EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL EXPERIMENTAL CENTRE

Review of techniques to support the EATMP Safety Assessment Methodology

Main Document

EEC Report No. XXX

Project XXX-X-XX

Issued: 11 April 2003

REPORT DOCUMENTATION PAGE

Reference: SMS-D5-Main-1.0	**Security Classification:** Unclassified
Sponsor: Barry KIRWAN	**Sponsor (Contract Authority) Name/Location:** EUROCONTROL Experimental Centre Centre de Bois des Bordes B.P.15 F - 91222 Brétigny-sur-Orge CEDEX FRANCE Telephone: +33 (0)1 69 88 78 86

TITLE:

Review of techniques to support the EATMP Safety Assessment Methodology

Contact **Patrick MANA** Patrick.mana@eurocontrol.int	**Date**	**Pages**	**Figures**	**Tables**	**Appendix**	**References**
	11/04/03	iv + 124	3	10	0	134

Descriptors (keywords):
Safety assessment techniques & methods, EATMP SAM, Air Traffic Management

Abstract:
This report presents the main results of a survey conducted, aimed at collecting and evaluating techniques and methods that can be used to support the guidelines of the EATMP Safety Assessment Methodology (SAM). Over 500 techniques were collected that can possibly support SAM. Nineteen of these techniques have subsequently been selected for more detailed evaluation along a template format. These 19 techniques are believed to be able to support the SAM either immediately, or with some tailoring or adaptation to the ATM context. The report explains how the collection process was organised, presents statistics on the 500 collected techniques, explains how 19 techniques were selected from these 500, explains how the template format was developed, and gives the detailed evaluation results for the 19 selected techniques. In addition, it provides techniques that are judged to be significantly important and therefore deserve further development. Many details are provided in a separate Technical Annex.

Table of contents

1. Introduction

The Safety Methods Survey report is the outcome of a project is conducted as part of the SAFBUILD project [SAFBUILD web], which concerns Building Safety into Design, and is a safety assurance research approach to help ATM increase design robustness. This section explains the objectives the Safety Methods Survey project, then it explains the objective and organisation of this report.

1.1 Objective of the Safety Methods Survey project

The EATMP SAM has two aspects:

- the methodology, and
- how to execute the methodology.

For the second aspect, SAM gives guidelines (through Guidance material) but also freedom on how to complete the safety assessment: several techniques and methods may be used to support it. The purpose of the current Safety Methods Survey project was to identify possible techniques and methods for this support (including those developed in other domains and industries such as nuclear, chemical, telecommunication, railways, software design, but excluding commercially available tools), and to evaluate which ones are most suitable for the SAM.

1.2 Objective of this document

This document contains the consolidated results of the identification and selection of techniques and methods to support EATMP SAM.

From the complete collection of about 500 techniques, a selection was made of 19 techniques that appeared most relevant to support SAM on the short term (possibly with minimal adaptation). A set of criteria was developed, to describe and evaluate all of these selected techniques in a 'template' format of 1-3 pages, and the 19 selected techniques were evaluated using this template. The pros and cons of each selected technique or method, in the context of ANS, were also listed.

1.3 Organisation of this document

This document is organised as follows.

- Section 2 discusses the EATMP Safety Assessment Methodology, explains its scope and the steps to be made to follow it.
- Section 3 explains how a list of about 500 safety assessment techniques was collected that could support the EATMP SAM guidelines, and provides some statistics on these techniques.

- Section 4 discusses the screening process to select from the list of 500 candidate techniques 19 techniques that were considered most relevant for EATMP SAM on the short term.
- Section 5 explains how a template format was developed, which would be used to evaluate the selected 19 techniques.
- Section 6 provides the evaluation results for the 19 selected techniques according to the template format.
- Section 7 discusses the main safety assessment areas identified that are not covered by one of the 19 techniques evaluated in this report, but which are very important areas of development or further study beyond short term.
- Section 8 gives conclusions.

Section 9 provides references used.

2. EATMP Safety Assessment Methodology

This section provides an outline of the current version of SAM. The purpose of this summary is to give a framework for the techniques and methods to be identified and evaluated for this Safety Methods Survey project. The summary should clarify the type and properties of the techniques and methods that are necessary to support the SAM steps. It does not intend to provide complete guidelines on how to perform the safety assessment through SAM; for this, we refer to reference [EHQ-SAM].

2.1 Aimed scope of SAM

EATMP SAM (in the version as documented in reference [EHQ-SAM]) aims to define the means for providing assurance that a Ground Air Navigation System, in this document referred to as Ground ANS, is safe for operational use. The objective of this subsection is to discuss the two keywords in this scope, i.e. Safety assurance and Ground ANS. However, since the ultimate aim of SAM is to cover both the Airborne and the Ground part of ANS, as specified by [ESARR 4], the extension to ANS (including Airborne and Ground ANS) is also discussed.

Safety assurance

SAM considers the safety aspects only. In particular,

- SAM does not address other attributes of the system, aiming, for example, to achieve capacity and/or efficiency objectives.
- SAM does not address Air Navigation System certification issues. However, the aim is that the application of the principles could prepare for and support a certification process.
- SAM does not address organisational aspects related to safety assessment. SAM prescribes for each project that organisational entities involved in the safety assessment process should be identified and that their respective responsibilities should be specified.

ANS and Ground ANS

The FHA V1.0 SAM version restricts to Ground ANS (though FHA V2.0 and PSSA and SSA apply to ANS), which (according to SAM document [Mana02]) consists of AIS (Aeronautical Information Services), SAR (Search and Rescue) and Ground ATM (Air Traffic Management). Here, ATM (both Ground and Airborne part) consists of ATFM (Air Traffic Flow Management), ATS (Air Traffic Services) and ASM (Air Space Management), where ATS consists of ATC (Air Traffic Control), FIS (Flight Information Services), Alerting service, and Advisory service.

Figure 1, which is from [Mana02], gives an overview of ANS, which covers both Ground ANS (i.e. AIS + SAR + Ground ATM) and Airborne ANS (i.e. AIS + SAR + Airborne ATM).

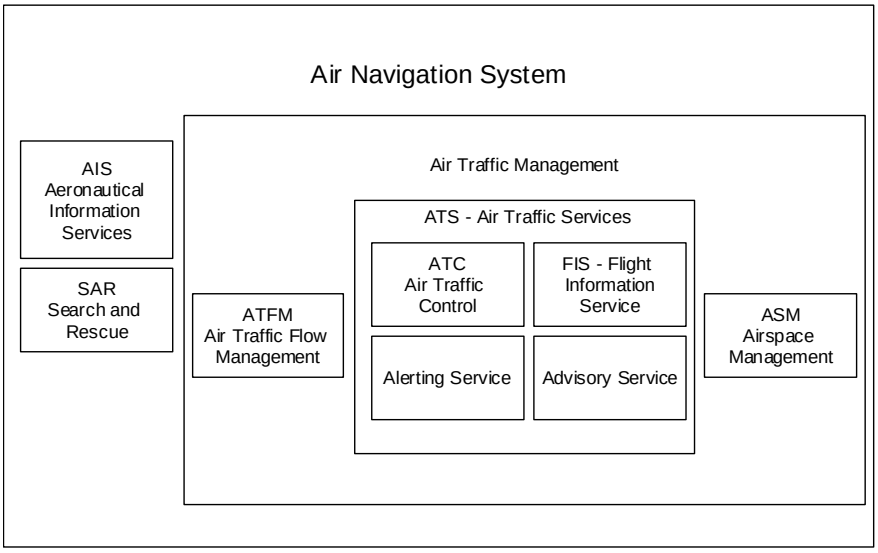


Figure 1: The Air Navigation System (according to [Mana02]) covers AIS, SAR and ATM (both ground and airborne part).

Reference [EATMS-CSD] provides a total picture of Ground ATM and Airborne ATM elements, see Figure 2. The Ground ANS elements have been made darker (with a medium shade for part coverage).

There are several issues that ANS (according to [EATMS-CSD]) does not appear to cover, for example:

- Airborne operations
- Behaviour of pilots
- Airborne procedures
- Interactions and situational awareness issues between pilots and air traffic controllers
- Effect of weather on airborne operations
- Non-functional interactions of ANS with any other system
- Risk due to acts of terrorism

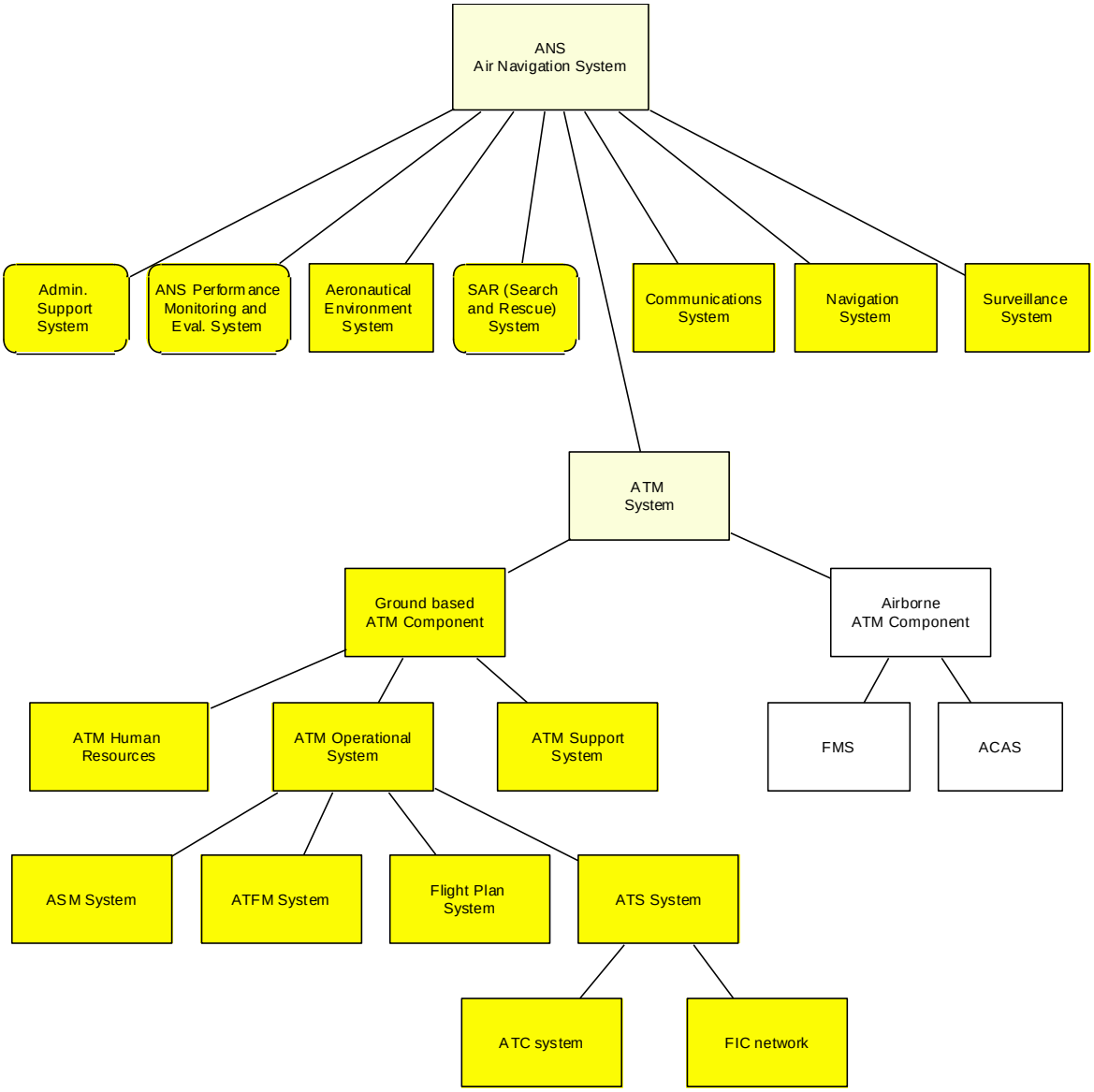


Figure 2: Overview of Air Navigation System according to [EATMS-CSD].

2.2 SAM overview

[EHQ-SAM] presents a general overview of a Air Navigation Systems safety assessment from an engineering perspective. The safety assessment activities are sub-divided into:

- Risk Assessment activities, to identify hazards, and evaluate the associated risk tolerability,
- Safety engineering activities, to select, validate and implement counter measures to mitigate these risks, and
- Safety assurance activities, which involve specific planned and systematic actions that together provide confidence that all relevant hazards and hazard effects have been identified, and that all significant issues that could cause or contribute to those hazards and their effects have been considered.

The objective of the methodology is to define a means for providing assurance that a Air Navigation System is safe for operational use. It is an iterative process conducted throughout the system development life cycle, from initial system definition, through design, implementation,

integration, transfer to operations, to operations and maintenance. The iterative process consists of a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and a System Safety Assessment (SSA), see Figure 3.

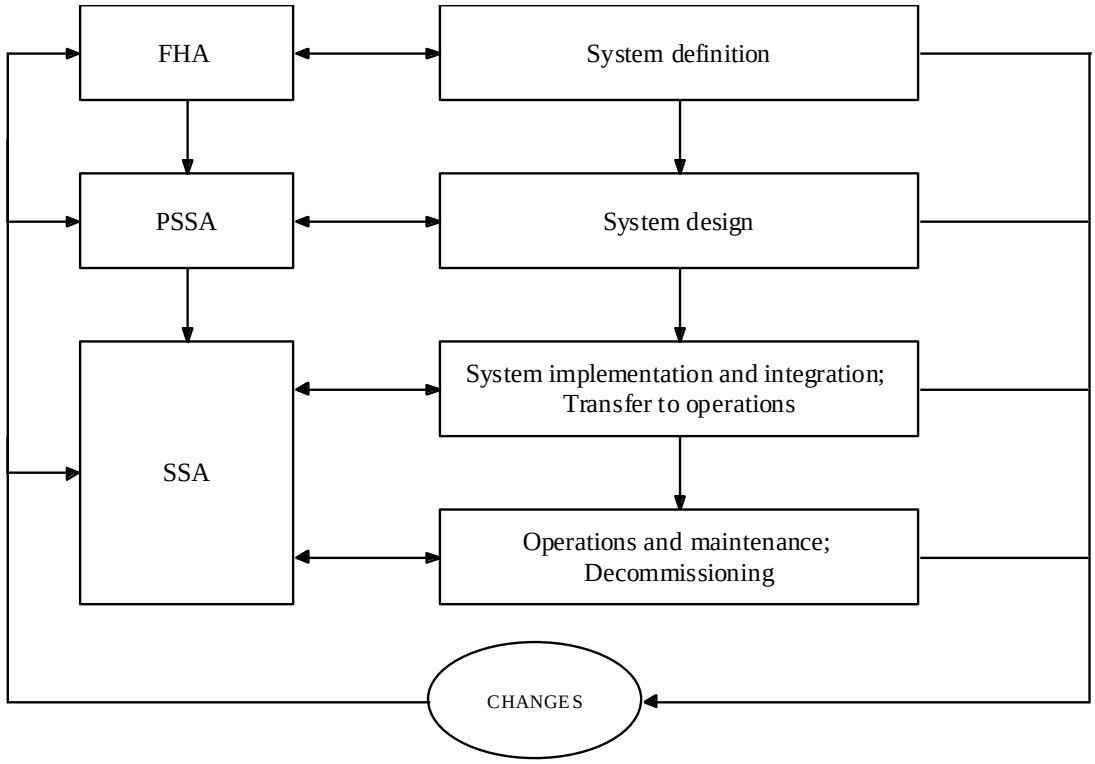


Figure 3: Safety Assessment Methodology [EHQ-SAM]

The objectives of the FHA, the PSSA and the SSA are:

- Functional Hazard Assessment (FHA) analyses the potential consequences on safety resulting from the loss or degradation of system functions. Using service experience, engineering and operational judgement, the severity of each hazard effect is determined qualitatively and is placed in a class 1, 2, 3, 4 or 5 (with class 1 referring the most severe effect, and class 5 referring to no effect). *Safety Objectives* determine the maximum tolerable probability of occurrence of a hazard, in order to achieve a tolerable risk level.
- Preliminary System Safety Assessment (PSSA) determines that the proposed system architecture is expected to achieve the safety objectives. PSSA examines the proposed system architecture and determines how faults of system elements and/or external events could cause or contribute to the hazards and their effects identified in the FHA. Next, it supports the selection and validation of mitigation means that can be devised to eliminate, reduce or control the hazards and their end effects. System *Safety Requirements* are derived from Safety Objectives; they specify the potential means identified to prevent or to reduce hazards and their end effects to an acceptable level in combination with specific possible constraints or measures.
- System Safety Assessment (SSA) collects arguments, evidence and assurance to ensure that each system element as implemented meets its safety requirements and that the system as implemented meets its safety objectives throughout its lifetime. It demonstrates that all risks have been eliminated or minimised as far as reasonably practicable in order to

be acceptable, and subsequently monitors the safety performance of the system in service. The safety objectives are compared with the current performances to confirm that they continue to be achieved by the system.

The FHA and PSSA are described in significantly more detail in [EHQ-SAM]. The SSA description is under construction.

In [EHQ-SAM], a very handy table is provided which gives an overview of the expertise required for each of these three assessment activities. This overview is copied in the table below.

Table 1: Expertise required for FHA, PSSA and SSA activities

Expertise required	**FHA activities**	**PSSA activities**	**SSA activities**
Operational	Identification of hazards and their effects	Evaluation of automation concepts	Design and validation of ATM procedures; Evaluation of HMI
Human factors	-	Identification of risk mitigation means related to human errors	Identification of risk mitigation means related to human errors
Ergonomic	-	Design of working position	Implementation of working position; Implementation of HMI
System engineering	Identification of hazards and their effects	Identification, selection and validation of risk mitigation means	Verification and validation
Software / hardware engineering	-	Design methods and assurance level determination (SWAL/HWAL)	Software and hardware implementation SWAL/HWAL satisfaction
ATM procedure	-	Design methods and assurance level determination (PAL)	ATM procedure implementation PAL satisfaction
Quality assurance	Quality assurance of FHA process	Quality assurance of the PSSA process	Quality assurance of implementation, integration, transfer to operations, operations and maintenance
Safety management	All activities	All activities	All activities

It can be noticed that, according to the table here above, human factors and ergonomic expertise and software/hardware engineering are not required during Functional Hazard Assessment.

