EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL EXPERIMENTAL CENTRE

Review of techniques to support the EATMP Safety Assessment Methodology

Technical Annex

EEC Report No. XXX

Project XXX-X-XX

Issued: 11 April 2003

REPORT DOCUMENTATION PAGE

Reference: SMS-D5-Annex-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 75 00

TITLE:

Review of techniques to support the EATMP Safety Assessment Methodology

Technical Annex

Contact **Patrick MANA** Patrick.mana@eurocontrol.int	**Date**	**Pages**	**Figures**	**Tables**	**Appendix**	**References**
	11/04/03	iv + 156	1	1	0	347

Distribution Statement:
(a) Controlled by: EEC
(b) Special Limitations: None
(c) Copy to NTIS: ~~YES~~ / NO

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

Abstract:
This is the Technical Annex to a report that presents the results of a survey 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. This technical annex explains how SAM support can be represented by different dimensions, gives details on the 500 techniques collected, explains in detail how 19 techniques were selected from these 500 during a Safety Techniques workshop, and explains how the template format was developed.

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 is the Technical Annex to the the Safety Methods Survey report. It contains details on the work produced by this project, which were not provided in the report itself.

1.3 Organisation of this document

This document is organised as follows.

- Section 2 provides a description of the issues that should be covered by the safety assessment techniques collected in this project, into different dimensions.
- Section 3 provides all techniques collected during the course of this project, in a table with columns providing details for the techniques.
- Section 4 provides details on how the template format was developed.
- Section 5 provides details on the Safety Techniques Workshop that was organised to select from the list of candidate techniques collected during WP2, about 20 techniques that were to be evaluated along the template format.
- Section 6 provides references used.
-

2. ANS safety assessment dimensions

2.1 Introduction

EATMP SAM's ultimate aim is to define the means for providing assurance that an Air Navigation System (ANS) is safe for operational use [EHQ-SAM]. An ANS is very complex due to the many issues and combinations of issues that have their influence on safety. Due to the diversity of these issues and the number of combinations possible it will be difficult to find or develop one technique that can support the safety assessment of all of them. Hence, this is not what we need to aim for; we need to be looking for a set of techniques that together cover all issues.

To get some grip on the diversity of issues involved, they can be looked at from several viewpoints. Each viewpoint groups the issues in another way:

- Grouping according to ATM elements: humans, equipment, procedures, organisation, including their combinations, interactions, teamwork, decision making, etc.
- Grouping according to the gate-to-gate process elements, i.e. not only en-route, but also airports, runway incursions, risk monitoring, maintenance, etc.
- Grouping according to ANS design life cycle elements, i.e. definition phase, design phase, implementation phase, operations and maintenance phase, decommissioning.

These viewpoints can be represented by dimensions that span the complete ANS, see Figure 1. Techniques and methods that support ANS safety assessment should cover all issues within the ANS boundaries. The view on the ANS as being spanned by dimensions serves the following advantages:

- Since elements in one group in one dimension may have similar qualities, techniques may exist that can cover (most of) the elements in one group.
- It can be verified easier that no group is forgotten in the safety assessment.

The following three subsections try to provide some more detail on the different dimensions.

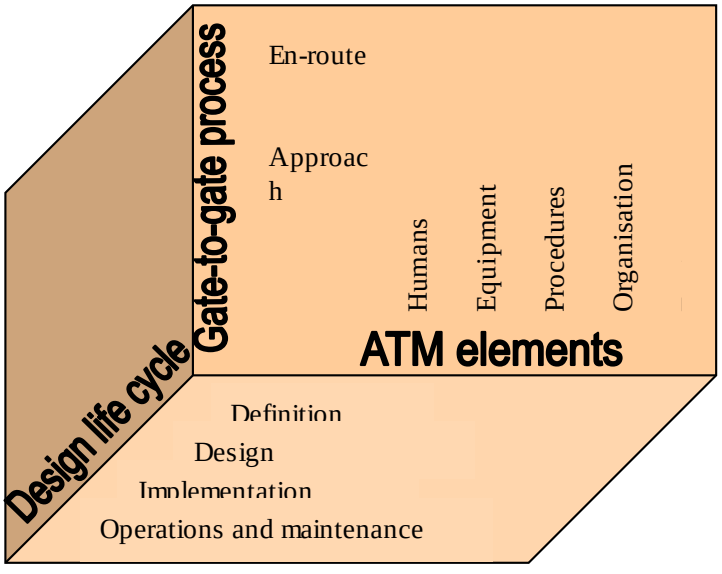

Figure 1: The Air Navigation System is spanned by groups of issues in several dimensions. (Note that this diagram is simplified to illustrate the idea more effectively.)

2.2 ATM elements

The Air Navigation System is defined as the aggregate of organisations, humans, infrastructure, equipment, procedures, rules and information used to provide the Airspace Users Air Navigation Services in order to ensure the safety, regularity and efficiency of international air navigation [EHQ-SAM]. A methodology that is to provide the safety assessment of such Air Navigation Systems should therefore capture all these ATM elements. Roughly, these elements can be divided into five groups:

Humans	E.g., operational personnel, maintenance personnel, engineering personnel, skills, training, team work
Equipment	E.g., ground equipment, aircraft equipment, satellites, man machine interface, external services, external facilities, software, hardware
Procedures	E.g., operational procedures, instructions, maintenance procedures, risk monitoring
Organisation	E.g., safety culture, airspace sectorisation, route structures, separation standards, air traffic flight management, air traffic services, decision making, space management
Environment	E.g., weather influences

These groups are closely linked, hence interactions between these elements and the interactions between the system and its environment (e.g. aircraft performances, adjacent centres capabilities, airport infrastructure, local weather phenomena, topography obstacles, noise sensitivity) also need to be taken into account, both during normal operation and during degraded modes of operation, when appropriate.

Previous surveys on safety assessment techniques show that there are numerous techniques and methods that support the safety assessment of technical systems. A lot of support exists for evaluating dependability aspects for these technical systems such as reliability, maintainability and availability. It appears that human and procedural aspects have only been studied recently. With regard to the human aspects, techniques to support the assessment of human error and mistakes are reasonably well off. However, recently, safety studies became aware that the human cannot be treated as a machine and plays a vital part in ATM safety due to factors like improvisation talent, which machines do not have. Also software issues have received limited attention, compared to hardware problems in ATM, yet software is becoming an increasingly critical part of system functioning.

2.3 Gate-to-gate flight phases

The Air Navigation System should also be looked at from a flight phase point of view. During the taxiing, take-off, cruise, and landing phases of a flight, an aircraft is supported by various services, which operate differently due to the different supporting tasks, and that also interact. Each service has a different effect on safety, hence different techniques could exist to support various services. Elements to be considered in this dimension would include:

Pre-flight planning	Pre-flight planning, weather information, cleaning, catering, loading passengers, loading luggage, maintenance
Taxiing	Push back, gates and stands, aprons and taxiways,
Take-off	Take-off, initial climb, TMA
Cruise	Continental en-route
Approach	Descent, holding, final approach, go-around, sequencing
Landing	Landing
Taxiing	Aprons and taxiways
Parking	Unloading passengers, unloading luggage, cleaning

Note that this list is not exhaustive. For more detailed phases, the HEIDI taxonomy is useful [HEIDI taxonomy], (http://www.eurocontrol.int/safety/GuidanceMaterials_HeidiTaxonomy.htm).

Three very important aspects with respect to this list, which should be taken into account, are

- A flight of an aircraft cannot always be split up into distinct flight phases.
- A flight does not always follow the same pattern or sequence of flight phases, e.g. due to external influences.
- A flight may also include non-nominal phases and situations, which are not (all) listed, but which do affect safety assurance.

Especially the last aspect makes it difficult to obtain an exhaustive list, but should not be forgotten.

2.4 ANS design lifecycle

The EATMP Safety Assessment Methodology follows an iterative process, which is to be conducted throughout all phases of the (Ground) ANS life cycle. In [EHQ-SAM], this lifecycle follows the following major phases:

System definition	covering the identification of ANS functions and the specification of the overall system requirements and interfaces
System design	covering the definition of the ANS architecture and the allocation of functions and requirements to the system elements
System implementation	covering the development of the individual ANS elements
System integration	covering the verification of individual ANS elements and their integration
Transfer into operations	covering the installation and integration of the ANS in its operational environment, and its validation
Operations and maintenance	covering the operations of the ANS and the preventive and corrective maintenance activities
Decommissioning	covering the steps that withdraw the ANS from operations

The safety assessment of the (Ground) Air Navigation System runs parallel with these phases. With each phase, different types of information is available, hence each phase will be supported by different techniques. To ensure that each phase is covered by a sufficient number of

techniques, it is logical that one dimension of the Air Navigation System follows the lifecycle phases.

It should be noted that not every project is required to perform a safety assessment up to the last lifecycle phase. For example, with operational concepts for which there is no immediate intention of implementation (such as research activities), there is no need to cover all lifecycle phases. This is expressed by the following table:

Table 1: EATMP project development horizons. Grey areas indicate that safety assessment for this lifecycle phase is less relevant

Lifecycle phase	Only concept development	Prototype development	Implementation intention
System definition			
System design			
System implementation			
System integration			
Transfer to operations			
Operations and maintenance			
Decommissioning			

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 collection considered techniques used in ATM and other industries, so that ATM can borrow or adapt techniques found to be effective elsewhere. The collection only included publicly available techniques and methods, hence no commercially available tools or facilities.

This section gives the complete overview of techniques and methods that have been identified for this project. The main document explains in more detail how the list was obtained and provides statistics. In the table below, for each technique the following information is provided (if available):

- Name
- Type of technique; two types of classes are specified. The first class specifies whether the technique is a (D) Database, a (G) Generic term, a (M) Mathematical model, an (I) Integrated method of more than one technique, or a (T) specific Technique. The second class specifies whether the technique is a (R) Risk assessment technique, a (H) Human performance analysis technique, a (M) hazard Mitigating technique, a (T) Training technique, a (Dh) hardware Dependability technique, or a (Ds) software Dependability technique.
- Age, expressed by date of birth of the technique. If uncertain, then words like ‘about’ or ‘or older’ are added.
- Aim/description of the technique. This description is very brief; one is referred to the references for a more complete description.
- Remarks, such as an assessment of the technique by the survey it was described in, or names of related techniques, or techniques that it could be used in combination with. The indicated recommendations are assessments made by the references used.
- Domains, i.e. the domains of application the technique has been used in, such as nuclear, chemical, ATM, aviation, aircraft development, computer processes.
- SAM, which lists the tasks of SAM the technique could be useful for (see [D5 Main Document] for these steps). 'None' indicates if it is apparent that the technique is beyond the scope of SAM. Note that software is written also in several stages, i.e. a definition, a design and an implementation phase, but these all fall under SAM step SSA.
- Application, i.e. applicable to hardware, software, human, procedures and organisation.
- References used in this survey. Note that the reference lists are not exhaustive and there may exist better (e.g. original) references to describe the techniques.

The last column gives an initial assessment by Patrick Mana (PM), by Mete Çeliktin (MC), and by Barry Kirwan and Oliver Sträter (KS) together, on whether they favoured the technique to be analysed further by means of a template in the next stage of the project. They gave their assessments as follows: R(Remove) = No, (C)luster with other techniques and decide later in the group, (F)urther = Consider for a template.

Id	Technique	Type		Age	Aim/ Description	Remarks, incl. ease of combining with other techniques, tools available	Domains	SAM	Application				References	Use for D4?
		GDIMT	TRDHM						Hardware	Software	Human	Procedures		

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
1.	3D-SART (3D-Situation Awareness Rating Technique)	T	H	1989	Is narrowed-down version from SART, covering only 3 dimensions (instead of 10 or 14): (a) *Demands on Attentional Resources* — a combination of Instability of Situation, Complexity of Situation, and Variability of Situation; (b) *Supply of Attentional Resources* — a combination of Arousal of Situation, Concentration of Attention, Division of Attention, and Spare Mental Capacity; and (c) *Understanding of Situation* — a combination of Information Quantity, Information Quality, and Familiarity.		aviation	S3c.1			X		• Safety Techniques Workshop • [Uhlarik&Comerford 02]	
2.	Absorbing boundary model	M		1964	Collision risk model; Reich-based collision risk models assume that after a collision, both aircraft keep on flying. This one does not.	Mainly of theoretical use only.	ATM	P3.2 S3a.1				X	• [Bakker&Blom93] • [MUFTIS3.2-II]	PM:R
3.	Accident Analysis	G		1992 or older	The purpose of the Accident Analysis is to evaluate the effect of scenarios that develop into credible and incredible accidents. Those that do not develop into credible accidents are documented and recorded to verify their consideration and validate the results.	Any accident or incident should be formally investigated to determine the contributors of the unplanned event. Many methods and techniques are applied. E.g. PHA, Subsystem HA.	nuclear	S3a.1 S3a.2	X	X	X	X	• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C MC:F KS:R
4.	Action Information Requirements	T	H	1986 or older	Helps in defining those specific actions necessary to perform a function and, in turn, those specific information elements that must be provided to perform the action. It breaks up the references function requirement into useful groupings of action requirements and information requirements.	Procedure for developing or completing action/information requirements forms is much more informal than that for most analysis methods.	defence	F3.1 P3.1			X	X	• [MIL-HDBK]	PM:R KS:R
5.	Activity Sampling	T	H	1950	Method of data collection which provides information about the proportion of time that is spent on different activities. By sampling an operator's behaviour at intervals, a picture of the type and frequency of activities making up a task can be developed		warehousing	S3c.1			X		• [Kirwan&Ainsworth 92]	PM:R
6.	ADSA (Accident Dynamic Sequence Analysis)	I	H	1994	Cognitive simulations which builds on CREWSIM.		nuclear	P3.2 S3a.2			X	X	• [Kirwan98-1]	KS:C PM:C
7.	AEA	T	H	1981	Action Error Analysis analyses interactions between	Any automated interface between	aircraft	F3.2	X		X	X	• [FAA00]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Action Error Analysis)				machine and humans. Is used to study the consequences of potential human errors in task execution related to directing automated functions. Very similar to FMEA, but is applied to the steps in human procedures rather than to hardware components or parts.	a human and automated process can be evaluated, such as pilot / cockpit controls, or controller / display, maintainer / equipment interactions		F3.3 P3.2 S3a.2					• [Leveson95] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97]	KS:FC
8.	AEMA (Action Error Mode Analysis)	T	H	2000 probably older	Resembles Human HAZOP. Human errors for each task are identified using guidewords such as 'omitted', 'too late', etc. Abnormal system states are identified in order to consider consequences of carrying out the task steps during abnormal system states. Consequences of erroneous actions and abnormal system states are identified, as well as possibilities for recovery.		offshore	F3.1 F3.2 F3.3 P3.2 P3.3			X		• [Vinnem00]	PM:C KS:FC
9.	Air-MIDAS (Air- Man-Machine Integrated Design and Analysis System)	I	H	1998 about	Predictive model of human operator performance (flight crew and ATC) to evaluate the impact of automation developments in flight management and air traffic control. The model is used to predict the performance of flight crews and ATC operators interacting with automated systems in a dynamic airspace environment. The purpose of the modelling is to support evaluation and design of automated aids for flight management and airspace management and to predict required changes in both domains.	Air MIDAS was developed by members of the HAIL (Human Automation Integration Laboratory) over the past 15 years. It is currently being used for the examination of advanced air traffic management concepts in projects sponsored by NASA ARC and Eurocontrol.	ATM	F3.2 F3.3 P3.1 P3.2 P3.3 P3.4 S3a.1 S3a.2	X		X	X	• [Air-MIDAS web] • [HAIL]	
10.	AIRS (Aircrew Incident Reporting System)			1999 or older	AIRS is a confidential human factors reporting system that provides airlines with the necessary tools to set up an in-house human performance analysis system. It was established to obtain feedback from operators on how well Airbus aircraft operate to identify the significant operational and technical human performance events that occur within the fleet; develop a better understanding of how the events occur; develop and implement design changes, if appropriate, and inform other operators of the "lessons learned" from the events. AIRS aims to provide an answer to "what" happened as well as to "why" a certain incident and event occurred. The analysis is essentially based on a causal factor analysis, structured around the incorporated taxonomy. The taxonomy is similar to the SHEL model that includes environmental, informational, personal, and organisational factors that may have had an influence on crew actions.	AIRS is part of the AIRBUS Flight Operations Monitoring package	aviation	F3.1 F3.2 F3.3 P3.2 S3c.1			X		• [HumanFactors]	
11.	Analysable Programs	G		1987 or older	Aim is to design a program in a way that program analysis is easily feasible. The program behaviour must be testable completely on the basis of the analysis	Recommended wherever possible. Essential if the verification process makes use of statistical	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	H w	S w	H u	P r	References	For D4
						program analysis techniques. Complementary to program analysis and program proving. Tools available. Software design & development phase								
12.	AoA (Analysis of Alternatives)	T	Dh	1975	Alternatives for a particular system or procedure are analysed, including no-action alternative.	AoA is the new name for Cost and Operational Effectiveness Analysis (COEA) or "Production readiness analysis".	nuclear defence road	P3.2	X			X	• [MIL-HDBK]	PM:R
13.	APHAZ (Aircraft Proximity HAZards)	D		1989	APHAZ reporting has been introduced by the UK CAA in 1989. In these reports air traffic controllers describe conflicts between aircraft, mostly in terminal manoeuvring areas.	One should note that the APHAZ reporting rate seemed to increase significantly after the introduction of Safety Monitoring Function.	aviation	F3.1 F3.2 F3.3 P3.2 S3c.1	X		X	X	• [CAA9095]	
14.	APJ (Absolute Probability Judgement)	T	H	1981 or older	Estimates human error probabilities. Two forms: Groups APJ and Single expert APJ. For the former, there are four major methods: Aggregated individual method. Delphi method, Nominal group technique, consensus group method.	Human reliability family. Does not restrict to human error only. Can be used together with PC. Other name for APJ is Direct Numerical Estimation	offshore nuclear	P3.2 S3a.2	X		X		• [Humphreys88] • [Kirwan94] • [MUFTIS3.2-I]	KS:FC PM:C
15.	APRECIH (Analyse PREliminaire des Conséquences de l'Infiabilité Humaine)	T	H	1999	Preliminary Analysis of Consequences of Human Unreliability. Consists of four consecutive steps: 1) Functional analysis of human-machine system; 2) Procedural and contextual analysis; 3) Identification of task characteristics; 4) Consequence analysis	Design phase	rail	P3.2			X		• [PROMAI5] • [Vanderhaegen&Telle98]	KS:F PM:C
16.	ARP 4761 (Aerospace Recommended Practice)	I	Dh Ds	1994	Guidelines and methods for conducting safety assessment on civil airborne systems and equipment. Like SAM, the methodology consists of the steps FHA, PSSA and SSA, but it is restricted to hardware and software.	[ARP 4754] is the higher level document dealing with general certification. [ARP 4761] gives a more detailed definition of the safety process.	aircraft	many	X	X			• [ARP 4754] • [ARP 4761] • [Klompstra&Everdij97] • [Lawrence99]	PM:F
17.	Artificial Intelligence Fault Correction	T	M	1995 or older	Aim is to react to possible hazards in a very flexible way by introducing a mix (combination) of process models and some kind of on-line safety and reliability analysis.	Software architecture phase	computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:C
18.	ASCOT (Assessment of Safety Culture in Organisations Team)	T	H	1994	Safety culture audit tool uses performance indicators, which are organised into groups. The scores on the sub-sets of safety performance areas are weighted and then translated into an overall index rating.	Qualitative	nuclear	S3c.1				X	• [Kennedy&Kirwan98]	PM:R KS:FC
19.	ASEP (Accident Sequence Evaluation Programme)	T	H	1987	Abbreviated and slightly modified version of THERP. ASEP comprises pre-accident screening with nominal human reliability analysis, and post-accident screening and nominal human reliability analysis facilities. ASEP provides a shorter route to human reliability analysis than THERP by requiring less training to use the tool, less	Is often used as screening method to identify human actions that have to be assessed in more detail using THERP. However, is more conservative.	nuclear	P3.2 S3a.2			X		• [HIFA_human] • [Kirwan94] • [Kirwan&Kennedy&Hamblen] • [Straeter00] • [Straeter01]	KS:FC PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					expertise for screening estimates, and less time to complete the analysis.									
20.	ASP (Accident Sequence Precursor)	D		1979	ASP is a program containing several models for risk assessment. It identifies nuclear power plant events that are considered precursors to accidents with the potential for severe core damage and uses risk assessment methodologies to determine the quantitative significance of the events. ASP models contain event trees that model the plant response to a selected set of initiating events. When a precursor to be analysed involves one of these initiating events, an initiating event assessment is performed. In 1994, INEEL started the development for US NRC of a Human Reliability Analysis methodology as part of ASP.	Established by the NRC in 1979 in response to the Risk Assessment Review Group report.	nuclear	P3.2 S3a.2	X		X		• [HRA Washington] • [NRC-status99] • [NSC-ANSTO]	KS:FC PM:C
21.	ASRS (Aviation Safety Reporting System)	D		1975	The Aviation Safety Reporting System (ASRS) receives, processes and analyses voluntarily submitted incident reports from pilots, air traffic controllers, and others. Reports submitted to ASRS describe both unsafe occurrences and hazardous situations. ASRS's particular concern is the quality of human performance in the aviation system. Individuals involved in aviation operations (pilots, crew members, ground personnel, etc.) can submit reports to the ASRS when they are involved in or observe a situation that they believe compromised safety. These reports are voluntary and submitted at the discretion of the individual. Teams of experienced pilots and air traffic controllers analyse each report and identify any aviation hazards.	The Aviation Safety Reporting System (ASRS) was established in 1975 under a memorandum of agreement between FAA and NASA.	aviation	F3.1 F3.2 F3.3 P3.2 S3c.1	X		X	X	• [ASRS web]	
22.	Assertions and plausibility checks	G		1976 or older	Aim is to produce code whose intermediate results are continuously checked during execution. In case of incorrect results a safety measure is taken	Recommended if no complete test or analysis is feasible. Related to self-testing and capability checking. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
23.	ATHEANA (A Technique for Human Error ANAlysis)	T	H	1996	Aim is to analyse operational experience and understand the contextual causes of errors, and then to identify significant errors not typically included in PSAs for nuclear power plants, e.g. errors of commission. Key human failure events and associated procedures etc. are identified from the PSA, and unsafe acts are then identified that could affect or cause these events. Associated error-forcing conditions are then identified that could explain why such unsafe acts could occur. The important point is that these forcing conditions are based on the system	Prototype. Currently the method relies on operational experience and expert judgement. It is the intention of the authors to produce guidance material on the technical basis of the model. Such material could reduce the reliance on expert judgement and increase the auditability of the technique. Goes beyond THERP in its	nuclear	S3c.1			X		• [Kirwan98-1]	PM:C MC:F KS:FC

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					being assessed, i.e. the real context that is the focus of the assessment.	capability to account for and predict human errors, by examining cognitive processes								
24.	Avalanche/stress testing	T	Ds	1995 or older	Helps to demonstrate robustness to overload. There are a variety of test conditions that can be applied. Under these test conditions, the time behaviour of the test object is evaluated. The influence of load changes is observed.		computer	S3a.2		X			• [EN 50128] • [Jones&Bloomfield &Froome&Bishop01] • [Rakowsky]	PM:C
25.	Avoidance of complexity	G		1987	To minimise the chance of error by making the system as simple as possible.	Less frequently used than it should be. Highly recommended for safety critical systems	computer	P3.2	X	X			• [Bishop90]	PM:C
26.	Back-to-back testing	T	Ds	1986 or older	To detect test failures by comparing the output of two or more programs implemented to the same specification. Also known as Comparison Testing	Recommended if two or more programs are to be produced as part of the normal development process	computer	S3a.2		X			• [Bishop90]	PM:C MC:R
27.	Backward Recovery	T	Ds	1995 probably older	Back-up to a previous state that was known to be correct; then no (or little) knowledge of the error is needed. The Backward Recovery approach tends to be more generally applicable than the forward recovery approach - errors are often unpredictable, as are their effects.	Software architecture phase	computer rail	S3a.2		X			• [EN 50128] • [Rakowsky] • [SSCS]	PM:C
28.	Barrier Analysis	T	M	1985	Is implemented by identifying energy flow(s) that may be hazardous and then identifying or developing the barriers that must be in place to form damaging equipment, and/or causing system damage, and/or injury	Any system comprised of energy, should this energy become uncontrolled accidents can result. Barrier analysis is an appropriate qualitative tool for systems analysis, safety reviews, and accident analysis. Combines with MORT. Can also be used to identify unimaginable hazards.	chemical nuclear road rail	F3.2 P3.2 P3.3 P3.4	X				• [FAA00] • [Kirwan&Ainsworth92] • [ΣΣ93, ΣΣ97]	PM:F KS:F
29.	BASIS (British Airways Safety Information System)	D		1992	Database based on voluntary reporting. BASIS Air Safety Reporting is used to process and analyse flight crew generated reports of any safety related incident. It has been regularly updated since its inception and has become the world's most popular aviation safety management tool (according to British Airways).	Supporting tools available.	aviation	F3.1 F3.2 F3.3 P3.2 S3c.1	X		X	X	• [BASIS web]	
30.	Bayesian Belief Networks	M			Belief networks (also known as Bayesian networks, Bayes networks and causal probabilistic networks), provide a method to represent relationships between propositions or variables, even if the relationships involve uncertainty, unpredictability or imprecision. They may be learned automatically from data files, created by an expert, or developed by a combination of the two. They capture knowledge in a modular form that can be transported from	Tools available	finance computer	P3.2 S3a.2	X		X	X	• [Belief networks]	

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					one situation to another; it is a form people can understand, and which allows a clear visualisation of the relationships involved. By adding decision variables (things that can be controlled), and utility variables (things we want to optimise) to the relationships of a belief network, a decision network (also known as an influence diagram) is formed. This can be used to find optimal decisions, control systems, or plans.									
31.	Beta-factor method	T	R	1981	Is used to quantify common cause effects identified by Zonal Analysis. The beta-factor represents the conditional probability of being a common-mode failure when a component failure occurs.	Static assessment family	aircraft	P3.2 S3a.2	X				• [Charpentier00] • [MUFTIS3.2-I] • [Pozsgai&Neher&Bertsche02]	KS:F PM:C
32.	Bias and Uncertainty assessment	T	R	2002	Aim is to get insight into the assumptions adopted during a model-based accident risk assessment, and on their effect on the assessment result. Technique assesses all model assumptions and parameter values on their effect on accident risk, and combines the results to get an estimate of realistic risk and a 95% credibility interval for realistic risk.		ATM	F4a.x P4a.x S3a.1 S3a.2	X		X	X	• [Everdij&Blom02]	
33.	Boundary value analysis	T	Ds	1992 probably older	Aims to remove software errors occurring at parameter limits or boundaries. Needs detailed knowledge of specification (when software is black box). In white box testing requires analysis of code. Boundary-value testing is **a** functional testing technique that uses the black-box method. Boundary-value testing of individual software components or entire software systems is an accepted technique in the software industry. Test cases using minimum, maximum, minimum - 1, and maximum + 1 input range values are developed and executed.		computer	S3a.2		X			• [EN 50128] • [Jones&Bloomfield&Froome&Bishop01] • [Rakowsky] • [Sparkman92]	PM:C
34.	Bow-Tie Analysis	T	M	1998 or older	Aim is to enhance communication between safety experts (who construct a Bow-Tie diagram) and operational experts (who identify hazard mitigating measures using the Bow-Tie diagram). The knot of the Bow-Tie represents a releasing event or a hazard. The left-hand side wing shows threats and Pro-active measures, which improve the chances to avoid entering the hazard; the right-hand side wing shows consequences and Re-active measures to improve the chances to escape from the hazard prior to its escalation. In some versions, the left-hand side wing is represented by a Fault Tree (which shows how initiation events lead to the hazard) and the right-hand-		chemical ATM	P3.2 P3.3 S3a.1	X		X	X	• [Blom&Everdij&Daams99] • [Edwards99] • [EHQ-PSSA] • [Trbojevic&Carr99]	PM:F MC:F KS:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					side wing is represented by an Event Tree (which shows consequences of the hazard).									
35.	BPA (Bent Pin Analysis)	T	Dh	1979	Bent Pin Analysis evaluates the effects should connectors short as a result of bent pins and mating or demating of connectors	Any connector has the potential for bent pins to occur. Connector shorts can cause system malfunctions, anomalous operations, and other risks. Combines with and is similar to CFMA. Applicable during maintenance operations.	aircraft	S3a.2	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
36.	Brainstorming	G			A group of experts sit together and produce ideas. Several approaches are known to improve the results, e.g. after some time, the experts write down ideas privately, and then gather these ideas.		all	F3.1 F3.2 F3.3 P3.1 P3.2 P3.3	X	X	X	X	• [Rakowsky]	PM:R KS:FC
37.	Bug-counting model	T	Ds	1990 or older	Model that tends to estimate the number of remaining errors in a software product, and hence the minimum time to correct these bugs.	Not considered very reliable, but can be used for general opinion and for comparison of software modules	computer	S3a.2		X			• [Bishop90]	PM:C
38.	CADA (Critical Action and Decision Approach)	T	H	1988	Psychologically-based tool. Attempts to bring generalised psychological theories or models into the rich context of a complex industrial work environment	Apparently not in current use or else used rarely	nuclear	P3.2 S3a.2			X		• [Kirwan98-1]	PM:R KS:R
39.	CAHR (Connectionism Assessment of Human Reliability)	T	H	1992 - 1998	The Database-System CAHR is a tool for analysing operational disturbances, which are caused by inadequate human actions or organisational factors. It was implemented using Microsoft ACCESS. CAHR contains a generic knowledge base for the event analysis that is extendable by the description of further events. The knowledge-base contains information about the system-state and the tasks as well as for error opportunities and influencing factors (PSFs).	Qualitative and quantitative. The term Connectionism was coined by modelling human cognition on the basis of artificial intelligence models. It refers to the idea that human performance is affected by the interrelation of multiple conditions and factors rather than singular ones that may be treated isolated. Developed 1992-1998.	nuclear	S3a.1 S3c.1			X	X	• [HRA Washington] • [Straeter&al99] • [Straeter_CAHR]	KS:FC PM:C but R if tool
40.	CAMEO/TAT (Cognitive Action Modelling of Erring Operator/Task Analysis Tool)	I	H	1994	Simulation approach acting as a task analysis tool, primarily to evaluating task design, but also for potential use in Human Reliability Assessment. It allows designers to ensure that operators can carry out tasks. Performance Shaping Factors used in the approach include task load, complexity, time pressure, opportunistic change of task order, multiple task environments, negative feedback from previously made decisions or actions, operator's policies and traits, etc.	This approach is relatively rare in Human Error Identification, where more usually either an 'average' operator is considered, or a conservatively worse than average one is conceptualised.	nuclear?	P3.1 P3.3 S3a.2			X	X	• [Kirwan98-1]	PM:R KS:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
41.	Causal Networks	G		1940 or older	Graph of random quantities, which can be in different states. The nodes are connected by directed arcs which model that one node has influence on another node	The idea of using networks to represent interdependencies of events seems to have developed with the systematisation of manufacturing in the early 1900s and has been popular since at least the 1940s. Early applications included switching circuits, logistics planning, decision analysis and general flowcharting. In the last few decades causal networks have been widely used in system specification methods such as Petri nets, as well as in schemes for medical and other diagnosis. Since at least the 1960s, causal networks have also been discussed as representations of connections between events in spacetime, particularly in quantum mechanics	manuf logistics medical	P3.2 S3a.2	X	X			• [Loeve&Moek&Arsenis96] • [Wolfram02]	KS:FC PM:R
42.	CCA (Common Cause Analysis)	T	R	1987	Common Cause Analysis will identify common failures or common events that eliminate redundancy in a system, operation, or procedure. Is used to identify sources of common cause failures and effects of components on their neighbours. Is subdivided into three areas of study: Zonal Analysis, Particular Risks Assessment, and Common Mode Analysis	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. Related to Root Cause Analysis.	aircraft energy space nuclear aircraft	P3.2 P3.3 S3a.1	X	X			• [ARP 4754] • [EN 50128] • [FAA AC431] • [FAA00] • [MUFTIS3.2-I] • [Rakowsky] • [ΣΣ93, ΣΣ97]	PM:F KS:F
43.	CCD (Cause Consequence Diagrams) or CCA (Cause Consequence Analysis)	T	R	1971	Aim is to model, in diagrammatical form, the sequence of events that can develop in a system as a consequence of combinations of basic events. Cause-Consequence Analysis combines bottom-up and top-down analysis techniques of event trees and fault trees. The result is the development of potential accident scenarios.	Developed at RISO laboratories in the 1970's to aid in the reliability analysis of nuclear power plants in Scandinavian countries. Recommended in assessment of hardware systems, more difficult to use in software systems. CCA is a good tool when complex system risks are evaluated. Related to ETA, FTA and Common Cause Analysis. Tools available. No task analysis	nuclear aircraft	P3.2 S3a.1	X	X			• [Bishop90] • [EN 50128] • [FAA00] • [Leveson95] • [MAS611-2] • [MUFTIS3.2-I] • [Rakowsky] • [Ridley&Andrews01] • [ΣΣ93, ΣΣ97]	PM:C KS:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						allowed								
44.	CCS (Calculus of Communicating Systems)	T	Ds	1983 about	CCS is an algebra for specifying and reasoning about concurrent systems. As an algebra, CCS provides a set of terms, operators and axioms that can be used to write and manipulate algebraic expressions. The expressions define the elements of a concurrent system and the manipulations of these expressions reveal how the system behaves.	Formal Method. Descriptive tool in cases where a system must consist of more than one process. Software requirements specification phase and design & development phase	telecom	P3.1 S3a.2		X			• [Bishop90] • [CCS] • [EN 50128] • [Rakowsky]	MC:R PM:C
45.	CDA (Code Data Analysis)	T	Ds	1996 or older	Code data analysis concentrates on data structure and usage in the coded software. Data analysis focuses on how data items are defined and organised. Ensuring that these data items are defined and used properly is the objective of CDA. This is accomplished by comparing the usage and value of all data items in the code with the descriptions provided in the design materials.		aircraft	S3a.2		X			• [NASA-GB-1740.13-96] • [Rakowsky]	PM:C MC:R
46.	Certificated Hardware Components	T	Dh	1990 or older	Aim is to assure that all hardware components that are used will not reveal inherent weaknesses after their use within the system by screening and segregating the positively certified components.	Recommended for safety critical systems. In some fields (e.g. military, space, avionics) they are mandatory. Tools available.	defence space avionics	S3a.2	X				• [Bishop90]	PM:C
47.	Certificated Software Components	T	Ds	1990 or older	Aim is to minimise the development of new software through the use of existing components of known level of confidence or quality.	Wherever possible, certificated components should be used. Additional validation and verification may be necessary. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
48.	Certificated Tools or Certified Tools and Certified Translators	T	Ds	1990 or older	Tools are necessary to help developers in the different phases of software development. Wherever possible tools should be certificated so that some level of confidence can be assumed regarding the correctness of their outputs	Recommended wherever available and appropriate. Tools available. Software design & development phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C
49.	CES (Cognitive Environment Simulation)	I	H	1987	Human performance assessment. Dynamic. Was developed for simulating how people form intentions to act in nuclear power plant personnel emergencies. CES can be used to provide an objective means of distinguishing which event scenarios are likely to be straightforward to diagnose and which scenarios are likely to be cognitively challenging, requiring longer to diagnose and which can lead to human error. Can also be used to predict human errors by estimating the mismatch between cognitive resources and demands of the particular problem-solving task	Human reliability family	nuclear	S3a.2			X		• [Kirwan98-1] • [MUFTIS3.2-I]	KS:R PM:R
50.	CESA (Commission Errors Search and Assessment)	T	H	2001	Aims at identifying potential Error of Commission situations, based on a catalogue of key actions required in the responses to the plant events.		nuclear	F3.1 F3.2 P3.2			X		• [HRA Washington]	KS:R PM:R
51.	CFMA	T	Dh	1979	Cable Failure Matrix Analysis identifies the risks	Should cables become damaged	aircraft	None	X				• [FAA AC431]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Cable Failure Matrix Analysis)				associated with any failure condition related to cable design, routing, protection, and securing. The CFMA is a shorthand method used to concisely represent the possible combinations of failures that can occur within a cable assembly.	system malfunctions can occur. Less than adequate design of cables can result in faults, failures and anomalies, which can result in contributory hazards and accidents. Similar to Bent Pin analysis.							• [FAA00] • [ΣΣ93, ΣΣ97]	MC:R
52.	CGHDS (Controlled General Hybrid Dynamical System)	M		1998	Interaction collection of dynamical (mathematical) systems, each evolving on continuous valued state spaces, and each controlled by continuous controls. Considers switching as a general case of impulses; the general term is jump. Each jump goes to a new dynamical system.		control	P3.2 S3a.2	X		X	X	• [Branicky&Borkar&Mitter98]	PM:R MC:R
53.	Change Analysis	T	R	1965 ?	Change Analysis examines the effects of modifications from a starting point or baseline. It is a technique designed to identify hazards that arise from planned or unplanned change. Four steps: review previous operation / current practice; 2) Review operational analysis of planned operation; 3) For each step / phase of the operation, identify differences (" changes") between the two; 4) Determine impact on risk of the operation. The change analysis systematically hypothesises worst-case effects from each modification from the baseline.	Any change to a system, equipment procedure or operation should be evaluated from a system safety view. Cause-Consequence analysis is also used during accident/ incident investigation.	management systems, all systems	F3.2 F3.3 P3.2 S3a.2 S3e.x	X			X	• [FAA AC431] • [FAA00] • [ORM] • [ΣΣ93, ΣΣ97]	PM:F KS:FC
54.	CHASE (Complete Health And Safety Evaluation)	T	H	1987	Safety culture audit tool uses performance indicators, which are organised into groups. The scores on the sub-sets of safety performance areas are weighted and then translated into an overall index rating.	Qualitative	health	S3c.1				X	• [Kennedy&Kirwan98]	KS:FC PM:R
55.	Check List Analysis	T	R	1974	Checklist Analysis is a comparison to criteria, or a device to be used as a memory jogger. The analyst uses a list to identify items such as hazards, design or operational deficiencies.	Checklist Analysis can be used in any type of safety analysis, safety review, inspection, survey, or observation. Checklists enable a systematic, step by step process. They can provide formal documentation, instruction, and guidance. Combines with What-if analysis or What-if checklist analysis.	chemical	F3.1 F3.2 F4a.x P3.1 P3.2 P4a.x S3a.2 S3c.1 S3c.2 S3e.x S4a.x	X	X	X	X	• [EN 50128] • [FAA00] • [Leveson95] • [ΣΣ93, ΣΣ97]	KS:FC PM:R
56.	CHIRP (Confidential Human Factor Incident Reporting Programme)	D		1982	The aim of CHIRP is to contribute to the enhancement of flight safety in the UK commercial and general aviation industries, by providing a totally independent confidential (not anonymous) reporting system for all individuals employed in or associated with the industries. Reporters' identities are kept confidential. Important information	CHIRP has been in operation since 1982 and is currently available to flight crew members, air traffic control officers, licensed aircraft maintenance engineers, cabin crew and the GA	aviation	F3.1 F3.2 F3.3 P3.2 S3c.1			X		• [CHIRP web] • For other systems like this, see [EUCARE web]	KS:F PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					gained through reports, after being disidentified, is made available as widely as possible, CHIRP provides a means by which individuals are able to raise issues of concern without being identified to their peer group, management, or the Regulatory Authority. Anonymous reports are not normally acted upon, as they cannot be validated.	community.								
57.	CIA (Code Interface Analysis)	T	Ds	1996 or older	Code interface analysis verifies the compatibility of internal and external interfaces of a software component. A software component is composed of a number of code segments working together to perform required tasks. These code segments must communicate with each other, with hardware, other software components, and human operators to accomplish their tasks. Check that parameters are properly passed across interfaces. CIA is intended to verify that the interfaces have been implemented properly.		aircraft	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C MC:R
58.	CIT (Critical Incident Technique)	T	M	1954	This is a method of identifying errors and unsafe conditions that contribute to both potential and actual accidents or incidents within a given population by means of a stratified random sample of participant-observers selected from within the population.	Operational personnel can collect information on potential or past errors or unsafe conditions. Hazard controls are then developed to minimise the potential error or unsafe condition. This technique can be universally applied in any operational environment.	nuclear aviation	S3c.1	X		X		• [FAA00] • [Infopolis2] • [Kirwan94] • [Kirwan&Ainsworth 92] • [ΣΣ93, ΣΣ97]	KS:F PM:C
59.	CLA (Code Logic Analysis)	T	Ds	1996 or older	Code Logic Analysis evaluates the sequence of operations represented by the coding program and will detect logic errors in the coded software. This analysis is conducted by performing logic reconstruction, equation reconstruction and memory coding.		aircraft computer	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C MC:R
60.	CMA (Common Mode Analysis)	T	R	1994 or older	Confirms the assumed independence that were considered in combination for a given failure condition. The effects of specification, design, implementation, installation, maintenance errors, manufacturing errors, environmental errors other than those already considered in the particular risk analysis. For example, hardware errors, software errors, installation errors, environmental such as temperature.	CMA is the third step in a Common Cause Analysis (CCA). Particular Risks Assessment is the second, and provides input to the CMA.	aircraft	F3.2 P3.2 S3a.1 S3a.2	X	X			• [ARP 4761] • [Dvorak00]	PM:C KS:FC
61.	CMA (Confusion Matrix Analysis)	T	H	1981	Determines human reliability. Is aimed specifically at two of the diagnostic error-forms, namely misdiagnoses and premature diagnoses. Identified scenarios are put on both the x and the y-axis of the matrix, and a panel of experts decides how confusable each scenario is with every other scenario.	Human reliability family. Is sometimes followed after an FSMA.	nuclear	P3.2 S3a.2			X		• [Kirwan94] • [Kirwan98-1] • [MUFTIS3.2-I]	KS:F PM:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
62.	CMFA (Common Mode Failure Analysis)	T	R	1979 about	Aim is to identify potential failures in redundant systems or redundant sub-systems that would undermine the benefits of redundancy because of the appearance of the same failures in the redundant parts at the same time.	The technique is not well developed but is necessary to apply, because without consideration of common mode failures, the reliability of redundant systems would be over-estimated. Related methods: ETA, CCA, FMEA	nuclear computer	P3.2 S3a.1	X	X			• [Bishop90]	PM:F KS:FC
63.	COCOM (COgnitive COntrol Model)	T	H	1993	Development of the argumentation that Human Error Assessment can only be done on the basis of a psychologically valid modelling of the context of the task in its environment. Human performance is dependent on the human's cognitive state: Strategic, Tactical, Opportunistic, or Scrambled.		ATM	S3a.2			X		• [Hollnagel93] • [Kirwan98-1]	KS:R PM:C
64.	CODA (Conclusions from Occurrences by Descriptions of Actions)	T	H	1997	Method for analysing human-related occurrences (i.e., incorrect human responses) from event cases retrospectively. The CODA method uses an open list of guidelines based on insights from previous retrospective analyses. It is recommended in this method to compile a short story that includes all unusual occurrences and their essential context without excessive technical details. Then the analysis should envisage major occurrences first. For their description, the method presents a list of criteria which are easy to obtain and which have been proved to be useful for causal analysis. For their causal analysis, various guidelines are provided. They are mainly of holistic, comparative and generalising nature. It is demonstrated by various event cases that CODA is able to identify cognitive tendencies (CTs) as typical attitudes or habits in human decision-making.	Quantification may be done with expert judgement or THERP.	nuclear	S3a.2			X		• [Reer97] • [Straeter&al99]	KS:R PM:C
65.	Code Analysis	T	Ds	1995 about ?	Code analysis verifies that the coded program correctly implements the verified design and does not violate safety requirements. The techniques used in the performance of code analysis mirror those used in design analysis.		aircraft computer	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C MC:R
66.	Code Coverage	T	Ds	1995 about ?	Check if all lines in the software code are used when running the program. Unused lines can be removed.		computer	S3a.2		X			• NLR expert	PM:C MC:R
67.	Code Inspection Checklists (including coding standards)	G			Coding standards are based on style guides and safe subsets of programming languages. Checklists should be developed during formal inspections to facilitate inspection of the code to demonstrate conformance to the coding standards.		aircraft computer	S3a.2		X			• [EN 50128] • [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C MC:R
68.	COGENT	T	H	1993	Extension of the THERP event tree modelling system,	It requires significant analytical	nuclear?	F3.3			X		• [Kirwan98-1]	KS:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(COGnitive EveNt Tree)				dealing particularly with cognitive errors, although the approach appears to deal with other errors as well. The aim is to bring current more cognitively-based approaches into the Human Error Identification process. This has led to a hybrid taxonomy with terms such as 'Skill-based slip', rule-based lapse, and knowledge-based lapses or mistakes. The approach thereafter is for the analyst to develop cognitive event trees.	judgement. At present, it appears to be a relatively simple step forward in modelling (representation), rather than in Human Error Identification.		P3.2 S3a.2							PM:C
69.	COMET (COMmission Event Trees)	T	H	1991	Modified event trees that deal with errors of commission and cascading errors whose source is either erroneous intention or a latent error. COMETs are developed e.g., using SNEAK, and are basically event trees, their results feeding into fault trees. The main significance of this approach appears to be as a means of integrating errors of commission into PSA and quantifying them. It does not help too much in terms of actually identifying errors of commission.	Relation with SNEAK and ETA.	?	P3.2 S3a.2				X		• [Kirwan98-1]	KS:FC PM:C
70.	Complexity Models	T	Ds	1976 about	Aim is to predict the reliability of programs from properties of the software itself rather than from its development or test history.	Can be used at the design, coding and testing phase to improve quality of software by the early identification of over-complex modules and by indicating the level of testing required for different modules. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
71.	Computer modelling and simulation	G		1978 or older	Involves the use of computer programs to represent operators and/or system activities or features. Human performance data that have been previously collected, or estimates of task components, error probabilities, etc., are entered into the computer program. The program either can then simulate graphically the environment and workspace or can dynamically run the task in real or fast time as a way of estimating complete cycle times and error likelihoods, etc.		all domains	P3.2 S3a.2	X		X	X	• [Kirwan&Ainsworth 92]	PM:F KS:FC
72.	Conduct Hazard Risk Assessment	G			Aim is to perform a system hazard risk assessment to identify and prioritise those safety critical computer software components that warrant further analysis beyond the architectural design level.		aircraft	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C
73.	Configuration Management	G		1980 about	Aim is to ensure the consistency of groups of development deliverables as those deliverables change. It applies to both hardware and software development	Should be regarded as mandatory technique. Tools available.	computer	S3a.2	X	X			• [Bishop90]	PM:R MC:R
74.	Confined Space Safety	T	R	1992	The purpose of this analysis technique is to provide a systematic examination of confined space risks. A confined	Any confined areas where there may be a hazardous atmosphere,	chemical	None	X			X	• [FAA00] • [ΣΣ93, ΣΣ97]	MC:R PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					space is defined to be an area that has both (1) insufficient ventilation to remove dangerous air contamination and/or oxygen deficiency, and (2) restricted access or egress.	toxic fume, or gas, the lack of oxygen, could present risks. Confined Space Safety should be considered at tank farms, fuel storage areas, manholes, transformer vaults, confined electrical spaces, race-ways.								
75.	Contingency Analysis	T	M	1972 ?	Contingency Analysis is a method of minimising risk in the event of an emergency. Potential accidents are identified and the adequacies of emergency measures are evaluated.	Contingency Analysis should be conducted for any system, procedure, task or operation where there is the potential for harm. Contingency Analysis lists the potential accident scenario and the steps taken to minimise the situation. It is an excellent formal training and reference tool.	many domains	P3.2 P3.3 S3a.1 S3b.x S3c.1	X		X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	KS:F PM:F
76.	Control Flow Checks or Control Flow Analysis	T	Dh	1990 or older	Aim is to detect computer mal-operation by detecting deviations from the intended control flow	Not necessary if the basic hardware is fully proven or self-checking. Otherwise, it is valuable technique for systems that can fail to a safe state where there is no hardware redundancy or no software diversity in the program or support tools. Tools available.	computer	S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	MC:R PM:C
77.	CORE (Controlled Requirements Expression)	T	Ds	1979	Aim is to ensure that all the requirements are identified and expressed. Intended to bridge the gap between the customer/end user and the analyst. Is designed for requirements expression rather than specification. Seven steps: 1) Viewpoint identification (e.g. through brainstorming); 2) Viewpoint structuring; 3) Tabular collection (Table with source, input, output, action, destination); 4) Data structuring (data dictionary); 5,6) Single viewpoint modelling and combined viewpoint modelling (model viewpoints as action diagrams, similar as in SADT); 7) Constraint analysis.	Developed for British Aerospace in the late 1970s to address the need for improved requirements expression and analysis. Despite its age, CORE is still used today on many projects within the aerospace sector. Is frequently used with MASCOT. Recommended for safety critical systems. Tools available.	computer	S3a.2		X			• [Bishop90] • [CS473] • [EN 50128] • [Rakowsky]	PM:R
78.	CORE-DATA (Computerised Human Error Database for Human Reliability Support)	D		1992 from	Database on human errors and incidents, for human reliability support. Currently contains about 1500 data points.	Originally collated from nuclear power industry, recently extended to other sectors, such as offshore lifeboat evacuation, manufacturing, offshore drilling, permit-to-work, electricity transmission, nuclear power plant	nuclear offshore manufacturing electr ATM	F3.1 F3.2 F3.3 P3.2 S3c.1			X		• [Kirwan&Basra&Taylor.doc] • [Kirwan&Basra&Taylor.ppt] • [Kirwan&Kennedy&Hamblen]	KS:F PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						emergency scenarios, calculator errors, and a small number of ATM-related human error probabilities have been developed								
79.	COSIMO (Cognitive Simulation Model)	I	H	1992	A parallel to CES in that it is a simulation of the human operator and his/her thought processes, using a computerised blackboard architecture. The simulated operator comprises a set of properties and attributes associated with particular incident scenarios, and 'packets' of process knowledge and heuristics rules of thumb. When diagnosing, each scenario and its associated attributes are contrasted to 'similarity-match' to the symptom set being displayed to the 'operator', and the simulated operator will either determine unequivocally which scenario matches the symptoms, or, if there is ambiguity, will 'frequency- gamble'. Once hypotheses are formulated, they are evaluated according to a confidence threshold, and may be accepted or rejected.	Human reliability family	nuclear	P3.2 S3a.2			X		• [Kirwan98-1] • [MUFTIS3.2-I]	KS:R PM:C
80.	CPA (Critical Path Analysis)	T	R	1950 s	Critical Path Analysis identifies critical paths in a Program Evaluation graphical network. Simply it is a graph consisting of symbology and nomenclature defining tasks and activities. The critical path in a network is the longest time path between the beginning and end events.	This technique is applied in support of large system safety programs, when extensive system safety-related tasks are required. Combines with PERT. Tools available.	safety management	P3.2 S3a.1	X			X	• [FAA AC431] • [FAA00] • [Kirwan&Ainsworth 92] • [ΣΣ93, ΣΣ97]	PM:F MC:?
81.	CPQRA (Chemical Process Quantitative Risk Analysis)	T	R	1989	Quantitative risk assessment within chemical process industry. Stands for the process of hazard identification, followed by numerical evaluation of incident consequences and frequencies, and their combination into an overall measure of risk when applied to the chemical process industry. Ordinarily applied to episodic events. Is related to Probabilistic Risk Assessment (PRA) used in the nuclear industry.	Processes of all types	chemical manuf	None	X			X	• [ΣΣ93, ΣΣ97] • [SOI terms]	KS:FC PM:C
82.	CRC (Control Rating Code Method)	T	M	1980 ?	Control Rating Code is a generally applicable system safety-based procedure used to produce consistent safety effectiveness ratings of candidate actions intended to control hazards found during analysis or accident analysis. Its purpose is to control recommendation quality, apply accepted safety principles, and priorities hazard controls.	Control Rating Code can be applied when there are many hazard control options available. The technique can be applied toward any safe operating procedure, or design hazard control.	defence	P3.2 P3.3 S3a.2	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:F
83.	CREAM (Cognitive Reliability and Error Analysis Method)	I	H	1993	Cognitive modelling approach. Attempts to bring cognitive psychology/science into the HEI arena, i.e. CREAM is aimed at being a more theoretically valid approach. It is a compound of SHERPA, SRK, and	Related to SHERPA, SRK and COCOM. The system is still under development. Process of studying	nuclear also outside nuclear	F3.2 F3.3 P3.2 S3a.2			X		• [Kirwan98-1]	KS:FC PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					COCOM. The approach can be applied retrospectively or prospectively, although further development is required for the latter. The 'meat' of CREAM is the Action-Error-Analysis Matrix. This shows relationships between 'causes' and 'effects', in both cases being a non-mutually-exclusive mixture of error mechanisms and performance shaping factors and some external error modes, occurring on both axes.	validity and reliability of CREAM is ongoing.								
84.	CREWPRO (CREW PRObIem solving simulation)	I	H	1994	Cognitive simulation which builds on CREWSIM		nuclear?	P3.2 S3a.2			X	X	• [Kirwan98-1]	KS:R PM:C
85.	CREWSIM (CREW SIMulation)	I	H	1993	Simulation model that models the response of an operating team in a dynamically evolving scenario. The model simulates operator interactions within a three-person crew, as well as the cognitive processes of the crewmembers, and the crew-plant dynamic interaction. Although the model has a knowledge base as other simulations do (e.g. COSIMO and CES), CREWSIM differs by using a set of prioritised lists that reflect the priorities of different concerns. Some other interesting aspects are 1) attentional resources control is simulated, such that diagnosis will be suspended while the operator is communicating or carrying out some other task. 2) the model's usage focuses particularly on transitions between procedures, and hence is looking in particular for premature, delayed, and inappropriate transfer within the emergency procedures system. 3) several error mechanisms are treated by the model: memory lapse; jumping to conclusions; communication failures; incorrect rules; and improper prioritisation.	Has been particularly developed to date to focus on a particular nuclear power plant scenario.	nuclear	P3.2 S3a.2			X	X	• [Kirwan98-1]	KS:R PM:C
86.	Criticality Analysis	T	R	1972 ?	The purpose of the Criticality Analysis is to rank each failure mode identified in a Failure Modes and Effect Analysis. Once critical failures are identified they can be equated to hazards and risks. Designs can then be applied to eliminate the critical failure, thereby eliminating the hazard and associated accident risk.	The technique is applicable to all systems, processes, procedures, and their elements. Combines with FMEA to become FMECA.	aircraft	F3.3 P3.2 P3.3	X			X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C KS:FC
87.	CRM (Collision Risk Model (ICAO))	T	R	1964	Collision risk model, adopted by ICAO. Also named Reich Collision risk model. Estimates of the level of risk of a mid-air collision between two aircraft. Based on 7 assumptions, two of which are rather restrictive. Calculates collision risk from traffic factors, aircraft parameters and navigational performance.	Mainly applies to largely strategic procedures only. No dynamic role for ATCos and pilots; basic logic is "navigational errors -> mid-air collisions"	ATM	P3.2 S3a.1				X	• [Bakker&Blom93] • [Brooker02] • [MUFTIS3.2-II] • [Reich64]	PM:F
88.	CSA	T	M	2000	Each safety hazard is investigated in the context of		ATM	P3.2	X		X	X	• [FAA00] (App B)	KS:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Comparative Safety Assessment)			or older	investment alternatives. The result is a ranking of alternative solutions by reduction in safety risk or other benefits.			P3.3					• [FAA tools]	PM:F
89.	CSP (Communicating Sequential Processes)	T	Ds	1978; update in 1985	Technique for the specification of concurrent software systems, i.e. systems of communicating processes operating concurrently. Allows one to describe systems as a number of components (processes) which operate independently and communicate with each other over well-defined channels. (The restriction that the component processes must be sequential was removed between 1978 and 1985, but the name was already established.)	Descriptive tool in cases where a system must consist of more than one process. Related to CCS. Software requirements specification phase and design & development phase	telecom	S3a.2		X			• [Bishop90] • [CSP] • [EN 50128] • [Rakowsky]	MC:R PM:C
90.	CSSA (Cryogenic Systems Safety Analysis)	T	R	1982	The purpose to specifically examine cryogenic systems from a safety standpoint in order to eliminate or to mitigate the hazardous effects of potentially hazardous materials at extremely low temperatures.	Use with PHA or SSHA. Cryogenic is a term applied to low-temperature substances and apparatus.	chemical	None	X				• [FAA AC431] • [ΣΣ93, ΣΣ97]	KS:R PM:R
91.	CSSM (Continuous Safety Sampling Methodology)	T	M	1997	This is a form of hazard analysis that uses observation and sampling techniques to determine and maintain a pre-set level of the operator's physical safety within constraints of cost, time, and operational effectiveness. This tool is used to determine whether activities are within tolerable limits. If outside tolerable limits, corrective action is then derived. However, it may focus more on industrial injury.		manuf	P3.2 P3.3 S3a.1	X		X		• [HIFA_safety]	PM:R
92.	CTA (Cognitive Task Analysis)	T	H	1994 or older	CTA thoroughly describes some aspect of human operation and cognitive processing within a work domain. CTA is used to design human-system interaction and displays, assess job requirements, develop training, or evaluate teamwork.	[MIL-HDBK] describes three examples for conducting CTA: 1) The Precursor, Action, Results and Interpretation method (PARI); 2) Conceptual Graph Analysis (CGA); 3) Critical Decision Method	defence	P3.1 P3.2 P3.3			X		• [CTA Resource] • [Davison] • [MIL-HDBK] • [Mislevy&al98]	KS:FC PM:F
93.	CTC (Comparison-To-Criteria)	T	R	1993	The purpose of CTC is to provide a formal and structured format that identifies safety requirements. Any deviations between the existing design requirements and those required are identified in a systematic manner, and the effect of such deviations on the safety of the process or facility is evaluated. The deviations with respect to system upsets are those caused by operational, external, and natural events. Operational events include, among others, individual component failures, human error interactions with the system (to include operation, maintenance, and testing), and support system failures. For systems that do not meet current design requirements, an upgrade is not done automatically until an assessment of their importance to safety is made.	Comparison-To-Criteria is a listing of safety criteria that could be pertinent to any FAA system. This technique can be considered in a Requirements Cross-Check Analysis. Applicable safety-related requirements such as OSHA, NFPA, ANSI, are reviewed against an existing system or facility.	nuclear	P3.1 P3.4	X	X	X		• [FAA00] • [McClure&Restrepo 99] • [ΣΣ93, ΣΣ97]	PM:F

