	In some cases evaluation studies of techniques have been carried out by regulatory authorities (notably the US Nuclear Regulatory Commission) which indicates some degree of approval for techniques which have been given positive evaluations. Techniques that

	have achieved positive evaluations will receive a higher rating on this criterion. This criterion will also be influenced by the theoretical rigour of a technique and the extent to which it has been subjected to objective evaluations. Finally, it covers numerical accuracy of the results produced.
Ease of integration:	Does the technique easily or usually combine with particular other techniques (e.g. in the SAM)? This criterion also covers complexity: the technique is relatively easy to understand and use.
Documentability:	High
Advantages:	The ability to define new patterns dynamically and search through a circumscribed set of flights is crucial for the kinds of exploratory analysis that safety personnel indicate they wish to conduct. It is not feasible to anticipate all of the potential patterns of interest in advance, so an ability to search dynamically 'on the fly' is critical.
Disadvantages:	Requires data from testing or operations.

There are even larger databases of textual data that are the best available sources of information about why an incident occurred. One example of such a database is the Aviation Safety Reporting System (ASRS) of voluntarily submitted confidential reports from all segments of the aviation community on events and incidents in the aviation system. (See Table A-12 below.) ASRS has been an extremely successful operation for over 28 years and currently has over 120,000 reports in this database. There are many commercial-off-the-shelf text analysis tools available. The ones described in Tables A12 through A-14 below are some examples of recent developments of some powerful tools based on combinations of statistical methods and natural language processing for extracting and merging information from such textual databases.

A-12. Analysis of Unstructured Text

References used:	• Everitt BS, S Landau, and M Leese. 2001. Cluster Analysis. Edward Arnold Ed. 4th edition • Daly DS, TA Ferryman, AR Chappell, AR Willse, and SK Cooley. 2000. *Analysis and Transformation of Aviation Safety Vocabularies for Rotary-Wing Aircraft*. PNWD-3071, Battelle Pacific Northwest Division, Richland, Washington. • Schutze H, DA Hunt, and JO Pedersen. 1995. "A Comparison of Classifiers and Document Representations for the Routing Problem." In *Proceedings of the 18th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, Seattle, Washington, July 9-13, pp. 229–237. ACM Press, New York. • Viane S, R Derrig, B Baesens, and G Dedene. 2002. "A comparison of state-of-the-art classification techniques for expert automobile insurance fraud detection." *Journal of Risk and Insurance* 69(3):373–421. • Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics and Speech Recognition Daniel Jurafsky, James H. Martin; Prentice Hall, 2000. • Manning, C. D., H. Schutze, Foundations of statistical natural language processing, The MIT Press, London England, 1999. • Posse, C.; A. White; B. Lindberg; A. Swickard; B. Amidan; T. Ferryman, 2003, An investigation into the Ability To Identify Candidate ASRS Reports for Alert Messages, PNWD-3343, Battelle Pacific Northwest Division, Richland, Washington. • And others
Alternate names:	Text Mining, Exploratory Data Analysis of Free Text, NLP, Bag-of-words
Primary objective:	Work the computer to review the corpus of documents, enable the user to get a broad survey of the nature of the documents in the corpus, find other documents that are similar to a specific document or a inquiry, categorize/classify the documents in to existing categories, monitor trends in time. Additionally to investigate a text based database to identify concepts and relate them to an envisioned scenario model including human behavior and contextual factors.
Description:	Collect a set of documents in the computer. Determine if the desire is to have the investigation be data-driven or expert-opinion driven. If data-driven, determine methods that can guide the investigation to reflect the user's perspective, without overwhelming the data signature. If the expert-opinion is to drive the analysis, key characteristics need to be determined and defined.
Process steps:	A loose conceptual description follows. Significant and important variations can be encounter in practice. The first process described is characterized as statistical analysis or bag-of-words process: 1. Collect the set of documents to be investigated, 2. Convert to a convenient format (such as ASCII or XML), 3. Create a document vs. term matrix where the rows represent each document and the columns are different terms (possibly all unique terms or an intelligently selected subset of terms) 4. Transform the Doc-Term matrix to characterize the underlying nature of the document in a manner that is more suitable for analysis. This might be simply: (a) word frequency, (b) word rate, (c) existence of a word), or more complex transformations 5. Use a clustering, classification, and/or distance measure depending on the mission of the investigation. Candidate methods include: k-means clustering, hierarchical clustering, linear discriminate analysis classification, logistic regression for classification, Mahalanobis distance for inquiries, and /or cosine distance