In the next three subsections, the activities to be followed for FHA, PSSA and SSA are detailed.

2.3 Functional Hazard Assessment (FHA)

The FHA part of reference [EHQ-SAM] gives more details on the FHA steps and provides guidelines on how to perform each step. It lists for each FHA step the objectives, the input necessary, the major tasks and the output provided. The objectives and major tasks are repeated in Table 2 below, with a numbering of the major tasks added.

The last column of the table indicates with Yes/No whether SAM developers would like to have supporting techniques or methods for the task. The Safety Methods Survey project aims to search for these techniques. Note that a Yes indicates that supporting techniques could be useful; it does not mean that supporting techniques exist. Also note that a Yes is also given if SAM guidelines already list some supporting techniques; in that case, the Safety Methods Survey may search for alternative techniques.

Table 2: Activities to be followed for a Functional Hazard Assessment

FHA STEP	Objectives	Major tasks	Support needed from a technique?
F1. FHA initiation	▪ Develop a level of understanding of the system, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out	F1.1. Gather all necessary information describing the system	No
		F1.2. Review this information to establish that it is sufficient to carry out the FHA	No
		F1.3. If not available, describe the operational environment of the system	Yes
		F1.4. Identify and record assumptions made	No
		F1.5. Put the input information under an appropriate documentation control scheme	No
F2. FHA planning	▪ Define the objectives and scope of the FHA, the activities to be carried out, their deliverables, their schedule and the required resources	F2.1. Identify and describe the more specific activities for the FHA step	No
		F2.2. Submit the plan to peer review to provide assurance of its suitability	No
		F2.3. Submit the plan for comment or approval to interested parties (including regulatory authorities), as appropriate	No
		F2.4. Put the plan under appropriate documentation control scheme	No
		F2.5. Disseminate the plan to all interested parties	No

FHA STEP	Objectives	Major tasks	Support needed from a technique?
F3. Safety objectives specification	▪ To identify all potential failures associated with the system ▪ To determine the safety consequences of failure occurrence and to identify potential hazards ▪ To assess the severity associated with each hazard (i.e. the severity of the worst credible consequences) of the failure occurrence on aircraft operations ▪ To derive safety objectives in accordance with the severity of the hazards	F3.1. For each function and combination of functions, identify potential failures (loss or degradation of function)	Yes
		F3.2. For each function and combination of functions, identify potential hazards (worst credible effects on aircraft operations)	Yes
		F3.3. For each function and combination of functions, assess the severity of hazard effects (severity classification)	Yes
		F3.4. For each function and combination of functions, specify Safety Objectives (maximum tolerable probability)	Yes
F4a. FHA Validation	▪ To ensure that the safety objectives are (and remain) correct and complete ▪ To ensure that all critical assumptions are credible, appropriately justified and documented	F4a.1. Review and analyse Safety Objectives to ensure their completeness and correctness	Yes
		F4a.2. Review and analyse the description of the operational environment to ensure their completeness and correctness	No
		F4a.3. Review, analyse, justify and document critical assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness	Yes
		F4a.4. Review and analyse traceability between functions, failures, hazards and Safety Objectives	Yes
		F4a.5. Review and analyse the sensitivity of derived Safety Objectives to the assumptions	Yes
F4b. FHA verification	▪ To demonstrate that the process followed in deriving the safety objectives is technically correct	F4b.1. Review and analyse the results of the FHA process	No
F4c. FHA assurance process	▪ To provide evidence that all FHA activities (including safety verification and safety validation) have been conducted according to plan ▪ To ensure that the results - and the assumptions on which	F4c.1. Check that applicable assessment approaches have been properly followed	No
		F4c.2. Check that outcomes of FHA validation and verification activities have been properly recorded	No

	they depend - are properly recorded and disseminated for use by those involved in later stages of the development / assessment cycle, and to future system users	F4c.3. Check that any deficiencies detected during validation and verification activities have been properly resolved	No
		F4c.4. Consider whether the assessment would be repeatable by personnel other than the original analyst(s)	No
		F4c.5. Check that the findings have been disseminated appropriately, and that there is awareness and understanding of them	No
F5. FHA completion	▪ To record the results of the complete FHA process ▪ To disseminate these results to all interested parties	F5.1. Document the results of the FHA process (including the results of FHA validation, verification and process assurance activities)	No
		F5.2. Put the FHA documentation under an appropriate documentation control scheme	No
		F5.3. Disseminate the FHA documentation to all interested parties	No

For the FHA steps for which supporting techniques need to be identified, a more extended description is given below:

Table 3: Description of FHA activities that need support from techniques

FHA STEP	Major tasks	Type of support needed from a technique
F1. FHA initiation	F1.3. If not available, describe the operational environment of the system	A taxonomy to help define the relevant characterisations of the operational environment might be useful.

FHA STEP	Major tasks	Type of support needed from a technique
F3. Safety objectives specification	F3.1 For each function and combination of functions, identify potential failures (loss or degradation of function): What could go wrong with the system? A function can fail in various ways and can be the result of a sequence of events.	This task requires techniques that help and guide the identification of all possible failures. The FHA guidelines on this task are quite thorough and recommend structured meetings with the users and developers of the system, e.g. guided by keywords. There might exist techniques that support the identification of failures in an even more exhaustive way, or that identify failures that are unimaginable for other techniques. There might also exist supporting tools that ensure a more efficient organisation of these group meetings (although the identification of these tools is not within the scope of the Safety Methods Survey). Finally, since group sessions tend to produce results not in a logical order, there might be techniques that support the consolidation of the results.
	F3.2. For each function and combination of functions, identify potential hazards (worst credible effects on aircraft operations): • What could happen if it did go wrong, and does it affect the safety of aircraft operations? Here, various elements should be considered: Effects on ability to provide safe Air Navigation Service, • Effects on ATCO or flight crew working conditions, • Effects on their ability to cope with adverse conditions, • The exposure to the hazard, and • The possibility of detection. ESARR4 criteria are used.	According to the FHA guidelines, the consequences of the failures can also be identified in group sessions. There might exist techniques that support the identification of hazards in an even more exhaustive way, or that identify hazards that are unimaginable for other techniques or techniques that identify additional hazards that are not necessarily the result of a failure. There might also exist supporting tools that ensure a more efficient organisation of these group meetings (beyond scope of survey). Finally, since group sessions tend to produce results not in a logical order, there might be techniques that support the consolidation of the results.
	F3.3. For each function and combination of functions, assess the severity of hazard effects (severity classification): How bad would those effects be? These consequences are dependent on flight phase and on variations in environmental and operational conditions.	The FHA guidelines suggest that this task can also be done in a group session, but if the system being assessed is complex, it may generally better be done by one or two assessors outside the meeting. There might be techniques that help combine assessments of different experts. Or there may be techniques that support the severity assessment through other means.

FHA STEP	Major tasks	Type of support needed from a technique
	F3.4. For each function and combination of functions, specify Safety Objectives (maximum tolerable probability): How often can we tolerate that?	This process makes use of the hazard classification scheme and risk classification scheme, defined by the Safety Regulation Commission (ESSAR 4). There may be techniques (although finding them has low priority) that support how to choose the most appropriate form for the safety objectives (e.g. relative or absolute; qualitative or quantitative) and on setting quantitative values where required.
F4a. FHA Validation	F4a.1. Review and analyse Safety Objectives to ensure their completeness and correctness	FHA guidance material provides checklists to guide this validation process. There may be other supporting methods, e.g. simulation facilities to verify controller reaction times that affect the classification of a hazard.
	F4a.3. Review, analyse, justify and document critical assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness	FHA guidance material provides checklists to guide this validation process. There may be other supporting methods.
	F4a.4. Review and analyse traceability between functions, failures, hazards and Safety Objectives	FHA guidance material provides checklists to guide this validation process. There may be other supporting methods.
	F4a.5. Review and analyse the sensitivity of derived Safety Objectives to the assumptions	FHA guidance material provides checklists to guide this validation process. There may be other supporting methods.

2.4 Preliminary System Safety Assessment (PSSA)

The PSSA part of reference [EHQ-SAM] gives more details on the PSSA steps and provides guidelines on how to perform each step. It lists for each PSSA step the objectives, the input necessary, the major tasks and the output provided. The objectives and major tasks are repeated in Table 4 below, with a numbering of the major tasks added. The last column of the table indicates whether support is necessary from additional techniques, methods or facilities.

Table 4: Activities to be followed for a Preliminary System Safety Assessment

PSSA STEP	Objectives	Major tasks	Support needed from a technique?
P1. PSSA Initiation	▪ Develop a level of understanding of the system design framework, its	P1.1. Gather all necessary information describing the system design.	No

PSSA STEP	Objectives	Major tasks	Support needed from a technique?
	operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.	P1.2. Review this information to establish that it is sufficient to carry out the PSSA.	No
		P1.3. Update the operational environment description (OED) of the system (since FHA and to add PSSA-related OED data).	Yes
		P1.4. Identify and record assumptions made.	No
		P1.5. Put the input information under an appropriate documentation control scheme.	No
P2. PSSA Planning	▪ Define the objectives and scope of the PSSA, the activities to be carried out, their deliverables, their schedule and the required resources.	P2.1. Identify and describe the more specific activities for the PSSA step.	No
		P2.2. Submit the plan to peer review to provide assurance of its suitability.	No
		P2.3. Submit the plan for comment or approval to interested parties (including regulatory authorities), as appropriate.	No
		P2.4. Put the plan under appropriate documentation control scheme.	No
		P2.5. Disseminate the plan to all interested parties.	No
P3. Safety Requirements Specification	▪ To refine the functional breakdown. ▪ To evaluate system architecture. ▪ To apply risk mitigation strategies. ▪ To apportion Safety Objectives into Safety Requirements. ▪ To balance Safety Requirements	P3.1. For each function and combination of functions, refine the functional breakdown.	Yes
		P3.2. For each function and combination of functions, evaluate system architecture(s)	Yes
		P3.3. For each function and combination of functions, apply risk mitigation strategies.	Yes
		P3.4. For each function and combination of functions, apportion Safety Objectives into Safety Requirements.	Yes
		P3.5. For each function and combination of functions, balance Safety Requirements	Yes
P4a. PSSA Validation	▪ To ensure that the Safety Requirements are (and remain) correct and complete;	P4a.1. Review and analyse Safety Requirements to ensure their completeness and correctness;	Yes

	▪ To ensure that all critical assumptions are credible, appropriately justified and documented.	P4a.2. Review and analyse the description of the operational environment to ensure its completeness and correctness;	Yes
		P4a.3. Review, analyse, justify and document critical assumptions about the system design, its operational environment and its regulatory framework to ensure their completeness and correctness.	Yes
		P4a.4. Review and analyse traceability between Safety Objectives and Safety Requirements.	Yes
		P4a.5. Review and analyse the sensitivity of derived Safety Requirements to the assumptions.	Yes
P4b. PSSA Verification	▪ To demonstrate that the process followed in deriving the Safety Requirements is technically correct	P4b.1. Review and analyse the results of the PSSA process.	Yes
P4c. PSSA Assurance Process	▪ To provide evidence that all PSSA activities (including Safety Verification and Safety Validation) have been conducted according to the plan; ▪ To ensure that the results – and the assumptions on which they depend - are properly recorded and disseminated for use by those involved in later stages of the development/assessment cycle, and to future system users.	P4c.1. Check that applicable assessment approaches have been properly followed.	No
		P4c.2. Check that outcomes of PSSA Validation and Verification activities have been properly recorded.	No
		P4c.3. Check that any deficiencies detected during Verification or Validation activities have been properly resolved.	No
		P4c.4. Consider whether the assessment would be repeatable by personnel other than the original analyst(s);	No
		P4c.5. Check that the findings have been disseminated appropriately, and that there is awareness and understanding of them.	No
P5. PSSA Completion	▪ To record the results of the complete PSSA process ▪ To disseminate these results to all interested parties	P5.1. Document the results of the PSSA process (including the results of PSSA Validation, Verification and Process Assurance activities).	No
		P5.2. Put the PSSA documentation under an appropriate documentation control scheme.	No
		P5.3. Disseminate the PSSA documentation to all interested parties.	No

For the PSSA steps for which supporting techniques need to be identified, a more extended description is given below:

Table 5: Description of PSSA activities that need support from techniques

PSSA STEP	Major tasks	Type of support needed from a technique
P1. PSSA Initiation	P1.3. Update the operational environment description (OED) of the system (since FHA and to add PSSA-related OED data).	None identified
P3. Safety Requirements Specification	P3.1. For each function and combination of functions, refine the functional breakdown. In this task, sub-functions are identified which do not participate to the worst case hazard, hence can be associated to a lower level safety objective.	Techniques may be identified to support the functional breakdown into subfunctions, and to support the severity and likelihood assessment of these subfunctions. Tools may be identified for graphical representation (although it was noted that it was only necessary to identify the existence of such tools).
	P3.2. For each function and combination of functions, evaluate system architecture(s). This step extends and refines the identification of hazards carried out in previous steps by considering the alternative architectures, and evaluates the risk of the associated potential incident/accident sequence. Architectures that generate intolerable hazards, or that violate assumptions, or that have a wrong automation level are rejected.	Here additional hazard identification techniques may be used. Techniques that could not be used during FHA might be used here, since during PSSA more information on the design of the system is available. Human reliability assessment, human error identification techniques and (misuse, disuse and abuse of) automation issues become more relevant. Also, common cause analysis or common mode analysis techniques and zonal analysis techniques will be necessary. The PSSA guidelines give some tips on how best to organise groups sessions, and discuss various automation and human factors issues.
	P3.3. For each function and combination of functions, apply risk mitigation strategies. These should lead to hazard elimination. If this is not possible then to hazard reduction (reduction of frequency), and for remaining hazards, to hazard control.	Techniques might be used to check if the effect of the mitigating means is according to expectation.

	P3.4. For each function and combination of functions, apportion Safety Objectives in to Safety Requirements. These requirements are allocated to system elements, which include human elements (e.g. training requirements), procedure elements (e.g. operational limitations for procedure) and equipment (both hardware and software) elements (e.g. dependability requirements, provision of feedback).	Techniques might be used to check if the effect of the Safety Requirements is according to expectation. For example, one may perform an ATC procedure safety assessment. For hardware safety requirements, techniques that decompose the system may be used to verify the safety objective quantitatively. Additional techniques are required for analysis of human errors and operator tasks and for situational awareness issues. The PSSA guidelines recommend using more than one technique (especially for human actions and procedure assessment), and to use both bottom-up approaches and top-down approaches. Moreover they recommend to take the limitations of the used techniques into account, and to use expert and engineering judgement to complement them. Simulations might also be used.
	P3.5. For each function and combination of functions, balance Safety Requirements. Here, the requirements are consolidated and adjusted, and the design is optimised (to ensure coherence and to avoid over-engineering). It is verified if the Safety Requirements are credible (taking into account technological and business constraints), and if the architecture meets credibly the Safety Objectives.	The PSSA recommends bottom-up approaches to be used for this.
P4a. PSSA Validation	P4a.1. Review and analyse mitigating means and Safety Requirements to ensure their completeness and correctness;	PSSA guidelines provide checklists to support this task. Operational or engineering judgement will be involved, but also tests through specific analysis, modelling or simulation may be useful, for example to test actual human reaction time to a failure.
	P4a.2. Review and analyse the description of the operational environment to ensure its completeness and correctness;	PSSA guidance material provides checklists to guide this validation process. There may be other supporting methods.
	P4a.3. Review, analyse, justify and document critical assumptions about the system design, its operational environment and its regulatory framework to ensure their completeness and correctness.	PSSA guidance material provides checklists to guide this validation process. There may be other supporting methods.
	P4a.4. Review and analyse traceability between Safety Objectives and Safety Requirements.	PSSA guidance material provides checklists to guide this validation process. There may be other supporting methods.

	P4a.5. Review and analyse the sensitivity of derived Safety Requirements to the assumptions.	PSSA guidance material provides checklists to guide this validation process. There may be other supporting methods.
P4b. PSSA Verification	P4b.1. Review and analyse the results of the PSSA process, including validation.	PSSA guidance material provides checklists to guide this verification process. There may be other supporting methods.

2.5 System Safety Assessment (SSA)

The SSA guidelines are still under construction. The following information is based on draft documents. These documents provide objectives and major tasks for the SSA steps as gathered in the table below.