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
94.	DADs (Decision Action Diagrams)	T	H	1992	Aim is to show how to navigate a system, based on decisions and actions. Actions are drawn as rectangles, decisions as diamonds, and possible decision outcomes are labelled on arrows from decision diamonds. Decisions can be phrased as yes/no or as multiple choice questions	Similar in appearance and logic to the mechanical handling diagrams which are used in mechanical HAZOPs. Also known as Information Flow Charts or Decision-Action-Information Diagrams. Also similar to functional flow diagrams	defence nuclear	P3.1 P3.2 S3a.2			X		• [Kennedy&Kirwan98] • [Kirwan94] • [Kirwan&Ainsworth92] • [MIL-HDBK] • [Silva&al99]	KS:FC PM:F
95.	Data Flow Analysis	T	Ds	1995 or older	Data flow analysis is a static analysis technique that is performed both at procedure level and also as part of the system wide analysis, which is one aspect of integration testing. It identifies data flow anomalies in the program, e.g. the use of uninitialised variables; no annotations are needed for that kind of analysis.		computer	S3a.2		X			• [EN 50128] • [Rakowsky] • [SPARK web]	PM:C MC:R
96.	Data Flow Diagrams	T	Ds	1989 or older	Data flow diagrams illustrate how data is processed by a system in terms of inputs and outputs. Different nodes and arrows exist: Processes, Datastores, Dataflows, External entities. DFD can be drawn in several nested layers.	The purpose and value of the data flow diagram is primarily *data* discovery, not *process* mapping Several tools exist.	computer	S3a.2		X			• [AIS-DFD] • [EN 50128] • [Rakowsky] • [Smartdraw]	PM:C MC:R
97.	Data Recording and Analysis	D			Detailed records are maintained during a project, both on a project and individual basis.	Software design & development phase and software maintenance phase	computer	S3a.2 S3c.2		X			• [EN 50128] • [Rakowsky]	PM:C
98.	Data Security	G		1975 or older	Aim is to guard against external and internal threats which can either accidentally or deliberately endanger the objectives of design and may lead to unsafe operation	Essential for safety-related systems. Tools available.	computer	S3a.1 S3a.2		X			• [Bishop90]	PM:C
99.	DCPN (Dynamically Coloured Petri Nets)	M		1997	Extension of Petri Nets to include dynamic colours, i.e. variables attached to Petri net tokens that can take on real values and that can change through time according to the solutions of stochastic differential equations. The transitions of tokens are according to Poisson point processes or based on the values of the tokens reaching a boundary.	DCPN can be mapped to and from Piecewise Deterministic Markov Processes. They are the modelling format used for the TOPAZ methodology.	ATM	P3.1 P3.2 S3a.1 S3a.2 S3c.1	X	X	X	X	• [Everdij&Blom&Klompstra97]	MC:R
100.	DD (Dependence Diagrams)	T	R	1994 or older	Structured, deductive, top-down analysis that identifies the conditions, failures, and events that would cause each defined failure condition. Graphical method of identifying the logical relationship between each particular failure condition and the primary element or component failures, other events, or combinations of these that can cause the failure condition. Similar to FTA, except that a Fault Tree Analysis is failure-oriented and is conducted from the perspective of which failures must occur to cause a defined failure condition. A Dependence Diagram Analysis is success-oriented and is conducted from the perspective of	In some references stated to be equivalent to Reliability Block Diagrams (RBD).	aircraft	P3.2 S3a.2	X				• [ARP 4761] • [FAA memo02]	PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					which failures must not occur to preclude a defined failure condition.									
101.	Decision Tables	T	R	1995 or older	Is based on the logic that a set of premises logically entails a conclusion, if every interpretation that satisfies the premises also satisfies the conclusion. Logical entailment is checked by comparing tables of all possible interpretations.	Hazard identification family. Can be seen as a rigorous generalisation of FMEA. Equal to Truth tables	computer	F3.3 F4a.x P3.2	X	X			• [EN 50128]	PM:C
102.	Defensive Programming	G		1988 or older	Aim is to produce programs which detect anomalous control flow, data flow or data values during their execution and react to these in a predetermined and acceptable manner	Recommended where there is insufficient confidence in the environment or the software. Tools available. Software architecture phase	computer	S3a.2		X			• [Bishop90] • [EN 50128]	PM:C
103.	Delphi Knowledge Elicitation Method or Delphi Method	G		1950 about	The Delphi method allows experts to deal systematically with a complex problem or task. The technique comprises a series of questionnaires sent either by mail or via computerised systems, to a pre-selected group of geographically dispersed experts. These questionnaires are designed to elicit and develop individual responses to the problems posed and to enable the experts to refine their views as the group's work progresses in accordance with the assigned task. The group interaction in Delphi is anonymous; comments, forecasts, and the like are not identified as to their originator but are presented to the group in such a way as to suppress any identification.	The main point behind the Delphi method is to overcome the disadvantages of conventional committee action. Anonymity, controlled feedback, and statistical response characterise Delphi.	defence aircraft	F3.1 F3.2 F3.3 F4a.x P3.2 P3.3 S3a.1 S3a.2 S3c.1	X		X		• [Delphi] • [Rakowsky]	KS:FC PM:C
104.	DES (Discrete Event Simulation)	M		1982 about ?	An event calendar is constructed which indicates what events are scheduled to occur and when. The simulation executes the first event on the calendar, which may lead to a state change, and next updates the calendar. Can be seen as special case of Monte Carlo Simulation	Dynamic assessment family. Humans can be incorporated, but only if there is a good underlying model for human (cognitive) behaviour.	many	P3.2 S3a.1 S3a.2	X		X	X	• [MUFTIS3.2-I]	PM:C
105.	Design and Coding Standards	G			Code is easier to read and modify if it's written to a consistent standard.	Software design and development phase	computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:C
106.	Design Constraint Analysis	T	Ds	1996 or older	Evaluates restrictions imposed by requirements, the real world and environmental limitations, as well as by the design solution. The design materials should describe all known or anticipated restrictions on a software component.		aircraft computer	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:R
107.	Design Data Analysis	T	Ds	1996 or older	Evaluates the description and intended use of each data item in the software design. Data analysis ensures that the structure and intended use of data will not violate a safety requirement. Description to use of each data item in the design logic is compared.		aircraft computer	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C
108.	Design for Testability (Hardware)	G		1969	Aim is to enable all hardware components to be fully tested both on and off line	Should be used wherever fault tolerance and redundancy is	computer	S3a.2 S3c.1	X				• [Bishop90]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						applied. Tools available.								
109.	Design for Testability (Software)	G		1980 or older	Aim is to make software amenable to thorough testing	Strongly recommended. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
110.	Design Interface Analysis	T	Ds	1996 or older	Verifies the proper design of a software component's interfaces with other components of the system. This analysis will verify that the software component's interfaces and control and data linkages between interfacing components have been properly designed.		aircraft	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96]	PM:C
111.	DETAM (Dynamic Event Tree Analysis Method)	I	R	1991	Generalisation of DYLAM to allow scenario branching based on stochastic variations in operator state	Dynamic assessment family	nuclear chemical	P3.1 P3.2 P3.3 S3a.2	X		X	X	• [MUFTIS3.2-I]	KS:FC PM:C
112.	Development Standards	G		1990 or older	To enhance software quality by using standard approaches to the software development process	Essential for safety critical systems. Necessary for implementing in a quality assurance program. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
113.	DFM (Dynamic Flowgraph Analysis)	I	Ds	1996 about	Is an integrated, methodical approach to modelling and analysing the behaviour of software-driven embedded systems for the purpose of dependability assessment and verification. DFM has two fundamental goals: 1) to identify how events can occur in a system; 2) to identify an appropriate testing strategy based on an analysis of system functional behaviour. To achieve these goals, DFM employs a modelling framework in which models expressing the logic of the system being analysed are developed in terms of causal relationships between physical variables and temporal characteristics of the execution of software modules.	New technique, not widely used and still in the experimental phase of evaluation. It combines the benefits of conventional SFTA and Petri nets	aircraft	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:R
114.	DFMM or DFM (Double Failure Matrix Method)	T	R	1981	Inductive approach that considers the effects of double failures. All possible failures are placed on the vertical and the horizontal axis of a matrix, and all combinations are considered and put into severity classes.	Static assessment family. Its use is feasible only for relatively noncomplex systems. Not very common technique and rarely used.	nuclear	F3.2 F3.3 P3.2	X				• [FT handbook02] • [MUFTIS3.2-I] • [OORM00]	PM:F
115.	Digraph Utilization Within System Safety	T	R	1992	Directional Graphs (digraphs) have been used to model failure effect scenarios within large complex systems, thereby modelling FMEA data. Digraphs can also be used to model hazardous events and reconstruct accident scenarios. As a result, both hazard analysis and accident investigation processes can be improved via modelling event sequences.	Model complex systems similar to FTA. Combines with FMEA	?	P3.2 S3a.2	X				• [FAA AC431] • [ΣΣ93, ΣΣ97]	PM:C
116.	Dispersion Modelling	T	R		Quantitative tool for environmental and system safety		chemical	P3.2	X				• [MAS611-2]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					engineering. Used in chemical process plants, can determine seriousness of chemical release. Internationally recognised model.			S3a.2						
117.	Diverse Programming or N-version Programming	T	Ds	1969 ?	Diverse Programming involves a variety of routines satisfying the same specification being written in isolation from one another. When a result is sought, voting takes place and the routine giving the most satisfactory answer wins. Aim is to detect and mask residual software design faults during execution of a program in order to prevent safety critical failures of the system, and to continue operation for high reliability	Software architecture phase Recommended for safety relevant fault compensating systems. Tools are not applicable.	computer nuclear	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky] • [SSCS] • [Storey96]	PM:C
118.	Diversity: The Safety Bag	T	M	1969 ?	Aim is to protect against residual specification and implementation faults in software that adversely affect safety. In this technique, an external monitor, called a safety bag, is implemented on an independent computer using a different specification. The primary function of the safety bag is to ensure that the main system performs safe - but not necessarily correct - operations. The safety bag continually monitors the main system to prevent it from entering an unsafe state. If a hazardous state does occur, the system is brought back to a safe state by either the safety bag or the main system.	Should be considered for fail-systems, provided there is adequate confidence in the dependability of the safety bag itself. Tools are not applicable. Software architecture phase. The Safety Bag is a form of Fault Detection and Diagnosis (FDD).	nuclear	S3a.2		X			• [Bishop90] • [EN 50128] • [Sparkman92]	PM:R
119.	DLA (Design Logic Analysis)	T	Ds	1996 or older	DLA evaluates the equations, algorithms and control logic of the software design. Logic analysis examines the safety-critical areas of a software component. Each function performed by the software component is examined. If it responds to, or has the potential to violate one of the safety requirements, it should be considered critical and undergo logic analysis.		aircraft	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C
120.	DMEA (Damage Mode and Effects Analysis)	T	R	1977	Damage Modes and Effects Analysis evaluates the damage potential as a result of an accident caused by hazards and related failures. It provides early criteria for survivability and vulnerability assessments. The DMEA provides data related to damage caused by specified threat mechanisms and the effects on system operation and mission essential functions.	Risks can be minimised and their associated hazards eliminated by evaluating damage progression and severity. Related to and combines with FMEA.	aviation defence	F3.3 P3.2 P3.3	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
121.	DO-178B (RTCA/EUROCAE ED-12B DO-178B)	I	Ds	1992	International standard on software considerations in airborne systems and equipment certification. Describes issues like systems aspects relating to software development, software lifecycle, software planning, etc, until aircraft and engine certification.	First version was released in 1981. Relates to civil aircraft and represents agreement between Europe and US.	aircraft	S3a.2		X			• [DO178B] • [Storey96]	PM:R
122.	DREAMS (Dynamic Reliability	I	H	1995	DYLAM-related technique. Human behaviour is modelled as dependent of the external world and the internal world.	Human reliability family	nuclear	P3.1 P3.2			X		• [MUFTIS3.2-I]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	technique for Error Assessment in Man-machine Systems)				These aspects are determined with dynamic simulation and may lead to human error or to random occurrence of errors.			S3a.2						
123.	DSA (Deactivation Safety Analysis)	T	M	1997 or older	This analysis identifies safety and health (S&H) concerns associated with facilities that are decommissioned/closed. The S&H practices are applicable to all deactivation activities, particularly those involving systems or facilities that have used, been used for, or have contained hazardous or toxic materials. The deactivation process involves placing the system or facility into a safe and stable condition that can be economically monitored over an extended period of time while awaiting final disposition for reuse or disposal. The deactivation methodology emphasises specification of end-points for cleanup and stabilisation based upon whether the system or facility will be deactivated for reuse or in preparation for disposal.	The deactivation process involves placing a facility into a safe mode and stable condition that can be monitored if needed. Deactivation may include removal of hazardous materials, chemical contamination, spill cleanup.	chemical	S3e.x	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:F
124.	DTA (Decision Tree Analysis)	T	R	1997	Decision Trees are tools for helping one to choose between several courses of action. They provide a structure within which one can lay out options and investigate the possible outcomes of choosing those options. They also help to form a balanced picture of the risks and rewards associated with each possible course of action.	Looks very similar to Fault Trees, including the quantification part of FTA.	nuclear	P3.2 S3a.2	X		X		• [MindTools-DTA] • [Straeter01]	PM:C
125.	DYLAM (Dynamic Logical Analytical Methodology)	I	R	1985	Implementation of concept of Dynamic Event Tree Analysis. A physical model for the system is constructed which predicts the response of system process variables to changes in component status. Next, the undesired system states are defined in terms of process variable levels. At the end of the first time interval all possible combinations of component states are identified and their likelihoods are calculated. These states are then used as boundary conditions for the next round of process variable updating. This is continued until an absorbing state is reached.	Dynamic assessment family	nuclear chemical	P3.1 P3.2 P3.3 S3a.2	X		X	X	• [Cacciabue&Amendola&Cojazzi86] • [Cacciabue&Carpignano&Vivalda92] • [Cojazzi&Cacciabue92] • [Kirwan98-1] • [MUFTIS3.2-I]	KS:FC PM:C
126.	Dynamic Event Tree Analysis	I	R	1985	Couples the probabilistic and physical behaviour of a dynamic process, for more detailed reliability analysis. Presents tree-based representation of an accident scenario.	Dynamic assessment family	nuclear chemical	P3.1 P3.2 S3a.2	X		X	X	• [MUFTIS3.2-I]	PM:C
127.	Dynamic Logic	T	Ds	1973 or older	Aim is to provide self-supervision by the use of a continuously changing signal	Essential in non-redundant systems. Desirable in redundant systems as a means of distinguishing faulty channels	computer	S3a.2		X			• [Bishop90]	PM:C
128.	Dynamic Reconfiguration	T	Ds	1971 or older	Aim is to maintain system functionality despite an internal fault	Valuable where high fault tolerance and high availability are both required, but costly and difficult to validate.	computer	S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						Software architecture phase								
129.	ED-78A (RTCA/EUROCAE ED-78A DO-264)	I	Dh	2000	Safety assessment methodology with steps OSED (Operational Service and Environment Definition), OHA (Operational Hazard Analysis), ASOR (Allocation of Safety Objectives and Requirements), together also named Operational Safety Assessment (OSA).	OSA is a requirement development tool based on the assessment of hazard severity. The OSA is normally completed during the Mission Analysis (MA) phase. Development of the OSA should begin as soon as possible in the MA process.	data communicat ion	F1.3 F3.1 F3.2 F3.3 F3.4 F4a.x P3.3	X		X		• [FAA00] chap 4 • [FAA tools]	PM:R
130.	Ego-less programming	T	Ds	2000 ?	A way of software programming that does not create an environment in which programmers consider the code as their own property, but are willing to share.		computer	S3a.2		X			• NLR expert	PM:C
131.	Electromagnetic Protection	G		1990 or older	Aim is to minimise the effects of electromagnetic interference (EMI) of the system by using defensive methods and strategies	Strongly recommended. Tools available.	electr	P3.3	X				• [Bishop90]	PM:R
132.	EMC (Electromagnetic Compatibility Analysis and Testing)	T	R	1989	The analysis is conducted to minimise/prevent accidental or unauthorised operation of safety- critical functions within a system. The output of radio frequency (RF) emitters can be coupled into and interfere with electrical systems which process or monitor critical safety functions. Electrical disturbances may also be generated within an electrical system from transients accompanying the sudden operation of electrical devices. Design precautions must be taken to prevent electromagnetic interference (EMI) and electrical disturbances. Human exposure to electromagnetic radiation is also a concern.	Adverse electromagnetic environmental effects can occur when there is any electromagnetic field. Electrical disturbances may also be generated within an electrical system from transients accompanying the sudden operations of solenoids, switches, choppers, and other electrical devices, Radar, Radio Transmission, transformers.	defence, avionics, and more	P3.2 P3.3 S3a.2 S3c.1	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
133.	Emergency Exercises	G			Practising the events in an emergency, e.g. leave building in case of fire alarm		nuclear	S3a.1 S3c.1				X	• [NEA01]	PM:R
134.	Energy Analysis	T	R	1972 or older	The energy analysis is a means of conducting a system safety evaluation of a system that looks at the "energetics" of the system.	The technique can be applied to all systems, which contain, make use of, or which store energy in any form or forms, (e.g. potential, kinetic mechanical energy, electrical energy, ionising or non-ionising radiation, chemical, and thermal.) This technique is usually conducted in conjunction with Barrier Analysis.	chemical electr	None?	X				• [FAA00] • [ΣΣ93, ΣΣ97]	KS:FC PM:C
135.	Energy Trace Checklist	T	R	1972 or older	Similar to Energy Trace and Barrier Analysis, Energy Analysis and Barrier Analysis. The analysis aids in the identification of hazards associated with energetics within a system, by use of a specifically designed checklist.	The analysis could be used when conducting evaluation and surveys for hazard identification associated with all forms of energy. The use of a checklist can	chemical electr	F3.2 F4a.x P3.2 S3a.2 S3c.1	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						provide a systematic way of collecting information on many similar exposures.								
136.	EOCA (Error of Commission Analysis)	T	H	1995	HAZOP-based approach whereby experienced operators consider procedures in detail, and what actions could occur other than those desired. Particular task formats, error mode keywords, and PSF (Performance Shaping Factor) are utilised to structure the assessment process and to prompt the assessors. Identified significant errors are then utilised in the PSA fault and/or event trees. This approach has only been used once, albeit successfully, in a real PSA.		nuclear?	F3.1 F3.2 F3.3 P3.2 P3.3			X	X	• [Kirwan94] • [Kirwan98-1]	MC:C KS:F PM:C
137.	Equivalence Classes and Input Partition Testing	T	Ds	1995 or older	Aim is to test the software adequately using a minimum of test data. The test data is obtained by selecting the partitions of the input domain required to exercise the software. This testing strategy is based on the equivalence relation of the inputs, which determines a partition of the input domain. Test cases are selected with the aim of covering all the partitions previously identified. At least one test case is taken from each equivalence class.		computer	S3a.2		X			• [EN 50128] • [ISO/IEC 15443] • [Rakowsky]	PM:C MC:R
138.	ERA (Environmental Risk Analysis)	T	R	1993 or older	The analysis is conducted to assess the risk of environmental non-compliance that may result in hazards and associated risks.	The analysis is conducted for any system that uses or produces toxic hazardous materials that could cause harm to people and the environment.	chemical	P3.2 S3a.1 S3c.1 S3e.x	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
139.	Ergonomics Checklists	G		1992 or older	These are checklists, which an analyst can use to ascertain whether particular ergonomics are being met within a task, or whether the facilities that are provided for that task are adequate.		nuclear	P3.2 S3a.2 S3c.1	X				• [Kirwan&Ainsworth 92]	KS:FC PM:R
140.	Error Detecting and Correcting Codes	M		1975 or older	Aim is to detect and correct errors in sensitive information. Describes how to transit bits over a possibly noisy communication channel. This channel may introduce a variety of errors, such as inverted bits and lost bits.	May be useful in systems where availability and response times are critical factors. Software architecture phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C MC:R
141.	Error Guessing	T	M	1995 or older	Error Guessing is the process of using intuition and past experience to fill in gaps in the test data set. There are no rules to follow. The tester must review the test records with an eye towards recognising missing conditions. Two familiar examples of error prone situations are division by zero and calculating the square root of a negative number. Either of these will result in system errors and garbled output.		computer	S3a.2		X			• [EN 50128] • [ErrorGuess] • [Rakowsky]	PM:R
142.	Error Seeding	T	Ds	1989	Technique that can be used to evaluate the ability of		computer	S3a.2		X			• [EN 50128]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
				or older	language processors to detect and report errors in source programs. The essence of the technique is to have a program which accepts correct programs ("target programs") as input, and subjects them to random variations, hence producing as output corrupted programs which can be used to assess the ability of a processor to detect errors which have been 'seeded' in them.								• [Meek&Siu89] • [Rakowsky]	
143.	ESAT (Expertensystem zur Aufgaben-Taxonomie (Expert-System for Task Taxonomy))	I	H	1992	Method established in the aviation field. Artificial intelligence concepts are used to describe the tasks.		aviation	P3.2 S3a.1			X		• [Straeter01]	PM:R
144.	ESC AIRS (Environmental Systems Corporation - Area Information Records System)	D			The Area Information Records System (AIRS) is a group of integrated, regional systems for the storage, analysis, and retrieval of information by public safety and justice agencies through the efficient and effective use of electronic data processing.	The Area Information Records System, is technically obsolete and no longer meets the current needs of participating agencies.	?	F3.1 F3.2 F3.3 P3.2 S3c.1	X				• [AIRS]	
145.	ESD (Event Sequence Diagrams)	T	R	1992 or older	An event-sequence diagram is a schematic representation of the sequence of events leading up until failure. In other words, it is a flow chart with a number of paths showing the 'big picture' of what happened - a holistic view. It is a variation of Cause Consequence Diagram and generalisation of ETA, not restricted to representation of event sequences, repairable systems can be modelled	Static assessment family	?	P3.2 S3a.2	X				• [MUFTIS3.2-I]	PM:C
146.	ESSAI (Enhanced Safety through Situation Awareness Integration in training)	I	T	2000 from	The ESSAI project aims at training solutions for problems that occur in cockpits when pilots are confronted with extreme situations (a Crisis) for which they do not have appropriate procedures. These extreme situations may be the result of a rare chain of events, but may also occur because of lack of Situation Awareness of the crew. The project plans to develop training tools and techniques and their implementation in training programmes.		ATM	F3.2 F3.3 P3.1 P3.2 P3.3 P3.4 S3a.1 S3a.2			X	X	• [ESSAI web]	
147.	ETA (Event Tree Analysis)	T	R	1980	An Event Tree models the sequence of events that results from a single initiating event and thereby describe how serious consequences can occur. Can be used for developing counter measures to reduce the consequences. The tool can be used to organise, characterise, and quantify potential accidents in a methodical manner. The analysis is accomplished by selecting initiating events, both desired and undesired, and develop their consequences through consideration of system/ component failure-and-success alternatives.	Former name is CTM (Consequence Tree Method). Recommended in conjunction with fault tree analysis as an alternative to cause-consequence diagrams. Mainly for technical systems; human error may also be modelled. Tools available.	nuclear offshore aircraft	F3.3 P3.2 S3a.2	X		X		• [Bishop90] • [EN 50128] • [FAA00] • [Leveson95] • [Kirwan94] • [Kirwan&Ainsworth 92] • [MUFTIS3.2-I] • [Rakowsky] claims this one does handle software	PM:F MC:F KS:FC

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
													• [ΣΣ93, ΣΣ97]	
148.	ETBA (Energy Trace and Barrier Analysis for Hazard Discovery and Analysis)	T	R	1973	Energy Trace and Barrier Analysis is similar to Energy Analysis and Barrier Analysis. The analysis can produce a consistent, detailed understanding of the sources and nature of energy flows that can or did produce accidental harm. The ETBA method is a system safety-based analysis process developed to aid in the methodical discovery and definition of hazards and risks of loss in systems by producing a consistent, detailed understanding of the sources and nature of energy flows that can or did produce accidental harm. Outputs support estimation of risk levels, and the identification and assessment of specific options for eliminating or controlling risk. These analyses are routinely started in conjunction with the System Hazard Analysis and may be initiated when critical changes or modifications are made.	The technique can be applied to all systems, which contain, make use of, or which store energy in any form or forms, (e.g. potential, kinetic mechanical energy, electrical energy, ionising or non-ionising radiation, chemical, and thermal.) Developed as part of MORT.	chemical electr	None?	X				• [FAA AC431] • [FAA00] • [MAS611-2] • [ΣΣ93, ΣΣ97]	KS:FC PM:C
149.	Event and Causal Factor Charting	G			Event and Casual Factor Charting utilises a block diagram to depict cause and effect.	The technique is effective for solving complicated problems because it provides a means to organise the data, provides a summary of what is known and unknown about the event, and results in a detailed sequence of facts and activities.	nuclear	F3.1 F3.2 F3.3 F4a.x P3.1 P3.2 S3c.1	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
150.	Explosive Safety Analysis	T	R	1997 or older	This method enables the safety professional to identify and evaluate explosive hazards associated with facilities or operations. The purpose is to provide an assessment of the hazards and potential explosive effects of the storage, handling or operations with various types of explosives from gram to ton quantities and to determine the damage potential.	Explosives Safety Analysis can be used to identify hazards and risks related to any explosive potential, i.e. fuel storage, compressed gases, transformers, batteries.	chemical	F3.2 P3.2	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
151.	External Events Analysis	T	R	1992 or older	The purpose of External Events Analysis is to focus attention on those adverse events that are outside of the system under study. It is to further hypothesise the range of events that may have an effect on the system being examined.	The occurrence of an external event such as an earthquake is evaluated and affects on structures, systems, and components in a facility are analysed.	nuclear chemical	F3.2 F3.3 P3.2 S3a.2 S3c.1	X				• [FAA00] • [Region I LEPC] • [ΣΣ93, ΣΣ97]	PM:R
152.	FACE (Framework for Analysing Commission Errors)	I	H	1999	Framework for analysing errors of commission. The framework consists of five generic phases: I) Target selection, II) identification, III) screening, IV) modelling, V) probability assessment		nuclear	P3.1 P3.2 S3a.2			X		• [HRA Washington] • [Straeter01]	KS:FC PM:C
153.	Factor Analysis	G		1900	The purpose of factor analysis is to discover simple patterns in the pattern of relationships among the variables. In particular, it seeks to discover if the observed		?	S3a.2	X				• [Darlington] • [Rakowsky]	KS:R PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					variables can be explained largely or entirely in terms of a much smaller number of variables called *factors*.									
154.	Fail safety	T	Ds	1987 or older	Aim is to design a system such that failures will drive the system to a safe state	Strongly recommended for systems where there are safe plant states	computer	P3.3	X	X			• [Bishop90]	PM:C
155.	Failure Assertion Programming	T	Ds	1995 or older	This technique entails programming pre- and post-condition checks.	Software architecture phase	computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:C
156.	Failure Tracking	T	Dh Ds	1983 or older	Aim is to minimise the consequences of detected failures in the hardware and software.	Desirable for safety-related applications. Tools available.	computer	P3.3 S3a.2	X	X			• [Bishop90]	PM:C
157.	Fallible machine Human Error	T	H	1990	A model of human information processing that accounts for a variety of empirical findings. The important feature of the model is that items in a long term "Knowledge base" (such as task knowledge) are "activated" and recalled into working memory by processes that depend in the current contents of the working memory and sensory inputs. Items that are recalled will ultimately be used in making decisions that result in motor outputs. Central to the operation of this 'machine' are the processes by which long term memory items are 'activated' in a way that allows them to be selected for use. According to the model, two processes govern the activation of long term memory items: *similarity matching* and *frequency gambling*. Briefly stated, similarity matching means that items are activated on the basis of how closely they match environmental and task dependent cues, and frequency gambling means that items receive greater activation if they have been activated more frequently in the past.		?	P3.2 S3a.1 S3a.2			X		• [Fields01] • [Reason90]	
158.	FAST (Functional Analysis System Technique)	T	Dh	1973	This tool is used in the early stages of design to investigate system functions in a hierarchical format and to analyse and structure problems (e.g., in allocation of function). The aim of FAST is to understand how systems work and how cost effective modification can be incorporated. It asks 'how' a sub-task links to tasks higher up the task hierarchy, and 'why' the super-ordinate tasks are dependent on the sub-tasks.		?	P3.1 P3.2 P3.3	X				• [HIFA_sysdesig] • [Kirwan&Ainsworth 92]	KS:R PM:C
159.	Fault Injection	T	Ds	1984 ?	Faults are injected into the code to see how the software reacts.		computer	S3a.2		X			• [FaultInjection]	PM:C MC:F
160.	Fault Isolation Methodology	T	Dh	1985	The method is used to determine and locate faults in large-scale ground based systems. Examples of specific methods applied are: Half-Step Search, Sequential Removal/ Replacement, Mass replacement, and Lambda	Determine faults in any large-scale ground based system that is computer controlled.	automotive	S3a.2	X	X			• [FAA00] • [Rakowsky] • [ΣΣ93, ΣΣ97]	MC:C PM:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					Search, and Point of Maximum Signal Concentration.									
161.	Fault Schedule and Bounding Faults	T	R		The purpose of a fault schedule is to identify hazards to operators and to propose engineered, administrative and contingency controls to result in acceptable risks.		nuclear	F3.2 P3.2 P3.3			X		• [Kirwan&Kennedy&Hamblen]	KS:F
162.	FDD (Fault Detection and Diagnosis scheme)	T	Ds	1995 or older	Fault detection is the process of checking a system for erroneous states caused by a fault. A fault is evaluated by means of a classification into non-hazard and hazard classes that are represented by fuzzy sets. Through the use of diagnostic programs, the software checks itself and hardware for incorrect results.	Software architecture phase	computer	S3a.2	X	X			• [EN 50128] • [Rakowsky] • [Schram&Verbrugge n98] • [Sparkman92]	PM:C
163.	FHA (Fault Hazard Analysis)	T	R	1965 about	A system safety technique that is an offshoot from FMEA. It is similar to FMEA however failures that could present hazards are evaluated. Hazards and failure are not the same. Hazards are the potential for harm, they are unsafe acts or conditions. When a failure results in an unsafe condition it is considered a hazard. Many hazards contribute to a particular risk.	Any electrical, electronics, avionics, or hardware system, sub-system can be analysed to identify failures, malfunctions, anomalies, and faults, that can result in hazards. Hazard analysis during system definition and development phase. Emphasis on the cause. Inductive. FHA is very similar to PHA and is a subset of FMEA.	electr avionics	F3.1 F3.2 P3.2 P3.3	X				• [FAA AC431] • [FAA00] • [FT handbook02] • [Leveson95] • [ΣΣ93, ΣΣ97]	PM:C
164.	FHA (Functional Hazard Analysis)	T	Dh	1992 or older	Evaluation of functional system failures on system for every major operational phase. The severity and consequences of the scenarios are categorised in four hazard classes, based on subjective opinion of experts.	Hazard identification family. Note that this method has the same acronym as SAM's FHA, but is restricted to equipment failures only.	aircraft	F3.1 F3.2 F3.3 P3.2	X				• [MUFTIS3.2-I]	KS:R PM:R
165.	Finite State Machines	M		1962	Looks like Petri Nets. Aim is to define or implement the control structure of a system.	A simple yet powerful technique that should be considered for event driven systems. Tools available. Similar to State Transition Diagrams	computer	P3.1 P3.2 S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C MC:F C
166.	Finite State semi-Markov processes	M			These are Markov processes having a finite state space, that also allow non-exponential distributions		?	P3.2 S3a.2	X		X	X	• [Markov process]	
167.	Fire Hazards Analysis	G			Fire Hazards Analysis is applied to evaluate the risks associated with fire exposures. There are several fire-hazard analysis techniques, i.e. load analysis, hazard inventory, fire spread, scenario method. Other reference mentions as subtechniques: Preliminary Fire Hazard Analysis, Barrier Analysis, Fuel Load ANalysis, National Fire Protection Association Decision Tree Analysis	Any fire risk can be evaluated.	rail	F3.2 P3.2 S3a.1 S3c.1	X			X	• [FAA AC431] • [FAA00] • [Peacock&al01] • [ΣΣ93, ΣΣ97]	PM:R
168.	FIs (Fagan Inspections)	I	Ds	1976	The inspection process involves the following steps - 1) Identify Deliverable To Inspect 2) Choose Moderator and Author 3) Run Deliverable Through Code Validator 4)	One of the best methodologies available to evaluate the quality of code modules and program sets	aircraft	S3a.2		X			• [EN 50128] • [NASA-GB-1740.13-96]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					Identify Concerns (Create Inspection Checklist) 5) Choose Reviewers and Scribe 6) Hold Initial Briefing Meeting 7) Perform the Inspection Itself 8) Hold the Inspection Meeting 9) Generate Issues Report 10) Follow-up on Issues And the following people - a) Author b) Moderator c) Reviewer d) Scribe								• [Rakowsky] • [SPS2001]	
169.	Five Star System	T	H	1988	Safety culture audit tool uses performance indicators, which are organised into groups. The scores on the sub-sets of safety performance areas are weighted and then translated into an overall index rating.	Qualitative	?	S3c.1				X	• [Kennedy&Kirwan98]	PM:C
170.	Flow Analysis	T	Dh	1982 or older	The analysis evaluates confined or unconfined flow of fluids or energy, intentional or unintentional, from one component/sub-system/ system to another. Also used to detect poor and potentially incorrect program structures. Two types: Control FA and Data FA	The technique is applicable to all systems which transport or which control the flow of fluids or energy. Complementary to inspection methods. Recommended especially if there is suitable tool support. Tools available.	chemical electr computer	P3.1 S3a.2	X	X			• [Bishop90] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
171.	FMEA (Failure Mode and Effect Analysis) or SFMEA (Systems Failure Mode and Effect Analysis)	T	Dh	1949	FMEA is a reliability analysis that is a bottom up approach to evaluate failures within a system. It provides check and balance of completeness of overall safety assessment. It systematically analyses the components of the target system with respect to certain attributes relevant to safety assessment.	Any electrical, electronics, avionics, or hardware system, sub-system can be analysed to identify failures and failure modes. Recommended in all system reliability analyses. Tools available. Not suitable for humans and software	nuclear chemical space windturbine rail	F3.2 F3.3 P3.2 S3a.2	X				• [Bishop90] • [Cichocki&Gorski] • [FAA00] • [Kirwan&Ainsworth92] • [Leveson95] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97] • [Storey96]	PM:F KS:FC
172.	FMECA (Failure Mode Effect and Criticality Analysis)	T	Dh	1967	Is FMEA completed with a measure for criticality (i.e. probability of occurrence and gravity of consequences) of each failure mode. Aim is to rank the criticality of components that could result in injury, damage or system degradation through single-point failures in order to identify those components that might need special attention and control measures during design or operation.	Recommended for safety critical hardware systems where reliability data of the components is available. Less relevant technique now that HAZOP is developed.	aircraft chemical offshore windturbine rail	P3.2 S3a.2	X				• [Bishop90] • [FAA00] • [Leveson95] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97]	PM:F KS:FC
173.	FMES (Failure Modes and Effects Summary)	T	Dh	1994 or older	Groups failure modes with like effects. FMES failure rate is sum of failure rates coming from each FMEA. Is used as an aid to quantify primary FTA events.		aircraft	P3.2 S3a.2	X				• [ARP 4761]	PM:C
174.	Formal Inspections	T	Ds	1996 or older	A safety checklist, based on safety requirements, is created to follow when reviewing the requirements. After inspection, the safety representative reviews the official findings of the inspection and translates any that require safety follow-up on to a worksheet.		aircraft	P4a.x S3a.2		X			• [NASA-GB-1740.13-96]	PM:C MC:R
175.	Formal Methods	M			Formal methods consist of a set of techniques and tools	Generation of code is the ultimate	aircraft	S3a.2		X			• [DO178B]	MC:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					based on mathematical modelling and formal logic that are used to specify and verify requirements and designs for computer systems and software.	output of formal methods. In a pure formal methods system, analysis of code is not required. In practice, however, attempts are often made to apply formal methods to existing code after the fact.	computer						• [EN 50128] • [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky] • [Storey96]	C PM:C
176.	Formal Proof	T	Ds	1995 or older	A number of assertions are stated at various locations in the program and they are used as pre and post conditions to various paths in the program. The proof consists of showing that the program transfers the preconditions into the post conditions according to a set of logical rules and that the program terminates	Software verification and testing phase	computer	S3a.2 S4b.x		X			• [EN 50128] • [Rakowsky]	PM:C
177.	Formally Designed Hardware	G		1988 or older	Aim is to prove that the hardware design meets its specification	Best applied in context where all components are formally proven. Can be used in combination with N out of M voting. Tools available.	rail computer	P3.2 P4a.x	X				• [Bishop90]	PM:C
178.	Forward Recovery	T	Ds	1995 or older	Apply corrections to the damaged state; some understanding of errors that have occurred is needed. If errors are very well understood, the Forward Recovery approach can give rise to efficient and effective solutions.	Software architecture phase	computer	S3a.2		X			• [EN 50128] • [Rakowsky] • [SSCS]	PM:C
179.	FPC (Flow Process Chart)	T	Dh	1986 or older	A Flow Process Chart is a graph with arrows and six types of nodes: Operation, Move, Delay, Store, Inspect process, and Decision. It allows a closer examination of the overall process charts for material and/or worker flow and includes transportation, storage and delays.		defence	P3.1 S3a.2	X			X	• [MIL-HDBK] • [MurTon]	PM:C
180.	Front-End Analysis	I	M	1993	Comprises four analyses: (1) Performance analysis: Determine if it is a training/ incentive/ organisational problem. I.e., identify who has the performance problem (management/ workers, faculty/learners), the cause of the problem, and appropriate solutions. (2) Environmental analysis: Accommodate organisational climate, physical factors, and socio-cultural climate to determine how these factors affect the problem. (3) Learner analysis: Identify learner/ trainee/ employee characteristics and individual differences that may impact on learning / performance, such as prior knowledge, personality variables, aptitude variables, and cognitive styles. (4) Needs assessment: Determine if an instructional need exists by using some combination of methods and techniques.	Also referred to as Training Systems Requiremenets Analysis	road	S3a.2			X	X	• [FEA web] • [IDKB]	PM:R
181.	FSMA (Fault-Symptom Matrix	T	R	1994 or	A Fault-Symptom Matrix is a matrix with vertically the faults of a system and horizontally the possible	Linked to Confusion Matrix Approach	nuclear	P3.2 S3a.2	X				• [Kirwan94] • [Qiu&al]	KS:FC PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Analysis)			older	symptoms. The boxes contain probabilities of occurrence.									
182.	FSSA (Facilities System Safety Analysis)	T	R	1992 or older	System safety analysis techniques are applied to facilities and its operations. Safety analyses, within the FSSA, document the safety bases for and commitments to the control of subsequent operations. This includes staffing and qualification of operating crews; the development, testing, validation, and inservice refinement of procedures and personnel training materials; and the safety analysis of the person-machine interface for operations and maintenance. In safety analyses for new facilities and safety-significant modifications to existing facilities, considerations of reliable operations, surveillance, and maintenance and the associated human factors safety analysis are developed in parallel and integrated with hardware safety design and analysis. Once a facility or operation is in service, the responsible contractor and safety oversight activities use the report.	Facilities are analysed to identify hazards and potential accidents associated with the facility and systems, components, equipment, or structures.	nuclear chemical	P3.2 S3a.2	X		X	X	• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
183.	FTA (Fault Tree Analysis)	T	R	1961	A Fault Tree Analysis is a graphical design technique that could provide an alternative to block diagrams. It is a top-down, deductive approach structured in terms of events. Starting at an event that would be the immediate cause of a hazard (the top event), analysis is carried out along a tree path. Combinations of causes are described with logical operators (And, Or, etc). Faults are modelled in terms of failures, anomalies, malfunctions, and human errors.	Former name is CTM (Cause Tree Method). Any complex procedure, task, system, can be analysed deductively. Recommended for system safety analysis and HAZOPs. Tools available. Developed in 1961 for US ICBM program; guide published in 1981. The logical operations are covered within IEC 1025 international standard. For software it can be used during the software architecture phase. Can incorporate human errors.	nuclear offshore windturbine aircraft	P3.1 P3.2 S3a.2	X	X	X		• [Bishop90] • [EN 50128] • [FAA00] • [FT Handbook02] • [Kirwan&Ainsworth 92] • [Kirwan94] • [Leveson95] • [MAS611-2] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97] • [Storey96]	PM:F MC:C KS:F
184.	Function allocation trades	T	M	1986 or older	Working in conjunction with project subsystem designers and using functional flows and other human error methods, plus past experience with similar systems, the practitioner makes a preliminary allocation of the actions, decisions, or functions shown in the previously used charts and diagrams to operators, equipment or software.	Several techniques are proposed to work out the details in this method.	defence	P3.1 S3a.2	X	X	X		• [MIL-HDBK]	KS:R PM:R
185.	Functional Flow Diagram	T	Dh	1986 or older	Block diagram that illustrates the relationship between different functions. It is constructed by identifying the functions to be performed in the system, and then arranging these as a sequence of rectangular blocks, which represent the interrelationships between the functions. AND and OR gates are used to represent necessary	Is called the most popular systems method for the determination of system requirements.	defence	P3.1 P3.3 P3.4	X				• [Kirwan&Ainsworth 92] • [MIL-HDBK]	PM:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					sequences of functions or alternative courses of action.									
186.	Fuzzy Logic	M		1960	Fuzzy logic is a superset of conventional (Boolean) logic that has been extended to handle the concept of partial truth: truth values between "completely true" and "completely false".	It was introduced by Dr. Lotfi Zadeh of UC/Berkeley in the 1960's as a means to model the uncertainty of natural language. Software design & development phase	computer	S3a.2		X			• [EN 50128] • [FuzzyLogic] • [Rakowsky]	PM:C
187.	Gain scheduling	G			Ad-hoc methodology to achieve fault tolerance by storing pre-computed gain parameters. It requires an accurate FDD (Fault Detection and Diagnosis scheme) system that monitors the status of the system.	Popular methodology	?	S3a.2	X				• [Schram&Verbrugge n98]	PM:R
188.	Gas model	M			Analytical accident risk model to determine probability of collision between aircraft or to assess air traffic controller workload. Based on the physical model of gas molecules.		ATM	P3.2 S3a.1	X		X	X	• [MUFTIS1.2]	PM:R
189.	GEMS (Generic Error Modelling System)	T	H	1987	GEMS is an error classification model that is designed to provide insight as to why an operator may move between skill-based or automatic rule based behaviour and rule or knowledge-based diagnosis. Errors are categorised as slips/lapses and mistakes. The result of GEMS is a taxonomy of error types that can be used to identify cognitive determinants in error sensitive environments. GEMS relies on the analyst either having insight to the tasks under scrutiny or the collaboration of a subject matter expert, and an appreciation of the psychological determinants of error.	Psychologically-based tool. Attempts to bring generalised psychological theories or models into the rich context of a complex industrial work environment. Rarely used as tool on its own.	nuclear	S3a.2 S3c.1			X		• [Kirwan94] • [Kirwan98-1]	KS:R PM:R
190.	Generalised gas model	M			Analytical model. Based on the gas model, but the aircraft do not always fly in random directions. Aim is to determine probability of collision between aircraft or to assess air traffic controller workload.		ATM	P3.2 S3a.1	X		X	X	• [MUFTIS1.2]	PM:R
191.	Generalised Reich collision risk model	T	R	1993	Generalisation of Reich collision risk model (CRM). For the determination of collision risk between aircraft. Does not need two restrictive assumptions that Reich's CRM needs. Used within TOPAZ.		ATM	P3.2 S3a.1	X		X	X	• [Bakker&Blom93] • [Blom&Bakker02] • [MUFTIS3.2-II]	PM:C
192.	GFCM (Gathered Fault Combination Method)	T	Dh	1991 or older	Extension and generalisation of FMEA. A FMECA is made for all components of the system. Next, failure modes (or their combinations), which have the same effect are gathered in a tree	Hazard identification family. Qualitative and quantitative	aeronautics electr	P3.1 P3.2 S3a.2	X				• [MUFTIS3.2-I]	PM:C
193.	GO charts	T	Dh	1975	Is used for reliability analysis of complex systems (including components with two or more failure modes), mainly during the design stage	Recommended for a qualitative analysis during the design stage. Related techniques: FTA, Markov analysis. Tools available	?	P3.2	X				• [Bishop90]	PM:C
194.	GOMS (Goals, Operators,	I	H	1983	GOMS is a task modelling method to describe how operators interact with their systems. Goals and sub-goals	GOMS is mainly used in addressing human-computer	defence	P3.1			X	X	• [HIFA_taskanalysis] • [Kirwan&Ainsworth	KS:R PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Methods and Systems)				are described in a hierarchy. Operations describe the perceptual, motor and cognitive acts required to complete the tasks. The methods describe the procedures expected to complete the tasks. The selection rules predict which method will be selected by the operator in completing the task in a given environment.	interaction and considers only sequential tasks.							92]	
195.	Graceful Degradation	T	Ds	1978 ?	Aim is to maintain the more critical system functions available despite failures, by dropping the less critical functions	Highly recommended for systems with no fail-safe state	computer	P3.1 S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C
196.	GSN (Goal Structuring Notation)	T	R	1996 or older	Allows the capture and manipulation of logical arguments, and supports the distinction between high level argumentation and supporting evidence in safety cases.	Tools available	avionics defence	P3.2 S3a.2	X		X	X	• [Pygott&al99] • [Wilson&al96]	PM:R KS:F
197.	Hardware/ Software Safety Analysis	T	Dh Ds	1985 or older	The analysis evaluates the interface between hardware and software to identify hazards within the interface.	Any complex system with hardware and software.	computer	S3a.2	X	X			• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
198.	HATLEY	T	Ds	1987	The Hatley notation uses visual notations for modelling systems. Belongs to a class of graphical languages that may be called "embedded behaviour pattern" languages because it embeds a mechanism for describing patterns of behaviour within a flow diagram notation. Behaviour patterns describe different qualitative behaviours or modes, together with the events that cause changes in mode, for the entity being modelled. The flow notation models the movement of information through the system together with processes that use or change this information. Combining these two modelling capabilities makes it possible to model control of processes. A process may, for example, be turned on or off when a change in mode occurs.		computer	S3a.2		X			• [Williams91]	
199.	Hazard Analysis	G			Includes generic and specialty techniques to identify hazards. Generally, it is a formal or informal study, evaluation, or analysis to identify hazards.	Multi-use technique to identify hazards within any system, sub-system, operation, task or procedure.	aircraft	F3.2 P3.2	X		X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
200.	Hazard coverage based modelling	T	R	1998	Safety modelling that checks after each modelling iteration if and how all identified hazards have been modelled. The following modelling iteration will focus on the main hazards that have not been modelled yet. The last iteration ends with an assessment of the effect of non-coverage of the remaining hazards.		ATM	F3.1 F3.2 F3.3 F4a.x P3.2 P3.3 P.4a S3a.1 S3a.2 S3b.x	X	X	X	X	• NLR expert	