	measures for inquirers. 6. Present the results using, tables, figures, graphs, and/or interactive software. The next process described is characterized as NLP (Natural Language Processing): 1. Determine the factors to capture in the reports. 2. For each factor a spreadsheet is circulated amongst experts to identify phrases that indicate the presence of the factor. 3. Identify additional natural expressions for each of the factors, possibly using tools such as GREP or WordNet 4. Identify reports with the concepts of interest. We use GATE software. A key task is to create JAPE computer code to capture all the variations on the natural expressions. 5. The performance of the code is tested against human subjects and revised as needed. 6. Process all the reports through the GATE processing and the result is a matrix with identifies what concepts were associated with which reports.
Applicability range:	The techniques can be used to investigate: human error, human behavior, equipment (hardware, software, including HMI) performance, organization behavior and countless other fields of interest that have text (even non-English). The technique assesses human error and human behavior and context factors that can lead to anomalous situations.
Life cycle stage:	NA
Experience in application to air traffic:	The technique has been applied to aviation safety but not real-time air traffic control or air traffic management?
Related methods:	This technique can relate to Natural Language Processing (NLP), analysis of numeric, and categorical data. This technique can work with many mathematical/statistical data analysis tools to detect patterns, atypical events, trends over time and pre-cursor events.
Availability and tool support:	The tool set is still at the prototype stage and not yet generally available. The tools set is moving toward a maturity that is more appropriate to share, but not ready yet. Other domains need to motivate that growth. Regarding NLP: The technique is under development and is leveraging of current research that is being undertaken at Battelle PNWD to push the limits of NLP. Software and that supports the work is GATE/JAPE for information extraction, WordNet for identifying synonyms, and GREP for searching on specific words.
Maturity:	The technique is probably around a TRL 4-7. It has been used on real world data and the results viewed as useful by domain experts. It has not been rehosted for independent operation from the creating team. These techniques have been developed and applied to other applications and proven useful.
Acceptability:	The acceptability of the tool set is as judged by domain safety is appropriate for its level of development, but not ready for independent use. No formal testing and assessments have occurred.
Ease of integration:	The tool set can be integrated with other tools with modest effort.
Documentability:	The tool set is considered at a research-code-level. Documentation is minimal.
Advantages:	There are 100,000+ incident reports in the ASRS database. This tool can provide a user with a good understanding of the general nature of the incidents by creating clusters of similar reports and presenting keywords and synopses for the user to read instead of hundreds. An introduction to the nature of the reports could occur in a few hours instead of months. The report can perform automatic classification of the reports in any of numerous different categories that could be set up to represent human error, equipment failure, weather issues, etc. (Examples focus on aviation related issues, but could be refocused to other domains.) The technique can find similar reports. For instance, an accident report can be submitted and find numerous incident reports that are similar and

	provide the safety expert with a broad understanding of the information in the ASRS database. This capability could be reapplied to nearly any domain with a collection of unstructured text documents.
Disadvantages:	The key disadvantage is it is not fully mature and ready for application to a variety of domains. Also, some "tuning" or guiding by the user can help focus the investigations from the perspective of the user. (This capability could be developed but has not, as of yet.)

