ANNEX A

SAFETY ASSESSMENT TOOLS AND TECHNIQUES

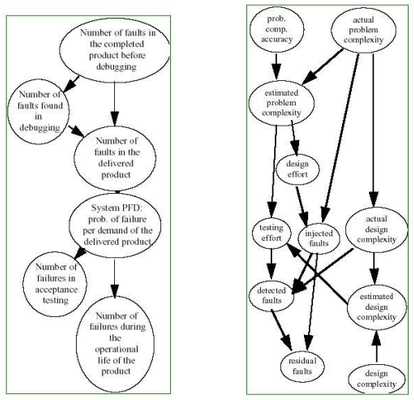
Note: The right tool applied to the right situation can contribute to the efficiency of an investigation or an analysis. Tools can help to facilitate teamwork, enable a systematic and transparent approach, communicate findings, and manage complex investigations. However, the benefits of using tools are far from automatic.
The table in this Annex has been compiled from a variety of sources (ranging from textbooks, publications, and the internet, to personal experience of friends, colleagues and acquaintances).
Each of these tools has its own advantages and disadvantages and the extent to which these can be used in during various phases of the product lifecycle, and the degree to which it can be applied to Safety Assessments, vary. A toolkit (rather than "one-size-fits-all") approach is advocated as each tool has a distinctive function and range of application. Listed in alphabetical order, the tools/techniques most frequently used by the author have been shaded.

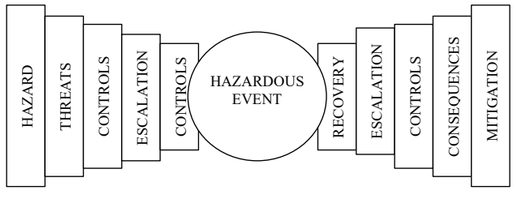
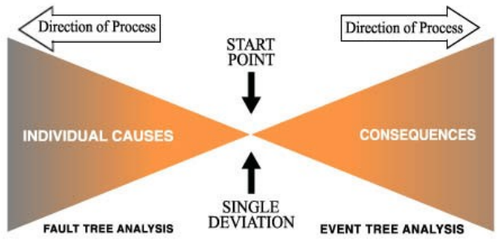
It is extremely important to note that as the complexity of the tool increases so does the degree of training required for the user and/or the need for an experienced evaluation team to conduct the evaluation. On the plus side, the data derived from the more complex methodologies may be more supportable. Unfortunately, the primary disadvantage of such tools is that "trained subject matter experts" may have limited experience in the actual operational environment and, therefore, their evaluations may not be entirely applicable to the certification

This table is intended to be thought provoking but has all the limitations of generic data. In no circumstances should it be considered complete, applicable to all systems or wholly objective. Many entries have no advantages/limitations listed, and space is provided for the reader to add data if desired.

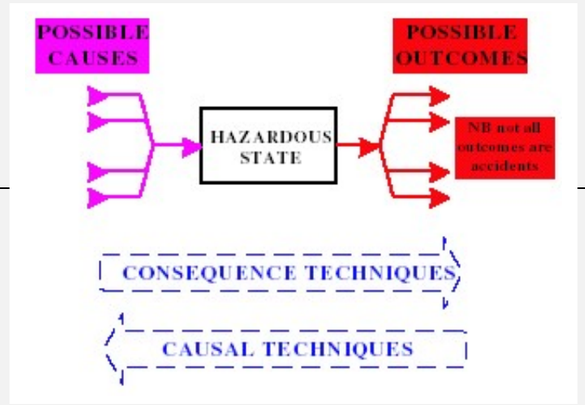
The author will gladly receive any comments/suggestions/recommendations. For the latest update on this table (including links to relevant websites), see www.aircraftsystemsafety.com

SAFETY ASSESSMENT TOOLS AND TECHNIQUES

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Accident Analysis	The purpose of the Accident Analysis is to evaluate the effect of scenarios that develop into credible and incredible accidents. Any accident or incident should be formally investigated to determine the contributors of the unplanned event. Many methods and techniques are applied.	▪	▪
Accident Sequence Evaluation Programme (ASEP)	This tool is based on the Technique for Human Error Rate Prediction (Swain and Guttman, 1983). ASEP comprises pre-accident screening with nominal human reliability analysis, and post-accident screening and nominal human reliability analysis facilities [Swain, 1987; Kirwan, 1994]	• ASEP provides a shorter route to human reliability analysis than THERP by requiring less training to use the tool, less expertise for screening estimates, and less time to complete the analysis.	•
Action Error Analysis	Action Error Analysis analyzes interactions between machine and humans. It is used to study the consequences of potential human errors in task execution related to directing automated functions. Any automated interface between a human and automated process can be evaluated, such as pilot / cockpit controls, or controller / display, maintainer / equipment interactions.	▪	▪
ATLAS	ATLAS is a software package for use in support of systems design and analysis work. it combines the elements of graphically-based task analysis with the advantages of a database. ATLAS supports a variety of conventional task analysis methods and incorporates more than 60 human performance, workload, and human reliability algorithms. [Hamilton, 1997]	•	•
Barrier Analysis	Any system is comprised of energy, should this energy become uncontrolled accid Barrier Analysis method is implemented by identifying energy flow (s) that may b prevent the unwanted energy flow form damaging equipment, and/or causing system damage. Barrier Analysis is an appropriate qualitative tool for systems analysis, safety revie [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 20  Figure 4.2. Example BBNs used in DATUM be in place to	▪	▪
Bayesian Belief Networks	A BBN is a graphical network that represents probabilistic relationships among events in a network structure. In a nutshell, it is a statistical procedure which utilizes prior distribution data to assess the probability of the result. These are often called conditional probabilities. The definition that explains it best for me comes from the last of these – it is: "The probability of a hypothesis C given some evidence E equals our initial estimate of the probability times the probability of the evidence given the hypothesis C divided by the sum of the probabilities of the data in all possible hypotheses." With BBNs, it is possible to articulate expert beliefs about the dependencies between different variables and to propagate consistently the impact of evidence on the probabilities of uncertain outcomes, such as 'future system reliability'[Falla, Ch4] The BBN on the left uses comparatively little evidence, depending only on the observed reliabilities and defect counts of previous products of the same process, and on the defects discovered in the current product during debugging. The topology of the graph is used to indicate probabilistic relationships among the variables described in the nodes. The BBN on the right includes subjective indicators, like problem complexity and design effort. Thus, this network is meant to be populated with probabilities that are not all derived from statistical inference, but at least in part from expert opinion. BBNs are also sometimes called Causal Probabilistic Networks, Probabilistic Cause-Effect Models or Probabilistic Influence Diagrams	• Provide decision-support for a wide range of problems involving uncertainty and probabilistic reasoning. • BBNs enable reasoning under uncertainty and combine the advantages of an intuitive visual representation with a sound mathematical basis in Bayesian probability. • BBNs allow an injection of scientific rigour when the probability distributions associated with individual nodes are simply "expert opinions". • A BBN will derive all the implications of the beliefs that are input to it, and some of these implications are statements of fact that can be checked against the observed reality of a software project, or simply against the experience of the experts and decision makers themselves.	• Because BBNs have a rigorous, mathematical meaning, software tools (i.e. efficient algorithms) are needed that can interpret them and perform the complex calculations needed in their use. •

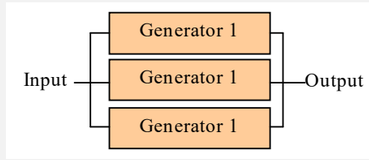
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Bellcore TR332 (now Telcordia)	The Bellcore approach is widely used in the telecommunications industry and has been updated to SR-332(in May 2001). Bellcore's approach is very similar to that of MIL-HDBK-217 but it's based primarily on telecommunications data and covers five separate use environments. The approach also assumes an exponential failure distribution and calculates reliability in terms of failures per billion part operating hours, or FITs. Its empirically based models are in three categories: The Method I parts count approach that applies when there is no field failure data available, the Method II modification to Method I to include lab test data and the Method III variation that includes field failure tracking. • Method I includes a first year modifier to account for infant mortality. • Method II includes a Bayes weighting procedure that covers three approaches depending on the level of previous burn-in the part or unit has undergone. • Method III includes a Bayes weighting procedure as well but it is based on three different cases depending on how similar the equipment is to that from which the data was collected. For the most widely used Method I case where the burn-in varies, the steady-state failure rate depends on the basic part steady-state failure rate and the quality, electrical stress and temperature factors as follows: $\lambda_{SSi} = \lambda_{Gi}\, \pi_{Qi}\, \pi_{Si}\, \pi_{Ti}$	▪ TR-332 is widely used in the telecommunications industry and is generally believed to more accurately predict the reliability of telecomm equipment than MIL-HDBK-217F	▪
Benefits Analysis	A assessment (either qualitative and/or quantitative) used to determine the potential benefits to be derived from following (or not following) a particular course of action See Cost Benefits Analysis	• Effective to compare/contrast different options	• Can be very subjective
Bent Pin Analysis	Connector shorts can cause system malfunctions, anomalous operations, and other risks. 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. [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000]	▪	▪
Bottom-Up Analysis Approach	Also known as the "hardware" methods, this starts with the hardware failure modes which can occur, and analyses the effects of these on the sub-system and the system. An example bottom-up approach is the FMEA	▪ Useful to identify the various failure modes of a specific module – especially if that module is safety critical ▪ Smaller parts are more manageable and lend themselves to controlled testing & evaluation [Garland, et at].	▪ A bottom-up approach for a complex system (with many combinations of failures together with the effects of crew and maintenance errors) may results in an impossible number of combinations. This may drive you to a top-down approach. ▪ May loose sight of the "big picture" ▪ Can be expensive and time consuming ▪ The whole is often more that the sum of its parts.
Bow Tie Analysis	Uses a methodology known as the Hazards and Effects Management Process, which requires hazards to be identified, assessed, controlled and if subsequently they are released, recovery measures to be in place to return the situation to normal if possible. The stages worked through in the Bow Tie are: • Proactive measures: - Identification of the Hazard. - Identification of the Threats that could release the hazard. - Assessment of the Threat Controls already in place and the identification of additional controls that may be necessary to manage the threat effectively. - Identification of the Escalation Factors that are conditions that prevent a threat control being effective. - Assessment of the Escalation Controls, which are further measures needed to maintain control of the escalation factor. - Identification of the Hazardous Event, which is the initial release of the hazard that can lead to an accident.   • Reactive measures: - Assessment of the Recovery Measures that would be appropriate to return the situation to as near to normal as possible. - Identification of the Escalation Factors that are conditions that prevent a recovery measure being effective. - Assessment of the Escalation Controls, which are further measures needed to maintain control of the escalation factor.	• Has both proactive and reactive elements that systematically works through the hazard and its management. • The output of the bow tie analysis is tested against the risk assessment matrix, where judgements can be made as to the probability of a hazardous event occurring and the severity of its consequences. • Useful aid to any Safety Management System	• Very time consuming and expensive to generate if not adequately prioritised. • Needs continuous management to reflect the current reliability
Brain storming	Uses a team of knowledgeable people to work in an imaginative and non-critical atmosphere to solve problems. .	• This can be applied to hazard identification, where "thinking the unthinkable" can suggest possible accidents and problems which the designer may never have considered.	• There is little framework to ensure that the exercise is systematic and **all** hazards have been identified. •
Cable Failure Matrix Analysis	Less then adequate design of cables can result in faults, failures, and anomalies, which can result in contributory hazards and accidents. Should cables become damaged system malfunctions can occur. Cable Failure Matrix Analysis identifies the risks associated with any failure condition related to cable design, routing, protection, and securing. [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000]	▪	▪

