FOURTEENTH EUROPEAN ROTORCRAFT FORUM

Paper No. 42

THE SAFETY ANALYSIS APPROACH FOR THE EH-101

Alan J. Wilson
Westland Helicopter Ltd
Yeovil, UK

Francesco Cortellini
Costruzioni Aeronautiche G. Agusta
Cascina Costa (VA), Italy

20-23 September, 1988
MILANO, ITALY

ASSOCIAZIONE INDUSTRIE AEROSPAZIALI
ASSOCIAZIONE ITALIANA DI AERONAUTICA ED ASTRONAUTICA

THE SAFETY ANALYSIS APPROACH FOR THE EH101

Alan J. Wilson
Westland Helicopter Ltd

Francesco Cortellini
Costruzioni Aeronautiche G. Agusta

1. Introduction

With the increase in technical complexity of modern aircraft, there has been an associated increase in the number of systems having safety-critical functions. As aircraft have grown more complicated, they have also required many more interactions between systems. Some of these interacting systems perform similar or associated functions, such that their interfaces are relatively easy to determine, but, increasingly, there are interactions between systems performing totally different functions.

It is the ability to detect and evaluate the potential hazard to the aircraft from the combinations of failures, sometimes across different system boundaries, that is the most important benefit of Safety Analysis as a technique.

This paper examines the background to the requirement for Safety Analysis as a discipline, and explains the logic behind the generation of the rotorcraft Safety Analysis requirements. Using these requirements as a basis, the paper then describes an idealised procedure for performing the Safety Analysis function, using a "top-down" analysis technique.

The technique described by the paper is one that has been agreed by the UK and Italian Airworthiness Authorities, and which is in use by Westland Helicopters and Agusta on the EH101 rotorcraft project.

2. Background

Up until relatively recently aircraft systems have been evaluated against requirements that were specific to that type of system, and which generally used the "single fault" criterion. Typically this approach is represented by requirements that say: "No failure shall result in .....", and the traditional method of showing compliance with this type of requirement is by means of a "bottom-up" Failure Modes and Effects Analysis (FMEA) where the consequences to the aircraft of the failure of each individual system component is evaluated.

As we know, however, airworthiness requirements do allow the occurrence of failures that do not have a critical effect. (Figure 1). Broadly speaking, the intention of the requirements is shown in this figure, and can be summarised as: "The more serious the fault, the less often it should occur". Obviously, this statement is a little imprecise, and this has led to a quantification of the requirements, as shown on the figure. The probability terms are now almost universally recognised in the aerospace industry.

Historically, the acceptable probabilities of occurrence for failures of a given criticality were arrived at by an examination of the rate of past accidents, and by factoring this probability to account for existing and/or hoped for improvements in safety of current technology. There is every reason to believe that further increases in safety will be expected and demanded by the Airworthiness Authorities.

3. The Requirements

The Basis of Certification for the EH101 helicopter includes FAR Part 29 to amendment 24, and BCAR Section G, as amended by BCAR Paper G780. Both of these sets of documents consequently contain similar Safety Objectives.

Far 29.1309 states that: "Failure Conditions which would prevent Continued Safe Flight and Landing must be Extremely Improbable" and: "Any other Failure Conditions which would reduce the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions must be Extremely Remote."

BCAR Paper G780 states that: "The design of the rotorcraft shall be such that, with the exception of the rotor and transmission systems, the probability of a Catastrophic effect from all systems causes is Extremely Remote."

For those who are unfamiliar with the term, a Failure Condition is "an adverse aircraft condition resulting from a single event, or a combination of related faults, failures, operating conditions or environments." The important point to understand is that it is not a failure, but an aircraft state following one or more failures.

Thus far, the basic requirements are no different to those our fixed-wing colleagues work to, apart from the recognition in BCAR Paper G780 that a rotorcraft's "extra systems" require special treatment.

The difficulty with these requirements is that it is not possible to say whether they have been met until all the systems on the rotorcraft have been collectively analysed. Moreover, if the requirements were not met, it might not be practical to determine which system should be modified to enable the requirements to be met, or it might be too late in the design programme to be able to make cost-effective and significant changes.