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
								S3c S3e.x S4a.x						
201.	Hazard Indices	T	Dh	1995 or older	Hazard indices measure loss potential due to fire, explosion, and chemical reactivity hazards in the process industries. Can be useful in general hazard identification, in assessing hazard level for certain well-understood hazards, in the selection of hazard reduction design features for the hazards reflected in the index, and in auditing an existing plant	Originally developed primarily for insurance purposes and to aid in the selection of fire protection methods.	chemical	F3.2 F3.3 P3.2 S3c.1	X				• [Leveson95]	PM:R
202.	HAZid (Hazard Identification)	T	H	1993 or older	Modification of HAZOP especially to be used for identification of human failures. It has an additional first column with some guidewords to lead the keywords.	Hazard identification family.	ATC	F3.1 F3.2 F3.3 P3.2 P3.3			X		• [MUFTIS3.2-I]	PM:C
203.	HAZOP (Hazard and Operability study)	T	M	1974	Group review using structured brainstorming using keywords. Aim is to discover potential hazards, operability problems and potential deviations from intended operation conditions. Also establishes likelihood and consequence of event. Hazardous events on the system should be identified with other technique.	Began with chemical industry in the 1960s. Any process or product using brainstorming This technique should be considered mandatory for safety related systems. Analysis covers all stages of project life cycle. In practice, the name HAZOP is sometimes (ab)used for any "brainstorming with experts to fill a table with hazards and their effects".	chemical rail ATM computer nuclear	F3.1 F3.2 F3.3 P3.2 P3.3 S3a.1 S3a.2 S3c.1 S3c.2 S3e.x	X	X	X		• [Bishop90] • [EN 50128] • [Kennedy slides] • [Kirwan-sages] • [Kirwan&Ainsworth 92] • [Kirwan94] • [Kirwan98-1] • [Leveson95] • [MUFTIS3.2-I] • [Rakowsky] • [Reese&Leveson97] • [ΣΣ93, ΣΣ97] • [Storey96]	PM:F MC:F KS:F
204.	HCA (Human Centred Automation)	I	M	1996	Design and development concept. Can be used to study whether explicit information on the actions of the plant automation system improves operator performance when handling plant disturbances caused by malfunctions in the automation system.		ATM	P3.1 P3.2 S3a.2			X		• [Kirwan&al97] • [Kirwan_HCA]	KS:F PM:C
205.	HCR (Human Cognitive Reliability model)	T	H	1982 from	Method for determining probabilities for human errors after trouble has occurred in the time window considered. Probability of erroneous action is considered to be a function of a normalised time period, which represents the ration between the total available time and the time required to perform the correct action. Different time-reliability curves are drawn for skill-based, rule-based and knowledge-based performance.	Human reliability family. Not considered as very accurate.	nuclear	P3.2 S3a.2			X		• [Humphreys88] • [Kirwan94] • [MUFTIS3.2-I]	KS:R PM:C
206.	HEA	G			Method to evaluate the human interface and error potential	Human Error Analysis is	many	P3.2	X		X	X	• [FAA AC431]	KS:FC

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Human Error Analysis)				within the human /system and to determine human-error-related hazards. Many techniques can be applied in this human factors evaluation. Contributory hazards are the result of unsafe acts such as errors in design, procedures, and tasks. This analysis is used to identify the systems and the procedures of a process where the probability of human error is of concern. The concept is to define and organise the data collection effort such that it accounts for all the information that is directly or indirectly related to an identified or suspected problem area. This analysis recognises that there are, for practical purposes, two parallel paradigms operating simultaneously in any human/machine interactive system: one comprising the human performance and the other, the machine performance. The focus of this method is to isolate and identify, in an operational context, human performance errors that contribute to output anomalies and to provide information that will help quantify their consequences.	appropriate to evaluate any human/machine interface.		S3a.2						• [FAA00] • [HEA practice] • [HEA-theory] • [ΣΣ93, ΣΣ97]	PM:C
207.	HEART (Human Error Assessment and Reduction Technique)	T	H	1985	Quantifies human errors in operator tasks. 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.	Human reliability family. Popular technique.	nuclear chemical defence	P3.2 S3a.2			X		• [Humphreys88] • [Kennedy] • [Kirwan94] • [MUFTIS3.2-I] • [Williams88]	KS:FC PM:C
208.	HEMECA (Human Error Mode, Effect and Criticality Analysis)	T	H	1989	A FMECA-type approach to Human Error Analysis. It uses a HTA (Hierarchical Task Analysis) followed by error identification and error reduction. The PSF (Performance Shaping Factors) used by the analyst are primarily man-machine interface related, e.g. workplace layout, information presentation, etc. Typically, an FMEA approach identifies many errors, primarily through detailed consideration of these PSF in the context of the system design, in relation to the capabilities and limitations of the operator, based on Ergonomics knowledge. Only those errors that are considered to be probable within the lifetime of the plant are considered further.		?	P3.2 P3.3 S3a.2			X		• [Kirwan98-1]	KS:R PM:C
209.	HERA I and HERA II (Human Error in ATM)	I	H	2000	Method of human error identification developed by Eurocontrol for the retrospective diagnosis during ATM system development. HERA places the air traffic incident in its ATM context by identifying the ATC behaviour,	HERA is TRACEr for European use.	ATM	S3a.2 S3c.1			X		• [Isaac&al99] • [Isaac&Pounds01] provides pros and cons compared to	PM:R KS:FC

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					the equipment used and the ATC function being performed.								HFACS • [Kirwan98-2] • [Shorrock01]	
210.	HFACS (Human Factors Analysis and Classification System)	I	H	1997 or older	Human factors taxonomy. HFACS examines instances of human error as part of a complex productive system that includes management and organisational vulnerabilities.	Originally developed for the US navy for investigation of military aviation incidents. Is currently being used by FAA to investigate civil aviation incidents.	navy aviation	S3a.1 S3a.2			X		• [Isaac&Pounds01] provides pro-s and con's compared to HERA	KS:R PM:C
211.	HHA (Health Hazard Assessment)	T	R	1988 or older	The method is used to identify health hazards and risks associated within any system, sub-system, operation, task or procedure. The method evaluates routine, planned, or unplanned use and releases of hazardous materials or physical agents.	The technique is applicable to all systems which transport, handle, transfer, use, or dispose of hazardous materials of physical agents.	chemical nuclear	P3.2 S3a.2 S3c.1	X			X	• [FAA00] • [FAA tools] • [ΣΣ93, ΣΣ97]	PM:R
212.	HITLINE (Human Interaction Timeline)	I	R	1994	Incorporates operator errors of commission in probabilistic assessments. It is based on a cognitive model for operators errors of omission and commission. The result of the methodology is similar to a human event tree, with as initiating event an error of commission. The generic events that determine the branch splittings are called performance influencing factors. The quantification part is performed using mapping tables.	Human reliability family Tool available	nuclear	P3.2 S3a.2			X		• [Macwan&Mosley94] • [MUFTIS3.2-I]	KS:FC PM:C
213.	HMEA (Hazard Mode Effects Analysis)	T	Dh	1997 or older	Method of establishing and comparing potential effects of hazards with applicable design criteria. Introductory technique.	Multi-use technique	aircraft	P3.2	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
214.	HOL (Higher Order Logic)	T	Ds	1993 or older	Formal Method. Refers to a particular logic notation and its machine support system. The logic notation is mostly taken from Church's Simple Theory of Types. Higher order logic proofs are sequences of function calls. HOL consists of 1) two theories, called 'min' and 'bool'; 2) eight primitive inference rules, and 3) three rules of definition.	Software requirements specification phase and design & development phase	computer	S3a.2		X			• [EN 50128] • [Melham&Norrish01] • [Rakowsky]	PM:C MC:R
215.	HPED (Human Performance Events Database)	D			Database of events related to human performance that can be used to identify safety significant events in which human performance was a major contributor to risk.		nuclear	F3.2 F4a.x P3.2 S3c.1			X		• [NUREG CR6753]	PM:R
216.	HPLV (Human Performance Limiting Values)	T	H	1990	HPLV represent a quantitative statement of the analyst's uncertainty as to whether all significant human error events have been adequately modelled in the fault tree. Special attention to (in)dependence of human errors.	Relation with Fault Trees. JHEDI applies HPLV to fault trees.	nuclear?	P3.2 P4a.x S3a.2 S4a.x			X		• [Kirwan94]	KS:F PM:C
217.	HPRA (Human Performance Reliability Analysis)	G			Consists of an analysis of the factors that determine how reliably a person will perform within a system or process. General analytical methods include probability compounding, simulation, stochastic methods, expert	Among published HPRA methods are THERP, REHMS-D, SLIM-MAUD, MAPPS	nuclear aerospace transport biomedical	P3.2 S3a.2			X		• [MIL-HDBK]	KS:F PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					judgement methods, and design synthesis methods.		defence							
218.	HRA (Human Reliability Analysis)	G			The purpose of the Human Reliability Analysis is to assess factors that may impact human reliability in the operation of the system.	The analysis is appropriate were reliable human performance is necessary for the success of the human-machine systems.	many	S3a.2 S3c.1			X		• [FAA00] • [NEA98] • [Petkov99] • [ΣΣ93, ΣΣ97]	KS:F PM:C
219.	HRAET (Human Reliability Analysis Event Tree)	T	H	1983	Tool used for THERP. Is a simpler form of event tree, usually with diagonal line representing success, and individual branches leading diagonally off the success diagonal representing failure at each point in the task step.	Human reliability family. Can also be used for maintenance errors.	nuclear	P3.2 S3a.2			X		• [Kirwan&Ainsworth 92] • [Kirwan&Kennedy& Hamblen] • [MUFTIS3.2-I]	KS:F PM:C
220.	HRMS (Human Reliability Management System)	T	H	1990	Psychologically-based tool. Attempts to bring generalised psychological theories or models into the rich context of a complex industrial work environment.	Apparently not in current use or else used rarely. JHEDI is a derivative of HRMS and provides a faster screening technique.	nuclear	S3a.2			X		• [Kirwan94] • [Kirwan98-1] • [Seignette02]	KS:R PM:R
221.	HSIA (Hardware/Software Interaction Analysis)	T	Dh	1991 or older	The objective of HSIA 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.	HSIA is obligatory on ESA (European Space Agency) programmes and is performed for all functions interfacing the spacecraft and / or other units.	computer	P1.3 P3.1 S3a.2	X	X			• [Hoegen97] • [Parker&al91] • [Rakowsky]	PM:R
222.	HSMP (Hybrid-State Markov Processes)	M			Combines deterministic stochastic evolution with switching of mode processes. The Hybrid Markov state consists of two components, an n-dimensional real-valued component, and a discrete valued component. The HSMP is represented as a solution of a stochastic differential or difference equation on a hybrid state space, driven by Brownian motion and point processes. The evolution of the probability density on the hybrid state space is the solution of a partial integro-differential equation.	Dynamic assessment family. Underlying modelling framework for TOPAZ. Numerical evaluation requires elaborated mathematical techniques.	ATM	P3.1 P3.2 S3a.1 S3a.2	X		X	X	• [Blom90] • [MUFTIS3.2-I]	PM:R
223.	HTA (Hierarchical Task Analysis)	T	H	1971	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.		ATC nuclear chemical	P3.1 S3a.2 S3c.1			X		• [Kirwan&Ainsworth 92] • [Kirwan94] • [Stanton&Wilson00]	KS:FC PM:R
224.	HTLA (Horizontal Timeline	T	H	1987 or	Investigates workload and crew co-ordination, focuses task sequencing and overall timing. Is constructed from the		nuclear offshore	P3.1 S3a.2			X	X	• [Kirwan&Kennedy& Hamblen]	KS:FC PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Analysis)			older	information in the VTLA to determine the likely time required to complete the task. Usually a graphical format is used, with sub-tasks on the y-axis and time proceeding on the x-axis. The HTLA shows firstly whether the tasks will be achieved in time, and also where certain tasks will be critical, and where bottlenecks can occur. It also highlights where tasks must occur in parallel, identifying crucial areas of co-ordination and teamwork.			S3c.1					• [Kirwan94] • [Task Time]	
225.	HTRR (Hazard Tracking and Risk Resolution)	T	R	2000 or older	Method of documenting and tracking hazards 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 safety hazards and risks. Each program must implement a Hazard Tracking System (HTS) to accomplish HTRR.	HTRR 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.	aviation	P3.2 S3a.2	X	X			• [FAA00] • [FAA tools]	PM:C
226.	Human (Error) HAZOP (Human (Error) Hazard and Operability study)	T	R	1988	Extension of the HAZOP technique to the field of procedures performed by humans. More comprehensive error identification, including the understanding of the causes of error, in order to achieve more robust error reduction.		chemical nuclear	F3.1 F3.2 F3.3 P3.2 P3.3 S3a.2			X	X	• [Cagno&Acron&Mancini01] • [Kirwan&Ainsworth92] • [Kirwan94]	MC:C KS:FC PM:C
227.	Human Error Data Collection	T	H		Aim is to collect data on human error, in order to support credibility and validation of human reliability analysis and quantification techniques.	An example of a Human Error Data Collection initiative is CORE-DATA.	nuclear	F3.1 F3.2 F3.3 P3.2 S3c.1			X		• [Kirwan&Basra&Taylor.doc]	
228.	Human error recovery	T	H	1997	Pilots typically introduce and correct errors prior to those errors becoming critical. The error correction frequency is decreasing under stress.		aviation	P3.2 S3a.1			X		• [Amalberti&Wioland97]	
229.	Human Factors Analysis	G			Human Factors Analysis represents an entire discipline that considers the human engineering aspects of design. There are many methods and techniques to formally and informally consider the human engineering interface of the system. There are specialty considerations such as ergonomics, bio-machines, anthropometrics. The Human Factors concept is the allocation of functions, tasks, and resources among humans and machines. The most effective application of the human factors perspective presupposes an active involvement in all phases of system development from design to training, operation and, ultimately, the most overlooked element, disposal. Its	Human Factors Analysis is appropriate for all situations were the human interfaces with the system and human-related hazards and risks are present. The human is considered a main sub-system.	many	P3.1 P3.2 S3a.2	X		X	X	• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	KS:FC PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					focus ranges from overall system considerations (including operational management) to the interaction of a single individual at the lowest operational level. However, it is most commonly applied and implemented, from a systems engineering perspective, to the system being designed and as part of the SHA.									
230.	Human Factors Case	T	H		A Human Factors Case is a framework for human factors integration, similar to a Safety Case for Safety Management. The 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.	New technique developed in HUM in Eurocontrol.	ATM	many			X		• [Eurocontrol strategy] • [HFC]	KS:F
231.	Hybrid Automata	M		1993	These combine discrete transition graphs with continuous dynamical systems. Hybrid Automata are mathematical models for digital systems that interact with analogue environments. Can be viewed as infinite-state transition systems.		nuclear chemical	P3.1 P3.2 S3a.2	X				• [Alur93] • [Lygeros&Pappas&Sastry98] • [Schuppen98] • [Sipser97] • [Tomlin&Lygeros&Sastry98] • [Weinberg&Lynch&Delisle96]	PM:R MC:R
232.	HzM (Multi-level HAZOP)	T	R	2001 or older	HzM maintains the HAZOP approach, but breaks down the analysis in two directions: vertical (hierarchical breakdown of each procedure in an ordered sequence of steps) and horizontal (each step is further broken down into the three logical levels operator, control system and plant/ process). This allows recording how deviations may emerge in different logical levels and establishing specific preventive/ protective measures for each.	Combined use with HEART, THERP and Event trees possible.	chemical	P3.1 P3.2 P3.3 S3a.2	X		X		• [Cagno&Acron&Mancini01]	PM:C
233.	IAEA TECDOC 727	I	R	1993	Aim is to classify and prioritise risks due to major industrial accidents. The method is the tool to identify and categorise various hazardous activities and hazardous substances. Includes hazard analysis and quantified risk assessment. The categorisation of the effect classes is by means of maximum distance of effect, and affected area.		chemical rail road	F3.2 F3.3 P3.2 S3c.1	X			X	• [Babibec&Bernatik&Pavelka99]	PM:C
234.	IDA (Influence Diagram Approach) or STAHR (Socio-Technical Assessment of Human Reliability)	T	H	1980	Determines human reliability by the combined influences of factors, which influences are in turn affected by other lower level influences. The effect of each identified influence is evaluated quantitatively, with the resulting values used to calculate human error probability estimates.	Human reliability family. Supporting tool commercially available. Developed in the field of decision analysis. IDA (1980) is now also known as STAHR (1985). IDA is not considered very accurate.	nuclear offshore	P3.2 S3a.2			X		• [Humphreys88] • [Kirwan&Ainsworth92] • [Kirwan94] • [MUFTIS3.2-I]	KS:R PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
235.	IDEF (Integrated Computer-Aided Manufacturing Definition)	I	Dh	1993	Method of system modelling that enables understanding of system functions and their relationships. Using the decomposition methods of structural analysis, the IDEF methodology defines a system in terms of its functions and its input, outputs, controls and mechanisms.	Currently, IDEF comprises a suite of methods named $IDEF_0$, $IDEF_1$, etc.	defence	F1.3 F3.1 P3.1	X				• [MIL-HDBK]	KS:FC PM:R
236.	IMAS (Influence Modelling and Assessment System)	T	H	1986	Aims to model cognitive behaviour aspects of performance, in terms of relationships between knowledge items relating to symptoms of events (for diagnostic reliability assessment)	Not currently in use	chemical	P3.1 P3.2 S3a.2			X		• [Kirwan98-1]	KS:R PM:R
237.	IMM (Interacting Multiple Model algorithm)	M		1988	Suboptimal hybrid filter that has been shown to be one of the most cost-effective hybrid state estimation schemes. The main feature of this algorithm is its ability to estimate the state of a dynamic system with several behaviour modes which can "switch" from one to another. In particular, the IMM estimator can be a self-adjusting variable-bandwidth filter, which makes it natural for tracking manoeuvring targets. It is the best compromise available currently between complexity and performance		ATM	P3.2 S3a.1	X		X	X	• [Blom&Bar-Shalom88] • [Mazor&al95]	PM:R
238.	Impact Analysis	G			Prior to modification or enhancement being performed on the software, an analysis is undertaken to identify the impact of the modification or enhancement on the software and also identify the affected software systems and modules.	Software maintenance phase	computer	S3a.2 S3c.2		X			• [EN 50128] • [Rakowsky]	PM:C
239.	Importance Sampling	M			Technique to enable more frequent generation of rare events in Monte Carlo Simulation. Rare events are sampled more often, and this is later compensated for.	Dynamic assessment family. Combine with simulations	many	P3.2 S3a.1 S3a.2	X		X	X	• [MUFTIS3.2-I]	PM:C
240.	Information Hiding, Information Encapsulation	T	Ds	1979 ?	Aim is to increase the reliability and maintainability of software. Encapsulation (also information hiding) consists of separating the external aspects of an object, which are accessible to other objects, from the internal implementation details of the object, which are hidden from other objects. If an internal state is encapsulated it cannot be accessed directly, and its representation is invisible from outside the object.	Highly recommended for all types of software system. Closely related to object-oriented programming and design. Tools available.	computer	S3a.2 S3c.2		X			• [Bishop90] • [EN 50128] • [McCraw-Hill02] • [Rakowsky]	PM:C MC:R
241.	Input-output (block) diagrams	G		1974	The technique involves first selecting the system, task or step of interest and then identifying all the inputs and outputs which are necessary to complete this task or step. The inputs are listed along an incoming arc to a block representing the system, task or step of interest, and the outputs are listed along an outgoing arc.		chemical?	F1.3 P1.3 P3.1 S1.3	X	X	X		• [Kirwan&Ainsworth 92]	KS:FC PM:R
242.	Inspections and Walkthroughs	G		1976 or older	Aim is to detect errors in some product of the development process as soon and as economically as possible. An inspection is the most formal type of group	Very effective method of finding errors that should be adopted throughout the software	computer	S3a.2	X	X			• [Bishop90] • [Inspections]	PM:C KS:FC

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					review. Roles (producer, moderator, reader and reviewer, and recorder) are well defined, and the inspection process is prescribed and systematic. During the meeting, participants use a checklist to review the product one portion at a time. Issues and defects are recorded, and a product disposition is determined. When the product needs rework, another inspection might be needed to verify the changes. In a walkthrough, the producer describes the product and asks for comments from the participants. These gatherings generally serve to inform participants about the product rather than correct it.	development process. Can be used with any method that produces something that can be inspected.								
243.	INTENT	T	H	1991	Is aimed at enabling the incorporation of decision-based errors into PSA, i.e. errors involving mistaken intentions, which appears to include cognitive errors and rule violations, as well as EOCs. Four categories of error of intention are identified: action consequence; crew response set; attitudes leading to circumvention; and resource dependencies. A set of 20 errors of intention (and associated PSF (Performance Shaping Factor)) are derived, and quantified using seven experts.		?	P3.1 P3.2			X		• [Kirwan98-1]	KS:R PM:C
244.	Interface Analysis, Interdependence Analysis	T	Dh	1995 or older	The analysis is used to identify hazards due to interface incompatibilities. The methodology entails seeking those physical and functional incompatibilities between adjacent, interconnected, or interacting elements of a system, which, if allowed to persist under all conditions of operation, would generate risks.	Interface Analysis is applicable to all systems. All interfaces should be investigated; machine-software, environment- human, environment-machine, human-human, machine-machine, etc.	space	P3.2 S3a.2	X	X		X	• [FAA00] • [Leveson95] • [Rakowsky] • [ΣΣ93, ΣΣ97]	PM:F
245.	Interface Surveys	G		1977	Interface surveys are a group of information collection methods that can be used to gather information about specific physical aspects of the person-machine interface at which tasks are carried out. Examples of these techniques are Control/Display Analysis; Labelling Surveys; Coding Consistency Surveys; Operator modifications surveys; Sightline surveys; Environmental Surveys		nuclear	P1.3 P3.1 S3a.2	X				• [Kirwan&Ainsworth 92]	KS:FC PM:R
246.	Interface testing	G			Interface testing is essentially focused testing. It needs reasonably precise knowledge of the interface specification. It has three aspects: 1) Usability testing (to discover problems that users have); 2) Correctness testing (to test whether the product does what it is supposed to do); 3) Portability testing (to make a program run across platforms).	Software design & development phase	computer	S3a.2		X			• [EN 50128] • [Jones&Bloomfield &Froome&Bishop01] • [Rakowsky] • [Rowe99]	PM:C
247.	INTEROPS (INTEgrated Reactor OPerator System)	I	H	1991	Cognitive performance simulation, which uses the SAINT simulation methodology. Has three independent models: a nuclear power plant model; a network model of operator	The INTEROPS model allows the following to be simulated: forgetting, tunnel-vision;	nuclear	P3.1 P3.2 S3a.2			X		• [Kirwan98-1]	KS:R PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					tasks; and a knowledge base, the operator model being distributed between the latter two. The model is a single operator model. It diagnoses by observance of plant parameters, and subsequent hypothesis generation and testing of the hypothesis. The approach uses Markovian modelling to allow opportunistic monitoring of plant parameters. The model also simulates various errors and PSF (Performance Shaping Factor). Cognitive workload is also modelled, in terms of the contemporary information processing theory of concurrent task management. Also, INTEROPS can utilise a confusion matrix approach to make diagnostic choices.	confirmation bias; and mistakes.								
248.	Invariant Assertions	T	Ds	1967 or older	Aim is to detect whether a computer system has deviated from its intended function. An invariant assertion of an automaton A is defined as any property that is true in every single reachable state of A. Invariants are typically proved by induction on the number of steps in an execution leading to the state in question. While proving an inductive step, we consider only critical actions, which affect the state variables appearing in the invariant.	To be used on non-time critical safety related systems. Related to formal specification methods and fault containment techniques.	computer	S3a.2 S3c.1		X			• [Bishop90] • [Keidar&Khazan00]	PM:R MC:R
249.	IPME (Integrated Performance Modelling Environment)	I	H	2000 ?	IPME is a Unix-based integrated environment of simulation and modelling tools for answering questions about systems that rely on human performance to succeed. IPME provides: 1) A realistic representation of humans in complex environments; 2) Interoperability with other models and external simulations; 3) Enhanced usability through a user friendly graphical user interface. IPME provides i) a full-featured discrete event simulation environment built on the Micro Saint modelling software; ii) added functionality to enhance the modelling of the human component of the system; iii) a number of features that make it easier to integrate IPME models with other simulations on a real-time basis including TCP/IP sockets and, in the near future, tools for developing simulations that adhere to the Higher Level Architecture (HLA) simulation protocols that are becoming standard throughout the world.	Relation with Micro-SAINT	navy defence	P3.1 P3.2 S3a.2			X		• [IPME web]	PM:R
250.	ISRS (International Safety Rating System)	T	H	1988	Safety culture audit tool that uses performance indicators, which are organised into groups. The scores on the sub-sets of safety performance areas are weighted and then translated into an overall index rating.	Qualitative	many	S3c.1				X	• [Kennedy&Kirwan98]	KS:FC PM:C
251.	JAR 25	I	Dh	1994 or	Joint Aviation Requirements for large airplanes. Includes safety assessment methodology for large airplanes that	JAR-25 is used as basis for many other safety assessment	aircraft	many	X				• [JAR 25.1309] • [Klompstra&Everdij	PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
				older	runs in parallel with the large aeroplane lifecycle stages.	methodologies, e.g. ARP 4761, SAM							97]	
252.	Jelinski-Moranda models	T	Ds	1990 or older	This is a model that tends to estimate the number of remaining errors in a software product, which is considered a measure for the minimum time to correct these bugs	Not considered very reliable, but can be used for general opinion and for comparison of software modules	computer	S3a.2		X			• [Bishop90]	PM:R
253.	JHEDI (Justification of Human Error Data Information)	I	H	1990	JHEDI is derived from the Human Reliability Management System (HRMS) and is a quick form of human reliability analysis that requires little training to apply. The tool consists of a scenario description, task analysis, human error identification, a quantification process, and performance shaping factors and assumptions. JHEDI is a moderate, flexible and auditable tool for use in human reliability analysis. Some expert knowledge of the system under scrutiny is required.		nuclear	P1.3 P3.1 P3.2 S3a.2			X		• [HIFA_human] • [Kirwan94] • [Kirwan98-1] • [PROMAI5]	KS:R PM:R
254.	Job Safety Analysis	T	M	1960 about	This technique is used to assess the various ways a task may be performed so that the most efficient and appropriate way to do a task is selected. Each job is broken down into tasks, or steps, and hazards associated with each task or step are identified. Controls are then defined to decrease the risk associated with the particular hazards.	Job Safety Analysis can be applied to evaluate any job, task, human function, or operation.	construction	F3.2 F3.3 P3.1 P3.2 P3.3 S3a.2 S3c.1			X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	KS:F PM:C
255.	JSD (Jackson System Development)	I	Ds	1983	JSD is a system development method for developing information systems with a strong time dimension from requirements through code. JSD simulates events dynamically as they occur in the real world. Systems developed using JSD are always real-time systems. JSD is an object-based system of development, where the behaviour of objects is captured in an entity structure diagram. It consists of three main phases: the modelling phase; the network phase; and the implementation phase. JSD uses two types of diagrams to model a system, these are Entity Structure Diagrams and Network Diagrams. When used to describe the actions of a system or of an entity, JSD Diagrams can provide a modelling viewpoint that has elements of both functional and behavioural viewpoints. JSD diagrams provide an abstract form of sequencing description, for example much more abstract than pseudocode.	Developed by Michael A. Jackson and John Cameron. Should be considered for real-time systems where concurrency can be allowed and where great formality is not called for. Similarities with MASCOT. Tools available. Software requirements specification phase and design & development phase	computer	S3a.2			X			• [Bishop90] • [EN 50128] • [Jackson] • [Rakowsky]	PM:C MC:R
256.	KTT (Kinetic Tree Theory)	T	R	1970	Mathematical technique used to quantify top effect of fault trees, allowing for evaluation of instantaneous reliability or availability. Complete information is obtained from the existence probability, the failure rate, and the failure	Static assessment family. Used for fault trees.	see FTA	P3.2 S3a.2	X				• [MUFTIS3.2-I] • [Vesely70]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					intensity of any failure (top, mode or primary) in a fault tree. When these three characteristics are determined, subsequent probabilistic information, both pointwise and cumulative, is obtained for all time for this failure. The application of the addition and multiplication laws of probability are used to evaluate the system unavailability from the minimal cut sets of the system.									
257.	Laser Safety Analysis	T	Dh	1980 or older	This analysis enables the evaluation of the use of Lasers from a safety view. The purpose is to provide a means to assess the hazards of non-ionising radiation. As such, its intent is to also to identify associated hazards and the types of controls available and required for laser hazards.	The analysis is appropriate for any laser operation, i.e. construction, experimentation, and testing.	medical defence	None	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R MC:R
258.	Library of Trusted, Verified Modules and Components	D			Well designed and structured PESs are made up of a number of hardware and software components and modules which are clearly distinct and which interact with each other in clearly defined ways. Aim is to avoid the need for software modules and hardware component designs to be extensively revalidated or redesigned for each new application. Also to advantage designs which have not been formally or rigorously validated but for which considerable operational history is available.	Software design & development phase	computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:R
259.	Link Analysis (1)	T	H	1959	Is used to identify relationships between an individual and some part of the system. A link between two parts of the system will occur when a person shifts his focus of attention, or physically moves, between two parts of the system.	Typical applications include equipment layout for offices and control rooms, and the layout of display and control systems.	nuclear	P3.1	X		X		• [Kirwan&Ainsworth 92] • [Kirwan94]	KS:FC PM:R
260.	Link Analysis (2)	M			This is a collection of mathematical algorithms and visualisation techniques aimed at the identification and convenient visualisation of links between objects and their values.	Tools available. Can be used in conjunction with Timeline Analysis to help determine travel times, etc	defence	P3.1	X				• [Megaputer Web] • [MIL-HDBK]	KS:C PM:R
261.	Littlewood	M		1957	Mathematical model that tends to provide the current failure rate of a program, and hence minimum time required to reach a certain reliability.	Not considered very reliable, but can be used for general opinion and for comparison of software modules	computer	S3a.2		X			• [Bishop90]	PM:R
262.	Littlewood-Verrall	M		1957	A Bayesian approach to software reliability measurement. Software reliability is viewed as a measure of strength of belief that a program will operate successfully. This contrasts with the classical view of reliability as the outcome of an experiment to determine the number of times a program would operate successfully out of say 100 executions. Almost all published models assume that failures occur randomly during the operation of the program. However, while most postulate simply that the	Not considered very reliable, but can be used for general opinion and for comparison of software modules	computer	S3a.2		X			• [Bishop90] • [Narkhede02]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					value of the hazard rate is a function of the number of faults remaining, Littlewood and Verrall modelled it as a random variable. One of the parameters of the distribution of this random variable is assumed to vary with the number of failures experienced. The value of the parameters of each functional form that produce the best fit for that form are determined. Then the functional forms are compared (at the optimum values of the parameters) and the best fitting form is selected.									
263.	LOTOS (Language for Temporal Ordering Specification)	I	Ds	1987	Formal Method. A means for describing and reasoning about the behaviour of systems of concurrent, communicating processes. Is based on CCS with additional features from related algebras CSP and Circuit Analysis (CIRCAL).	Software requirements specification phase and design & development phase	computer	S3a.2 S3a.2		X			• [EN 50128] • [Rakowsky]	MC:R PM:R
264.	MANAGER (MANagement Assessment Guidelines in the Evaluation of Risk)	I	H	1990	Safety management assessment audit tool linked to Quantitative Risk Assessment-type of approach. The tool consists of approximately 114 questions, divided into 12 areas such as Written procedures, Safety policy, Formal safety studies, Organisational factors, etc. MANAGER was the first technique to consider linking up ratings on its audit questions with PSA results.		nuclear	S3a.1 S3c.1				X	• [Kennedy&Kirwan98] • [Kirwan94]	KS:R PM:F
265.	MAPPS (Maintenance Personnel Performance Simulations)	I	H	1984	Computer-based, stochastic, task-oriented model of human performance. It is a tool for analysing maintenance activities in nuclear power plants, including the influence from environmental, motivational, task and organisational variables. Its function is to simulate a number of human 'components' to the system, e.g. the maintenance mechanic, the instrument and control technician together with any interactions (communications, instructions) between these people and the control-room operator.		nuclear	S3c.2			X	X	• [Kirwan94] • [MIL-HDBK] • [THEMES01]	KS:R PM:R
266.	Markov Chains or Markov Modelling	M		1910 about	Other name for SSG where the transitions to the next stage only depend on the present state. Only for this type of SSG, quantification is possible. Can be used to evaluate the reliability or safety or availability of a system	Named after Russian mathematician A.A. Markov (1856-1922). Recommended for dependability evaluation of redundant hardware. A standard method in these cases. Combines with FMEA, FTA, CCD. Tools available	many	P3.1 P3.2 S3a.2	X	X			• [Bishop90] • [EN 50128] • [FT handbook02] • [MUFTIS3.2-I] • [NASA-GB-1740.13-96] • [Rakowsky] • [Sparkman92] • [Storey96]	PM:F
267.	MASCOT (Modular Approach to Software Construction, Operation and Test)	I	Ds	1970 s	A method for software design aimed at real-time embedded systems from the Royal Signals and Research Establishment, UK. It is not a full method in the current sense of design methodology. It has a notation and a clear	MASCOT originated within the UK defence industry in the 1970s. The MASCOT III standard was published in its final form in	defence computer	S3a.2		X			• [Bishop90] • [EN 50128] • [MASCOT] • [Rakowsky]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					mapping between the design and physical components. Also, it lacks a distinct process. Its success has been partly because it is available: There has been a shortage of real-time design methods, while MASCOT is sufficiently effective to be worthwhile. MASCOT III copes better with large systems than did earlier versions, through better support for the use of sub-systems. Some users feel that basic structure of system is harder to follow than with previous versions.	1987. Should be considered for real-time systems where concurrency has to and can be used. Related to JSD. Tools available. Software requirements specification phase and design & development phase								
268.	Materials Compatibility Analysis	T	Dh	1988 or older	Materials Compatibility Analysis provides an assessment of materials utilised within a particular design. Any potential degradation that can occur due to material incompatibility is evaluated. System Safety is concerned with any physical degradation due to material incompatibility that can result in contributory hazards or failures that can cause mishaps to occur. Material compatibility is critical to the safe operation of a system and personnel safety. The result of a material misapplication can be catastrophic.	Materials Compatibility Analysis in universally appropriate throughout most systems. Proper material compatibility analysis requires knowledge of the type, concentration and temperature of fluid(s) being handled and the valve body and seal material.	chemical	P3.2	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
269.	Maximum Credible Accident/ Worst Case	T	R	1972 or older	The technique is to determine the upper bounds on a potential environment without regard to the probability of occurrence of the particular potential accident.	Similar to Scenario Analysis, this technique is used to conduct a System Hazard Analysis. The technique is universally appropriate.	aircraft	F3.3 P3.2 S3a.1 S3a.2	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
270.	Measurement of Complexity	G			As a goal, software complexity should be minimised to reduce likelihood of errors. Complex software also is more likely to be unstable, or suffer from unpredictable behaviour. Modularity is a useful technique to reduce complexity. Complexity can be measured via McCabe's metrics and similar techniques.		computer	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	KS:FC PM:C
271.	MEDA (Maintenance Error Decision Aid)	I	H	1996 or older	MEDA is a widely used attempt to systematise evaluation of events, problems and potential problems by using a repeatable, structured evaluation program. MEDA is a structured investigation process used to determine the factors that contribute to errors committed by maintenance technicians and inspectors. MEDA is also used to help develop corrective actions to avoid or reduce the likelihood of similar errors. Most of these corrective actions will be directed towards the airline maintenance system, not the individual technical or inspector. The MEDA process involves five basic steps: Event, Decision, Investigation, Prevention Strategies, and Feedback.	MEDA was developed by Boeing as part of the Boeing Safety Management System (BSMS). The company has been encouraging its customers to employ the technique.	aviation	P3.1 S3a.1 S3a.2			X	X	• [Bongard01] • [Escobar01] • [HIFA_human] • [MEDA]	KS:FC PM:R
272.	Memorizing Executed	T	Ds	1987	Aim is to force the software to fail-safe if it executes an	Little performance data available.	computer	S3a.2		X			• [Bishop90]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Cases			or older	unlicensed path. During licensing, a record is made of all relevant details of each program execution. During normal operation each program execution is compared with the set of licensed executions. If it differs a safety action is taken.	Related to testing and fail-safe design. Software architecture phase							• [EN 50128] • [Rakowsky]	
273.	MERMOS (Méthode d'Evaluation de la Réalisations des Missions Opérateur pour la Sureté)	I	H	1998	Probabilistic Human Reliability Analysis technique that aims more closely to integrate the human and organisational factors.	Developed by Electricité de France, since early 1998.	electr nuclear	P3.1 P3.2			X		• [HRA Washington] • [Jeffcott&Johnson] • [Straeter&al99] • [THEMES01]	KS:R PM:C
274.	Metrics	G			These models evaluate some structural properties of the software and relate this to a desired attribute such as reliability or complexity. Software tools are required to evaluate most of the measures.	Software verification and testing phase	computer	S3a.2 S4b.x		X			• [EN 50128] • [Rakowsky]	PM:C
275.	MHD (Mechanical Handling Diagram)	T	R	1998 or older	Mechanical HAZOP		chemical	F3.1 F3.2 F3.3 P3.2 P3.3 S3a.2	X				• [Kennedy&Kirwan98]	PM:R
276.	MIDAS (Man-Machine Integrated Design and Analysis System)	I	H	1986	MIDAS is an integrated suite of software components to aid analysts in applying human factors principles and human performance models to the design of complex human systems; in particular, the conceptual phase of rotorcraft crewstation development and identification of crew training requirements. MIDAS focuses on visualisation, contains different models of workload and situation awareness within its structure and contains an augmented programming language called the Operator Procedure Language (OPL) incorporated into its programming code.	Developed by Jim Hartzell, Barry Smith and Kevin Corker in 1986, although the original software has been changed since. MIDAS is currently still being used and augmented by the HAIL in a collaborative effort with NASA ARC through a parallel development effort termed Air-MIDAS.	rotorcraft	P3.1 P3.2 P3.3 P3.4			X	X	• [DND_SECO_MIDAS] • [HAIL]	KS:F PM:R
277.	Mission Analysis	G		1986 or older	Is used to define what tasks the total system (hardware, software, and lifeware) must perform. The mission or operational requirements are a composite of requirements starting at a general level and progressing to a specific level.	Two methods, Mission Profile, and Mission Scenarios are especially recommended for mission analysis.	defence	F1.3 F3.1 P3.1	X	X	X		• [MIL-HDBK]	PM:F
278.	Mission Profile	G		1986 or older	Component of Mission Analysis. Provides a graphic, 2D representation of a mission segment		defence	F1.3 F3.1 P3.1	X	X	X		• [MIL-HDBK]	
279.	Mission Scenarios	G		1986 or older	Component of Mission Analysis. Describes each distinct event occurring during projected mission		defence	F1.3 F3.1 P3.1	X	X	X		• [MIL-HDBK]	
280.	MLD (Master Logic Diagrams)	T	R		Deductive approach similar to fault tree. Four levels: first level is the top event, second level are formed by loss of		space	P3.1 P3.2	X				• [Statematelatos]	MC:F PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					functions leading to this top event, third level are the system failures leading to the loss of functions. Fourth level are the initiators			S3a.2						
281.	MMAC (Multiple Model Adaptive Control)	M		1977	Uses FDD (Fault Detection and Diagnosis scheme). Each fault hypothesis corresponds to one model (e.g. a Kalman filter) and one control mode. The control mode that corresponds to the model with the highest likelihood is selected by multi-hypothesis testing.	Computationally very extensive since not only each component must be hypothesised but the type and the magnitude must be modelled as well.	aviation medicine	P3.2 S3a.2	X				• [Schram&Verbrugge n98]	PM:R
282.	MMFC (Multiple Model Fuzzy Control)	M		1998	Combines advantages of Gain Scheduling and MMAC. Like in MMAC, for the most important fault types, a control model is derived beforehand. However, in contrast to the MMAC approach, through the use of the fuzzy measures that indicate exactly the fault states, a gradual interpolation between the control modes is achieved. A smooth transition from the nominal control model to a fault mode is automatically achieved like in the gain-scheduling approach. However, through the use of multiple models, different control structures can still be formulated.		aviation medicine	P3.2 S3a.2	X				• [Schram&Verbrugge n98]	PM:R
283.	MMSA (Man-Machine System Analysis)	T	H	1983	The MMSA sets up to 10 steps: 1) Definition: analysis if different types of human actions; 2) Screening: identify the different types of human interactions that are significant to the operation and safety of the plant; 3) Qualitative analysis: detailed description of the important human interactions and definition of the key influences; 4) Representation: modelling of human interactions in logic structures; 5) Impact integration: exploration of the impact of significant human actions; 6) Quantification: assignment of probabilities of interactions; 7) Documentation: making the analysis traceable, understandable and reproducible. Other steps are excluded since they are relevant for the design process but not for the Human reliability analysis process.	The MMSA steps can be arranged as a subset of the SHARP process.	nuclear	S3a.2	X		X		• [Straeter01]	PM:R
284.	Modelling / Simulation	G			There are many forms of modelling techniques that are used in system engineering. Failures, events, flows, functions, energy forms, random variables, hardware configuration, accident sequences, operational tasks, all can be modelled.	Modelling is appropriate for any system or system safety analysis.	all	P3.2 P4a.x S3a.1 S3a.2	X		X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
285.	MoFL (Modell der Fluglotsenleistungen (Model of air traffic controller performance))	I	H	1997	The implementation of the model MoFl is based on a production system in the programming language ACT-R (Adaptive Control of Thought - Rational). ACT-R includes a broad and detailed theoretical framework of human cognition. The basic assumption is that cognitive		ATC	P3.2 S3a.1			X		• [Leuchter&al97] • [Niessen&Eyferth01] • [Niessen&Leuchter& Eyferth98]	

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					skills are composed of production rules. A production rule is a modular piece of knowledge. Combining these rules into a sequence represents complex cognitive processes. For the most part, ACT-R is suitable for modelling the cognitive performance of en-route air traffic controllers. But, modelling in ACT-R is limited for some relevant aspects of dynamic situations.									
286.	MONACOS	I	H	1999	MONACOS is a method of retrospective analysis of actual accidents and incidents. Based on MERMOS.		nuclear	S3c.1			X		• [HRA Washington]	PM:R
287.	Monte Carlo Simulation	M		1777	A pattern of system responses to an initiating event is built up by repeated sampling. State transition times are generated by direct modelling of the behaviours of system components (including operators) and their interactions.	Dynamic assessment family. Method has been used for centuries. The name stems from WW II.	ATM, many other	P3.1 P3.2 S3a.1 S3a.2 S3c.1	X	X	X	X	• [EN 50128] • [MUFTIS3.2-I] • [Rakowsky] • [Sparkman92]	PM:F
288.	MORT (Management Oversight and Risk Tree Analysis)	I	R	1975 – 1980	MORT technique is used to systematically analyse an accident in order to examine and determine detailed information about the process and accident contributors. To manage risks in an organisation, using a systemic approach, in order to increase reliability, assess risks, control losses and allocate resources effectively. Is standard fault tree augmented by an analysis of managerial functions, human behaviour, and environmental factors.	This is an accident investigation technique that can be applied to analyse any accident. Useful in project planning, functional specification of a target (sub)system, accident/ incident analysis and safety programme evaluation. Tools available.	nuclear energy	S3c.1	X		X	X	• [Bishop90] • [FAA00] • [Kirwan&Ainsworth 92] • [Kirwan94] • [Leveson95] • [MAS611-2] • [ΣΣ93, ΣΣ97]	KS:FC PM:R
289.	MSC (Message Sequence Chart)	T	Ds		Message Sequence Chart (MSC) is a graphical way of describing asynchronous communication between processes. A chart does not describe the total system behaviour, but is rather a single execution trace. For this reason an extension to MSCs, called High Level MSCs has also been proposed; HLMSCs allow for the combination of traces into a hierarchical model. MSCs have been used extensively in telecommunication systems design and in particular with the formal Specification and Description Language (SDL). They are used at various stages of system development including requirement and interface specification, simulation, validation, test case specification and documentation. HLMSCs have greatly increased the descriptive capabilities of MSCs as they allow for modular specifications.	Message Sequence Chart (MSC) specifications have found their way into many software engineering methodologies and CASE tools, in particular in the area of telecommunications and concurrent real-time systems. MSC Specifications often represent early life-cycle requirements and high-level design specifications.	telecom	P3.2 S3a.2		X			• [MSC]	
290.	Multiple Agent Based Modelling	G		2001	Way of modelling where agents are identified as entities which have situational awareness. After the identification of the agents of the operation, the modelling process zooms in, and models the agents in more detail, after which the interconnections between agents are modelled.	The agents can be modelled with techniques such as Dynamically Coloured Petri Nets	ATM	P3.2 S3a.1 S3a.2	X		X	X	• [Corker??] • [Stroeve&al01]	

