A98-31690

ICAS-98-6,7,3

SAFETY ASSESSMENT OF AIRCRAFT MOUNTED SYSTEMS

Luigi TROTTA, Riccardo BUFFARDI, Rodolfo QUERZOLI
Alenia Aerospazio, Aeronautics Division
Corso Marche 41, 10146 Torino - Italy

Abstract

This contribution will highlight the methodology to assess the Safety aspects of Military Aircraft Systems, being part of a Fly-By-Wire A/C.
The correlations between FMECA and Safety Assessment will be shown to identify all possible hazards caused by single failures.
A tool using Fault Tree Analysis approach, to assess from a quantitative and qualitative point of view the discovered hazards, will identify the minimal cut sets and critical items in the System configuration.
Through the Zonal Hazard Analysis it will be shown how to identify the hazards due to the physical location of the system components and the possible effects due to component failures, disadvantageous operating conditions, maintenance errors and environment induced faults.
Software Safety Assessment is performed to analyse and assess the safety of the software configuration items of a System and ensures that a risk classification is allocated appropriate to the severity of hazard which could be caused by a software error.
These results will lead to define the critical areas and the possible corrective actions to give a compliance statement to System Qualification and Airworthiness requirements.

Introduction

Safety concept has always been present in the designer's mind, since the first flight in the 1903 of the Wright brothers aircraft, but it was treated in a deterministic way, while now a probabilistic approach is considered.
Safety is generally considered as one of the primary objectives in the aeronautical programmes and requires to be given equal priority with reliability, maintainability, performance, cost and timescale during all phases.
A safety assessment is performed to identify, assess and eliminate (or reduce to an acceptable level) the effects of hazards. Results of this activity will represent a positive statement against System Qualification and Airworthiness requirements.

Failure Analysis of the System

A failure analysis starts from the system configuration and it identifies the involved items with their mutual relationship. It is finalised to discover all possible single failure modes and final effect at System level.

Functional Block Diagram

A Functional Block Diagram shows the System functions, their relationships and the System input/output interfaces. Each function is then represented through blocks and for each block a list of the various associated components is provided.

Component Part List and Reliability Prediction

A Component Part List and Primary Defect Rate prediction analysis identifies all the component parts which belong to the System. Further a Primary Defect Rate in the specified operational/environmental conditions is predicted for each component.
The purpose of this activity is to verify, wherever possible, the quality of the selected components and their Reliability prediction.
The quality of the components is verified through a predefined table where the design can be controlled in great detail. Through this table the following parameters are verified:

- engineering safety factor intended as the ratio between allowable and applied limit stress for the material.
- Fatigue factor to take into account the fatigue analysis.
- Material treatment by considering the kind of material component, its protection, possible corrosion and/or contact with other materials.

A Reliability prediction is performed for each one of the components identified as above. This prediction is based on:

- data bank and handbooks universally recognised (MIL-HDBK-217E; NPRD 3; FARADA, etc...);

21st ICAS Congress
13-18 September 1998
Melbourne, Australia

- Internal data bank of the System Design responsible having experience on the involved System.

Taking into account the environmental/operational conditions an adjustment factor is identified in order to adapt the base predicted defect rate at a realistic figure/condition. These adjustment factors take into account the different stress, environment, etc. of the involved System.

Hazard Analysis

The purpose of this activity is to identify all events, "Hazards", that can jeopardise the System/personnel Safety. The identification of the Hazards can be based on the "known hazards" from other similar programmes and from "Analyses" such as Preliminary Hazard Analysis, Zonal Hazard Analysis, Failure Mode Effect and Criticality Analysis.

a) "Known Hazards"

The first step in the identification of the Hazards is the experience accumulated from other similar programmes. Accident, incidents and safety critical occurrences occurred from other similar programmes will be taken into consideration.
These "known" Hazards will be analysed jointly by System and Safety Engineers in the light of the actual design characteristics.

b) Analyses

The Safety analysis is a continuous process during System concept, development and production phases. A Safety analysis requires a clear definition of the System in form of understandable block diagrams, see above point 3.3, for all the modes of operation. A Safety analysis will be based on the top down approach in order to discover Safety critical areas and to identify interface Hazards, it is performed for each function of the system.
Three questions are considered for each function to identify relevant Functional Failure, these are:

- Loss of function
- Function supplied not correctly (e.g. insufficient performance of the System function).
- Function supplied correctly when not required (e.g. false warning).