4. The History

Perhaps at this point it would be useful to examine the method by which the requirements evolved. (Figure 2).

In the beginning, the authorities examined their historical records and determined that the probability of a Catastrophe for large fixed-wing aircraft was approximately once in every million flying hours, or 1 x 10^{-6}/hour. (Fixed-wing aircraft were initially chosen to be examined because there was more information available on this class). By a closer examination of the data, it was noted that about 10% of the Catastrophes were caused by aircraft system failures.

Logically, then, for a newly-designed aircraft to be no worse than existing aircraft, the probability of an aircraft Catastrophe from all system causes should be not greater than 1 x 10^{-7}/hour. (Extremely Remote).

As previously mentioned, the difficulty with this type of requirement lies in making a positive statement that it has been met, until all the aircraft systems have been analysed collectively. For this reason, and also in order to provide a workable probability target, the authorities assumed, arbitrarily, that there were 100 potential aircraft Failure Conditions that could cause a Catastrophe. Remember the definition: A Failure Condition is an aircraft state resulting from a single failure or combination of failures.

The result, if the allowable risk is apportioned equally amongst the Failure Conditions, is a probability for a Catastrophic Failure Condition that should be no greater than 1 x 10^{-9}/hour (Extremely Improbable).

The view was taken that, for rotorcraft, target probabilities should be no different to fixed-wing targets. However, it was soon recognised that the attainment of fixed-wing levels of safety was limited by the state of the art on the design of a rotorcraft's "extra systems", principally rotors and transmissions. BCAR Paper G780 recognises that the attainment of probability levels less than Very Remote (numerically from 1 x 10^{-6}/hour to 1 x 10^{-7}/hour) for rotor and transmission systems is limited. The Safety Objective for these systems is such that the probability of a rotorcraft Catastrophe from all systems causes is required to be no grater than 1 x 10^{-6}/hour.

It should be noted that FAA regulations also recognise the problems in applying fixed-wing safety objectives to these systems, and imply that 29.1309 does not apply to them (AC29-2A and the response to proposal 2-58 in the discussion papers for amendment 29-24 to FAR Part 29 refer).

For all systems other than rotors and transmission the collective safety objective of Extremely Remote (or 1 x 10^{-7}/hour) from all system causes will be assumed to have been achieved by achieving an objective of

Extremely Improbable (or 1 x 10^{-9}/hour) for each identified Catastrophic Failure Condition.

5. The Practicalities (Figure 3)

Now we must consider the practical methods by which compliance with the requirements can be demonstrated. This is achieved through what is essentially a three-stage procedure. The first step identifies the Failure Conditions associated with a system, and assesses their criticality. The second step assesses the likelihood of occurrence of the more critical Failure Conditions, and also identifies the failure modes leading to these Failure Conditions. The third step is, of course, presenting the results of all this activity to the Airworthiness Authorities.

6. The Hazard Assessment

The first step is intended to be carried out at an early stage in the design process, when the system architecture or initial design has been determined, but when the detailed design has not yet commenced. This is in contrast to earlier design practice, when FMEA's were employed to check out the system design, but, of necessity, at a later stage in the design process. For this reason, the first stage of Safety Analysis uses a "top down" approach, and is known as a Hazard Assessment. The important thing to realise about a Hazard Assessment is that it is not an FMEA, and is in fact a much less detailed task. The reason for this is that a Hazard Assessment does not consider individual components that go to make up a system, but rather deals with the Functions of the system.

In order to carry out a Hazard Assessment properly, one must first acquire sufficient knowledge of the system being analysed to allow the following data to be determined:

(i) The boundaries of the system

(ii) Its interfaces with other systems

(iii) Its interfaces with the crew

(iv) All required inputs to the system

(v) The intended output functions of the system

(vi) All other incidental functions

It should be noted that the performance parameters, limits and departures that constitute failure need to be determined. The parameters may well be the allowable limits about a mean, outside of which the system would not function satisfactorily, and would therefore constitute a failure. In addition, the environments within which the system functions need to be

established, particularly where it passes from one environment to another. (For example: where a fuel line, immersed in fuel inside a fuel tank passed through a tank wall into a dry environment).