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
291.	Multiple Greek Letters method	T	R	1991 or older	Is used to quantify common cause effects identified by Zonal Analysis. It involves the possible influences of one component on the other components of the same common cause group. Slight generalisation of Beta-factor method when the number of components involved is greater than two.	Static assessment family	?	P3.2	X				• [Charpentier00] • [MUFTIS3.2-I]	PM:R
292.	Multiple Resources	T	H	1992	The Multiple Resources Theory proposed by Wickens offers predictions of patterns of interference between competing tasks during periods of time-sharing. The theory has made the global assumption that interference is minimised when different resources are demanded. This assumption has been empirically validated in experiments over the past five years. According to Wickens, there are 4 dimensions to resources: (1) Stages – Perceptual/central processing vs. response selection/execution (2) Input modalities - Auditory vs. visual (3) Processing codes - Spatial vs. verbal (4) Responses - Vocal vs. manual		ATM	P3.2 S3a.1			X		• [Wickens92]	
293.	Murphy Diagrams	T	H	1981	Psychologically-based tool. Attempts to bring generalised psychological theories or models into the rich context of a complex industrial work environment. Method starts from a description of an accident (or significant error sequence) and then an attempt is made to identify all the individual sources of error which occurred, using a standard set of eight Murphy diagrams (event-tree-like diagrams) to describe these errors. These Murphy diagrams define, at a general level, all the likely errors associated with decision processes.	Apparently not in current use or else used rarely. Name is based on the axiom of Murphy's law, which states that 'if anything can go wrong, it will'.	electr	P3.1 S3a.2			X		• [Kirwan&Ainsworth 92] • [Kirwan94] • [Kirwan98-1]	KS:R PM:R
294.	Musa models	M			This is a mathematical model that tends to estimate the number of remaining errors in a software product, as a measure for the minimum time to correct these bugs	Not considered very reliable, but can be used for general opinion and for comparison of software modules	computer	S3a.2		X			• [Bishop90]	PM:R
295.	N out of M vote	T	Dh	1981 ?	Voting is a fundamental operation when distributed systems involve replicated components (e.g. after Diverse Programming). It involves a voter who chooses between several replicated options, and sends his choice back to the user. Aim of N out of M vote is to reduce the frequency and duration of system failure. To allow continued operation during test and repair. For example, 2 out of 3 voting scheme means that if one of three components fails, the other two will keep the system operational.	Essential for systems where any break in service has serious consequences. 'N out of M' is usually denoted by 'NooM', e.g. as in 1oo2 or 2oo3.	computer	P3.3 S3c.1		X			• [Bishop90]	PM:F
296.	N out of M vote,	T	Dh	1971	Aim is to avoid that, in voting systems, fault masking	Very valuable technique. Most	computer	S3a.2		X			• [Bishop90]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Adaptive voting			?	ability deteriorates as more copies fail (i.e. faulty modules outvote the good modules)	useful in high availability systems where servicing is difficult or impossible								
297.	Naked man	T	R	1963 or older	This technique is to evaluate a system by looking at the bare system (controls) needed for operation without any external features added in order to determine the need/value of control to decrease risk.	The technique is universally appropriate.	?	P3.2 P3.3	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
298.	NDI (Non-Destructive Inspection technique)	G		1914 - 1918 war	Generic term rather than a specific technique. NDI can be defined as inspection using methods that in no way affect the subsequent use or serviceability of the material, structure or component being inspected. An NDI method explores a particular physical property of a material or component in an effort to detect changes in that property which may indicate the presence of some fault. Visual inspection is the most commonly used NDI technique.	NDI is very commonly referred to as Non-destructive Testing (NDT) which is historically the original term used - this is the more commonly used term in the manufacturing environment where the testing of the suitability of materials to be used is often undertaken non-destructively. The "non-destructive" description was adopted to differentiate it from the various "destructive" mechanical tests already in use. The term Non-destructive Evaluation (NDE) is also used, most particularly in the sphere of R & D work in the laboratory.	many	S3a.2	X				• [Hollamby97] • [Wassell92]	PM:R
299.	NE-HEART (Nuclear Electric Human Error Assessment and Reduction Technique)	T	H	1999 or older	Extended HEART approach, which adds several new generic error probabilities specific to Nuclear Power Plant tasks and systems.		nuclear electr	P3.2 S3a.2			X		• [Kirwan&Kennedy& Hamblen]	KS:R PM:R
300.	Network Logic Analysis	T	Dh	1972 or older	Network Logic Analysis is a method to examine a system in terms of a Boolean mathematical representation in order to gain insight into a system that might not ordinarily be achieved.	The technique is universally appropriate to complex systems that can be represented in bi-model elemental form.	?	P3.1 S3a.2	X	X			• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
301.	Neural networks	M		1958 - 1985 about	Information-processing paradigm inspired by the way the densely interconnected, parallel structure of the mammalian brain processes information. Neural networks are collections of mathematical models that emulate some of the observed properties of biological nervous systems and draw on the analogies of adaptive biological learning. The key element of the paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements that are analogous to neurones and are tied together with weighted connections that are analogous to synapses.	In [May97], neural networks are used to model human operator performance in computer models of complex man-machine systems	aviation and many other	S3a.2	X		X		• [May97]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
302.	NLR Air Safety Database	D		1998	This database consists of accident data from a large number of sources including, for instance, official international reporting systems (e.g. ICAO ADREP), Accident Investigation Agencies, and insurance companies. These sources provide data for virtually all reported ATM related accidents. The database also contains exposure data (e.g. number of flights) and arrival and departure data of commercial aircraft at airports worldwide.		ATM	F3.1 F3.2 F3.3 P3.2 S3c.1	X	X	X	X	• [VanEs01]	
303.	NOMAC (Nuclear Organisation and Management Analysis Concept)	I	H	1994	NOMAC is an analysis framework that assesses the safety culture health of the organisation by looking for the presence or absence of indicators of safety performance.	Qualitative	nuclear	S3c.1				X	• [Kennedy&Kirwan98]	KS:R PM:R
304.	NOTECHX	T	H		New technique on assessing non-technical skills		?	P3.2 S3a.1			X		• Safety Techniques Workshop	
305.	NSCCA (Nuclear Safety Cross-Check Analysis)	T	Ds	1976	The NSCCA provides a technique that verifies and validates software designs associated with nuclear systems. The NSCCA is also a reliability hazard assessment method that is traceable to requirements-based testing.	At present applies to military nuclear weapon systems.	nuclear defence	None	X	X			• [FAA AC431] • [Rakowsky] • [ΣΣ93, ΣΣ97]	PM:R
306.	Nuclear Criticality Analysis	T	M	1987 or older	Aim is to ensure nuclear safety by eliminating possibility of a nuclear reaction	All facilities that handle fissile material	nuclear	None	X			X	• [ΣΣ93, ΣΣ97]	PM:R
307.	Nuclear Explosives Process Hazard Analysis	T	R	1997 or older	Aim is to identify high consequence (nuclear) activities to reduce possibility of nuclear explosive accident	Nuclear or similar high risk activities	nuclear	None	X			X	• [ΣΣ93, ΣΣ97]	PM:R
308.	Nuclear Safety Analysis	T	M	1980 or older	The purpose is to establish requirements for contractors responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities or equipment to develop safety analyses that establish and evaluate the adequacy of the safety bases of the facility/equipment. The Department of Energy (DOE) requires that the safety bases analysed include management, design, construction, operation, and engineering characteristics necessary to protect the public, workers, and the environment from the safety and health hazards posed by the nuclear facility or non-facility nuclear operations. The Nuclear Safety Analysis Report (NSAR) documents the results of the analysis.	All nuclear facilities and operations. DOE and NRC have rigid requirements	nuclear	None	X			X	• [FAA AC431] • [ΣΣ93, ΣΣ97]	PM:R
309.	O&SHA (Operating and Support Hazard Analysis)	T	R	1982 or older	The analysis is performed to identify and evaluate hazards/risks associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system. This analysis identifies and	The analysis is appropriate for all operational and support efforts. Goes beyond a JSA.	aviation	S3a.2 S3c.1 S3c.2	X	X	X	X	• [FAA AC431] • [FAA00] • [FAA tools] • [ΣΣ93, ΣΣ97]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					evaluates: a) Activities which occur under hazardous conditions, their time periods, and the actions required to minimise risk during these activities/time periods; b) Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or S&TE to eliminate hazards or reduce associated risk; c) Requirements for safety devices and equipment, including personnel safety and life support and rescue equipment; d) Warnings, cautions, and special emergency procedures; e) Requirements for PHS&T and the maintenance and disposal of hazardous materials; f) Requirements for safety training and personnel certification.									
310.	OATS (Operator Action Trees)	T	H	1982	Deals with operator errors during accident or abnormal conditions and is designed to provide error types and associated probabilities. The method employs a logic tree, the basic operator action tree, that identifies the possible postaccident operator failure modes. Three error types are identified: 1) failure to perceive that event has occurred; 2) failure to diagnose the nature of event and to identify necessary remedies; 3) failure to implement those responses correctly and in timely manner. Next, these errors are quantified using time-reliability curves.	Human reliability family	nuclear	P3.2 S3a.2			X		• [Kirwan&Ainsworth 92] • [MUFTIS3.2-I]	KS:R PM:C
311.	OBJ	T	Ds	1985 about	OBJ (not an acronym) is an algebraic Specification Language to provide a precise system specification with user feed-back and system validation prior to implementation	Powerful yet natural formal specification language for both large- and small-scale systems developments. Tools available. Software requirements specification phase and design & development phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C MC:R
312.	ObjectGEODE	I	Ds	2001 or older	ObjectGeode is a toolset dedicated to analysis, design, verification and validation through simulation, code generation and testing of real-time and distributed applications. It supports a coherent integration of complementary object-oriented and real-time approaches based on the UML, SDL and MSC standards languages. ObjectGeode provides graphical editors, a powerful simulator, a C code generator targeting popular real-time OS and network protocols, and a design-level debugger. Complete traceability is ensured from Requirement to code.	Real-time and distributed applications. Such applications are used in many fields such as telecommunications, aerospace, defence, automotive, process control or medical systems.	telecom aerospace, defence, automotive, process control, medical systems	P3.1 P3.2 S3a.2		X			• [Telelogic Objectgeode]	PM:R MC:F C
313.	Object-oriented Design and Programming	G		1966 or older	Aim is to reduce the development and maintenance costs and enhance reliability, through the production of more maintainable and re-usable software	Recommended as one possible option for the design of safety-related systems. Also	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						recommended for construction of prototypes. Related to JSD and OBJ. Tools available. Software design & development phase.								
314.	Observational Techniques	G		1990	General class of techniques whose objective is to obtain data by directly observing the activity or behaviour under study. Examples of these techniques are direct visual observation, remote observation via closed-circuit television or video recording, participant observation, time-lapse photography		telecom	S3c.1			X		• [Kirwan&Ainsworth 92]	PM:R
315.	Occupational Health Hazard Analysis	T	R	1999 or older	Is carried out to identify health hazards and to recommend measures to be included in the system, such as provision of ventilation, barriers, protective clothing, etc., to reduce the associated risk to a tolerable level. Is carried out by means of audit and checklists.		defence	P3.2 P3.3 P3.4 S3a.2	X			X	• [DS-00-56]	PM:R
316.	Ofan	T	H	1996 or older	Modelling framework describing human interaction with systems that have modes. The Ofan modelling framework is based on the Statecharts and Operator-Function models. In Ofan, five concurrently active modules are used to describe the human-machine environment, namely the Environment, the Human Functions/Tasks, the Controls, the Machine, and the Displays. Applying the Ofan framework allows the identification of potential mismatches between what the user assumes the application will do and what the application actually does. The Ofan framework attempts to separate out the components of the whole environment.		road	P3.1 P3.2 S3a.2	X		X		• [Andre&Degani96] • [Smith&al98]	PM:C
317.	OFM (Operation Function Model)	T	H	1987	Describes task-analytic structure of operator behaviour in complex systems. The OFM is focused on the interaction between an operator and automation in a highly proceduralised environment, such as aviation. The OFM is a structured approach to specify the operator tasks and procedures in a task analysis framework made up of modes and transitions. Using graphical notation, OFM attempts to graph the high level goals into simpler behaviours to allow the supervision of the automation.	The power of OFM is based upon several important observations: the event-driven nature of automation, the proceduralised nature of high risk tasks, and the fact that many of the transitions and decisions made during system operation are discrete in nature.	aviation	P3.1 S3a.2			X		• [Botting&Johnson98] • [Vakil00]	PM:C
318.	OHA (Operating Hazard Analysis)	T	R	1983 or older	Focuses on hazards resulting from tasks, activities, or operating systems functions that occur as the system is stored, transported, or exercised. Iterative process	Is applied early in system development cycle.	transport	F3.2	X		X		• [DOT-FTA00] • [Moriarty83]	PM:C
319.	OMOLA	T	Dh	1989	Object-oriented language tool for modelling combined discrete events and continuous time dynamical systems. OmSim is an environment for modelling and simulation		thermal-power-plant	P3.1 P3.2 S3a.2	X				• [Andersson93] • [OmolaWeb]	PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					based on OMOLA.									
320.	Operator Task Analysis	T	H	1988 or older	Operator Task Analysis is a method to evaluate a task performed by one or more personnel from a safety standpoint in order to identify undetected hazards, develop note / cautions / warnings for integration in order into procedures, and receive feedback from operating personnel. Also known as Procedure Analysis, which is a step-by-step analysis of specific procedures to identify hazards or risks associated with procedures.	Any process or system that has a logical start/stop point or intermediate segments, which lend themselves to analysis. This methodology is universally appropriate to any operation, which there is a human input, is performed. Other name for Procedure Analysis and often referred to as Task Analysis.	many	P3.2 P3.3 S3a.2 S3c.1			X	X	• [FAA00] • [Leveson95] • [ΣΣ93, ΣΣ97]	PM:F KS:F
321.	OPL (Operator Procedure Language)	I	M		Augmented programming language used in MIDAS. This computational human performance modelling tool possesses structures that represent human cognition and the agent's operational work environment and includes a comprehensive visualisation component to its output.		aviation	P3.2 S3a.2			X		• [HAIL] • [Sherry&al00] • [Sherry&al01]	
322.	Organisational learning	G			Organisational learning is the process of "detection and correction of errors." Organisations learn through individuals acting as agents for them: The individuals' learning activities, in turn, are facilitated or inhibited by an ecological system of factors that may be called an organisational learning system	Four constructs are integrally linked to organisational learning: knowledge acquisition, information distribution, information interpretation, and organisational memory.	many	S3a.2 S3c.1				X	• Huge reference list on OL: [Polat96]	KS:F PM:R
323.	ORR (Operational Readiness Review)	T	R	1997 or older	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.	DOE requirement. Systematic approach to any complex facility. The details of the ORR will be dependent on the application.	nuclear	S3b.x	X	X		X	• [DOE-3006] • [Dryden-ORR] • [ΣΣ93, ΣΣ97]	KS:F PM:R
324.	OSD (Operational Sequence Diagram)	T	H	1961	An operational sequence is any sequence of control movements and/or information collecting activities, which are executed in order to accomplish a task. Such sequences can be represented graphically in a variety of ways, known collectively as operational sequence diagrams. Examples are the Basic OSD, the Temporal OSD, the Partitioned	Is called probably the most powerful single manual analysis method that the Human Error practitioner can use. Is particularly useful for the analysis of highly complex systems	defence	P3.1 P3.2 S3a.1 S3a.2			X		• [Kirwan&Ainsworth 92] • [MIL-HDBK]	KS:FC PM:F

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					OSD, the Spatial OSD, Job Process Charts.	requiring many time critical information-decision-action functions between several operators and equipment items.								
325.	OSTI (Operant Supervisory Taxonomy Index)	T	H	1986	Analysis framework that assesses the safety culture health of the organisation by looking for the presence or absence of indicators of safety performance.	Qualitative	?	S3c.1				X	• [Kennedy&Kirwan98]	KS:R PM:R
326.	Particular Risk Analysis	T	R	1994 probably older	Common cause analysis related technique. Defined as those events or influences outside the system itself. For example, fire, leaking fluids, 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	Is the second activity in a Common Cause Analysis; Zonal Analysis being the first and Common Mode Analysis being the third.	chemical	F3.2 F3.3 P3.2 S3a.1	X				• [Dvorak00]	
327.	Partitioning	T	Ds		Technique for providing isolation between functionally independent software components to contain and/or isolate faults and potentially reduce the effort of the software verification process. If protection by partitioning is provided, the software level for each partitioned component may be determined using the most severe failure condition category associated with that component.		computer aviation	S3a.2		X			• [DO178B] • [Skutt01]	
328.	Parts Count method	T	Dh	1981	Crude way of approximating the reliability of a system by counting active parts. Inductive approach. Very pessimistic since it assumes that every subsystem failure can lead to total system failure.	Static assessment family	nuclear	S3a.2 S3c.1	X				• [FT handbook02] • [MUFTIS3.2-I] • [OORM00]	PM:R
329.	PC (Paired Comparisons)	T	H	1966	Estimates human error probabilities by asking experts which pair of error descriptions is more probable. Result is 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.	Human reliability family. Does not restrict to human error only. Can be used together with APJ	transport nuclear	P3.2 S3a.2	X		X		• [Humphreys88] • [Kirwan94] • [MUFTIS3.2-I]	KS:FC PM:C
330.	PEAT (Procedural Event Analysis Tool)	I	M	1999	PEAT is a structured, cognitively based analytic tool designed to help airline safety officers investigate and analyse serious incidents involving flight-crew procedural deviations. The objective is to help airlines develop effective remedial measures to prevent the occurrence of future similar errors. The PEAT process relies on a non-punitive approach to identify key contributing factors to crew decisions. Using this process, the airline safety officer would be able to provide recommendations aimed at controlling the effect of contributing factors. PEAT	Boeing made PEAT available to the airline industry in 1999	aviation	P3.2 P3.3 S3c.1			X	X	• [HIFA_human]	KS:R PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					includes database storage, analysis, and reporting capabilities.									
331.	Performance Modelling	G		1961 or older	Aim is to ensure that the working capacity of the system is sufficient to meet the specified requirements. The requirements specification includes throughput and response requirements for specific functions, perhaps combined with constraints on the use of total system resources. The proposed system design is compared against the stated requirements by 1) defining a model of the system processes, and their interactions; 2) identifying the use of resources by each process; 3) Identifying the distribution of demands placed upon the system under average and worst-case conditions; 4) computing the mean and worst-case throughput and response times for the individual system functions.	Extremely valuable provided modelling limitations are recognised. Tools available.	computer	P4a.x S3a.1 S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:F
332.	Performance Requirements Analysis	T	Ds	1995 or older	Aim is to establish that the performance requirements of a software system have been satisfied. An analysis is performed of both the system and the software requirements specifications to identify all general and specific explicit and implicit performance requirements. Each of these performance requirements is examined in turn to determine: 1) the success criteria to be obtained; 2) whether a measure against the success criteria can be obtained; 3) the potential accuracy of such measurements; 4) the project stages at which the measurements can be estimated; 5) the project stages at which measurements can be made. The practicability if each performance requirement is then analysed in order to obtain a list of performance requirements, success criteria and potential measurements.		computer	S3a.2	X	X			• [EN 50128] • [Rakowsky]	PM:C
333.	PERT (Program Evaluation Review technique)	T	M	1950	A PERT shows all the tasks, a network that logically connects the tasks, time estimates for each task and the time critical part.	Developed by US navy in 1950s	navy and many more	P3.1 P3.2 S3c.1				X	• Internet	PM:R
334.	Petri Net Analysis	M		1962	Petri Net Analysis is a method to model unique states of a complex system. Aim is to model relevant aspects of the system behaviour and to assess and possibly improve safety and operational requirements through analysis and re-design. Petri Nets can be used to model system components, or sub- systems at a wide range of abstraction levels; e.g., conceptual, top – down, detail design, or actual implementations of hardware, software, or combinations. Ordinary Petri Nets are a special case of SSG. Many	The technique is universally appropriate to complex systems. Potentially very valuable for small systems or small parts of larger systems. CSP and CCS are alternative methods. Also Temporal logic can be used in combination. Plenty of tools available, also free.	all do-mains (manuf, rail computer ATC)	P3.1 P3.2 S3a.1 S3a.2	X	X	X		• [Bishop90] • [EN 50128] • [FAA AC431] • [FAA00] • [Kirwan&Ainsworth 92] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97]	KS:F MC:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					extensions exist through which almost any system, including human cognitive mode models, can be treated.									
335.	Petri Net extensions	M		1962 from	Modelling and evaluation tool. Can be used for modelling almost everything, depending on the type of Petri Net extension used. There exist at least two extensions used for ATM applications: GSPN (Generalised Stochastic Petri Nets, which was used to model an ATC technical support system), and DCPN (Dynamically Coloured Petri Nets, which is being used to model aircraft behaviour through time, influenced by nominal and non-nominal human behaviour, technical system behaviour, weather, etc.) In addition, SPN (Synchronised Petri Network) has been used for modelling Human Operator tasks	Plenty of tools available, also free.	all	P3.1 P3.2 S3a.1 S3a.2 S3c.1	X	X	X	X	• Huge amount of literature available, see for an overview e.g. [PetriNets World] • [Abed&Angue94] • [Everdij&Blom&Klompstra97]	PM:C MC:R
336.	PHA (Preliminary Hazard Analysis)	T	R	1972 about	Identification of unwanted consequences for people as result of disfunctioning of system. Aim is to determine during system concept or early development the hazards that could be present in the operational system in order to establish courses of action. Sometimes it consists of PHI and HAZOP and/or FMEA. The PHA is an extension of a Preliminary Hazard List. As the design matures, the PHA evolves into a system of sub-system hazard analysis.	Hazard identification family. The technique is universally appropriate. Should be considered for specification of systems which are not similar to those already in operation and from which much experience has been gained. Design and development phase. Use with FTA, FMEA, HAZOP. Initial effort in hazard analysis during system design phase. Emphasis on the hazard and its effects. Inductive and deductive	aircraft rail	F3.2 F3.3 P3.2 P3.3	X	X			• [Bishop90] • [FAA AC431] • [FAA00] • [FAA tools] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97]	PM:C
337.	PHASER (Probabilistic Hybrid Analytical System Evaluation Routine)	T	R	1997 or older	Software tool that has the capability of incorporating subjective expert judgement into probabilistic safety analysis (PSA) along with conventional data inputs. The basic concepts involve scale factors and confidence factors that are associated with the stochastic variability and subjective uncertainty (which are common adjuncts used in PSA), and the safety risk extremes that are crucial to safety assessment. These are all utilised to illustrate methodology for incorporating dependence among analysis variables in generating PSA results, and for importance and Sensitivity measures associated with the results that help point out where any major sources of safety concern arise and where any major sources of uncertainty reside, respectively.	Describes the potential for failure and helps in weighing cost/ benefit analysis. Applies to modelling where inputs lack precise definition or have dependence.	?	F3.1	X				• [Cooper96] • [ΣΣ93, ΣΣ97]	PM:R
338.	PHEA	T	M	1993	Simplified version of the earlier SHERPA. Comprises an	Equivalent to Human HAZOP.	chemical	F3.1			X		• [Kirwan98-1]	KS:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Predictive Human Error Analysis technique)				error checklist. Focuses on particular task types depending on the industry concerned. Steps are: 1) Identify task steps where errors may result in accidents; 2) Specify the nature of the error; 3) Identify possible recovery; 4) Recommend preventative measures. Errors of several types are analysed: Planning Errors, Action Errors, Checking Errors, Retrieval Errors, Information Communication Errors, Selection Errors.			F3.2 F3.3 F4a.x P3.1 P3.2 P3.3 S3a.2							PM:C
339.	PHECA (Potential Human Error Causes Analysis)	T	H	1988	Psychologically-based tool. Attempts to bring generalised psychological theories or models into the rich context of a complex industrial work environment. It is a computerised system based on the identification of error causes, which interact with performance shaping factors. It has a wider application than just error identification (e.g. potential error reduction strategies). Like HAZOP it uses guidewords to identify hazards.	Apparently not in current use or else used rarely	?	P3.1 P3.2 S3a.2			X		• [Kirwan98-1] • [PROMAI5]	KS:R PM:R
340.	PHI (Preliminary Hazard Identification)	T	R	1991 or older	Reduced version of PHA, only containing a column with hazards. The results are recorded in the Preliminary Hazard List (PHL). Is sometimes considered a generic term rather than a specific technique.	Hazard identification family. Performed in the early stages of lifecycle.	aircraft	F3.2	X				• [MUFTIS3.2-I] • [Storey96]	PM:C
341.	PHL (Preliminary Hazard List)	T	R	1989 or older	Is an initial analysis effort within system safety. Lists of initial hazards or potential accidents are identified during concept development. The PHL may also identify hazards that require special safety design emphasis or hazardous areas where in-depth safety analyses are needed as well as the scope of those analyses. At a minimum, the PHL should identify: The Hazard; When identified (phase of system life cycle); How identified (analysis, malfunction, failure) and by whom; Severity and Probability of Occurrence; Probable/ actual cause(s); Proposed elimination/mitigation techniques; Status (Open-action pending /Closed-eliminated/Mitigated; Process of elimination/mitigation; Oversight/approval authority.	The technique is universally appropriate. Usually the results are fed into a PHA.	aircraft	F3.2	X	X			• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
342.	PHRA (Probabilistic Human Reliability Analysis)	T	H	1990	Update of HCR (Human COgnitive Reliability), in which advantages of HCR have been used and disadvantages have been tried to eliminate. Time-related method. A distinction is made between routine operation and operation after the event. Error probabilities are calculated for identified classes of routine operation with the help of simple evaluation instructions. Simulator experiments can be performed to evaluate the reliability of human actions after trouble has materialised. Various time-reliability		electr	P3.2 S3a.2			X		• [Straeter00] • [Straeter01]	PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					curves for varying the complex trouble situations are determined from the experiments. Error probabilities are determined from the time-reliability curves.									
343.	Piecewise Deterministic Markov Process (PDP)	M		1984	A PDP is a process on a hybrid state space, i.e. a combination of discrete and continuous. The continuous state process flows according to an ordinary differential equation. At certain moments in time it jumps to another value. The time of jump is determined either by a Poisson point process, or when the continuous state hits the boundary of an area.		ATM	P3.2 S3a.2	X		X	X	• [Davis84]	
344.	Plant walkdowns/ surveys	T	R		Site-based systematic surveys, developed for rapid identification of hazards, effects and controls		chemical	S3a.2	X			X	• [EQE Web]	PM:R
345.	PMA (Phased Mission Analysis)	T	R	1984	Mathematical technique used to quantify top effect of fault trees, accounting for different phases of a task, and allowing repairable components under certain conditions	Static assessment family	?	P3.2 S3a.2	X				• [MUFTIS3.2-I]	PM:C
346.	PRA (Probabilistic Risk Assessment based on FTA/ETA) or PSA (Probabilistic Safety Assessment)	I	R	1965	Quantified analysis of low probability, high severity events. Evaluates the risks involved in the operation of a safety critical system. The risk assessment forms the basis of design decisions. It is a systematic, logical, comprehensive discipline that uses tools like FMEA, FTA, Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), Master Logic Diagrams (MLD), Reliability Block Diagrams (RBD), etc. to quantify risk.	Static assessment family. Initially nuclear power industry, now any system with catastrophic accident potential. Recommended before major design decisions. Not reasonable for the minor system aspects.	nuclear chemical defence aerospace	P3.2	X				• [Bishop90] • [FAA00] • [Kirwan94] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97] • [Statematelatos]	KS:FC PM:R C
347.	PRASM (Predictive Risk Assessment and Safety Management)	I	M	2000	Methodology for incorporating human and organisational factors in the risk evaluation and safety management in industrial systems. The methodology includes the cost-benefit analysis of the risk control measures and options to enable elaborating a rational risk control strategy for implementing more effective safety related undertakings in different time horizons.		nuclear?	P4a.x S4a.x			X	X	• [Kosmowski00]	PM:R
348.	PREDICT (PRocedure to Review and Evaluate Dependency In Complex Technologies)	T	R	1992	Is targeted at the relatively unpredictable or bizarre event sequences that characterise events, in that such events are incredible or not predictable until accidents give us 20:20 hindsight. The method utilises a group to identify errors, and is thus HAZOP-based, with keyword systems, followed by three categories of assumption-testing keywords. The technique essentially allows the analyst to test the assumptions underpinning the design and safety cases for plants. The method allows inserting a keyword randomly to enable the analyst to consider more 'lateral' possible causal connections.		?	P3.2	X		X		• [Kirwan98-1]	KS:R PM:C
349.	PRIMA (Process RIsk	T	R	1996	Safety management assessment linked to Quantitative Risk Assessment-type of approach. The PRIMA		aviation	S3c.1				X	• [Kennedy&Kirwan98]	KS:FC PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Management Audit)				modelling approach provides insight into the management factors influencing the accident risk, but does not permit this insight to be translated into a detailed quantitative influence.								• [Roelen&al00]	
350.	PRISM (Professional Rating of Implemented Safety Management)	T	H	1993	Safety culture audit tool uses performance indicators that are organised into groups. The scores on the sub-sets of safety performance areas are weighted and then translated into an overall index rating.	Qualitative	?	S3c.1				X	• [Kennedy&Kirwan98]	KS:FC PM:R
351.	PRMA (Procedure Response Matrix Approach)	T	R	1994	Aim is to identify errors of commission, which are more closely linked to cognitive errors (global and local misdiagnoses), and slip-based EOCs during emergencies. PRMA to some extent represents a more sophisticated and detailed investigation than the FSMA, though one that is more resource-intensive. The approach has several major stages: develop a PRM for all initiating events that produce significantly different plant responses; for each PRM review the decision points in the procedural pathway; identify potential incorrect decisions resulting from misinterpretation or failure of the plant to provide the appropriate information, or due to a procedural omission (lapse).	Related to SHERPA and SCHEMA and TEACHER-SIERRA. The approach has strong affinities with FSMA, which has faults on one axis of its matrix and symptoms on the other one. The technique is useful for considering how system status indications and procedures will affect performance in abnormal or emergency events, such as a nuclear power plant emergency scenario requiring diagnosis and recovery actions using emergency procedures. As such, it can be used to evaluate alarm system design adequacy, for example.	nuclear	P3.2	X		X		• [Kirwan98-1]	KS:FC PM:C
352.	Probabilistic Hazard Analysis	G			Combination of FMECA, ETA and FTA. Goes beyond the qualitative hazard analysis techniques by providing probability information using the event trees and fault trees.		computer	F3.2 F3.3 P3.2 S3a.2	X				• [Storey96]	PM:C
353.	Probabilistic testing	T	Ds	1995 or older	Probabilistic considerations are based either on a probabilistic test or on operating experience. Usually the number of test cases or observed operating cases is very large. Usually, automatic aids are taken which concern the details of test data provision and test output supervision.	Software verification and testing phase and validation phase	computer	S3a.2 S4b.x		X			• [EN 50128] • [Jones&Bloomfield&Froome&Bishop01] • [Rakowsky]	PM:R
354.	Process charts	T	R	1921	These are top-down flow diagrams of the task in which each behavioural element is classified and then represented by a particular symbol (five possible symbols exist).		?	F3.1 P3.1 S3a.2			X		• [Kirwan&Ainsworth92]	PM:R
355.	Process Hazard Analysis	G	M	1989 or older	It is a means of identifying and analysing the significance of potential hazards associated with the processing or handling of certain highly hazardous chemicals.	Requirement of 29 CFR 1910.119 for chemical process industry	chemical	None	X				• [FAA AC431] • [ΣΣ93, ΣΣ97]	PM:R
356.	Process simulation	G			Aim is to test the function of a software system, together with its interface to the outside world, without allowing it	Hard to accumulate sufficient tests to get high degree of confidence in	rail	S3a.1 S3a.2	X	X			• [EN 50128] • [Rakowsky]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					to modify the real world in any way. The simulation may be software only or a combination of software and hardware. This is essentially testing in a simulated operational situation. Provides a realistic operational profile, can be valuable for continuously operating systems (e.g. process control).	reliability.								
357.	PROCRU (Procedure-oriented Crew Model)	T	H	1980	Control-theoretic model that permits systematic investigation of questions concerning the impact of procedural and system design changes on the performance and safety of commercial aircraft operations in the approach-to-landing phase of a flight. It is a closed-loop system model incorporating submodels for the aircraft, the approach and landing aids provided by ATC, three crew members, and an air traffic controller.	Human reliability family	ATM	P3.1 P3.2	X		X	X	• [CBSSE90, p30] • [MUFTIS3.2-I]	KS:R PM:C
358.	Production System Hazard Analysis	T	R	1985 or older	Production System Hazard Analysis is used to identify hazards that may be introduced during the production phase of system development which could impair safety and to identify their means of control. The interface between the product and the production process is examined	The technique is appropriate during development and production of complex systems and complex subsystems.	aircraft	S3a.1 S3a.2	X				• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
359.	Program Proving	G		1969 or older	Aim is to check whether software fulfils its intended function.	Should be used for the key software components of a safety critical system. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
360.	Protected airspace models	T	R	1996 or older	Analytical models. The number of conflicts can be estimated, based on simple quantities. Primary motive: Workload/safety		ATM	P3.2 S3a.1			X	X	• [MUFTIS1.2]	PM:C
361.	Prototype Development or Prototyping	G		1982 or older	Aim is to check the feasibility of implementing the system against the given constraints. To communicate the specifiers interpretation of the system to the customer, in order to locate misunderstandings. Prototype Development provides a Modelling / Simulation analysis the constructed early pre-production products so that the developer may inspect and test an early version.	This technique is appropriate during the early phases of pre-production and test. Valuable if the system requirements are uncertain or the requirements need strict validation. Related to performance simulation. Tools available.	many	P3.2 S3a.2	X	X			• [Bishop90] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
362.	Prototyping or Animation	G			Sometimes referred to as other name for Simulation. A subset of system functions, constraints and performance requirements are selected. A prototype is built using high level tools. The prototype is evaluated against the customers criteria and the system requirements may be modified in the light of this evaluation.		many	P3.2 P3.3	X	X			• [EN 50128] • [Rakowsky]	PM:R
363.	PTS (Predetermined Time Standards)	T	H	1986 or older	PTSs are internationally recognised time standards used for work measurement. They are employed to estimate performance times for tasks that can be decomposed into		defence	S3a.2 S3c.1			X		• [MIL-HDBK]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					smaller units for which execution times can be determined or estimated. The time necessary to accomplish these fundamental motions should be constants.									
364.	PUMA (Performance and Usability Modelling in ATM)	I	H	1995 about	PUMA is a toolset designed to enable the prediction and description of controller workload for ATC scenarios. It is capable of assessing the effect on controller workload of various computer assistance tools. PUMA uses observational task analysis to try to capture all the relevant information about cognitive activities in a task, usually based on video analysis of someone (i.e. an ATCO) performing the task. Each task or activity is then classified by a PUMA analyst and its impact on workload calculated as a function of its usage of cognitive resources, and as a function of other activities' (competing) resource requirements. Some tasks or activities will conflict more with each other as they are demanding the same cognitive resources, as defined in a 'conflict matrix' within PUMA. Central to the PUMA methodology is a workload prediction algorithm, which calculates how different task types will impact on workload alone, and together. This algorithm is based on the Wickens (1992) multiple resource theory. The output is a prediction of MWL as it changes throughout the overall task.	The PUMA Toolset was developed for NATS by Roke Manor Research Limited. PUMA has been applied to a number of future operational concepts, providing useful information in terms of their likely workload impacts, and potential improvements in the designs of future tools for the ATCO. The motivation for using PUMA stems from the fact that real time simulation is resource intensive, requiring a lot of manpower to plan, prepare for, conduct, analyse and report each trial. It is therefore highly useful to apply the PUMA 'coarse filter' to new operational concepts before expensive real time simulation. This allows the more promising and the less promising options to be identified, before proceeding with the better options, to full simulation.	ATC	P3.2 S3a.1 S3a.2			X		• [Kirwan&al97]	
365.	QCT (Quantified Causal Tree)	T	R	1996 or older	Bayesian method to determine probability of top event from the probabilities of the basic events of a causal tree.		aviation	P3.2 S3a.2	X				• [Loeve&Moek&Arsenis96]	PM:C
366.	Quality Assurance	G		1984 or older	Aim is to ensure that pre-determined quality control activities are carried out throughout development	Should be considered mandatory for safety related systems. Tools available	computer	S3a.1 S3a.2	X	X			• [Bishop90]	PM:R
367.	Questionnaires	G		1975 or older	Questionnaires are sets of predetermined questions arranged on a form and typically answered in a fixed sequence		many	F3.1 F3.2 F3.3 P3.2 P3.3 S3c.1			X	X	• [Kirwan&Ainsworth92]	PM:R KS:FC
368.	Radiological Hazard Safety Analysis	T	R	1997 or	Structured approach to characterisation and categorisation of radiological hazards.	Broadly applicable to all facilities engaged in managing radioactive	nuclear chemical	None	X				• [ΣΣ93, ΣΣ97]	KS:R PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
				older		materials								
369.	RAIT (Railway Accident Investigation Tool)	I	H	2000 probably older	Tool developed to investigate accidents by identifying contributions to and aggregate Railway Problem Factors, i.e. representative of significant organisational and managerial root causes of railway infrastructure accidents. RAIT starts with the accident outcome and then traces back to the active and latent failures that originated higher up within the organisation.	Developed for use at British rail. Also used as basis for training courses.	rail	None	X		X	X	• [PROMAI5] • [RAIT slides]	KS:R PM:R
370.	Rapid Risk Ranking	T	R		Rapid qualitative judgements of the expected frequency and consequences of the identified hazards, enables trivial hazards to be screened out, such that the subsequent quantitative work focuses on the significant hazards only		chemical	F3.3 P3.2	X				• [EQE Web]	PM:F
371.	RBD (Reliability Block Diagrams) or SDM (Success Diagram Method)	T	R	1972 about	Technique related to FTA where one is looking for a success path instead of failure path. Aim is to model, in a diagrammatical form, the set of events that must take place and conditions which must be fulfilled for a successful operation of a system or task	Useful for the analysis of systems with relatively straightforward logic, but inferior to fault tree analysis for more complex systems. In some references referred to as Dependence Diagrams (DD). RBD is also sometimes referred to as equivalent to a Fault Tree without repeated events. Tools available, but tools for FTA may also be useful.	aircraft	P3.2 S3a.2	X				• [Bishop90] • [EN 50128] • [FT handbook02] • [MUFTIS3.2-I] • [Sparkman92]	PM:F
372.	RCM (Reliability Centered Maintenance)	T	Dh	1990	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. It optimises preventive maintenance programmes in three phases: 1) ranking the components and evaluation of failure mode criticality; 2) identification of degradation mechanisms at work; 3) for each critical failure, determine most efficient reliability-based and cost-based maintenance task.		aviation ATM electr defence manuf nuclear	S3c.2	X		X		• [Cotaina&al00] • [Moubray00]	PM:C
373.	Real-time Yourdon	I	Ds	1985	Complete software development method consisting of	Worth considering for real-time	computer	S3a.2		X			• [Bishop90]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					specification and design techniques oriented towards the development of real-time systems. The development scheme underlying the technique assumes a three phase evolution of a system being developed: 1) building an 'essential model' that describes the behaviour required by the system; 2) building an implementation model which describes the structures and mechanisms that, when implemented, embody the required behaviour; 3) actually building the system in hardware and software.	systems without a level of criticality that demands more formal approaches. Related to SADT. Tools available. Software requirements specification phase and design & development phase							• [EN 50128] • [Rakowsky]	MC:R
374.	Recovery blocks or Recovery Block Programming	T	Ds	1975 ?	Aim is to increase the likelihood of the program performing its intended function. A number of routines are written (in isolation) using different approaches. In addition, an Acceptance Test is provided and the first routine to satisfy the acceptance test is selected.	Effective in situations without strict temporal constraints. Software architecture phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky] • [Sparkman92] • [SSCS]	PM:C
375.	RECUPARARE	T	R	2000	Model based on systematic analysis of events including Human Reliability in Nuclear Plants	Developed by IPSN for operating experience feedback analysis	nuclear	S3c.1			X		• [Straeter01]	PM:R
376.	Redundancy for Fault Detection	T	Dh	1980 ?	By employing redundancy, checks may be made for differences between units to determine sub-system failures	Should always be used in safety computer applications	computer	P3.2	X				• [Bishop90]	PM:C
377.	Refined Reich collision risk model	T	R	1993	Refinement of Reich collision risk model (CRM) to evaluate risk of collision between aircraft. Replaces the two restrictive Reich assumptions by one less restrictive one.		ATM	P3.2 S3a.1				X	• [Bakker&Blom93] • [Mizumachi&Ohmura77] • [MUFTIS3.2-II]	PM:C
378.	REHMS-D (Reliable Human Machine System Developer)	I	M	1999 about	REHMS-D uses a six-stage system engineering process, a cognitive model of the human, and operational sequence diagrams to assist the designer in developing human-machine interfaces subject to top-level reliability or yield requirements. Through its system engineering process, REHMS-D guides the designer through the understanding of customer requirements, the definition of the system, the allocation of human functions, the basic design of human functions, the assignment of job aids, and the design of tests to verify that the human functions meet the allocated reliability requirements. REHMS-D can be used for both the synthesis of new systems and the analysis of existing systems.	REHMS-D is called a major advance in system and reliability engineering that has broad application to systems and processes. It can be used to synthesise or analyse radar and sonar systems, control rooms and control systems, communications systems, geographic information systems, manufacturing processes, maintenance processes, biomedical systems, transportation systems, and other systems and processes that involve human-computer interfaces. Commercially available.	defence manuf transport	P3.1 P3.2 S3a.2	X				• [MIL-HDBK] • [REHMS-D]	PM:C
379.	Relative Ranking	T	Dh	1992 or older	Rank hazardous attributes (risk) of process. Hazards can be ranked based on e.g. frequency of occurrence or on severity of consequences, etc. The ranking may lead to prioritisation of mitigating measures.	Any system wherein a ranking approach exists or can be constructed	nuclear	F3.3 P3.2	X				• [ΣΣ93, ΣΣ97]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
380.	Reliability Growth Models	T	Ds	1972	Aim is to predict the current software failure rate and hence the operational reliability. After a software component has been modified or developed, it enters a testing phase for a specified time. Failures will occur during this period, and software reliability can be calculated from various measures such as number of failures and execution time to failure. Software reliability is then plotted over time to determine any trends. The software is modified to correct the failures and is tested again until the desired reliability objective is achieved.	Some problems during application. Tools available.	computer	S3a.2		X			• [Bishop90] • [Sparkman92]	PM:R
381.	Repetitive Failure Analysis	T	R	1991 or older	Aim is to model recurring events that prevent the system from performing its function. It provides a systematic approach to address, evaluate and correct repetitive failures.	Currently used in nuclear industry. Potential for transfer to other fields.	nuclear, other	P3.2 S3a.2 S3c.1	X				• [ΣΣ93, ΣΣ97]	PM:R
382.	Requirements Criticality Analysis	T	Ds	1996 or older	Criticality analysis identifies program requirements that have safety implications. A method of applying criticality analysis is to analyse the hazards of the software/ hardware system and identify those that could present catastrophic or critical hazards. This approach evaluates each program requirements in terms of the safety objectives derived for the software component.		aviation	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96]	PM:C
383.	Re-try Fault Recovery	T	M	1990 or older	Aim is to attempt functional recovery from a detected fault condition by re-try mechanisms, i.e. re-executing the same code or by re-booting. There are three general categories of methods used to recover to a previous state: (1) checkpointing, (2) audit trails, and (3) recovery cache.	Should be used with care and always with full consideration of the effect on time-critical events, and the effect of lost data during re-boot. Combine with software time-out checks or watchdog timers. Software architecture phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky] • [Sparkman92]	PM:R
384.	Return to Manual Operation	T	M	1990 or older	Aim is to provide the operator or supervisor the information and the means to perform the function of the failed automatic control system.	Useful provided it is used with care	computer	S3a.2	X				• [Bishop90]	PM:R
385.	RIAN	T	Dh	1991 or older	PC-based prototype software package for risk assessment. Can take as input data the quantified basic events from CLASS and the consequence trees from the FTA tool		?	P3.2	X				• [Parker&al91]	PM:R
386.	RIF diagram (Risk Influencing Factor Diagram)	T	R	2000 or older	Alternative to fault trees and event trees. Systematic approach to identify and evaluate risk reduction strategies for a given activity or system.		space	P3.2	X		X		• [Vinnem00]	PM:R
387.	Risk classification schemes	T	R		These are matrices that relate the severity of risk or hazard to its maximum tolerated probability.	These exist for different domains and different types of systems, see the references for a collection.	many	F3.4	X				• [Storey96]	PM:R
388.	Risk decomposition	T	R	1996	Since the probability of an accident usually is extremely small, and cannot be evaluated e.g. by straightforward fast-		ATM	P3.2 S3a.2	X		X	X	• [Blom&al98,01]	

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					time simulation of a model that describes the behaviour of aircraft through time, accident risk is decomposed into terms and factors that each can be evaluated through mathematics and/or simulation.									
389.	Risk-Based Decision Analysis	T	M	1993 or older	Risk-Based Decision Analysis is an efficient approach to making rational and defensible decisions in complex situations. It can be regarded as a generic term, or as an integrated approach, covering decision analysis tools, such as decision trees, influence diagrams, Monte Carlo analysis, Bayesian update analysis, and simulation modeling. The concepts involved in decision analysis are particularly significant in regard to activities where information relative to a specific state of an activity may be insufficient and/or inadequate.	The technique is universally appropriate to complex systems.	nuclear health many other	P3.2 S3a.2	X				• [ARES-RBDA] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
390.	RMA (Rate Monotonic Analysis)	T	Ds	1980 s	Is a useful analysis technique for software. It ensures that time critical activities will be properly verified. RMA is a collection of quantitative methods and algorithms that allows engineers to specify, understand, analyse, and predict the timing behaviour of real-time software systems, thus improving their dependability and evolvability. RMA can be used by real-time system designers, testers, maintainers, and troubleshooters, as it provides 1) mechanisms for predicting real-time performance; 2) structuring guidelines to help ensure performance predictability; 3) insight for uncovering subtle performance problems in real-time systems. This body of theory and methods is also referred to as generalised rate monotonic scheduling (GRMS).		computer aircraft	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky] • [RMA web]	PM:C
391.	Root Cause Analysis	T	R	1981 or older	This method identifies causal factors to accident or near-miss incidents. The technique goes beyond the direct causes to identify fundamental reasons for the fault or failure; it asks why things happen, instead of treating the symptoms. It is a systematic process of gathering and ordering all relevant data about counter-quality within an organisation; then identifying the internal causes that have generated or allowed the problem; then analysing for decision-makers the comparative benefits and cost-effectiveness of all available prevention options. To accomplish this, the analysis methodology provides visibility of all causes, an understanding of the nature of the causal systems they form, a way to measure and compare the causal systems, an understanding of the principles that govern those causal systems, and a	Any accident or incident should be formally investigated to determine the contributors of the unplanned event. The root cause is underlying contributing causes for observed deficiencies that should be documented in the findings of an investigation. Several training courses, tools and supporting packages are (commercially) available.	aviation health other	P3.2 P3.3 S3a.1 S3c.1	X		X	X	• [FAA00] • Several Internet sources • [ΣΣ93, ΣΣ97]	KS:FC PM:F

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					visibility of all internal opportunities for the organisation to control the systems.									
392.	RSM (Requirements State Machines)	T	R	1996 or older	An RSM is a model or depiction of a system or subsystem, showing states and the transitions between states. Its goal is to identify and describe all possible states and their transitions.	Are sometimes called Finite State Machines (FSM)	aviation	S1.3 S3a.2	X	X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:R
393.	Rule violation techniques	G			These are techniques that try to avoid violations of rules, e.g. by designing the system such that the violation is prohibited, or such that an alert follows after the violation.	See also TOPPE	offshore computer	P1.3		X	X		• [HSEC02]	PM:R
394.	SADA (Architectural Design Analysis or Safety Architectural Design Analysis)	T	Ds	1996 or older	Analysis performed on the high-level design to verify the correct incorporation of safety requirements and to analyse the Safety-Critical Computer Software Components (SCCSCs). It uses input from the Architectural Design, the results of the Software Safety Requirements Analysis (SSRA), and the system hazard analyses. The SADA examines these inputs to: a) Identify as SCCSCs those software components that implement the software safety requirements identified by the SSRA. Those software components that are found to affect the output of SCCSCs shall also be identified as SCCSCs; b) Ensure the correctness and completeness of the architectural design as related to the software safety requirements and safety-related design recommendations; c) Provide safety-related recommendations for the detailed design; d) Ensure test coverage of the software safety requirements and provide recommendations for test procedures. The output of the SADA is used as input to follow-on software safety analyses.		computer	S3a.2		X			• [FAA00] • [NASA-STD-8719] • [Rakowsky]	PM:R
395.	SADT (Structured Analysis and Design Technique)	T	Dh	1977	Aim is to model and identify, in a diagrammatical form using information flows, the decision making processes and the management tasks associated with a complex system. A type of structured analysis methodology, SADT is a framework in which the nouns and verbs of any language can be embedded for the representation of a hierarchical presentation of an information system. SADT is composed of a graphic language and a method for using it. A SADT model is an organised sequence of diagrams, each with supporting text. SADT also defines the personnel roles in a software project.	Good analysis tool for existing systems, and can also be used in the design specification of systems. Software requirements specification phase and design & development phase	computer	P3.1 S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	KS:FC PM:C MC:R
396.	Safe Language Subsets or Safe Subsets of Programming Languages	T	Ds	1990 or older	Aim is to reduce the probability of introducing programming faults and increase the probability of detecting any remaining faults. A language is considered suitable for use in a safety-critical application if it has a	Software design & development phase Highly recommended for safety related software. Tools available.	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [FAA00] • [NASA-GB-	PM:C MC:?