The effect of the Functional Failures on the Aircraft and/or personnel is given and the severity of the hazard categorised. Furthermore the Safety Analysis is used to extend the Hazard investigation into hazardous areas in more detail by qualitative and quantitative method. The final aim will be to demonstrate that the required Safety level has been met.

Preliminary Hazard Analysis (PHA)

A Preliminary Hazard Analysis is the first one produced by System and Safety Engineers during the early system design. It must not be a cursory analysis because of the major influence it will have on the design philosophy, impact on design and on the production System Safety potential.
This analysis is performed in order to identify Safety critical areas and to determine Safety design criteria to be used.
The Preliminary Hazard Analysis is based on the best available data and past experience ("lesson learnt") to discover a preliminary list of Hazards which may lead to a Safety critical occurrence.
The steps of the analysis are:

- System Safety requirements definition.
- System historical data evaluation, accident and incident data together with their consequences from similar systems . Further their effect on the System will be postulated.
- Functional Failure analysis using a "Top Down" approach. This analysis considers single and double failures within the System; System failure that in combination with other system failures generate an Hazard.
- Evaluation of System Safety impact relevant to physical location (Zonal Hazard Analysis report).
- List of the identified Hazards and evaluation of Safety risk based on figures.
- Identify Safety features to reduce Safety risk.
- Conclusions to highlight areas requiring further work and areas where an unacceptable Safety risk has been identified. In this last occurrence the action that could be taken to alleviate or reduce the risk will be considered.

Failure Mode Effect and Criticality Analysis (FMECA)

The above paragraphs have identified the functions performed by the System and the related failure rates. The System has then been identified and now the failure modes are taken into consideration. With regard to this aim a FMECA is performed. The System and the Safety Engineers analyse in turn each functional block in order to highlight all the possible failure modes of its components. Once identified the failure modes, their effect on the System must be established.
In order to follow a logical and self-explanatory sequence to assess the failure mode effects, the following steps are applicable:

a) identify the effect, at functional block level, of the failure induced by components belonging to that functional block.
b) Evaluate the final effect, at System level, of the functional block failure.

The following figure explains better the situation:

Functional analysis:

Component ⇒ **Functional Block** ⇒ **System**

Failure analysis:

Failure Mode of the Component ⇒ **Effect on Functional Block** ⇒ **Effect on System**

Applying the above procedure to all the Functional Blocks and relevant components of the System, a comprehensive analysis of the System failure modes/effects is performed.
In order to assess the criticality of the failure effects, a criticality classification is established. The System and Safety Engineers decide jointly to highlight some failure effects whose occurrence could jeopardise the flight safety of the System/Aircraft.
The categories are defined as follows:

a) Flight Safety Critical. Indicates that a defect mode of the System can cause a Hazard. This is independent of the fact that internal redundancy may or may not prevent a hazardous single defect.
b) Flight Safety Involved. Indicated that a defect mode of the System can only cause a Hazard in combination with additional defect mode(s)/event(s) external to that System.

All the remaining System failure effects not falling down into one of the two above classes, are assessed upon one of the following effects:

- failures causing a mission loss/degradation.
- failures causing an unscheduled maintenance.

All the above steps, performed during the FMECA activity, have identified all the possible critical events caused by single failures. At this stage of the FMECA activity the failure modes and effects of the System have been identified; all the failure modes having an impact on the Safety and then identified through the categories "a" and "b" shown above, will be considered as "Hazards".