The Hazard Assessment itself must then determine the consequential effect on the rotorcraft (or Failure Condition) of a failure of each function, taking into account the various operational phases of the rotorcraft and the effect of the failure on other systems, including other relevant adverse events.

Where a Failure Condition resulting from a Functional Failure of a system can be made worse by additional Functional Failures or adverse events, either from within the system under examination or externally from a separate system, then this combination must be considered.

The Hazard Assessment procedure for a system (Figure 4) can thus be summarised as:

What does it do?
How can it stop doing it and how can it get worse?
When's the most awkward time it can do so?
Will it affect anything else?
What happens to the aircraft?
How serious is it?

The last two points, of course, not only identify those areas of a system that are of interest to a designer and an Airworthiness Authority Surveyor, but also identify Safety Objectives for various parts of a system by reference to the Criticality/ Probability acceptability criteria (ref Figure 1).

It should be noted that the Hazard Assessment does not examine the probability of occurrence of a Failure Condition: this is not necessary at this point, and will only need to be covered during the later detailed analysis.

It is important to note that the consequential effect on the rotorcraft of Functional Failures and adverse events may not be capable of being determined at an individual system level. It is therefore essential that adequate coordination between the different systems takes place. (Figure 5)

This task is accomplished by the analyst of the system, in co-operation, when appropriate, with the system analysts of other interrelated systems. An overall perspective should be maintained by an arbitrator to ensure that no gaps are left by the individual system Hazard Assessments.

For a comprehensive understanding of the processes involved in the Hazard Assessment, a tabular format or presentation has been adopted by Westland Helicopters and Agusta and serves as a summary. (Figure 6)

7. The Detailed Analysis

Once the Safety-critical areas have been identified in the Hazard Assessment, a detailed investigation of these areas must be made to discover whether the probability of occurrence of any Failure Conditions more severe than Minor is acceptable. To decide whether a probability of a Failure Condition is acceptable, we use the Safety Objectives determined by reference to the criteria given in the requirements (Figure 7).

A principal objective in applying such techniques is to ensure that the Safety Analysis has been carried out logically and facilitates the understanding by other persons not directly involved in the study. In particular the design should be assessed for the vulnerability to:

Common Cause Failures
Cascade Failures
Maintenance Errors
Flight Crew Errors
Hidden Faults
Faults in related systems
Environmental Effects
Lightning Effects.

For systems for which relevant datum experience exists from similar systems on other rotorcraft the relevant data must be made available to the Authorities including a statement of the extent of similarity between the two systems. In service data should also be available to substantiate the compliance with the safety objectives.

During the consideration of flight crew errors, the consequences of likely incorrect actions must be considered for each system, for the following two categories:

(i) Erroneous crew action when no system malfunction has occurred.

(ii) Erroneous or omitted corrective action following a malfunction of the system.

Possible maintenance errors following maintenance tests - the repercussions on the system of possible errors following maintenance tests such as: reset omissions, test selectors left in test position, etc should also be investigated.

The methods by which detailed investigation of a system can be carried out vary considerably from FMEA's to Fault Trees to Dependance Diagrams to Fault Hazard Analyses. However, the Civil Authorities preferred method is by the use of logic diagrams, in other words by Fault Trees or Dependance Diagrams as they illustrate the original analyst's thought processes in a clear and concise manner that can be relatively easily interpreted and checked at a later date.

The Fault Tree approach (Figure 8) is most appropriate when the system being analysed is redundant, has functions dependent on several other systems or has been found to have dependent Causal Failures (Common Mode or Common Element).

These Fault Trees are constructed from the top event (the Failure Condition) downwards, to determine what contributory events are necessary to bring about the top event.