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					precise definition, is logically coherent, and has a manageable size and complexity. With the "safe subset" approach, a language definition is restricted to a subset; only the subset is used in the programming. The reasons are: 1) some features are defined in an ambiguous manner; 2) some features are excessively complex. The language is examined to identify programming constructs that are either error-prone or difficult to analyse, for example, using static analysis methods. A language subset is then defined which excludes these constructs.								1740.13-96] • [Rakowsky]	
397.	Safety monitoring	T	Ds		Safety monitoring is a means of protecting against specific failure conditions by directly monitoring a function for failures that would contribute to the failure condition. Monitoring functions may be implemented in hardware, software, or a combination of hardware and software. Through the use of monitoring technique, the software level of the monitored function may be reduced to the level associated with the loss of its related system function.		computer aviation	S3a.2	X	X			• [DO178B]	
398.	Safety Review, Safety Audit	G			A Safety Review assesses a system, identifies facility conditions, or evaluates operator procedures for hazards in design, the operations, or the associated maintenance.	Periodic inspections of a system, operation, procedure, or process are a valuable way to determine their safety integrity. A Safety Review might be conducted after a significant or catastrophic event has occurred.	aviation computer	S3c.1				X	• [FAA00] • [Storey96] • [ΣΣ93, ΣΣ97]	KS:FC PM:C
399.	Safety targets setting	T	R	2001 or older	Setting requirements for the level of safety that is tolerated.		ATM and many other	F3.4	X		X		• [SPF-safety01]	PM:C
400.	SAGAT (Situation Awareness Global Assessment Technique)	T	H	1995	SAGAT is a specialised questionnaire for querying subjects about their knowledge of the environment. This knowledge can be at several levels of cognition, from the most basic of facts to complicated predictions of future states. It is administered within the context of high fidelity and medium fidelity part-task simulations, and requires freezing the simulation at random times.	Most known uses of SAGAT have been in the context of fighter aircraft although its application within the ATM domain has also been investigated.	defence aircraft ATM	S3a.2 S3c.1			X		• [Endsley97] • [HIFA_perform] • [MIL-HDBK]	KS:FC PM:R
401.	SAINT or Micro-SAINT (Systems Analysis of Integrated Networks or Micro-Systems Analysis of Integrated Networks)	I	H	1977	Micro SAINT is a discrete-event task network modelling tool. It can be used to analyse and improve any system that can be described by a flow diagram. It can be used to answer questions about the costs of alternative training, about how crew workload levels or reaction times affect system performance, and about the allocation of functions between people and machines.		avionics submarine displays	P3.2 S3a.2	X		X		• [CBSSE90, p40] • [DND_SECO] • [Kirwan94] • [Kirwan98-1] • [THEMES01]	KS:FC PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
402.	SART (Situation Awareness Rating Technique)	T	H	1989	SART is a multi-dimensional rating scale for operators to report their perceived situational awareness. It examines the key areas of SA: understanding, supply and demand. These areas are further broken down into the 14 dimensions ([Uhlarik02] mentions 10 dimensions). From the ratings given on each of the dimensions situational awareness is calculated by using the equation SA =U-(D-S) where U is summed understanding, D is summed demand and S is summed supply.	SART is simple, quick and easy to apply.	defence aviation	S3c.1			X		• [MIL-HDBK] • [Uhlarik&Comerford 02]	KS:FC PM:C
403.	SATORE	D			Incident reporting system.		?	F3.2 P3.2 S3c.1	X		X		• [Minutes 10 Sept]	KS:FC PM:R
404.	Scenario Analysis	T	R	1979 or older	Scenario Analysis identifies and corrects hazardous situations by postulating accident scenarios where credible and physically logical.	Scenarios provide a conduit for brainstorming or to test a theory in where actual implementation could have catastrophic results. Where system features are novel, subsequently, no historical data is available for guidance or comparison, a Scenario Analysis may provide insight.	many	F3.2 P3.2	X			X	• [FAA00] • [ΣΣ93, ΣΣ97]	KS:F PM:R
405.	SCHAZOP (Safety Culture Hazard and Operability)	T	R	1996	HAZOP adapted for safety management assessment. By application of 'safety management' guidewords to a representation of the system, it identifies: Areas where the safety management process is vulnerable to failures; the potential consequences of the safety management failure; the potential failure mechanisms associated with the safety management failure; the factors which influence the likelihood of the safety management failures manifesting themselves; error recovery and reduction measures.		chemical?	S3a.1 S3a.2 S3c.1				X	• [Kennedy&Kirwan98]	KS:FC PM:C
406.	SCHEMA (System for Critical Human Error Management and Assessment OR Systematic Critical Human Error Management Approach)	T	H	1992	Determines human reliability. It has a flowchart format following the SHERPA method.	Human reliability family. Originated from SHERPA.	chemical	P3.2 S3a.2			X		• [Kirwan98-1] • [MUFTIS3.2-I]	KS:R PM:C
407.	SDA (Sequence Dependency Analysis)	T	H	1999 or older	SDA follows from TLA and notes the dependency between different task elements. It can also estimate the qualitative uncertainty in time estimates for each sub-task, and the timing data source used. SDA is useful in identifying tasks whose reliability is critical, and therefore		nuclear	P3.1 P3.2 P3.3 P3.4 S3a.2			X		• [Kirwan&Kennedy&Hamblen]	KS:FC PM:F

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					tasks that require a high quality of human factors design. SDA can therefore lead to error reduction recommendations (often via the TTA and Ergonomics Review) that will have a general effect on human reliability across a scenario or several scenarios. SDA also helps to identify the longest time likely for the task sequence, and where it may perhaps be best to gain more accurate time estimates to ensure the TLA is accurate.			S3c.1						
408.	SDA (Software Deviation Analysis)	T	Ds	1996	Safeware hazard analysis technique that incorporates the beneficial features of HAZOP (e.g. guidewords, deviations, exploratory analysis, systems engineering strategy) into an automated procedure that is capable of handling the complexity and logical nature of computer software.		computer	S3a.2		X			• [Reese&Leveson97]	PM:C
409.	SDL (Specification and Description Language)	I	Ds	1987 or older	Aims to be a standard language for the specification and design of telecommunication switching systems. SDL is an object-oriented, formal language defined by The International Telecommunications Union–Telecommunications Standardization Sector (ITU–T) as recommendation Z.100. The language is intended for the specification of complex, event-driven, real-time, and interactive applications involving many concurrent activities that communicate using discrete signals.	Should be considered as a possible option for a specification and design methodology, especially for telecommunication systems. Based on Extended FSM, similar to SOM. Tools available. Software requirements specification phase and design & development phase	telecom	S3a.2	X	X			• [Bishop90] • [EN 50128]	PM:R MC:FC
410.	SEAMAID (Simulation-based Evaluation and Analysis support system for MAn-machine Interface Design)	I	H	1996	Cognitive simulations. Has similar functionality to CAMEO-TAT. SEAMAID was being developed to simulate the behaviour of operators, Human System Interface (HSI) and plant behaviour.	In 1998 it has been applied to model a team of the operators in a complicated situation, after which a validation of SEAMAID has been carried out. In 1999, several HSI design configurations were examined to compare the workload that were the key factors of human error.	nuclear	P3.2 S3a.2			X		• [IHF-SEAMAID] • [Kirwan98-1]	KS:R PM:R
411.	SEEA (Software Error Effects Analysis)	T	Ds	1995 or older	Similar to SFMEA (Software FMEA).	Software architecture phase	computer	S3a.2		X			• [EN 50128] • [Lutz&Woodhouse96] • [Rakowsky]	PM:R
412.	Seismic Analysis	T	M	1984 or older	Aim is to ensure structures and equipment resist failure in seismic event	Physical structures and equipment	nuclear	None	X				• [ΣΣ93, ΣΣ97]	PM:R
413.	Self testing and Capability testing	G		1978 or older	Aim is to verify on-line that the system maintains its capability to act in the correct and specified manner	Essential on a normally dormant primary safety system	computer	S3a.2	X	X			• [Bishop90]	PM:R
414.	Semi-Markov Chains	M			Markov chains that also allow non-exponential transitions.	Dynamic assessment family. Tools available (e.g. ASSIST:	many	P3.2 S3a.2	X		X	X	• [Butler&Johnson95] • [MUFTIS3.2-I]	PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						Abstract Semi-Markov Specification Interface to the SURE Tool)		S3c.1					• [NASA-Assist01]	
415.	SFMEA (Software Failure Modes and Effects Analysis)	T	Ds	1979	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. SFMEA was based on FMEA and has a similar structure.	Software is embedded into vital and critical systems of current as well as future aircraft, facilities, and equipment. SFMEA can be used for any software process; however, application to software controlled hardware systems is the predominate application. It can be used to analyse control, sequencing, timing monitoring, and the ability to take a system from an unsafe to a safe condition.	aircraft	S3a.2	X	X			• [FAA00] • [Lutz&Woodhouse96] • [ΣΣ93, ΣΣ97]	PM:C
416.	SFTA (Software Fault Tree Analysis)	T	Ds	1984 or older	This technique is employed to identify the root cause(s) of a "top" undesired event. To assure adequate protection of safety critical functions by inhibits interlocks, and/or hardware. Based on Fault Tree Analysis.	Any software process at any level of development or change can be analysed deductively. However, the predominate application is software controlled hardware systems.	computer aviation	S3a.2	X	X			• [FAA00] • [Leveson95] • [NASA-GB-1740.13-96] • [ΣΣ93, ΣΣ97]	PM:C MC:FC
417.	SHA (System Hazard Analysis)	T	Dh	1993 or older	System Hazard Analysis purpose is to concentrate and assimilate the results of the Sub-System Hazard Analysis (SSHA) into a single analysis to ensure the hazards of their controls or monitors are evaluated to a system level and handles as intended. SHA built on preliminary hazard analysis (PHA) as a foundation. SHA considers the system as a whole and identifies how system operation, interfaces and interactions between subsystems, interface and interactions between the system and operators, and component failures and normal (correct) behaviour could contribute to system hazards. The SHA refines the high-level design constraints generated during PHA. Conformance of the system design to the design constraints is also validated. Through SHA, safety design constraints are traced to individual components based on the functional decomposition and allocation.	Any closed loop hazard identification and tracking system for an entire program, or group of subsystems can be analysed. Identifies system design features and interface considerations between system elements that create hazards. Inductive	aircraft	P3.2 P4a.x	X				• [FAA00] • [FAA tools] • [SEC-SHA] • [ΣΣ93, ΣΣ97]	PM:C
418.	SHARD (Software Hazard Analysis and Resolution in Design)	T	Ds	1994	Adaptation of HAZOP to the high-level design of computer-based systems. Has been shown to be cost-effective in revealing potential safety problems in designs.	Developed by DCSC (Dependable Computing Systems Centre).	computer	S3a.2		X			• [DCSC02] • [McDermid01] • [McDermid&Pumfrey]	PM:C MC:R
419.	SHARP (Systematic Human	T	H	1984	Helps practitioners picking up the right Human Reliability Analysis method to use for a specific action /	Human reliability family	electr	P2.x			X		• [MUFTIS3.2-I] • [Wright&Fields&Ha	KS:R PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Action Reliability Procedure)				situation. It employs a 4-phase procedure: 1) Identification of potential human errors (using detailed description of operator tasks and errors, and techniques like FMEA); 2) Selecting significant errors (e.g. based on likelihood and whether it leads directly to undesirable event); 3) Detailed analysis of significant errors (likelihood analysis); 4) Integration into a system model (studying the dependence between human errors and system errors and the dependence of human errors on other errors).									rrison94]	
420.	SHERPA (Systematic Human Error Reduction and Prediction Approach)	T	M	1986	Focuses on particular task types depending on the industry concerned. Root of TRACEr, HERA I, HERA II. The description of activities developed using HTA is taken task-by-task and scrutinised to determine what can go wrong. Each task is classified into one of 5 basic types (i.e. checking, selection, action, information communication and information retrieval) and a taxonomy of error types is applied. The immediate consequences for system performance are recorded. For each error type, an assessment of likelihood and criticality is made. Finally, potential recovery tasks and remedial strategies are identified.	Related to SCHEMA and PHEA. Equivalent to FMEA used in reliability Technology. Also does it work like a human HAZOP.	nuclear	P3.1 P3.2 P3.3				X		• [Kirwan94] • [Kirwan98-1]	KS:R PM:C
421.	Shock method	T	R	1991 or older	Is used to quantify common cause effects identified by Zonal Analysis	Static assessment family	aircraft	P3.2	X				• [MUFTIS3.2-I]	PM:C
422.	Signal Flow Graphs	T	Dh	1966	Identifies the important variables and how they relate within the system. The analysis is conducted by selecting a system output variable and then identifying all the variables that could influence this. The network presents the system variables as nodes connected by flows		electr	P3.1			X		• [Kirwan&Ainsworth 92]	PM:R MC:R
423.	Simulators/mock-ups	G		1981 or older	Involves the development and use of some form of simulation of systems. This simulation might range from a full-scale high fidelity or full-scope simulators through some simple mock-up of a single piece of equipment.	Usually used when the real equipment is not available for analysis work.	many	P3.2 S3a.2 S3c.1	X				• [Kirwan&Ainsworth 92]	KS:F PM:R
424.	Situational Awareness Error Evolution	T	H	2001 about	Technique based on the premise that a situation awareness error can evolve and expand as it is picked up by other humans (snowball effect).		ATM	P3.2 S3a.1			X	X	• [Stroeve&Blom&Park03]	
425.	SLIM (Success Likelihood Index Methodology)	T	H	1984	Estimates human error probabilities. Two modules: MAUD (Multi-Attribute Utility Decomposition, used to analyse a set of tasks for which human error probabilities are required) and SARAH (Systematic Approach to the Reliability Assessment of Humans, used to transform success likelihoods into human error probabilities)	Human reliability family. Similar to APJ. Can be reserved for difficult HEP assessments that HEART and THERP are not designed for	nuclear chemical	P3.2 S3a.2				X		• [Humphreys88] • [Kirwan&Kennedy&Hamblen] • [Kirwan94] • [MUFTIS3.2-I]	KS:FC PM:C
426.	SMHA	T	Ds	1987	Used to identify software-related hazards. A state machine	Often used in computer science.	avionics	S3a.2		X			• [Leveson95]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(State Machine Hazard Analysis)				is a model of the states of a system and the transitions between them. Software and other component behaviour is modelled at a high level of abstraction, and faults and failures are modelled at the interfaces between software and hardware.	For complex systems, there is a large number of states involved. Related to Petri nets. Procedure can be performed early in the system and software development process.								
427.	SNEAK (Sneak Circuit Analysis)	T	R	1967 / 1991	Sneak-Circuit Analysis identifies unintended paths or control sequences that may result in undesired events or inappropriately time events. Sneak Analysis starts with the development of a stepwise flowchart of the task sequence. Clue application is next carried out using the computerised system. A number of the questions will require a relatively detailed human factors analysis of the installation if they are to be answered. For each question, there is back-up information expanding on what constitutes an acceptable system configuration in human factors terms. Sneak paths are then identified by considering the logical possibilities for flows in the system. Barriers that are present must be considered at this point.	Should be considered for those components that are safety critical. This technique is applicable to control and energy-delivery circuits of all kinds, whether electronic/ electrical, pneumatic, or hydraulic. Tools available. Originally developed (Boeing) to look at unintended connections in wiring systems. Later (1991) adapted considerably to consider errors of commission in HRA. Highly resource-intensive.	aircraft nuclear	P3.1 P3.2 P3.3 S3a.2	X	X	X		• [Bishop90] • [EN 50128] • [FAA AC431] • [FAA00] • [Kirwan98-1] • [MAS611-2] • [Rakowsky] • [ΣΣ93, ΣΣ97] • [Sparkman92]	KS:FC PM:R
428.	SOCRATES (Socio-Organizational Contribution to Risk Assessment and the Technical Evaluation of Systems)	I	R	1998	Analysis of organisational factors. Is intended to aid conceptualising the role that organisational factors play in shaping plant performance and how they influence risk.	Developed by Idaho National Engineering and Environmental Laboratory (INEEL)	nuclear	P3.2 S3a.1	X			X	• [HRA Washington] • [NEA99]	PM:R
429.	Software configuration management	G			Requires the recording of the production of every version of every significant deliverable and of every relationship between different versions of the different deliverables. The resulting records allow the developer to determine the effect on other deliverables of a change to one deliverable.	Technique used throughout development. In short it is "To look after what you've got so far"	computer	S3a.2		X			• [EN 50128] • [Jones&Bloomfield &Froome&Bishop01] • [Rakowsky] • [SCM biblio]	PM:R
430.	Software Time-out Checks	T	Ds	1980 or older	Aim is to provide time limits for software running non-deterministic tasks	Should always be used to provide determinism on non-deterministic task in safety computer systems. Related to error-recovery and time-out checks.	computer	S3a.2		X			• [Bishop90]	PM:C MC:R
431.	SOM (Systems Development by an Object-oriented Methodology)	I	Dh Ds	1987 or older	SOM is a development language and methodology covering the development of systems consisting of software and hardware from requirements to implementation, with special emphasis on real-time systems	Should be used as an option for a development methodology. Based on Extended FSM, related to SBC, CCS, SDL, SADT. Tools available.	computer	S3a.2	X	X			• [Bishop90]	PM:C
432.	SPAM	T	H	1998	SPAM is a method of measuring situation awareness		ATC	S3a.2			X		• [HIFA_perform]	KS:FC

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Situation-Present Assessment method)				(SA). In contrast to SAGAT, the SPAM method uses response latency as the primary dependent variable and does not require a memory component. It acknowledges that SA may sometimes involve simply knowing where in the environment to find some information, rather than remembering what that information is exactly.			S3c.1						PM:R
433.	SPAR HRA (Simplified Plant Analysis Risk Human Reliability Assessment)	T	H	2001 or older	Quick easy to use screening level (i.e. not full scope) HRA technique. Significant revision of ASP, has incorporating advantages of other human reliability assessment methods (e.g. IPE, HPED, INTENT)	Qualitative and quantitative	nuclear	P3.2 S3a.2 S3c.1			X		• [HRA Washington]	PM:C
434.	SPC (Statistical Process Control)	T	Dh	1920s	Aim is to understand and control variations in process. Four general steps: 1) Describe the distribution of a process; 2) Estimate the limits within which the process operates under 'normal' conditions; 3) Determine if the process is 'stable', sample the output of the process and compare to the limits. Decide: a) 'process appears to be OK; leave it alone, or b) 'there is reason to believe something has changed' and look for the source of that change; 4) Continuous process improvement.	Any process where sufficient data can be obtained. Many training courses available.	computer	S3a.2 S3c.1		X			• [Leavengood98] • [ΣΣ93, ΣΣ97]	PM:R
435.	Specification Analysis	G		1990 or older	Specification Analysis evaluates the completeness, correctness, consistency and testability of software requirements. Well-defined requirements are strong standards by which to evaluate a software component. Specification analysis should evaluate requirements individually and as an integrated set.		aircraft	S3a.2		X			• [NASA-GB-1740.13-96]	PM:C
436.	SpecTRM (Specification Tools and Requirements Methodology)	I	Ds	2002	Methodology and supporting toolset for building embedded, software-intensive, safety-critical systems that focuses on the system engineering aspects of software and the development of safe and correct requirements.	Is based on the principle that critical properties must be designed into a system from the start. As a result, it integrates safety analysis, functional decomposition and allocation, and human factors from the beginning of the system development process.	aircraft	S3a.1 S3a.2		X			• [Leveson02]	PM:R MC:F
437.	SPFA (Single-Point Failure Analysis)	T	Dh	1980	This technique is to identify those failures that would produce a catastrophic event in items of injury or monetary loss if they were to occur by themselves. The SPFA is performed by examining the system, element by element, and identifying those discrete elements or interfaces whose malfunction or failure, taken individually, would induce system failure. The technique is equally applicable to hardware, software and formalised human operator procedures.	This approach is applicable to hardware systems, software systems, and formalised human operator systems. It is sometimes referred to as another standard name for FMEA.	space	P3.2	X	X	X		• [DAN97] • [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:F

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
438.	SRK (Skill, Rule and Knowledge-based behaviour model)	T	H	1981	Psychologically-based tool. Attempts to bring generalised psychological theories or models into the rich context of a complex industrial work environment	Rarely used as tool on its own.	many	P3.1 S3a.2			X		• [Kirwan98-1]	KS:R PM:R
439.	SRS-HRA (Savannah River Site Human Reliability Analysis)	D		1994	Data-based approach based on data collected from four existing SRS databases (based on incidents, logs, etc.): fuel processing; fuel fabrication; waste management; and reactors. The approach is contextual and taxonomy-based.	Related to JHEDI	nuclear	P3.2 S3c.1			X		• [Kirwan98-1]	KS:R PM:R
440.	SSAR (System Safety Assessment Report)	T	R	1996 or older	The general purpose is to perform and document a comprehensive evaluation of the accident risk being assumed before test or operation of a system. This means that the SSAR summarises the safety analyses and assessments conducted on the program.		aircraft	S3a.2	X	X			• [FAA tools]	PM:R
441.	SSCA (Software Sneak Circuit Analysis)	T	Ds	1976 or older	Software Sneak Circuit Analysis (SSCA) is designed to discover program logic that could cause undesired program outputs or inhibits, or incorrect sequencing/ timing.	The technique is universally appropriate to any software program.	computer	S3a.2		X			• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
442.	SSG (State Space Graphs (or Discrete State Space Graphs))	M		1991 or older	Models all discrete states of a system and associates to each discrete state a level of severity of consequences on the service delivered. Petri Nets may be used during the modelling.	Dynamic assessment family	many	P3.2 S3a.1 S3a.2	X		X	X	• [MUFTIS3.2-I]	PM:R
443.	SSHA (Subsystem Hazard Analysis)	T	R	1972 or older	The SSHA is performed to identify and document hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and assemblies within the subsystems as well as their external interfaces. It includes software whose performance, degradation, functional failure or inadvertent functioning could result in a hazard. It also includes a determination of the modes of failure including reasonable human errors, single point failures and the effects on safety when failures occur within subsystem components and assemblies.	This protocol is appropriate to subsystems only.	aircraft	P3.2	X				• [FAA AC431] • [FAA00] • [FAA tools] • [ΣΣ93, ΣΣ97]	PM:C
444.	SSRFA (Software Safety Requirements Flowdown Analysis)	T	Ds	1996 or older	Safety requirements are flowed down into the system design specifications. Tools and methods for requirements flowdown analyses include checklists and cross references. A checklist of required hazard controls and their corresponding safety requirements should be created and maintained.		avionics	S3a.2		X			• [NASA-GB-1740.13-96]	PM:C
445.	STEP or STEPP (Sequentially- Timed Events Plot or	T	R	1978 or older	This method is used to define systems; analyse system operations to discover, assess, and find problems; find and assess options to eliminate or control problems; monitor future performance; and investigate accidents.	In accident investigation, a sequential time of events may give critical insight into documenting and determining	?	P3.2 P3.3 S3a.2 S3c.2	X			X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	Sequential Times Event Plotting Procedure)				It is an events-analysis-based approach in which events are plotted sequentially (and in parallel, if appropriate) to show the cascading effect as each event impacts on others. It is built on the management system embodied in the Management Oversight and Risk Tree (MORT) and system safety technology.	causes of an accident. The technique is universally appropriate.									
446.	Stochastic Differential Equations in ATM	M		1990	These are differential equations with stochastic elements. The stochastic elements may model noise variations in processes, or the occurrence of random events.		ATM	P3.2 S3a.2	X		X	X	• [Blom90]	
447.	Stress Reduction	G			Aim is to ensure that under all normal operational circumstances both hardware components and software activity are operated well below their maximum stress levels.	In safety critical systems, stress reduction techniques should always be used when practical.	computer	P4a.x S3c.1	X	X			• [Bishop90]	PM:C
448.	Strongly Typed Programming Languages	G		1983 or older	Aim is to reduce the probability of faults by using a language that permits a high level of checking by the compiler.	Highly recommended. Tools available. Software design & development phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C
449.	Structural Safety Analysis	T	R	1979 or older	Is used to validate mechanical structures. Inadequate structural assessment results in increased risk due to the potential for latent design problems causing structural failures, i.e., contributory hazards. Structural design is examined via mathematical analysis to satisfy two conditions: 1) Equilibrium of forces, and 2) Compatibility of displacements. The structure considered as a whole must be in equilibrium under the action of the applied loads and reactions; and, for any loading, the displacements of all the members of the structure due to their respective stress-strain relationships must be consistent with respect to each other.	The approach is appropriate to structural design; i.e., airframe.	aircraft	P4a.x S3a.2 S3c.1	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R
450.	Structure Based Testing	T	Ds	1995 or older	Based on an analysis of the program, a set of input data is chosen such that a large fraction of selected program elements are exercised. The program elements exercised can vary depending upon level of rigour required.		computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:C
451.	Structure Diagrams	T	Ds	1995 or older	Notation which complements Data Flow Diagrams. They describe the programming system and a hierarchy of parts and display this graphically, as a tree, with the following symbols: 1) rectangle annotated with the name of the unit; 2) an arrow connecting these rectangles; 3) A circled arrow, annotated with the name of data passed to and from elements in the structure chart. Structure Diagrams document how elements of a data flow diagram can be implemented as a hierarchy of program units.		computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:R
452.	Structured Interviews	G		1972 or	Is more commonly used for the general collection of task-based information. The structuring offers the opportunity		many	F3.1 F3.2			X		• [Kirwan&Ainsworth 92]	PM:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
				older	for more systematic collection of data.			F3.3 P3.2 P3.3 S3c.1						
453.	Structured Methodology	G			Main aim is to promote the quality of software development by focusing attention on the early parts of the lifecycle. The method aims to achieve this through both precise and intuitive procedures and notations to identify the existence of requirements and implementation features in a logical order and a structured manner.	A range of structured methodologies exist.	computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:C
454.	Structured Programming	G		1976 or older	Aim is to design and implement the program in a way that makes the analysis of the program practical. This analysis should be capable of discovering all significant program behaviour. The program should contain the minimum of structural complexity. Complicated branching should be avoided. Loop constraints and branching should be simply related to input parameters. The program should be divided into appropriately small modules, and the interaction of these modules should be explicit.	Should be used wherever possible. Tools available. Software design & development phase	computer	S3a.2		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C
455.	Structuring the System according to Criticality	T	Ds	1989	Aim is to reduce the complexity of safety critical software	Strongly recommended where applicable. Info from HAZOP, FTA, FMEA can be used.	computer	S3a.2		X			• [Bishop90]	PM:C
456.	SUSI (Safety Analysis of User System Interaction)	T	R	1994 or older	HAZOP has been modified to handle Human-computer interaction. The approach adopted in the SUSI methodology is a natural extension of standard hazard analysis procedures. The principal development has been in the creation of an appropriate representation of user system interaction. A major advantage of this process is that the dataflow representation gives an overview of the complete system. The representation of the system as processes and data/control flows is understood by individuals with no software design training, such as operators and users. The review process can lead to detailed insights into potential flaws in the procedures and processes. Designers with different viewpoints are able to use a common representation and believe that it increases their understanding of the total system.		transport	P3.1 P3.2 P3.3 S3a.2	X		X	X	• [Chudleigh&Clare94] • [Falla97] • [Stobart&Clare94]	PM:C
457.	SWHA (Software Hazard Analysis)	G	Ds	1984 or older	The purpose of this technique is to identify, evaluate, and eliminate or mitigate software hazards by means of a structured analytical approach that is integrated into the software development process. The SWHA identifies hazardous conditions incident to safety critical operator	This practice is universally appropriate to software systems.	computer	S3a.2		X			• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					information and command and control functions identified by the PHA, SHA, SSHA and other efforts. It is performed on safety critical software-controlled functions to identify software errors/paths that could cause unwanted hazardous conditions. The SWHA can be divided into two stages, preliminary and follow-on.									
458.	SYBORG (System for the Behaviour of the Operating Group)	I	H	1996	A cognitive simulation approach which is the first to try to deal with emotional aspects of performance. It aims to predict what emotions personnel will experience when dealing with difficult nuclear power plant events, and aims to determine how these emotions will affect attention, thought, action, and utterances. The emotions considered include fear, anxiety, tension, surprise, etc. SYBORG is possibly the first approach that, in the future, may be able to identify idiosyncratic errors, or errors caused by extreme stress in a situation.	There is ongoing work to determine how emotions interact with each other and with error forms.	nuclear	P3.1 P3.2 S3a.2			X		• [Kirwan98-1]	KS:R PM:C
459.	Symbolic Execution	T	Ds	1976	Aim is to show the agreement between the source code and the specification. The program is executed substituting the left hand side by the right hand side in all assignments. Conditional branches and loops are translated into Boolean expressions. The final result is a symbolic expression for each program variable. This can be checked against the expected expression.	Recommended for safety critical software providing the number of paths is small and there is good tool support. Tools available.	computer	S3a.2 S4a.x		X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C
460.	Synchronous Data Flow Specification Languages	T	Ds	1988 or older	A structured specification and implementation expressed in terms of parallel processes and data flow.	Should be considered as possible approach for the implementation of concurrent real-time control systems. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:R
461.	Systematic Inspection	G			This technique purpose is to perform a review or audit of a process or facility. The inspection may involve the use of checklists.	The technique is universally appropriate.	nuclear chemical	S3a.2	X			X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
462.	Systematic Occupational Safety Analysis	T	R	1992 or older	Aim is to evaluate a facility from an OSHA (Occupational Safety and Health Administration) standpoint	Any operation with personnel involved	nuclear chemical	P3.2 S3a.2 S3c.1	X			X	• [ΣΣ93, ΣΣ97]	PM:R
463.	T/LA (Time/ Loss Analysis for Emergency Response Evaluation)	T	R	1980 or older	This technique is a system safety analysis-based process to semi-quantitatively analyse, measure and evaluate planned or actual loss outcomes resulting from the action of equipment, procedures and personnel during emergencies or accidents. T/LA procedures produce objective, graphic time/loss curves showing expected versus actual loss growth during emergencies or mishaps. The expected versus actual loss data is used to describe the change in the outcome produced by intervention actions at successive states of the emergency response.	Any airport, airline and other aircraft operators should have an emergency contingency plan to handle unexpected events can be analysed. This approach defines organise data needed to assess the objectives, progress, and outcome of an emergency response; to identify response problems; to find and assess options to	aviation	S3c.1	X		X	X	• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					Although it is a system level analysis, due to lack of design definition and maturity, it is not usually initiated until after the SSHA has begun and uses the SSHA data before it is integrated into the SHA.	eliminate or reduce response problems and risks; to monitor future performance; and to investigate accidents.								
464.	Table-top analysis	G		1974	A group of experts who have an understanding of a specific aspect of a system, meet together as a discussion group to define or assess particular aspects of a task. The discussions must be directed around some basic framework.		many	F3.1 F3.2 F3.3 P3.1 P3.2 P3.3 P3.4	X		X		• [Kirwan&Ainsworth 92]	KS:FC PM:C
465.	TAFEI (Task Analysis For Error Identification)	T	H	1991	Task analysis method based on State Space Diagrams, describing user interactions with equipment in terms of transition (input-output) boxes (non-Markovian: qualitative in nature). For a particular task the network of transition boxes is developed, and then examined to determine what illegal transitions could take place, such as skipping over task elements, sequence errors, etc., though in theory EOCs could be developed from such networks.	Related to State Space Diagrams.	?	P3.1 P3.2 S3a.2 S3c.1	X		X		• [Kirwan98-1]	KS:FC PM:C
466.	TALENT (Task Analysis-Linked EvaluatioN Technique)	I	H	1988	An assessment framework which also contains a strong task analysis bias, utilising Task Analysis or Sequential Task Analysis Timeline Analysis, and Link Analysis for each task sequence. Then, tasks are identified for inclusion in the fault and event trees, through a collaborative effort between the behavioural scientists and the safety assessors. PSF (Performance Shaping Factor) are then identified for each task, and then the tasks are quantified using either THERP or SLIM.	TALENT was apparently applied in a large European PSA/HRA exercise, and for an evaluation of the US Peach bottom nuclear power plant. It has not been used substantially recently.	nuclear	P3.1 P3.2 S3a.2			X		• [Kirwan98-1]	KS:R PM:R
467.	Talk-Through	T	M	1986	Similar to Walk-Through, but is undertaken more remotely from the normal task location, so that the tasks are verbalised rather than demonstrated		many	P3.1 S3c.1			X		• [Kirwan&Ainsworth 92]	KS:FC PM:R
468.	Task Decomposition	T	H	1953	Task decomposition is a structured way of expanding the information from a task description into a series of more detailed statements about particular issues which are of interest to the analyst.		many	P3.1 S3a.2			X		• [Kirwan&Ainsworth 92]	
469.	Task Description Analysis	T	H	1986 or older	Method supported by several different methods designed to record and analyse how the human is involved in a system. It is a systematic process in which tasks are described in terms of the perceptual, cognitive, and manual behaviour required of an operator, maintainer or support person.		defence	P3.1 S3a.2			X		• [MIL-HDBK]	KS:FC PM:C
470.	TEACHER/ SIERRA	I	R	1993	Alternative HRA framework more aimed at lower		chemical	P3.1			X		• [Kirwan98-1]	KS:R

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	(Technique for Evaluating and Assessing the Contribution of Human Error to Risk [which uses the] Systems Induced Error Approach)				consequence accidents than PSA traditionally aims at. It has a number of components. The first is SIERRA. This states that humans have basic error tendencies that are influenced by PIFs. TEACHER focuses on defining a task inventory, then determining the prioritisation of critical tasks according to their risk potential, leading to a rating on a risk exposure index for each task. Following the screening analysis a HTA and PHEA analysis are carried out, following which, those errors with significant consequence potential are analysed with respect to a set of PIF audit questions, to develop remedies for the error. Each PIF audit question allows the analyst to rate the task according to, e.g., the extent to which procedures are defined and developed by using task analysis, on a seven-point semantic differential, anchored at each end-point. Risk reduction is then determined by the analyst.			P3.2 P3.3 S3a.2						PM:C
471.	Telelogic Tau	I	Ds	2001 or older	Telelogic Tau provides specialised tool sets for every phase of a project: 1) Telelogic Tau UML Suite for requirement capture and analysis; 2) Telelogic Tau SDL Suite for design and implementation, and 3) Telelogic Tau TTCN Suite for comprehensive testing. In addition, a) SCADE Suite (sold to Esterel) facilitates the capture of unambiguous software specifications. It allows detecting corner bugs in the early stages of the development and reduces the coding and testing efforts. b) Telelogic Tau Logiscope Detects Coding Errors in C, C++, Ada and Java, Identifies and Locates Error-Prone Modules and Provides Code Coverage Analysis	Software tools that cover all phases of the development process: analysis, design, implementation and testing.	computer	S3a.2		X			• [Telelogic Tau]	PM:R MC:F C
472.	Temporal Logic	T	Dh Ds	1986 or older	Direct expression of safety and operational requirements and formal demonstration that these properties are preserved in the subsequent development steps. Formal Method. It extends First Order Logic (which contains no concept of time) by adding model operators. These operators can be used to qualify assertions about the system. Temporal formulas are interpreted on sequences of states (behaviours). Quantified time intervals and constraints are not handled explicitly in temporal logic. Absolute timing has to be handled by creating additional time states as part of the state definition.	Useful as descriptive and demonstrative technique for small systems or small parts of large systems. Computer based tools are necessary for large systems. Related methods are Petri nets, finite state machines. Software requirements specification phase and design & development phase	computer	P3.1 P3.2 S3a.2	X	X			• [Bishop90] • [EN 50128] • [Rakowsky]	PM:C MC:F C
473.	TESEO (Tecnica Empirica Stima Errori Operatori (Empirical technique to	T	H	1980	Assesses probability of operator failure. Used more as a tool of comparison between different designs of the man-machine system than for obtaining absolute probabilities. Human Error Probability (HEP) is the product of five	Human reliability family. Not considered very accurate.	chemical nuclear	P3.2			X		• [Humphreys88] • [MUFTIS3.2-I]	KS:R PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
	estimate operator errors))				values: (1) complexity of action, requiring close attention or not. (2) time available to carry out the activity. (3) experience and training of the operator. (4) operators emotional state, according to the gravity of the situation. (5) man-machine and environment interface.									
474.	Test Adequacy Measures	T	M	1972 or older	Aim is to determine the level of testing applied using quantifiable measures.		computer	S3a.2		X			• [Bishop90]	PM:C
475.	Test Coverage	G			For small pieces of code it is sometimes possible to achieve 100% test coverage. However due to the enormous number of permutations of states in a computer program execution, it is not often not possible to achieve 100% test coverage, given the time it would take to exercise all possible states. Several techniques exist to reach optimum test coverage. There is a body of theory that attempts to calculate the probability that a system with a certain failure probability will pas a given number of tests. Monte Carlo simulation may also be useful.		avionics	S3a.2		X			• [DO178B] • [FAA00]	PM:C
476.	Tests based on Random Data	G		1984 or older	Aim is to cover test cases not covered by systematic methods. To minimise the effort of test data generation.	Recommended if there is some automated means of detecting anomalous or incorrect behaviour.	computer	S3a.2		X			• [Bishop90]	PM:C
477.	Tests based on Realistic data	G		1976 or older	Aim is to detect faults likely to occur under realistic operating conditions.	Not particularly effective or appropriate at the early stages of software development. Recommended for system testing and acceptance testing	computer	S3a.2		X			• [Bishop90]	PM:C
478.	Tests based on Software structure	G		1976 or older	Aim is to apply tests that exercise certain subsets of the program structure.	Essential part of an overall test strategy for critical systems. Tools available.	computer	S3a.2		X			• [Bishop90]	PM:C
479.	Tests based on the Specification	G			Aim is to check whether there are any faults in the program that cause deviations from the specified behaviour of the software.	Essential part of an overall test strategy	computer	S3a.2		X			• [Bishop90]	PM:C
480.	THERP (Technique for Human Error Rate Prediction)	T	H	1981	Aim is to predict human error probabilities and evaluate degradation of a man-machine system likely to be caused by human error, equipment functioning, operational procedures and practices, etc. This technique provides a quantitative measure of human operator error in a process.	Longest surviving HRA technique. Developed in 1960-1970; released in 1981. This technique is the standard method for the quantifying of human error in industry.	nuclear defence	P3.2	X		X	X	• [FAA00] • [Humphreys88] • [Kirwan94] • [Kirwan98-1] • [MUFTIS3.2-I] • [ΣΣ93, ΣΣ97]	KS:FC PM:C
481.	Threat Hazard Analysis	T	R	1997 or older	Aim is to evaluate potential threats (enemy) and self induced (accident) throughout life cycle.	Weapons systems. Mandatory requirement of MIL STD 2105B	defence	F3.2 F3.3 P3.2 S3a.1 S3c.1	X				• [ΣΣ93, ΣΣ97]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
								S3e.x						
482.	Timeline Analysis	T	H	1987	Analytical technique for the derivation of human performance requirements which attends to both the functional and temporal loading for any given combination of tasks. Timeline Analysis examines the precise sequence of events in a scenario. Visualises events in time and geographically.	Timeline Analysis has been used for years by the defence and intelligence communities, primarily for predicting foreign government actions and responses to world events. Tools available	nuclear offshore defence	P3.1 P3.2 P3.4 S3c.1			X		• [FAS_TAS] • [Kirwan&Ainsworth 92] • [Kirwan94] • [MIL-HDBK] • [Mucks&Lesse01] • [Timeline Web]	KS:FC PM:C
483.	Timing, Throughput and Sizing Analysis	T	Ds	1996 or older	Timing and sizing analysis for safety critical functions evaluates software requirements that relate to execution time and memory allocation. It focuses on program constraints. Typical constraint requirements are maximum execution time and maximum memory usage.		aviation	S3a.2		X			• [NASA-GB-1740.13-96]	PM:C
484.	TOPAZ (Traffic Organisation and Perturbation AnalyZer)	I	R	1993	Safety assessment methodology that assesses the accident risk of an ATM operation, influenced by behaviour of technical systems (hardware and software), humans, environment, procedures, and interactions between these elements. It gives special attention to the interactions between these elements and to cognitive human behaviour. The first hazard analysis phase is qualitative. The second, quantitative, phase is based on Generalized Reich expression for collision risk, the parameters of which are determined through dedicated Monte Carlo simulations of Dynamically Coloured Petri Nets. The quantitative phase is completed with safety criticality assessments and a Bias and Uncertainty Assessment of all model assumptions and parameter values used.	The methodology combines many individual techniques, some of which do not have specific names. The methodology is supported by a tool set and a database with hazards from previous studies, previous submodels, simulation environments, etc.	ATM	F1.3 F3.2 F3.3 F3.4 F4a.x P3.1 P3.2 P3.3 P3.4 P4a.x S3a.1 S3a.2 S3c.1 S3e.x S4a.x S4b.x	X	X	X	X	• [Blom&Bakker93] • [Blom&al98,01] • [Blom&Daams&Nijhuis00] • [Blom&Stroeve&Daams&Nijhuis01] • [Blom&Stroeve&Everdij&Park02] • [Daams&Blom&Nijhuis00] • [DeJong&al01] • [Everdij&Blom02] • [Kos&al00] • [MUFTIS3.2-II]	PM:R
485.	TOPAZ hazard database	D			Database of hazards gathered using dedicated TOPAZ-based hazard brainstorms for various ATM operations		ATM	F3.1 F3.2 F3.3 P3.2 S3c.1	X	X	X	X	• NLR expert	
486.	TOPAZ-based hazard brainstorm	T	R	1996	Hazard identification through brainstorming with experts. Allows identification of many hazards that are unimaginable for some other approaches.		ATM	F3.2 P3.2	X	X	X	X	• NLR expert	PM:R
487.	TOPPE (Team Operations Performance and Procedure Evaluation)	T	H	1991	A procedure validation and team performance evaluation technique. It uses judges to evaluate team performance when carrying out emergency procedures. It is therefore not designed as a Human Error Identification tool. However, it can identify procedural errors (omissions, wrong procedural transitions etc.), and team leadership or		nuclear	S3a.2			X	X	• [Kirwan98-1]	KS:FC PM:C

Id	Technique	Ty	pe	Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					co-ordination problems. As such, an approach could be developed to determine credible procedural and co-ordination errors of these types, based on observation of emergency exercises which all nuclear power plant utilities are required to carry out.									
488.	TRACEr (Technique for the Retrospective Analysis of Cognitive Errors in Air Traffic Management)	I	M	1999	Aim is to predict human errors that can occur in ATM systems, and to derive error reduction measures for ATM. The design process is aided 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.	Human factors in ATM; Reduced scope version of TRACEr is named TRACEr lite (2001).	ATM ATC	P3.2 P3.3			X		• [HIFA_human] • [Shorrock01] • [Shorrock&Kirwan98] • [Shorrock&Kirwan99] • [TRACEr lite_xls]	PM:C BK:F KS:FC
489.	Translator Proven in Use	G			A translator is used whose correct performance has been demonstrated in many projects already. Translators without operating experience or with any serious known errors are prohibited. If the translator has shown small deficiencies the related language constructs are noted down and carefully avoided during a safety related project.	Software design & development phase	computer	S3a.2		X			• [EN 50128] • [Rakowsky]	PM:R
490.	TRIPOD	I	M	1994	Tripod-Beta is a system for conducting analysis of an incident, in parallel with the investigation itself, to enable investigators to confirm facts and identify hidden causes in a systematic and comprehensive approach. The underpinning Tripod methodology allows logical inconsistencies to be highlighted and resolved while the investigation is active, and a definitive report produced. This saves time and effort and enables a clearer understanding of appropriate actions necessary to make significant and lasting improvements in loss prevention.	Safety culture analysis framework. Tools available	petro-chem	S3c.1					X	• [EQE Web_TRIPOD] • [Kennedy&Kirwan98] • [PROMAI5]	KS:FC PM:R
491.	TRM or CRM (Team Resource Management or Crew Resource Management)	I	T	1998 about	CRM training examines how and why human error occurs. It examines the implications of human factors and limitations, and the effect they have on performance. It introduces the concept of the 'Error Chain', the application of which can lead to recognition of incipient error situations, and develops tools for error intervention and avoidance.		ATM and more	P3.2 P3.3 S3a.2			X	X	• [TRM web]	KS:F PM:R
492.	TSA (Test Safety Analysis)	T	M	1979 or older	Test Safety Analysis ensures a safe environment during the conduct of systems and prototype testing. It also provides safety lessons to be incorporated into the design, as application. Each test is evaluated to identify hazardous materials or operations. Is not an analysis technique.	A lessons learned approach of any new systems 'or potentially hazardous subsystems' is provided. This approach is especially applicable to the	space	S3a.2	X				• [FAA AC431] • [FAA00] • [ΣΣ93, ΣΣ97]	PM:R

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
						development of new systems, and particularly in the engineering/ development phase								
493.	TTA (Tabular Task Analysis)	T	M	1989 or older	Aim is to specify the context in which important task steps take place and to identify aspects that may be improved. The TTA usually follows on from a Hierarchical Task Analysis (HTA) and is columnar in format. It takes each particular task-step or operation and considers specific aspects, such as Who is doing the operation, What displays are being used.		nuclear?	P3.1 P3.3			X		• [Kirwan94] • [Vinnem00]	KS:FC PM:R
494.	TTM (Truth Table Method)	T	Dh	1991 or older	Is based on the logic that a set of premises logically entails a conclusion, if every interpretation that satisfies the premises also satisfies the conclusion. Logical entailment is checked by comparing tables of all possible interpretations.	Hazard identification family. TTM can be seen as a rigorous generalisation of FMEA. Equal to Decision Tables	computer	F3.3 F4a.x P3.2	X	X			• [EN 50128] • [Genesereth00] • [MUFTIS3.2-I] • [Rakowsky] • [Sparkman92]	PM:C MC:R
495.	UML (Unified Modelling Language)	T	Ds		UML is the industry-standard language for specifying, visualising, constructing, and documenting the artefacts of software systems. It simplifies the complex process of software design, making a "blueprint" for construction.		computer	S3a.2		X			• [UML]	
496.	Uncertainty Analysis	G			Uncertainty Analysis addresses, quantitatively and qualitatively, those factors that cause the results of an analysis to be uncertain.	All analyses should address uncertainty explicitly. This is a region of great potential application. See also Bias and Uncertainty Assessment.	many	P3.2 P4a.x S4a.x	X	X	X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
497.	Unused Code Analysis	T	Ds	1996 or older	A common real world coding error is generation of code that is logically excluded from execution; i.e., preconditions for the execution of this code will never be satisfied. There is no particular technique for identifying unused code; however, unused code is often identified during the course of performing other types of code analysis. It can be found during unit testing with COTS coverage analyser tools.		avionics	S3a.2		X			• [NASA-GB-1740.13-96] • [Rakowsky]	PM:C MC:R
498.	Update Criticality Analysis	T	Ds	1996 or older	Identifies all those software components that implement software safety requirements or components that interface with safety critical computer software components.		avionics	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C
499.	Update Design Constraint Analysis	T	Ds	1996 or older	The criteria for design constraint analysis applied to a detailed design can be updated using final code. At the code phase, real testing can be performed to characterise the actual software behaviour and performance in addition to analysis.		avionics	S3a.2		X			• [FAA00] • [NASA-GB-1740.13-96] • [Rakowsky]	PM:C
500.	Usability Heuristic Evaluation	T	H	1994	Usability heuristic evaluation is a usability inspection method for finding the usability problems in a human-	Heuristic evaluation is the most popular of the usability methods,	computer	P3.1 S3a.2	X				• [HIFA_usability]	PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					computer interface design so that they can be attended to as part of an iterative design process. Heuristic evaluation involves having a small set of evaluators examine the interface and judge its compliance with recognised usability principles (the "heuristics").	particularly as it is quick, easy and cheap.								
501.	VDM (Vienna Development Method)	T	Ds	1980 about	Systematic specification and implementation of sequential programs. Formal Method. Mathematically based specification technique and a technique for refining implementations in a way that allows proof of their correctness with respect to the specification. The specification language is model-based in that the system sate is modelled in terms of set-theoretic structures on which are defined invariants (predicates) and operations on that state are modelled by specifying their pre-and post conditions in terms of the system state. Operations can be proved to preserve the system invariants.	Recommended especially for the specification of sequential programs. Established technique, training courses available. Closely related to Z. Tools available. Software requirements specification phase and design & development phase	computer	S3a.2		X			• [Bishop90] • [EN 50128]	PM:C MC:R
502.	Verbal Protocols	T	M	1972 or older	Verbal protocols are verbalisations made by a person while they are carrying out a task, in the form of a commentary about their actions and their immediate perceptions of the reasons behind them.		nuclear chemical	S3c.1			X	X	• [Kirwan&Ainsworth 92]	KS:FC PM:R
503.	Verification and Validation	G		1982 or older	Verification: to build the product right; Validation: to build the right product	Essential for safety-related systems. Tools available.	all	F4a.x P4a.x P4b.1 S4a.x S4b.x	X	X			• [Bishop90]	PM:R
504.	Vital Coded Processor	T	Ds	1989	Aim is to be fail-safe against computer processing faults in the software development environment and the computer hardware. In this technique, three types of errors – operation, operator and operand errors – can be detected by redundant code with static signatures.	Overcomes most of the insecurities associated with microprocessor-based technology. Should be considered for use on relatively simple applications that have a safe state	computer	S3a.2	X	X			• [Bishop90]	PM:C
505.	VTLA (Vertical Timeline Analysis)	T	H	1987 or older	Investigates workload and crew co-ordination, focuses on crew activities and personnel. A series of columns are used: task; sub-task (action) description; time the sub-task begins; time the sub-task ends; and a column each for the operators involved in the whole task/scenario, indicating in each row which operators are involved in the sub-task. If an operator moves from their usual location this is noted under the column for that operator at the time it happens. The VTLA helps to identify where team co-ordination will be particularly required, and also where workload may be unevenly spread, and where human resources may be insufficient. The VTLA can also discriminate between		nuclear offshore	S3c.1			X		• [Kirwan&Kennedy& Hamblen] • [Kirwan94] • [Task Time]	KS:FC PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					actions and monitoring, and can show potential actions given other plant failures or system recoveries. Lastly, key system/transient events can be indicated on the x-axis.									
506.	Walk-Through Task Analysis	T	M	1986	This technique is a systematic analysis that should be used to determine and correct root causes of unplanned occurrences related to maintenance.	This technique is applicable to maintenance.	?	S3a.2 S3c.2	X		X	X	• [FAA00] • [EN 50128] • [Kirwan&Ainsworth 92] • [Kirwan94] • [ΣΣ93, ΣΣ97]	KS:FC PM:C
507.	Watchdog timers	T	Dh Ds	1977 or older	Aim is to provide a non-software related reliable hardware checking method of the software operation. A watchdog in computer terms is a very reliable hardware that ensures that the computer is always running. The computer has to "say hello" from time to time to the watchdog hardware to let it know that it is still alive. If it fails to do that then it will get a hardware reset. Watchdog timers are hardware devices with the capability to reset (reboot) the system should the watchdog not be periodically reset by software.	Should be used on all safety critical and real-time control systems. Related to software time-out checks.	computer	S3a.2	X	X			• [Bishop90] • Internet	PM:R PM:C
508.	What- If Analysis	T	R	1992 or older	What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence.	The technique is universally appropriate.	many	F3.2 P3.2	X		X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:F
509.	What- If/ Checklist Analysis	T	R	1992	What-If or Checklist Analysis is a simple method of applying logic in a deterministic manner.	The technique is universally appropriate.	many	F3.2 P3.2	X		X	X	• [FAA00] • [ΣΣ93, ΣΣ97]	PM:C
510.	Wind/ Tornado Analysis	T	R	1988 or older	Analysis of hazards resulting from all types of winds	All structures and buildings	nuclear	F3.2 F3.3 P3.2	X				• [ΣΣ93, ΣΣ97]	PM:R
511.	Workload Analysis (MIL)	T	H	1986 or older	Provides an appraisal of the extent of operator or crew task loading, based on the sequential accumulation of task times. Method permits an evaluation of the capability of the operator or crew to perform all assigned tasks in the time allotted by mission constraints. As capability is confirmed, hardware design requirements can be more precisely designated. If limitations are exposed, alternate function allocations and operator or crew task assignments are considered and implemented.		defence	P3.2 P3.3 P3.4 S3a.2	X		X		• [MIL-HDBK]	KS:FC PM:C
512.	WPAM (Work Process Analysis Model)	I	R	1994	Safety management assessment linked to PSA-type of approach. The first part (WPAM-I) is qualitative; basically a task analysis is performed on the work process to which the tasks involved, actions and the defences in the task, and their failure modes are investigated. Next, the organisational factors matrix is defined for each key work process. The organisational factors influencing each	A point to note about the WPAM is that it may double-count the dependence of the organisational factors, if the HEPs used have already taken into the account the underlying factors, which may at times be implicitly modelled.	nuclear	F3.1 F3.2 F3.3 P3.1 P3.2				X	• [Kennedy&Kirwan98] • [Keong97]	KS:FC PM:C

Id	Technique	Type		Age	Aim/Description	Remarks	Domains	SAM	Hw	Sw	Hu	Pr	References	For D4
					task in the given work process are then ranked according to their importance. WPAM-II is next used to modify minimal cut set frequencies to include organisational dependencies among the PSA parameters, i.e. candidate parameter group. The next step in the WPAM-II is quantification. SLIM is used to find new frequencies for each minimal cut set.									
513.	WSA (Work Safety Analysis)	T	H	1981	Systematic investigation of working methods, machines and working environments in order to find out direct accident potentials. Similar to HAZOP, but the search process is applied to work steps.	Related to Barrier Analysis, but looks more in detail at each step of the task to see what hazards could occur, and to provide a rough quantitative calculation of their relative risks, and hence what barriers are needed.	manuf	F3.2 F3.3 P3.2 P3.3	X		X		• [Kirwan&Ainsworth 92] • [Leveson95]	KS:FC PM:C
514.	Z	T	Ds	1984 ?	Specification language notation for sequential systems and a design technique that allows the developer to proceed from a Z specification to executable algorithms in a way that allows proof of their correctness with respect to the specification	Formal Method. Powerful specification notation for large systems. Commercial training available. Related to VDM. Tools available. Software requirements specification phase and design & development phase	rail	S3a.2		X			• [Bishop90] • [Cichocki&Gorski] • [EN 50128]	PM:F MC:R
515.	ZA or ZSA (Zonal (Safety) Analysis)	T	Dh	1991 ?	Used to identify sources of common cause failures and effects of components on their neighbours. Zonal Analysis 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.	Hazard identification family.	aircraft	P3.2	X				• [ARP 4761] • [DS-00-56] • [Dvorak00] • [MUFTIS3.2-I]	PM:F

4. Development of a Template format

The third phase of the project involved the development of a template format along which a selection of the techniques gathered during the second phase were to be evaluated. This template was to be formed by a list of evaluation criteria for these techniques, such as Maturity, Acceptability, Advantages, Disadvantages, etc. This section provides the details 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, with a summary in Subsection 4.3). Next, the selected set was formed into a template format (Subsection 4.4).