<u>Zonal Hazard Analysis</u>

Failure Analyses are usually performed using functional block diagrams which do not take into account installation aspects. Then a Zonal Hazard Analysis is required to enable the Safety levels to be fully established. The Zonal Hazard Analysis considers the physical location of the System components and the possible effects due to failures and disadvantageous operating conditions, maintenance and environment induced faults.
One of the aim of this analysis is to verify if each functional redundancy is considered with regard to its physical location. The implementation of all corrective actions required as consequence of previous Zonal Hazard Analyses on drawings, tridimensional schemes and Mock-ups will be verified on prototypes and production system. Any potential critical areas will be investigated.
The Zonal Hazard Analysis starts from the beginning of the installation design and continues during project development. At different steps of the project development different tools can be used, such as check list, drawings, CAD systems, Mock-ups, prototype and production system. The figure 1 shows the relationship between documents to use and the stage of the design.
Before prototype assembly a check list is prepared jointly by System/Design/Safety Engineers. In order to prepare this list the System Engineer defines the installation requirements/criteria based on installation rules contained in MIL-STDs, STANAGs and/or design requirements related to the programme, and/or design practices. The list of the requirements/criteria with relevant reference is included in a report using a dedicated table.
After this, a check list is prepared. This list consists of a series of simple questions which allow the System Engineer to verify, from a safety point of view, that the design complies with the requirements. The check list is prepared and updated during each stage of the design by the Safety Engineer together with the System/Design Engineers.
At the end of this stage a report is prepared listing all the cases of not-compliance with recommendations for necessary corrective actions using a dedicated table This report includes also the list of the Hazards, if they exists.
All the above identified corrective actions are verified during the assembly phase on the aircraft. The Safety Engineer performs this analysis by physical check inspections on the assembled aircraft. An investigation, for further critical areas, will be done with a depth of analysis compatible to the current assembling phase.
At the end of this phase a report is prepared describing the corrective actions introduced and listing all the new hazards identified.

DOCUMENTS	PHASES		
	BEFORE PROTOTYPE ASSEMBLY	PROTOTYPE ASSEMBLY	PRODUCTION
Installation Requirements Relevant to the System	▼———▼		
Preliminary Zonal Hazard Analysis Using Dedicated Check List	▼————▼		
Zonal Hazard Analysis Before Prototype Assembly		▼	
Zonal Hazard Analysis During Prototype Assembly		▼--------------------------▼	
Zonal Hazard Analysis Before Production Phase			▼------------------▼

Fig. 1 - Time schedule of the zonal hazard analysis report

Finally during production phase the same approach, used previously, is applicable.

Fault Tree Analysis

A Fault Tree Analysis is described as an analytical technique, whereby an undesired event is specified (Top Event), and then analysed with a top down approach, in the context of its environment and operation to find all credible paths in which it can occur. The Fault Tree itself is a graphic model of the various parallel and sequential combinations (Boolean representation) of faults that result in the occurrence of the predefined undesired event. The faults are events that are associated with component hardware failures, human errors or any other pertinent events which can lead to the undesired event. A typical Fault Tree is composed of a number of symbols which are described in the Fig.2.

One of the main purposes of representing a Fault Tree in terms of Boolean equations is to determine the associated Fault Tree "minimal cut sets". A minimal cut set is defined as the smallest combination of component failures which, if they occur, cause the Undesired Event to occur.

The minimal cut sets define the "Failure Modes" of the Undesired Event and are usually obtained when a Fault Tree is evaluated. Once the minimal cut sets are obtained, the quantification of the Fault Tree is achieved through the minimal cut set unavailabilities summation. A minimal cut set thus identifies an Undesired Event. If one of the failures in the cut set does not occur, then the Undesired Event does not occur by this combination. Any Fault Tree consists of a finite number of minimal cut sets, which are unique for that Undesired Event. Once a Fault Tree is build up, it can be evaluated to obtain qualitative and/or quantitative results.

Qualitative results includes: the minimal cut sets of the Fault Tree , qualitative components importances. The qualitative importance give a "qualitative ranking" on each component with regard to its contribution to the System failure.

The quantitative results obtained from the evaluation includes: probability figures for Undesired Event and minimal cut sets, quantitative importance of components and of minimal cut sets, Sensitivity and relative probability evaluations.

The quantitative importance give the percentage of time that system failure is caused by a particular minimal cut sets on a particular component failure. The sensitivity and relative probability evaluations determine the effects of changing maintenance and checking times, implementing design modifications and changing components reliability. Also included in the sensitivity evaluations are error analysis to determine the effects of uncertainties in failure rate data.