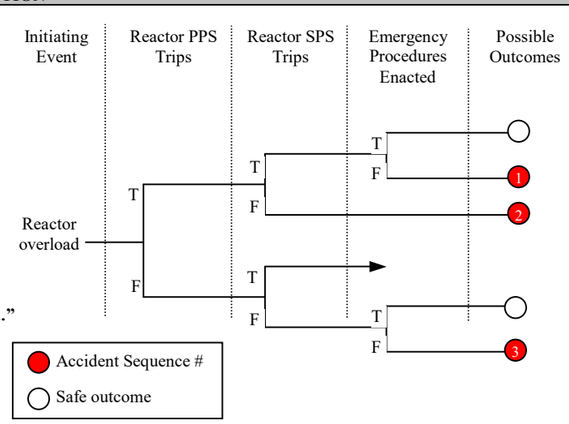
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Causal Analysis	Deductive analysis, which investigates the possible outcome of an undesired event. Uses techniques such as FTA, Software FTA, FMECA.	• Determines all credible combinations or sequences of causal factors that can lead to a hazard occurring. • Enables the calculation of the probability of a hazard occurring, which in turn can be used to determine the risk of an accident due to that hazard. •	• Hard to use, requires skilled analyst(s) • Difficulty of modelling increases very rapidly with system complexity.
Cause Consequence Analysis	Integration of deductive (e.g. fault tree) and inductive (e.g. event tree) analysis into a single method and notation. Mainly used in nuclear industries, no good examples found in other industries yet. See also Consequence Analysis.	• Very expressive notation with high information density • Can express interactions of multiple failures and protective mechanisms. • Works through consequences related failures. • Can be used for probability analysis, but becomes very complex. • Particularly suited to analysis of systems which include protective mechanisms	• Hard to use, requires skilled analyst(s) • Difficulty of modelling increases very rapidly with system complexity. • Not widely adapted yet, but will improve due to new software tools.
Change Analysis	Change Analysis examines the effects of modifications from a starting point or baseline.	▪	▪
Checklists	In the past, Hazards Identification relied on the experience of individual engineers and on previous accidents. Sometimes this knowledge would be embodied in Hazard Checklists. A checklist is, as its name implies, a list of questions, features or key points against which something is assessed ("checked") to determine its acceptability. Checklists can be constructed for many purposes and can be short or long, simple or complex. In fact, checklists are as varied as the systems being designed or evaluated or the tasks to be performed. Checklists incorporate past experiences in convenient lists of "do's" and "don'ts". The list is more of a prompt to the imagination of the user than a checklist which can guarantee identifying all possible Hazards. Some useful checklists include: • The **ATC Electronic Checklist**, developed by the Volpe Center and the FAA, provides a checklist of human factors issues that should be considered in the design and evaluation of air traffic control systems and equipment. The checklist points controllers and other operations specialists to questions that they may wish to consider in the evaluation of new systems or subsystems or a new component of an existing system (see http://www.hf.faa.gov/) • The **Ergonomics Audit Program (ERNAP)** is a computerized checklist to help managers design and/or evaluate procedures for aviation maintenance and inspection. ERNAP is simple to use and evaluates existing and proposed tasks and set-ups by applying ergonomic principles. ERNAP allows the auditor to maintain Audits for further reference. ERNAP was developed under the auspices of the FAA, and can be downloaded from the Human Factors in Aviation Maintenance and Inspection (HFAMI) website. See http://www.hfskyway.com/jobaids.htm) • **CRT display checklist**, whicht forms Appendix A to NUREG/CR-3557. It provides subjective comparisons of methods for displaying screen information but is also used as a design checklist [refer Kirwan and Aisworth, 1992; Blackman et al, 1983] • **Ravden & Johnson Checklist,** which is a comprehensive checklist of items that evaluate the usability of human-computer interfaces. It is easy to administer but its 156 questions make it somewhat lengthy. It generates much data on interface factors including visual clarity, consistency, compatibility, feedback, explicitness, functionality, control, error management, help facilities, and the usability of help facilities [Ravden and Johnson, 1988]. • **NUREG-0700**: US Nuclear Regulation Commission (NRC) has produced several human factors guidance documents. NUREG-0700 is a detailed checklist for control room design (or more precisely, design review) in the nuclear power industry. The checklist addresses individual instruments, so using this checklist is time-consuming process because of its detail. The guidelines, first issued in 1981, were recently revised to take into account the introduction of computer-based, human-computer interface technology (NRC, 1995). [NRC, 1981, 1995; Kirwan and Ainsworth, 1992].	• Useful for revealing otherwise overlooked hazards • Easy to use (if it does exist) evaluation against existing guidelines • Based on experience • Requires minimum manpower • Useful when more precise methods (e.g. FMEA, HAZOPS) are not possible or practical. • Particularly useful if combined with "What-if" analysis. • ***Hazard Checklists*** are available from various sources such as Def Stan 00-56 and BSEN 1050 and they range from the very general to industry specific.	• Satisfactory for known hazards only (i.e. if they have been met before). Cannot foresee new hazards (e.g. for new technology) • Need to be continually supplemented to remain valid. • Not predictive • Can be box ticking exercise. • Generally better at identifying Physical Hazards than Functional Hazards, unless the checklist is system-specific • Checklists are generally better at suggesting relevant Physical Hazards than Functional Hazards.
Chi-squared method	A method for detecting differences between a binomial and a multinomial population. Observations may fall into one or more categories and compare two or more samples	• Useful in statistical analysis for RAM data	
Cognitive Event Tree System (COGENT)	Human error reliability assessment.		
Cognitive Reliability Assessment Technique (CREATE)	Human error reliability assessment.		
Cognitive Work Analysis (CWA)	Traditional approaches to work analysis tend to emphasise centralised work organisations, whereas turbulent, dynamic environments tend to require more distributed work organisations. The focus of the CWA framework is on identifying the constraints that shape behaviour rather than trying to predict behaviour itself. Rasmussen's (1986) framework for Cognitive Work Analysis (CWA) provides separate descriptions of different classes of constraints: Work Domain (The functional structure of the work domain in which behaviour takes place); Control Tasks (The generic tasks that are to be accomplished); Strategies (The set of strategies that can be used to carry out those tasks); Social-Organisational (The organisation structure); Worker Competencies (The competencies required of operators to deal with these demands). [http://www.mie.utoronto.ca/labs/cel/research/frameworks/cwa.htm, 5/9/05]	• A complement to traditional task analysis in that it retains the benefits of these methods but also adds the capability for designing for the unanticipated by describing the constraints on behaviour rather than behaviour per se	•



TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Common Cause Analysis (CCA)	Generic term encompassing ZSA, PRA and CMA (see SAE ARP4761) Although most systems employ redundancy techniques (i.e. fail safe design), it will be found on examination that many of them have a "single cause" (e.g. EMI/EMC), or "common point" (e.g. common bus-bar or common controller), that could cause multiple failures. A Common Mode Failure is a failure which has the potential to fail more than one safety function and to possibly cause an initiating event or other event simultaneously. For instance: • Common Part Failure: For instance, three totally independent flying control systems may merge together in a common part – the pilots control column. A failure of this common part causes total system failure. • Common cause failure: For instance, a fire in a compartment might destroy all the channels of a system running through that compartment. Likewise, contaminated hydraulic fluid could cause all the channels of the hydraulic system to fail, or mechanical failures in an electrical loom. • Common mode failure: For instance, Identical software in a dual redundant system will fail when exposed to the same inputs; jamming of a mechanical system (either due to failure or due to FOD); overheating of avionic equipment; etc. • Cascade failures: For instance, a single failure may overload the remaining channels, thereby increasing the probability of their failure. Or, an initial minor failure (e.g. a deflated tyre) causes a cascade of events (e.g. Concord). The CCA (consisting of the ZHA, PRA and the CMA) provides the tools to verify required independence, or to identify specific dependencies. It identifies failures which by-pass or invalidate redundancy/independency assertions	• Identifies failure modes or external events which could lead to a hazardous failure condition. • Supports the selection of system architecture through determination that appropriate independence can be achieved. • Most other techniques concentrate on the functionality. CCA ensures that the *installed* design is free from common casues which can undermine design, qualitative and quantitative predictions. • Analyses system architectures that rely on redundancies. Establishes and validates physical and functional separation and isolation requirements between systems. • Crosses system boundaries, and should identify the fault containment strategies needed. ▪ May identify common development errors (e.g. software design errors, installation error, etc). ▪ May identify common environmental hazards (e.g. HIRF, moisture, temperature, etc) ▪ Validates independence. ▪ CCA fault sources include S/W errors, Requirement errors, Repair process errors, Environmental factors, H/W design errors, Production errors, installation errors, operational errors, cascading failures, etc.	• Used throughout design process, but more cost-effective if done earlier because of the influence on system architecture. However, confirmation is often only feasible when the implementation is complete. • Difficult to be rigorous. • Requires detail knowledge of the system • Difficult to identify hazards in isolation, best suited to brainstorming sessions with multiple input (preferably using checklists as prompts)
Common Mode Analysis (CMA)	Provides evidence that the failures assumed to be independent are truly independent in the actual implementation. Covers the effect of design, manufacturing and maintenance errors and the effects of common component errors (e.g. considers independence of duplicate systems due Design Errors (e.g. S/W), Lightning, HIRF, Cooling, Fire, contamination, etc) A common mode failure has the potential to fail more than one safety function and to possibly cause an initiating event or other abnormal event simultaneously. Rare in technical systems, but typical in human actions (e.g. maintenance).	▪ Verifies that the "AND"-ed events in the FTA/DD/MA are independent in the actual implementation. ▪ A good second line check on design. ▪ Covers the effects of design errors (e.g. S/W error, Requirements error), manufacturing errors (e.g. production process error), maintenance errors, operational errors (e.g. operator failure), the effects of common component failures (e.g. common S/W in redundant systems), cascading faults, common external source faults, etc.	▪ Relies on acceptance that seemingly unlikely events will occur. ▪ Difficult to be rigorous. ▪
Comparison-To-Criteria	The purpose of Comparison-To-Criteria is to provide a formal and structured format that identifies safety requirements. Comparison-To-Criteria is a listing of safety criteria that could be pertinent to any 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. [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000]	▪	▪
Confined Space Safety	The purpose of this analysis technique is to provide a systematic examination of confined space risks. Any confined areas where there may be a hazardous atmosphere, 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. [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000]	▪	▪
Consequence Analysis	Inductive analysis, which takes a given event (usually a failure) as a starting point, and works forward to determine the possible outcome (see also Cause Consequence Analysis) The Consequence Analysis will determine the relationship between hazards and the accidents to which they lead. The forward looking part of HAZOPS, SWIFT and Functional FME(C)A are all Consequence Analyses. Includes ETA, Cause Consequence Diagrams, etc.	• Determines the relationship between hazards and the accidents to which they lead. • Enables the calculation of risk for each accident. • Enables either: a. The calculation of risk of each accident – carrying probabilities up the accident model. b. The setting of a safety target – moving targets down the accident model to the system(s) presenting the hazard.	• Accident sequence needs to include ability of pilot/technician/maintainer to influence the outcome based on their expected levels of training and experience. This tends to lead to high levels of subjective judgment to compensate for factors such as high workload or stress. • In many situations it is difficult to be certain about the scale of the consequences. There may be little quantitative data available on rare events such as major explosions and releases of toxic gas clouds. • It explores all the consequences, not all of which may result in harm.
Contingency Analysis	Contingency Analysis is a method of minimizing 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 minimize the situation. It is an excellent formal training and reference tool. [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000]	▪	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Continuous Safety Sampling Methodology (CSSM)	This is a form of hazard analysis that uses observation (e.g. control charting) and work sampling techniques to • determine and maintain a pre-set level of the operator's physical safety within constraints of cost, time, and operational effectiveness. • observe the occurrence of conditions that may become hazardous in a given system. These conditions, known as dendritics, may become hazards and could result in an accident or occupational disease. Continuous Safety Sampling Methodology performs a random sampling for the occurrence of these dendritics. The collected data are then used to generate a control chart. Based on the pattern of the control chart, a system "under control" is not disturbed whereas a system "out of control" is investigated for potential conditions becoming hazardous. Appropriate steps are then taken to eliminate or control these conditions to maintain a desired safe system This tool is used to determine whether activities are within tolerable limits. If outside tolerable limits, corrective action is then derived. [Quintana and Nair, 1997]	• Proactive methodology for accident prevention	• It may focus more on industrial injuries
Control Rating Code	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 here are many hazard control options available. The technique can be applied toward any safe operating procedure, or design hazard control. [FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000]	▪	▪
Cost Benefit Analysis	A weighing scale approach to decision making. All the plusses (e.g. cash savings, lives saved) are put on one side of the balance and all the minuses (e.g. costs, disadvantages) are put on the other. Whichever weigh the heavier wins. Frequent made mistake is to use non-discounted amounts for calculating costs and benefits. A method like “Net Present Value (NPV)” and “Economic Value Added” is strongly recommended, because all these account for the time value of money. Another frequent problem is that typically the costs are tangible, hard and financial, whilst the benefits are hard and tangible , but also soft and intangible. Care should be taken here against claims that “if you cannot measure it, then it does not exist/it has no value”	•	Often not socially (and even legally) acceptable
Critical Incident Technique	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 minimize the potential error or unsafe condition. This technique can be universally applied in any operational environment. [Tarrents, 1980]	▪	▪
Critical Path Analysis	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.	▪	▪
Damage Modes and Effects Analysis	Evaluates the damage potential as a result of an accident caused by hazards and related failures. Risks can be minimised and their associated hazards eliminated by evaluating damage progression and severity. [Tarrents, 1980]	▪	▪
Deactivation Safety Analysis	This analysis identifies safety concerns associated with facilities that are decommissioned/closed. 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.	▪	▪
Decision analysis	Decision analysis is a broad term to describe tools for facilitating, understanding or structuring decision-making processes. The essence of decision analysis is to break down a complicated decision into its component parts or elementary qualities, and in particular to separate clearly the subjective and objective aspects of that decision. Decision analysis originates in the field of operations research but has links to economics, mathematics, psychology and human factors. A wide range of tools have been developed which utilize a variety of methods such as influence diagrams, decision trees, voting methods, multi-attribute utility methods and so on. See http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_decisionanalysis.html	•	
Deductive Analysis	Analysis which works back from a given event (failure) to identify its causes. It starts from known effects to seek unknown causes. A deductive argument is where the conclusion is implicit in the evidence used to support the argument.	• Useful during incident/accident analysis	
Defect/Failure Reporting Analysis and Corrective Action System (DRACAS/FRACAS)	Closed loop data reporting system to aid design; identify actions; and evaluate results.	• Useful to identify common mode failures and trends. •	• Historical data technique (relies on past experience) • Primarily a reliability tool • Depends on accurate data collection. • Depends upon ability to find similar data. • Does not address unknown hazards.