The contributory events are further broken down and this process is continued until the undesired event is expressed as a combination of basic events or failures (this is the greatest advantage offered by this technique compared with the FMEA).

The probability of these basic events or failures can then be combined, in accordance with the Fault Tree logic, to calculate the overall probability of the top event.

BCAR Paper No. G778 states that: " It is recognised that the probability of prime failures of certain transmission and rotor system single elements (eg. shafts, spindles, etc.) cannot be sensibly estimated in numerical terms. Where the failure of such elements is likely to result in Hazardous or worse effects, reliance must be placed on their meeting requirements aimed at providing high integrity, such as ground endurance tests, overtorque and overspeed tests, fatigue life substantiations, etc, and where this is so it should be stated in the Safety Assessment".

If a precise numerical probability value for a particular failure is not available, then approximate or estimated values based on experience and engineering judgement can be used to enable the assessment to be made.

8. Presenting the results of the Safety Analysis

The results of all this activity are summarised and presented to the Civil Authorities by means of the Safety Assessment Report.

Typically, the document should contain the following: (Figure 9)

(i) A description of the system (including functional block diagrams, schematics, safety features, warnings, inputs and outputs, etc).
(ii) Derivations of any failure rates quoted (supporting data sources, etc). Note: arguments claiming similarity with existing certificated systems should be quoted here.
(iii) A statement of conformity with the requirements (which should summarise the analysis carried out)
(iv) A listing of safety checks and inspections required to meet the Safety Objectives

It is important to note that the objective of the Safety Assessment Report is to provide the Airworthiness Authorities with the end results of the analysis, and with sufficient information to enable them to know which individual area of detailed analysis to ask for to follow up any areas of specific interest.

9. Conclusions

In conclusion, it should be pointed out that the major advantage of Safety Analysis is that it is the only design safety evaluation technique that looks upon safety in a co-ordinated and integrated manner. That is to say that combinations of failures from different systems can be assessed in a systematic manner in order to assure that there are no devious Catastrophic combinations. This is something that cannot be achieved with any degree of confidence or repeatability using other methods.