Table 6: Activities to be followed for a System Safety Assessment

SSA STEP	Objectives	Major tasks	Support needed from a technique?
S1. SSA Initiation	▪ To develop a level of understanding of the system implementation and its rationale ▪ To update the description of its operational environment ▪ To identify, when appropriate, regulatory requirements and/or standards applicable to the system implementation, integration, transfer into operation, operation, maintenance and decommissioning.	S1.1. Gather all necessary information describing the system implementation	No
		S1.2. Review this information to establish that it is sufficient to carry out the SSA.	No
		S1.3. Upgrade the operational environment description of the system to add any system implementation, integration, transfer into operation, operation, maintenance and decommissioning related data.	Yes
		S1.4. Identify and record assumptions made. Areas in which assumptions are commonly necessary relate to the operational scenarios, the system functions, the system architecture and the system environment.	No
		S1.5. Put the input information under an appropriate documentation control scheme.	No
S2. SSA Planning	▪ To define the objectives and scope of the SSA, the activities to be carried out, their deliverables, their schedule and the required resources.	S2.1. Identify and describe the more specific activities for the SSA step.	No
		S2.2. Define and describe the strategy to be used.	No
		S2.3. Identify methods and techniques to be used in the safety assessment.	No
		S2.4. Identify interdependencies with the design process	No
		S2.5. Submit the plan to peer review to provide assurance of its suitability.	No
		S2.6. Submit the plan for comment or approval to interested parties (including regulatory authorities), as appropriate.	No

SSA STEP	Objectives	Major tasks	Support needed from a technique?
		S2.7. Put the plan under appropriate documentation control scheme.	No
		S2.8. Disseminate the plan to all interested parties.	No

S3a. Safety Evidences Collection during Implementation & Integration (including Training)	▪ To provide assurance that each system (people, procedure, equipment) element as implemented meets its safety requirements, that the system as implemented meets its safety objectives and requirements throughout its operational lifetime and that it will satisfy the users expectations with respect to safety.	S3a.1. Verification that system as implemented meets its Safety Objectives	Yes
		S3a.2. Verification that system elements (People, Procedures, Equipment) as implemented meet their Safety Requirements.	Yes
S3b. Safety Evidences Collection during Transfer to Operations		S3b.1. Verification that system as transferred to operations meets its Safety Objectives and that system elements meet their Safety Requirements,	Yes
		S3b.2. Validation of the system as transferred to operations with respect to users' Safety expectations.	Yes
		S3b.3. Safety assessment of transfer into operation phase.	Yes
S3c. Safety Evidences Collection during Operations & Maintenance	▪ To provide assurance that each system (people, procedure, equipment) element as implemented meets its safety requirements, that the system as implemented meets its safety objectives and requirements throughout its operational lifetime and that it will satisfy the users expectations with respect to safety.	S3c.1. Data collection and monitoring of safety performances with respect to Safety Objectives and Requirements,	Yes
		S3c.2. Safety assessment of maintenance interventions.	Yes

S3d. Safety Evidences Collection during System changes (People, Procedures, Equipment)	▪ To provide assurance that each system (people, procedure, equipment) element as implemented meets its safety requirements, that the system as implemented meets its safety objectives and requirements throughout its operational lifetime and that it will satisfy the users expectations with respect to safety.	S3d.1. Any change to the system and its elements (People, Procedures, Equipment) leads to the re-iteration of the overall Safety Assessment process, through: FHA, PSSA and SSA	No, or refer to other steps
S3e. Safety Evidences Collection during Decommissioning	▪ To provide assurance that each system (people, procedure, equipment) element as implemented meets its safety requirements, that the system as implemented meets its safety objectives and requirements throughout its operational lifetime and that it will satisfy the users expectations with respect to safety.	S3e.1. Assessment of the safety impact on global ATC operations of the system withdrawing	Yes
		S3e.2. Safety assessment of the decommissioning process.	Yes

S4a. SSA Validation	To ensure that the outputs of the SSA process are correct and complete, i.e. that: ▪ The Safety Evidences are (and remain) correct and complete; ▪ All critical assumptions are credible, appropriately justified and documented.	S4a.1. Review and analyse the Safety Evidences to ensure their completeness and correctness;	Yes
		S4a.2. Review and analyse the description of the operational environment to ensure it is complete and correct;	Yes
		S4a.3. Review, analyse, justify and document critical assumptions about the system, its operational environment and its regulatory framework to ensure they are complete and correct.	Yes
		S4a.4. Review and analyse traceability between: ▪ Safety Requirements and Safety Evidences, ▪ Safety Objectives and Safety Evidences.	No
		S4a.5. Review and analyse the sensitivity of Safety Evidences to the assumptions.	Yes
S4b. SSA Verification	▪ To demonstrate that the process followed in collecting Safety Evidences is technically correct.	S4b.1. This is carried out by a review and analysis of the results of the SSA process.	Yes

S4c. SSA Assurance Process	▪ To provide evidence that all SSA activities (including Safety Verification and Safety Validation) have been conducted according to the plan; ▪ To ensure that the results – and the assumptions on which they depend - are properly recorded and disseminated for use by those involved in later stages of the development/assessment cycle, and to future system users.	S4c.1. Check that applicable assessment approaches have been properly followed.	No
		S4c.2. Check that outcomes of SSA Validation and Verification activities have been properly recorded.	No
		S4c.3. Check that any deficiencies detected during Verification or Validation activities have been properly resolved.	No
		S4c.4. Consider whether the assessment would be repeatable by personnel other than the original analyst(s);	No
		S4c.5. Check that the findings have been disseminated appropriately, and that there is awareness and understanding of them.	No
		S4c.6. Ensure that there is a valid configuration management system in place to that covers everything that is required to achieve or demonstrate safety.	No
S5. SSA Completion	▪ To record the results of the complete SSA process; ▪ To disseminate these results to all interested parties.	S5.1. Document the results of the SSA process (including the results of SSA Validation, Verification and Process Assurance activities).	No
		S5.2. Put the SSA documentation under an appropriate document control or configuration management scheme.	No
		S5.3. Disseminate the SSA documentation to all interested parties.	No

For the SSA steps for which supporting techniques need to be identified, a more extended description is given below.

Table 7: Description of SSA activities that need support from techniques

SSA STEP	Major tasks	Type of support needed from a technique
S1. SSA Initiation	S1.3. Upgrade the operational environment description of the system to add any system implementation, integration, transfer into operation, operation, maintenance and decommissioning related data.	None identified

S3a. Safety Evidences Collection during Implementation & Integration (including Training)	S3a.1. Verification that system as implemented meets its quantitative and qualitative Safety Objectives. The SSA guidelines identify several subtasks (collecting evidence, consolidating evidence, verifying objectives).	Satisfaction of quantitative safety objectives may be verified through risk assessment techniques. For the qualitative safety objectives, techniques supporting system integration tests, factory acceptance tests, real-time simulations, pre-operational trials, maintenance analysis, human error analysis, operating procedure analysis and common cause analysis, etc., can be identified.
	S3a.2. Verification that system elements (People, Procedures, Equipment) as implemented meet their Safety Requirements. The SSA guidelines identify eight subtasks.	Techniques that may support these tasks include: risk assessment techniques, factory acceptance tests and integration tests, real-time simulations, pre-operational trials, maintenance analysis, operating procedure analysis, technical studies, common cause analysis, software code inspection activities, etc.
S3b. Safety Evidences Collection during Transfer to Operations	S3b.1. Verification that system as transferred to operations meets its Safety Objectives and that system elements meet their Safety Requirements. The SSA guidelines identify four subtasks.	Supporting techniques include site acceptance tests, qualification tests, etc.
	S3b.2. Validation of the system as transferred to operations with respect to users' Safety expectations. The SSA guidelines identify three subtasks.	Techniques would support operational trials, transition analysis, etc.
S3c. Safety Evidences Collection during Operations & Maintenance	S3c.1. Data collection and monitoring of safety performances with respect to Safety Objectives and Requirements. The SSA guidelines identify five subtasks.	Techniques would support events detection and notification, factual information gathering, event reconstruction, event analysis, monitoring, updating initial safety assessments, safety auditing activities, common factors analysis, etc. Data collected formally and informally (e.g. through anonymous reporting systems) should be analysed in a timely fashion for the system and its organisation to learn from events, and hence to anticipate and mitigate future hazardous events.
	S3c.2. Safety assessment of maintenance interventions.	Techniques would support risk analysis of planned maintenance interventions.
S3e. Safety Evidences Collection during Decommissioning	S3e.1. Assessment of the safety impact on global ANS operations of the system withdrawing. This comes down to performing a formal safety assessment of the 'hosting' system that remains in place after the target system has been withdrawn	Techniques for this could be identified by looking at other domains, e.g. nuclear, chemical industry.

	S3e.2. Safety assessment of the decommissioning process. This means ensuring that risks induced on on-going ANS operations by the decommissioning operations are under control.	Techniques for this could be identified by looking at other domains, e.g. nuclear, chemical industry.
S4a. SSA Validation	S4a.1. Review and analyse the Safety Evidences to ensure their completeness and correctness;	Checklists could be identified to support these tasks. But there should also be other techniques to support this task.
	S4a.2. Review and analyse the description of the operational environment to ensure it is complete and correct;	Checklists could be identified to support these tasks.
	S4a.3. Review, analyse, justify and document critical assumptions about the system, its operational environment and its regulatory framework to ensure they are complete and correct.	Checklists could be identified to support these tasks.
	S4a.5. Review and analyse the sensitivity of Safety Evidences to the assumptions.	Checklists could be identified to support these tasks. But there should also be other techniques to support this task.
S4b. SSA Verification	S4b.1. This is carried out by a review and analysis of the results of the SSA process.	Checklists could be identified to support these tasks.

2.6 Urgency of safety assessment support needs

With respect to techniques to be identified to support the SAM steps, the following urgency list was given by SAM developers. For the first SAM steps on this list supporting techniques are needed with highest urgency. The last SAM steps on the list have the lowest urgency.

1. Step F3 (the third FHA step) and step P3 (the third PSSA step)
2. Steps F1, F2, F4, F5 (the other FHA steps) and steps P1, P2, P4, P5 (the other PSSA steps)
3. Step S3 (the third SSA step)
4. Steps S1, S2, S4, S5 (the other SSA steps)

Note that this urgency list reflects the fact that SAM is still in development, and hence the urgency is for tools to support the FHA and PSSA processes. However, the final list of methods selected may reflect a more balanced set based on importance in terms of adding safety to the SAM process.

3. Candidate safety assessment techniques

The second phase of the project involved a comprehensive survey of methods from a range of industries (e.g. nuclear power, telecommunications, aviation, etc.) that can assist in assuring safety in Air Traffic Management. Examples of methods to be considered included hazard and risk analysis techniques such as HAZOP, FMEA and FMECA, fault and event tree analysis, as well as collision risk modelling approaches, simulation modelling including fast and real-time simulations, mathematical modelling techniques such as Markov Analysis techniques, Human Reliability Assessment techniques, other System Reliability Engineering approaches including software reliability techniques, system/software modelling and verification techniques, etc. The review considered techniques used in ANS and other industries, so that ANS can borrow or adapt techniques found to be effective elsewhere. The review only considered publicly available techniques and methods, hence no commercially available tools or facilities.

The complete list of techniques collected during this project, i.e. about 500 techniques, is provided in the technical annex to this report [Technical Annex]. Subsection 3.1 below explains how the list was obtained. Subsections 3.2 through 3.6 provide some statistics on what types of techniques were collected.

3.1 Statistics

The complete list of 500 techniques collected according to the approach described in the previous subsection is provided in [Technical Annex], with some details for each technique or method such as year of birth, aim/description, domain of application, references used, etc. The following subsections present some statistics on these data.

To illustrate that techniques from different domains may be useful in some domains in some respects, but not in others, see the following table, the first four columns of which are from [Garrick88].

Hazard characteristics	**Chemical**	**Nuclear**	**Space**	**ATM**
Single-concentrated hazard locations	Sometimes	Always	Always	Sometimes
Distributed sources of hazard	Almost always	Reactor only	Rarely	Almost always
Chemical toxicity	Often	Rarely, radiation effect dominates	Always by secondary to fire and explosions	Almost never
Fires	Often	Often as the result from core melt effects	Major hazard	Quite rarely
Explosions	Often	Often as the result from core melt effects	Major hazard	Quite rarely
Radioactivity	Rarely	Always	Payload dependent	Almost never

Changing configuration or operating mode	Not important except in transportation	Not important except in transportation and spent fuel pool	Important	Important
Human error	Important	Important	Important	Important

3.2 Division amongst ATM concept elements

One of the details provided for each technique listed in [Technical Annex] is whether it is aimed at assessing Hardware elements, Software elements, Human elements, or Procedures and organisation. Some statistics on these results are given below. It appeared that out of the 515 techniques collected,

- 255 techniques (i.e. about 50%) can be used to assess hardware elements.
- 195 techniques (i.e. about 38%) can be used to assess software elements.
- 216 techniques (i.e. about 42%) can be used to assess human elements. These include both human reliability and human cognitive behaviour.
- 124 techniques (i.e. about 24%) can be used to assess procedures and organisation elements.

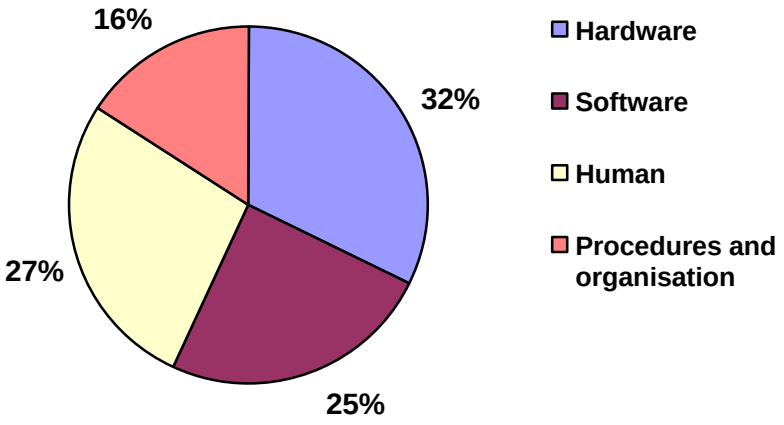
Note that one technique may cover several of these ATM concept elements, so some techniques are counted more than once.

The following table shows how many techniques cover only one, or more than one of these elements. For example, the first row of this table indicates that there are 90 techniques that cover hardware elements only. The fifth row indicates that there are 48 techniques that cover both hardware and software elements. The last row indicates that there are 13 techniques that cover all four types of ATM concept elements.

Hardware	**Software**	**Human**	**Procedures & Organisation**	**Number of techniques in this class**
X				90
	X			120
		X		95
			X	19
X	X			48
X		X		26
X			X	20
	X	X		1
	X		X	0
		X	X	25
X	X	X		11
X	X		X	2
X		X	X	45
	X	X	X	0
X	X	X	X	13
255	**195**	**216**	**124**	**515**

The following pie chart shows how many techniques cover the four types of ATM concept elements relative to each other.

Hardware	255
Software	195
Human	216
Procedures and organisation	124



3.3 Division amongst application to flight phases

Another interesting characteristic of the techniques collected is whether they are applicable to en-route phase of flight, or rather to TMA or Tower operations. However, except for the typical collision risk models, which generally apply to airborne operations (including final approach, etc), no significant information could be found on whether techniques apply to one flight phase or another. Therefore, no statistics are made available on this issue.

3.4 Division amongst domains of application

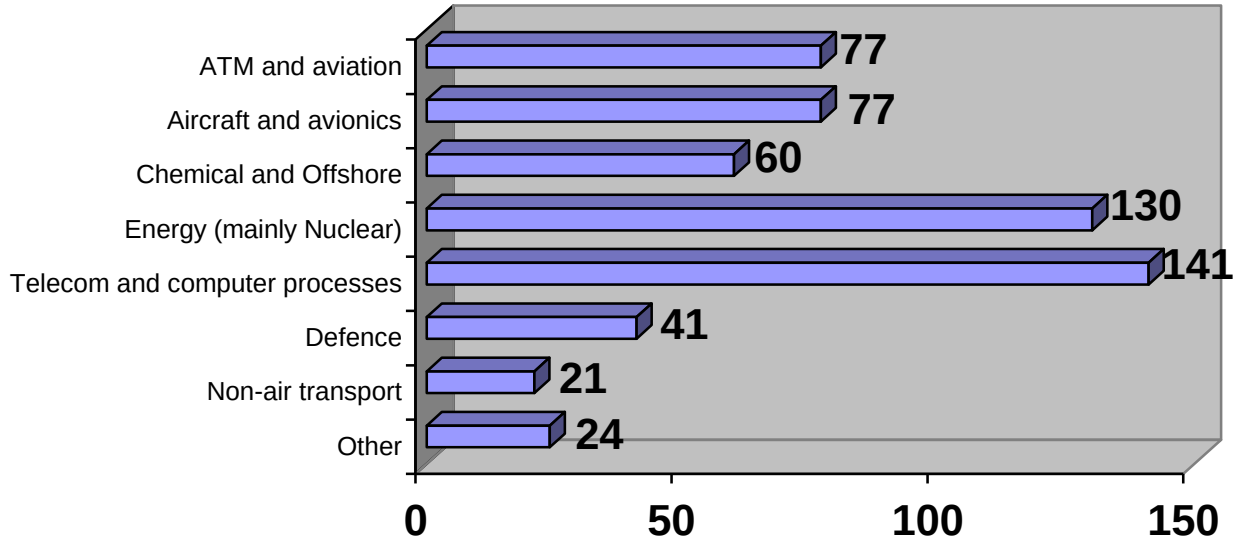
The Safety Methods Survey aimed at not only searching for techniques available in the ATM area, but also looked in other domains of application, such as nuclear industry, chemical industry, telecommunications, etc. The reason was that ATM can borrow or adapt techniques found to be effective elsewhere. The list of candidate techniques collected in [Technical Annex] provides details on this aspect. For each technique it is indicated in which domains of application it has been used to date. Note that exhaustiveness of this statistic is not guaranteed, since the information was sometimes difficult to find.

The histogram below shows how many of the techniques collected have been applied in the different domains of application. These domains have been grouped as follows:

Group of application domains	Number of techniques found	Application domains included in this group
ATM and aviation	77	ATM 37, ATC 7, Aviation 33
Aircraft and avionics	77	Aircraft equipment 54, Space 8, Avionics 10, Rotorcraft 1, Aerospace 2, Aeronautics 1
Chemical	60	Chemical industry 49, Offshore business 10, Petro-chemical

		industry 1
Energy (mainly Nuclear)	130	Nuclear power plants and nuclear industry 111, Energy 1, Electricity 14, Windturbines 3, Thermal power plant 1
Telecom and computer processes	141	Telecommunications 6, Computer processes 134, Data communications 1
Defence	41	Defence 38, Navy 2, Submarine displays 1
Non-air transport	21	Rail 12, Road 4, Other transport (except airborne) 5
Other	24	Manufacturing 7, Medical and medicine 5, Biomedical 1, Automotive 2, (Process) control 2, Safety management 1, Management systems 1, Finance 1, Construction 1, Warehousing 1, Logistics 1, Health 1

Note that one technique may cover several of these domains, so some techniques are counted multiple times. Also, for some techniques the domain of application was unclear, hence these are not counted at all.



3.5 Coverage of SAM steps

As explained in Section 2, SAM needs support of techniques and methods for several FHA, PSSA and SSA tasks. The list of candidate techniques in [Technical Annex] indicates for each technique for which of these tasks it could be applicable. This subsection provides some statistics on these results.

The three tables below repeat Tables 3, 5 and 7 of Section 2, which provide the FHA, PSSA and SSA tasks divided into subtasks, but with an additional column that indicates how many techniques have been collected in [Technical Annex] to (possibly) support or partially support each task. Note that a high number of techniques indicated does not necessarily mean that that task is completely supported by techniques. For example, all of these techniques may focus on only one aspect of the task, and forget another aspect. On the other hand, if only one technique is indicated to support the task, the task may be completely covered by this technique.