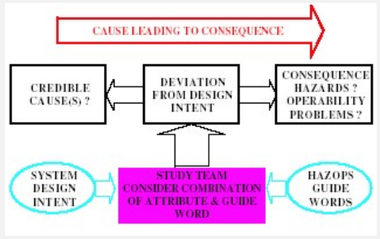
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Dependence Diagrams (DD)	Similar to the FTA, but replaces the logic gates by paths to show the relationship of the failures. A dependence diagram analysis is success-oriented, and is conducted from the perspective of which failures must not occur to preclude a defined Failure Condition.  Each block defines, for example, a failure of a part of a system and the conditions related to it and, where needed, the estimated frequency of occurrence. The blocks are arranged in series or parallel to represent" and" or "or "gates respectively. See SAE ARP4761	• Illustrates the failure combination of the system. • Less complicated than FTA (adopted by some European Aircraft constructors). • Very useful where numerical assessment of the probabilities is needed. • Like the FTA and MA, it identifies the failure events which could collectively or individually lead to the occurrence of the undesired top event. • Establishes crew and maintenance tasks and intervals needed to meet the safety objectives. • S/W errors can be qualitatively represented. • Rapidly identifies critical failure sequences (i.e. minimum cutsets)	• Assumes failure modes are independent • Assumes failure rates are small and constant over time. • Not an exhaustive analysis tool
Design Appraisal	A qualitative appraisal of the integrity and safety of the system design. Can be used to consider a range of issues, such as: - What Happens If ? - Possibility of Maintenance Induced Failures - Suitability/compatibility of Materials	• Simple and pragmatic • Quick, hence an effective tool at the early stages to identify potential problem areas.May be used effectively on all systems	• Highly subjective, often not systematic. • Not a rigorous method and very dependent on the analyst's experience.
Electromagnetic Compatibility Analysis	The analysis is conducted to minimize/prevent accidental or unauthorized operation of safety critical functions within a system. 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. [Tarrents, 1980]	▪	▪
Energy Analysis	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 Energy Analysis [Tarrents, 1980]	▪	▪
Energy Trace Checklist	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 provide a systematic way of collecting information on many similar exposures. [Tarrents, 1980]	▪	▪
Energy Trace Analysis	This hazard analysis approach addresses all sources of uncontrolled and controlled energy that have the potential to cause an accident. Examples include utility electrical power and aircraft fuel [FAA System Safety Handbook, Chapter 9] Sources of energy causing accidents can be associated with the product or process (e.g., flammability or electrical shock), the resource if different than the product/process (e.g., smoking near flammable fluids), and the items/conditions surrounding the system or resource of concern (e.g., vehicles or taxing aircraft). A large number of hazardous situations are related to uncontrolled energy associated with the product or the resource being protected (e.g., human error). Some hazards are passive in nature (e.g., sharp edges and corners are a hazard to a maintenance technician working in a confined area). The purpose of energy trace analysis is to ensure that all hazards and their immediate causes are identified. Once the hazards and their causes are identified, they can be used as top events in a fault tree or used to verify the completeness of a fault hazard analysis. Consequently, the energy trace analysis method complements but does not replace other analyses, such as fault trees, sneak circuit analyses, event trees, and FMEAs.	•	•
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 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.) [Tarrents, 1980]	▪	▪
Environment Analysis	Human error reliability assessment technique. The Environment Analysis can be performed concurrently along with the user and task analysis. Activities or basic tasks that are identified in the task analysis should be described with respect to the specific *environment* in which the activities are performed (Whiteside, Bennett, & Holtzblatt, 1988; Wixon et al., 1990).	•	• In most cases, the user characteristics need to be considered in a particular environment •
Environmental Risk Analysis	The analysis is conducted to assess the risk of environmental noncompliance 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. [Tarrents, 1980]	▪	▪
Event and Casual Factor Charting	Utilizes a block diagram to depict cause and effect. The technique is effective for solving complicated problems because it provides a means to organize the data, provides a summary of what is known and unknown about the event, and results in a detailed sequence of facts and activities. [Tarrents, 1980]	▪	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Event Tree Analysis (ETA)	ETA is an inductive technique which considers the consequence of an initiating event and the expected frequency of each occurrence. It is a graphical technique which starts from an initial occurrence (e.g. lightning strike or system condition, such as a rupture of a fuel pipe or loss of power supply) and builds upon this by sequencing the possible events. It is illustrated as a tree of possible TRUE/FALSE outcomes against each mitigating Mechanism. Event Tree Analysis starts with a hazard, but instead of working backwards as in the Fault Tree, it works forward to describe all the possible subsequent events and so identify the event sequences that could lead to a variety of possible consequences. Originally devised to assess the protective systems and safety of nuclear reactors, it operates with inductive (i.e. forward) logic by asking the question: **"*What happens if...*"**  	• IDs all possible outcomes (i.e. consequences) of an event (e.g. accident sequences). • Displays at a glance the sequences of events that relate to the proper functioning of a system. • Effectively explores how design copes with different accident scenarios. • Complements FMEA and HAZOP by tracing the chain of events resulting from a component failure. • Useful in accident sequence studies. • Useful to model mitigation (highlights insufficient mitigating mechanisms). • It can be quantified if the probabilities of success and failure at each branching point can be established. • Easy to understand, with time basically running from right to left. • Event Tree Analysis complements Fault Tree Analysis in much the same way as FMEA complements HAZOP.	▪ Does not consider equipment/system degradation. ▪ Reliant on experience of human actions. ▪ Very subjective. ▪ Can become very complex. ▪ Only deals with success/failure combinations cannot deal with delayed recovery. ▪ The event tree shows all possible outcomes from an initiating event, ranging from major accidents to safe results. ▪ Separate ETA diagrams are required for each initiating event being examine, so interaction of various events/outcomes not easily modeled. ▪
Explosives Safety	This method enables the safety professional to identify and evaluate explosive hazards associated with facilities or operations. Explosives Safety Analysis can be used to identify hazards and risks related to any explosive potential, i.e. fuel storage, compressed gases, transformers, batteries. [Tarrents, 1980]	▪	▪
Extended Master Plan Logic Diagram (MPLD)	Extended from MPLD to include the additional category of couplings which originate common cause failures [A logic diagram that shows how functional, equipment and component failure combine to cause a system malfunction. These are represented in fault-tree-like structure, except that basic event are not represented as leaf event but are listed in the lower left part of the tree and connected to gates though a sort of matrix [Mauri, 2000]	▪	▪
External Events Analysis	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 hypothesize 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. [Tarrents, 1980]	▪	▪
Facility System Safety Analysis	System safety analysis techniques are applied to facilities and its operations. Facilities are analysed to identify hazards and potential accidents associated with the facility and systems, components, equipment, or structures. [Tarrents, 1980]	▪	▪
Failure Logic Analysis for System Hierarchies (FLASH)	Developed to enable the assessment of a hierarchically described system from the functional level down to the low levels of its hardware and software implementation. Each module of the architecture (i.e. sub-system or basic component) is systematically examined for potential failure modes and how those failure modes relate/propagate to other modules in the system hierarchy. [Mauri, 2000]	▪ Contributes towards improving consistency, completeness and correctness in safety analysis by integrating well-established safety analysis techniques [Mauri, 2000]	▪ FLASH has recently resulted from a doctoral study at York University [Mauri, 2000], and is yet to be proven in industry. ▪ It is complex, and may need software automation to reduce workload and repetitive errors.
Failure Mode and Effects Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA)	A systematic, hardware (i.e. bottom-up) approach of identifying failure modes of a system or item, and determining the effects on a higher level. It answers the question "*if this part fails, what will be the next result?*" The FMEA is performed at a certain level (System, Subsystem, Module, Part/Item, etc) by postulating the ways the chosen level's specific implementation may fail. Can be developed to the level of the smallest replaceable item (i.e. piece part FMEA) or functional level (i.e. Functional FMEA, which could be the same as an FHA). Piece part FMEA is useful to determine the theoretical failure probability of the Part being considered, whilst a function FMEA uses predetermined probabilities as an input. Failure effects leading to the same system condition can be identified and grouped together in a FMES Does not have to be quantitative. Best suited to mechanical and electrical hardware systems. Although very extensive, the "*devil is in the details*". It is generated to support the Safety Assessment, so it is important to understand the expectations and requirements on the FMEA before any work on it commences (e.g. its sole purpose may be to support verification of the FTA through a comparison of FMEA failure modes with the basic events of the fault tree). Coordinate required scope of FMEA with the user requesting it. If the failure rates from a Functional FMEA allow the PSSA targets to be met, then a Piece Part FMEA may not be necessary. See MIL-STD-1629 and BS 5760 Part 5 and SAE ARP4761 For useful software tools, see www.byteworx.com	▪ Simple, flexible concept that identifies those failures (including dormant/latent failures) that could cause a loss of a specific function. ▪ Very systematic at lower levels (i.e. individual components). Identifies the cause of each failure mode. ▪ Useful for the preparation of diagnostic routines (e.g. flowcharts or fault finding tables) by conveniently listing all the failure modes. ▪ Good record for future reviews. ▪ Identifies the possible causes of each failure mode and so assists with BIT, failure indications and redundancy. ▪ Complements the FTA when an item has particularly significant potential consequences. ▪ FMECA provides a numerical probability level as well as a criticality classification for each failure. ▪ Provides RAM data to the LSA process. ▪ Provides source data for the FTA/DD/MA. ▪ Functional FMEA suitable for designs not finalised to component level.	▪ Lists only single failures (assumes rest of system is working perfectly), some of which may be of no safety concern ▪ Primary a reliability technique. Good at generating maintainability data. ▪ Can be very detailed (critical aspects may be lost in the detail). Level of analysis must be decided (piece-part/LRU/Subsystem/system). ▪ In FME**C**A severity can only be allocated if it is taken through to system level (e.g. adding a safety severity to a resistor failure is meaningless). ▪ Time consuming and expensive to generate (often iterative). ▪ Needs continuous management to keep it current. ▪ An empirical, rather than a relative measure. ▪ Often too much reliance is placed on the FMEA/FMECA, while ignoring threats which can arise from outside the system (e.g. common cause failures, human error, multiple failures, etc.). ▪ Cannot cope with human induced hazards/errors. ▪ Piece part FMEA is not practically feasible for modern microcircuit based LRU and systems.

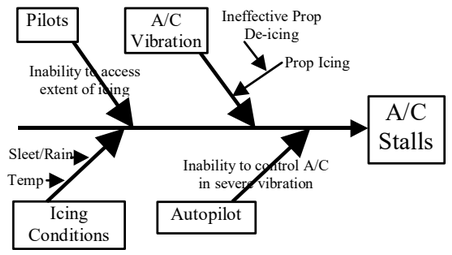
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Failure Mode and Effects Summary (FMES)	Summary of lower level FMEA failure modes with the same effect. The failure rate for each failure mode is the sum of the failure rates coming from the individual FMEAs See SAE ARP4761.	▪ Used as input into the FTA (and others). ▪ Simplifies the FTAs (reduces the number of OR-gates) by combining the effect of item failures (and failures of the installation that have the same effect) as one single event.	▪
Failure Propagation and Transformation Notation (FPTN)	Hierarchical graphical notation that represents system behaviour. It represents a system as a set of interconnected moduels; these might represent anything form a complete system to a few lines of program code. The connections between these modules are failure modes, which propagate between them [Mauri, 2000].	▪	▪
Fault Hazard Analysis	A system safety technique that is an offshoot from FMEA. Similar to FMEA above 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 analyzed to identify failures, malfunctions, anomalies, faults, that can result is hazards. [Tarrents, 1980]	▪	▪
Fault Isolation Methodology	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 Search, and Point of Maximum Signal Concentration. Determine faults in any large-scale ground based system that is computer controlled. [Tarrents, 1980]	▪	▪
Fault Tree Analysis (FTA)	A graphical model (developed in the 1960's) for illustrating: ▪ logical relationships between a particular failure condition and the failures or other causes leading to a particular undesired event. ▪ the pathways within a system that can lead to a foreseeable, undesirable loss event. The pathways interconnect contributory events and conditions, using standard logic symbols. It is a top-down (deductive) analysis proceeding through successively more detailed (i.e. lower) levels of the design until the risk of occurrence of the top event (the feared event) can be predicted It is the opposite process to the FMECA: The FTA goes down to a Primary Event (i.e. an event which does not need to be broken down any further). The primary events can be hardware failures, human errors, software faults or external factors like the weather. Developed in the 1960's and has since then been readily adopted by a range of engineering disciplines as one of the primary methods of predicting system reliability and availability parameters. FTA is essentially a systematic qualitative technique to which a quantitative analysis can usually be applied if suitable failure data exists. Even in situations where failure data does not exist, it may still be useful to perform an FTA due to the insight it yields concerning a system's potential failure behaviour. FTA provides valuable information through qualitative analysis but can also be quantified with event probabilities or rates to give an estimate of how often the top event will occur. Computerised FTA provides good graphic output, quick evaluation of changes, more sophisticated algorithm, BUT can lead to less understanding by analyst and a temptation to become overly complex.	▪ Gives a visual representation of combinations of failures. ▪ Establishes deeper understanding than just understanding of the correct functioning. ▪ Provides insight into the relationship between the various functional elements. Allows for the identification of common mode/cause failures. ▪ Useful to determine what single failure (i.e. component failure or human error) or combination of failures exist at the lower levels that might lead to a higher level (e.g. functional) failure. (i.e. identified hazard causes and cause combinations) ▪ Unlike the FMECA, the FTA analyses only the detail contributing to the top event and hence the costs are significantly reduced by concentrating effort where is has most effect. ▪ Good for fault diagnostics (e.g. during maintentnace and operatations) and sensitivity assessments. ▪ Well-defined semantics and clear structure. ▪ Complementary information available from qualitative and quantitative analysis ▪ Can be used to verify compliance with PSSA objectives. ▪ Can include operational, environmental and human models ▪ Can establish crew and maintenance tasks and intervals needed to meet the safety objectives. ▪ Useful during MEL consideration. ▪ Supports qualitative and quantitative analysis, although not easily in combination. S/W errors can be qualitatively represented. ▪ FTA intrinsically generates the documentation required to support an audit trail. ▪ ▪ Particularly useful to model complex systems. ▪ Assist with allocation probability budgets. ▪ Useful for sensitivity analysis (e.g. evaluating sensitivity of failure rates) ▪ Useful for systems with redundancy (two or more ways of achieving a function) and looking at the number of separate events required to cause the undesired top event. ▪ It can also identify potential problems with "dependent failures" which might affect several apparently separate redundant equipments (e.g. both the duty and standby power supplies). ▪ Allocates budgets to lower level events	▪ FTA is not a technique for Hazard Identification. ▪ Requires good understanding of the design, its components and how they fail, so design needs to be quite mature. ▪ Complex and tedious to prepare. Substantial experience needed to produce useful, well structured trees in a reasonable time. ▪ There is the potential for failure paths to be missed. ▪ Large trees difficult to understand/follow. ▪ Logically over precise. ▪ Can be drawn in many ways. ▪ May miss common cause failures at lower levels. ▪ Less valuable for revealing system design deficiencies unless they are directly related to, or within, a component. ▪ Poor at evaluating human errors ▪ Cannot consider accident sequences (where timing is important) and transient effects. ▪ Prone to error (vulnerable to mistakes at base levels). ▪ Difficulty with common cause or common effect failures. ▪ Where do you stop? (When sufficient detail to satisfy the top level hazard requirement has been identified). ▪ Difficult in complex designs (e.g. computer systems) ▪ Illusive quantitative base event data. ▪ Qualitative FTA only identifies the events that contribute to a scenario, it does not provide quantitative results. ▪ If the undesirable top-event is not defined very specifically, the fault tree produced would quickly become large, complex and unmanageable. ▪ Not sufficient for addressing the interaction of components, maintenance actions, repairability and redundancies.