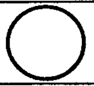
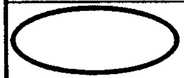
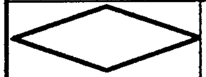
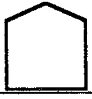
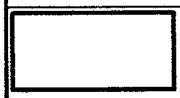
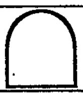
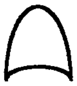
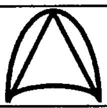
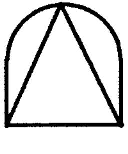
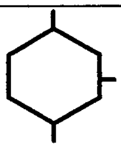
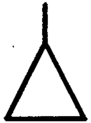
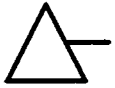
PRIMARY EVENT SYMBOL	
	**BASIC EVENT** - A basic initiating fault requiring no further development.
	**CONDITION EVENT** - Specific conditions or restrictions that apply to any logic gate (used primary with PRIORITY AND and INHIBIT gates).
	**UNDEVELOPMENT EVENT** - An event which is not further developed either because it is of insufficient consequence or because information unavailable.
	**EXTERNAL EVENT** - An event which is normally expected to occur.
INTERMEDIATE EVENT SYMBOL	
	**INTERMEDIATE EVENT** - A fault event that occurs because of one or more antecedent causes acting through logic gates.
GATE SYMBOL	
	**AND** - Output fault occurs if all of the input faults occur.
	**OR** - Output fault occurs if at least one of the input faults occurs.
	**EXCLUSIVE OR** - Output fault occurs if exactly one of the input faults occurs.
	**PRIORITY AND** - Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)
	**INHIBIT** - Output fault occurs if the (single) input fault occurs in the presence of and enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate).
TRANSFER SYMBOLS	
	**TRANSFER IN** - Indicates that the tree is developed further at occurrence of the corresponding TRANSFER OUT.
	**TRANSFER OUT** - Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN.

Fig. 2 - Fault Tree Symbols

All the relevant reliability figures, for the component failures, are taken from the reliability analyses such as Primary Defect Rate prediction, Functional Block Diagram, Failure Mode Effect and Criticality Analysis.

Hazard Log

The purpose of this activity is to document and track the Hazards highlighted during the above Hazard Analyses and the progress made towards alleviation and/or elimination of the associated risk. A Central Automatic Data Processing (ADP) is compiled and maintained by the Safety Engineer as the administration method employed to catalogue, file and track all the Hazards identified. It does not in itself lead to the identification of the Hazards.
The information submitted is standardised and comprise as a minimum the following:

1) Hazard Title and unique Identification Number;
2) Hazard Description;
3) Affected System;
4) Hazard Severity;
5) Hazard Probability (where available);
6) Hazard Risk Index;
7) Effects of Hazard;
8) Influence of Human Factors on Hazard;
9) Influence of Environment plus Operating Conditions on Hazards;
10) Influence of Software on Hazard;
11) Action taken or Measures implemented for Hazard resolution or rationale and authority for no further action.

In order to entry each Hazard into the log a unique identification number is assigned out. Hazards which are considered to be resolved can be transferred to an archive section of the log.

Hazard Risk Assessment

In order to give priority to the treatment of Hazards and to thus ensure that the greatest effort in alleviating and resolving Hazards is expanded where the greatest risk exist, a method of risk assessment is implemented. For any Hazard the severity is firstly determined and when possible a probability of occurrence assigned.
The combination of the above mentioned severity and probability define the Hazard Risk Index associated with Hazard. This is the factor in deciding the priority for treatment of Hazard.
The Hazard severity expresses the qualitative results of the worst possible, but credible, effects of the Hazard. An Hazard severity category range is assigned by the Safety Engineer in accordance with Fig.3.

Description	Category	Definition
Catastrophic	I	Death and/or aircraft loss.
Critical	II	Severe injury, severe occupational illness, and/or major aircraft damage.
Marginal	III	Minor injury, minor occupational illness, and/or minor aircraft damage.
Negligible	IV	Less than minor injury, occupational illness, and/or aircraft damage.

Fig. 3 - Hazard Severity Categories

The assignment of the severity category is done jointly with the System Engineer. The qualitative risk assessment remains a fairly simple method in order not to introduce delay into the procedure to cover Hazards. The quantitative risk assessment for the Hazard, which expresses the likelihood that the Hazard occurs, is assigned as early as possible. For this purpose the Fig.4 is used.

Fault Tree technique is used to show the interdependence of events and contributing factors which lead to the Hazards and establish the probability of the Hazards. Probabilities of component failures are obtained from the Reliability analyses (Component Part List & Primary Defect Rate prediction, Functional Block Diagram, Failure Mode Effect and Criticality Analysis).