Table 8: Description of FHA activities that need support from techniques (see Table 3 for more details on the steps)

FHA STEP	Sub step	# techniques found
F.1. **FHA initiation**		7
F.3. Safety Objectives Specification	**F.3.1**	37
	F.3.2	64
	F.3.3	54
	F.3.4	4
F.4.1. **FHA Validation**		13

Table 9: Description of PSSA activities that need support from techniques (see Table 4 for more details on the steps)

PSSA STEP	Sub step	# techniques found
P.1. **PSSA Initiation**		5
P.3. **Safety Requirements Specification**	P.3.1	91
	P.3.2	247
	P.3.3	61
	P.3.4	12
	P.3.5	0
P.4a **PSSA Validation**		14
P.4b **PSSA Verification**		1

Table 10: Description of SSA activities that need support from techniques (see Table 5 for more details on the steps)

SSA STEP	Sub step	# techniques found
S.1. **SSA Initiation**		2
S.3a **Safety Evidences Collection during Implementation & Integration (including Training)**	S.3a.1	62
	S.3a.2	331
S.3b **Safety Evidences Collection during Transfer to Operations**		3

SSA STEP	Sub step	# techniques found
S.3c Safety Evidences Collection during Operations & Maintenance	S.3c.1	91
	S.3c.2	10
S.3e Safety Evidences Collection during Decommissioning		8
S.4a SSA Validation		8
S.4b SSA Verification		5

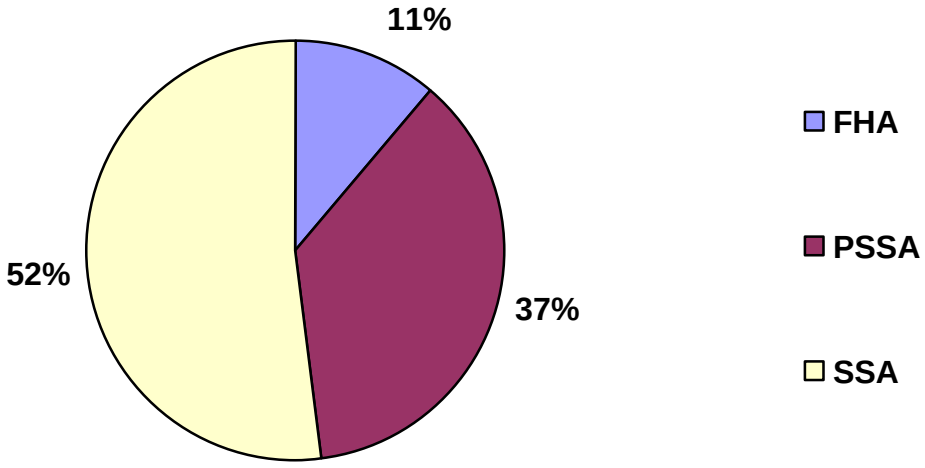
Note that for only one task (i.e. PSSA task 3.4: For each function and combination of functions, balance Safety Requirements) no supporting techniques were found. EUROCONTROL already indicated that a project was started up to fill this gap.

A summary distribution of techniques among FHA, PSSA and SSA is given below. It appeared that out of the 515 techniques collected,

- 89 techniques support one or more FHA subtasks.
- 298 techniques support one or more PSSA subtasks.
- 416 techniques support one or more SSA subtasks.

The pie chart below shows how many techniques support FHA, PSSA and SSA steps relative to each other.

FHA	89
PSSA	298
SSA	416



4. Development of a Template format

The third phase of the project involved the development of a template format along which a selection of safety assessment techniques were to be evaluated in more detail. This template was to be formed by a list of evaluation criteria for these techniques, such as Maturity, Acceptability, Advantages, Disadvantages, etc. Full details on how this template was developed are given in the technical annex to this report [Technical Annex]. This section provides a summary of the template development process.

The template was developed in three steps. First, candidate evaluation criteria for this template were gathered (Subsection 4.1), next these candidate evaluation criteria were analysed and a useful selection was made (Subsection 4.2). Next, the selected set was formed into a template format (Subsection 4.3).

4.1 Collection of candidate evaluation criteria

The first step in the template format development was to collect candidate evaluation criteria, and to provide a glossary for these criteria. The idea was to make full use of technique evaluations performed in previous survey studies, and start with the evaluation criteria used by those sources. It was tried to use studies that together cover a variety of techniques.

The sources used were (listed chronologically):

- [Humphreys88], which is a human reliability assessors guide, providing criteria for the evaluation of human reliability assessment techniques;
- [Bishop90], which contains a directory of evaluated techniques to assess the dependability of critical computer systems;
- [ΣΣ93,ΣΣ97], which contains a collection of evaluated (technical) system safety analysis techniques;
- [MUFTIS3.2-I], which contains a collection of hazard analysis and safety assessment techniques for use in the ATM/ATC domain;
- [Kirwan98-1], which contains a collection of evaluated techniques dealing with identifying human errors in high risk complex systems;
- [Minutes SMS], which contains the minutes for Safety Methods Survey kick-off meeting, during which some criteria were suggested.

The candidate evaluation criteria used by these sources were gathered in a table, ordered alphabetically, and a description as provided by the reference was added. Obviously, several similar criteria appeared in different sources. These were still listed individually, since sometimes the indicated description was different. The table is provided in the Technical Annex to this report [Technical Annex].

4.2 Analysis of candidate evaluation criteria

In the next step, the list of candidate evaluation criteria was analysed. The glossary list of the previous subsection was repeated where equivalent or similar candidate evaluation criteria were

gathered in groups. For example, the different sources used all had a criterion that covered 'Advantages' of the technique evaluated, although sometimes formulated as 'Major advantages', 'Pros', 'Relative advantages', etc. Such similar criteria were numbered with a similar Id, e.g. 1a, 1b, 1c and 1d, but with their respective descriptions provided in a separate column.

Next, a column was added headed by 'Use in template?', which gave room for assessment if the criterion could be used in the eventual template format. These last assessments were subsequently developed by EUROCONTROL staff, in a few iterations. The possible assessments were:

- D - The criterion is descriptive. It will/can/should be used to describe the method or technique, but not as a criterion to compare it with other methods.
- E - The criterion will be used in the template to compare the method or technique with other techniques
- N - The criterion does not have to be used in the template.

Often, a criterion was selected for the template, but in combination with other criteria. For example, 'Availability of the technique' was combined with 'Availability of supporting tools', in a new criterion named 'Availability and tool support'.

The complete assessment results are provided in the technical annex to this report [Technical Annex].

4.3 Template format developed

The final step was to gather the evaluation criteria selected into a template format. The criteria assessed with a 'D' (descriptive) were listed first, and the criteria assessed with an 'E' (evaluation criteria) were listed next with a different background colour. All criteria were ordered in a way that seemed 'logical', in terms of readability. The result is given below.

'Name of the technique'	
References used:	References to books and papers used for the assessment of the technique
Alternate names:	Other names or speciality 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 practised the use of the technique
Applicability range:	Does the technique assess humans (human error, human behaviour), equipment (hardware, software, including HMI) or procedures/organisation?
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 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:	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 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:	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 utilised 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.
Relevance to ATM:	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.
Con's and resources:	Any restrictions on applicability, e.g. problem scale, generality, accuracy, ease of use, cost, availability, maturity, use of resources, data requirements, etc.

5. Results of a Safety Techniques Selection Process

This section provides the main results of the safety techniques selection process. The aim of this procecss was to make a selection of about 20 techniques from the list of about 500 candidate techniques gathered. Section 5.1 explains the aim of the selection process that was used. Section 5.2 provides the list of techniques eventually selected. Section 5.3 provides another output of the process: a list of areas that deserve further research and development. For more details on the process, see [Technical Annex].

5.1 Aim of selection process

The process consisted in a review of the list of candidate safety assessment techniques gathered (i.e. about 500 techniques), and in a selection from this list of about 20 techniques that would be evaluated in more detail, using a template format. The techniques that would come out of the detailed evaluation process positively, could be recommended by EUROCONTROL to support the EATMP Safety Assessment Methodology SAM Guidelines.

A division of the list of techniques was made into 9 groups:

Group		**# elements**
1	Databases	5
2	Generic terms (rather than specific techniques)	77
3	Mathematical models	29
4	Individual techniques and Integrated methods (i.e. methods that use two or more techniques), used for both hardware and software dependability, or for hardware dependability only	49
5	Individual techniques and Integrated methods, used for software dependability	83
6	Risk assessment techniques	96
7	Human performance techniques	79
8	Hazard mitigation techniques	32
9	Integrated methods, other than those already included in groups 4 and 5	54

Within a group, the techniques were ordered on age (if known), the oldest techniques first.

During the process, a selection of experts went through all techniques, one group at the time, and assessed which techniques would not pass the selection, which would definitely get selected for further evaluation, and which were borderline (i.e. possibly of use). If the list of borderline techniques was too long, then a further classification within the group was applied, and one technique from each class could be selected.

The initial criteria for not selecting a technique were:

- Inappropriate or not suitable for ATM safety assessment (e.g., specifically for safety assessment in nuclear or chemical process plants)
- Outdated; not used (anymore)

- Superseded by another technique on the list
- Less suitable for SAM than another technique on the list
- Proprietary to a particular organisation (and hence unavailable in the public domain)
- Commercial tool (EUROCONTROL does not want to promote one commercial tool over another)
- Too general; more a generic term than a specific technique
- Too specific, detailed or limited

The list of candidate techniques included some very useful techniques that would pass these initial de-selection criteria, but that would still not be selected for a template in the next phase of the project. These criteria were:

- Already addressed by SAM (for example, SAM is already addressing software assessment techniques in its recommendations documents)
- Not sufficiently developed at this stage
- More useful for design than for safety assessment

In the last two cases, further development could be considered within EUROCONTROL's SAFMOD or SAFBUILD projects.

For more details on the workshop and the selection process, see [Technical Annex].

5.2 List of selected techniques

The workshop selection process eventually led to the following list of techniques to be evaluated using a template format, in alphabetical order, and with the main reason for selection indicated:

Nr	Technique	Main reason for selection
1.	Bias and Uncertainty assessment	An important step in any model-based evaluation, including sensitivity evaluations.
2.	Bow-Tie Analysis	Major integrative approach used in several industries.
3.	CCA (Common Cause Analysis)	Common causes are often very important sources of safety critical situations.
4.	ETA (Event Tree Analysis)	This technique is well known, very popular and often used. However the limitations of the technique are often forgotten and it can be abused. For this reason it deserves more detailed guidance for ATM usage.
5.	External Events Analysis	This technique was selected since events that influence the system from the outside (including interactions at the 'boundaries' of the system being considered) may have a significant impact on safety
6.	FMECA (Failure Modes Effects and Criticality Analysis)	Very popular hazard identification technique for technical systems. Covers the also popular FMEA, hence was selected in favour of FMEA.
7.	FTA (Fault Tree Analysis)	This technique is well known, very popular and often used. However the limitations of the technique are often forgotten and it is sometimes abused. For this reason it deserves more detailed guidance for ATM usage.
8.	HAZOP (Hazard and Operability	One of the most popular hazard identification techniques.

	study)	Its popularity is partly due to it being promoted and used as a solution generator. Hence, it deserves evaluation.
9.	HEART (Human Error Assessment and Reduction Technique)	One of the more accurate and useful approaches to quantify human error values if no statistical data are available. JHEDI would be a competitor for a template, but is not publicly or commercially available.
10.	HTA (Hierarchical Task Analysis)	Basic task analysis approach, used for three decades in many industries. The disadvantage of HTA is that it tends to focus on the "what" rather than the "why" of tasks and subtasks. However, it is well defined, whereas many other techniques, such as Cognitive Task Analysis, exist in many variations, not just one.
11.	HTRR (Hazard Tracking and Risk Resolution)	Selected in order to have on the list a technique that maintains a systematic list of how each identified hazard is addressed or resolved in the system development life cycle.
12.	Human Error Data Collection	Reason of selection is to see whether it can support a programme of human error probability data collection in the ATM area; this would be useful in the PSSA stage of the SAM.
13.	Human Factors Case	New rapid evaluation technique developed in HUM in EUROCONTROL for addressing Human Factors issues; deserves evaluation for SAM.
14.	ORR (Operational Readiness Review)	One of the techniques used in other industries to ensure a safe transition to operations. Something similar is required for ATM especially given the amount of change that will happen to ATM in the near and mid-term.
15.	RCM (Reliability Centred Maintenance)	Reason for selection is that it is one of the few techniques covering maintenance, a significant source of error and risk in other industries.
16.	SFMEA (Software Failure Modes and Effects Analysis)	Reason for selection is that there is a growing dependency on software-mediated systems in ATM. There is a need to consider software-caused risks, and risks from interactions between software and hardware/lifeware.
17.	SMHA (State Machine Hazard Analysis)	Reason for selection is that a modelling technique for software should be on the list.
18.	TRACER-Lite (Predictive Technique for the Analysis of Cognitive Errors)	Leading technique for human error assessment in ATM.
19.	Use of Expert Judgement	Expert judgement is very often used, especially where statistical data is scarce, but needs to be treated with special care. There are well-proven protocols for maximising and testing its validity. Therefore, it deserves a template.

In Section 6 of this document, each of these techniques is evaluated using the template format developed in Section 4.

5.3 Areas for further research and development

The previous section listed 19 techniques identified by the Safety Techniques Workshop that it is believed can support the EATMP Safety Assessment Methodology (SAM) either immediately, or with some tailoring or adaptation to the ATM context. These 19 techniques are therefore for short-term implementation. However, in addition to these techniques that are evaluated according to a template format, the project workshop identified several techniques that are judged to be significantly important and therefore deserve consideration for further development by EUROCONTROL. It should be noted that for some of these areas, further developments for ATM are already well underway, either inside or outside EUROCONTROL. The areas are:

- Understanding cognitive behaviour and errors of commission of a human agent
- Understanding cognitive behaviour in interactions with other humans and systems
- Formal approaches to master complexity of Air Traffic Management
- Organisational learning
- Safety data bases
- Safety culture maturity

These areas and their importance for safety assessment are further outlined in Section 7.

6. Evaluated techniques

This section provides an evaluation of the 19 safety assessment techniques selected during the Safety Techniques Workshop, according to the template format as provided in Section 4.

6.1 Bias and Uncertainty Assessment

Bias and Uncertainty Assessment

References used:	Key references: • [Everdij&Blom02] Other references: • [FT handbook02] • [Henley&Kumamoto92] • [Kumamoto&Henley96] • [Nurdin02]
Alternate names:	None
Primary objective:	When risk (e.g. accident risk) is assessed using a 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 modelling, 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. However, the technique can be applied to any model-based output (including output of fault trees). 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 substeps 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.

6.2 Bow-Tie Analysis

Bow-Tie Analysis

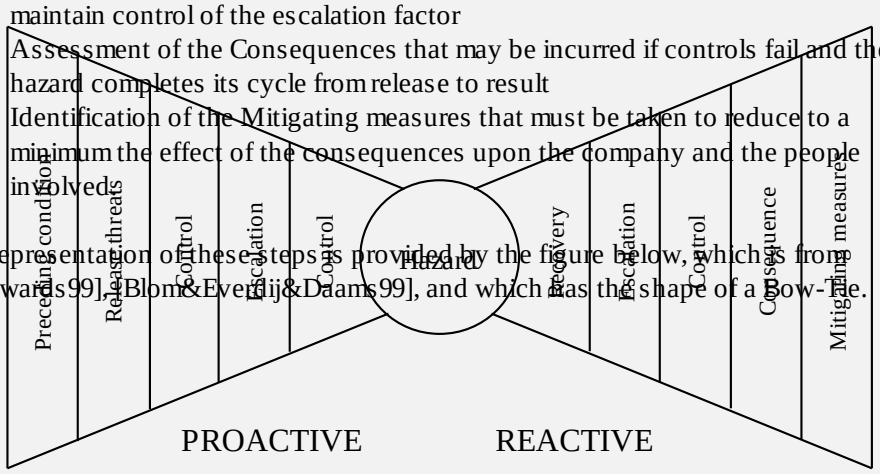
References used:	Key references: • [Edwards99] • [Zuijderduijn99] Other references: • [Bishop90] • [Blom&Everdij&Daams99] • [DNV-HSE01] • [EHQ-PSSA] • [EN 50128] • [GenericBT] • [MHF-RGN10] • [Rademakers&al92] • [SGS-FSR] • [Trbojevic&Carr99] • [Villemeur91-1] Additional reading: • [Petrolekas&Haritopoulos01]
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:	Bow-Tie Analysis is used by Safety experts to communicate with Operational experts. 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 stages worked through in a Bow-Tie are [Edwards99] (note that some terminology has been changed in these steps in order to match SAM recommendations, i.e. “Hazard” has been changed into “Preceding condition”, and “Hazardous event” has been changed into “Hazard”) Proactive measures:

- Identification of the Preceding condition
- Identification of the Threats that could release the Preceding condition
- Assessment of the Threat controls already in place and the identification of additional controls that may be necessary to manage the threat effectively
- Identification of the Escalation factors that are conditions that prevent a threat control being effective
- Assessment of the Escalation controls which are further measures needed to maintain control of the escalation factor
- Identification of the Hazard that can lead to an accident

Reactive measures:

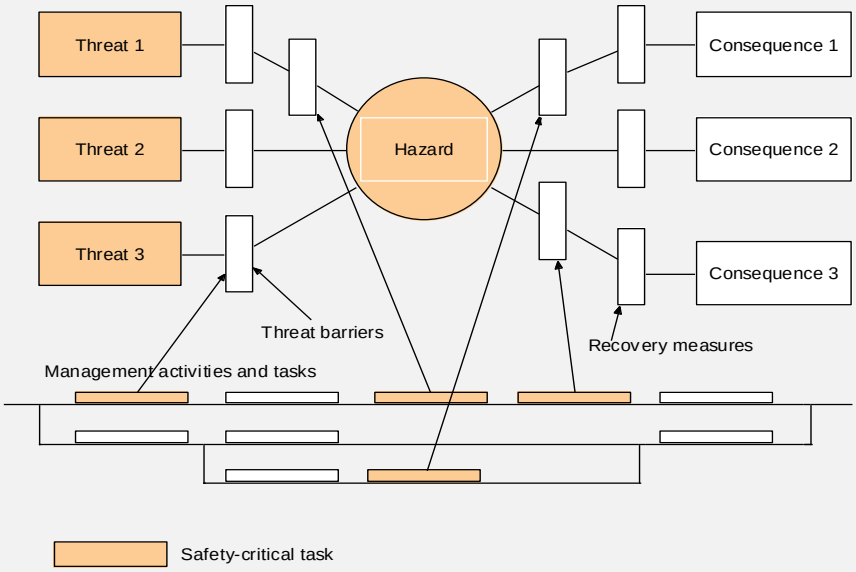
- Assessment of the Recovery measures that would be appropriate to return the situation to as near to normal as possible
- Identification of the Escalation factors that are conditions that prevent a recovery measure being effective
- Assessment of the Escalation controls which are further measures needed to maintain control of the escalation factor
- 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 below, which is from [Edwards99], [Blom&Everdij&Daams99], and which has the shape of a Bow-Tie.