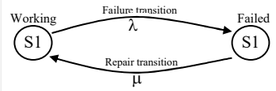
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Fire Hazards Analysis	Fire Hazards Analysis is applied to evaluate the risks associated with fire exposures. There are several firehazard analysis techniques, i.e. load analysis, hazard inventory, fire spread, scenario method. Any fire risk can be evaluated. [Tarrents, 1980]	▪	▪
Flow Analysis	The analysis evaluates confined or unconfined flow of fluids or energy, intentional or unintentional, from one component/sub-system/ system to another. The technique is applicable to all systems which transport or which control the flow of fluids or energy. [Tarrents, 1980]	▪	▪
Function and Task Analysis	Human error reliability assessment technique. Detailed analysis of the functions to be accomplished by the human/machine/environment system and the tasks performed by the human to achieve those functions. • Function Analysis: An analysis of basic functions performed by the "system" (which may be defined as human-machine, human-software, human-equipment-environment, etc.). The functional description lists the general categories of functions served by the system. Functions represent general transformations of information and system state that help people achieve their goals, but do not specify particular tasks. • Task Analysis: Task analysis is one of the most important tools to understand the user and can vary substantially in its level of detail and completeness. The preliminary task analysis traditionally specifies the jobs, duties, tasks, and actions that a person will be doing.	•	In general, the more complex the system, such as air traffic control, the more detailed the function and task analysis. It is not unusual for ergonomists to spend several months performing this analysis for a product or system. The analysis would result in an information base that includes user goals, functions and major tasks to achieve goals, information required, output, and so on.
Functional Analysis System Technique (FAST)	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-tasks link to tasks higher up the task hierarchy, and 'why' the super-ordinate tasks are dependent one the sub-tasks[Creasy, 1980; Kirwan and Ainsworth, 1992; Adams and Lenzer, 1997].	▪	▪
Functional Failure Analysis (FFA)	See Functional Hazard Analysis	▪	▪
Functional Failure Path Analysis	A method of determining the safety critical aspects of an implementation. A structured, top-down, iterative analysis which identifies functional paths and associated failures	• Identify functions and required design assurance levels for those functions. • Functional divisions may cut across system boundaries (multiple systems my contribute to the performance of more than one safety function) • Considers means of implementing functions. •	▪
Functional Hazard Analysis (FHA)	A systematic, comprehensive examination of a system's functions to identify and classify failure conditions (conditions which the system can cause or contribute to, not only if it malfunctions or fails to function, but also in its normal response to unusual or abnormal external factors) of those functions according to their severity. The FHA provides a top-level analysis of the functions performed by the system and the risks presented by these functions following failure or misuse. These hazards produced by the system are categorized according to their level of severity. Potential effects on the aircraft or on crew workload determine each hazard's associated severity.	▪ Provides a systematic approach to the derivation of critical failure conditions ▪ Determines the scope and depth of further safety assessments. ▪ Determines the integrity requirements of the function. ▪ Predictive and target setting: Determines the system's safety objectives without any architectural limitations. ▪ Systematic and a good record. ▪ Useful as primary mechanism in the identification of safety critical and safety involved failures of a system. ▪ Highlights functional failures that affect another aircraft system (through interfaces/ dependencies/boundaries). ▪ Improves understanding of how the design relates to safety. ▪ Assists in limiting the scope of the Safety Assessment by determining the safety assessment requirements of the system. ▪ Provides the FTA Top Events.	▪ Addresses only functional hazards. ▪ May be disproportionately time consuming. The "*law of diminished returns*" applies. Beware of taking the analysis too far by selecting the appropriate system level and assessthe worst case confitions only. ▪ The determination of the hazard severity level does not attempt to account for the system failures necessary for occurrence; it only seeks to determine the appropriate limits for probability of occurrence for a given hazard.
Gathered Fault Tree Combination	Formalised extension of FMES (developed in France, used on Airbus and Concorde)	▪	▪
Generic Error Modelling System (GEMS)	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 (frequently skill-based errors) and mistakes (usually knowledge based errors). 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 [Reason, 1990].	▪	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Goals, Operators, Methods and Systems (GOMS)	GOMS is a task modelling method to describe how operators interact with their systems. Goals and sub-goals 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. GOMS is mainly used in addressing human-computer interaction and considers only sequential tasks [Card, Moran and Newell, 1983].	• Assists in definition of human interface requirements at the earliest stages of design, so indirectly influences safety in this manner. • Can be used to model how skilled people will use a system [http://ei.cs.vt.edu/~cs5724/g2/] • Gives designers the ability to make quantitative predictions about skilled behavior without having to train people [http://ei.cs.vt.edu/~cs5724/g2/] • Parameter-free estimates makes the GOMS approach useful in design because it allows comparisons of different design alternatives [http://ei.cs.vt.edu/~cs5724/g2/]	Not designed to be a safety assessment tool. Card et al. (1980) provided the most detailed list of the weaknesses of GOMS. The weaknesses are as follows: • The model applied to skilled users, not to beginners or intermediates. • The model doesn't account for either learning of the system or its recall after a period of disuse. • Even skilled users occasionally make errors; however, the model doesn't account for errors. • Within skilled behavior, the model is explicit about elementary perceptual and motor components. The cognitive processes in skilled behavior are treated in a less distinguished fashion. • Mental workload is not addressed in the model. • The model doesn't address functionality. That is the model doesn't address which tasks should be performed by the system. The model addresses only the usability of a task on a system. • Users experience fatigue while using a system. The model does not address the amount and kind of of fatigue. • Individual differences among users is not accounted for in the model. • Guidance in predicting whether users will judge the system to be either useful or satisfying, or whether the system will be globally acceptable is not included in the model. • How computer-supported work fits or misfits office or organizational life is not addressed in the model.
GSN (Goal Structured Notation)	GSN is a graphical representation of an argument showing how it is to be accomplished A convincing argument Safety Assessment/Safety Case requires three elements: • Safety Objective • Supporting Evidence • A clearly discernable "thread" or argument that flows through the document. GSN shows show how goals ▭ are broken into sub-goals, and eventually supported by evidence (solutions) ◯ whilst making clear the strategies ▱ adopted, the rationale for the approach (assumptions, justifications) ⬭ and the context ▭ in which goals are stated. The Goal Structuring Notation (GSN) – a graphical argumentation notation – explicitly represents the individual elements of any safety argument (requirements, claims, evidence and context) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument). When the elements of the GSN are linked together in a network they are described as a 'goal structure'. The principal purpose of any goal structure is to show how goals (claims about the system) are successively broken down into sub-goals until a point is reached where claims can be supported by direct reference to available evidence (solutions). As part of this decomposition, using the GSN it is also possible to make clear the argument strategies adopted (e.g. adopting a quantitative or qualitative approach), the rationale for the approach and the context in which goals are stated (e.g. the system scope or the assumed operational role). Developed for use in Safety Cases by Tim Kelly, John McDermid (Department of Computer Science, University of York)	▪ Improved comprehension of existing arguments. ▪ Useful way to define Safety Assessment/Case strategy. ▪ Easy to read, even to a novice. ▪ Present logical argument to get from a goal to its logical solution (forces a logical argument) ▪ Identifies holes in an argument. ▪ Positively identifies assumptions. ▪ Removes ambiguity (i.e. you have to define measurable goals) ▪ Assist in managing programme risk (i.e. solution planning and prioritising) ▪ Ease to audit ▪ Prevent duplication of solutions ▪ Prevents unnecessary work (e.g. if not required by a goal) ▪ Defines scope of work, so assist in planning and budgeting ▪ Arguments can be re-used in another project	▪ Takes a lot of effort to develop the arguments. ▪ Can easily go into to much complicated detail (e.g. some times it is more efficient to make the solution a separate Compliance Matrix rather than trying to argue compliance via GSN). ▪ Arguments are always subjective, so every person will compile a GSN differently. Human actions always involve some interpretation of the person's goals and motives. The individuals involved may be unaware of their actual goals and motivation or may be subject to various types of pressures to reinterpret their actions. ▪ Can spend a lot of time agreeing an argument, so it may be more efficient to restrain GSN to a top level argument only , i.e. do not repeat each finding which exist in tabular format (e.g. FHA) ▪ Needs experience and skill ▪ Not as user friendly in hardcopy format, because complex GSN needs hyperlinks ▪
Hardware/Software Safety Analysis	The analysis evaluates the interface between hardware and software to identify hazards within the interface [Tarrents, 1980].	▪	▪
Hazard Analysis	A generic term describing a whole collection of techniques whose combined strengths have a good chance of revealing and evaluating/analysing hazards. A multi-use technique to identify hazards within any system, subsystem, operation, task or procedure. [Tarrents, 1980] Also referred to as a System Safety Analysis [JAR 25.1309]. Includes both top-down techniques oriented to tracing back from potential real-world hazards to the sources of failures which could lead to accidents; and bottom-up techniques which follow through hypothetical component failures to determine their hazardous consequences. (Strictly these are 'middle-out' because one also looks at how the component could come to fail).	Top-down techniques provide, in effect, a way of supporting lateral thinking about that most error-prone stage of development, the requirement specification.	Bottom-up techniques, like Event Tree Analysis, can be very resource intensive because of the combinatorially explosive growth in consequences. A number of techniques are well established for electrical and electronic systems but there has been much debate as to how relevant these techniques are when applied to software.

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
HAZard and OPerability Studies (HAZOPs) ***IEC 61882*** ***Def Stan 00-58***	A team based structured brainstorming technique for identification of hazards before they arise. HAZOP starts with a deviation from normal system operation and examines how that deviation might occur and the consequences should such a deviation occur. For each hardware item, system function or operating stage a systematic and structured evaluation of each attribute of the systems takes place based on predetermined "guidewords" in order to suggest possible deviations and Hazards. • The attributes are chosen according to the technology of the system. For example: - a chemical facility might use attributes such as "Temperature", "Pressure" and "Flow Rate" - a communications system might be examined with attributes such as "Bandwidth", "Data Rate" and "Protocol". The attribute of "temperature" taken with the guide word "More of" would suggest that the temperature at that point in the system is higher than intended and the team would discuss possible causes and consequences of this deviation. • Each guideword is applied to each attribute, so a thorough search for all possible deviations is carried out in a structured manner. An example of a guideword is 'more' (which in some cases may be interpreted as 'greater' or 'higher'). On applying this to the attribute 'data value', the team enquire into whether there is a conceivable cause of the value of the data being higher than the design intent likely causes are then briefly investigated. A connection between two entities (usually on a graphical representation), denoting the logical or physical interconnection of one component of the system to another, is selected and the flow between the components which the line represents identified. For example: - In a chemical plant, the flow may be of a fluid, with attributes such as pressure, temperature, and rate of flow - In software, the flow may be of data, with attributes such as value, sequence, and bit rate. The purpose is to identify what variations from the intended design values (the 'design intent') could occur in the relevant attributes, and then to determine their possible causes and consequences. From their possible consequences, it is seen whether the deviations could cause hazards. The technique was developed by ICI in the 1960's and is well established in the petrochemical sector. **Guideword** / **Standard Interpretation for Chemical Industry** / **Example Interpretation for PES** no / no part of intention is achieved / no data or control signal passed more / a quantitative increase / data is passed at a higher rate than intended less / a quantitative decrease / not used here because this is already covered by 'part of as well as / all design intent achieved but with additional results / not used here because this is already covered by 'more' part of / only some of the intention is achieved / the data or control signals are incomplete reverse / covers reverse flow in pipes and reverse chemical reactions / normally not relevant other than / a result other than the original intention is achieved / the data or control signals are complete but incorrect early / not used / the signal arrives too early with reference to clock time late / not used / the signal arrives too late with reference to clock time before / not used / the signal arrives earlier than intended within a sequence after / not used / the signal arrives later than intended within a sequence Table 3.1. HAZOP Guidewords 	• Wide-ranging, comprehensive and methodical. • Most useful if applied to continuous process systems (e.g. fluid and thermal systems) • allows the members to brainstorm opinions and viewpoints using the experience from within their own fields of expertise • Can be applied to each item/function /operation/ process/procedure, etc), but more effective if aimed at the very high level operating system model • "Structured brainstorming" considers individual items and procedures, using a set of guide words as prompts. • Good at identifying operational failures. • Generates operating procedures. • Flexible to the system being analysed. • Useful for electronic systems (sending transit data). • Has both inductive and deductive phases. • The team approach brings a variety of expertise and viewpoints onto a common problem. • The discipline of focusing on hazard identification (rather than just looking for errors) leads to productive sessions and, gratifyingly, there is rarely a defensive approach by the system designers and users. The fact that a team is involved means that there is much less impact caused by a mistake by one team member, in contrast to other techniques that are carried out by individuals [Falla, Ch3]. • The presence on the team of key personnel associated with the system under analysis means that problem areas are brought immediately to their attention. Because the intent of the HAZOP is to identify hazards, not find errors, it is complementary to other activities of analysis and testing. [Falla, Ch3]	• 6-8 people required, including the services of an experienced HAZOP team leader and minute taker. • Very lengthy to conduct. • Multi-disciplined team approach is expensive – must be shown to be cost-effective. • Guidewords can be hard to relate to. • Can produce lot of output. • More operability problems than hazards are usually found. • Requires specially trained team lead. • Requires thorough preparation before the meeting. • Variability is inherent in this approach. • More effective at higher system levels (e.g. FMECA is more effective at lower levels) •
Hazard Identification Study (HAZID)	A structured brainstorming technique developed for the marine industry. Considers systems or equipments. Used by the International Maritime Organisation [IMO Paper MSC 69/INF 14 dd 98/2/12] for its Safety Assessments.	• Similar to SWIFT & HAZOP, but more systematic.	
Hazard Log (HL)	A management tool used to track the identification, mitigation and acceptance of risk and also the control of residual risks associated with the operation. Note that hazards are properties of an entire system and may be defined at any system level (see Ch 6 para 2). However, it is essential to select the right level soas to ensure consistence in the Hazard Log: - A common mistake is to select it too low, which results in too many hazards, no system properties, expensive (impossible) to track and over-engineering. - If you select it too high, then it is hard to ensure the identification and management of all hazards.	• A powerful management aid, when implemented on a user-friendly database, to focus on activities requiring action. • Useful for logging failures which are not attributable to equipment functionality (e.g. wind shear) • Hazards are properties (states) of an entire system and may be defined at any level. However, it is essential to select the right level. A common fault is to select it to low, which results in too many hazards, no system properties, expensive (impossible) to track and over-engineering. If you select it to high, then it is hard to ensure complete management.	▪ Must be coupled to a logical decision process. ▪ Needs to be rigorously followed up to be affective. ▪ Duplicates information contained elsewhere (e.g. in FMEA and HAZOP). ▪ Not a technique, only a management tool. ▪ MoD intent is it as a management tool for operational safety and continued airworthiness. In this instance it can only be effective if all modifications on the platform uses the same (predefined) Safety Criteria. ▪
Hazardous Materials (HAZMAT) List	Not an assessment technique, but a list of hazardous materials contained in a product.	• Provides warning information\ to those responsible for the handling, maintenance and disposal of materials.	Seldom provides guidance as to the events/actions needed to cause risk of hazardous exposure.
Health Hazard Assessment	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. [Tarrents, 1980]	▪	▪
Health Hazard Analysis (HHA)	Identifies health hazards and recommend measures (e.g. such as ventilation and barriers) to reduce exposure to health hazards. See Mil Std 882C Task 207	Should consider presence of toxic/ inflammable/ explosive materials, systemic poisons, asphyxiates or respiratory irritants, noise, vibration, shock (physical/electrical), heat/cold stress, radiation (ionised and non-ioninised), etc.	