A-13. PLADS

PLADS	
References used:	No books or papers were directly referenced for this work. General background material include: • Manning, Christopher D. and Hinrich Schültze. Foundations of Statistical Natural Language Processing, MIT Press. 2000
Alternate names:	None
Primary objective:	To standardize the vocabulary of the unstructured text being analyzed.
Description:	PLADS is composed of software (Java, Matlab, and Perl) and lexicons. PLADS is designed to: • **P**hrases identified and concatenated. Identify phrases in the unstructured text by statistical means by identify 2-, 3-, 4-, 5-word strings that occur more often that one would expect based solely on the individual word frequency. Then concatenate the phrase together in to what would be identified as a single word to subsequent software: e.g.; ClassCAirspace, UnitedStatesOfAmerica. • **L**eave some words unprocessed • **A**ugment some words to make the meaning more useful for computer analysis by subsequent software. Some words have "too much" information; that is they may be abbreviations for instruments and/or concepts with made/model/series, or numeric values of selected concepts. Examples include: o "B-757-300" might be augmented with the word "airplane" o "FL28" ("FL26", "FL30") means "flight level at approximately 28,000 (26,000, 30,000) feet". Augmenting with "FlightLevel" enables subsequent software to identify these 3 (and others) relate to a flight level concept and leave the refinements of which flight level to finer grain analysis. o "24L", "24R", "25L", "25R" all relate to runways. Augmenting with the word "runway" enables the software to capture that concept. o Proper names are often augmented with the more general concept; e.g. "Dallas" augmented with "city" o Airport abbreviations are often augmented with the word "airport"; e.g. "LAX", "ORD", "DFW" • **D**elete some words to simply the analysis. These are often called "stop" words. Examples include: "the", "a", "an". Some times numbers are dropped out. • Substitute some words for others. Often there are many ways to express the same concept. This includes synonyms, abbreviations, jargon, and slang. For example "pilot" might be substituted for these words: "pilot", "pilots", "co-pilot", "captain", "co-captain", "left seater", "PIC", "Pilot-in-Charge", "plt", and "plts". Standard abbreviations can be checked and full meanings substituted. Numbers that are spelled out may be replaced by the numeral.
Process steps:	1. Identify corpus for vocabulary standardization. 2. Pre-process unstructured text through the Phrase identification code 3. Define lexicons using past lexicons, updating them, or creating new lexicons.

	4. Run the PLADS software referencing the corpus and lexicons expressions.
Applicability range:	The technique does not directly assess anything. It can facilitate other software analysis that might include efforts to identify human error and human behavior and context factors that can lead to anomalous situations.
Life cycle stage:	The technique can be used in conjuncture with other text analysis tools by diverse projects through their life cycle; during research to identify applicable reference documents in pre-design, design, production, maintenance, and decommissioning.
Experience in application to air traffic:	The technique previously been never been applied directly to air traffic or air traffic management.
Related methods:	PLADS is intended as a pre-processing for use by statistical (e.g.; bag-of-words) and NLP (Natural Language Processing) tools. (e.g.; Table A-14)
Availability and tool support:	The technique has been developed to about the TRL 6-7. It has not been necessary for the primary tasks that it supports to take it to a higher level. The software and lexicons are documented as appropriate for R&D projects.
Maturity:	The technique has been used on a few different unstructured corpora and in conjunction with both statistical and NLP analysis techniques. The software is moderately mature. The lexicons could be considered marginally mature; in that refines can always enhance their effectiveness. Application to different domains warrant enhancing or replacing the existing lexicons.
Acceptability:	The process is straight-forward and deemed accurate to the limits of the lexicons. "Certification" is not applicable.
Ease of integration:	The technique is easily incorporated in other text analysis processes as a front end processor to standardize the language. It can create XML tags.
Documentability:	The technique is documented as appropriate for R&D efforts and TRL 6-7. It is, for the most part easy to use, with only one or two areas with even modest complexity. It has been ported to a different location for use by other software people with minimal effort.
Advantages:	Currently all (almost all) organizations have receives hundreds, thousands or even millions of reports with massive amounts of information in unstructured text. Access to the insight that could be gained based on that information is generally considered to be very valuable. However the cost of generating the insight via human review of the reports is prohibitive. This has lead to the use of computerized tools to analyze the massive corpora. Often this has resulted in considerable insight. Unfortunately, this has also lead to uninformative analysis. On numerous occasions this is due to the failure to standardize the vocabulary. PLADS was created in response to that exact problem. After pre-processing the text data, analysis was fruitful. This tool was developed for NASA's Aviation Safety program but is useful to nearly any unstructured text analysis problem.
Disadvantages:	The lexicons require human effort when applied to a new domain for the first time. To get significant benefits, we generally recommend an investment of about 100 hours by a domain expert and PLADS knowledgeable expert.