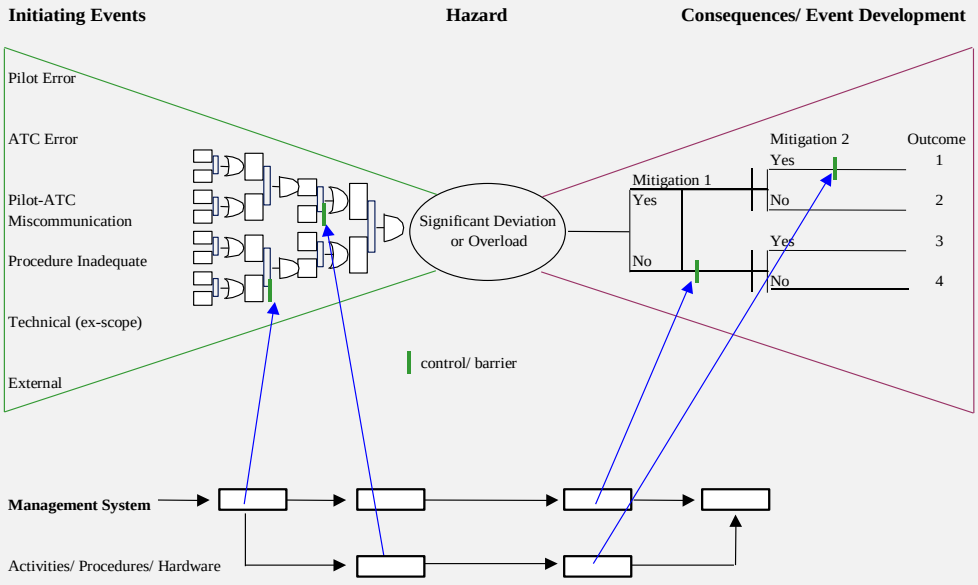


The pictorial representation of the Bow-Tie exists in several versions, depending on the application and preferences of the users. Still, in most representations, the knot of the Bow-Tie represents a Releasing Event, the left-hand side wing includes hazards leading to threats that can cause the releasing event, the right-hand side wing includes consequences of the releasing event. However, in order to match SAM recommendations, in this template, all referenced figures have been changed by putting the Hazard in the knot of the Bow-Tie, its causes and threat barriers in the left-hand side wing, and its consequences and recovery measures in the right-hand-side wing.

One version presented in the figure below seems to be often used, and is taken from [Trbojevic&Carr99].



In a more specific 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); see for an example the figure below, which is from [EHQ-PSSA]. The Bow-Tie in this figure is specific for the PSSA step of SAM.



Whichever Bow-Tie representation is used, the diagram size is preferably limited to a single A3 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. Short-hand notations make these diagrams much more compact and allow a complex tree to be captured on one page.

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.
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.
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 colour coding can be used to differentiate technical and procedural safeguards, and potentially the role of specific individuals or groups. [DNV-HSE01]
Relevance to ATM:	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
Con's and resources:	Once a good Bow-Tie is produced, the resources required to use it in communication with operational experts are rather limited. 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).

6.3 CCA (Common Cause Analysis)

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 analysed includes COTS (Commercial Off The Shelf) equipment or software. 4. It is difficult to know where to stop the analysis.

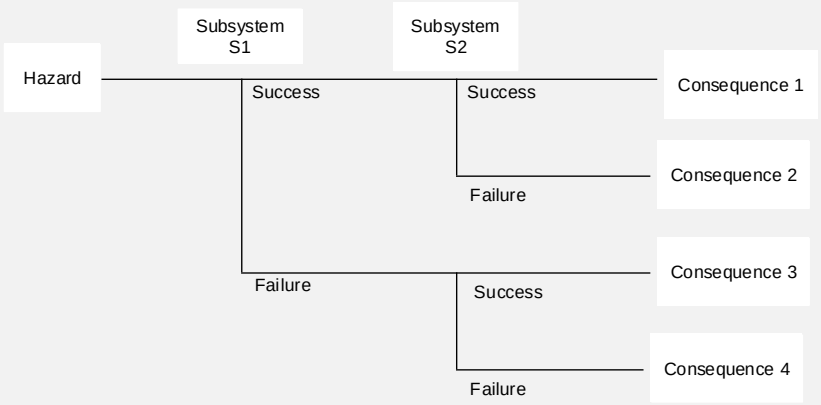
6.4 ETA (Event Tree Analysis)

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 generalisation 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 modelled. They can be extended to include accident scenarios in which the operating crew is treated in a behavioural 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 enormously time-consuming, sometimes many person-years of effort. The exploration of all wanted and unwanted events and their consequences, increases the effort substantially beyond that required for FTA or FMEA. 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 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.

6.5 External Events Analysis

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 analysed. 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 modelling 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 substeps 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 specialised expertise.

6.6 FMECA (Failure Modes Effects and Criticality Analysis)

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. 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.
7. Re-evaluate the RPN based on the new estimates of the severity, occurrence, and detection rankings.

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) programmes 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.
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 a number of 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.
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 generalisation of FMEA is the Truth Table Method, see [Villemeur91-1]. Another extension and generalisation is Gathered Fault Combination Method (GFCM), see [Villemeur91-1].
Availability and tool support:	The technique is widely available. Supporting tools exist.
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].

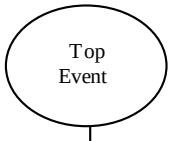
Acceptability:	Recommended in all system reliability analyses, in particular for safety critical hardware systems where reliability data of the components is available. The final document of a FMEA analysis is often used in a formal way to certificate the system, if no other dependability study is available. 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 integration:	The output of FMECA can be used for FTA. The level of mastery needed to perform the 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.
Relevance to ATM:	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. 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]
Con's and resources:	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 labour 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 optimised 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]

6.7 FTA (Fault Tree Analysis)

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. H



	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 analyse 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

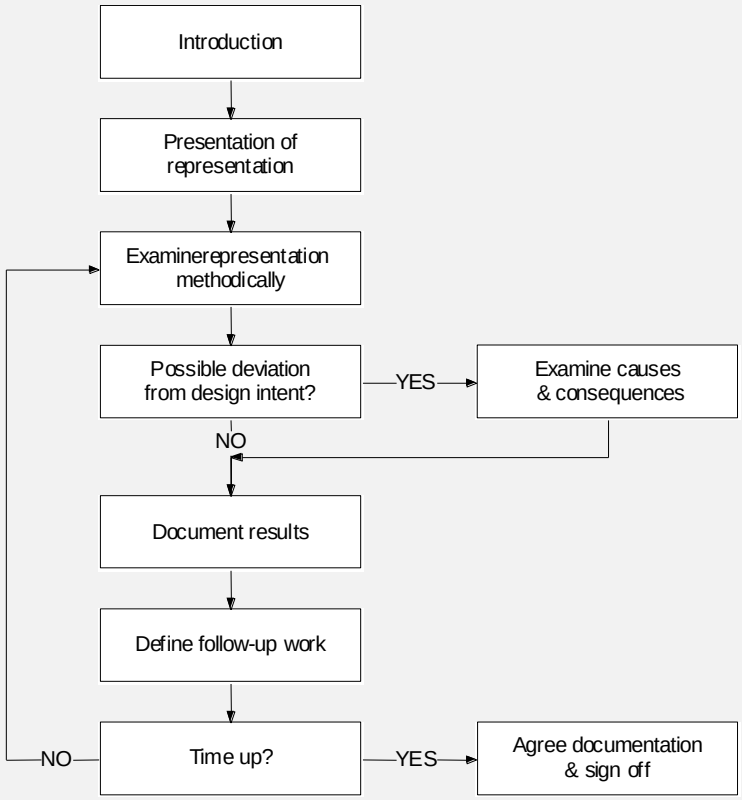
	probability of occurrence of a minimal cut set is taken equal to the product of the probabilities of occurrence of its basic events, provided there are no dependent events in a minimal cut set. The probability of the top event is equal to the sum of the probabilities of the minimal cut sets, provided 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. 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. 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. [Howat02] gives a nice introduction to FTA. [Henley&Kumamoto92] give an extended explanation, covering most FTA issues. See [FT handbook02] for a complete overview of FTA, including examples to Aerospace applications.
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 analysed, and their contributors, must be foreseen, and each of the undesirable system events must be analysed individually.
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. 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 e.g. [Kumamoto&Henley96] for a list.
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 utilisation. 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.
Relevance to ATM:	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.
Con's and resources:	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 standardised 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 is rather difficult to understand and 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 behaviour (except for human error) are not addressed particularly well. 9. FTA can account for some dependencies only, by using additional approximative 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. Whilst 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]

6.8 HAZOP (Hazard and Operability study)

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 behaviour, prompted by guidewords. The consequences of deviations from the intended functioning of the system are also considered. The five HAZOP requirements are [Kennedy slides]: 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, i.e. • 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 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 [Kennedy slides].  [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. 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”.
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 analysing 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.
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).
Relevance to ATM:	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 recognises existing safeguards and develops recommendations for additional ones. 3. Unlike FMEA it does not require the systematic study of the failure modes of each 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 organisations 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.
Con's and resources:	According to some references, a HAZOP can be very time consuming and labour 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 optimised 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 behaviour, but it does not analyse whether the design, under normal operating conditions, yields expected behaviour or if the expected behaviour 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 favour 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.

6.9 HEART (Human Error Assessment and Reduction Technique)

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 judgement, 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 modelling 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 Judgement; 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

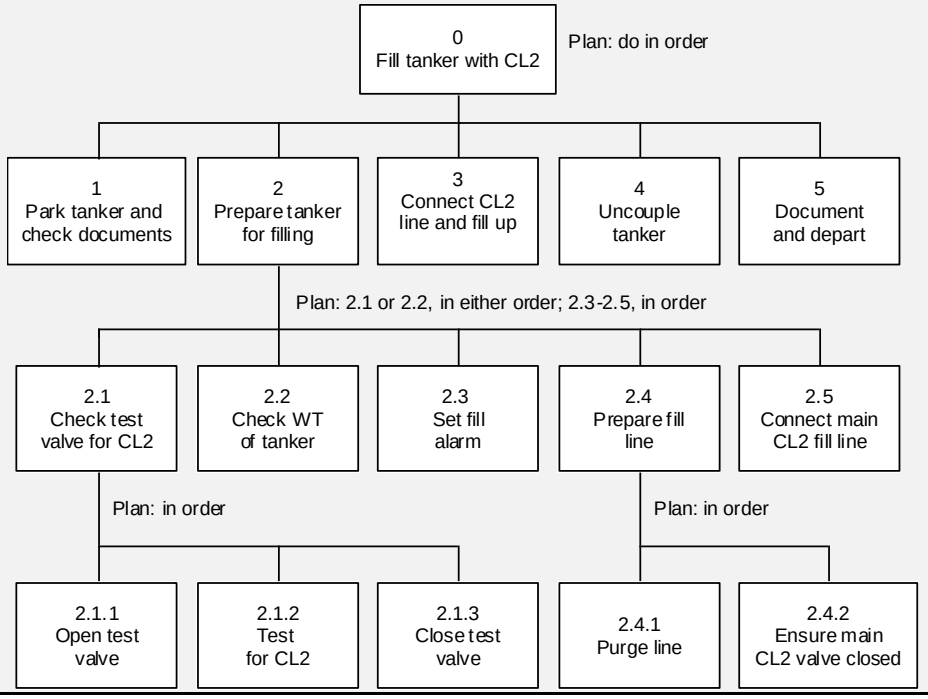
<table>
<tr><td></td><td>on these criteria by a panel of experts, in the form of marks from 1 to 5, where 5 means evaluated high (positive) and 1 means evaluated low (negative). These criteria evaluations are next weighted and added for each technique. The results are presented in the table below. According to this table, HEART receives the highest Preference Index of the techniques evaluated.
<table>
<tr><th>Criteria (weight)</th><th>APJ</th><th>PC</th><th>TESEO</th><th>THERP</th><th>HEART</th><th>IDA</th><th>SLIM</th><th>HCR</th></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>
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.</td></tr>
<tr><td>Ease of integration:</td><td>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.</td></tr>
<tr><td>Documentability:</td><td>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.</td></tr>
<tr><td>Relevance to ATM:</td><td>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</td></tr>
</table>

	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 modelled 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 modelling of task / error dependence

6.10 HTA (Hierarchical Task Analysis)

HTA (Hierarchical Task Analysis)

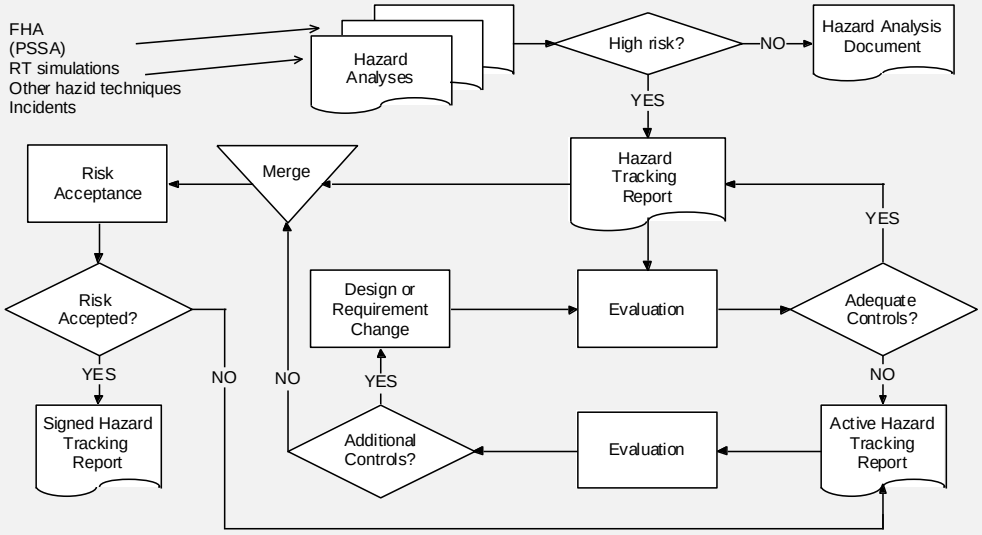
References used:	Key references: • [Shepherd01] • [Kirwan&Ainsworth92] • [Kirwan94] Other references: • [Kirwan&al97] • Additional reading: • [Stanton&Wilson00]
Alternate names:	None
Primary objective:	HTA is a method of task analysis that describes tasks in terms of operations that people do to satisfy 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 judgement 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 organisation, 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 organising 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 modelling 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 organisations 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 analyse 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.

6.11 HTRR (Hazard Tracking and Risk Resolution)

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 realised (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.

6.12 Human Error Data Collection

Human Error Data Collection

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 (Computerised 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 categorised. 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 programme 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	Some preliminary work has been carried out to generate a small number of human

application to air traffic:	error probabilities as part of the ongoing CORE-DATA work programme.
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 computerised 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.

6.13 Human Factors Case

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. • Organisation 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 Programme 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.

6.14 ORR (Operational Readiness Review)

ORR (Operational Readiness Review)	
References used:	Key references: • [DOE-3006] • [Dryden-ORR] Other references: • [Enterprise-ORR] • [ESH-ORR] • [MDA press release97] Additional reading: • [NNSA-ORR], [ΣΣ97]
Alternate names:	Transition Study
Primary objective:	An ORR is a structured method for determining that a project, process, facility or software application is ready to be operated or occupied (e.g. a new Air Traffic Control Centre; a new tower; a new display system, etc.). The ORR is used to provide a communication and quality check between Development, Production, and Executive Management as development is in the final stages and production implementation is in progress. This process should help management evaluate and make a decision to proceed to the next phase, or hold until risk and exposure can be reduced or eliminated. This review process can also be used to evaluate post operational readiness for continuing support and will also provide information to make necessary system/procedural modifications, and error and omissions corrections.
Description:	The details of the ORR will be dependent on the application. For example, for complete facilities such as NASA-DFRC (Dryden Flight Research Center), the review is done by an independent Committee, the members of which have to conform to certain guidelines (see [Dryden-ORR] for such guidelines). The purpose for the ORR is to verify that the facilities being started up or restarted: • Are constructed in accordance with the approved design and requirements; • Can be operated safely and efficiently; • Will be operated, maintained, and supported by trained and competent personnel; • Are designed and will be operated in conformance with applicable standards and regulatory requirements; • Will be operated so that there is no undue risk to employees, the public, the environment, the stockholders, or the corporation results; • All of the activities noted above are formally and adequately documented. A proper ORR will keep the facility or operation in compliance and cost effective. The functions of the Committee who is to perform the facility ORR includes or should include: 1. Conducting an independent review and assessment of the total program or operation and ensure that adequate and proper planning and preparation is accomplished to result in meeting required objectives under acceptable safety conditions. A major goal is the development of current and correct operating instructions effective configuration control, and positive safety and quality procedures. 2. Providing engineering and technical recommendations to concerned personnel, while recognising that it is not a function of the Committee to request or direct the actual work effort.