Following assignment of severity and probability categories, the overall risk of the Hazard is determined by using the combination matrix in Fig.5.

The above analyses have identified all the possible Hazards to which the System may subject or contribute to. These Hazards are assessed from a qualitative and quantitative point of view in order to evaluate the risk induced by them.

Following this, three possible cases exist:

1) the risk level is acceptable.
2) The risk level is not completely satisfactory.
3) The risk level is unacceptable.

In the first case no further action are requested and the above theoretical analyses are sufficient to provide a compliance input to Airworthiness certification activity.

In the second case a further discussion with the Customer is needed. The discussion defines if further analyses steps are necessary or if the confidence level can be increased and accepted.

In the third case action is needed to eliminate the hazardous conditions or to reduce the risk level following the below actions:

a) redesign.

b) Incorporate Safety devices.

c) Incorporate warning devices.

d) Apply procedures or training.

The above steps must be applied in order of preference with regard to their applicability. Once decided the corrective action, the Safety Engineers will monitor that it does not jeopardise again the existing Safety level.

Software Safety Assessment

Scope of this activity is to analyse and assess the safety of the software configuration items of a system and ensures that software is given a risk classification appropriate to the severity of hazard which could be caused by a software error. The software safety assessment is performed by System Designers/Engineers, Software Developers and Safety Engineers and covers the System Design and Software Development Phases. It requires analysis of functions from the highest level down to Line Replacement Item (LRI) processing specification followed by analysis throughout the software development phases from Preliminary Design to Code& Unit Testing. The software safety assessment is performed in parallel with the System Design and Software Development, the phasing of the activities is shown in figure 6.

Software Classification

Three software risk classifications are defined. Risk class 1 is the highest risk classification, risk class 2 is the intermediate classification and risk class 3 is the lowest classification. The general descriptions of the software risk classifications are:

Risk class 1 - Software for which the occurrence of any failure condition or design error would prevent the continued safe flight or landing of the aircraft or lead to an inadvertent arming, release or non-release of stores.

Risk class 2 - Software for which the occurrence of any failure condition or design error would significantly reduce the capability of the aircraft or the ability of the crew to continue the assigned mission safely.

Approximate Hazard Probability Ranking	Category	Specific Item	Probability	Fleet Frequency(1000 aircraft)
Frequent	A	Likely to occur frequently	$>10^{-3}$	Likely to be continuously experienced during the fleet life
Probable	B	Will occur several times in life of an item	$<10^{-3}$ to $>10^{-5}$	Will occur frequently during the aircraft fleet life
Occasional	C	Likely to occur sometimes in life of an item	$<10^{-5}$ to $>10^{-7}$	Will occur several times during the aircraft fleet life
Extremely Remote	D	Unlikely but possible to occur in life of an item	$<10^{-7}$ to $>10^{-9}$	Unlikely but can reasonably be expected to occur during the aircraft fleet life
Improbable	E	So unlikely, it can be assumed occurrence will not be experienced during the life of the fleet	below 10^{-9}	Unlikely to occur during the aircraft fleet life (but possible)

Fig. 4 - Hazard Probability Categories

FREQUENCY OF OCCURRENCE	HAZARD CATEGORIES			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
(A) Frequent	1	3	7	13
(B) Probable	2	5	9	16
(C) Occasional	4	6	11	18
(D) Extremely Remote	8	10	14	19
(E) Improbable	12	15	17	20

Hazard Risk Index	Suggested Criteria
1 -5	Unacceptable
6 - 9	Undesirable (MA decision required)
10 - 17	Acceptable with review by MA
18 - 20	Acceptable without review

Fig. 5 - Hazard Risk Assessment

Risk class 3 - Software for which failures or design errors would not significantly degrade mission capability or crew ability.

In addition to these classifications an additional asterisk (*) attribute is introduced which applies to risk classes 2 and 3. The asterisk (*) is used to indicate that some "ancestor" of the function has a higher risk classification than the function itself. For functional failures which could be caused by software error, the software risk class (1, 2, 3) is established based upon the risk assessment. Three distinct cases are considered.

Firstly the case where a single software fault can lead to the identified functional failure mode. Secondly the case where a single software fault in combination with an independent event can lead to a failure mode, and thirdly the case where at least two different software faults must be present in order to lead to or contribute to the identified functional failure mode.