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Historical Data & Past Experience	Use information from past experience and accident/incident reports of similar equipment as part of the Hazard Identification.	▪ Cheap to obtain (where held in a consistent and usable format ▪ Scenarios are realistic ▪ Contains the lessons learned. ▪ Feeds into all HA techniques (e.g. FHA, FMEA). ▪ Useful for mature technologies (e.g. mechanical, hydraulic, etc.) ▪ Validation can be made via good engineering judgement.	▪ Equipment analysed may be obsolete. ▪ Does not address every potential hazard. ▪ Can be difficult to obtain the "real" causes from the data. ▪ Not always readily available, especially for uncommon hazards. ▪ Possibly different installation, operation, environmental exposure, etc. ▪ Validations require good substantiation
Human Error Probability (HEP)	*TBD*	•	
Human Error Analysis (HEA)	A method to evaluate the human interface and error potential 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. [Tarrents, 1980]	▪ Appropriate to evaluate any human/machine interface • Good at analysing procedures or processes. ▪ Good at identifying results of human error.	▪ Requires detailed procedural input
Human Error Assessment and Reduction Technique (HEART)	HEART is an error quantification process that is quick to use. The process defines a set of generic error probabilities for the types of tasks being examined and identifies the error producing conditions associated with them. For each of the error producing conditions the human error probability is multiplied by the error producing condition multiplier. The tool also provides some guidance on approaches towards error reduction [Kirwan, 1994, 1997; Williams, 1986] A human performance model-based technique utilising some standard probabilities. Data-based method to assess and reduce human error and improve operational performance.	• Can assess significant sequences within a scenario. ▪ Does show areas of vulnerability	• Time consuming. ▪ Accuracy of quantification questionable
Human Factors Analysis	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. 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. [Tarrents, 1980]	▪	▪
Human Hazard Analysis (HHA)	Examines the ease of use, the effects of error during use, task distribution, and the adequacy of feedback to the user in terms of his ability to recognise quickly if the desired result of his actions have not been achieved [Flight International, 11-17 Aug 1999, p3]	Human error remains a causal factor in the majority of serious aircraft accidents. Human error causes accidents of fail-safe, fully functional designs.	• Modelling of human performance and the quantification of human error probability are complex and time consuming procedures, which require input form specialist industrial psychologists. • Does not identify action required to eliminate the danger.
Human Reliability Analysis	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 in necessary for the success of the human-machine systems. [Tarrents, 1980] For more information, see Gu*ide to Practical Human Reliability Assessment*, Barry Kirwan, ISBN: 0748401113	▪	▪
Incident Reviews	These might be for the system itself or for similar systems used elsewhere	• One of the best ways of identifying possible Hazards is to look at previous accidents and incidents. • valuable for the purpose of identifying that a particular Hazard is possible.	• Often data reporting systems are sketchy and this makes them imperfect for estimating rates of occurrence.
Inductive Analysis	Analysis which works forward from a given event (failure) to determine the possibility outcomes (e.g. see Consequence Analysis). It starts from known cuases to forecast unknown effects. Inductive argument is where the argument is firmly based on the evidence presented, but extrapolates beyond the available evidence.	•	•
Installation Appraisal	A qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.	•	• An effective appraisal requires experienced judgement
Integrated Performance Modelling Environment (IPME)	IPME is a Unix/Silicon Graphics based software tool providing a suite of tools to aid human factors practitioner in understanding human-system performance. IPME incorporates mission analysis, function analysis, function allocation, task analysis, and workload/performance analysis and prediction. It is a tool that does require training in the use of the tool and can be time consuming to use in complex models [Dahn et al, 1997] See http://www.eurocontrol.int/eatmp/hifa/hifa/HIFAdata_tools_sysdesig_analysis.html	•	•
Interface Analysis	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. [Tarrents, 1980]	▪	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Ishikawa Diagrams	Also called Cause-and-Effect or Fishbone diagram. Problem of interest (e.g. haz or accident) is entered at end of main "bone". All possible causes are then "fleshed out". 	• Identify all possible contributory causes to an accident. • Good at evaluating events if causes + event is known.	• Practical maximum depth is usually about 4 or 5 levels. • Not good at drawing out causes vs events • Nor necessarily time ordered (but can be if first event is on far left and last event on right)
Job Safety Analysis	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. Job Safety Analysis can be applied to evaluate any job, task, human function, or operation. Each job is broken down into tasks, or steps, and hazards associated with each task or step are identifies. Controls are then defined to decrease the risk associated with the particular hazards. [Tarrents, 1980]	▪	▪
Justification of Human Error Data Information (JHEDI)	JHEDI is derived from the Human Reliability Management System (HMRS) 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. JEDHI is a moderate, flexible and auditable tool for use in human reliability analysis. Some expert knowledge of the system under scrutiny is required [Kirwan, 1994]		
Key Issues Tool (KIT)	KIT is a software tool designed to support the EHFA (Early Human Factors Analysis). It makes the EHFA process easier by providing structure and supporting the difficult aspects of tracking and linking many items. The output from KIT acts as an input to a project's overall risk register, allowing the project manager to see the human factors integration (HFI) risks in a manner which is comparable to other areas of project risk. The tool provides a full record of the analysis conducted on any issue over the life of a project [McLeod and Walters, 1999]		
Laser Safety Analysis	This analysis enables the evaluation of the use of Lasers from a safety view. The analysis is appropriate for any laser operation, i.e. construction, experimentation, and testing. [Tarrents, 1980]	▪	▪
Layer of Protection Analysis (LOPA)	Used for SIL determination. Is a relatively new method, developed by the American Institute of Chemical Engineers (CCPS) group in response to the requirements of ISA S84.01 and was formally published in 2001. It effectively combines a number of different techniques into a composite method that is well tailored to assessing process risks and development of hazardous scenarios. As indicated by its name, it involves assessing layers of protection other than just the instrument protective functions. For instance, a contribution toward risk reduction by Independent Protective Layers (IPLs) such as 'alarms and operators' or 'basic process control' is explicitly defined as a risk reduction factor. The combination of the risk reduction factors for all IPLs provides the total risk reduction possible. It is fundamentally a simplified quantitative method that considers the risk reduction contributed from each IPL typically by order of magnitude risk reduction (i.e., say 0.1 for a DCS, or 0.01 for a relief valve, etc). [Kirkwoodm D, *Current issues with SIL assessment methods*, Functional Safety Professional Network, Technical Advisory Panel, david.kirkwood@rtel.com]	• A defined and obvious procedural approach that guides the user to consider a range of factors that contribute to risk reduction. • It is more intuitive than quantitative analysis (for most people involved in the exercise). • It is aligned with assessing the development of hazardous scenarios and consequently provides an additional dimension to the assessment process. • It is also aligned with the assessment process required for mitigation systems. In general, it is quicker than quantitative analysis techniques. • Provides the capability of accounting for risk reduction factors at a finer level than risk graph assessments. • Consider the issue of an alarm to an operator. • Risk graphs provide the user with a digital choice of Pa or Pb with a resultant step of one SIL rating in the result. LOPA however provides a more graduated approach, allowing the user to select an intermediate value with an incremental effect on the final result.	• The disadvantages of the LOPA method is the additional time and effort required to conduct the exercise if environmental impact and asset protection are also considered. • The reliability and safety data on which the exercise relies is often defined subjectively (e.g. consider the contributing factor for a basic control system) There may be a strong temptation for users to simply enter 0.1 for the risk reduction provided by the system without considering the actual performance of the system further and taking into account factors that may change this result. If this is repeated for several IPLs then misleading results could occur. The reliability of elements such as valves and transmitters ultimately depends on their service conditions; it is well understood in industry that reliability is very dependent on environmental factors and the degree of wear and tear of elements. • There is also a potential danger with LOPA that we assume a false degree of accuracy in the results because numerical values are assigned to the elements of the calculation. • LOPA is also slower than typical risk graph techniques and therefore assessing a large number of safety functions could prove prohibitive.
Maintenance Error Decision Aid (MEDA)	Boeing has invested decades of research in maintenance error. It has developed a widely used maintenance error decision aid (MEDA) which is an attempt to systematise evaluation of events, problems and potential problems by using a repeatable, structured evaluation program. The company has been encouraging its customers to employ the technique [Allen and Rankin, 1996] See	•	•
Management Oversight and Risk Tree (MORT)	MORT technique is used to systematically analyze an accident in order to examine and determine detailed information about the process and accident contributors. This is an accident investigation technique that can be applied to analyze any accident. [Tarrents, 1980]	▪	▪