	3. Maintaining effective communication among Committee members, program/operation personnel, and the Centre Director or his representative. 4. Submitting a formal report of Committee activity, findings, and recommendations to the Centre Director or his representative. Submittal of this report should be early enough in the schedule to allow for timely and effective action as required. An Operational Readiness Review Checklist may be used by concerned operational / support personnel and the ORR Committee to help determine that specific requirements have been considered and are properly complied with or are not applicable to the operation. A NASA-DFRC (Dryden Flight Research Center) Operational Readiness Review Checklist is available at [Dryden-ORR]. It covers issues like Facility, Support Services, and Equipment and Process Control; Organisation and Staffing; Safety, Health, and Environmental Control; Tests and Operations; Field Centre Considerations; Any other factors having a direct or indirect bearing on the safe operation of the facility, equipment, or processes or its ability to support critical program needs. [DOE-3006] gives a full description and requirements for ORR for Nuclear facilities. An ORR for other applications, such as for implementation of an application software system, may follow other details. According to [Enterprise-ORR], the deliverables from an ORR are as follows: • A presentation to Executive Management reviewing the system readiness with assessments of business expectations, risks, and exposures. • A report containing check lists and readiness evaluation criteria from each functional area affected by the system changes. • Disposition and/or schedule for completion of unfinished activities or unresolved concerns with business risk or exposures explained. And the following procedures should be followed: • A Check list should be prepared for each functional area containing questions related to the preparedness of that function for a successful implementation. • These check-lists should be completed for each department within each functional area. They are then delivered to the Implementation Project Manager. • These evaluation check-lists should contain any exposures or risk concerns with expected resolution decisions or completion dates. • All of the check-lists should be reviewed with Project Management and summarised based on priority and exposure or risk. • The decision to proceed or schedule a new implementation date is made. • All scheduling decisions and mandatory requirements should then be communicated to the implementation team. Resources are adjusted to provide the most efficient implementation with lowest possible risk. • The ORR check-lists should be maintained until completion of all critical tasks. These check-lists should be used as input to the next phase of the Continuous Improvement Process. Enterprise Application Software Systems provides an Online check-list at [Enterprise-ORR] (only application component review portion). For both Software Readiness and Data Requirements Review, it covers issues such as Data Conversions, Documentation, Training, Dependencies, Alternative Capabilities, IT Maintenance.
Applicability range:	ORR is applicable to an operation, process, project or facility, and to software applications.
Life cycle stage:	The ORR precedes the occupancy or operation at a time when credible review and assessment can be made without delaying the operational schedule. For example, for

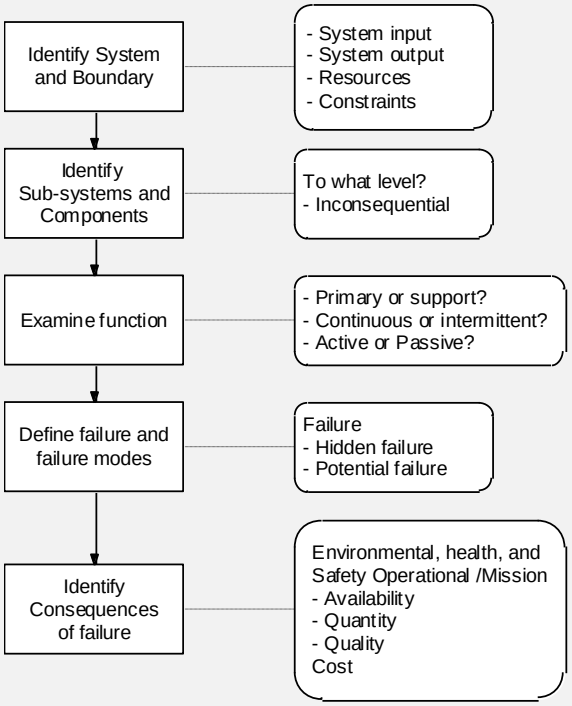
	complete facilities, the performance-based review is performed, driven by current regulatory and institutional requirements, by an independent Committee when the new facility is started up or an existing facility is restarted after an extended shutdown for modifications, repairs, or other reasons. For software applications, an ORR should take place as the System Testing and implementation preparations are being completed.
Experience in application to air traffic:	ORRs are being and have been performed for several ATM systems in Europe. An ATCC system that passed an ORR in 1997 is described in [MDA press release97]. Certain other new centres in Europe have undergone or are undergoing their own form of acceptance testing and readiness reviews. The EGNOS system (European Geostationary Navigation Overlay System) system will be subject to an ORR in 2004.
Related methods:	Link to MORT (Management Oversight and Risk Tree Analysis) An Accelerator Readiness Review (ARR) is a structured method for verifying that hardware, personnel, and procedures associated with the commissioning of routine operations are ready to permit the activity to be undertaken safely. [ESH-ORR] There is a potential useful link to Hazard Tracking and to Organisational Learning, since hazards may be identified in the very late (transition) stages prior to implementation and operation of a new system. Such hazards may arise because the system is being finally tested on the exact local conditions and traffic patterns, and being adapted to local controller working practices and methods. Errors or problems at this point must be tracked and resolved or monitored accordingly as the system proceeds towards operation. Information at this stage may also be useful for tailoring training to the whole controller community that will operate the system.
Availability and tool support:	The ORR technique is available for various applications. Tools support will mostly comprise checklists.
Maturity:	1990 or older. The ORR process is used in many industries. ORR techniques were used to guide the construction of a major nuclear waste management facility at Argonne-West.
Acceptability:	ORR is required for the startup or restart of U.S. Department of Energy (DOE) facilities [DOE-3006].
Ease of integration:	ORR usually requires a high level of expertise in both the application to be assessed and in evaluation methods.
Documentability:	A high level of documentability is essential for the level of confidence in the results. Standard forms are available to document the review findings.
Relevance to ATM:	ORR can be relevant for ATM applications both at a subsystem level (e.g. introduction of a new software application) and at a system level (e.g. return to operation of a modified ATC centre). General advantages are: 1. The approach is structured and comprehensive. 2. An ORR can provide information for modifications or for mitigating measures for main hazards and evaluate post operational readiness for continuing support. 3. An ORR can find previously missed hazards, 'bugs' or vulnerabilities in the system, and can resolve or otherwise prepare for these in actual operation.
Con's and resources:	The resources required depend on the application. Ideally, the ORR should be performed by independent experts, who have sufficient knowledge of the system or facility concerned, and of evaluation processes and methods. A full ORR, including all preparations, communications, consolidations, reporting and post-actions (e.g. lessons learned), generally takes a lot of time. General weaknesses are:

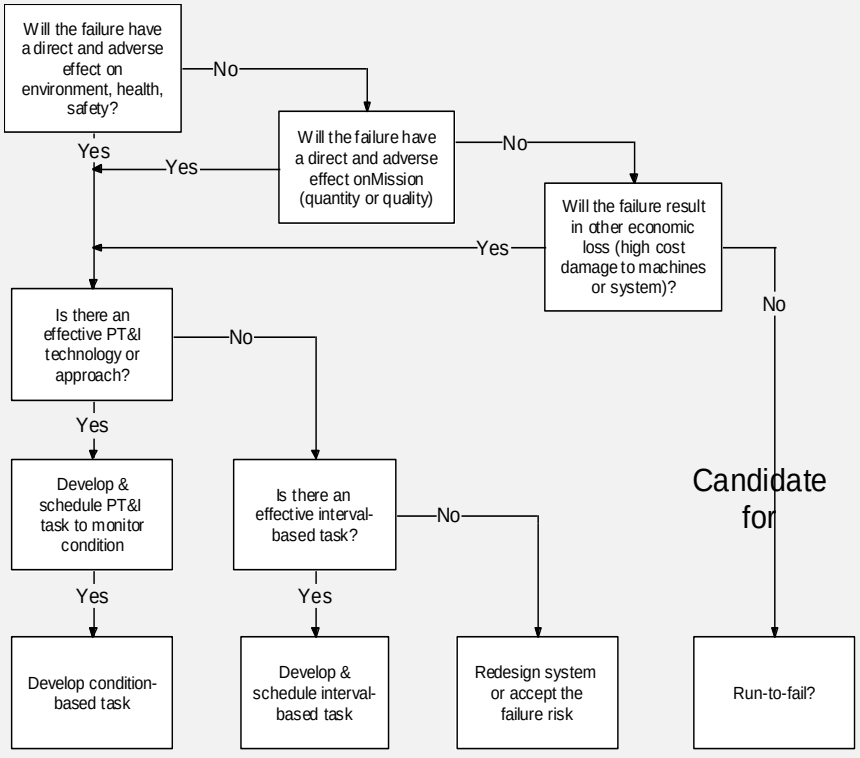
	1. The checklists are application-dependent. If they are applicable to a set of similar applications, they may be too general to pick up all operational readiness details. If they are too specific for a particular application, they may need extensive modification and review before they can be applied to another application. 2. For systems or facilities where the human tasks are very complex, simple checklists are not sufficient; additional human factors analysis techniques should support the review. 3. It may be difficult to find independent review experts who have the required expertise.

6.15 RCM (Reliability Centred Maintenance)

RCM (Reliability Centred Maintenance)	
References used:	Key references: • [Cotaina&al00] • [Rausand&Vatn98] Other references: • [Moubray00] • [NASA-RCM] • [SINTEF-RCM] Additional reading: • [Relex-RCM]
Alternate names:	The industrial version of RCM is known as RCM 2.
Primary objective:	Reliability Centred Maintenance (RCM) is the concept of developing a maintenance scheme based on the reliability of the various components of the system or product in question. RCM can improve the efficiency of the system undergoing maintenance, and all other products or processes that interact with that system - allowing one to anticipate the times when the system is down for maintenance, and scheduling other activities or processes accordingly. RCM can help to inform the safety of all aspects of maintenance operations, including determining what maintenance intervals to adopt to maximise safety, and what combinations of concurrent maintenance of equipment sub-systems are risky.
Description:	There is no common approach to RCM. Adaptations are used in the various industries. Reference [Cotaina&al00] gives a very good overview. According to [NASA-RCM], the RCM philosophy employs Preventive Maintenance (PM), Predictive Testing and Inspection (PT&I), Repair (also called reactive maintenance) and Proactive Maintenance techniques in an integrated manner to increase the probability that a machine or component will function in the required manner over its design life cycle with a minimum of maintenance. There are many paths or processes that lead to the final goal. [NASA-RCM] specifies three of these paths: 1. Rigorous RCM analysis. This has been used extensively by the aircraft, space, defence, and nuclear industries where functional failures have the potential to result in large losses of life, national security implications, and/or extreme environmental impact. It is based on a detailed FMECA and includes probabilities of failure and system reliability calculations. The analysis is used to determine appropriate maintenance tasks to address each of the identified failure modes and their consequences. 2. Streamlined or Intuitive RCM analysis. This is more appropriate to use for facilities systems maintenance, due to the high analysis cost of the rigorous approach, the relatively low impact of failure of most facilities systems, the type of systems and components maintained, and the amount of redundant systems in place. The streamlined approach uses the same principles as the rigorous one (i.e. FMECA), but recognises that not all failure modes will be analysed. 3. A combination of rigorous (formal) and intuitive analysis. This is sometimes the most economical and efficient approach, depending on system criticality and failure impact. For example, if a streamlined or intuitive RCM process has been utilised and the resultant reliability is still unacceptable in terms of safety, cost, or mission impact, an additional more rigorous analysis may be taken.

The two figures below illustrate the RCM approach and the interactive streamlined process according to [NASA-RCM]. Note that in other references, and for other industries, different approaches have been developed. See for example [Cotaina&al00].



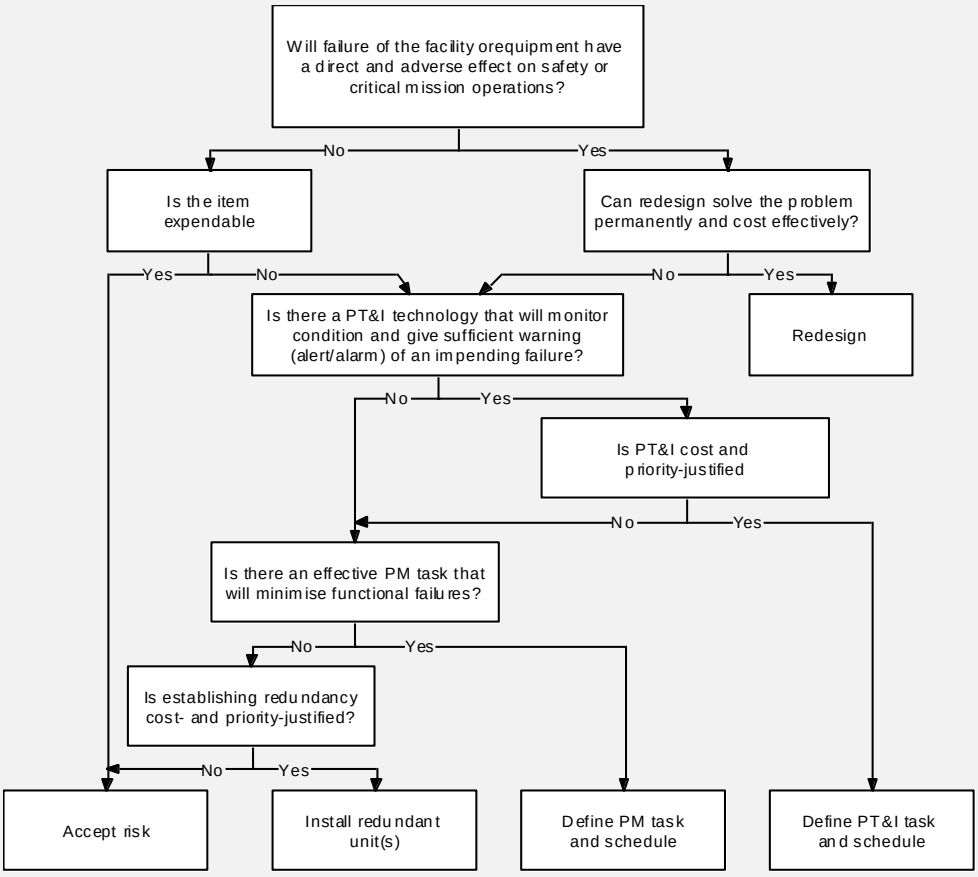


Note that the maintenance analysis process, as illustrated in the last figure, has only four possible outcomes:

- Perform Interval (Time- or Cycle-)-Based actions

- Perform Condition-Based actions
- Perform no action and choose to repair following failure
- Or determine that no maintenance action will reduce the probability of failure AND that failure is not the chosen outcome (Redesign or Redundancy).

A formal RCM analysis of each system, subsystem, and component is normally performed on new, unique, high-cost systems such as aircraft and spacecraft systems and structures. This approach is rarely needed for most facilities and collateral equipment items because their construction and failure modes are well understood. Regardless of the technique used to determine the maintenance approach, the approach must be reassessed and validated. The following figure depicts an iterative RCM process that can be used for a majority of facilities and collateral equipment.



[NASA-RCM] lists the eleven RCM principles and gives details: 1) RCM is Function Oriented; 2) RCM is System Focused; 3) RCM is Reliability Centred; 4) RCM Acknowledges Design Limitations; 5) RCM is Driven by Safety and Economics; 6) RCM Defines Failure as Any Unsatisfactory Condition; 7) RCM Uses a Logic Tree to Screen Maintenance Tasks; 8) RCM Tasks Must Be Applicable; 9) RCM Tasks Must Be Effective; 10) RCM Acknowledges Three Types of Maintenance Tasks; 11) RCM is a Living System.

According to [SINTEF-RCM], there is no common approach to an RCM analysis, but according to their experience the following steps have been found to cover the main elements of an RCM analysis:

1. Study preparation
2. System selection and definition
3. Functional failure analysis
4. Critical item selection

	5. Data collection and analysis 6. FMECA 7. Selection of maintenance actions 8. Determination of maintenance intervals 9. Preventive maintenance comparison analysis 10. Treatment of non-critical items 11. Implementation 12. In-service data collection and updating The industrial version of RCM is named RCM 2, which is a process used to decide what must be done to ensure that any physical asset, system or process continues to do whatever its users want it to do. What users expect from their assets is defined in terms of primary performance parameters such as output, throughput, speed, range and carrying capacity. Where relevant, the RCM 2 process also defines what users want in terms of risk (safety and environmental integrity), quality (precision, accuracy, consistency and stability), control, comfort, containment, economy, customer service and so on. The next step in the RCM 2 process is to identify ways in which the system can fail to live up to these expectations (failed states), followed by an FMEA (failure modes and effects analysis), to identify all the events which are reasonably likely to cause each failed state. Finally, the RCM 2 process seeks to identify a suitable failure management policy for dealing with each failure mode in the light of its consequences and technical characteristics. Failure management policy options include: - predictive maintenance - preventive maintenance - failure-finding – change the design or configuration of the system - change the way the system is operated – run-to-failure. The RCM 2 process provides powerful rules for deciding whether any failure management policy is technically appropriate. It also provides precise criteria for deciding how often routine tasks should be done. Heavy emphasis on the expectations of the user is one of the many features of RCM 2 that distinguish it from other less rigorous interpretations of the RCM philosophy. Another is the use of cross-functional RCM review groups of users and maintainers to apply the process. With careful training, such groups are able to use RCM 2 to produce robust and cost-effective maintenance programs, even in situations where they have access to little or no historical data. [Cotaina&al00] notes that in other industries, e.g. the chemical industry, many more hazard identification and analysis techniques are used for RCM, in addition to FMEA or FMECA (which are less applicable for chemical processes), such as What-If Analysis, Checklist Analysis, What-If/Checklist Analysis, Hazard and Operability (HAZOP) Analysis, FTA.
Applicability range:	RCM is applicable to hardware systems.
Life cycle stage:	RCM is done during the operational stage of the lifecycle.
Experience in application to air traffic:	RCM has its roots in the aviation industry. RCM has been used extensively in the military and commercial aerospace sector. Examples of industries in this field are airline operators (e.g. Air Canada), manufacturers, air traffic management systems and baggage handling systems. Rigorous RCM analysis has been used extensively by the aircraft, space, defence, and nuclear industries where functional failures have the potential to result in large losses of life, national security implications, and/or extreme environmental impact.
Related methods:	FMECA (Failure Modes Effects and Criticality Analysis), HAZOP (Hazard and Operability study).
Availability and	Various consulting and training courses in RCM and RCM 2 are available. In addition,

tool support:	numerous supporting tools exist, e.g. a supporting RCM 2 Toolkit, which includes RCM worksheets as well as formulas to assist in identifying such tasks as the failure finding intervals. In addition, several databases with reliability data exist. See [Cotaina&al00] for a long list of RCM tools and databases.
Maturity:	RCM finds its roots in the early 1960's, with the initial development work done by the North American civil aviation industry. The term "Reliability Centred Maintenance" was coined in a report by Stanley Nowlan and Howard Heap of United Airlines (1978). This report represented a considerable advance on RCM thinking. Nowadays, RCM, and in particular RCM 2, is extensively used in various industries. See [Moubray00] and [Cotaina&al00] for full descriptions of RCM history.
Acceptability:	RCM 2 complies with SAE Standard JA1011 "Evaluation Criteria for Reliability-Centred Maintenance RCM Processes." The standard was published in August 1999. It is a brief document setting out criteria that any process must satisfy to be called RCM when it is applied to any particular asset or system.
Ease of integration:	An important part of an effective RCM is to analyse the system or product using FMEA, which determines the different ways a system can fail. Other reliability and maintainability analyses which are important parts of RCM include FTA, which shows the specific steps involved in a system failure, whether mechanical problem or human error, and ETA, which illustrates the different consequences of component or system failure.
Documentability:	Documentability is similar as for FMECA, which is supported by standardised forms to complete, hence documentability is high. The difference is that RCM is a living process, hence the level of good documentability is more essential for its effectiveness. In the RCM concept all decisions are taken based on a set of analytical steps, all of which should be documented in the analysis.
Relevance to ATM:	Maintenance problems are often important sources of hazards in ATM, hence techniques like RCM appear to be relevant to ATM. However, RCM mainly covers hardware issues, whereas in ATM, human factors issues and procedures are also very important. Other general advantages are: 1. RCM is not a simple and straightforward way of optimising maintenance, but ensures that one does not jump to conclusions before all the right questions are asked and answers given. 2. RCM can improve the efficiency of the system undergoing maintenance, and all other products or processes that interact with that system. 3. Developing an effective RCM program will optimise the maintainability of the system - allowing anticipation of the times when the system is down for maintenance, and scheduling other activities or processes accordingly. 4. One of the most significant advantages of RCM is that it systematically analyses and documents the basis for initial decisions, and, hence, can better utilise operating experience to adjust that decision as operating experience is collected. The full benefit of RCM is therefore only achieved when operation and maintenance experience is fed back into the analysis process. 5. RCM can lead to significantly lower costs by eliminating unnecessary maintenance or overhauls 6. It leads to reduced charge of sudden equipment failure 7. It is able to focus maintenance activities or critical components 8. It leads to increased component reliability 9. It uses Cross-discipline of knowledge. For an RCM, typically, the following experts are required: System/reliability analyst, Maintenance/operation specialist, Designer/manufacturer. 10. The high documentability of the technique allows traceability of decisions