Single Software Fault

The software fault alone can lead to the functional failure. The hazard severity determines the software function risk classification according to the table 1.

HAZARD SEVERITY			
CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
CLASS 1		CLASS 2	CLASS 3

Table 1 - Risk Classification for Single Software Fault

Single Software Fault and Independent Event

Independent events must occur or conditions exist in combination with the software malfunction in order to lead to the identified functional failure. The independent event or events may be of many kinds. The principle in all cases, however, is to establish that the events or conditions are truly independent from the software fault and could not be commonly caused by a single software fault. The probability of independent events or conditions will be assessed although this may necessarily be qualitative in the early project stages. When the failure frequency of the combined independent factors has been assessed, the software function classification can be determined from the table 2.

Double Software Faults

Just as there is a general requirement to consider coincident failures of independent hardware components as part of the risk assessment process, it is necessary, when establishing software function classification, to consider the combined effects of independent software malfunctions.

The malfunctions may be in different systems/subsystem, on different processors in the same system/subsystem, or on the same processor. In any case the complete independence and diverse nature of the functions must be established if this section of the guidelines is to be applicable. If a complete independence and diversity argument cannot be made then both will be treated as a combined software function and the Single Software Faults guidelines applied.

FREQUENCY OF INDEPENDENT EVENT		HAZARD SEVERITY			
QUALITATIVE	QUANTITATIVE	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
Frequent	> 10^{-3}	CLASS 1	CLASS 1	CLASS 2	CLASS 3
Probable	10^{-3} - 10^{-5}	CLASS 1	CLASS 2	CLASS 2	CLASS 3
Occasional	10^{-5} - 10^{-7}	CLASS 2	CLASS 2	CLASS 3	CLASS 3
Remote	10^{-7} - 10^{-9}	CLASS 2	CLASS 3	CLASS 3	CLASS 3
Improbable	< 10^{-9}	CLASS 3	CLASS 3	CLASS 3	CLASS 3

Table 2 - Risk Classification of Software for a Single Software fault in conjunction with an Independent Event

Use of similar algorithms, common routines, common operating systems, similar data structures, common memory areas, common I/O addressing, etc. during software development can easily invalidate arguments based on functional independence and diversity made at the system safety assessment stage. Such arguments, therefore, are particularly onerous to implement and to maintain throughout the life of a product and it is recommended not to invoke them, particularly for failure modes classed as "loss of function".

Where a complete functional independence and diversity argument can be made then the classification of both software functions can be determined from the table 3.

HAZARD SEVERITY			
CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
2 x CLASS 2		2 x CLASS 3	

Table 3 - Risk Classification for Double Software Fault in Diverse Functions

System Design Activities

The System Design comprises the System Requirement Analysis phase and the Software Requirement Analysis phase. In the System Requirement Analysis phase, which may itself be phased, the system/subsystem functional requirements are defined providing the functional baseline. In the Software Requirement Analysis phase the software functional requirements are defined and assembled into individual LRI processing specification forming the allocated baseline. By the end of the System Requirement Analysis phase all the hazards which have been identified will be associated with identified functional failure modes or combined failure modes. The hazards will be categorised by severity (figure 3) and entered in the hazard log.

The following steps will be performed to provide the first functional classification:

a) Establish risk classification
Each function will be assigned a classification based on the highest hazard severity of its failure modes.

b) Record the classification
The initial classifications will be recorded against the identified functions in the formal design documentation.

c) Provide a justification
A justification for the classification will be included in the Preliminary Hazard Analysis and referenced in the Hazard Log.

Following the initial classifications the classifications in the subsequent phases of functional decomposition will be established and justified against the classifications assigned to their higher level function(s).