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 studies, and start with the evaluation criteria used by those sources. It was tried to use studies that evaluated techniques of various types.

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 the 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 meaning was different. The table is provided below.

Candidate criterion	**Meaning**	**Reference**
Acceptability to assessors	Given equal acceptance of several techniques by potential users of the results, techniques which require least resources and which have been most extensively applied are likely to be rated as the most acceptable by assessors	[Humphreys88]
Acceptability	In some cases evaluation studies of techniques have been carried	[Humphreys88]

to regulatory bodies	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 which have achieved positive evaluations will receive a higher rating on this subcriterion	
Acceptability to scientific community	This subcriterion will be influenced mainly by the theoretical rigour of a technique and the extent to which it has been subjected to objective evaluations	[Humphreys88]
Advantages	Main advantages of the technique	[MUFTIS3.2-I]
Aim	A sentence to summarise the main aim of this technique	[Bishop90]
Alternate names	Other names and specialty names are provided	[ΣΣ93]
Applicability range	Range of tasks/systems to which the technique can be applied	[Minutes SMS]
Applicability requirements	Applicability requirements within each standard; i.e. technique just recommended to be used, highly recommended, or really mandatory within that specific domain	[Minutes SMS]
Applicable to human, equipment, procedures or organisation?	Does the technique assess humans (human error, human behaviour), equipment (hardware, software, incl. HMI) or procedures/organisation?	[Minutes SMS]
Applicable to which life cycle	To which SAM lifecycle (e.g. design, definition, implementation) is the technique applicable	[Minutes SMS]
Application	Special system/subsystem/component areas to which the technique may be applicable are noted, as are processes/activities/procedures. Areas of inapplicability are also delineated, where this has been appropriate. Techniques that are especially applicable to manned systems, activities and procedures are so identified	[ΣΣ93]
Application	Is it preliminary or successive to other methods and is it a qualitative hazard analysis technique or also a quantitative technique	[MUFTIS3.2-I]
Assessment	The EWICS TC7 assessment of this technique. This may include a specific recommendation for its use on a safety-related project	[Bishop90]
Auditability	The degree to which the workings, calculations, and assumptions used (including those of the experts) during the application of the technique can be scrutinised and evaluated by auditors	[Humphreys88]
Availability	Acceptability 2: Availability of technique. This criterion indicates that the technique is either available (a rating of 'yes'), or else it is unavailable because it has been discontinued (in the case of PHECA), commercially related to one organisation (in the case of HRMS), or still at the prototype stage and not yet generally available (in the case of CES).	[Kirwan98-1]
Availability of supporting tools	Availability of commercial/non-commercial tools supporting the technique	[Minutes SMS]
Breadth of applicability	The applicability of the technique to a wide range of industry sectors and problem areas	[Humphreys88]
Character	Is the technique inductive, when determining the effect of a particular event, or deductive, when determining which cause contributes to a particular event	[MUFTIS3.2-I]
Comparative	The degree to which the results of the technique agree with those	[Humphreys88]

validity	produced by other techniques applied to the same problem (also called convergent validity)	
Compatibility	The 'innovation' is compatible with existing values, skills and work practices of potential adopters	[Minutes SMS]
Complexity	Complexity: the 'innovation' is relatively easy to understand and use	[Minutes SMS]
Comprehensive-ness	The range of task types, behaviours and types of mental processes that the technique can be applied to	[Humphreys88]
Comprehensive-ness	Comprehensiveness of human behaviour assessed: the degree to which the technique addresses skill, rule, and knowledge-based behaviour, rule violations, and errors of commission etc. [abbreviated to S, R, K, RVa, and EOC respectively]	[Kirwan98-1]
Conditions	Any pre-conditions to be met before the technique can be applied	[Bishop90]
Con's	Con's of technique or method, in the context of ATM	[Minutes SMS]
Consistency	The consistency of the use of the technique, such that if used on two occasions by independent experts, reasonably similar results are derived	[Humphreys88]
Consistency of outputs	Consistency of outputs (e.g. can results vary widely with different users)	[Minutes SMS]
Current maturity	The extent to which the technique has been developed technically and has proven itself useful in applications	[Humphreys88]
Current usage within ATM	Current usage within ATM (with examples)	[Minutes SMS]
Data requirements	The comprehensiveness and availability of the data, required by the technique, both in terms of qualitative information (about the operator task), and numerical calibration data	[Humphreys88]
Definition	Definition	[Minutes SMS]
Degree of decomposition	The degree of decomposition of the problem required by the technique, i.e. the extent to which complex task needs to be broken down into subtasks and task elements	[Humphreys88]
Description	A short description of the means used to meet the stated aims	[Bishop90]
Development potential	The degree to which the technique could be developed in the future to enhance its performance against one or more of the above criteria	[Humphreys88]
Difficulty of application	Presuming that a given technique has been adequately mastered and that its is not mis-applied, its use may produce acceptable results either with relative ease or at great expense in time and resources. Comments on these features are provided here	[ΣΣ93]
Disadvantages	Main disadvantages of the technique	[MUFTIS3.2-I]
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).	[Kirwan98-1]
Ease of combining with other technique	Does the technique easily or usually combine with particular other techniques	[Minutes SMS]
Ease of integration	Ease of integration with other ATM safety assurance approaches and tools	[Minutes SMS]
Ease of use	Does the technique need a lot of experience	[Minutes SMS]

EEM/PEM/PSF	Theoretical validity 2: whether the technique simply assesses External Error Modes (EEMs: what happened, e.g. closed wrong valve), or whether it also predicts Psychological Error Mechanisms (PEMs: how the operator failed internally, e.g. pattern recognition failure) and/or Performance Shaping Factors (PSF: situational factors that contribute to the likelihood of the error's occurrence, e.g. poor interface design; etc).	[Kirwan98-1]
Equipment and personnel resource requirements	The number of different personnel, their availability and length of their time required by the study, as well as equipment and administrative support requirements	[Humphreys88]
Experience in application to air traffic	Has the technique previously been applied in air traffic or air traffic management?	[Minutes SMS]
Expert review	The extent to which a technique has been subjected to an independent expert review process by individuals other than its developers	[Humphreys88]
Experts required	Resources 3: the requirement for an expert panel or task-domain experts. This is rated simply on a yes/no basis.	[Kirwan98-1]
Experts tool	Resources 2: training required to use the system, i.e. the degree to which it is an expert's tool. This is simply rated as yes or no, since although this criterion could be rated as low, moderate and high these judgements would be very difficult to make without having used the systems comparatively.	[Kirwan98-1]
General comments	Miscellaneous notes and precautions drawn largely from discussions with practitioners of the techniques are presented, where applicable	[ΣΣ93]
How does it help ATM safety assurance	How the methods helps ATM safety assurance	[Minutes SMS]
Layout	How does the technique work, e.g. outline of through table or graph	[MUFTIS3.2-I]
Life cycle stage?	Life cycle stage applicability: the earliest life cycle stage at which the technique can probably be applied (concept; detailed design; commissioning; and existing/operational life cycle phases).	[Kirwan98-1]
Major advantages	Reasons for adopting this technique	[Bishop90]
Mastery Required	Some techniques lend themselves to each application by the untrained novice, whereas others may require formal study and some practical experience. An attempts has been made to indicate the degree of preparation required for the successful use of each technique	[ΣΣ93]
Maturity	Is the technique mature, where maturity has two components, i.e. how long ago has it been developed, and, how often has it been used in applications.	[Minutes SMS]
Method	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	[ΣΣ93]
Model-based?	Theoretical validity 1: whether the technique is based on a model of human performance. Techniques are rated as low (indicating a classification-based system), moderate (indicating that the	[Kirwan98-1]

	technique makes reference to a model of human performance), or high (meaning that the tool is an embodiment/interpretation of a model of human performance).	
Modelling validity	The degree to which the technique explores, elicits, and incorporates modelling and general information regarding factors influencing human reliability	[Humphreys88]
Numerical accuracy	The accuracy of the final human error probability (HEP) produced, i.e. the extent to which the estimated numerical error probability approaches that derived from empirical frequency data, where the latter are available	[Humphreys88]
Observability	(Definition from Amodeus system modelling glossary): Property that the presentation of a system contains sufficient information to allow the user to determine the functional state of the system. (Definition from Everett Rogers, Diffusion of Innovations glossary of terms): Observability is the degree to which the results of an innovation are visible to others.	[Minutes SMS]
Observability	The results and benefits of use of the 'innovation' can be easily observed and communicated to others	[Minutes SMS]
Perceived validity	The degree to which the method appears reasonable and plausible to the potential user (also called face validity)	[Humphreys88]
Primary objective	Primary objective of the technique: the original purpose or function of the technique.	[Kirwan98-1]
Problems or disadvantages	Any restrictions on applicability, e.g. problem scale, generality, accuracy, ease of use, cost, availability, maturity, etc.	[Bishop90]
Pro's	Pro's of technique or method, in the context of ATM	[Minutes SMS]
Purpose	A succinct statement of the use of this process which describes when and why the technique should be used	[ΣΣ93]
Qualitative usefulness	The degree to which the technique allows specific qualitative recommendations to be made concerning ways to change human reliability if desired (for example for design purposes or cost benefit analysis)	[Humphreys88]
Quantifiable?	HEI output quantifiability: whether a special HRA quantification technique-HEI technique partnership exists between the HEI tool and e.g. Success Likelihood Index Method (SLIM: Embrey et al, 1984), Absolute Probability Judgement (APJ) or Paired Comparisons (PC: see Kirwan, 1994), or THERP, or indeed whether the error forms developed are potentially beyond quantification at this stage.	[Kirwan98-1]
References	References to the descriptions of the technique, principally text books and articles in the open literature	[Bishop90]
References	Identified here are formal publications from which descriptive information has been drawn. These references are listed elsewhere, and the rationale for their selection is described under purpose. Expert practitioners may also be cited.	[ΣΣ93]
References	References	[Minutes SMS]
References used	References to books and papers used for the assessment of the technique	[MUFTIS3.2-I]
Related methods	Alternative, overlapping or complementary techniques	[Bishop90]
Relative advantage	The 'innovation' is better (in terms of cost, functionality, image, etc) than the technology it supersedes	[Minutes SMS]

Relevance to ATM	Relevance to ATM	[Minutes SMS]
Remarks	Any other information, e.g. related techniques, alternative names	[MUFTIS3.2-I]
Resource limitations	The extent to which the technique can produce useful results with limited information or data	[Humphreys88]
Resource usage	Resource usage (including any data requirements, such as failure probabilities etc., and the availability of such data sources)	[Minutes SMS]
Resources usage	Resources 1: likely resource usage in actually applying the technique, in terms of assessor/expert time. Resources were rated as low, moderate or high, depending on the judged extent of time each technique would take to apply.	[Kirwan98-1]
Robustness to life cycle updates	Is the technique robust with respect to updates in lifecycle	[Minutes SMS]
Scope	Indication of what one obtains with application of the technique	[MUFTIS3.2-I]
Sensitivity analysis capability	The extent to which the effects of changing the input data to the technique can be evaluated, in terms of changes in the output error probabilities	[Humphreys88]
Structuredness	Consistency: in terms of the degree to which the technique is structured, and so more likely to yield consistency of results, versus a technique which is open-ended, in which case the results are likely to be highly assessor-dependent. Techniques are rated as low (meaning a relatively open-ended technique), moderate (meaning that the assessor has flexibility within a detailed framework), or high (meaning that the tool is highly structured and likely to lead different assessors down the same error identification routes, given the same information and assumptions).	[Kirwan98-1]
Theoretical validity	The degree to which the technique is consistent with current theories of human performance. Where expert judgement is utilised as part of the technique, this criterion also refers to the extent to which theories of human judgement are taken into account by the technique	[Humphreys88]
Thoroughness	By their nature, some techniques are well suited to broad, superficial studies. Others lend themselves to finely detailed, in-depth explorations. Comments on these aspects of thoroughness are provided	[ΣΣ93]
Tools	Any tools to support this technique	[Bishop90]
Training requirements	The degree of assessor knowledge/training required both in the technical context of the problem and in the use of the technique itself	[Humphreys88]
Triability	The 'innovation' can be experimented with on a trial basis without undue effort and expense; it can be implemented incrementally and still provide a net positive effect	[Minutes SMS]
Usage in PSA	Acceptability 1: PSA usage to date. This is very difficult to judge, since so little has been published on usage of the techniques. A rating of low indicates that it appears that the technique has been developed but has only been used as a prototype. A rating of moderate indicates that it appears to have been used in a small number of assessments. A rating of high indicates that it has received extensive usage.	[Kirwan98-1]
Usefulness	Usefulness: the degree to which the technique can generate *error reduction mechanisms*, irrespective of whether these are based on analysis of root causes or not. This is judged as low (little concern	[Kirwan98-1]

	of the technique with error reduction), moderate (suggesting that the technique is capable of error reduction), or high (meaning that error reduction is a primary focus of the approach, and that effective error reduction mechanisms will be generated either via detailed understanding of the error, or via sound engineering/design experience in devising alternative operational configurations of systems to avoid error opportunities). Usefulness also implicitly includes the criterion of *Diagnosticity*, here meaning the insight into the causes of the error, which allows (diagnostic) determination of error reduction measures.	
What can you assess with the technique	What can you assess with the technique	[Minutes SMS]

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 meanings 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 to compare the method or technique with other techniques
- N - The criterion does not have to be used during the detailed evaluation in the remainder of the project.

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 table below.

Id	Candidate criterion	Meaning	Reference	Use in template?

Id	Candidate criterion	Meaning	Reference	Use in template?
1a	Acceptability to assessors	Given equal acceptance of several techniques by potential users of the results, techniques which require least resources and which have been most extensively applied are likely to be rated as the most acceptable by assessors	[Humphreys88]	N
1b	Acceptability to regulatory bodies	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 which have achieved positive evaluations will receive a higher rating on this subcriterion	[Humphreys88]	E; combine 1b, 1c, 31a
1c	Acceptability to scientific community	This subcriterion will be influenced mainly by the theoretical rigour of a technique and the extent to which it has been subjected to objective evaluations	[Humphreys88]	E; combine 1b, 1c, 31a
2a	Advantages	Main advantages of the technique	[MUFTIS3.2-I]	N; is covered by 35
2b	Major advantages	Reasons for adopting this technique	[Bishop90]	N; is covered by 35
2c	Pro's	Pro's of technique or method, in the context of ATM	[Minutes SMS]	N; is covered by 35
2d	Relative advantage	The 'innovation' is better (in terms of cost, functionality, image, etc) than the technology it supersedes	[Minutes SMS]	N; is covered by 35
3a	Aim	A sentence to summarise the main aim of this technique	[Bishop90]	D; combine 3a, 3b, 3c, 3d, 3e
3b	Primary objective	Primary objective of the technique: the original purpose or function of the technique.	[Kirwan98-1]	D; combine 3a, 3b, 3c, 3d, 3e
3c	Purpose	A succinct statement of the use of this process which describes when and why the technique should be used	[ΣΣ93]	D; combine 3a, 3b, 3c, 3d, 3e
3d	Scope	Indication of what one obtains with application of the technique	[MUFTIS3.2-I]	D; combine 3a, 3b, 3c, 3d, 3e
3e	What can you assess with the technique	What can you assess with the technique	[Minutes SMS]	D; combine 3a, 3b, 3c, 3d, 3e
4a	Alternate names	Other names and specialty names are provided	[ΣΣ93]	D
4b	Ease of combining with other technique	Does the technique easily or usually combine with particular other techniques	[Minutes SMS]	E; combine 4b, 4c, 23a

Id	Candidate criterion	Meaning	Reference	Use in template?
4c	Ease of integration	Ease of integration with other ATM safety assurance approaches and tools	[Minutes SMS]	E; combine 4b, 4c, 23a
4d	Related methods	Alternative, overlapping or complementary techniques	[Bishop90]	D; combine 4d, 7a, 7b
5a	Applicable to human, equipment, procedures or organisation?	Does the technique assess humans (human error, human behaviour), equipment (hardware, software, incl. HMI) or procedures/organisation?	[Minutes SMS]	D; combine 5a, 5b, 5c
5b	Applicability range	Range of tasks/systems to which the technique can be applied	[Minutes SMS]	D; combine 5a, 5b, 5c
5c	Application	Special system/subsystem/component areas to which the technique may be applicable are noted, as are processes/activities/procedures. Areas of inapplicability are also delineated, where this has been appropriate. Techniques that are especially applicable to manned systems, activities and procedures are so identified	[ΣΣ93]	D; combine 5a, 5b, 5c
6a	Applicable to which life cycle	To which SAM lifecycle (e.g. design, definition, implementation) is the technique applicable	[Minutes SMS]	D; combine 6a, 6b
6b	Life cycle stage?	Life cycle stage applicability: the earliest life cycle stage at which the technique can probably be applied (concept; detailed design; commissioning; and existing/operational life cycle phases).	[Kirwan98-1]	D; combine 6a, 6b
7a	Application	Is it preliminary or successive to other methods and is it a qualitative hazard analysis technique or also a quantitative technique	[MUFTIS3.2-I]	D; combine 4b, 7a, 7b
7b	Quantifiable?	HEI output quantifiability: whether a special HRA quantification technique-HEI technique partnership exists between the HEI tool and e.g. Success Likelihood Index Method (SLIM: Embrey et al, 1984), Absolute Probability Judgement (APJ) or Paired Comparisons (PC: see Kirwan, 1994), or THERP, or indeed whether the error forms developed are potentially beyond quantification at this stage.	[Kirwan98-1]	D; combine 4b, 7a, 7b
8a	Assessment	The EWICS TC7 assessment of this technique. This may include a specific recommendation for its use on a safety-related project	[Bishop90]	N

Id	Candidate criterion	Meaning	Reference	Use in template?
8b	Applicability requirements	Applicability requirements within each standard; i.e. technique just recommended to be used, highly recommended, or really mandatory within that specific domain	[Minutes SMS]	N
9a	Auditability	The degree to which the workings, calculations, and assumptions used (including those of the experts) during the application of the technique can be scrutinised and evaluated by auditors	[Humphreys88]	E; combine 9a, 9b, 9d, 18a, 18c
9b	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).	[Kirwan98-1]	E; combine 9a, 9b, 9d, 18a, 18c
9c	Observability	(Definition from Amodeus system modelling glossary): Property that the presentation of a system contains sufficient information to allow the user to determine the functional state of the system. (Definition from Everett Rogers, Diffusion of Innovations glossary of terms): Observability is the degree to which the results of an innovation are visible to others.	[Minutes SMS]	N
9d	Observability	The results and benefits of use of the 'innovation' can be easily observed and communicated to others	[Minutes SMS]	E; combine 9a, 9b, 9d, 18a, 18c
10a	Availability	Acceptability 2: Availability of technique. This criterion indicates that the technique is either available (a rating of 'yes'), or else it is unavailable because it has been discontinued, commercially related to one organisation, or still at the prototype stage and not yet generally available.	[Kirwan98-1]	E; combine 10a, 11a, 11b
11a	Availability of supporting tools	Availability of commercial/non-commercial tools supporting the technique	[Minutes SMS]	E; combine 10a, 11a, 11b
11b	Tools	Any tools to support this technique	[Bishop90]	E; combine 10a, 11a, 11b
12a	Breadth of applicability	The applicability of the technique to a wide range of industry sectors and	[Humphreys88]	N

Id	Candidate criterion	Meaning	Reference	Use in template?
		problem areas		
13a	Character	Is the technique inductive, when determining the effect of a particular event, or deductive, when determining which cause contributes to a particular event	[MUFTIS3.2-I]	N
14a	Comparative validity	The degree to which the results of the technique agree with those produced by other techniques applied to the same problem (also called convergent validity)	[Humphreys88]	N
15a	Comprehensive-ness	Comprehensiveness of human behaviour assessed: the degree to which the technique addresses skill, rule, and knowledge-based behaviour, rule violations, and errors of commission etc. [abbreviated to S, R, K, RVa, and EOC respectively]	[Kirwan98-1]	N
15b	Comprehensive-ness	The range of task types, behaviours and types of mental processes that the technique can be applied to	[Humphreys88]	N
16a	Compatibility	The 'innovation' is compatible with existing values, skills and work practices of potential adopters	[Minutes SMS]	N
17a	Conditions	Any pre-conditions to be met before the technique can be applied	[Bishop90]	N
17b	Data requirements	The comprehensiveness and availability of the data, required by the technique, both in terms of qualitative information (about the operator task), and numerical calibration data	[Humphreys88]	N
17c	Experts required	Resources 3: the requirement for an expert panel or task-domain experts. This is rated simply on a yes/no basis.	[Kirwan98-1]	N
18a	Consistency	The consistency of the use of the technique, such that if used on two occasions by independent experts, reasonably similar results are derived	[Humphreys88]	E; combine 9a, 9b, 9d, 18a, 18c
18b	Consistency of outputs	Consistency of outputs (e.g. can results vary widely with different users)	[Minutes SMS]	N

Id	Candidate criterion	Meaning	Reference	Use in template?
18c	Structuredness	Consistency: in terms of the degree to which the technique is structured, and so more likely to yield consistency of results, versus a technique which is open-ended, in which case the results are likely to be highly assessor-dependent. Techniques are rated as low (meaning a relatively open-ended technique), moderate (meaning that the assessor has flexibility within a detailed framework), or high (meaning that the tool is highly structured and likely to lead different assessors down the same error identification routes, given the same information and assumptions).	[Kirwan98-1]	E; combine 9a, 9b, 9d, 18a, 18c
19a	Current maturity	The extent to which the technique has been developed technically and has proven itself useful in applications	[Humphreys88]	E
19b	Maturity	Is the technique mature, where maturity has two components, i.e. how long ago has it been developed, and, how often has it been used in applications.	[Minutes SMS]	N
19c	Usage in PSA	Acceptability 1: PSA usage to date. This is very difficult to judge, since so little has been published on usage of the techniques. A rating of low indicates that it appears that the technique has been developed but has only been used as a prototype. A rating of moderate indicates that it appears to have been used in a small number of assessments. A rating of high indicates that it has received extensive usage.	[Kirwan98-1]	N
20a	Degree of decomposition	The degree of decomposition of the problem required by the technique, i.e. the extent to which complex task needs to be broken down into subtasks and task elements	[Humphreys88]	N
21a	Definition	Definition	[Minutes SMS]	D; combine 21a, 21b, 21c, 21d, 30b
21b	Description	A short description of the means used to meet the stated aims	[Bishop90]	D; combine 21a, 21b, 21c, 21d, 30b
21c	Layout	How does the technique work, e.g. outline of through table or graph	[MUFTIS3.2-I]	D; combine 21a, 21b, 21c, 21d, 30b

Id	Candidate criterion	Meaning	Reference	Use in template?
21d	Method	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	[ΣΣ93]	D; combine 21a, 21b, 21c, 21d, 30b
22a	Development potential	The degree to which the technique could be developed in the future to enhance its performance against one or more of the above criteria	[Humphreys88]	N
23a	Complexity	Complexity: the 'innovation' is relatively easy to understand and use	[Minutes SMS]	E; combine 4b, 4c, 23a
23b	Difficulty of application	Presuming that a given technique has been adequately mastered and that its is not mis-applied, its use may produce acceptable results either with relative ease or at great expense in time and resources. Comments on these features are provided here	[ΣΣ93]	N
23c	Ease of use	Does the technique need a lot of experience	[Minutes SMS]	N
23d	Experts tool	Resources 2: training required to use the system, i.e. the degree to which it is an expert's tool. This is simply rated as yes or no, since although this criterion could be rated as low, moderate and high these judgements would be very difficult to make without having used the systems comparatively.	[Kirwan98-1]	N
23e	Mastery required	Some techniques lend themselves to each application by the untrained novice, whereas others may require formal study and some practical experience. An attempts has been made to indicate the degree of preparation required for the successful use of each technique	[ΣΣ93]	N
23f	Training requirements	The degree of assessor knowledge/training required both in the technical context of the problem and in the use of the technique itself	[Humphreys88]	N
24a	Con's	Con's of technique or method, in the context of ATM	[Minutes SMS]	E; combine 24a, 24b, 24c, 26b, 26c
24b	Disadvantages	Main disadvantages of the technique	[MUFTIS3.2-I]	E; combine 24a, 24b, 24c, 26b, 26c

Id	Candidate criterion	Meaning	Reference	Use in template?
24c	Problems or disadvantages	Any restrictions on applicability, e.g. problem scale, generality, accuracy, ease of use, cost, availability, maturity, etc.	[Bishop90]	E; combine 24a, 24b, 24c, 26b, 26c
25a	EEM/PEM/PSF	Theoretical validity 2: whether the technique simply assesses External Error Modes (EEMs: what happened, e.g. closed wrong valve), or whether it also predicts Psychological Error Mechanisms (PEMs: how the operator failed internally, e.g. pattern recognition failure) and/or Performance Shaping Factors (PSF: situational factors that contribute to the likelihood of the error's occurrence, e.g. poor interface design; etc).	[Kirwan98-1]	N
25b	Thoroughness	By their nature, some techniques are well suited to broad, superficial studies. Others lend themselves to finely detailed, in-depth explorations. Comments on these aspects of thoroughness are provided	[ΣΣ93]	N
26a	Equipment and personnel resource requirements	The number of different personnel, their availability and length of their time required by the study, as well as equipment and administrative support requirements	[Humphreys88]	N
26b	Resources usage	Resources 1: likely resource usage in actually applying the technique, in terms of assessor/expert time. Resources were rated as low, moderate or high, depending on the judged extent of time each technique would take to apply.	[Kirwan98-1]	E; combine 24a, 24b, 24c, 26b, 26c
26c	Resource usage	Resource usage (including any data requirements, such as failure probabilities etc., and the availability of such data sources)	[Minutes SMS]	E; combine 24a, 24b, 24c, 26b, 26c
27a	Experience in application to air traffic	Has the technique previously been applied in air traffic or air traffic management?	[Minutes SMS]	D; combine 27a, 27b
27b	Current usage within ATM	Current usage within ATM (with examples)	[Minutes SMS]	D; combine 27a, 27b
28a	Expert review	The extent to which a technique has been subjected to an independent expert review process by individuals other than its developers	[Humphreys88]	N
29a	General comments	Miscellaneous notes and precautions drawn largely from discussions with practitioners of the techniques are presented, where applicable	[ΣΣ93]	N
29b	Remarks	Any other information, e.g. related techniques, alternative names	[MUFTIS3.2-I]	N

Id	Candidate criterion	Meaning	Reference	Use in template?
30a	Model-based?	Theoretical validity 1: whether the technique is based on a model of human performance. Techniques are rated as low (indicating a classification-based system), moderate (indicating that the technique makes reference to a model of human performance), or high (meaning that the tool is an embodiment/interpretation of a model of human performance).	[Kirwan98-1]	N
30b	Modelling validity	The degree to which the technique explores, elicits, and incorporates modelling and general information regarding factors influencing human reliability	[Humphreys88]	D; combine 21a, 21b, 21c, 21d, 30b
31a	Numerical accuracy	The accuracy of the final human error probability (HEP) produced, i.e. the extent to which the estimated numerical error probability approaches the one derived from empirical frequency data, where the latter are available	[Humphreys88]	E; combine 1b, 1c, 31a
32a	Perceived validity	The degree to which the method appears reasonable and plausible to the potential user (also called face validity)	[Humphreys88]	N
33a	Qualitative usefulness	The degree to which the technique allows specific qualitative recommendations to be made concerning ways to change human reliability if desired (for example for design purposes or cost benefit analysis)	[Humphreys88]	E; combine 33a, 35a, 35b, 36a
34a	References	References to the descriptions of the technique, principally text books and articles in the open literature	[Bishop90]	D; combine 34a, 34b, 34c, 34d
34b	References	Identified here are formal publications from which descriptive information has been drawn. These references are listed elsewhere, and the rationale for their selection is described under purpose. Expert practitioners may also be cited.	[ΣΣ93]	D; combine 34a, 34b, 34c, 34d
34c	References used	References to books and papers used for the assessment of the technique	[MUFTIS3.2-I]	D; combine 34a, 34b, 34c, 34d
34d	References	References	[Minutes SMS]	D; combine 34a, 34b, 34c, 34d
35a	Relevance to ATM	Relevance to ATM	[Minutes SMS]	E; combine 33a, 35a, 35b, 36a
35b	How does it help ATM safety assurance	How the methods helps ATM safety assurance	[Minutes SMS]	E; combine 33a, 35a, 35b, 36a
36a	Resource limitations	The extent to which the technique can produce useful results with limited	[Humphreys88]	E; combine 33a, 35a,

Id	Candidate criterion	Meaning	Reference	Use in template?
		information or data		35b, 36a
37a	Robustness to life cycle updates	Is the technique robust with respect to updates in lifecycle	[Minutes SMS]	N
38a	Sensitivity analysis capability	The extent to which the effects of changing the input data to the technique can be evaluated, in terms of changes in the output error probabilities	[Humphreys88]	N
39a	Theoretical validity	The degree to which the technique is consistent with current theories of human performance. Where expert judgement is utilised as part of the technique, this criterion also refers to the extent to which theories of human judgement are taken into account by the technique	[Humphreys88]	N
40a	Triability	The 'innovation' can be experimented with on a trial basis without undue effort and expense; it can be implemented incrementally and still provide a net positive effect	[Minutes SMS]	N
41a	Usefulness	Usefulness: the degree to which the technique can generate *error reduction mechanisms*, irrespective of whether these are based on analysis of root causes or not. This is judged as low (little concern of the technique with error reduction), moderate (suggesting that the technique is capable of error reduction), or high (meaning that error reduction is a primary focus of the approach, and that effective error reduction mechanisms will be generated either via detailed understanding of the error, or via sound engineering/design experience in devising alternative operational configurations of systems to avoid error opportunities). Usefulness also implicitly includes the criterion of *Diagnosticity*, here meaning the insight into the causes of the error, which allows (diagnostic) determination of error reduction measures.	[Kirwan98-1]	N; since covered by 35a

4.3 Selected evaluation criteria for template

The following table provides the list of evaluation criteria, together with their definitions, that have been given assessment type ‘E’ in the previous subsection. These criteria will be used in the template format of the Safety Methods Survey project. The template evaluation criteria are at this stage equally weighted, and are therefore not in any priority order.

Template	Definition	Combination

evaluation criterion		of which criteria
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 which 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.	1b, 1c, 31a
Availability and tool support	This criterion indicates that the technique is either available (a rating of 'yes'), 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 (yes/no) of computer tools that can support application of the technique.	10a, 11a, 11b
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.	24a, 24b, 24c, 26b, 26c
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.	9a, 9b, 9d, 18a, 18c
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	4b, 4c, 23a
Maturity	The extent to which the technique has been developed technically and has proven itself useful in applications.	19a
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.	33a, 35a, 35b, 36a

The following table provides the list of evaluation criteria, together with their definitions, that have been given assessment type 'D' in the previous subsection. These criteria will also be used in the template format of the Safety Methods Survey project, but not to compare techniques but rather to describe them. Again, these template evaluation criteria are equally weighted, and are therefore not in any priority order.

Template	Definition	Combination

descriptive criterion		of which criteria
Alternate names	Other names and specialty names are provided	4a
Applicability range	Does the technique assess humans (human error, human behaviour), equipment (hardware, software, incl. HMI) or procedures/organisation?	5a, 5b, 5c
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	21a, 21b, 21c, 21d, 30b
Experience in application to air traffic	Has the technique previously been applied in air traffic or air traffic management?	27a, 27b
Life cycle stage?	Life cycle stage applicability: the earliest Ground ANS life cycle stage at which the technique can probably be applied (concept; detailed design; commissioning; and existing/ operational life cycle phases).	6a, 6b
Primary objective	Primary objective of the technique: the original purpose or function of the technique.	3a, 3b, 3c, 3d, 3e
References used	References to books and papers used for the assessment of the technique	34a, 34b, 34c, 34d
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.	4d, 7a, 7b

4.4 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 Ground ANS life cycle stage at which the technique can probably be applied (definition; design; implementation; operations and maintenance; decommissioning).
Experience in application to air	Has the technique previously been applied in air traffic or air traffic management?

traffic:	
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. Safety Techniques Workshop

This section provides details on the process followed and the results obtained during the Safety Techniques Workshop for the Safety Methods Survey project on 4 and 5 December 2002 in Amsterdam.

5.1 Introduction

The aim of the Safety Techniques Workshop was to select, from the complete list of about 500 candidate techniques collected during WP2 of the project, about 20 techniques that would be evaluated in more detail along a template format during WP4. The main input for the workshop was a paper providing this complete list of techniques collected, but without most of the details and with the techniques ordered in a special way as explained below. Note that this list of candidate techniques was an earlier version than the list of candidate techniques provided in Section 3 of this Technical Annex. In fact, the table in Section 3 includes some additional techniques that were identified during the workshop. For this input paper, each technique had been assessed on two issues (note that these assessments are provided in Section 3 of this Technical Annex, in the third and fourth columns of the table):

First issue: specifies whether the technique is a
- (D) Database,
- (G) Generic term,
- (M) Mathematical model,
- (T) specific Technique,
- (I) Integrated method of more than one technique.

Second issue: specifies whether the technique is a
- (R) Risk assessment technique,
- (H) Human performance analysis technique,
- (M) hazard Mitigation technique,
- (T) Training technique,
- (Dh) hardware Dependability technique,
- (Ds) software Dependability technique.

Next, all techniques are grouped according to their issue types, as follows

Group		**First issue**	**Second issue**	**# elements in group**
1	Databases	D	any	5
2	Generic terms	G	any	77
3	Mathematical models	M	any	29
4	Techniques and integrated methods; both hardware and software dependability, or hardware only	I or T	Dh+Ds or Dh	49
5	Techniques and integrated methods; software dependability	I or T	Ds	83
6	Techniques; Risk assessment	T	R	96

7	Techniques; Human performance	T	H	79
8	Techniques; hazard Mitigation	T	M or T	32
9	Integrated methods, except for dependability	I	R or H or M or T	54

For each group its techniques were listed in a table, with their group type provided in an additional column. Also, the ages (dates of 'birth') of the techniques (if known) were provided in a column. Within a group, the techniques were ordered on age, the oldest techniques first.

Before the workshop, EUROCONTROL staff had given an early assessment on whether techniques are useful to be evaluated along a template format during the next phase of the project. Here, a technique was considered useful if it could support one or more steps of the EATMP Safety Assessment Methodology SAM. These assessments were included in an additional column in the tables of candidate techniques (column "Candidate?"), where PM, MC and KS are the abbreviated names of the EUROCONTROL assessors, and the possible assessments are:

F: Consider Further
C: Cluster with other techniques and select one technique from the cluster
R: Remove: do not consider further in the remainder of the project

During the Safety Techniques Workshop, these assessments were used, together with additional support from EUROCONTROL and NLR expert staff, to come to a final evaluation of all techniques. This evaluation was done in sessions, each session covering one or more groups as listed in the table above. In total, nine experts participated in the workshop, but the team differed per session, based on expertise required for the group of techniques to be assessed.

Note that during the workshop, some techniques were given another type, hence should be moved to another group. This moving has not been done in the subsections below, in order to preserve the original order and numbering of the techniques. Also, after the workshop, during the writing of the final report, it appeared that the indicated Ages of several techniques needed to be updated. These changes have been made below, but the order of the techniques has not been updated according to their updated chronology.

The evaluation led to the following list of selected techniques:

Id	**Technique**	**Type**		**Age**	**Candidate?**	**Workshop evaluation**
-	Use of Expert Judgement	G				New technique in Group 2. This technique will incorporate at least APJ (nr 351) and PC (nr 345).
113	FMECA (Failure Mode Effect and Criticality Analysis)	T	Dh	1967	PM:F KS:FC	
142	RCM (Reliability Centered Maintenance)	T	Dh	1990	PM:C	Eurocontrol staff will check after the workshop if this technique is worth a template.
145	HSIA (Hardware/Software Interaction Analysis)	T	Dh	1991 or older	PM:R	Selected only if sufficient references can be found. If not selected, then a general subsection in [D5 Main Document] will be dedicated to

Id	Technique	Type		Age	Candidate?	Workshop evaluation
						it.
178	SFTA (Software Fault Tree Analysis)	T	Ds	1984 or older	PM:C MC:FC	Either this one or SMHA (nr 189) is selected.
189	SMHA (State Machine Hazard Analysis)	T	Ds	1987	PM:C	Either this one or SFTA (nr 178) is selected.
210	SFMEA (Software Failure Modes and Effects Analysis)	T	Ds	1979	PM:C	
250	FTA (Fault Tree Analysis)	T	R	1961	PM:F MC:C KS:F	
273	ETA (Event Tree Analysis)	T	R	1980	PM:F MC:F KS:FC	
282	CCA (Common Cause Analysis)	T	R	1987	PM:F KS:F	
299	External Events Analysis	T	R	1992 or older	PM:R	
326	Operational Readiness Review	T	R	1997 or older	KS:F PM:R	
334	HTRR (Hazard Tracking and Risk Resolution)	T	R	2000 or older	PM:C	
339	Bias and Uncertainty assessment	T	R	2002		Selected with addition of sensitivity analysis
341	Human Factors Case	T	H		KS:F	
346	HTA (Hierarchical Task Analysis)	T	H	1971	KS:FC PM:R	
363	HEART (Human Error Assessment and Reduction Technique)	T	H	1985	KS:FC PM:C	
-	Human Error Data Collection	T	H			New technique in Group 7.
427	HAZOP (Hazard and Operability study)	T	M	1974	PM:F MC:F KS:F	
449	Bow-Tie	T	M	1998 or older	PM:F MC:F KS:F	
500	TRACEr (Technique for the Retrospective Analysis of Cognitive Errors in Air Traffic Management)	I	H	1999	PM:C KS:FC	

One may notice that four techniques (i.e. RCM, HSIA, SFTA, and SMHA) were only provisionally selected during the workshop. After the workshop it was decided that RCM and SMHA would be selected, and HSIA and SFTA would not.

The evaluation process details are provided in the subsections below.

5.2 Selection process of techniques from Group 1

Group 1 consisted of Databases. The number of elements was 5. The techniques in this group were evaluated one by one, without clustering first.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
1	HPED (Human Performance Events Database)	D			PM:R	To be considered for SAFMOD and SAFBUILD
2	Library of Trusted, Verified Modules and Components	D			PM:R	To be considered for SAFMOD and SAFBUILD
3	SATORE	D			KS:FC PM:R	To be considered for SAFMOD and SAFBUILD
4	CHIRP (Confidential Human Factor Incident Reporting Programme)	D		1982	KS:F PM:R	To be considered for SAFMOD and SAFBUILD
5	CORE-DATA (Computerised Human Error Database for Human Reliability Support)	D		1992 from	KS:F PM:C	To be considered for SAFMOD and SAFBUILD. Can also be linked to Human Error Data Collection (new technique in Group 7)

The following databases were newly identified for this list:

	BASIS	D				To be considered for SAFMOD and SAFBUILD
	ASRS (Aviation Safety Reporting System)	D				To be considered for SAFMOD and SAFBUILD
	NLR Air Safety Database	D				To be considered for SAFMOD and SAFBUILD
	TOPAZ hazard database	D				To be considered for SAFMOD and SAFBUILD
	ESC-AIRS	D				To be considered for SAFMOD and SAFBUILD

Also, the following techniques appeared in other groups and should be moved to this group:

9	Data Recording and Analysis	D			PM:C	To be considered for SAFMOD and SAFBUILD
401	SRS-HRA (Savannah River Site Human Reliability Analysis)	D		1994	KS:R PM:R	To be considered for SAFMOD and SAFBUILD
466	ASP (Accident Sequence Precursor)	D		1979	KS:FC PM:C	To be considered for SAFMOD and SAFBUILD

The workshop also concluded that a section on databases and their importance for safety assessment should be added to the final deliverable [D5 Main Document].