	11. The RCM way of planning and updating maintenance requires more professional skills, and is therefore a greater challenge for skilled engineers. It also provides the engineers with a broader and more attractive way of working with maintenance than what sometimes is common today. 12. RCM has the following advantages over traditional Preventive Maintenance (PM) programs: • By careful analysis of the failure consequences, the amount of PM tasks can often be reduced, or replaced by corrective tasks or more dedicated tasks. • Emphasis has been changed from periodic rework or overhaul tasks of the large assemblies/units to more dedicated object oriented tasks. Consequently, condition monitoring has been more frequently used to detect specific failure modes. • Requirement for spare parts has been reduced as a result of a better justification for replacements. • Design solutions have been discovered that were not optimal from a safety and plant economic point of view. For more advantages, see the FMECA template.
Con's and resources:	Developing an effective RCM program requires extensive knowledge about the reliability and maintainability of the system and all of its subsequent components. Some general weaknesses are: 1. RCM can have significant startup costs, in Manpower, Equipment and Training 2. There is a danger in only focusing on components that appear maintenance critical; components should not be prematurely discarded as non-critical. 3. It is often difficult to collect significant reliability data. Two reasons are that available data often concerns repair rates rather than failure rates, and failure rates dependent on the ageing process are often difficult to estimate. 4. A trade-off is required to balance the four major criteria for the assessment of the consequences of a failure (i.e. safety, environment, production availability, and economic losses) against different consequences. During the analysis, one has to quantify these measures to some extent to be able to use them as decision criteria. 5. RCM does not basically include any “tool” for deciding optimal intervals. For other general weaknesses, see the FMECA template.

6.16 SFMEA (Software Failure Modes and Effects Analysis)

SFMEA (Software Failure Modes and Effects Analysis)

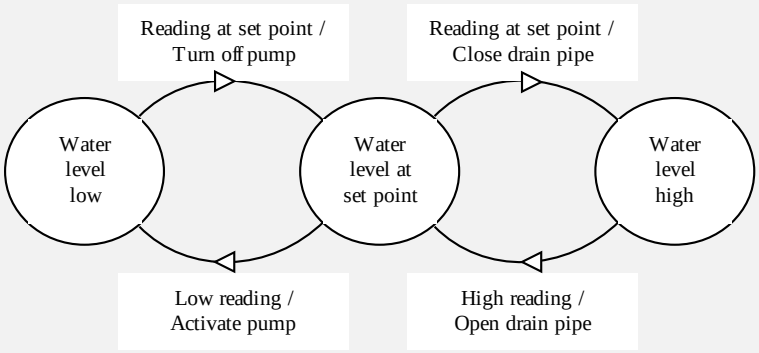
References used:	Key references: • [Pentti&Atte02] Other references: • [Ippolito&Wallace95] • [ΣΣ93, ΣΣ97] Additional reading: • [FAA00], [Lutz&Woodhouse96]
Alternate names:	Software Fault Hazard Analysis (SFHA), Software Hazardous Effects Analysis (SHEA). Software FMEA is sometimes abbreviated to SWFMEA.
Primary objective:	This technique identifies software related design deficiencies through analysis of process flow-charting. It also identifies areas for verification/ validation and test evaluation. It can be used to analyse control, sequencing, timing monitoring, and the ability to take a system from an unsafe to a safe condition. This should include identifying effects of hardware failures and human error on software operation. It uses inductive reasoning to determine the effect on the system of a component (includes software instructions) failing in a particular failure mode.
Description:	SFMEA was based on FMEA (which analyses hardware) and has a similar structure. The performer of SFMEA has to find out the appropriate starting point for the analyses, set up a list of relevant failure modes and understand what makes those failure modes possible and what are their consequences. The failure modes in SFMEA should be seen in a wide perspective reflecting the failure modes of incorrect behaviour of the software and not for example just as typos in the software code. The failure mode and effects analysis for hardware or software has certain distinguishing characteristics: [Pentti&Atte02] Hardware FMEA: • May be performed at functional level or part level. • Applies to a system considered as free from failed components. • Postulates failures of hardware components according to failure modes due to ageing, wearing or stress. • Analyses the consequences of these failures at system level. • States the criticality and the measures taken to prevent or mitigate the consequences. Software FMEA: • Is only practicable at functional level. • Applies to a system considered as containing software faults that may lead to failure under triggering conditions. • Postulates failures of software components according to functional failure modes due to potential software faults. • Analyses the consequences of these failures at system level. • States the criticality and describes the measures taken to prevent or mitigate the consequences. Measures can, for example, show that a fault leading to the failure mode will be necessarily detected by the tests performed on the component, or demonstrate that there is no credible cause leading to this failure mode due to the software design and coding rules applied.

	[Pentti&Atte02] note that the term failure mode is different for hardware and software. For the hardware components this in general is straightforward and can be based on operational experience of the same and similar components. Component manufacturers often give failure modes and frequencies for their products. For the software components such information does not exist and failure modes are unknown (if a failure mode would be known, it would be corrected). Therefore, the definition of failure modes is one of the hardest parts of the FMEA of a software-based system. The analysts have to apply their own knowledge about the software and postulate the relevant failure modes. [Pentti&Atte02] give from literature different general lists of failure modes. As an example, one of these is: Computational, Logic, Data I/0, Data Handling, Interface, Data Definition, Data Base, Other. Software failure modes are caused by inherent design faults in the software; therefore when searching the causes of postulated failure modes, the design process should be looked at. The frequency of occurrence is much harder to define for a software-based system than it is for a hardware-based system. The manifestation of an inherent software fault as a failure depends not only on the software itself, but also on the operational profile of the system, i.e. on the frequency of the triggering event that causes the fault to lead to failure. This frequency is usually not known because the defects have not yet been discovered. Also the probability of detection is hard to define, since only a part of software failures can be detected with self-diagnostic methods. [ΣΣ93] propose to use preliminary hazard analysis and subsystem hazard analysis to identify safety critical areas. To ensure completeness, they develop a functional flowchart from the software specification. They analyse each block in the flowchart for accurate, complete, and timely execution as compared to the actual/proposed operation, and identify and correct deficiencies or enhancements in the software or hardware specification. As a result, a table is drawn with (for example) the following column headings: 1. Hazard 2. Software 3. Cause 4. Effects 5. Criticality 6. Recommended 7. Function 8. Change
Applicability range:	Can be used for any software process; however, application to software controlled hardware systems is the predominant application.
Life cycle stage:	SFMEA is used after the writing of the software specification. The results of other hazard analyses, if complete, can be used as a guide for focusing the analysis. This allows engineering changes (software or hardware) early in the development cycle where these changes are easier and less costly to make.
Experience in application to air traffic:	Although SFMEA is mentioned by the FAA, references to actual applications have not been found.
Related methods:	Link to SEEA (Software Error Effects Analysis). The output of SFMEA can be used to assist the FTA.
Availability and tool support:	SFMEA is available, but not as widely used as FMEA.
Maturity:	One of the first articles on SFMEA dates from 1979 (by D.J. Reifer). There is no explicit standard for SFMEA, but the standard IEC 60812 published in 1985 is often

	referred to when carrying out FMEA for software-based systems.
Acceptability:	[Ippolito&Wallace95] did not find documentation defining SFMEA specifically for software *hazard* analysis; however, the U.S. Patent and Trademark Office recently approved it for use as a software *reliability* technique. [Pentti&Atte02] also note that no specific standard or guideline concentrating on the special issues of software-based system FMEA has yet been published.
Ease of integration:	[Pentti&Atte02] state that SFMEA is usually more difficult than FMEA: Failure modes of components such as relays and resistors are generally well understood. Reasons for the component failures are known and their consequences may be studied. Mechanical and electrical components are supposed to fail, due to some reason such as wearing, ageing or unanticipated stress. The analysis may not always be easy, but at least, the safety engineers can rely on data provided by the component manufacturers, results of tests and feedback of available operational experience. For software-based systems the situation is different. The failure modes of software are generally unknown. The software modules do not fail; they only display incorrect behaviour. To find out this incorrect behaviour the safety engineer has to apply his own knowledge about the software to set up an appropriate FMEA approach. [Pentti&Atte02] also present a list of analysis steps in which SFMEA is combined with FTA: 1) Description and familiarisation of the system; 2) Preliminary FTA (fault tree construction and minimal cut set search); 3) Preliminary SFMEA (identification of failure modes corresponding to the fault tree basic events in the shortest minimal cut sets); 4) Detailed FTA (modification of the fault tree using the SMEA results, documentation, and minimal cut set search); 5) Detailed SMEA (more detailed SMEA, documentation)
Documentability:	Documentability is similar to that of FMEA, i.e. high.
Relevance to ATM:	SFMEA can be relevant to reliability analysis of software systems in ATM. Other general advantages are: 1. It can give guidance for other verification and validation efforts; by revealing the possible weak points it can e.g. help generating test cases for system testing [Pennti&Atte02] 2. It can reveal unforeseen hazards since possible hazards do not need to be identified up front. 3. SFMEA is systematic. For more general advantages, see the FMECA template.
Con's and resources:	As for FMEA, for larger systems, SFMEA can be very extensive and time-consuming. Other general weaknesses are: 1. FMEA is applicable to software-based systems only to a limited extent, i.e. at the application function level [Pentti&Atte02] 2. A non-software specialist can begin the analysis; however, finishing the analysis requires a software expert. A thorough understanding of the system operation is required throughout the analysis. 3. Analysis can be time-consuming and tedious and requires a focused work procedure. Difficulty of the analysis increases with the complexity of the system being assessed. 4. It does not consider multiple failures. 5. It should be combined with other safety and reliability engineering methods such as FTA. For more general weaknesses, see the FMECA template.

6.17 SMHA (State Machine Hazard Analysis)

SMHA (State Machine Hazard Analysis)

References used:	Key references: • [Leveson95] Other references: • [Houmb02]
Alternate names:	None
Primary objective:	SMHA can be used to analyse a design for safety and fault tolerance, to determine software safety requirements (including timing requirements if the model includes timing) directly from the system design, to identify safety-critical software functions, and to help in the design of failure detection and recovery procedures and fail-safe requirements.
Description:	A state machine is a model of the states of a system (circles) and the transitions between them (arrows). When a condition on a transition from a state becomes true and the machine is in that state, the machine changes to a new state and takes an output action. The following figure presents a simple example for a water level control, which is from [Leveson95]. In this example, depending on the sensor reading of the water level and the current state of the machine, the machine will activate the pump, turn off the pump, open the drain, or close the drain.  The large number of states that must be specified, especially for complex systems, can be reduced by using models (meta-models) that use a small number of higher-level states, from which the entire state machine can be generated. The complete state space may never be generated, but many properties of the state space can be inferred from the higher-level model. Software and other component behaviour are modelled at a high level of abstraction, and faults and failures are modelled at the interfaces between software and hardware. Once a model of the system is created and its entire state space generated, a hazard identification can be performed in various ways: 1. Forward search for hazardous states, which starts from the initial state of the system, generates all possible paths from that state, and determines whether any of them are hazardous. This approach is usually impractical since the computational effort of this approach is usually very large, even if computers are used. 2. Backward and top-down search, starting with the hazardous states and working backward from each to see if the initial state is reached. If so, then the hazardous state is reachable and the model is unsafe. This approach is also usually

	impractical. 3. Start from a hazardous state and only work far enough back along paths to determine how to change the model to make the hazardous state unreachable. A small drawback with this approach is that the hazardous states eliminated from the design might not actually have been reachable, so more hazards may be eliminated than were actually present.
Applicability range:	State machine models are used often in computer science and are used to identify software-related hazards.
Life cycle stage:	SMHA works on a model, not the design itself. Therefore, it can theoretically be used at any stage of the lifecycle, including early in the conceptual stage, to evaluate alternative designs and design features. The procedure is most effective if performed before the detailed design of the system components begins.
Experience in application to air traffic:	A higher-level abstraction of SMHA has been incorporated in the Requirements State Machine Language (RSML), which was adopted by the FAA to model the system requirements of TCAS II.
Related methods:	Related to Petri nets.
Availability and tool support:	Since the model used is formal (i.e., it has a mathematical definition), the analysis procedures can be implemented on a computer.
Maturity:	SMHA was developed in 1987 to identify software-related hazards. The method is being extended to include hybrid (discrete plus continuous) state models.
Acceptability:	The method is usually very hard to learn and use without an advanced degree in mathematics, hence the resulting models cannot be readily understood and reviewed by engineers and application experts who do not have this training. This undermines confidence in the results by these application experts.
Ease of integration:	Petri nets or other Discrete state space models could be used to determine the underlying state machine. The method is usually very hard to learn and use without an advanced degree in mathematics.
Documentability:	Since the analysis is performed on a formal, written model, it can be automated and does not depend on the analysts' mental model of how the system works. The model is explicitly specified and can be checked for correctness by expert review and sometimes for various desirable properties by additional automated procedures.
Relevance to ATM:	Some general strengths are: 1. State machine models seem to match the internal models many people use in trying to understand complex systems. 2. The method works on a model, not on the design itself, and is therefore well suited for analysing future systems. [Houmb02]
Con's and resources:	For the qualitative part of the analysis this method seems to be very time consuming and difficult to perform compared to other qualitative methods [Houmb02]. Other general weaknesses are [Leveson95]: 1. All states and transitions must be specified, which makes the method impractical for large and complex systems. 2. A model must be built, which may be difficult and time consuming. 3. The SMHA analysis is performed on a model, not on the system itself, hence the results are only valid if the system matches the model. 4. The method is usually very hard to learn and use without an advanced degree in mathematics, hence the resulting models cannot be readily understood and reviewed by engineers and application experts who do not have this training. This undermines confidence in the results by these application experts.

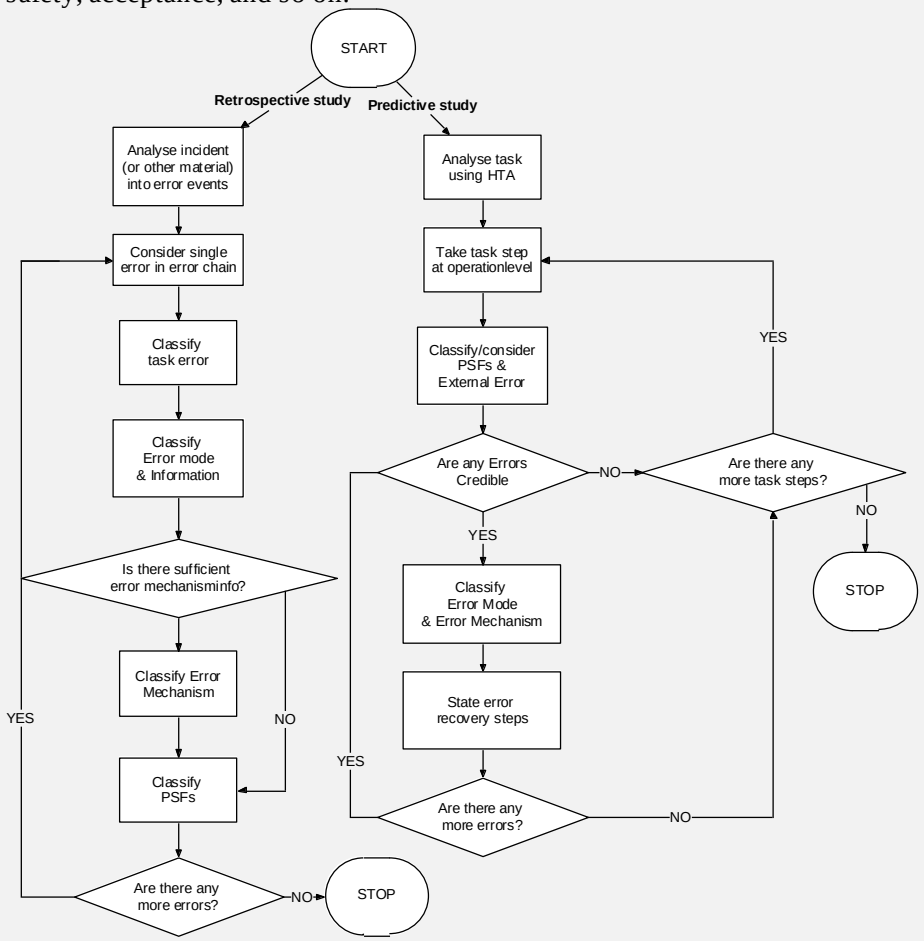
6.18 TRACER-Lite (Technique for the Retrospective Analysis of Cognitive Errors)

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

References used:	Key references: • [Shorrock01] Other references: • [HIFA_human] Additional reading: • [Shorrock&Kirwan98], [TRACEr lite_xls]
Alternate names:	None
Primary objective:	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.
Description:	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].