The following steps will be performed:

i) Assign risk classification
At the subsequent functional classification stage a function shall inherit the classification of its parent function unless safety features have been incorporated which allow the risk classification to be reduced.
Once the asterisk has been established it must be inherited by all "descendants" of a function. The asterisk attribute is an indicator that safety requirements additional to those normally associated with the risk classification may exist. It is provided as a safeguard, particularly important in the maintenance phase of a product, which will ensure that safety related design decisions made early in the design process are not corrupted or invalidated by modifications to low level components.

ii) Analyse risk classification
The risk classifications of the functions will be analysed to ensure the classifications have been correctly inherited. Where the risk classification has been reduced the functions will be analysed to ensure they fulfil the higher level safety requirements.

iii) Justify the classification
Where the risk classification of a function has been reduced a justification will be provided. The justification argument must take account of all safety related features which have been introduced into the design (e.g. hard-wired interlocks, watchdogs, reversionary safe states, comparators,....) and safety related testing requirements which must be fulfilled by lower levels.
Each justification statement made during the System Requirements Analysis phase is documented in one of the Preliminary Hazard Analysis reports and is traceable by unique reference to the Hazard Log and functional requirements.

iv) Analyse for new hazards
For all risk class 1 functions an analysis of the functional requirements/processing specification is performed, the analysis will be used to identify any dangerous failure modes of the function not

ICAS - 98 - 6.7.3 TROTTA

identified in the Hazard Log. In addition functions reduced to risk class 2 (i.e. risk class 2* functions) will be analysed to ensure that the hazard risks have been reduced or eliminated and no new hazards have been introduced. Any new hazards identified by the analyses of risk class 1 and 2* items will be transferred to the Hazard Log.

v) Record analysis
The results of the analysis will be recorded in the hazard analysis document and referenced in the Hazard Log.

Software Development Activities

The Aims of the software safety assessment during the Software Development phase are:

1) substantiating the initial hazard analyses, assessments and software function classifications by detailed analyse and
2) identifying new or additional hazards and hazardous failure modes of software.

The software related hazard analysis activities are phased, in line with the software development process, through Preliminary Design and Detailed Design to Code and Unit Test (see figure 6) and the results documented within each phase.
At each phase of the software development life-cycle the relevant requirements from the previous hazard analyses will be incorporated in the design and test requirements. The following steps will be performed:

i) Assign Risk Classification
ii) Analyse Risk Classification
iii) Justify the Risk Classification
iv) Analyse for New Hazards
v) record the Analysis

Hazard Tracking

There are two components which combine to give a complete tracking system enabling lowest level software items to be unambiguously related to highest level weapon system hazards. These are the Hazard Log to System Design Documentation link and the internal System Design Documentation tracking scheme (figure 6). Both are relevant to System Engineering activities but the latter pervades all stages of the System/Software life-cycle.
The mechanism will provide traceability between the Hazard Log and the functions specified in the System Functional Requirements Documents which will be established through cross-references. Each entry in the Hazard Log will identify the functional requirements relevant to the failures which can contribute to the hazard. Conversely all functions within the functional requirements which are associated with identified hazards will include the relevant, unique Hazard Log reference code in their descriptions. Compatibility of the two reference directions will be maintained. In addition both Hazard Log and function description will include the safety justification argument which establishes the relationship between the hazard severity categorisation and the criticality classification of the relevant functional requirement.
For subsequent design decomposition the tracking mechanism shall provide traceability between each level of the software documentation down to the detailed design.
Figure 6 shows the system life-cycle with the safety assessment activities which occur in parallel. The links between each life-cycle phase and the corresponding safety assessment hazard analysis indicates references to the design documentation by the hazard analysis and references to the justification statement from the design documentation. The links between design phases indicate the requirement traceability. All hazard are tracked within the design documentation from the System Functional Requirements Documents downwards.

References

1. MIL-STD-882C
"System Safety Program Requirements".
2. MIL-STD-1629A
"Procedures for Performing a Failure Mode Effects and Criticality Analysis".
3. NUREG-0492
"Fault Tree Handbook", January 1981.
4. 99/NT/T810D/930541
"Manuale di Affidabilita', Sicurezza, Manutenibilita' e Testabilità", Issue 2 May 1993.
5. DA-QED-11A
"Verifica della sicurezza nel progetto dei sistemi mediante system safety assessment", Rev. 1 September 1996.
6. DS-QSPT-H08-02
"Verifica della Sicurezza nella installazione dei Sistemi mediante Analisi Zonale", Issue 2 April 1993.
7. DS-QSPT-H08-03
"Check List per la verifica della sicurezza nel Progetto Installativo dei Sistemi", Issue 2 May 1993.