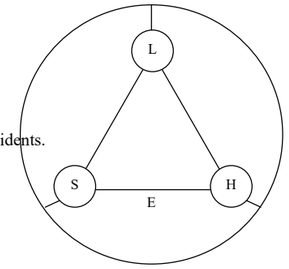
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Man-Machine Integration Design and Analysis Systems (MIDAS)	MIDAS is a Silicon Graphics software tool designed to aid the application of human factors principles and performance models to the design of complex systems. It is intended for use at the earliest stages of the design process and consequently is likely to reduce some of the costs of simulation and prototyping. MIDAS describes a system's operating environment and procedures, and incorporates human performance models into the design process [Dean, 1997]	•	•
Markov Analysis (MA)	A method named after a Russian mathematician, best known for his work on stochastic processes, where a collection of random variables represents the evolution of some system of random values over time. Markov analysis, or State-space analysis, is commonly used in the analysis of repairable complex systems that can exist in multiple states, including degraded states1, and where the use of a reliability block analysis would be inadequate to properly analyse the system. The nature of the Markov analysis techniques lends itself to the use of software. There are several to choose from on the market. The Markov analysis process is a quantitative technique and can be discrete (using probabilities of change between the states) or continuous (using rates of change across the states). To quote ISO 31010:"The Markov analysis technique is centred around the concept of "states", e.g. "available" and "failed", and the transition between these two states over time based on a constant probability of change. A stochastic transitional probability matrix is used to describe the transition between each of the states to allow the calculation of the various outputs."2 The inputs essential to a Markov analysis are as follows: • list of various states that the system, sub-system or component can be in (e.g. fully operational, partially operation (i.e. a degraded state), failed state, etc); • a clear understanding of the possible transitions that are necessary to be modelled. For example, failure of a car tyre needs to consider the state of the spare wheel and hence the frequency of inspection; • rate of change from one state to another, typically represented by either a probability of change between states for discrete events, or failure rate (λ) and/or repair rate (ì) for continuous events.3 The output from a Markov analysis is the various probabilities of being in the various states, and therefore an estimate of the failure probabilities and/or availability, one of the essential components of a system. Similar to the DD and FTA, but additionally calculates the probability of the system being in various states as a function of time. Here airworthiness is not a simple mathematical calculation, but depends on relative states of part of the system. Provides a means for analysing reliability/availability of systems whose components exhibit strong dependencies. The Encyclopaedia Britannica defines the Markov process as " *A sequence of possible dependent random variables (x_1, x_2, x_3,…) - identified by increasing values of a parameter, commonly time –with the property that any prediction of the value x_n, knowing the value x_1, x_2….x_{n-1}, may be based on x_{n-1} alone. That is, the future value of the variable depends upon the present value and no the sequence of past values".* See SAE ARP4761 Step 1: Begin State 1 with full functionality. Step 2: Study consequences of each failure. Group LRU failures. Step 3: Assign failure states for unique consequences of phase 2. Step 4: Connect arrows between States and add failure rate(s) of each. Step 5: Repeat Step 2 to 4 for each state. Step 6: Continue until equipment is totally unserviceable. Allows transition between 2 states to occur with specific distributions:  	• Provides great flexibility in modeling the timing of events. • Considers transient effects (e.g. shift in Cof G due to fuel displacement) • Useful when dealing with deferred maintenance scenarios. • Useful in multi-channel system where certain failures may be tolerated but not in conjunction with some failure conditions. • Allows modelling of common cause failures. • Allows modelling of failure characteristics of mixed H/W & S/W systems. • Useful for systems where a number of interrelated states may be valid (i.e. when airworthiness depends upon the relative states of parts of the system) • Establishes crew and maintenance tasks and intervals needed to meet the safety objectives. • S/W errors can be qualitatively represented. • Unlike other methods, this does not assume component independence. • Apart from this obvious drawback (complexity), a true Markovian process would only consider constant transition rates, which may not be the case in a real-world systems. Events are statistically independent since future states are treated as independent of all past states, except for the state immediately prior. In this way the Markov model does not need to know about the history of how the state probabilities have evolved in time in order to calculate future state probabilities. However, computer programs are being marketed that allow time-varying transition rates to be defined	• Most expensive reliability and system model. • Assumes constant failure rate and constant repair rate. For other distributions (e.g. Weibull failure rate processes or fixed repair times) Monte Carlo simulations methods are more appropriate. • Markov diagrams for large systems are often too large and complicated to be of value in most business contexts and inherently difficult to construct. • Markov models are more suited to analysing smaller systems with strong dependencies requiring accurate evaluation. Other techniques, such as Fault Tree analysis, may be used to evaluate large systems using simpler probabilistic calculation techniques. • Markov analysis requires knowledge of matrix operations and the results are – unsurprisingly! – hard to communicate with non-technical personnel.
Master Plan Logic Diagram (MPLD)	An Outgrowth of the Master Logic Diagram to represent all the physical interrelationships among various plant systems and subsystems in a simple logic diagram. It is used for probabilistic assessments to model and integrate the relationship between all plant functions and equipment [Mauri, 2000]	▪ Represents the interrelationships amongst various components and can model relationships between functions and systems [Mauri, 2000] ▪ Generates and quantifies accident sequences [Mauri, 2000]	▪ Does not allow the mapping of couplings which originate common cause failures [Mauri, 2000]
Materials Compatibility Analysis	Provides as assessment of materials utilized within a particular design. Any potential degradation that can occur due to material incompatibility is evaluated. Materials Compatibility Analysis in universally appropriate throughout most systems. [Tarrents, 1980]	▪	▪
Maximum Credible Accident/Worst Case	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. [Tarrents, 1980]	▪	▪
Micro Saint	Micro-Saint is a discrete-event task network-modelling tool that can be described by flow diagrams can be analysed to test, for example, alternative solutions or options, assess workload, function allocation, and temporal analysis (albeit based on time estimates). The analysis process requires input from subject matter experts on the task under investigation, training and familiarity with using the tool, and it can be difficult and time consuming to use [Dean, 1997]	▪	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
MIL-HDBK-217	"Reliability Prediction of Electronic Equipment" - Even though this handbook is no longer being kept up to date by the US military, it remains the most widely used approach by both commercial and military analysts. MIL-HDBK-217 has been the mainstay of reliability predictions for about 40 years but it has not been updated since 1995, and there are no plans by the military to update it in the future. For more than ten years Quanterion's Seymour Morris was DoD program manager for MIL-HDBK-217. The handbook includes a series of empirical failure rate models developed using historical piece part failure data for a wide array of component types. There are models for virtually all electrical/electronic parts and a number of electromechanical parts as well. All models predict reliability in terms of failures per million operating hours and assume an exponential distribution (constant failure rate), which allows the addition of failure rates to determine higher assembly reliability. The handbook contains two prediction approaches: the parts stress technique and the parts count technique and covers 14 separate operational environments, such as ground fixed, airborne inhabited, etc. • As the names imply, the parts stress technique requires knowledge of the stress levels on each part to determine its failure rate, while • the parts count technique assumes average stress levels as a means of providing an early design estimate of the failure rate. Typical factors used in determining a part's failure rate include a temperature factor (π_T), power factor (π_p), power stress factor (π_S), quality factor (π_Q) and environmental factor (π_p) in addition to the base failure rate λ_b. For example, the model for a resistor is as follows: $\lambda_{Resistor} = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E$	▪ Even though MIL-HDBK-217 is becoming more obsolete every day, it remains the most widely used technique for electronics.	▪
Models		▪ Provide a means for understanding phenomena and recording that understanding in a way that can be communicated to others.	▪ Note that all models are abstractions—they simplify the thing being modeled by abstracting away what are assumed to be irrelevant details and focusing on the features of the phenomenon that are assumed to be the most relevant. That selection process in most cases is arbitrary and dependent entirely on the choice of the modeler, but it is critical in determining the usefulness and accuracy of the model in predicting future events. [Nancy G. Leveson , System Safety Engineering: Back To The Future, Aeronautics and Astronautics, Massachusetts Institute of Technology, 2002]
Modelling/Simulation	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. [Tarrents, 1980]	▪ Modeling is appropriate for any system or system safety analysis.	▪
Monte Carlo Analysis	Systems are sometimes too complex for the effects of uncertainty on them to be modelled using analytical techniques. However, they can be evaluated by considering the inputs as random variables and running a number N of calculations (so-called simulations) by sampling the input in order to obtain N possible outcomes of the wanted result. Monte-Carlo analysis can be developed using spreadsheets, but software tools are readily available to assist with more complex requirements, many of which are now relatively inexpensive. Monte-Carlo analysis can be developed using spreadsheets, but software tools are readily available to assist with more complex requirements, many of which are now relatively inexpensive. Monte Carlo simulations require you to build a quantitative model of your business activity, plan or process. This is often done by using Microsoft Excel with a simulation tool plug-in – a relatively inexpensive set of tools. To deal with uncertainties using Monte Carlo analysis in your model, you'll replace certain fixed numbers — for example in spreadsheet cells — with functions that draw random samples from probability distributions. And to analyze the results of a simulation run, you'll use statistics such as the mean, standard deviation, and percentiles, as well as charts and graphs.4 For risk assessment using the Monte Carlo simulation, triangular distributions or beta distributions are commonly used.	▪	▪
Monte-Carlo Analysis (as used by FAA for Fuel Tank Safety Assessments)	Analytical method to determine flammability exposure time of a fuel tank. The percentage fleet flammability exposure result can be used to determine if the fuel tanks exist in a flammable state for a long period of time, thereby requiring more rigorous analysis in the SSA. Spreadsheet that simulates uncertain parameters by randomly selecting values from distribution tables. The calculation is performed repetitively and averaged to approximate real conditions.	▪ Analytical, repeatable results to replace traditional argument.	▪ Very dependant on input parameters and can produce results without the user understanding the process, increasing the likelihood of false results. ▪ Restricted input data limits applicability, requiring several scenarios to be considered. ▪ Dependant on fuel flash point and LEL values which are dependant on tank characteristics (which are not modelled).
MORT Checklist	Johnsontried to put management factors into fault trees (a technique called MORT or Management Oversight Risk Tree), but ended up simply providing a general checklist for auditing management practices. While such a checklist can be very useful, it presupposes that every error can be predefined and put into a checklist form. The checklist is comprised of a set of questions that should be asked during an accident investigation. Examples of the questions from a DOE MORT User's Manual are: - Was there sufficient training to update and improve needed supervisory skills? - Did the supervisors have their own technical staff or access to such individuals? - Was the technical support of the right discipline(s) sufficient for the needs of supervisory programs and review functions? - Were there established methods for measuring performance that permitted the effectiveness of supervisory programs to be evaluated? Was a maintenance plan provided before startup? - Was all relevant information provided to planners and managers? Was it used? - Was concern for safety displayed by vigorous, visible personal action by top executives? . [William G. Johnson. MORT Safety Assurance System, New York: Marcel Dekker, 1980.]	▪ Johnson originally provided hundreds of such questions, and additions have been made to his checklist since Johnson created it in the 1970s so it is now even larger.	▪ The use of the MORT checklist is feasible because the items are so general, but that same generality also limits its usefulness

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Network Logic Analysis	A method to examine a system in terms of mathematical representation in order to gain insight into a system that might not ordinarily be achieved. The technique is universally appropriate to complex systems. [Tarrents, 1980]	▪	▪
NPRD-95	The Nonelectronic Parts Reliability Data (NPRD-95) databook is a widely used data book published by the Reliability Analysis Center that provides a compendium of historical field failure rate data on a wide array of mechanical assemblies The document provides detailed failure rate data on over 25,000 parts for numerous part categories grouped by environment and quality level. Because the data does not include time-to-failure, the document is forced to report average failure rates to account for both defects and wearout. Cumulatively, the database represents approximately 2.5 trillion part hours and 387,000 failures accumulated from the early 1970's through 1994. The environments addressed include the same ones covered by MIL-HDBK-217; however, data is often very limited for some environments and specific part types. For these cases, it then becomes necessary to use the "rolled up" estimates provided, which make use of all data available for a broader class of parts and environments. Although the data book approach is generally thought to be less desirable, it remains an economical means of estimating "ballpark" reliability for mechanical components.	For mechanical components, NPRD-95 is the most widely used	
NSWC-94/L07	Handbook of Reliability Prediction Procedures for Mechanical Equipment developed by the Naval Surface Warfare Center – Carderock Division This handbook presents a unique approach for prediction of mechanical component reliability by presenting failure rate models for fundamental classes of mechanical components Examples of the specific mechanical devices addressed by the document include belts, springs, bearings, seals, brakes, slider-crank mechanisms, and clutches. Failure rate models include factors that are known to impact the reliability of the components. For example, the most common failure modes for springs are fracture due to fatigue and excessive load stress relaxation. The reliability of a spring will therefore depend on the material, design characteristics and the operating environment. NSWC-94/L07 models attempt to predict spring reliability based on these input characteristics. See	▪ For mechanical components, NSWC-94/L07 offers a more accurate alternative than NPRD-95 if the required detailed input data is available and manufacturing defects can be ignored	▪ The drawback of the approach is that, like the physics of failure models for electronics, the models require a significant amount of detailed input data (e.g., material properties, applied forces, etc.) that is often not readily available. . ▪ Does not address the issue of manufacturing defects
Occupational Health Hazard Analysis (OHHA)	Identifies health hazards and recommends provisions such as ventilation, barriers, protective clothing, etc	▪ Logical model of a system is repeatedly exercised, each run sues different values of the distributed parameters. ▪ Cab be used for system dependability modelling	▪ Very expensive in computer time
Operability Analysis	The aim of carrying out Operability Analysis is to highlight any issues that have a bearing on the operability of a system/equipment. An Operability Analysis should act designed for operation in the simplest and easiest way possible. Carrying out an Operability Analysis involves the following: • Task Analysis • Workload analysis • Human reliability analysis • Taking due account of the prevailing environmental conditions Effort invested in the Operability Analyses will vary with the criticality of the equipment, its interfaces and interactions with other equipment. Therefore the scope of operability assessments can be restricted to a single task or cover a range of tasks Methods include: • Anthopemetrical Studies can be used to provide known physical data on the population to assess workplace layout and architecture. • Rapid prototype modelling permits varied configurations to be tested over comparatively short timescales. This technique permits feedback from subject matter expert to be incorporated into the model, and assessed promptly, before possible inclusion into the design. • Task analysis involves a study of the workforce (operators) to ascertain what is required to achieve the system goals. This allows comparison between the task demands and the operator's capabilities. • Workload analysis is an analysis of the demand placed on the operator by the task requirements. • Human reliability analysis recognises the critical area where human error may affect performance. • Operational scenario analysis is an analysis that the activities required to be undertaken, can be successfully completed using the manpower and facilities provided for the purpose.	An Operability Analyses will: □ Highlight possible operability problems early in the design phase □ Provide the means to remove operability problems from the design □ Instill confidence in the finalised design □ Provide a demonstration of the operability of new and /or modified systems	▪
Operating &Support Hazard Analysis (0SHA)	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 [Tarrents, 1980] Evaluates hazardous operating, maintenance and support tasks by systematically evaluating each phase of operation and support. Can be divided into 2 separate analyses: ▪ The Operating Hazard Analysis ▪ Support Hazard Analysis	▪ Identifies the nature and duration of actions that occur under hazardous conditions	▪ Requires input from experienced operators/maintainers.
Pareto Analysis	A ranking technique based only on past data that identifies the most important items among many. Uses the 80-20 rule, which states that about 80% of the problems are caused by about 20% of the causes.	▪ Can be used for any type of system, process, or activity as long as enough historical data are available ▪ Identifies the most important risk contributor so that more detail risk assessment can be performed later.	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Particular Risk Assessment (PRA)	A form of CCA. Technology or circumstance dependant analysis which considers common events or influences that are outside the system(s) concerned (e.g. fire, lighting) which may violate failure independence claims. Some of these risks may also be the subject of specific airworthiness requirements. PRA examines common events that are external to the systems concerned, but which may violate independence requirements (e.g. uncontained engine rotor failure; fire; bird strike; lightning; HIRF; Human Factors, etc). (e.g. Damage may result in multiple systems failing; Incorrect pilot response could lead hazardous flying condition). Each risk is then examined to assess any simultaneous or cascading effects of each risk.	▪ Allows effects of non-related systems on each other to be evaluated. ▪ May address several zones at the same time. ▪ Typical risks include Fire, High Energy Devices, Leaking Fluids, Hail, Ice, Snow, Bird Strike, Tread Separation from Tire, Wheel Rim Release, Lightning, HIRF, etc.	▪ Best done at a late design stage to ensure complete picture. ▪ May involve complex calculations or simulation (e.g. trajectories of debris after fan/tyre burst. ▪ Only identifies the risks with respect to the design under consideration, each applicable risk should then be subject to a specific study to examine and document the simultaneous or cascading effect(s) of each risk.
Petri Net Analysis	Petri Net Analysis is a method to model unique states of a complex system. Petri Nets can be used to model system components, or subsystems at a wide range of abstraction levels; e.g., conceptual, top – down, detail design, or actual implementations of hardware, software, or combinations [Tarrents, 1980]	▪	▪
Physics-of-Failure	This family of approaches differs significantly from the other empirical reliability prediction methodologies and is used primarily at the sub-device level during the design stage. Physics-of-Failure approaches attempt to identify the "weakest link" of a design to ensure that the required equipment life is exceeded by the design. The methodology generally ignores the issue of defects escaping from the manufacturing process and assumes that product reliability is strictly governed by the predicted life of the weakest link. Example models address microcircuit die attach fatigue, bond wire flexure fatigue and die fatigue cracking. The models are very complex and require detailed device geometry information and materials properties. In general, the models are thought to be most useful in the early stages of designing devices (e.g., hybrids) but not at the assembly level when flexibility no longer exists to change device designs. See	▪	▪
PRISM	PRISM is a new technique (release in 2000 based on the Reliability Analysis Centre's databases) which has the ability to model the effects of thermal cycling and dormancy. It provides the ability to update predictions based on test data and addresses factors such as development process robustness. Available as an automated tool (as opposed to a handbook compendium of models like the others), PRISM interfaces directly with RAC's electronic and nonelectronic automated databases and provides an elaborate methodology to assess the quality of the system development process. It includes a means to include software reliability but is limited by the fact that it does not yet include models for all commonly used devices. The PRISM system reliability model is: $\lambda_S = \lambda_{IA}(\pi_P\pi_{IM}\pi_E + \pi_D\pi_G + \pi_M\pi_{IM} + \pi_E\pi_G + \pi_S\pi_G + \pi_I\pi_E + \pi_N + \pi_W\pi_E) + \lambda_{SW}$ where λ_{IA} is the initial assessment failure rate (based on "RACRates" component failure rate models incorporated into PRISM) for the system based on its parts and the remaining factors address parts processes (π_P), infant mortality (π_{IM}), environment (π_E), design processes (π_D), reliability growth (π_G), manufacturing processes (π_M), system management processes (π_S), induced processes (π_I), no-defect processes (π_N), and wear-out processes (π_W). λ_{SW} is the software failure rate. Quantitative values for the individual factors are determined through an extensive question and answer process intended to benchmark the extent that measures known to enhance reliability are used in design, manufacturing and management processes.	▪ provide improved modelling capability compared to MIL-HDBK-217 ▪	▪ At this time it's rather limited from a device coverage standpoint but it shows potential for community acceptance as it matures. ▪ will need to be expanded to include more part categories, and further evaluated by industry prior to widespread adoption.
Procedural Event Analysis Tool (PEAT)	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 of PEAT 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 includes database storage, analysis, and reporting capabilities.	•	▪
Procedure Analysis	Procedure Analysis is a step-by-step analysis of specific procedures to identify hazards or risks associated with procedures. The technique is universally appropriate. [Tarrents, 1980]	▪	▪
Production System Hazard Analysis	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 [Tarrents, 1980]	▪	▪
Prototype Development	Prototype Development provides a Modeling/Simulation analysis the constructors 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.	▪	▪
Qualitative Assessment	A collective term for the various methods of assessing causes, severities, and likelihood of potential Failure Conditions. Typical types of analysis include Design Appraisal, Installation Appraisal, FMEA, FTA, DD, Reliability Block Diagrams, etc.	▪ Supports experienced engineering and operational judgement.	▪ Not all of these methods are structured