5.3 Selection process of techniques from Group 2

Group 2 consisted of Generic terms rather than specific techniques. The number of elements was 77. The techniques in this group were evaluated one by one, without clustering first.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
6	Brainstorming	G			PM:R KS:FC	Link to HAZOP (nr 427)
7	Code Inspection Checklists (including coding standards)	G			PM:C MC:R	Not selected
8	Conduct Hazard Risk Assessment	G			PM:C	Not selected
9	Data Recording and Analysis	D			PM:C	Move to Group 1. To be considered for SAFMOD and SAFBUILD
10	Design and Coding Standards	G			PM:C	Not selected
11	Emergency Exercises	G			PM:R	To be considered for SAFBUILD. Link to TRM (nr 503)
12	Ergonomics Checklists	G		1992 or older	KS:FC PM:R	Link to Human Factors Case (nr 341)
13	Event and Causal Factor Charting	G			PM:C	Not selected
14	Fire Hazards Analysis	G			PM:R	Not selected
15	Gain scheduling	G			PM:R	Not selected
16	Hazard Analysis	G			PM:C	Not selected
17	HEA (Human Error Analysis)	G			KS:FC PM:C	Not selected
18	HPRA (Human Performance Reliability Analysis)	G			KS:F PM:C	Not selected
19	HRA (Human Reliability Analysis)	G			KS:F PM:C	Not selected
20	Human Factors Analysis	G			KS:FC PM:C	Not selected
21	Impact Analysis	G			PM:C	Not selected
22	Interface testing	G			PM:C	Not selected
23	Measurement of Complexity	G			KS:FC PM:C	Not selected
24	Metrics	G			PM:C	Not selected
25	Modelling / Simulation	G			PM:R	To be considered for SAFBUILD and SAFSIM
26	Organisational learning	G			KS:F PM:R	Not selected. Name may change.
27	Probabilistic Hazard Analysis	G			PM:C	Not selected
28	Process simulation	G			PM:C	Not selected
29	Prototyping or Animation	G			PM:R	Link to Modelling/Simulation (nr 25)
30	Rule violation techniques	G			PM:R	Link to Error of Commission (e.g. nr 405). To be considered for SAFMOD.
31	Safety Review, Safety Audit	G			KS:FC PM:C	Not selected
32	Software configuration management	G			PM:R	Not selected
33	Stress Reduction	G			PM:C	Not selected
34	Structured Methodology	G			PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
35	Systematic Inspection	G			PM:C	Not selected
36	Test Coverage	G			PM:C	Not selected
37	Tests based on the Specification	G			PM:C	Not selected
38	Translator Proven in Use	G			PM:R	Not selected
39	Uncertainty Analysis	G			PM:C	Not selected
40	Factor Analysis	G		1900	KS:R PM:R	Not selected
41	Link Analysis	M		1959	KS:FC PM:R	This technique will be split up into two different techniques with the same name. One of these will be moved to Group 3 and is not selected. The other one (with the Kirwan references) will be moved to Group 7 and is linked to HTA (nr 346)
42	Performance Modelling	G		1961 or older	PM:F	Not selected
43	Object-oriented Design and Programming	G		1966 or older	PM:C	Not selected
44	Design for Testability (Hardware)	G		1969	PM:C	Not selected
45	Program Proving	G		1969 or older	PM:C	Not selected
46	Structured Interviews	G		1972 or older	PM:R	Not selected
47	Input-output (block) diagrams	G		1974	KS:FC PM:R	Not selected
48	Table-top analysis	G		1974	KS:FC PM:C	Not selected
49	Data Security	G		1975 or older	PM:C	Link to External Events Analysis (nr 299)
50	Questionnaires	G		1975 or older	PM:R KS:FC	Link to Use of expert Judgement (new technique in Group 2)
51	Assertions and plausibility checks	G		1976 or older	PM:C	Not selected
52	Inspections and Walkthroughs	G		1976 or older	PM:C KS:FC	Not selected
53	Structured Programming	G		1976 or older	PM:C	Not selected
54	Tests based on Realistic data	G		1976 or	PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
				older		
55	Tests based on Software structure	G		1976 or older	PM:C	Not selected
56	Interface Surveys	G		1977	KS:FC PM:R	Link to Human Factors Case (nr 341)
57	Computer modelling and simulation	G		1978 or older	PM:F KS:FC	Link to Modelling / Simulation (nr 25)
58	Self testing and Capability testing	G		1978 or older	PM:R	Not selected
59	Configuration Management	G		1980 about	PM:R MC:R	Not selected
60	Design for Testability (Software)	G		1980 or older	PM:C	Not selected
61	Simulators/mock-ups	G		1981 or older	KS:F PM:R	Link to Modelling / Simulation (nr 25)
62	Prototype Development or Prototyping	G		1982 or older	PM:R	Link to Modelling / Simulation (nr 25)
63	Verification and Validation	G		1982 or older	PM:R	Not selected
64	Strongly Typed Programming Languages	G		1983 or older	PM:C	Not selected
65	Quality Assurance	G		1984 or older	PM:R	Not selected
66	Tests based on Random Data	G		1984 or older	PM:C	Not selected
67	SWHA (Software Hazard Analysis)	G	Ds	1984 or older	PM:C	Not selected
68	Mission Analysis	G		1986 or older	PM:F	Not selected
69	Mission Profile	G		1986 or older		Not selected
70	Mission Scenarios	G		1986 or older		Not selected
71	Analysable Programs	G		1987 or older	PM:C	Not selected
72	Avoidance of complexity	G		1987	PM:C	Not selected
73	Defensive Programming	G		1988 or older	PM:C	Not selected
74	Formally Designed Hardware	G		1988	PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
				or older		
75	Process Hazard Analysis	G	M	1989 or older	PM:R	Not selected
76	Development Standards	G		1990 or older	PM:C	Not selected
77	Electromagnetic Protection	G		1990 or older	PM:R	Not selected
78	Observational Techniques	G		1990	PM:R	Link to Human Error Data Collection (new technique in Group 7)
79	Specification Analysis	G	Ds	1990 or older	PM:C	Not selected
80	Accident Analysis	G		1992 or older	PM:C MC:F KS:R	Not selected
81	Causal Networks	G		1940 or older	KS:FC PM:R	Not selected
82	Multiple Agent Based Modelling	G		2001		To be considered for SAFBUILD requirements engineering

The following techniques were newly identified for this list:

	Use of Expert Judgement	G				**SELECTED.** Will include at least the techniques APJ (nr 351) and PC (nr 345)

The following techniques appeared in another group and should be moved to this group:

296	NDI (Non-Destructive Inspection technique)	G		1914-1918 war	PM:R	Not selected.
419	Delphi Knowledge Elicitation Method or Delphi Method	G		1950 about	KS:FC PM:C	Link to Use of Expert Judgement (new technique in Group 2)

5.4 Selection process of techniques from Group 3

Group 3 consisted of Mathematical models. The number of elements was 29. The techniques in this group were evaluated one by one, without clustering first.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
83	Finite State semi-Markov	M				A section in [D5 Main

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	processes					Document] will be dedicated to the use of mathematical models
84	Formal Methods	M			MC:FC PM:C	A section in [D5 Main Document] will be dedicated to the use of mathematical models
85	Gas model	M			PM:R	Not selected
86	Generalised gas model	M			PM:R	Not selected
87	HSMP (Hybrid-State Markov Processes)	M			PM:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models
88	Importance Sampling	M			PM:C	A section in [D5 Main Document] will be dedicated to the use of mathematical models
89	Littlewood	M		1957	PM:R	Not selected
90	Littlewood-Verrall	M		1957	PM:R	Not selected
91	MMAC (Multiple Model Adaptive Control)	M		1977	PM:R	Not selected
92	MMFC (Multiple Model Fuzzy Control)	M		1998	PM:R	Not selected
93	Musa models	M			PM:R	Not selected
94	Petri net extensions	M			PM:C MC:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models
95	Semi-Markov Chains	M			PM:C	A section in [D5 Main Document] will be dedicated to the use of mathematical models
96	Monte Carlo Simulation	M		1777	PM:F	A section in [D5 Main Document] will be dedicated to the use of mathematical models
97	Neural networks	M		1958-1985 about	PM:R	Not selected
98	Markov Chains or Markov Modelling	M		1910 about	PM:F	A section in [D5 Main Document] will be dedicated to the use of mathematical models
99	Fuzzy Logic	M		1960	PM:C	A section in [D5 Main Document] will be dedicated to the use of mathematical models
100	Finite State Machines	M		1962	PM:C MC:FC	A section in [D5 Main Document] will be dedicated to the use of mathematical models
101	Petri Net Analysis	M		1962	KS:F MC:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models
102	Absorbing boundary model	M		1964	PM:R	Not selected
103	Error Detecting and Correcting Codes	M		1975 or older	PM:C MC:R	Not selected
104	DES (Discrete Event Simulation)	M		1982 about ?	PM:C	A section in [D5 Main Document] will be dedicated to

Id	Technique	Type		Age	Candidate?	Workshop evaluation
						the use of mathematical models
105	Piecewise Deterministic Markov Processes	M		1984		A section in [D5 Main Document] will be dedicated to the use of mathematical models
106	IMM (Interacting Multiple Model algorithm)	M		1988	PM:R	Not selected
107	Stochastic Differential Equations in ATM	M		1990		A section in [D5 Main Document] will be dedicated to the use of mathematical models
108	SSG (State Space Graphs (or Discrete State Space Graphs))	M		1991 or older	PM:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models
109	Hybrid Automata	M		1993	PM:R MC:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models
110	Dynamically Coloured Petri Nets	M		1997	MC:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models
111	CGHDS (Controlled General Hybrid Dynamical System)	M		1998	PM:R MC:R	A section in [D5 Main Document] will be dedicated to the use of mathematical models

The following techniques were newly identified for this list:

	Bayesian Belief Networks	M				A section in [D5 Main Document] will be dedicated to the use of mathematical models

Also, the following techniques appeared in other groups and should be moved to this group:

41	Link Analysis	M		1959	KS:FC PM:R	Not selected
404	SPN (Synchronised Petri Network)	M		1994 or older	PM:R	This technique will be merged with Petri Net Extensions (nr 94)

5.5 Selection process of techniques from Group 4

Group 4 consisted of Techniques and Integrated methods of techniques, which considered both hardware and software dependability, or hardware dependability only. The number of elements was 49. The techniques in this group were evaluated one by one, without clustering first.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
112	Signal Flow Graphs	T	Dh	1966	PM:R MC:R	Not selected
113	FMECA (Failure Mode Effect and Criticality Analysis)	T	Dh	1967	PM:F KS:FC	**SELECTED.**
114	N out of M vote, Adaptive	T	Dh	1971?	PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	voting					
115	Network Logic Analysis	T	Dh	1972 or older	PM:C	Not selected
116	AoA (Analysis of Alternatives)	T	Dh	1975	PM:R	Not selected
117	GO charts	T	Dh	1975	PM:C	Link to FTA (nr 250)
118	FMEA (Failure Mode and Effect Analysis) or SFMEA (Systems Failure Mode and Effect Analysis)	T	Dh	1949	PM:F KS:FC	Link to FMECA (nr 113)
119	SADT (Structured Analysis and Design Technique)	T	Dh	1977	KS:FC PM:C MC:R	Not selected
120	Watchdog timers	T	Dh Ds	1977 or older	PM:R PM:C	Not selected
121	BPA (Bent Pin Analysis)	T	Dh	1979	PM:C	Not selected
122	CFMA (Cable Failure Matrix Analysis)	T	Dh	1979	PM:R MC:R	Not selected
123	FAST (Functional Analysis System Technique)	T	Dh	1973	KS:R PM:C	Not selected
124	SPFA (Single-Point Failure Analysis)	T	Dh	1980	PM:F	Not selected
125	Laser Safety Analysis	T	Dh	1980 or older	PM:R MC:R	Not selected
126	Redundancy for Fault Detection	T	Dh	1980?	PM:C	Not selected
127	Parts Count method	T	Dh	1981	PM:R	Not selected
128	N out of M vote	T	Dh	1981?	PM:F	Not selected
129	Flow Analysis	T	Dh	1982 or older	PM:C	Not selected
130	Failure Tracking	T	Dh Ds	1983 or older	PM:C	Link to HTRR (nr 334)
131	Fault Isolation Methodology	T	Dh	1985	MC:C PM:F	Not selected
132	Hardware/ Software Safety Analysis	T	Dh Ds	1985 or older	PM:C	Not selected
133	Temporal Logic	T	Dh Ds	1986 or older	PM:C MC:FC	Not selected
134	FPC (Flow Process Chart)	T	Dh	1986 or older	PM:C	Not selected
135	Functional Flow Diagram	T	Dh	1986 or older	PM:F	Link to FTA (nr 250)
136	SOM (Systems Development by an Object-oriented Methodology)	I	Dh Ds	1987 or older	PM:C	Not selected
137	Materials Compatibility Analysis	T	Dh	1988 or older	PM:R	Not selected
138	OMOLA	T	Dh	1989	PM:R	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
139	SPC (Statistical Process Control)	T	Dh	1920s	PM:R	Not selected
140	Certificated Hardware Components	T	Dh	1990 or older	PM:C	Not selected
141	Control Flow Checks or Control Flow Analysis	T	Dh	1990 or older	MC:R PM:C	Not selected
142	RCM (Reliability Centred Maintenance)	T	Dh	1990	PM:C	Provisionally **SELECTED.**
143	TTM (Truth Table Method)	T	Dh	1991 or older	PM:C MC:R	Not selected
144	GFCM (Gathered Fault Combination Method)	T	Dh	1991 or older	PM:C	Link to FMECA (nr 113)
145	HSIA (Hardware/Software Interaction Analysis)	T	Dh	1991 or older	PM:R	Provisionally **SELECTED.**
146	RIAN	T	Dh	1991 or older	PM:R	Not selected
147	ZA (Zonal Analysis)	T	Dh	1991?	PM:F	Link to CCA (nr 282). Merge with Zonal Safety Analysis (nr 155)
148	FHA (Functional Hazard Analysis)	T	Dh	1992 or older	KS:R PM:R	Not selected
149	Relative Ranking	T	Dh	1992 or older	PM:R	Not selected
150	IDEF (Integrated Computer-Aided Manufacturing Definition)	I	Dh	1993	KS:FC PM:R	To be considered for SAFBUILD
151	SHA (System Hazard Analysis)	T	Dh	1993 or older	PM:C	Link to External Events Analysis (nr 299)
152	ARP 4761 (Aerospace Recommended Practice)	I	Dh Ds	1994	PM:F	Not selected
153	JAR 25	I	Dh	1994 or older	PM:R	Not selected
154	FMES (Failure Modes and Effects Summary)	T	Dh	1994 or older	PM:C	Link to FMECA (nr 113)
155	ZSA (Zonal Safety Analysis)	T	Dh	1994 or older	PM:C	Link to CCA (nr 282). Merge with Zonal Analysis (nr 147)
156	Hazard Indices	T	Dh	1995 or older	PM:R	Not selected
157	Interface Analysis, Interdependence Analysis	T	Dh	1995 or older	PM:F	Link to External Events Analysis (nr 299)
158	HMEA (Hazard Mode Effects Analysis)	T	Dh	1997 or older	PM:C	Link to FMECA (nr 113)
159	ED-78A (RTCA/EUROCAE ED-78A DO-264)	I	Dh	2000	PM:R	Not selected
160	ObjectGEODE	I	Ds	2001 or older	PM:R MC:FC	Moved to Group 5. Not selected

5.6 Selection process of techniques from Group 5

Group 5 consisted of Techniques and Integrated methods of techniques, which considered software dependability. The number of elements was 83. The techniques in this group were evaluated as follows: First, all techniques that were obviously not selected (based on pre-workshop assessments by EUROCONTROL staff) were labelled Not selected. The remaining techniques were next grouped into the following clusters:

R Requirements
D Design
V Verification and Testing
I Integration
H Hazard identification / link with System Safety Assessment
M Maintenance

Next, each cluster was considered separately and one (or no) techniques were selected from each cluster.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
161	Invariant Assertions	T	Ds	1967 or older	PM:R MC:R	Not selected
162	Diversity: N-version Programming	T	Ds	1969 ?	PM:C MC:R	Cluster H. Not selected. Same as N-version programming (nr 210) and and Diverse Programming (nr 204), so these can be merged into one technique
163	Dynamic Reconfiguration	T	Ds	1971 or older	PM:C	Cluster RD.
164	Dynamic Logic	T	Ds	1973 or older	PM:C	Cluster R
165	Recovery blocks or Recovery Block Programming	T	Ds	1975?	PM:C	Cluster D
166	Complexity Models	T	Ds	1976 about	PM:C	Cluster D
167	FIs (Fagan Inspections)	I	Ds	1976	PM:C	Cluster V
168	Nuclear Safety Cross- Check Analysis	T	Ds	1976	PM:R	Not selected
169	SSCA (Software Sneak Circuit Analysis)	T	Ds	1976 or older	PM:C	Cluster H
170	Symbolic Execution	T	Ds	1976	PM:C	Cluster V
171	Graceful Degradation	T	Ds	1978?	PM:C	Cluster D
172	Information Hiding, Information Encapsulation	T	Ds	1979?	PM:C MC:R	Not selected
173	Software Time-out Checks	T	Ds	1980 or older	PM:C MC:R	Not selected
174	VDM (Vienna Development	T	Ds	1980	PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	Method)			about	MC:R	
175	Reliability Growth Models	T	Ds	1972	PM:R	Not selected
176	CCS (Calculus of Communicating Systems)	T	Ds	1983 about	MC:R PM:C	Not selected
177	Z	T	Ds	1984 ?	PM:F MC:R	Cluster R
178	SFTA (Software Fault Tree Analysis)	T	Ds	1984 or older	PM:C MC:FC	Cluster H. Either this one or SMHA (nr 189) is **SELECTED.**
179	Fault Injection	T	Ds	1984?	PM:C MC:F	Cluster V
180	CSP (Communicating Sequential Processes)	T	Ds	1979; update in 1985	MC:R PM:C	Cluster RD
181	Real-time Yourdon	I	Ds	1985	PM:C MC:R	Cluster RD. To be considered for SAFMOD.
182	OBJ	T	Ds	1985 about	PM:C MC:R	Not selected
183	Back-to-back testing	T	Ds	1986 or older	PM:C MC:R	Not selected
184	JSD (Jackson System Development)	I	Ds	1983	PM:C MC:R	Cluster D
185	Fail safety	T	Ds	1987 or older	PM:C	Cluster D
186	LOTOS (Language for Temporal Ordering Specification)	I	Ds	1987	MC:R PM:R	Not selected
187	MASCOT (Modular Approach to Software Construction, Operation and Test)	I	Ds	1970s	PM:C	Cluster RDV
188	SDL (Specification and Description Language)	I	Ds	1987 or older	PM:R MC:FC	Cluster (R)DVI. To be considered for SAFMOD.
189	SMHA (State Machine Hazard Analysis)	T	Ds	1987	PM:C	Cluster H. Either this one or SFTA (nr 178) is **SELECTED.**
190	Memorizing Executed Cases	T	Ds	1987 or older	PM:C	Cluster D
191	Synchronous Data Flow Specification Languages	T	Ds	1988 or older	PM:R	Not selected
192	Error Seeding	T	Ds	1989 or older	PM:C	Cluster V
193	Vital Coded Processor	T	Ds	1989	PM:C	Cluster D
194	Data Flow Diagrams	T	Ds	1989 or older	PM:C MC:R	Not selected
195	Bug-counting model	T	Ds	1990 or older	PM:C	Cluster V
196	Certificated Software Components	T	Ds	1990 or	PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
				older		
197	Certificated Tools or Certified Tools and Certified Translators	T	Ds	1990 or older	PM:C	Not selected
198	CORE (Controlled Requirements Expression)	T	Ds	1979	PM:R	Not selected
199	Jelinski-Moranda models	T	Ds	1990 or older	PM:R	Not selected
200	Safe Language Subsets	T	Ds	1990 or older	PM:C MC:?	Not selected. Will be merged with Safe Subsets of Programming Languages (nr 445) since appears to be the same.
201	SFMEA (Software Failure Modes and Effects Analysis)	T	Ds	1979	PM:C	Cluster H. **SELECTED.**
202	DO-178B (RTCA/EUROCAE ED-12B DO-178B)	I	Ds	1992	PM:R	Not selected
203	HOL (Higher Order Logic)	T	Ds	1993 or older	PM:C MC:R	Not selected
204	SHARD (Software Hazard Analysis and Resolution in Design)	T	Ds	1994	PM:C MC:R	Cluster H
205	Code Analysis	T	Ds	1995 about ?	PM:C MC:R	Not selected
206	Code Coverage	T	Ds	1995 about ?	PM:C MC:R	Not selected
207	Avalanche/stress testing	T	Ds	1995 or older	PM:C	Not selected
208	Data Flow Analysis	T	Ds	1995 or older	PM:C MC:R	Not selected
209	Diverse Programming	T	Ds	1995 or older	PM:C	Cluster H. Same as N-version programming (nr 210) and Diversity: N-version Programming (nr 157), so these can be merged into one technique
210	Equivalence Classes and Input Partition Testing	T	Ds	1995 or older	PM:C MC:R	Cluster V
211	Failure Assertion Programming	T	Ds	1995 or older	PM:C	Cluster D
212	FDD (Fault Detection and Diagnosis scheme)	T	Ds	1995 or older	PM:C	Cluster H
213	Formal Proof	T	Ds	1995 or older	PM:C	Cluster V
214	Forward Recovery	T	Ds	1995 or older	PM:C	Cluster D
215	N-version Programming	T	Ds	1995 or older	PM:C	Cluster H. Same as Diverse programming (nr 204) and Diversity: N-version Programming (nr 157), so these can be merged into one

Id	Technique	Type		Age	Candidate?	Workshop evaluation
						technique
216	Performance Requirements Analysis	T	Ds	1995 or older	PM:C	Cluster R
217	Probabilistic testing	T	Ds	1995 or older	PM:R	Not selected
218	SEEA (Software Error Effects Analysis)	T	Ds	1995 or older	PM:R	Cluster H. Link to SFMEA (nr 201)
219	Structure Based Testing	T	Ds	1995 or older	PM:C	Cluster V
220	Structure Diagrams	T	Ds	1995 or older	PM:R	Not selected
221	Backward Recovery	T	Ds	1995 probably older	PM:C	Cluster D
222	Boundary value analysis	T	Ds	1992 probably older	PM:C	Cluster V
223	DFM (Dynamic Flowgraph Analysis)	I	Ds	1996 about	PM:R	Not selected
224	SDA (Software Deviation Analysis)	T	Ds	1996	PM:C	Cluster H
225	CDA (Code Data Analysis)	T	Ds	1996 or older	PM:C MC:R	Not selected
226	CIA (Code Interface Analysis)	T	Ds	1996 or older	PM:C MC:R	Cluster D
227	CLA (Code Logic Analysis)	T	Ds	1996 or older	PM:C MC:R	Cluster D
228	Design Constraint Analysis	T	Ds	1996 or older	PM:R	Cluster D
229	Design Data Analysis	T	Ds	1996 or older	PM:C	Cluster D
230	Design Interface Analysis	T	Ds	1996 or older	PM:C	Cluster D
231	DLA (Design Logic Analysis)	T	Ds	1996 or older	PM:C	Cluster D
232	Formal Inspections	T	Ds	1996 or older	PM:C MC:R	Not selected
233	Rate Monotonic Analysis	T	Ds	1980s	PM:C	Cluster V
234	Requirements Criticality Analysis	T	Ds	1996 or older	PM:C	Cluster H
235	SADA (Architectural Design Analysis or Safety Architectural Design Analysis)	T	Ds	1996 or older	PM:R	Not selected
236	SSRFA (Software Safety Requirements Flowdown Analysis)	T	Ds	1996 or older	PM:C	Cluster D
237	Timing, Throughput and Sizing Analysis	T	Ds	1996 or older	PM:C	Cluster V
238	Unused Code Analysis	T	Ds	1996 or older	PM:C MC:R	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
239	Update Criticality Analysis	T	Ds	1996 or older	PM:C	Cluster D
240	Update Design Constraint Analysis	T	Ds	1996 or older	PM:C	Cluster D
241	Ego-less programming	T	Ds	2000?	PM:C	Cluster DV
242	Telelogic Tau	I	Ds	2001 or older	PM:R MC:FC	Not selected. Could be split up into SDL (nr 188), UML and MSC (added as new techniques in Group 6)
243	SpecTRM (Specification Tools and Requirements Methodology)	I	Ds	2002	PM:R MC:F	Cluster RDIH. To be considered for SAFMOD

The following techniques were newly identified for this list:

	UML	T	Ds			Not selected
	MSC (Message Sequence Chart)	T	Ds			Cluster D. To be considered for SAFMOD
	HATLEY	T	Ds			To be considered for SAFMOD
	Partitioning	T	Ds			Cluster D. Not selected
	Safety monitoring	T	Ds			Cluster D. Not selected

Also, the following techniques appeared in other groups and should be moved to this group:

160	ObjectGEODE	I	Ds	2001 or older	PM:R MC:FC	Not selected
438	Structuring the System according to Criticality	T	Ds	1989	PM:C	Not selected
445	Safe Subsets of Programming Languages	T	Ds	1996 or older	PM:C	Not selected. Will be merged with Safe Language Subsets (nr 195) since appears to be the same.

It was noted that the individual techniques from Cluster V (Verification and Testing) are generally adequate, but Formal techniques are not used enough. Safety formal verification techniques are not adapted to safety enough and should be promoted. This could be done in SAFMOD.

5.7 Selection process of techniques from Group 6

Group 6 consisted of Techniques that considered Risk assessment. The number of elements was 96. The techniques in this group were evaluated as follows: First, all techniques that are obviously not selected (based on the pre-workshop assessments by Eurocontrol staff) are labelled Not selected. The remaining techniques were next grouped into the following clusters:

I Identification
M Make a model

R Run the model
F Interpretation and Feedback
S Mitigation

Next, each cluster was considered separately and one (or no) techniques were selected from each cluster.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
244	Dispersion Modelling	T	R		PM:R	Not selected
245	MLD (Master Logic Diagrams)	T	R		MC:F PM:C	Cluster M
246	Plant walkdowns/ surveys	T	R		PM:R	Cluster I. To be considered for SAFBUILD
247	Rapid Risk Ranking	T	R		PM:F	Cluster F. Link with Criticality Analysis (nr 264)
248	Risk classification schemes	T	R		PM:R	Not selected
249	Process charts	T	R	1921	PM:R	Not selected
250	FTA (Fault Tree Analysis)	T	R	1961	PM:F MC:C KS:F	Cluster M. **SELECTED**
251	Naked man	T	R	1963 or older	PM:C	Cluster I
252	CRM (Collision Risk Model (ICAO))	T	R	1964	PM:F	Cluster M
253	FHA (Fault Hazard Analysis)	T	R	1965 about	PM:C	Cluster IM
254	Change Analysis	T	R	1965?	PM:F KS:FC	Cluster I. Link to HAZOP (nr 427) and to External Events Analysis (nr 299)
255	SNEAK (Sneak Circuit Analysis)	T	R	1967 / 1991	KS:FC PM:R	Not selected
256	KTT (Kinetic Tree Theory)	T	R	1970	PM:C	Cluster M
257	CCD (Cause Consequence Diagrams) or CCA (Cause Consequence Analysis)	T	R	1971	PM:C KS:F	Cluster M
258	PHA (Preliminary Hazard Analysis)	T	R	1972 about	PM:C	Cluster I
259	RBD (Reliability Block Diagrams) or SDM (Success Diagram Method)	T	R	1972 about	PM:F	Cluster M. Link to FTA (nr 250)
260	Energy Analysis	T	R	1972 or older	KS:FC PM:C	Cluster M
261	Energy Trace Checklist	T	R	1972 or older	PM:C	Cluster M
262	Maximum Credible Accident/ Worst Case	T	R	1972 or older	PM:C	Cluster I. Link to HAZOP (nr 427) and to External Events Analysis (nr 299)
263	SSHA (Subsystem Hazard Analysis)	T	R	1972 or older	PM:C	Cluster I

Id	Technique	Type		Age	Candidate?	Workshop evaluation
264	Criticality Analysis	T	R	1972?	PM:C KS:FC	Cluster F. Link to FMECA (nr 113)
265	ETBA (Energy Trace and Barrier Analysis for Hazard Discovery and Analysis)	T	R	1973	KS:FC PM:C	Cluster I. Link to External Events Analysis (nr 299)
266	Check List Analysis	T	R	1974	KS:FC PM:R	Cluster I
267	CPA (Critical Path Analysis)	T	R	1950s	PM:F MC:?	Cluster I
268	DMEA (Damage Mode and Effects Analysis)	T	R	1977	PM:C	Cluster I
269	STEP or STEPP (Sequentially- Timed Events Plot or Sequential Times Event Plotting Procedure)	T	R	1978 or older	PM:R	Not selected
270	CMFA (Common Mode Failure Analysis)	T	R	1979 about	PM:F KS:FC	Cluster I. Link to CCA (nr 282)
271	Scenario Analysis	T	R	1979 or older	KS:F PM:R	Cluster I. Link to External Event Analysis (nr 299)
272	Structural Safety Analysis	T	R	1979 or older	PM:R	Not selected
273	ETA (Event Tree Analysis)	T	R	1980	PM:F MC:F KS:FC	Cluster M. **SELECTED.**
274	T/LA (Time/ Loss Analysis for Emergency Response Evaluation)	T	R	1980 or older	PM:C	Cluster IM
275	DFMM (Double Failure Matrix Method)	T	R	1981	PM:F	Cluster M. Link to ETA (nr 273)
276	Root Cause Analysis	T	R	1981 or older	KS:FC PM:F	Cluster I
277	CSSA (Cryogenic Systems Safety Analysis)	T	R	1982	KS:R PM:R	Not selected
278	O&SHA (Operating and Support Hazard Analysis)	T	R	1982 or older	PM:C	Cluster I. Link to External Events Analysis (nr 299)
279	OHA (Operating Hazard Analysis)	T	R	1983 or older	PM:C	Cluster I
280	PMA (Phased Mission Analysis)	T	R	1984	PM:C	Cluster M
281	Production System Hazard Analysis	T	R	1985 or older	PM:C	Cluster I
282	CCA (Common Cause Analysis)	T	R	1987	PM:F KS:F	Cluster I. **SELECTED.**
283	Human (Error) HAZOP (Human (Error) Hazard and Operability study)	T	R	1988	MC:C KS:FC PM:C	Cluster I. Link to HAZOP (nr 427)
284	HHA (Health Hazard Assessment)	T	R	1988 or older	PM:R	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
285	Wind/ Tornado Analysis	T	R	1988 or older	PM:R	Not selected
286	CPQRA (Chemical Process Quantitative Risk Analysis)	T	R	1989	KS:FC PM:C	Cluster M
287	EMC (Electromagnetic Compatibility Analysis and Testing)	T	R	1989	PM:R	Not selected
288	PHL (Preliminary Hazard List)	T	R	1989 or older	PM:C	Cluster I
289	Beta-factor method	T	R	1981	KS:F PM:C	Cluster M. Link to CCA (nr 282)
290	Shock method	T	R	1991 or older	PM:C	Cluster MR. Link to CCA (nr 282)
291	Multiple Greek Letters method	T	R	1991 or older	PM:R	Not selected
292	PHI (Preliminary Hazard Identification)	T	R	1991 or older	PM:C	Cluster I
293	Repetitive Failure Analysis	T	R	1991 or older	PM:R	Not selected
294	Confined Space Safety	T	R	1992	MC:R PM:R	Not selected
295	Digraph Utilization Within System Safety	T	R	1992	PM:C	Cluster MR
296	ESD (Event Sequence Diagrams)	T	R	1992 or older	PM:C	Cluster M
297	PREDICT (PRocedure to Review and Evaluate Dependency In Complex Technologies)	T	R	1992	KS:R PM:C	Not selected
298	What- If/ Checklist Analysis	T	R	1992	PM:C	Cluster I
299	External Events Analysis	T	R	1992 or older	PM:R	Cluster I. **SELECTED.**
300	Facilities System Safety Analysis	T	R	1992 or older	PM:R	Not selected
301	NDI (Non-destructive Inspection Technique)	G		1914-1918 war	PM:R	Not selected. Should be moved to Group 2.
302	Systematic Occupational Safety Analysis	T	R	1992 or older	PM:R	Cluster I. Link to External Events Analysis (nr 299)
303	What- If Analysis	T	R	1992 or older	PM:F	Cluster I
304	CTC (Comparison- To- Criteria)	T	R	1993	PM:F	Cluster F
305	Generalised Reich collision risk model	T	R	1993	PM:C	Cluster M
306	Refined Reich collision risk model	T	R	1993	PM:C	Cluster M
307	ERA (Environmental Risk Analysis)	T	R	1993 or older	PM:R	Cluster I. Link to External Events Analysis (nr 299)
308	PRMA (Procedure Response Matrix Approach)	T	R	1994	KS:FC PM:C	Cluster I

Id	Technique	Type		Age	Candidate?	Workshop evaluation
309	CMA (Common Mode Analysis)	T	R	1994 or older	PM:C KS:FC	Cluster I. Link to CCA (nr 282)
310	DD (Dependence Diagrams)	T	R	1994 or older	PM:R	Not selected
311	FSMA (Fault-Symptom Matrix Analysis)	T	R	1994 or older	KS:FC PM:R	Not selected
312	SUSI (Safety Analysis of User System Interaction)	T	R	1994 or older	PM:C	Cluster I
313	Decision Tables	T	R	1995 or older	PM:C	Cluster MR
314	PRIMA (Process RIsk Management Audit)	T	R	1996	KS:FC PM:C	Cluster I
315	Risk decomposition	T	R	1996		Cluster M
316	SCHAZOP (Safety Culture Hazard and Operability)	T	R	1996	KS:FC PM:C	Cluster I. To be considered for SAFMOD. Link to HAZOP (nr 427)
317	TOPAZ-based hazard brainstorm	T	R	1996	PM:R	Cluster I
318	GSN (Goal Structuring Notation)	T	R	1996 or older	PM:R KS:F	Not selected
319	Protected airspace models	T	R	1996 or older	PM:C	Cluster M
320	QCT (Quantified Causal Tree)	T	R	1996 or older	PM:C	Cluster M
321	RSM (Requirements State Machines)	T	R	1996 or older	PM:R	Not selected
322	SSAR (System Safety Assessment Report)	T	R	1996 or older	PM:R	Not selected
323	DTA (Decision Tree Analysis)	T	R	1997	PM:C	Cluster M
324	Explosive Safety Analysis	T	R	1997 or older	PM:R	Not selected
325	Nuclear Explosives Process Hazard Analysis	T	R	1997 or older	PM:R	Not selected
326	Operational Readiness Review	T	R	1997 or older	KS:F PM:R	Cluster IS. **SELECTED.**
327	PHASE (Probabilistic Hybrid Analytical System Evaluation)	T	R	1997 or older	PM:R	Not selected
328	Radiological Hazard Safety Analysis	T	R	1997 or older	KS:R PM:R	Not selected
329	Threat Hazard Analysis	T	R	1997 or older	PM:R	Not selected
330	Hazard coverage based modelling	T	R	1998		Cluster F
331	MHD (Mechanical Handling Diagram)	T	R	1998 or older	PM:R	Not selected
332	Occupational Health Hazard Analysis	T	R	1999 or older	PM:R	Not selected
333	RECUPARARE	T	R	2000	PM:R	Not selected
334	HTRR (Hazard Tracking and	T	R	2000 or	PM:C	Cluster F. **SELECTED.**

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	Risk Resolution)			older		
335	RIF diagram (Risk Influencing Factor Diagram)	T	R	2000 or older	PM:R	Not selected
336	Particular Risk Analysis	T	R	1994 probably older		Cluster I
337	HzM (Multi-level HAZOP)	T	R	2001 or older	PM:C	Cluster I. Link to CCA (nr 282)
338	Safety targets setting	T	R	2001 or older	PM:C	Not selected
339	Bias and Uncertainty assessment	T	R	2002		Cluster RF. **SELECTED,** with addition of sensitivity analysis

The following technique appeared in another group and should be moved to this group:

340	Fault Schedule and Bounding Faults	T	R		KS:F	Link to FTA (nr 250)

5.8 Selection process of techniques from Group 7

Group 7 consisted of Techniques that considered Human performance. The number of elements was 79. The techniques in this group were evaluated as follows: First, all techniques that were obviously not selected (based on the pre-workshop assessments by Eurocontrol staff) were labelled Not selected. The remaining techniques were next grouped into the following clusters:

S Safety Culture
T Task analysis and Sequencing
C Cognitive modelling
E Error of commission
Q Quantification
M Performance measurement

Next, each cluster was considered separately and one (or no) techniques are selected from each cluster.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
340	Fault Schedule and Bounding Faults	T	R		KS:F	Move to Group 6. Link to FTA (nr 250)
341	Human Factors Case	T	H		KS:F	**SELECTED.**
342	Activity Sampling	T	H	1950	PM:R	Not selected
343	Task Decomposition	T	H	1953		Cluster T. Link to HTA (nr 346)
344	OSD (Operational Sequence Diagram)	T	H	1961	KS:FC PM:F	Cluster T. Link to HTA (nr 346)
345	PC (Paired Comparisons)	T	H	1966	KS:FC PM:C	Cluster Q. Together with APJ (nr 351) this will be considered in the **SELECTED** technique

Id	Technique	Type		Age	Candidate?	Workshop evaluation
						Use of expert judgement (new technique in Group 2).
346	HTA (Hierarchical Task Analysis)	T	H	1971	KS:FC PM:R	Cluster T. **SELECTED.**
347	IDA (Influence Diagram Approach) or STAHR (Socio-Technical Assessment of Human Reliability)	T	H	1980	KS:R PM:C	Not selected
348	PROCRU (Procedure-oriented Crew Model)	T	H	1980	KS:R PM:C	Not selected
349	TESEO (Tecnica Empirica Stima Errori Operatori (Empirical technique to estimate operator errors))	T	H	1980	KS:R PM:C	Not selected
350	AEA (Action Error Analysis)	T	H	1981	PM:C KS:FC	Cluster E. Link to TRACEr (nr 500)
351	APJ (Absolute Probability Judgement)	T	H	1981 or older	KS:FC PM:C	Cluster Q. Together with PC (nr 345) this will be considered in the **SELECTED** technique Use of expert judgement (new technique in Group 2).
352	CMA (Confusion Matrix Analysis)	T	H	1981	KS:F PM:F	Cluster E. Link to TRACEr (nr 500)
353	Murphy Diagrams	T	H	1981	KS:R PM:R	Not selected
354	SRK (Skill, Rule and Knowledge-based behaviour model)	T	H	1981	KS:R PM:R	Cluster C. Link to TRACEr (nr 500)
355	THERP (Technique for Human Error Rate Prediction)	T	H	1981	KS:FC PM:C	Cluster Q. Link to TRACEr (nr 500)
356	WSA (Work Safety Analysis)	T	H	1981	KS:FC PM:C	Cluster E. Link to External Events Analysis (nr 299)
357	HCR (Human Cognitive Reliability model)	T	H	1982 from	KS:R PM:C	Not selected
358	OATS (Operator Action Trees)	T	H	1982	KS:R PM:C	Not selected
359	HRAET (Human Reliability Analysis Event Tree)	T	H	1983	KS:F PM:C	Link to ETA (nr 273)
360	MMSA (Man-Machine System Analysis)	T	H	1983	PM:R	Not selected
361	SHARP (Systematic Human Action Reliability Procedure)	T	H	1984	KS:R PM:C	Not selected
362	SLIM (Success Likelihood Index Methodology)	T	H	1984	KS:FC PM:C	Cluster Q
363	HEART (Human Error Assessment and Reduction Technique)	T	H	1985	KS:FC PM:C	Cluster Q. **SELECTED.**
364	IMAS (Influence Modelling and Assessment System)	T	H	1986	KS:R PM:R	Not selected
365	OSTI (Operant Supervisory Taxonomy Index)	T	H	1986	KS:R PM:R	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
366	Action Information Requirements	T	H	1986 or older	PM:R KS:R	Not selected
367	PTS (Predetermined Time Standards)	T	H	1986 or older	PM:R	Not selected
368	Task Description Analysis	T	H	1986 or older	KS:FC PM:C	Cluster T. Link to HTA (nr 346)
369	Workload Analysis (MIL)	T	H	1986 or older	KS:FC PM:C	Cluster M
370	ASEP (Accident Sequence Evaluation Programme)	T	H	1987	KS:FC PM:C	Cluster Q
371	CHASE (Complete Health And Safety Evaluation)	T	H	1987	KS:FC PM:R	Cluster S. To be considered for SAFMOD
372	GEMS (Generic Error Modelling System)	T	H	1987	KS:R PM:R	Not selected
373	Timeline Analysis	T	H	1987	KS:FC PM:C	Cluster T. Link to HTA (nr 346)
374	HTLA (Horizontal Timeline Analysis)	T	H	1987 or older	KS:FC PM:R	Cluster T. Link to HTA (nr 346)
375	VTLA (Vertical Timeline Analysis)	T	H	1987 or older	KS:FC PM:C	Cluster T. Link to HTA (nr 346)
376	CADA (Critical Action and Decision Approach)	T	H	1988	PM:R KS:R	Not selected
377	Five Star System	T	H	1988	PM:C	Cluster S. To be considered for SAFMOD.
378	ISRS (International Safety Rating System)	T	H	1988	KS:FC PM:C	Cluster S. To be considered for SAFMOD.
379	PHECA (Potential Human Error Causes Analysis)	T	H	1988	KS:R PM:R	Not selected
380	Operator Task Analysis	T	H	1988 or older	PM:F KS:F	Cluster T. Link to HTA (nr 346).
381	HEMECA (Human Error Mode, Effect and Criticality Analysis)	T	H	1989	KS:R PM:C	Not selected
382	SART (Situational Awareness Rating Technique)	T	H	1989	KS:FC PM:C	Cluster M
383	Fallible machine Human Error	T	H	1990		Cluster C
384	HPLV (Human Performance Limiting Values)	T	H	1990	KS:F PM:C	Cluster Q. Link to CCA (nr 282)
385	HRMS (Human Reliability Management System)	T	H	1990	KS:R PM:R	Not selected
386	PHRA (Probabilistic Human Reliability Analysis)	T	H	1990	PM:R	Not selected
387	COMET (COMmission Event Trees)	T	H	1991	KS:FC PM:C	Link to ETA (nr 273)
388	INTENT	T	H	1991	KS:R PM:C	To be considered for SAFMOD
389	TAFEI (Task Analysis For Error Identification)	T	H	1991	KS:FC PM:C	Cluster E
390	TOPPE (Team Operations Performance and Procedure Evaluation)	T	H	1991	KS:FC PM:C	Cluster M

Id	Technique	Type		Age	Candidate?	Workshop evaluation
391	DADs (Decision Action Diagrams)	T	H	1992	KS:FC PM:F	Cluster T. Link to HTA (nr 346)
392	Multiple Resources	T	H	1992		Cluster C
393	SCHEMA (System for Critical Human Error Management and Assessment OR Systematic Critical Human Error Management Approach)	T	H	1992	KS:R PM:C	Not selected
394	CAHR (Connectionism Assessment of Human Reliability)	T	H	1992-1998	KS:FC PM:C but R if tool	Cluster E. Link to Human Error Data Collection (new technique in Group 7)
395	COCOM (COgnitive COntrol Model)	T	H	1993	KS:R PM:C	Cluster C
396	COGENT (COGnitive EveNt Tree)	T	H	1993	KS:R PM:C	Not selected
397	PRISM (Professional Rating of Implemented Safety Management)	T	H	1993	KS:FC PM:R	Cluster S. To be considered for SAFMOD
398	HAZid (Hazard Identification)	T	H	1993 or older	PM:C	Link to HAZOP (nr 427)
399	ASCOT (Assessment of Safety Culture in Organisations Team)	T	H	1994	PM:R KS:FC	Cluster S. To be considered for SAFMOD. Is the leader of its cluster.
400	Situational Awareness Error Evolution	T	H	2001 about		Cluster C
401	SRS-HRA (Savannah River Site Human Reliability Analysis)	D		1994	KS:R PM:R	To be moved to Group 1. To be considered for SAFMOD and SAFBUILD
402	Usability Heuristic Evaluation	T	H	1994	PM:C	Cluster C. To be considered for SAFBUILD
403	CTA (Cognitive Task Analysis)	T	H	1994 or older	KS:FC PM:F	Cluster C. This field is not mature enough. To be considered for SAFBUILD.
404	SPN (Synchronised Petri Network)	M		1994 or older	PM:R	To be moved to Group 3, and then merged with Petri Net Extensions (nr 94).
405	EOCA (Error of Commission Analysis)	T	H	1995	MC:C KS:F PM:C	Cluster E. To be considered for SAFMOD.
406	SAGAT (Situation Awareness Global Assessment Technique)	T	H	1995	KS:FC PM:R	Cluster M
407	ATHEANA (A Technique for Human Error ANAlysis)	T	H	1996	PM:C MC:F KS:FC	Cluster E. To be considered for SAFMOD
408	Ofan	T	H	1996 or older	PM:C	Cluster C
409	CODA (Conclusions from Occurrences by Descriptions of Actions)	T	H	1997	KS:R PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
410	Human error recovery	T	H	1997		Cluster E. Link to TRACEr (nr 500)
411	SPAM (Situation-Present Assessment method)	T	H	1998	KS:FC PM:R	Cluster M
412	OFM (Operation Function Model)	T	H	1987	PM:C	Cluster T. Link to HTA (nr 346)
413	APRECIH (Analyse PREliminaire des Conséquences de l'Infiabilité Humaine)	T	H	1999	KS:F PM:C	Cluster E. Link to TRACEr (nr 500)
414	NE-HEART (Nuclear Electric Human Error Assessment and Reduction Technique)	T	H	1999 or older	KS:R PM:R	Not selected
415	SDA (Sequence Dependency Analysis)	T	H	1999 or older	KS:FC PM:F	Cluster T. Link to HTA (nr 346)
416	AEMA (Action Error Mode Analysis)	T	H	2000 probably older	PM:C KS:FC	Cluster E. Link to TRACEr (nr 500)
417	CESA (Commission Errors Search and Assessment)	T	H	2001	KS:R PM:R	Not selected
418	SPAR HRA (Simplified Plant Analysis Risk Human Reliability Assessment)	T	H	2001 or older	PM:C	Cluster E

The following technique was newly identified for this list:

	Human Error Data Collection	T	H			**SELECTED**.
	NOTECHX	T	H			New technique on assessing non-technical skills
	3D-SART	T	H			Is narrowed-down version from SART (nr 382), covering only 3 dimensions

Also, the following technique appeared in another group and should be moved to this group:

41	Link Analysis	T	H	1959	KS:FC PM:R	Link to HTA (nr 346)

5.9 Selection process of techniques from Group 8

Group 8 consisted of Techniques that considered hazard Mitigation. The number of elements was 32. The techniques in this group were evaluated one by one, without clustering first.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
419	Delphi Knowledge Elicitation Method or Delphi Method	G		1950 about	KS:FC PM:C	To be moved to Group 2; Link to Use of Expert Judgement (new technique in Group 2)
420	PERT (Program Evaluation	T	M	1950	PM:R	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	Review technique)					
421	CIT (Critical Incident Technique)	T	M	1954	KS:F PM:C	Link to HAZOP (nr 427)
422	Job Safety Analysis	T	M	1960 about	KS:F PM:C	To be considered for SAFBUILD. Link to HAZOP (nr 427)
423	Diversity: The Safety bag	T	M	1969 ?	PM:R	Not selected
424	Test Adequacy Measures	T	M	1972 or older	PM:C	Not selected
425	Verbal Protocols	T	M	1972 or older	KS:FC PM:R	Not selected
426	Contingency Analysis	T	M	1972?	KS:F PM:F	To be considered for SAFBUILD
427	HAZOP (Hazard and Operability study)	T	M	1974	PM:F MC:F KS:F	**SELECTED.**
428	TSA (Test Safety Analysis)	T	M	1979 or older	PM:R	Not selected
429	Nuclear Safety Analysis	T	M	1980 or older	PM:R	Not selected
430	CRC (Control Rating Code Method)	T	M	1980?	PM:F	Not selected
431	Seismic Analysis	T	M	1984 or older	PM:R	Not selected
432	Barrier Analysis	T	M	1985	PM:F KS:F	Cluster I. Link to External Events Analysis (nr 299)
433	SHERPA (Systematic Human Error Reduction and Prediction Approach)	T	M	1986	KS:R PM:C	Link to TRACEr (nr 500)
434	Talk-Through	T	M	1986	KS:FC PM:R	Cluster I. Link to HAZOP (nr 427)
435	Walk- Through Task Analysis	T	M	1986	KS:FC PM:C	Cluster I. Link to HAZOP (nr 427)
436	Function allocation trades	T	M	1986 or older	KS:R PM:R	Not selected
437	Nuclear Criticality Analysis	T	M	1987 or older	PM:R	Not selected
438	Structuring the System according to Criticality	T	Ds	1989	PM:C	Move to Group 5. Not selected
439	TTA (Tabular Task Analysis)	T	M	1989 or older	KS:FC PM:R	Link to HTA (nr 346)
440	Re-try Fault Recovery	T	M	1990 or older	PM:R	To be considered for SAFBUILD
441	Return to Manual Operation	T	M	1990 or older	PM:R	To be considered for SAFBUILD
442	PHEA (Predictive Human Error Analysis technique)	T	M	1993	KS:R PM:C	Link to TRACEr (nr 500)
443	Artificial Intelligence Fault	T	M	1995 or	PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	Correction			older		
444	Error Guessing	T	M	1995 or older	PM:R	Not selected
445	Safe Subsets of Programming Languages	T	Ds	1996 or older	PM:C	Move to Group 5. Not selected
446	CSSM (Continuous Safety Sampling Methodology)	T	M	1997	PM:R	To be considered for SAFBUILD occupational safety. Link to External Events Analysis (nr 299)
447	DSA (Deactivation Safety Analysis)	T	M	1997 or older	PM:F	Not selected
448	Risk-Based Decision Analysis	T	M	1993 or older	PM:R	Not selected
449	Bow-Tie	T	M	1998 or older	PM:F MC:F KS:F	**SELECTED.**
450	CSA (Comparative Safety Assessment)	T	M	2000 or older	KS:F PM:F	Not selected

5.10 Selection process of techniques from Group 9

Group 9 consisted of Integrated methods of more than one technique, dependability techniques excluded (since those are covered by Groups 4 and 5). The number of elements was 54. The techniques in this group were evaluated one by one, without clustering first.

Id	Technique	Type		Age	Candidate?	Workshop evaluation
451	SOFIA	I	H			Not selected
452	TOKAI	I	H			Not selected
453	SAINT or Micro-SAINT (Systems Analysis of Integrated Networks or Micro-Systems Analysis of Integrated Networks)	I	H	1977	KS:FC PM:R	Not selected
454	GOMS (Goals, Operators, Methods and Systems)	I	H	1983	KS:R PM:R	Link to HTA (nr 346)
455	MAPPS (Maintenance Personnel Performance Simulations)	I	H	1984	KS:R PM:R	Not selected
456	TALENT (Task Analysis-Linked EvaluatioN Technique)	I	H	1988	KS:R PM:R	Not selected
457	CES (Cognitive Environment Simulation)	I	H	1987	KS:R PM:R	Not selected
458	JHEDI (Justification of Human Error Data Information)	I	H	1990	KS:R PM:R	Not selected
459	MANAGER (MANagement Assessment Guidelines in the Evaluation of Risk)	I	H	1990	KS:R PM:F	To be considered for SAFMOD safety culture

Id	Technique	Type		Age	Candidate?	Workshop evaluation
460	INTEROPS (INTEgrated Reactor OPerator System)	I	H	1991	KS:R PM:C	Not selected
461	COSIMO (Cognitive Simulation Model)	I	H	1992	KS:R PM:C	Not selected
462	ESAT (Expertensystem zur Aufgaben-Taxonomie (Expert-System for Task Taxonomy))	I	H	1992	PM:R	Not selected
463	CREAM (Cognitive Reliability and Error Analysis Method)	I	H	1993	KS:FC PM:C	To be considered for SAFBUILD cognitive bag of tools
464	CREWSIM (CREW SIMulation)	I	H	1993	KS:R PM:C	Not selected
465	ADSA (Accident Dynamic Sequence Analysis)	I	H	1994	KS:C PM:C	Not selected
466	ASP (Accident Sequence Precursor)	D		1979	KS:FC PM:C	To be considered for SAFMOD and SAFBUILD
467	CAMEO/TAT (Cognitive Action Modelling of Erring Operator/Task Analysis Tool)	I	H	1994	PM:R KS:R	Not selected
468	CREWPRO (CREW PRObIem solving simulation)	I	H	1994	KS:R PM:C	Not selected
469	NOMAC (Nuclear Organisation and Management Analysis Concept)	I	H	1994	KS:R PM:R	To be considered for SAFBUILD safety culture
470	DREAMS (Dynamic Reliability technique for Error Assessment in Man-machine Systems)	I	H	1995	PM:C	Not selected
471	PUMA	I	H	1995 about		Not selected
472	MIDAS (Man-Machine Integrated Design and Analysis System)	I	H	1986	KS:F PM:R	Not selected
473	MEDA (Maintenance Error Decision Aid)	I	H	1996 or older	KS:FC PM:R	Not selected
474	SEAMAID (Simulation-based Evaluation and Analysis support system for MAn-machine Interface Design)	I	H	1996	KS:R PM:R	Not selected
475	SYBORG (System for the Behaviour of the Operating Group)	I	H	1996	KS:R PM:C	Not selected
476	HFACS (Human Factors Analysis and Classification System)	I	H	1997 or older	KS:R PM:C	Not selected
477	Air-MIDAS (Air- Man-Machine Integrated Design and Analysis System)	I	H	1998 about		To be considered for SAFBUILD cognitive bag of tools
478	MERMOS (Méthode d'Evaluation de la Réalisations	I	H	1998	KS:R PM:C	Not selected

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	des Missions Opérateur pour la Sureté)					
479	FACE (Framework for Analysing Commission Errors)	I	H	1999	KS:FC PM:C	To be considered for SAFMOD error of commission
480	MONACOS	I	H	1999	PM:R	Not selected
481	HERA I and HERA II (Human Error in ATM)	I	H	2000	PM:R KS:FC	Link to TRACEr (nr 500)
482	RAIT (Railway Accident Investigation Tool)	I	H	2000 probably older	KS:R PM:R	Not selected
483	IPME (Integrated Performance Modelling Environment)	I	H	2000?	PM:R	To be considered for SAFBUILD cognitive bag of tools
484	PRA (Probabilistic Risk Assessment based on FTA/ETA) or PSA (Probabilistic Safety Assessment)	I	R	1975 about	KS:FC PM:RC	Link to Bow-Tie (nr 449) and to FTA (nr 250) and ETA (nr 273)
485	MORT (Management Oversight and Risk Tree Analysis)	I	R	1975 – 1980	KS:FC PM:R	Link to Operational Readiness Review (nr 326)
486	DYLAM (Dynamic Logical Analytical Methodology)	I	R	1985	KS:FC PM:C	Not selected
487	Dynamic Event Tree Analysis	I	R	1985	PM:C	Not selected
488	DETAM (Dynamic Event Tree Analysis Method)	I	R	1991	KS:FC PM:C	Not selected
489	IAEA TECDOC 727	I	R	1993	PM:C	Not selected
490	TEACHER/ SIERRA (Technique for Evaluating and Assessing the Contribution of Human Error to Risk [which uses the] Systems Induced Error Approach)	I	R	1993	KS:R PM:C	Not selected
491	HITLINE (Human Interaction Timeline)	I	R	1994	KS:FC PM:C	To be considered for SAFBUILD and SAFMOD
492	WPAM (Work Process Analysis Model)	I	R	1994	KS:FC PM:C	To be considered for SAFMOD safety culture
493	SOCRATES (Socio-Organizational Contribution to Risk Assessment and the Technical Evaluation of Systems)	I	R	1998	PM:R	To be considered for SAFMOD safety culture
494	TOPAZ (Traffic Organisation and Perturbation AnalyZer)	I	R	1998	PM:R	To be considered for SAFBUILD
495	OPL (Operational Procedure Language)	I	M			To be considered for SAFBUILD
496	Front-End Analysis	I	M	1993	PM:R	Not selected
497	TRIPOD	I	M	1994	KS:FC PM:R	To be considered for SAFMOD safety culture
498	HCA (Human Centred Automation)	I	M	1996	KS:F PM:C	To be considered for SAFBUILD
499	PEAT (Procedural Event	I	M	1999	KS:R	To be considered for SAFMOD

Id	Technique	Type		Age	Candidate?	Workshop evaluation
	Analysis Tool)				PM:R	
500	TRACEr (Technique for the Retrospective Analysis of Cognitive Errors in Air Traffic Management)	I	H	1999	PM:C KS:FC	**SELECTED.**
501	REHMS-D (Reliable Human Machine System Developer)	I	M	1999 about	PM:C	Not selected
502	PRASM (Predictive Risk Assessment and Safety Management)	I	M	2000	PM:R	To be considered for SAFMOD safety culture
503	TRM or CRM (Team Resource Management or Crew Resource Management)	I	T	1998 about	KS:F PM:R	A section in [D5 Main Document] will be dedicated to this
504	ESSAI (Enhanced Safety through Situation Awareness Integration in training)	I	T	2000 from		Link to TRM (nr 503) and to be considered for SAFBUILD and SAFMOD

6. References

The list below contains all references used in both the main document [D5 Main Document] and this technical annex [D5 Technical Annex]. For a shortlist of key references, we refer to the main document.