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

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 • 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) programme. • 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 behaviour 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 favourable 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 feedforward and feedback loops that are available.
Con's and resources:	The TRACER method itself can be primarily used by human factors specialists only. The 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.

6.19 Use of Expert Judgement

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 judgement approaches.
Description:	Expert judgement 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 judgement process. Technically, if substantive experts are not available, then the derivation of judgements is called '*engineering judgement'* rather than expert judgement. The former may be used when no experts are available for example, but obviously such judgements 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 maximises the validity of the actual expertise of the expert(s). In particular, expert judgement techniques, whether qualitative or quantitative in nature, seek to avoid *biases* in expert judgement. 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 judgement 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 judgement 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 Judgement) 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 judgements, 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 organisation.
Life cycle stage:	Expert judgement 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 judgement (and more often, engineering judgement) is used frequently in ATM as in other domains.
Related methods:	Link to PC (Paired Comparisons), APJ (Absolute Probability Judgement), 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 judgement 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 judgement scenarios. Expert judgement 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 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.
Acceptability:	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.

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

[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 favour for APJ.

Ease of integration:

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.

Documentability:

Documentability is high, provided all steps and the rationale underlying judgements are recorded during the sessions.

Relevance to ATM:

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 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 judgements are often easier to give than quantitative judgements. 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 judgement 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 judgement 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. Areas for further research and development

The previous section summarised and evaluated 19 techniques that it is believed can support the EATMP Safety Assessment Methodology (SAM) either immediately, or with some tailoring or adaptation to the ATM context. The techniques in Section 6 are therefore for short-term implementation. However, in addition to the list of techniques that are evaluated above according to a template format, the project workshop also identified several techniques that are judged to be significantly important and therefore deserve further development by EUROCONTROL. It should be noted that for some of these techniques, further developments for ATM are already well underway, either inside or outside EUROCONTROL.

In this section, these additional techniques are gathered under some identified problem statements. Short titles for these problem statements are:

- Understanding cognitive behaviour and errors of commission of a human agent
- Understanding cognitive behaviour in interactions with other humans and systems
- Mathematical modelling of Air Traffic Management
- Organisational learning
- Safety data bases
- Safety culture maturity

Each of these problem statements is outlined below. Each subsection ends with the list of techniques gathered under the corresponding problem statement. More details on these techniques can be found in [Technical Annex].

7.1 Understanding cognitive behaviour and errors of commission of a human agent

Problem statement:
During the last decade it has become quite clear among cognitive psychologists that human cognitive facets such as human understanding, judgement and choice cannot be easily represented in a functional setting only, such as used with Hierarchical Task Analysis (HTA, see Section 6.10). One of the typical examples of non-functional behaviour are Errors of Commission. These occur as a result of e.g. a non-required action taken; something is done that should not have been done. Its functional counterpart is an Error of Omission, i.e. an error which occurs as a result of a required action not taken or taken late. Errors of Omission are often easier to identify and to analyse than Errors of Commission, since they generally simply concern omitted information (e.g., an airway was read in a clearance but not copied down), which can be identified and analysed from a task and functional analysis. Errors of Commission include for example information that was not present in the clearance but that was copied down nevertheless, extra airways copied that were not in the clearance, incorrect numbers, and incorrect navaid or airway names. More generally they occur as errors such as giving the right clearance to the wrong aircraft, for example.

This non-functional representation problem appears particularly relevant in ATM where we talk for example of the controller's 'mental picture', without having a clear idea of what this is and how it works. However, this 'picture' may be a critical part of the high reliability that ATM has

enjoyed over the last few decades and, furthermore, this picture could be altered or degraded by future system designs or traffic pattern changes. Therefore, it should be understood and as far as possible modelled.

Cognitive modelling approaches aim to model cognitive aspects of performance, either in terms of relationships between knowledge items relating to symptoms of events (for diagnostic reliability assessment) or in terms of how various factors will affect cognitive performance aspects of the task. This domain is perhaps the least mature of the human error analysis approaches, but also perhaps the most interesting, as it is an attempt to combine cognitive psychology, the currently dominant paradigm in psychology, with a human reliability (safety) attitude. This cognitive modelling approach is supported by human factors studies in 'laboratories', that focus on particular human factors issues (such as situation awareness, workload, error recovery, etc.)

Most relevant techniques identified	Type	Objective
ATHEANA (A Technique for Human Error ANAlysis)	Specific technique	Human performance analysis
CREAM (Cognitive Reliability and Error Analysis Method)	Integrated method of more than one technique	Human performance analysis
CTA (Cognitive Task Analysis)	Specific technique	Human performance analysis
EOCA (Error of Commission Analysis)	Specific technique	Human performance analysis
ESSAI (Enhanced Safety through Situation Awareness Integration in training)	Integrated method of more than one technique	Training
FACE (Framework for Analysing Commission Errors)	Integrated method of more than one technique	Human performance analysis
HCA (Human Centred Automation)	Integrated method of more than one technique	Hazard mitigation
OPL (Operator Procedure Language)	Integrated method of more than one technique	Hazard mitigation
PEAT (Procedural Event Analysis Tool)	Integrated method of more than one technique	Hazard mitigation

Additional relevant references are: [EHQ-MOD97], [EHQ-TASK98], [Endsley95], [Seamster&al93] and [Seamster&al97].

7.2 Understanding cognitive behaviour in interactions with other humans and systems

Problem statement:

The techniques listed in the previous subsection generally consider cognitive behaviour of one human operator, without considering interactions with other agents. Considering these interactions generally requires fast time cognitive simulation approaches. Fast-time means that mathematical models are used to simulate ATM operations including controller behaviour, but where the simulator clock is not equivalent to the real-world clock. Cognitive simulation means that the simulation is focused on modelling how the human agents will think in certain situations, and therefore how (s)he will react to the simulated situations. Cognitive simulations are generally computer simulations of operator performance. This is the most sophisticated cognitive modelling area, often relying on advanced simulation modelling frameworks to predict cognitive performance behaviour.

Other industries (notably nuclear power) have had significant research efforts in the cognitive modelling area, although their success has been limited. Quite simply, modelling the human mind is challenging. Given the significance of cognitive performance to ATM, this is seen as an important area for further research. In line with this there are already a few notable safety-directed cognitive simulation developments in ATM, see the table below

Most relevant techniques identified	Type	Objective
Air-MIDAS (Air- Man-Machine Integrated Design and Analysis System)	Integrated method of more than one technique	Human cognitive performance analysis
HITLINE (Human Interaction Timeline)	Integrated method of more than one technique	Pilot reliability assessment
IPME (Integrated Performance Modelling Environment)	Integrated method of more than one technique	Pilot performance analysis
MIDAS (Man-Machine Integrated Design and Analysis System)	Integrated method of more than one technique	Pilot performance analysis
MoFL (Modell der Fluglotsenleistungen (Model of air traffic controller performance))	Integrated method of more than one technique	Controller performance analysis
PUMA	Integrated method of more than one technique	Controller performance analysis
TOPAZ (Traffic Organization and Perturbation AnalyZer)	Integrated method of more than one technique	Human cognitive performance and accident risk assessment

7.3 Mathematical modelling of Air Traffic Management

Problem statement:
Mathematical modelling is used extensively in many industries, including ATM. Applied to safety, it involves creating and refining a mathematical model of the ATM process so that relative risks associated with the various component parts and processes of ATM can be predicted. Real data from incident and event reports and analysis can be used to quantify and

'validate' the model where such data are available. The resulting model can be used to run simulations. Hence, it does not require waiting until incidents happen to learn about safety, nor the running of large and expensive real-time simulations to evaluate a concept. The drawbacks with such models are that the data to run the model are often not available, or else have to be inferred by expert judgement, and also the complexities of an operation such as ATM may defy our ability to carry out realistic and valid modelling. Nevertheless, modelling can give 'best answers' to questions that otherwise are too difficult to answer, and any model can be refined and 'calibrated' when data from real life become available. Models therefore can be a good way to predict and to learn about ATM safety. Furthermore, a model-based approach is not only useful for assessing particular quantities such as accident risk - its major additional advantage is that it can help to learn where 'unsafety' comes from, how it is influenced, and which factors have the highest impact.
Failures, events, flows, functions, energy forms, random variables, hardware configuration, accident sequences, operational tasks, human behaviour, all can be modelled. Mathematical modelling is therefore a major ongoing research significant area in ATM safety applications[1].

Most relevant techniques identified	Type	Objective
SpecTRM (Specification Tools and Requirements Methodology)	Integrated method of more than one technique	Software dependability
TOPAZ (Traffic Organization and Perturbation AnalyZer)	Integrated method of more than one technique	Accident risk assessment

There is a whole spectrum of mathematical modelling techniques available for ATM modelling. Some specific mathematical modelling techniques identified during the Safety Techniques Workshop are:

Most relevant techniques identified	Type
Bayesian Belief Networks	Mathematical model
CGHDS (Controlled General Hybrid Dynamical System)	Mathematical model
DES (Discrete Event Simulation),	Mathematical model
Dynamically Coloured Petri Nets	Mathematical model
Finite State Machines	Mathematical model
Finite State semi-Markov processes	Mathematical model
Formal Methods	Mathematical model
Fuzzy Logic	Mathematical model
HSMP (Hybrid-State Markov Processes)	Mathematical model
Hybrid Automata	Mathematical model
Importance Sampling	Mathematical model
Markov Chains or Markov Modelling	Mathematical model
Monte Carlo Simulation	Mathematical model
Petri Net Analysis	Mathematical model

[1] One project in which several approaches towards modelling for ATM are addressed and further developed is HYBRIDGE (Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design). HYBRIDGE is a 3-year project (2002-2004) funded by the European Commission IST (Information Society Technologies; see http://www.nlr.nl/public/hosted-sites/hybridge/.

Petri Net Extensions	Mathematical model
Piecewise Deterministic Markov Processes	Mathematical model
Semi-Markov Chains	Mathematical model
SSG (State Space Graphs (or Discrete State Space Graphs))	Mathematical model
Stochastic Differential Equations	Mathematical model

7.4 Organisational learning

Problem statement:
Organisational Learning has already received some attention in ATM. For example, EUROCONTROL state in their Safety Research and Development plan 2002-2006 [EEC SRDP]:

> *Part of resilience (robustness against failure) is learning from past events, enabling organisations to anticipate and manage or even control new events in the future.*

This is a basic premise of recent management and quality theory. Systems that learn and continually adapt and improve survive, and those that do not, fail. This has been recognised in safety in airlines for some time, as typically an airline which suffers a large accident, fails economically within a relatively short time period. Therefore ANS organisations need to maximise the data available from past events, interpreting such data for managing safety and risk in the current and future systems. Safety reporting and predictive risk analysis techniques potentially offer a coherent way of interpreting past events and apparent trends for the near and further future term scenarios. Such an approach would mean that organisations would only be truly 'surprised' by events that were effectively not predictable. Safety learning (organisational learning about safety) should therefore allow timely dissemination of safety-related information to allow anticipation of new trends in safety-related events, enabling a type of 'early warning' or 'alerting' system. This means that essentially, particularly if information is shared, organisations can learn from each others' mistakes. On a longer timescale, safety-related information can be used to update and 'calibrate' safety and risk assessment approaches and models, making assessment more valid and anticipatory, and should also be able to feed forward lessons learned into designs to make future ATM more robust in safety terms. Safety learning is therefore a valuable property of a system such as ATM, and therefore deserves research to develop an appropriate framework to deliver this property. Some useful references on organisational learning are: [OL Glossary], [Polat96], [Malhotra96], and the references therein.

Most relevant techniques identified	**Type**	**Objective**
TRIPOD	Integrated method of more than one technique	Hazard mitigation

7.5 Safety data bases

Problem statement:
One of the main difficulties in any safety assessment is often the lack of significant input data, e.g. on hazards, hazard frequencies, failure and error probabilities, etc. And if data do exist, their

accuracy is often uncertain. They may not be entirely suitable for the domain or application under study, or may be based on too few reliable data. Direct expert judgement is one source of information to overcome this problem. The use of databases is another important source.

Note that there are two general types of databases:
- Databases that collect 'real' data, e.g. through measurements in practice, or through mandatory or voluntary reporting systems;
- Databases that collect 'indirect' data, e.g., from expert judgement or modelling exercises.

Both can be very useful in safety assessment exercises, however, an important weakness of databases with respect to using direct expert judgement, is that their structuring and collection (including keeping them up-to-date) is much more expensive and time consuming. The advantage is that they can be used over and over again.

Databases for hazard frequencies exist in many other industries and could be developed for ATM. In particular, during the project workshop, a database on 'real' human error probabilities was noted to be worth giving high priority, due to the need to carry out quantitative safety assessments involving the most critical safety component in ATM, namely the controller.

Most relevant techniques identified	Type	Objective
ASP (Accident Sequence Precursor)	Database	Precursors in nuclear
ASRS (Aviation Safety Reporting System)	Database	Incident reporting
BASIS	Database	Incident reporting
CHIRP (Confidential Human Factor Incident Reporting Programme)	Database	Human factors incident reporting
CORE-DATA (Computerised Human Error Database for Human Reliability Support)	Database	Human incident / error data
Data Recording and Analysis	Data collection and management	Software support
ECCAIRS	Database	Incident reporting
HPED (Human Performance Events Database)	Database	Human incident data (nuclear)
Library of Trusted, Verified Modules and Components	Database	Software support
NLR Air Safety Database	Database	Incident accident data
SATORI	Database	Incident reporting
SRS-HRA (Savannah River Site HRA)	Database	Nuclear incident data
TOPAZ hazard database	Database	Hazards in civil aviation

7.6 Safety culture maturity

Problem statement:
Safety culture is popularly defined as '*the way things are done around here'* and is interpreted as the underlying real commitment to safety, as opposed to 'lip service'. All the safety assessments in the world will not deliver real safety if there is no real commitment, or that commitment is misguided, towards safety. Safety culture arose as a subject area after

Chernobyl, Bhopal and Challenger Space Shuttle accidents around 1986, and led to the development of a number of safety culture assessment techniques over the next decade, which aimed to determine the level of safety culture, qualitatively and in some cases even quantitatively. The latest developments are in terms of Safety Culture Maturity Models (SCMMs). These latter models have the advantage that they show an organisation where it lies in terms of general safety culture, and how to improve to reach the next level of maturity.

These approaches are not addressing safety at the level of the specific ATM tool, system or centre, but at the level of the organisation operating or designing that tool, system or centre, and current accident theory (and common sense) suggests that the organisation is a key element determining real safety. Safety culture maturity models or equivalent approaches should therefore be developed for ATM.

Most relevant techniques identified	Type	Objective
ASCOT (Assessment of Safety Culture in Organisations Team)	Specific technique	Human performance analysis
CHASE (Complete Health And Safety Evaluation)	Specific technique	Human performance analysis
Five Star System	Specific technique	Human performance analysis
ISRS (International Safety Rating System)	Specific technique	Human performance analysis
MANAGER (MANagement Assessment Guidelines in the Evaluation of Risk)	Integrated method of more than one technique	Human performance analysis
NOMAC (Nuclear Organisation and Management Analysis Concept)	Integrated method of more than one technique	Human performance analysis
PRASM (Predictive Risk Assessment and Safety Management)	Integrated method of more than one technique	Hazard mitigation
PRISM (Professional Rating of Implemented Safety Management)	Specific technique	Human performance analysis
SCHAZOP (Safety Culture Hazard and Operability)	Specific technique	Risk assessment
WPAM (Work Process Analysis Model)	Integrated method of more than one technique	Risk assessment

8. Conclusions

The survey has identified a very large number of techniques and methods from a range of industries, including ATM, concerned with safety. These have been categorised and reviewed for their usefulness for ATM safety assessment by EATMP. Nineteen approaches have been identified as being able to give on short term concrete support to ATM safety assessment practice. A number of other technique areas have been identified for further research and development by EATMP. Several of these directions are already very well under development at some other ATM research institutes.

The next step is to begin using the techniques and develop case studies and associated guidance material, showing their integration with the EATMP Safety Assessment Methodology. Although nineteen techniques have been identified, this does not mean that they will all need to be used for a particular safety assessment – in many cases a much smaller subset will suffice. It is therefore envisaged that future EATMP SAM guidance will address this issue of what technique(s) to use for what assessment.

Some general references are given in the next section for the reader wishing to gain an overview of the safety assessment domain, and more information on the techniques discussed in this report. This short list is followed by a full set of references used in this document.

9. References

The first table below provides some references for the reader wishing to gain an overview of the safety assessment domain, and more information on most of the techniques discussed in this report. This short list is followed by a full set of references used in this document. For key references more specific to the 19 techniques evaluated in Section 6, we refer to the templates.

Shortlist of key references:

[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/.
[Cacciabue98]	P.C. Cacciabue, Modelling and human behaviour in system control, Advances in industrial control, Springer, 1998
[Henley&Kumamoto92]	E.J. Henley and H. Kumamoto, Probabilistic Risk Assessment; Reliability engineering, design, and analysis, IEEE Press, 1992
[Kirwan94]	B. Kirwan, A guide to practical human reliability assessment, Taylor and Francis, 1994
[Leveson95]	N.G. Leveson, Safeware, system safety and computers, a guide to preventing accidents and losses caused by technology, Addison-Wesley, 1995

Complete list of references:

The list below contains all references used in this main document. The technical annex to this report [Technical Annex] provides all references used in both this main document and the technical annex.

[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.)
[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
[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&Everdij&Daams 99]	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/.
[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
[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
[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.
[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.
[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
[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).
[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&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
[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
[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
[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
[Humphreys88]	P. Humphreys, Human reliability assessors guide, Safety and Reliability Directorate UKAEA (SRD) Report No TRS 88/95Q, October 1988.
[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
[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	B. Kirwan, G. Basra and S.E. Taylor-Adams, CORE-DATA: A computerised

.doc]	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"
[Kletz74]	T. Kletz, HAZOP and HAZAN – Notes on the identification and assessment of hazards, Rugby: Institute of Chemical Engineers, 1974.
[Kumamoto&Henley96]	H. Kumamoto and E.J. Henley, Probabilistic risk assessment and management for engineers and scientists, IEEE, New York, NY, 1996.
[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
[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
[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/System-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&Haritopoulos01]	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.
[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/
[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
[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"
[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
[Stroup]	R. Stroup, An approach to the software aspects of safety management, FAA, http://www2.faa.gov/aio/common/documents/Safety/SofSafMgmt.pdf
[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.
[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.