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Quantitative Assessment	A collective term for the various analyses (such as failure modes and effects, fault tree, or dependence diagram) which also includes numerical probability information. The probabilities of primary failures can be determined from failure rate data and exposure times, using failure rates derived from service experience on identical or similar items, or acceptable industry standards. The conventional mathematics of probability can then be used to calculate the estimated probability of each Failure Condition as a function of the estimated probabilities of its identified contributory failures or other events. Often used for Hazardous or Catastrophic Failure Conditions of systems that are complex, that have insufficient service experience to help substantiate their safety, or that have Attributes that differ significantly from those of conventional systems. Quantitative Probability Terms are usually expressed in terms of acceptable numerical probability ranges for each flight hour, based on a flight of mean duration for the aeroplane type (However, for a function which is used only during a specific flight operation; e.g., take-off, landing, etc., the acceptable probability should be based on, and expressed in terms of, the flight operation's actual duration): a. Probable Failure Conditions are those having a probability greater than of the order of 1×10^{-5}. b. Improbable Failure Conditions are divided into two categories as follows: (i) Improbable (Remote) Failure Conditions are those having a probability order of 1×10^{-5} or less but greater than of the order of 1×10^{-7}. (ii) Improbable (Extremely Remote) Failure Conditions are those having a probability of the order of 1×10^{-7} or less, but greater than of the order of 1×10^{-9}. c. Extremely Improbable Failure Conditions are those having a probability of the order of 1×10^{-9} or less.	▪ Used to compare the achieved reliability with the reliability target. If the target is not satisfied, then the design is adapted until it is met.	▪ It is recognised that, for various reasons, component failure rate data are not precise enough to enable accurate estimates of the probabilities of Failure Conditions. This results in some degree of uncertainty, as indicated by the expression “of the order of”. When calculating the estimated probability of each Failure Condition, this uncertainty should be accounted for in a way that does not compromise safety ▪ Quantifying risk that are based on combining probabilities of individual component failures and mutually exclusive events are not appropriate for systems controlled by software and by humans making cognitively complex decisions, and there is no effective way to incorporate management and organizational factors, such as flaws in the safety culture. As a result, these critical factors in accidents are often simply omitted from risk assessment because analysts do not know how to obtain a “failure” probability, or alternatively, a number is pulled out of the air for convenience.
RDF 2000	This is the latest and most comprehensive of the European methodologies developed by CNET. It hasn't yet received much attention in the US but it could evolve into the new international standard should MIL-HDBK-217 continue to become outdated. Like the PRISM approach, it also addresses thermal cycling and dormant system modeling. RDF 2000 is the new version of the CNET UTEC80810 reliability prediction standard that covers most of the same components as MIL-HDBK-217. The models take into account power on/off cycling as well as temperature cycling and are very complex with predictions for integrated circuits requiring information on equipment outside ambient and print circuit ambient temperatures, type of technology, number of transistors, year of manufacture, junction temperature, working time ratio, storage time ratio, thermal expansion characteristics, number of thermal cycles, thermal amplitude of variation, application of the device, as well as per transistor, technology related and package related base failure rates.	▪ As this standard becomes more widely used it could become the international successor to the US MIL-HDBK-217.	▪
Reliability Analysis	A full review of the reliability of an aircraft part or component, making use of past data to determine the reliability of a component or maintenance technique.	▪ Uses factual information ▪ Highlights areas which need improvement. ▪ Focuses resources. ▪ Feeds into FMEA.	▪ Many variables may underlie the data used. ▪ Data on failure modes may be out of date. ▪ Not applicable to new products.
Reliability Block Diagram	A graphical means of representing which set of correctly working components may combine to provide the system function. Constructed of blocks and connections representing devices in provision of a function.	• Establishes reliability/availability goals. • Identified design problems and assists in trade-off studies of alternative designs. • Can include failure probability calculations. • Assists in identifying the interdependencies (e.g. for FTA and FMEA)	▪ Block failures need to be independent of each other.
Repertory Grid Analysis	Based in clinical psychology and personality theory, Repertory Grid Analysis is a structured and theoretical form of interview method. Subjects group concepts and justify how the groups are similar and dissimilar. Although a simple technique it does require some familiarity for effective application [Baber, 1996]	•	
Risk-Based Decision Analysis	An efficient approach to making rational and defensible decisions in complex situations [Tarrents, 1980]	▪	▪
Root Cause Analysis	This method identifies causal factors to accident or near-miss incidents. The root causes are the underlying contributing causes for observed deficiencies that should be documented in the findings of an investigation [Tarrents, 1980]. Root causes are the most basic causes of an event that meet the following conditions: • they can be reasonably identified • management has the ability to fix or influence them Typically, root causes are the absence, neglect, or deficiencies of management systems that control human actions and equipment performance. Root cause analysis provides a means to determine how and why something occurred. Understanding the accident scenario is not enough. Scenarios tell us what happened, not why it happened. Events in accident scenarios are generally only symptoms of underlying problems in the administrative controls that are supposed to keep those events from occurring. Understanding only the scenario addresses the outward symptoms, but not the underlying problems. More investigation of the underlying problems is needed to find and correct those that will contribute to future accidents.	▪ Usefull for accident/incident analyses ▪ Goes beyond the direct causes to identify fundamental reasons for the fault or failure. • Root cause analysis provides a means to investigate underlying problems. • Facilitates understanding of how an accident event occurred by discovering the underlying root causes (management system weaknesses) of the key contributors (causal factors) • Developing and implementing practical and effective recommendations for preventing future accidents	▪
Safety Review	Assesses a system, identify facility conditions, or evaluate 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. [Tarrents, 1980]	▪	▪

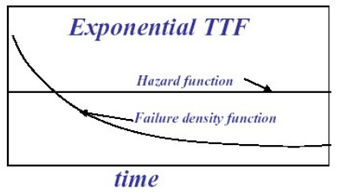
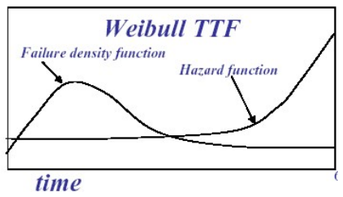
TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Scenario Analysis	Scenario Analysis identifies and corrects hazardous situation by postulating accident scenarios where credible and physically logical Scenarios provide a conduit for brainstorming or to test a theory in where actual implementation could have catastrophic results. Where system features are novel, subsequently, no historical data is available for guidance or comparison, a Scenario Analysis may provide insight. [Tarrents, 1980]	▪	▪
Scenario-Based Requirements Analysis (SCRAM)	An iterative scenario based technique based on a mixture of creative and systematic processes Question Probes: What could go wrong at next step? Influencing Factors: What is likely to make things go wrong at the next step? Consider Design Defence: How could the error/fault be prevented?	• Good for imagining possible events (i.e. works through expected problems. • Good at evaluating human operational effectiveness. • Builds on exiting practice (e.g. HAZOP, FMEA, etc) but adds another layer of analysis. •	• How many scenarios is enough? • How to find the "right" scenario? • Law of diminished returns apply (i.e. can continue safety analysis indefinitely but at what cost)
Sequencing Tools	Provide a means of reducing accidents to a collection of events and circumstantial facts; these facts can then be ordered using chronology and cause-and-effect relationships. The resulting structures can serve as models of the accident or incident. Examples of tools in this category include Events and Conditional Factor Analysis (ECFA) and Sequential times Events Plotting (STEP)	• Rigorous application of sequencing tools can clarify what actually did happen, a state of knowledge sometimes quite different from what the investigators (and sometime the witnesses) think happened.	•
SHEL Model	An illustration of the interrelationships between the 4 types of system resource and their environment • S = Software (i.e. rules, regulations, SOPs, customs, habits, etc • H= Harware (i.e. physical assets) • E = Environment (i.e. physical, political, social, economic) • L= Liveware (i.e. people) The usual interfaces: • L-H interface: The interaction between man and the machine (i.e. ergonomics) is probably the cause of most catastrophic accidents. • L-S interface: Considers the interaction of human characteristics with the requirements of the rules, procedures etc. • L-E interface: Considers how the human can cope in extreme conditions. Model can be extended to be 3D: • H-H interface (e.g. plug an play devices) • S-S interface (e.g. consistency of company operating procedures) • L-L interface (e.g. command and control)  	▪ Useful to illustrate how any changes ina single resource may have an impact on the systems integrity (e.g. change of H requires adaptation of S and L). ▪ ▪	
Single Function Diagram (SFD)	Shows schematically how a specific function is normally produced.	Provides the functional and timing relationships between the H/W, operator actions and S/W.	Does not consider malfunction situations in any way.
Single-Point Failure Analysis	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 This approach is applicable to hardware systems, software systems, and formalized human operator systems [Tarrents, 1980]	▪	▪
Sneak Analysis (or Sneak Circuit Analysis)	Looks for unintended paths (flows) within an electrical system. A Sneak Circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system, coded into the software program, or triggered by human error. The traditional approach to sneak circuit analysis is manually dissect the schematic drawings and transforming them into structures called network trees. Sneak clues are then applied to these trees. SNA can be performed using the Sneak Circuit Analysis Tool (SCAT), a PC based software package, and CapFast, an electrical circuit design and schematic editing tool. SCAT integrates with the schematic design package, CapFast. Original version was Sneak Circuit Analysis, devised after Mercury Redstone rocket launch accident (1961 See Def Stan 00-41 and Mil-Std-1543.	• Particularly useful for analysis electronic system diagrams. • Can also be used for sneak paths caused by H/W, S/W, operator, etc. • Sneaks are latent and are as a result of a failure, so cannot be analysis by FTA, FMEVA, etc. • This technique is applicable to control and energy-delivery delivery circuits of all kinds, whether electronic/electrical, pneumatic, or hydraulic. [Tarrents, 1980	This process is quite expensive and is often limited to highly critical (from the safety viewpoint) systems.
Software Failure Modes and Effects Analysis	This technique identifies software related design deficiencies through analysis of process flow-charting. It also identifies areas for verification/validation and test evaluation. [Tarrents, 1980]	▪ This methodology can be used for any software process; however, application to software controlled hardware systems is the predominate application. ▪ It can be used to analyze control, sequencing, timing monitoring, and the ability to take a system from an unsafe to a safe condition.	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Software Fault Tree Analysis	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 [Tarrents, 1980]	▪ Any software process at any level of development or change can be analyzed deductively. However, the predominate application is software controlled hardware systems.	▪
Software Hazard Analysis	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.	▪ This practice is universally appropriate to software systems.	▪
Software Hazard Analysis and Resolution in Design (SHARD)	Very HAZOP like, but with different keywords (i.e. Early, Late, Omission, Commission and Value). Developed by the University of York.	▪	▪
Software Sneak Circuit Analysis	Software Sneak Circuit Analysis (SSCA) is designed to discover program logic that could cause undesired program outputs or inhibits, or corrupts sequencing/timing [Tarrents, 1980]	▪ The technique is universally appropriate to any software program.	▪
Standard Ergonomics Assessment Methodology (SEAM)	One of the largest human factors teams in the UK, part of Qinetiq's Centre for Human Sciences, has been presented with the Ergonomics Society's 2004 award for Human Factors Integration, sponsored by Thales. In making the award, the Society recognised the importance of the team's development of a software tool (SEAM), which they used to make ergonomic assessments on the Bowman tactical communications system - one of the largest change programmes ever undertaken by the British Army, which will transform the Army's land vehicle and infantry communications. The Qinetiq team was tasked by the Defence Procurement Agency to assess Bowman at five key design stages. SEAM (Standard Ergonomics Assessment Methodology) helped them to make rigorous and consistent ergonomic assessments of the system. The software tool was designed for use by all members of the team irrespective of experience. It assisted them with data collection, data storage and report writing and will now be used for other military and civilian projects	The software tool was designed for use by all members of the team irrespective of experience and assisted them with data collection, data storage and report writing. Helps them make rigorous and consistent ergonomic assessments of the system. ▪	▪
Static Source Code Analysis	The process by which software developers check their code for problems and inconsistencies before compiling. Organizations can automate the source code analysis process by implementing a tool that automatically analyzes the entire program, generates charts and reports that graphically present the analysis results, and recommends potential resolutions to identified problems. Static analysis tools scan the source code and automatically detect errors that typically pass through compilers and become latent problems, including the following: • Syntax • Unreachable code • Unconditional branches into loops • Undeclared variables • Uninitialised variables • Parameter type mismatches • Uncalled functions and procedures • Variables used before initialization • Non-usage of function results • Possible array bound errors • Misuse of pointers	•	• Restricts language choices that may be used and the choice of the structures used within these languages. • Require highly skilled and experienced staff to carry out the tests and analyze the results. • It is not a complete answer for the validation and verification of safety-critical software even with the use of automated tools. Other forms of testing (for example dynamic) are required to verify certain aspects, like executing critical features. • Multitask applications software must be analyzed a task at a time. Another form of testing is required to check task interactions. • Dynamic aspects of the software (for example sequences of program execution) are difficult to model with static analysis techniques. • Most automated tools require translation to an intermediate language before they can analyze the code. Automatic translators are available for some languages, but for others one must either translate manually or write a new translator. Some language features do not have an equivalent in the intermediate language even with the automatic translators; they must be manually translated. The static analysis of the software depends on its translation model and the more skilled the analyst, the more skilled the model produced. The validation of the intermediate language model needs to be considered, as this can be a major problem. • Expensive means of validation of don to late in the development process • Most anomalies identified have no safety implications.