A-14. GATE

Natural Language Processing using GATE	
References used:	No books or papers were directly referenced for this work. General background material include: • Manning, Christopher D. and Hinrich Schültze. Foundations of Statistical Natural Language Processing, MIT Press. 2000
Alternate names:	NLP, GATE, GATE/JAPE, PLADS/GATE, PLADS/GATE/JAPE
Primary objective:	To identify evidence of specific concepts contained in unstructured text data (such as ASRS reports). The concepts may be vaguely defined, and phrased in text in a way as to require subtle insight to identify their existence.
Description:	Concepts are conceived of and defined by domain experts. A seed set of natural language expressions are identified for each concept based on expert judgment and enriched by text mining. A corpus of unstructured text data is identified. It will often be pre-processed through PLADS (see Table A-13) for vocabulary standardization. Natural language phrases are identified using GATE (a software package from University of Sheffield (United Kingdom) that acts as a sort of *software architecture for language engineering* and provides framework for text mining and the ability to apply customizable tools for data mining. Two of the capabilities that are used are Gazetteer and JAPE rules. These enable specific concepts to be identified even if they are expressed in unenvisioned phrases, but identifying synonyms and Boolean expressions that identify the expression. One written the GATE processing can be applied to 1 or a million documents. It can be modified and/or extended as appropriate for the investigation in work. The code is validated by comparing the judgments of experts with the performance of the computer tool for a sample of reports.
Process steps:	5. Identify corpus for analysis. 6. Determine the concepts to be identified and several sample phrases or key words that relate to the concept. This is done by both domain and NLP experts. 7. Use text mining techniques, such as GREP, to identify additional natural expressions for each of the factors. 8. Apply PLADS (Table A-13). (This is optional but performance is expected to be enhanced by doing so.) 9. Create synonyms via the Gazetteer, as appropriate. 10. Write JAPE computer code to capture a wide set of variations on the natural expressions. 11. Assess the performance of the code by both domain and NLP experts reviewing the results and revised codes as needed.
Applicability range:	The technique can identify concepts in unstructured text. Domain experts can look at which concepts are identified for which reports and assess if that indicates human error and/or specific kinds of human behavior that, in some context factors, might lead to anomalous situations. Concepts (and example quotes from the text to facilitate concept understanding) that this technique as been applied to and demonstrated to be effective on include: • Attitude - Any indication of unprofessional. ("contributing factor was complacency flying a very familiar approach, also it was our last leg get thereitis.") • Communication Environment - Interferences with communications. ("We were unable to hear because traffic alert and collision avoidance system was very loud.")