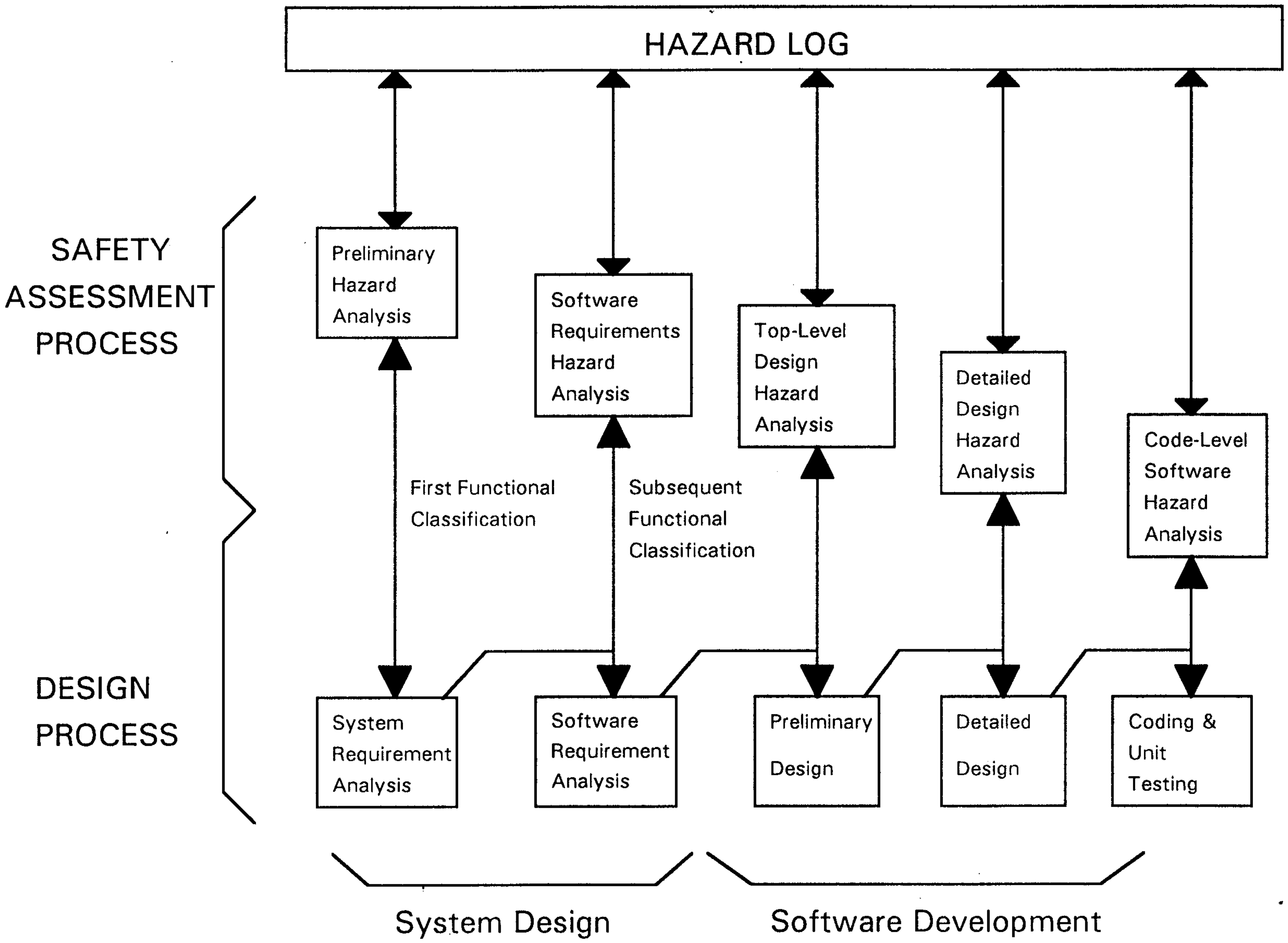

HAZARD LOG
SAFETY ASSESSMENT PROCESS
DESIGN PROCESS
Preliminary Hazard Analysis
Software Requirements Hazard Analysis
Top-Level Design Hazard Analysis
Detailed Design Hazard Analysis
Code-Level Software Hazard Analysis
First Functional Classification
Subsequent Functional Classification
System Requirement Analysis
Software Requirement Analysis
Preliminary Design
Detailed Design
Coding & Unit Testing
System Design
Software Development

Fig. 6 - Phasing of the Software Safety Assessment Process