[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.)
[Abed&Angue94]	M. Abed, J.C. Angue, A new method for conception, realisation and evaluation of man-machine, IEEE International Conference on Systems, Man and Cybernetics. Human, Vol 2, pp. 1420-1427, 1994
[Air-MIDAS web]	Air-MIDAS web page, http://caffeine.arc.nasa.gov/midas/Air_MIDAS.html
[AIRS]	Regional Information System (RIS), http://www.co.lane.or.us/BCC/documents/22RIS.pdf
[AIS-DFD]	Applied Information Science web, http://www.aisintl.com/case/dfd.html
[Alur93]	R. Alur, C. Courcoubetis, T. Henzinger, P-H. Ho, Hybrid Automata: An algorithmic approach to the specification and verification of hybrid systems, Hybrid Systems I, Lecture notes in computer science, Springer-Verlag, 1993, 209-229.
[Amalberti&Wioland97]	R. Amalberti and L. Wioland, Human error in aviation, Proc. Int. Aviation Safety Conf., VSP, Utrecht, 1997, pp. 91-108.
[Andersson93]	M. Andersson, Modelling of combined discrete event and continuous time dynamical systems, Preprints of the 12th IFAC world congress, Sydney, Australia, 1993, pp. 69-72.
[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.
[Andre&Degani96]	A. Andre, A. Degani, Do you know what mode you are in? An analysis of mode error in everyday things, Proceedings of 2nd Conference on Automation Technology and Human, pp. 1-11, March 1996
[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
[ARES-RBDA]	Risk-based decision analysis according to ARES corporation, http://www.arescorporation.com/ares/technicalupdates/96-10tec.pdf
[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.
[ARP 4761]	SAE ARP 4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, S-18 Committee, Society of Automotive Engineers, Inc. (SAE), March 1994.
[ASRS web]	ASRS web site, http://asrs.arc.nasa.gov/main.htm
[Ayyub01]	B.M. Ayyub, Elicitation of expert opinions for uncertainty and risks, CRC Press, Boca Raton, Florida, 2001.
[Babinec&Bernatik&Pavelka99]	F. Babinec, A. Bernatik, M. Vit, T. Pavelka, Risk sources in industrial region, November 1999, http://mahbsrv.jrc.it/proceedings/greece-nov-1999/D6-BAB-BERNATIC-z.pdf
[Bakker&Blom93]	G.J. Bakker, H.A.P. Blom, Air traffic collision risk modelling, 32nd IEEE Conference on Decision and Control, Vol 2, Institute of Electrical and

	Electronics Engineers, New York, Dec 1993, pp. 1464-1469.
[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
[BASIS web]	BASIS web site http://www.winbasis.com/
[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.
[Belief networks]	http://www.norsys.com/belief.html
[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&al98,01]	H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij, and M.B. Klompstra, Accident risk assessment for advanced ATM, 2nd USA/Europe Air Traffic Management R&D Seminar, FAA/Eurocontrol, 1998, http://atm-seminar-98.eurocontrol.fr/finalpapers/track3/blom.pdf, also in Eds G.L. Donohue, A.G. Zellweger, Air Transportation Systems Engineering, AIAA, pp. 463-480, 2001.
[Blom&Bakker02]	H.A.P. Blom and G.J. Bakker, Conflict Probability and Incrossing Probability in Air Traffic Management, Proc. Conference on Decision and Control 2002, pp. 2421-2426, December 2002.
[Blom&Bakker93]	H.A.P. Blom, G.J. Bakker, A macroscopic assessment of the target safety gain for different en route airspace structures within SUATMS, Working paper for the ATLAS study of the commission of European Communities, NLR report CR 93364 L, 1993.
[Blom&Bar-Shalom88]	H.A.P. Blom and Y. Bar-Shalom, The Interacting Multiple Model Algorithm for Systems with Markovian Switching Coefficients, IEEE Trans. on Automatic Control, Vol. 33, No. 8, 1988, pp. 780-783.
[Blom&Daams&Nijhuis 00]	H.A.P. Blom, J. Daams, H.B. Nijhuis, Human cognition modelling in ATM safety assessment, 3rd USA/Europe Air Traffic management R&D seminar, Napoli, 13-16 June 2000, http://atm-seminar-2000.eurocontrol.fr/acceptedpapers/pdf/paper92.pdf, also in Eds G.L. Donohue, A.G. Zellweger, Air Transportation Systems Engineering, AIAA, pp. 481-511, 2001.
[Blom&Everdij&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/.
[Blom&Stroeve&Daams &Nijhuis01]	H.A.P. Blom, S. Stroeve, J. Daams and H.B. Nijhuis, Human cognition performance model based evaluation of air traffic safety, 4th International Workshop on Human Error, Safety and Systems Development, 11-12 June 2001, Linköping, Sweden
[Blom&Stroeve&Everdi j&Park02]	H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij, M.N.J. van der Park, Human cognition performance model based evaluation of safe spacing in air traffic, ICAS 2002 Congress
[Blom90]	H.A.P. Blom, Bayesian estimation for decision-directed stochastic control, Ph.D. dissertation, Delft University of Technology, 1990.
[Bongard01]	J.A. Bongard, Maintenance Error Management through MEDA, 15th Annual

	Symposium - Human Factors in Maintenance and Inspection 27-29 March 2001, London, UK, http://www.hf.faa.gov/docs/508/docs/bongard15.pdf
[Botting&Johnson98]	R.M. Botting, C.W. Johnson, A formal and structured approach to the use of task analysis in accident modelling, International Journal Human-Computer studies, Vol 49, pp. 223-244, 1998
[Branicky&Borkar&Mitter98]	M.S. Branicky, V.S. Borkar, S.K. Mitter, A unified framework for Hybrid Control: model and optimal control theory, IEEE Transactions on Automatic Control, Vol 43, No 1, pp. 31-45, Jan 1998, http://www.vuse.vanderbilt.edu/~biswas/Courses/cs367/papers/branicky-control.pdf
[Brooker02]	P. Brooker, Future Air Traffic Management: Quantitative en route safety assessment, The Journal of Navigation, 2002, Vol 55, pp. 197-211, The Royal Institute of Navigation
[Butler&Johnson95]	R.W. Butler and S.C. Johnson, Techniques for modeling the reliability of fault-tolerant systems with Markov state-space approach, NASA Reference publication 1348, September 1995
[CAA9095]	CAA, Aircraft Proximity Hazard (APHAZ reports), CAA, Volumes 1-8, 1990-1995
[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.
[Cacciabue&Amendola&Cojazzi86]	P.C. Cacciabue, A. Amendola, G. Cojazzi, Dynamic logical analytical methodology versus fault tree: the case of the auxiliary feedwater system of a nuclear power plant, Nuclear Technology, Vol. 74, pp. 195-208, 1986.
[Cacciabue&Carpignano&Vivalda92]	P.C. Cacciabue, A. Carpignano, C. Vivalda, Expanding the scope of DYLAM methodology to study the dynamic reliability of complex systems: the case of chemical and volume control in nuclear power plants, Reliability Engineering and System Safety, Vol. 36, pp. 127-136, 1992.
[Cacciabue98]	P.C. Cacciabue, Modelling and human behaviour in system control, Advances in industrial control, Springer, 1998
[Cagno&Acron&Mancini01]	E. Cagno, F. Acron, M. Mancini, Multilevel HAZOP for risk analysis in plant commissioning, ESREL 2001, http://www.aidic.it/italiano/congressi/esrel2001/webpapersesrel2001/32.pdf
[CBSSE90, p30]	Commission on Behavioral and Social Sciences and Education, Quantitative Modeling of Human Performance in Complex, Dynamic Systems, 1990, page 30, http://books.nap.edu/books/030904135X/html/30.html
[CBSSE90, p40]	Commission on Behavioral and Social Sciences and Education, Quantitative Modeling of Human Performance in Complex, Dynamic Systems, 1990, page 40, http://books.nap.edu/books/030904135X/html/40.html#pagetop
[CCS]	http://ei.cs.vt.edu/~cs5204/fall99/ccs.html
[Charpentier00]	P. Charpentier, Annex 5: Tools for Software fault avoidance, Task 3: Common mode faults in safety systems, Final Report of WP 1.2, European Project STSARCES (Standards for Safety Related Complex Electronic Systems), Contract SMT 4CT97-2191, February 2000, http://www.safetynet.de/EC-Projects/stsarces/WP12d_Annex5_software_task3.PDF
[CHIRP web]	The CHIRP Charitable Trust Home Page, http://www.chirp.co.uk/
[Chudleigh&Clare94]	M.F. Chudleigh and J.N. Clare, The benefits of SUSI: safety analysis of user system interaction, Arthur D. Little, Cambridge Consultants, 1994
[Cichocki&Gorski]	T. Cichocki, J. Górski, Safety assessment of computerised railway signalling equipment supported by formal techniques, WS5, www.ifad.dk/Projects/FMERail/ws5proceedings/safety/adtranz.doc
[Cojazzi&Cacciabue92]	G. Cojazzi, P.C. Cacciabue, The DYLAM approach for the reliability analysis

	of dynamic systems. 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. 8-23. Springer-Verlag, 1994.
[Cooper96]	J.A. Cooper, PHASER 2.10 methodology for dependence, importance, and sensitivity: The role of scale factors, confidence factors, and extremes, Sandia National Labs., Dept. of System Studies, Albuquerque, NM USA, Sept. 1996, http://www.sti.nasa.gov/Pubs/star/9711/divg.pdf
[Corker00]	K.M. Corker, Cognitive models and control: human and system dynamics in advanced airspace operations, Eds: N. Sanders, R. Amalberti, Cognitive engineering in the aviation domain, Lawrence Erlbaum Ass., pp. 13-42, 2000
[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
[CS473]	CS473, VORD (Viewpoint Oriented Requirements methods), 7 November 2002, http://www.manningaffordability.com/S&tweb/PUBS/Man_Mach/annexi.html
[CSP]	Communicating Sequential Processes, http://www.formal.demon.co.uk/CSP.html
[CTA Resource]	CTA Resource Web Page, The on-line community for task analysis, http://www2.ctaresource.com/index.php
[D5 Main Document]	M.H.C. Everdij, Review of techniques to support the EATMP Safety Assessment Methodology, Main Document, Safety methods Survey Final report D5, 31 March 2003.
[D5 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.
[Daams&Blom&Nijhuis 00]	J. Daams, H.A.P. Blom, and H.B. Nijhuis, Modelling Human Reliability in Air Traffic Management, PSAM5 - Probabilistic Safety Assessment and Management, S. Kondo, and K. Furata (Eds.), Vol. 2/4, Universal Academy Press, Inc., Tokyo, Japan, 2000, pp. 1193-1200.
[DAN97]	Design analysis newsletter, 1st quarter 1997, Dedicated to Design Excellence, Design/Analysis Consultants, Inc., http://www.daci-wca.com/news197.htm
[Darlington]	R.B. Darlington, Factor Analysis, http://comp9.psych.cornell.edu/Darlington/factor.htm
[Davis84]	M.H.A. Davis, Piecewise Deterministic Markov Processes: A general class of non-diffusion stochastic models, Journal Royal Statistical Society (B), Vol 46, pp. 353-388, 1984
[Davison]	H. Davison, Cognitive task analysis: Current research, slides, http://web.mit.edu/16.459/www/CTA2.pdf
[DCSC02]	Safety Assessment: Topic IV of the DCSC Programme, March 2002, http://www.cs.york.ac.uk/hise/dcsc/safe.html
[DEFSTAN00-56]	Hazard analysis and safety classification of the computer and programmable electronic system elements of defence equipment, Int. Defence standard 00-56/1, April 1991.
[DeJong&al01]	H.H. De Jong, R.S. Tump, H.A.P. Blom, B.A. van Doorn, A.K. Karwal, E.A. Bloem, Qualitative Safety Assessment of a RIASS based operation at Schiphol airport including a quantitative model, Crossing departures on 01L/19R under good visibility conditions, NLR memorandum LL-2001-017, May 2001

[Delphi]	Web article on Delphi Method, http://www.iit.edu/~it/delphi.html
[DND_SECO]	DND SECO glossary of models and simulations, http://www.drdc-rddc.dnd.ca/seco/scripts/browse.pl?lang=en
[DND_SECO_MIDAS]	DND SECO glossary of models and simulations: MIDAS, http://www.drdc-rddc.dnd.ca/seco/scripts/view.pl?lang=en;id=106
[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
[DO178B]	RTCA DO178B, Software considerations in airborne systems and equipment certification, 1 December 1992
[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
[DOT-FTA00]	U.S. Department of Transportation, Federal Transit Administration, Hazard analysis guidelines for transit projects, U.S. Department of Transportation, Research and Special Programs Administration, Final Report, January 2000, http://transit-safety.volpe.dot.gov/Publications/Safety/Hazard/HAGuidelines.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.
[Endsley97]	M.R. Endsley, Situation Awareness, Automation & Free Flight, 1997, http://atm-seminar-97.eurocontrol.fr/endsley.htm
[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
[EQE Web]	EQE international webpage on hazard identification methods, http://www.eqe.co.uk/consulting/pdf/hazard.pdf
[EQE Web_TRIPOD]	EQE international webpage on TRIPOD beta, http://www.eqe.co.uk/consulting/pdf/tripod.pdf
[ErrorGuess]	Web page on Error Guessing, http://www.csst-technologies.com/genericError_Guessing.html
[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).
[Escobar01]	J. Escobar, Maintenance Error Decision Aid (MEDA), A process to help reduce maintenance errors, April 2001, http://www.evergreenairlines.com/safety_new/html/articles_maint/mt0002.html
[ESH-ORR]	ESH 1.3.2 Operational Readiness Review, https://sbms-authqa.bnl.gov/ld/ld08/ld08d071.htm
[ESSAI web]	ESSAI web page, http://www.nlr.nl/public/hosted-sites/essai/index.html
[EUCARE web]	European Confidential Aviation Safety Reporting Network webpage, http://www.eucare.de/
[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&Blom&Klompstra97]	M.H.C. Everdij, H.A.P. Blom, M.B. Klompstra, Dynamically Coloured Petri Nets for Air Traffic Management Purposes, Proceedings 8th IFAC Symposium on transportation systems, Chania, Greece, pp. 184-189, NLR report TP 97493, National Aerospace Laboratory NLR, Amsterdam, 1997
[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 AC431]	FAA Advisory Circular 431-35.2, Reusable launch and reentry vehicle System Safety Process, September 2000, http://ast.faa.gov/files/pdf/Ac4312a5.pdf
[FAA memo02]	FAA Memorandum, Policy no. ANE-2002-35.15-RO, Draft, November 2002, http://www.ihsaviation.com/memos/PM-ANE-2002-35.15-RO.pdf
[FAA SSMP]	US Department of Transportation, Federal Aviation Administration, NAS Modernization, System Safety Management Program, FAA Acquisition Management System, ADS-100-SSE-1, Rev 3.0, 1 May 2001, http://faculty.erau.edu/fitzg3f9/MAS611/NASModSSMP.pdf; section on HTRR also on FAA Acquisition System Toolset web page, http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10
[FAA tools]	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
[Falla97]	M. Falla, Results and Achievements from the DTI/EPSRC R&D Programme in

	Safety Critical Systems, Advances in Safety Critical Systems, June 1997, http://www.comp.lancs.ac.uk/computing/resources/scs/
[FAS_TAS]	FAS intelligence resource program: TAS webpage, http://www.fas.org/irp/program/process/tas.htm
[FaultInjection]	Web page on Fault Injection, http://www.cigitallabs.com/resources/definitions/fault_injection.html
[FEA web]	Front-End Analysis web page, http://www.ale.com/Pages/feamain.htm
[Fields01]	R.E. Fields, Analysis of erroneous actions in the design of critical systems, Submitted for the degree of Doctor of Philosophy, University of York, Human Computer Interaction Group, Department of Computer Science, January 2001, http://www.cs.york.ac.uk/ftpdir/reports/YCST-2001-09.pdf
[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
[FuzzyLogic]	Web page on Fuzzy Logic, http://www-2.cs.cmu.edu/Groups/AI/html/faqs/ai/fuzzy/part1/faq.html
[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
[Genesereth00]	M. Genesereth, Thruth Table Method and Propositional Proofs, Computational logic, Lecture 3, Spring 2000, http://logic.stanford.edu/classes/cs157/2002/lectures/lecture03.pdf
[HAIL]	Human Automation Integration Laboratory, (HAIL), http://www.engr.sjsu.edu/hfe/hail/software.htm
[HEA practice]	Human Error Analysis, Error Mode Analysis – Single assessor method, Emergency Shutdown Workshop, "hea-practice.ppt"
[HEA-theory]	Human error Analysis, Theory and Concepts, Techniques and Practice, Cognitive Error Analysis, “hea.theory.ppt”
[HEIDI taxonomy]	HEIDI taxonomy, http://www.eurocontrol.int/safety/GuidanceMaterials_HeidiTaxonomy.htm
[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
[HIFA_perform]	Eurocontrol EATMP HIFA data: performance assessment, http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_performanceasses.html
[HIFA_safety]	Eurocontrol EATMP HIFA data: safety analysis, http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_safetyanalysis.html
[HIFA_sysdesig]	Eurocontrol EATMP HIFA data: system design & analysis, http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_sysdesig_analysis.html
[HIFA_taskanalysis]	Eurocontrol EATMP HIFA data: task analysis,

	http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_taskanalysis.html
[HIFA_usability]	Eurocontrol EATMP HIFA data: usability, http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_usability.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
[Hollamby97]	D. Hollamby, Non Destructive Inspection, School of Aerospace and Mechanical Engineering, University of New South Wales, AMEC 4018, Course Notes, July 1997, http://octarine.adfa.edu.au:8080/~kks/NDI/chap1-intro.rtf
[Hollnagel93]	E. Hollnagel, Human Reliability analysis, context and control. Academic Press, London, 1993.
[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
[HRA Washington01]	Draft proceedings HRA Washington workshop, Building the new HRA - Errors of Commission - from research to application, Headquarters US NRC, Rockville, Maryland, USA, 7-9 May 2001, "Draft proceedings HRA Washington workshop.zip"
[HSEC02]	Health Safety and Engineering Consultants Ltd, Techniques for addressing rule violations in the offshore industries, Offshore Technology report 2000/096, 2002, http://www.hse.gov.uk/research/otopdf/2000/oto00096.pdf
[HumanFactors]	http://204.108.6.23/Working%20Groups/WGB/M&Ts/HF_tools.html#Aircrew%20Incident%20Reporting%20System%20(AIRS)
[Humphreys88]	P. Humphreys, Human reliability assessors guide, Safety and Reliability Directorate UKAEA (SRD) Report No TRS 88/95Q, October 1988.
[IDKB]	IDKB, Instructional Design Knowledge Base, Perform a Front-End analysis http://classweb.gmu.edu/ndabbagh/Resources/Resources2/FrontEnd.htm
[IHF-SEAMAID]	Institute of Human Factors, http://www.nupec.or.jp/english/1999_en/44-45.pdfhttp://www.nupec.or.jp/english/2000_en/46-47.pdf
[Infopolis2]	Infopolis 2 Consortium, Ergonomics Methods and Tools, http://www.ul.ie/~infopolis/methods/incident.html
[Inspections]	Reviews, Inspections, and Walkthroughs, http://www.ebgconsulting.com/Reviews-Inspection-Walkthroughs.pdf
[IPME web]	IPME web page, Micro Analysis & Design, http://www.maad.com/MaadWeb/products/ipme/ipmema.htm
[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
[Isaac&al99]	A. Isaac, S.T. Shorrock, R. Kennedy, B. Kirwan, H. Anderson, T. Bove, The Human Error in ATM (HERA) technique, 20 June 1999, "hera.doc"
[Isaac&Pounds01]	A.Isaac and J. Pounds, Development of an FAA-Eurocontrol Technique for the Analysis of Human Error in ATM, 4th USA/Europe ATM R&D Seminar,

	Santa Fe, 3-7 December 2001, http://atm2001.eurocontrol.fr/finalpapers/pap149.pdf
[ISO/IEC 15443]	ISO/IEC, Information technology - Security techniques - A framework for IT security assurance – Part 2: Assurance methods, ISO/IEC 15443-2 PDTR1, 2 Oct 2002, http://www.gammassl.co.uk/ist33/27n3234.pdf
[Jackson]	http://cisx2.uma.maine.edu/NickTemp/JSP&JSDLec/jsd.html and http://panoramix.univ-paris1.fr/CRINFO/dmrg/MEE/misop002/
[JAR 25.1309]	Joint Aviation Requirements JAR - 25, Large Aeroplanes, Change 14, 27 May 1994, and Amendment 25/96/1 of 19 April 1996, including AMJ 25-1309: System design and analysis, Advisory Material Joint, Change 14, 1994.
[Jeffcott&Johnson]	M. Jeffcott, C. Johnson, The use of a formalised risk model in NHS information system development, http://www.dcs.gla.ac.uk/~shellyj/NHS%20paper-CTW%20version.pdf
[Jones&Bloomfield&Froome&Bishop01]	C. Jones, R.E. Bloomfield, P.K.D. Froome, P.G. Bishop, Methods for assessing the safety integrity of safety-related software of uncertain pedigree (SOUP), Adelard, Health and safety executive, contract research report 337/2001, http://www.hse.gov.uk/research/crr_pdf/2001/crr01337.pdf
[Keidar&Khazan00]	I. Keidar and R. Khazan, A virtually synchronous group multicast algorithm for WANs: formal approach, http://www.ee.technion.ac.il/~idish/ftp/vs-sicomp.pdf, Extended paper version of 'A Client-Server Approach to Virtually Synchronous Group Multicast: Specifications and Algorithms', 20th International Conference on Distributed Computing Systems (ICDCS 2000), April 2000, pages 344-355.
[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"
[Keong97]	T.H. Keong, Risk Analysis Homepage, http://pachome1.pacific.net.sg/~thk/ and http://home.pacific.net.sg/~thk/quant_r.html
[Kirwan&Ainsworth92]	A guide to task analysis, edited by B. Kirwan and L.K. Ainsworth, Taylor and Francis, 1992
[Kirwan&al97]	B. Kirwan, A. Evans, L. Donohoe, A. Kilner, T. Lamoureux, T. Atkinson, and H. MacKendrick, Human Factors in the ATM System Design Life Cycle, FAA/Eurocontrol ATM R&D Seminar, 16 - 20 June, 1997, Paris, France, http://atm-seminar-97.eurocontrol.fr/kirwan.htm
[Kirwan&al97-II]	B. Kirwan, R. Kennedy, S. Taylor-Adams, B. Lambert, The validation of three human reliability quantifiction techniques – THERP, HEART and JHEDI: Part II – Results of validation exercise, Applied Ergonomics, Vol 28, No 1, pp. 17-25, 1997, http://www.class.uidaho.edu/psy562/Readings/Kirwin%20(1997)%20A%20II.pdf
[Kirwan&Basra&Taylor.doc]	B. Kirwan, G. Basra and S.E. Taylor-Adams, CORE-DATA: A computerised Human Error Database for Human reliability support, Industrial Ergonomics Group, University of Birmingham, UK, "IEEE2.doc"
[Kirwan&Basra&Taylor.ppt]	B. Kirwan, G. Basra and S.E. Taylor-Adams, CORE-DATA: A computerised Human Error Database for Human reliability support, Industrial Ergonomics Group, University of Birmingham, UK, "core-data.ppt"
[Kirwan&Kennedy&Hamblen]	B. Kirwan, R. Kennedy and D. Hamblen, Human reliability assessment in probabilistic safety assessment - guidelines on best practice for existing gas-cooled reactors, "Magnox-IBC-final.doc"
[Kirwan_HCA]	B. Kirwan, Developing human informed automation in Air Traffic

	Management, "HCApaper2.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
[Kirwan98-2]	B. Kirwan, Human error identification techniques for risk assessment of high risk systems – Part 2: Towards a framework approach, Applied Ergonomics, Vol 29, No 5, pp. 299-318, 1998, http://www.class.uidaho.edu/psy562/Readings/Kirwan%20(1998)%20A%202.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.
[Klompstra&Everdij97]	M.B. Klompstra, and M.H.C. Everdij, Evaluation of JAR and EATCHIP safety assessment methodologies, NLR report CR 97678 L, Amsterdam, 1997.
[Kos&al00]	J. Kos, H.A.P. Blom, L.J.P. Speijker, M.B. Klompstra, and G.J. Bakker, Probabilistic wake vortex induced accident risk assessment, 3rd USA/Europe Air Traffic Management R&D Seminar, FAA/Eurocontrol, 2000, http://atm-seminar-2000.eurocontrol.fr/acceptedpapers/pdf/paper56.pdf.
[Kosmowski00]	K.T. Kosmowski, Risk analysis and management on socio-technical systems, SafetyNet meeting, Athens, Greece, 7010 June 2000, http://www.safetynet.de/Publications/articles/Kosmowski.PDF
[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
[Leavengood98]	S. Leavengood, Techniques for Improving Process and Product Quality in the Wood Products Industry: An Overview of Statistical Process Control, A Microsoft Powerpoint Presentation, 16 May, 1998, http://wood.oregonstate.edu/spc/ppoint.htm
[Leuchter&al97]	S. Leuchter, C. Niessen, K. Eyferth, and T. Bierwagen, Modelling Mental Processes of Experienced Operators during Control of a Dynamic Man Maschine System, In: B.B. Borys, G. Johannsen, C. Wittenberg & G. Stätz (eds.): Proceedings of the XVI. European Annual Conference on Human Decision Making and Manual Control, pp. 268–276. Dec. 9-11, 1997, University of Kassel, Germany. http://www.zmms.tu-berlin.de/~sandro/doc/anumanu97.pdf
[Leveson02]	N.G. Leveson, An approach to designing safe embedded software, A

	Sangiovanni-Vincentelli and J. Sifakis (Eds): EMSOFT 2002, LNCS 2491, pp. 15-29, 2002, Springer-Verlag Berlin Heidelberg, 2002
[Leveson95]	N.G. Leveson, Safeware, system safety and computers, a guide to preventing accidents and losses caused by technology, Addison-Wesley, 1995
[Loeve&Moek&Arsenis96]	J.A. Loeve, G. Moek, S.P. Arsenis, Systematic Safety - Study on the feasibility of a structured approach using a quantified causal tree, WP2: Statistical work, NLR CR 96317 L, 1996
[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
[Lygeros&Pappas&Sastry98]	J. Lygeros, G.J. Pappas, S. Sastry, An approach to the verification of the Center-TRACON automation system, Proceedings 1st International Workshop Hybrid Systems: Computation and Control, 1998, pp. 289-304.
[Macwan&Mosley94]	A. Macwan, A. Mosley, A methodology for modelling operator errors of commision in probabilistic risk assessment, Reliability Engineering and System Safety, Vol. 45, pp. 139-157, 1994.
[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
[Markov process]	http://www-net.cs.umass.edu/pe2002/notes/markov2.pdf
[MAS611-2]	Powerpoint slides, www.ec.erau.edu/cce/faculty/mas611-2.ppt
[MASCOT]	Design of Real Time Systems Introduction, cs32005, Systems Engineering 3, http://www.dcs.napier.ac.uk/~rcr/cs32005/Mascot/tsld001.htm
[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
[May97]	A. May, Neural network models of human operator performance, The Aeronautical Journal, pp. 155-158. April 1997
[Mazor&al95]	E. Mazor, A. Averbuch, Y. Bar-Shalom, J. Dayan, Interacting Multiple Model Methods in Target Tracking: A Survey, http://www.ewh.ieee.org/soc/aes/taes/aes341/341103.htm
[McClure&Restrepo99]	P. J. McClure and L.F. Restrepo, Preliminary Design Hazard Analyses (PDHA) for the Capabilities Maintenance and Improvement Project (CMIP) and Integration of Hazard Analysis Activities at Los Alamos National Laboratory, 1999, http://www.efcog.org/publication/WG%20Minutes/sawg/1999%20Conference/docs/workshop/p5-2.pdf
[McCraw-Hill02]	McCraw-Hill, 2002, Chapter 6: Intermediate Object Technology, slides, http://www.aat1.com/mahnomen/cwuj2/062002jcnch6_slides.pdf
[McDermid&Pumfrey]	J.A. McDermid, D.J. Pumfrey, Software safety: why is there no consensus, http://www-users.cs.york.ac.uk/~djp/publications/ISSC_21_final_with_refs.pdf
[McDermid01]	J.A. McDermid: Software safety; where is the evidence, Sixth Australian workshop on industrial experience with safety critical systems and software (SCS01), Brisbane, Conferences in Research and Practice in information technology, Vol 3, P. Lindsay (Ed), 2001, http://www.jrpit.flinders.edu.au/confpapers/CRPITV3McDermid.pdf
[MDA press release97]	MDA press release, 27 November 1997, http://www.mda.ca/news/pr/pr71127A.html
[MEDA]	Boeing website on MEDA, http://www.boeing.com/commercial/flighttechservices/ftssafety03.html

[Meek&Siu89]	B. Meek and K.K. Siu, The effectiveness of error seeding, ACM Sigplan Notices, Vol 24 No 6, June 1989, pp 81-89, http://www.kcl.ac.uk/kis/support/cit/staff/brian/seed.html
[Megaputer Web]	Megaputer, Machine learning algorithms: Link analysis webpage, http://www.megaputer.com/products/pa/algorithms/la.php3
[Melham&Norrish01]	T. Melham and M. Norrish, Overview of Higher Order Logic Primitive Basis, University Glasgow, 2001, http://www.cl.cam.ac.uk/users/mn200/hol-training/basis.pdf; see also http://www.cl.cam.ac.uk/users/mn200/hol-training/
[MHF-RGN10]	Major Hazard Facilities Regulations Guidance Note, MHD-GN10, September 2001, http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN10.pdf
[MIL-HDBK]	MIL-HBDK-46855A, Department of Defense Handbook, Human Engineering Program Process and Procedures, 17 May 1999, http://www.hf.faa.gov/docs/46855ndx.pdf
[MindTools-DTA]	MindTools webpage, Decision Trees, http://www.mindtools.com/dectree.html
[Minutes 10 Sept]	M.H.C. Everdij, Minutes 10 September meeting Safety Methods Survey project
[Minutes SMS]	M.H.C. Everdij, Minutes of 9 July 2002 kick-off meeting Safety Methods Survey project, 16 July 2002, Final.
[Mislevy&al98]	R.J. Mislevy, L.S. Steinberg, F.J. Breyer, R.G. Almond, L. Johnson, A Cognitive task analysis, with implications for designing a simulation-based performance assessment, CSE Technical Report 487, August 1998, http://www.cse.ucla.edu/CRESST/Reports/TECH487.PDF
[Mizumachi&Ohmura77]	M. Mizumachi and T. Ohmura, Electronics and communications in Japan, Vol 60-B, pp. 86-93, 1977.
[Moek84]	G. Moek, "Methoden voor risicobepaling en risico evaluatie", NLR Memorandum MP 84019 U, 1984. (In Dutch)
[Moriarty83]	R. Moriarty, System safety engineering and management, Wiley Interscience, 1983.
[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
[MSC]	http://tele.informatik.uni-freiburg.de/~leue/msc.html and http://www.cs.uct.ac.za/Research/DNA/msc.html
[Mucks&Lesse01]	H.J. Mucks, L.A. Jesse, Web-enabled Timeline analysis system (WebTAS), http://www.whitehousedrugpolicy.gov/ctac/ctac01/pdfs/13/WebBasedTimelineAnalysisSystem.pdf
[MUFTIS1.2]	J.M. Gouweleeuw, A.J. Hughes, J.L. Mann, A.R. Odoni, K. Zografos, MUFTIS workpackage report 1.2 Final report on Global MSR studies Part 2: Review of available techniques/facilities, NLR TR 96406 L, 1996
[MUFTIS3.2-I]	M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom, O.N. Fota, MUFTIS work package report 3.2, final report on safety model, Part I: Evaluation of hazard analysis techniques for application to en-route ATM, NLR TR 96196 L, 1996
[MUFTIS3.2-II]	M.H.C. Everdij, M.B. Klompstra and H.A.P. Blom, MUFTIS workpackage report 3.2 Final report on Safety Model Part II: Development of mathematical techniques for ATM safety analysis, NLR TR 96197 L, 1996
[MurTon]	MurTon Quality toolbox web page, http://www.murtongroup.com/documentation/process1.htm
[Narkhede02]	D.D. Narkhede, Credit Seminar on Bayesian Model for Software Reliability,

	Reliability Engineering, Indian Institute of Technology, Bombay, 2002, http://www.ee.iitb.ac.in/uma/~dineshn/Bayesian.pdf
[NASA-Assist01]	NASA, Assist web page, 2001, http://shemesh.larc.nasa.gov/people/rwb/assist.html
[NASA-GB-1740.13-96]	NASA-GB-1740.13-96, NASA Guidebook for Safety Critical Software - Analysis and Development, NASA Lewis Research Center, Office of Safety and Mission Assurance, http://swg.jpl.nasa.gov/docs/safety/main_body.pdf
[NASA-RCM]	NASA Reliability Centered Maintenance Guide for Facilities and Collateral Equipment, http://www.hq.nasa.gov/office/codej/codejx/rcm-iig.pdf
[NASA-STD-8719]	NASA-STD-8719.13A, Software Safety NASA Technical Standard, 15 September, 1997, http://satc.gsfc.nasa.gov/assure/nss8719_13.html or http://satc.gsfc.nasa.gov/assure/distasst.pdf
[NEA01]	Nuclear Energy Agency, Experience from international nuclear emergency exercises, The INEX 2 Series, 2001, http://www.nea.fr/html/rp/reports/2001/nea3138-INEX2.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
[NEA99]	Nuclear Energy Agency, Identification and assessment of organisational factors related to the safety of NPPs, Contributions from Participants and Member Countries, September 1999, http://www.nea.fr/html/nsd/docs/1999/csni-r99-21-vol2.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
[Niessen&Eyferth01]	C. Niessen, K. Eyferth, A Model of the Air Traffic Controller's Picture. Safety Science, Vol. 37, pp. 187-202, 2001.
[Niessen&Leuchter&Eyferth98]	C. Niessen, S. Leuchter, K. Eyferth, A psychological model of air traffic control and its implementation. In: F.E. Ritter & R.M. Young (eds), Proceedings of the second European conference on cognitive modelling (ECCM-98). Nottingham: University Press. S. pp. 104-111, 1998.
[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/
[NRC-status99]	Nuclear Regulatory Commission, Status report on Accident Sequence Precursor program and related initiatives, 20 December 1999, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/1999/secy1999-289/1999-289scy.html
[NSC-ANSTO]	Report on the ANSTO application for a licence to construct a replacement research reactor, Addressing Seismic Analysis and Seismic Design Accident Analysis Spent Fuel and Radioactive Wastes, February 2002, http://www.arpansa.gov.au/pubs/rrrp/nsc150302.pdf
[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/
[NUREG CR6753]	US Nuclear Regulatory Commission NUREG, Review of findings for human error contribution to risk in operating events, August 2001, http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6753/
[OL glossary]	University of Mannheim Glossary, Organisational Learning entry, 10 November 1997, http://www.sfb504.uni-mannheim.de/glossary/orglearn.htm

[OmolaWeb]	Omola and Omsim webpage, http://www.control.lth.se/~cace/omsim.html
[OORM00]	Overview of reliability models, December 2000, http://www.jump.net/~arclight/reliability/lisa/
[ORM]	Operational Risk Management User Traning, slides http://www.safetycenter.navy.mil/presentations/aviation/sourcefile/ormusertraining.ppt
[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.
[Peacock&al01]	R.D. Peacock, R.W. Bukowski, P.A. Reneke, and J.D. Averill, S.H. Markos, Development of a fire hazard assessment method to evaluate the fire safety of passenger trains, Building and Fire Research Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, USAVolpe National Transportation Systems Center, U.S. Department of Transportation, Cambridge, MA 02142, USA, Reprinted from the Fire and Materials 2001. 7th International Conference and Exhibition. Proceedings. Interscience Communications Limited. January 22-24, 2001, San Antonio, TX, 67-78 pp, 2001, http://fire.nist.gov/bfrlpubs/fire01/PDF/f01160.pdf
[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
[Petkov99]	G. Petkov, Networked risk in human action context, http://www.cogtech.org/CT99/Petkov.htm
[PetriNets World]	Welcome to the Petri Nets world, http://www.daimi.aau.dk/~petrinet
[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
[Pozsgai&Neher&Bertsche02]	P. Pozsgai, W. Neher, B. Bertsche, Models to Consider Dependence in Reliability Calculation for Systems Consisting of Mechanical Components, 2002, http://www.math.ntnu.no/mmr2002/papers/contrib/Pozsgai.pdf
[PROMAI5]	Human factors contribution to quantitative methods survey, Progress in Maintenance and Management of Railway Infrastructure, Contribution to Report to Council of Decision Makers – 01/12/01, 2001, “PROMAI5.doc”, http://promain.server.de/servlet/is/270/PROMAI5.doc?command=downloadContent&filename=PROMAI5.doc
[Pygott&al99]	C. Pygott, R. Furze, I. Thompson and C. Kelly, Safety Case Assessment Approach for ATM, ARIBA WP5 final report, 1999, http://www.nlr.nl/public/hosted-sites/ariba/rapport5/frame.htm
[Qiu&al]	S. Qiu, A.M. Agogino, S. Song, J. Wu, S. Sitarama, A fusion of Bayesian and

	fuzzy analysis for print faults diagnosis, http://best.me.berkeley.edu/~aagogino/papers/ISCA-Fusion.pdf
[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.
[RAIT slides]	Slides on RAIT, http://faculty.erau.edu/dohertys/325/325_last.ppt
[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.
[Reer97]	B. Reer, Conclusions from Occurrences by Descriptions of Actions (CODA), Abstract of Meeting Paper, Society for Risk Analysis – Europe, 1997 Annual Meeting, http://www.riskworld.com/Abstract/1997/Europe97/eu7ab220.htm
[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
[REHMS-D]	Web page on REHMS-D, http://dtica.dtic.mil/ddsm/srch/ddsm107.html
[Reich64]	P.G. Reich, A theory of safe separation standards for Air Traffic Control, Technical report 64041, Royal Aircraft Establishment, U.K., 1964.
[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.
[Ridley&Andrews01]	L.M.Ridley and J.D.Andrews, Application of the Cause-Consequence Diagram Method to Static Systems, Department of Mathematical Sciences, Loughborough University, Loughborough, Leicestershire, 2001, http://www.lboro.ac.uk/departments/ma/preprints/papers01/01-22.pdf
[RMA web]	Web site on Rate Monotonic Analysis, http://www.sei.cmu.edu/str/descriptions/rma_body.html
[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.
[Roelen&al00]	A.L.C. Roelen (NLR), L.J. Bellamy (SAVE), A.R. Hale (DUT), R.J. Molemaker (NEI), M.M. van Paassen (DUT), A causal model for the assessment of third party risk around airports; Feasibility of the development of a causal model for the assessment of third party risk around airports, Main Report, April 2000, http://www.tripod.nl/Downloadables/Nieuw_april/Articles/causal.pdf
[Rowe99]	L.A. Rowe, Interface testing, Slides, April 1999, http://bmrc.berkeley.edu/courseware/cs160/spring99/Lectures/17b-InterfaceTesting/sld001.htm
[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
[Schram&Verbruggen98]	G. Schram, H.B. Verbruggen, A fuzzy logic approach to fault-tolerant control, Journal A, Vol 39, No 3, pp. 14-21, 1998
[Schuppen98]	J.H. van Schuppen, A sufficient condition for controllability of a class of hybrid systems, Proceedings 1st International Workshop Hybrid Systems: Computation and Control, 1998, pp. 374-383.
[SCM biblio]	Bibliography on Software Configuration Management, http://liinwww.ira.uka.de/bibliography/SE/scm.html
[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.
[SEC-SHA]	Safeware Engineering Corporation, System Hazard Analysis, http://www.safeware-eng.com/software-safety/system-analysis.shtml
[Seignette02]	R. Seignette, RINA, Formal safety assessment of bulk carriers, International collaborative study, Work Package 9b, Detailed task inventory, Report No: GM-R0342-0108-1400, 2002, http://www.mcga.gov.uk/aboutus/bulkcarriers/fsa/RR0342-1400_Rev2_final.pdf
[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
[Sherry&al00]	L.M. Sherry, M. Feary, P. Polson and E. Palmer, Autopilot totor: building and maintaining autopilot skills, In Proceedings Int. Conf. on Human Computer Interaction –AERO, Toulouse, France, 2000
[Sherry&al01]	L.M. Sherry et al., In: Int J. of Human Factors and Aerospace Safety, 2001.
[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"
[Shorrock&Kirwan99]	S. Shorrock and B. Kirwan, The development of TRACEr: a technique for the retrospective analysis of cognitive errors in ATM, Ed: D. Harris, Engineering psychology and cognitive ergonomics, Volume 3, Transportation systems, medical ergonomics and training, Ashgate, 1999, pp. 163-171.
[Shorrock01]	S.T. Shorrock, Error classification for Safety Management: Finding the right approach, DNV Ltd, 2001, “error-classification.doc”
[Silva&al99]	J.S. Silva, K.S. Barber, T. Graser, P. Grisham, S. Jernigan, L. Mantock, The knowledge-based integrated design and development environment (KIDDE) integrating a formal KA process and requirements representation with a JAD/RAD development approach, 1999, http://sern.ucalgary.ca/KSI/KAW/KAW99/papers/Silva1/Silva.pdf
[SINTEF-RCM]	SINTEF website on Reliability Centered Maintenance, http://www.sintef.no/units/indman/sipaa/prosjekt/rcm.html
[Sipser97]	M. Sipser, Introduction to the theory of computation, PWS publishing company, Boston, 1997.
[Siu94]	N. Siu, Risk assessment for dynamic systems: An overview, Reliability Engineering and System Safety, Vol. 43, pp. 43-73, 1994.
[Skutt01]	T. Skutt, Software Partitioning Technologies, Smiths Aerospace, 2001,

	http://www.dtic.mil/ndia/2001technology/skutt.pdf
[Smartdraw]	Smartdraw web page, How to draw data flow diagrams, http://www.smartdraw.com/resources/centers/software/dfd.htm; see also http://www.pitt.edu/~laudato/DATAFLOW/index.htm
[Smith&al98]	S. Smith, D. Duke, T. Marsh, M. Harrison and P. Wright, Modelling Interaction in Virtual Environments, 1998, http://www.cs.york.ac.uk/hci/inquisitive/papers/ukvrsig98/int98/smith-ukvrsig98b.pdf
[Smith9697]	E. Smith, Hazard analysis of route separation standards for Eurocontrol, DNV Technica, 1996 and 1997
[SOI terms]	Safety of Industry, Terminology and Abbreviations, http://mujweb.atlas.cz/www/bezpecnost/terminology.html
[SPARK web]	SPARK web page, http://www.cse.secs.oakland.edu/edslabs/about/spark.asp
[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
[SPF-safety01]	NATS/Eurocontrol, Strategic Performance Analysis and Forecast Service, SPF_SAFETY report, Issue 2.0, 27 July 2001, Ref. SCS/SPAF/FIM/DOC/00/12
[SPS2001]	SPS2001 Project Team, Fagan Inspections, http://proj-sps2001.web.cern.ch/proj-sps2001/Minutes/CodeReviews/FaganInspections.htm
[SQUALE99]	SQUALE Evaluation Criteria, January 1999, http://www.newcastle.research.ec.org/squale4.pdf
[SSCS]	Software for Safety Critical Systems, Fault Tolerant Systems, Lecture 12, www.cs.strath.ac.uk/teaching/ug/classes/52.422/fault.tolerance.doc
[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
[Statematelatos]	M.G. Stamatelatos, Risk assessment and management, tools and applications, slides, http://smo.gsfc.nasa.gov/crm/crm_publications/presentation_1.pdf
[Stobart&Clare94]	R. Stobart, J. Clare, SUSI methodology evaluating driver error and system hazard, 27th International Symposium on Advanced Transportation pp. 1-8, Oct 1994
[Storey96]	N. Storey, Safety-Critical Computer Systems, Addison-Wesley, Edinburgh Gate, Harlow, England, 1996
[Straeter&al99]	O. Straeter, B. Reer, V. Dang, S. Hirschberg, Methods, case studies, and prospects for an integrated approach for analyzing errors of commission, Safety and Reliability, Proceedings of the ESREL99 – The Tenth European Conference on Safety and Reliability, Munich-Garching, Germany, 13-17 September 1999, G.I. Schuëller and P. Kafka (Eds), A.A. Balkema, Rotterdam/Brookfield, 1999, “EOC-Esrel99.pdf” or “Esrel99-Str-ua.pdf”
[Straeter_CAHR]	O. Straeter, Illustration of CAHR Databank System, http://www.lfe.mw.tu-muenchen.de/cahr/W-CHARe.htm
[Straeter00]	O. Straeter, Evaluation of human reliability on the basis of operational experience, Dissertation, Gesellschaft für Anlagen und Reaktorsicherheit (GRS), August 2000, http://www.grs.de/grs_170.pdf
[Straeter01]	O. Straeter, The quantification process for human interventions, In: Kafka, P. (ed) PSA RID - Probabilistic Safety Assessment in Risk Informed Decision making. EURO-Course. 4.- 9.3.2001. GRS Germany, " L6_Paper.PDF"
[Stroeve&al01]	S.H. Stroeve, H.A.P. Blom, M.B. Klompstra, G.J. Bakker, M.N.J. van der Park, Accident risk assessment model for active runway crossing procedure, NLR-TR-2001-527, National Aerospace Laboratory NLR, 2001
[Stroeve&Blom&Park03	S.H. Stroeve, H.A.P. Blom, M. Van der Park, Multi-agent situation awareness

]	error evolution in accident risk modelling, 5th FAA/Eurocontrol ATM R&D seminar, 23-27 June 2003
[Stroup]	R. Stroup, An approach to the software aspects of safety management, FAA, http://www2.faa.gov/aio/common/documents/Safety/SofSafMgmt.pdf
[Task Time]	Powerpoint slides on Timeline analysis, "Task-time.ppt"
[Telelogic Objectgeode]	Telelogic Objectgeode webpage, http://www.telelogic.com/products/additional/objectgeode/index.cfm
[Telelogic Tau]	Telelogic Tau webpage, http://www.telelogic.com/products/tau/
[Terpstra84]	K. Terpstra, Phased mission analysis of maintained systems. A study in reliability and risk analysis, Netherlands energy research foundation, ECN Memorandum, 1984.
[THEMES01]	THEMES WP4, Deliverable D4.1, Report on updated list of methods and critical description, D'Appolonia S.p.A, June 2001
[Timeline Web]	Visualize Analyze Communicate, Timeline analysis webpage, http://www.i2.co.uk/techniques/timeline.html
[Tomlin&Lygeros&Sastry98]	C. Tomlin, J. Lygeros, S. Sastry, Synthesising controllers for nonlinear hybrid systems, Proceedings 1st International Workshop Hybrid Systems: Computation and Control, 1998, 360-373.
[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
[TRM web]	Web page on Crew Resource Management, http://www.globalairtraining.com/business_trm.htm
[Uhlarik&Comerford02]	J. Uhlarik and D. Comerford, A review of situation awareness literature relevant to pilot surveillance functions, Department of Psychology, Kansas State University, March 2002, http://www.cami.jccbi.gov/AAM-400A/Abstracts/2002/FULL%20TEXT/0203.pdf
[UML]	http://www.rational.com/uml/index.jsp?SMSESSION=NO
[Vakil00]	S.S. Vakil, Analysis of Complexity Evolution Management and Human Performance Issues in Commercial Aircraft Automation Systems, Submitted to the Department of Aeronautics and Astronautics in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy at the Massachusetts Institute of Technology, May 19, 2000, http://icat-server.mit.edu/Library/Download/98_ICAT-2000-3.pdf
[Vanderhaegen&Telle98]	F. Vanderhaegen and B. Telle, APRECIH : vers une méthode d'analyse des conséquences de l'infiabilité humaine, Compte-Rendu de la Réunion S3 du 19 mai 1998, http://www.univ-lille1.fr/s3/fr/cr-19-5-98.htm
[VanEs01]	G.W.H. Van Es, A Review of Civil Aviation Accidents Air Traffic Management Related Accidents:1980-1999, 4th International Air Traffic Management R&D Seminar New-Mexico, December 3rd-7th, 2001
[Vesely70]	W.E. Vesely, A time dependent methodology for fault tree evaluation, Nuclear engineering and design, Vol. 13, pp. 337-360, 1970.
[Villemeur91-1]	A. Villemeur, Reliability, availability, maintainability and safety assessment, Volume 1: Methods and Techniques, John Wiley and Sons, Inc., 1991.
[Vinnem00]	J.E. Vinnem, R&D into operational safety aspects of FPSO/Shuttle Tanker collision hazard, 2000, http://213.179.37.66/Preventor/ukooa_05122000_jev.pdf
[Wassell92]	A.B. Wassell, Safety and reliability in the air, 16th Croxson Memorial Lecture, Cranfield, pp. 315-318, Dec 1992
[Weinberg&Lynch&De	H.B. Weinberg, N. Lynch, N. Delisle, Verification of automated vehicle

lisle96]	protection systems, Hybrid Systems III, Verification and control, R. Alur et al. (eds.), Springer, 1996, pp. 101-113
[Wickens92]	C.D. Wickens, Engineering, psychology and human performance, Merrill, 1992
[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.
[Williams91]	L.G. Williams, Formal Methods in the Development of Safety Critical Software Systems, Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48, November 1991
[Wilson&al96]	S.P. Wilson, J.A. McDermid, C.H. Pygott, D.J. Tombs, Assessing complex computer based systems using the goal structuring notation, pp. 1-8, 1996
[Wolfram02]	S.A Wolfram, New Kind of Science, Notes for Chapter 9: Fundamental Physics, Section: Time and Causal Networks, Page 1032, http://www.wolframscience.com/reference/notes/1032f
[Wright&Fields&Harrison94]	P. Wright, B. Fields and M. Harrison, Deriving human error tolerance Requirements from tasks, Proceedings ICRE'94 – IEEE International Conference on Requirements Engineering, Colorado 1994, www.cs.mdx.ac.uk/staffpages/bobf/papers/ICRE94.ps
[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.