	• Duty Cycle - A strong indication of an unusual duty cycle. ("Flight had previously been delayed and we had minimum rest period coming up, less than 9 hours.") • Familiarity - Any indication of a lack of familiarity (factual knowledge as opposed to proficiency). ("Both pilots were unfamiliar with the airport.") • Illusion - Any indication of an illusion. ("I was flying and was experiencing a black hole effect.") • Physical Environment - Unusual physical conditions. ("This occurred because of the intense glare of the sun.") • Physical Factors - Pilot ailment. ("I allowed fatigue and stress to cloud my judgment.") • Preoccupation - A preoccupation, distraction, or division of attention. ("My attention was divided inappropriately.") • Pressure - Psychological pressure. ("I felt rushed to complete the checklist in time.") • Proficiency - A general deficit in capabilities such as inexperience. ("The biggest safety factor here is the lack of adequate training in the newer autopilot system.") • Resource Deficiency - Absence, insufficient number, or poor quality of a resource. ("Later I learned the minimum equipment list was wrong.") • Taskload - Indicators of a heavy workload. ("Due to high workload, I forgot to switch to tower.") • Unexpected - Something sudden and surprising. ("Had we known of him prior to takeoff we would have made adjustments.") This is in no way an indication of the limitations of the technique, but rather an indication of the subtleness of the concepts identified. There is virtually no limit to the breadth of concepts that can be investigated and successfully identified. The limits to the ability to identify subtle expressions of a given concept has not be defined or even approached.
Life cycle stage:	The technique can be used by diverse projects through their life cycle; during research to identify applicable reference documents in pre-design, design, production, maintenance, and decommissioning. Corpora that might be investigated include, but are not limited to: • Technical publications of diverse scientific domains to identify specific topics and/or concepts of interest • Lessons Learned from previous projects that document project management issues • Maintenance reports that identify specific symptoms to the results of investigations to the final corrective actions taken. • Investigations of EPA standards for regulations relating to specific decommissioning activities.
Experience in application to air traffic:	The technique previously been never been applied directly to air traffic or air traffic management.
Related methods:	Statistical analysis, often called Bag-of-words, techniques provide a different approach means to text analysis. It may be effective, but NLP via GATE is believed to be more effective at identifying specific concepts. There are numerous other methods of doing NLP without using GATE. GATE had great success at TREC (Text REtrieval Conference series) co-sponsored by NIST, Information Technology Laboratory's (ITL) Retrieval Group of the Information Access Division (IAD), and ARDA of the DOD in direct head-to-head competition with numerous other techniques.
Availability and	The specific use of GATE to do NLP to identify specified concepts is under

tool support:	development and is leveraging of current research that is being undertaken at PNWD to push the limits of NLP. Software and that supports the work is GATE/JAPE for information extraction, WordNet for identifying synonyms, and GREP for searching on specific words, all of which are available to the public.
Maturity:	This technique is still relatively immature. It has been successfully applied to 13 concepts and one data set (ASRS reports). It is approximately at the TRL 5-6 level.
Acceptability:	The accuracy, (false positive and false negative rates) has not been measured.
Ease of integration:	The use of GATE enables additional techniques to be incorporated with moderate ease.
Documentability:	The technique has not been documented other that as appropriate for R&D explorations.
Advantages:	Currently all (almost all) organizations have receives hundreds, thousands or even millions of reports with massive amounts of information in unstructured text. Access to the insight that could be gained based on that information is generally considered to be very valuable. However the cost of generating the insight via human review of the reports is prohibitive. This has lead to the use of computerized tools to analyze the massive corpora. Often this has resulted in considerable insight. The task of identifying specific concepts can enable relationships between concepts to be established, frequency to be quantified, and precursor activities to be objectively proven to exist. This would require prohibitive resources if it were to be attempted using human resources alone. Use of this technique can enable that in a cost effective manner. This tool was developed for NASA's Aviation Safety program but is useful to nearly any unstructured text analysis problem.
Disadvantages:	The effort to setup the capability is cost effective for important problems and moderate or larger data sets. It may not be cost effective for extremely small data sets, unless continued growth is anticipated.