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Statistical Distributions	When carrying out the tasks assigned to it, the "output" of a system can be expressed as statistical distribution which describes the probabilities that the system output will reach or exceed any particular values.	• Distribution can be determined by simulations measurement/testing.	• For complex, systems which are affected by many variables (e.g. environmental factors), random testing will not suffice. •
Structural Safety Analysis	This method is used to validate mechanical structures. Inadequate structural assessment results in increased risk due to potential for latent design problems [Tarrents, 1980]	▪ The approach is appropriate to structural design; i.e., airframe	▪
Structured What If Technique (SWIFT)	High level structured brainstorming technique that originated from the process/manufacturing industry. As the name implies, this process is based around a series of structured and well-defined questions aimed at brainstorming possible failure mechanisms for the system at an early stage of the design. Considers complete systems, subsystems and processes. Has many similarities to HAZOPS, in that it is team-based brainstorming and uses prompts (e.g. checklists) to explore the behaviour of a system and identify hazards. Instead of Guide Words, SWIFT uses a series of questions which usually, but not always start "what if ...". For example: What if; ➢ A specific item of equipment fails? ➢ The operator fails to carry out the correct procedure? ➢ The level Control fails to operate? ➢ A fire occurs in a particular part of the plant? ➢ A flood occurs? ➢ the maintainer tried to work without isolating the power supply ? [Defence Procurement Management Guide, DPMG/TEC/320 Iss1 (Sept98), http//dawn_10_1/modref/cdpiweb/dpmgs/tech/320.htm, 02/09/99]	• Useful for identifying hazards of a complete system/operation. • Systematic and thorough. • Effective alternative to HAZOP, but more system orientated. • Efficient, because it focuses on areas of importance (more pertinent than HAZOP). • Strengthened by the use of checklists resulting in additional level of thoroughness. • Scenario based, so useful to identify and evaluate contingency plans. • Generally a higher level than the HAZOPS process and results in a quicker study. •	• Not as rigorous as HAZOP. • Requires thorough preparation before the meeting (The first stage of the process is to generate the list of questions and this should draw on the experience and imagination of team members as well as standard hazard checklists and other documents relevant to that type of system) • The success of the process is reliant, primarily, on the experience of the personnel conducting the review.
Systematic Inspection	This technique purpose is to perform a review or audit of a process or facility[Tarrents, 1980]	▪	▪
Task analysis	Task analysis is a fundamental human factors method and underlies many other techniques. A small selection of known tools include: • Applied Cognitive Task Analysis (ACTA) • ATLAS • Functional Analysis System Technique (FAST) • Goals, Operators, Methods and Systems (GOMS) • Micro Saint (software programme) • Repertory Grid Analysis 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 notes/cautions/ warnings for integration in order into procedures, and receive feedback from operating personnel [Tarrents, 1980]	• Universally appropriate to any operation where there is a human input [Tarrents, 1980]	• Not strictly speaking a safety tool, but does contribute to the HF requirements (e.g. . design specification) which can influence safety. • Somewhat surprisingly perhaps, few computer-based tools have been developed to support it [Tarrents, 1980]
Technique For Human Error Rate Prediction (THERP)	This technique provides a quantitative measure of human operator error in a process [Tarrents, 1980] Widely used technique, which encompasses other human factor methods (e.g. FTA, Task Analysis, Performance Shaping Factors)	▪ This technique is the standard method for the quantifying of human error in industry.	▪
Technique for the Retrospective Analysis if Cognitive Error (TRACEr)	TRACEr provides a human error identification technique specifically for use in the air traffic control domain. It builds on error models in other fields and integrates Wickens' (1992) model of information processing in ATC. TRACEr is represented in a series of decision flow diagrams. [Shorrock and Kirwan, 1999] Based on models of human information processing where errors are caused by breakdown in: - Perception (misperceive or fail to perceive info correctly) - Decision (error of judgement, planning or decision making) - Memory (info forgotten or misrecalled). - Action (error in carrying out the task) Developed by NATS (see Burret, G & Foley, S, *Integrating Human Error Management Strategies Throughout the System Lifecycle,* National Air Traffic Services, Bournemouth, UK, presented *in Current Issues in Safety Critical Systems,* Proceedings of the 11th Safety Critical Systems Symposium 4-6 Feb 2003).	▪ Assists in identifying sources of human error . Knowing how and why an error occurred is the only way to successful intervention. ▪ Uses a standardised series of pick-lists and decision trees to enable consistent classification or error information. ▪ The method marks a shift away from knowledge based errors in other error analysis tools to better reflect the visual and auditory nature of ATM [Shorrock and Kirwan, 1999]. ▪ It has proved successful in analysing errors in AIRPROX reports to derive measures for reducing errors and their adverse effects [Shorrock and Kirwan, 1999]	▪ Largely reactive ▪ Needs to be combined with other techniques to enable allocation of safety targets.
Test Safety Analysis	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. This approach is especially applicable to the development of new systems, and particularly in the engineering/development phase. [Tarrents, 1980]	▪ A lessons learned approach of any new systems 'or potentially hazardous subsystems' is provided.	▪
Tests	Often analysis alone cannot accurately predict precise effects or probability of failures., so it becomes essential to conducts actual tests (i.e. on rigs or in situ). Essential in the following circumstances • With circuits which use integrating and differentiating functions or other processing which may be sensitive to changes in time constants. • In control system where it is often necessary to have cross-connections between channels in order to achieve synchronization or load sharing or cross-monitoring.	• Verify correct functionality • Inducing failures can be the only way to verify system performance. • Validates assumptions made during the development process.	• Generally more expensive than analysis. • Cannot test everything (e.g. software).

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
The IEEE Gold Book	IEEE STD 493-1997, IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems, provides data on commercial power distribution systems. Provides data concerning equipment reliability used in industrial and commercial power distribution systems. Reliability data for different types of equipment are provided along with other aspects of reliability analysis for power distribution systems, such as basic concepts of reliability analysis, probability methods, fundamentals of power system reliability evaluation, economic evaluation of reliability, and cost of power outage data. The handbook was updated in 1997; however, the most recent reliability data reflected in the document is only through 1989.	▪	▪
The Sequentially-Timed Events Plot Investigation System (STEP)	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 [Tarrents, 1980]	▪ In accident investigation a sequential time of events may give critical insight into documenting and determining causes of an accident.	▪
Time/Loss Analysis For Emergency Response Evaluation	Any airport, airline and other aircraft operators should have an emergency contingency plan to handle unexpected events. 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. This approach organises data needed to assess the objectives, progress, and outcome of an emergency response; to identify response problems; to find and assess options to eliminate or reduce response problems and risks; to monitor future performance; and to investigate accidents. [Tarrents, 1980]	▪	▪
Top-Down Analysis Approach	Starts by identifying the failure condition to be investigated and then proceeds to derive those failure modes (and combinations of failure modes) which can produce it. Built on the assumption that evaluation can be best served by examining the system as a whole (its goals, objectives, operating environment, etc.), the examining the individual sub-systems or components [Garland, et at]. An example top-down approach is the Functional Hazard Analysis (FHA)	▪ Requires an evaluation of the system as a whole (i.e. the "big picture"	▪
Trend(ing) Analysis	Trending is performed by sorting various characteristics of events of interest.	• Good to learn lessons form history • Facilitates performance assessments and projections Identifies persistent management deficiencies (root causes) Highlights unique, unrecognized, or improperly defined risks Identifies misallocated management resources Flags sudden changes in performance, either positive or negative Provides correlation of changes in performance to events producing such changes Highlights risk assessment weaknesses	Backward looking Does not allow for effects caused by aging systems (e.g. aircraft)
Uncertainty Analysis	Addresses, quantitatively and qualitatively, those factors that cause the results of an analysis to be uncertain [Tarrents, 1980]	▪	▪ This discipline does not typically address uncertainty explicitly and there are arguments that all analyses should ▪
User Analysis	Human hazard assessment technique Potential system users (including maintainers and installers) are identified and characterized for each stage of the system lifecycle. The most important user population is those people who will be regular users or "operators" of the product or system.	•	Even if user characteristics are identified, a simple list of characteristics often fails to influence design. Disembodied user characteristics may result in an "elastic user" whose characteristics shift as various features are developed. Designing for an elastic user may create a product that fails to satisfy any real user.
Walk-Trough Analysis	This technique is a systematic analysis that should be used to determine and correct root causes of unplanned occurrences related to maintenance [Tarrents, 1980]	▪	▪

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS

Weibull Analysis	Most reliability analysis uses an Exponential Time To Failure (TTF) distribution, which says that the instantaneous rate of failure is constant over time, and the item is as likely to fail at one moment as another (i.e. it is "memoryless" – that is, the item is not more likely to fail the next moment simply because it has operated for a long time)
	This is not good enough when considering the effect of ageing, when the failure rates are increasing. The question is: how often should this inspection be performed? One very useful distribution for modeling TTF in the presence of aging is the Weibull Distribution, which has the advantages of:
	(1) being very flexible to fit a large number of field data samples, and
	(2) (collapsing to the exponential TTF distribution when the field data is fairly flat over time, and
	(3) being a theoretical "limiting distribution" (which is somewhat beyond the scope of this brief).
	 
	 
	In Weibull analysis, the practitioner attempts to make predictions about the life of all products in the population by "fitting" a statistical distribution to life data from a representative sample of units. The parameterized distribution for the data set can then be used to estimate important life characteristics of the product such as reliability or probability of failure at a specific time, the mean life for the product and failure rate. Life data analysis requires the practitioner to:
	• Gather life data for the product.
	• Select a lifetime distribution that will fit the data and model the life of the product.
	• Estimate the parameters that will fit the distribution to the data.
	• Generate plots and results that estimate the life characteristics, like reliability or mean life, of the product
		• Is a powerful tool that provides the Reliability Engineer with a means to quantify the effect that various design options will have on reliability and cost.
		• Predict failure rates and provides a description of the failure of parts and equipment.
		• Provides useful insight into the following issues.
		  • Characteristic life
		  • Standard Deviation of Life
		  • Mean Life
		  • Reliability Functions
		  • Reliable Life
		  • Median Life Initial Failure Rate Per Unit Time
		
		http://www.bassengineering.com/weibull.htm	

What if Analysis	What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. [Tarrents, 1980] A problem solving approach that uses loosely structured questioning to (1) suggest upsets that may result in accidents or system performance problems and (2) make sure the proper safeguards against those problems are in place Typical qualitative probability terms are: a. Probable Failure Conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane. b. Improbable Failure Conditions are divided into two categories as follows: (i) Remote. Unlikely to occur to each aeroplane during its total life but which may occur several times when considering the total operational life of a number of aeroplanes of the type. (ii) Extremely Remote. Unlikely to occur when considering the total operational life of all aeroplanes of the type, but nevertheless has to be considered as being possible. c. Extremely Improbable Failure Conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type	▪ Useful for any type of system, process or activity. ▪ Useful when more precise methods (e.g. FMEA, HAZOPS) are not possible or practical. ▪ Especially useful if combined with Checklists.	▪
Life Data Analysis	See Weibull Analysis	▪	▪
Subjective Workload Assessment Technique (SWAT)	Human Factors evaluative tool	▪ Subjective in terms of safety implications	▪ Subjective
NASA-Task Load Index	Human Factors evaluative tool	▪ Subjective in terms of safety implications	▪ Subjective
Modified Cooper-Harper Scale	Human Factors evaluative tool	▪ Subjective in terms of safety implications	▪ Subjective
Bedford Scale	Human Factors evaluative tool	▪ Subjective in terms of safety implications	▪ Subjective

TECHNIQUE	DESCRIPTION	ADVANTAGES	LIMITATIONS
Pilot Subjective Evaluation (PSE)	Human Factors evaluative tool	▪ Subjective in terms of safety implications ▪ Accepted as a means of compliance by the FAA. Requires only limited training since it uses a comparison methodology. This makes it possible for a broad range of operational pilots with both domestic and international experience to participate in an assessment [Barnes, R. B, et al].	▪ Subjective ▪ The PSE's major short coming is in the data analysis. A large sample population having reference aircraft experience would be required to achieve statistical confidence. Consideration of age/rank, "seat" experience, and type of aircraft flown expand the sample matrix dramatically. However, the FAA does not require a statistical approach but rather looks for human performance trends and a detailed explanation for any outlyers in the data. Such outlyers which can not be resolved by any other means are usually corrected with "more training." Unfortunately, the result is that training once again becomes a primary method to mitigate poor or inadequate design [Barnes, R. B, et al].
Modified Pilot Subjective Evaluation (MPSE),	Human Factors evaluative tool Features custom modifications of the PSE which permit it to be adapted as necessary to meet the specific requirements of a certification while retaining the proven elements of the PSE.	▪ Subjective in terms of safety implications	▪
Dynamic Workload Scale	Human Factors evaluative tool	▪ Subjective in terms of safety implications	▪
What-If/Checklist Analysis	What-If or Checklist Analysis is a simple method of applying logic in a deterministic manner. [Tarrents, 1980]	▪	▪
Zonal Safety Analysis (ZSA)/Zonal Hazard Analysis (ZHA)	CCA technique which specifically considers physical proximity of different technologies. Theoretical and visual examination of each physical zone to ensure that interference and interactions with adjacent systems do not violate the independence requirements. Used to: • determine compliance with the installation rules, • identify any potential cascade failures due to system interaction, • identify any potential areas for maintenance errors, • identify potential areas for system malfunction due to environmental factors. This technique is used to look at the complex interactions that can occur between high-energy systems and is specifically concerned with their physical position in relation to each other. The Zonal Hazard Analysis techniques are also used to assess the effects of the proliferation of hazards into adjacent physical areas or compartments. They can be used to identify the routes by which the hazards may spread and in so doing, solutions can be developed to control and mitigate the effects of the hazard. See SAE ARP5754 p38	▪ Highlights potential hazards from adjacent non-related systems (e.g. heating pipes near sensitive electronic equipment, hot air leaks, drips from pipes, multi-channels through same connectors, EMI effects on multi-channel configurations, etc). ▪ Considers any potential interactions between high-energy sources and sensitive items. ▪	▪ Best done at a later stage in the design when all equipment can be considered. This means that changes are likely to be expensive ▪ Tends to be very subjective, difficult to systematise. ▪ Restricted to each specific zone considered. ▪ Requires system experience. ▪ Checklists can be utilised in the process to identify hazards, they can also be used to check that designs comply with certain standards and codes of practice, or that protective measures are correctly employed. They are however, reliant on the knowledge and experience of those persons compiling the lists