Appendix B – Acronyms

ALARP - As Low as Reasonably Practical

APMS – Aviation Performance Management System

APS- Accident Prone Situations

ASAP - Aviation Safety Action Program

ASRP - Aviation Safety Reporting Program

ASRS - Aviation Safety Reporting System

ATC - Air Traffic Control

ATM - Air Traffic Management

ATO - Air Traffic Organization

ATS – Air Traffic Services

EATMP – European Air Traffic Management Programme

ELS – Error Likely Situations

ESA – European Space Agency

ESARR – EUROCONTROL Safety Regulatory Requirement

ETA – Event Tree Analysis

EUROCONTROL - European organisation for the Safety of Air Navigation

FAA - Federal Aviation Administration

FAST - FAA Acquisition System Toolset

FAST – Future Aviation Safety Team

FDM – Flight Data Monitoring

FHA - Functional Hazard Analysis

FMEA - Failure Modes and Effects Analysis

FMECA - Failure Modes, Effects, and Criticality Analysis

FOQA – Flight Operational Quality Assurance

FTA - Fault Tree Analysis

GAIN – Global Aviation Information Network

HAZid – Hardware/Software Interaction Analysis

HAZOP - Hazard and Operability Tool

HEMP – Hazards and Effect Management Process

HMI – Human machine Interface

HSIA - Hardware/Software Interaction Analysis

JHA - Job Hazard Analysis

LI Comp- Linear Interpolating Leader

LoR – Level of Risk

LPV – Lowest Practical Value

MES - Multi-Linear Event Sequencing Tool

MORT - Management Oversight and Risk Tree

NAS - National Airspace System

NAPA – National Academy of Public Administrators

NASA - National Aeronautics and Space Administration

NATS – National Air Traffic Services

PDARS – Performance Data Analysis and Reporting System

PHA – Preliminary Hazard Analysis

PLI – Progressive Linear Interpolation

PRA – Probabilistic Risk Assessment

PSA – Probabilistic Safety Assessment

RGCSP – Review of the General Concepts of Separation Panel

RPN – Risk Prioritization Number

SAM – Safety Assessment Methodology

SCHAZOP – Safety Culture Hazard and Operability

SFMEA – Systems Failures Modes and Effect Analysis

SRM - Safety Risk Management

SSH - System Safety Handbook

SSHA – Sub-System Hazard Analysis

SSMP - System Safety Management Program

TCAS – Traffic Collision Avoidance System

TLS – Target Level of Safety

TOPAZ – Traffic Organization and Perturbation Analyzer

Appendix C: Participants (present & past)

Name	Organization	Email Address
Abigail Smith	Federal Aviation Administration	Abigail.Smith@faa.gov
Alessandro Boschiero	Ente Nazionale di Assistenza al Volo, ENAV (Italy)	aboschiero@enav.it
Alexander Krastev	Eurocontrol	Alexander.Krastev@eurocontrol.int
Alfredo Colon Secretary	Federal Aviation Administration	acolon@cssiinc.com
Christophe Berthelé	Centre d'Etudes de la Navigation Aérienne (CENA)	berthele@cena.fr
Barry Kirwan Co-Chair	Eurocontrol Experimental Centre (EEC)	barry.kirwan@eurocontrol.int
Brian Smith	National Aeronautics Space Administration	besmith@mail.arc.nasa.gov
Dave Bush	National Air Traffic Services	David.Bush@nats.co.uk
Dino Piccione	Federal Aviation Administration	dino.piccione@faa.gov
Eric Perrin Secretary	Eurocontrol Experimental Centre (EEC)	eric.perrin@eurocontrol.int
Neil May	National Air Traffic Services (NATS)	Neil.May@nats.co.uk
Hans de Jong	National Aerospace Laboratory NLR	hdejong@nlr.nl
Henk Blom	National Aerospace Laboratory NLR	blom@nlr.nl
Herman Nijhuis	EUROCONTROL	Herman.nijhuis@eurocontrol.int
Irv Statler	National Aeronautics Space Administration	Irving.C.Statler@nasa.gov
James Daum	Federal Aviation Administration	James.Daum@faa.gov
Joerg Leonhardt	Deutsche Flugsicherung, DFS (Germany)	Joerg.leonhardt@dfs.de
Jos Kuijper	Eurocontrol HQ, Safety & Security Management	jos.kuijper@eurocontrol.int
Keith Slater	National Air Traffic Services	Keith.slater@nats.co.uk
Kevin Corker	San Jose State University	Kcorker@email.sjsu.edu
Mike Allocco	Federal Aviation Administration	Michael.allocco@faa.gov
Michael Woldring	Eurocontrol Experimental Centre (EEC)	michael.woldring@eurocontrol.int
Oliver Straeter	Eurocontrol HQ, Safety & Security Management	oliver.straeter@eurocontrol.int
Patrick Mana	Eurocontrol	Patrick.mana@eurocontrol.int
Paul Humphreys	Eurocontrol	Paul.humphreys@eurocontrol.int
Ronald Stroup Co-Chair	Federal Aviation Administration	Ronald.l.stroup@faa.gov