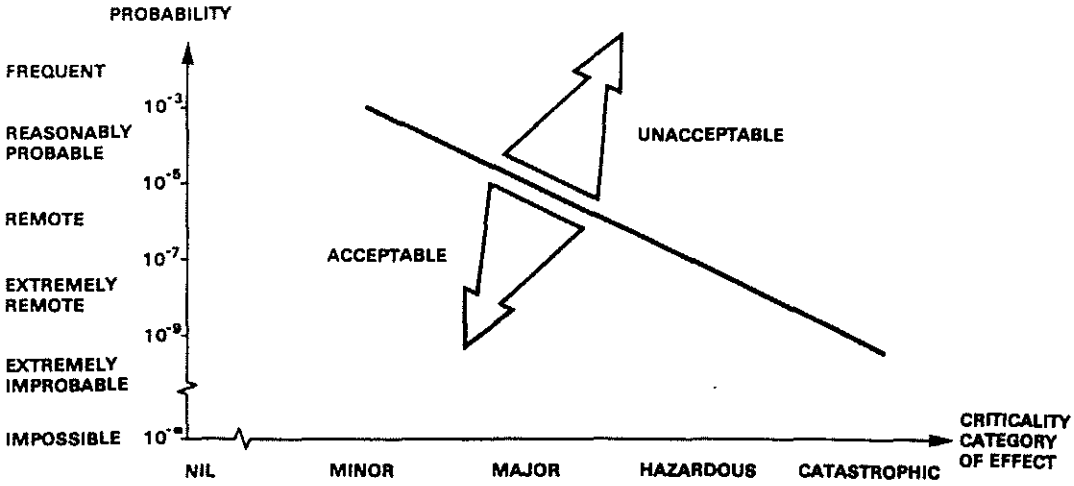

FIGURE 1 - Criteria for acceptability of occurrence of failures

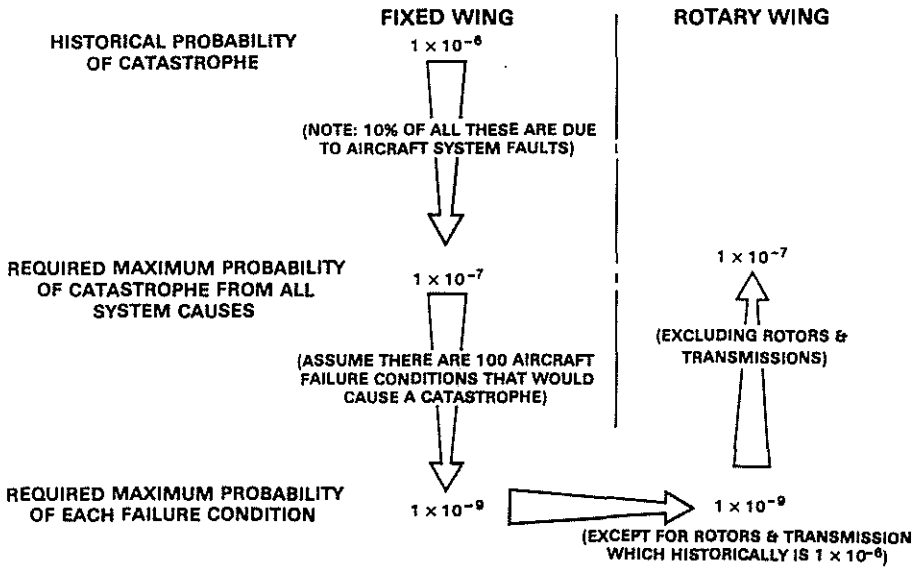

FIGURE 2 - Derivation of the existing requirements

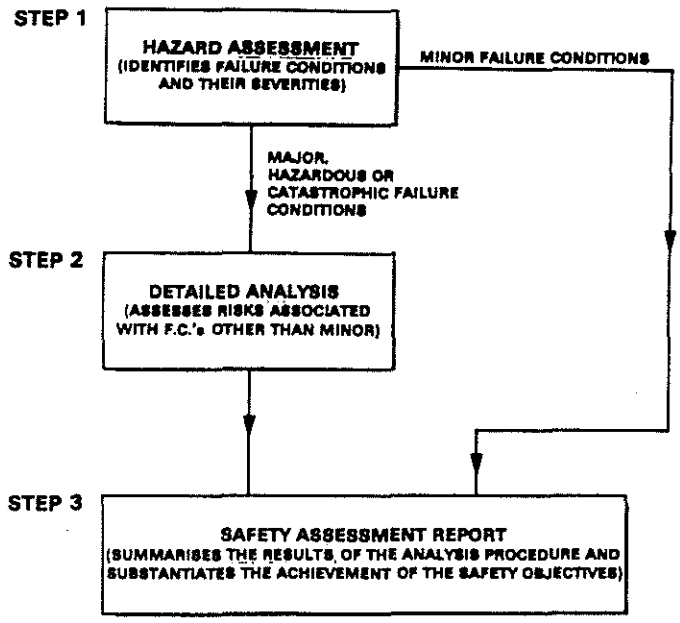

FIGURE 3 - The Safety Analysis procedure

IDENTIFY FOR EACH SYSTEM:

1. **ITS FUNCTIONS**
   (What jobs does it do?)
2. **ITS FUNCTIONAL FAILURES**
   (How does it stop doing them & how can it get worse?)
3. **THE CRITICAL OPERATIONAL PHASE**
   (When's the failure most awkward?)
4. **THE EFFECT ON OTHER SYSTEMS**
   (Does it affect anything else?)
5. **THE ROTORCRAFT FAILURE CONDITIONS**
   (What state is the helicopter left in?)
6. **THE SEVERITY OF THE FAILURE CONDITIONS**
   (How serious is it?)

DESIRED RESULT OF THE HAZARD ASSESSMENT:

'TO IDENTIFY AREAS OF A SYSTEM THAT NEED DETAILED ANALYSIS'

FIGURE 4 - The Hazard Assessment procedure

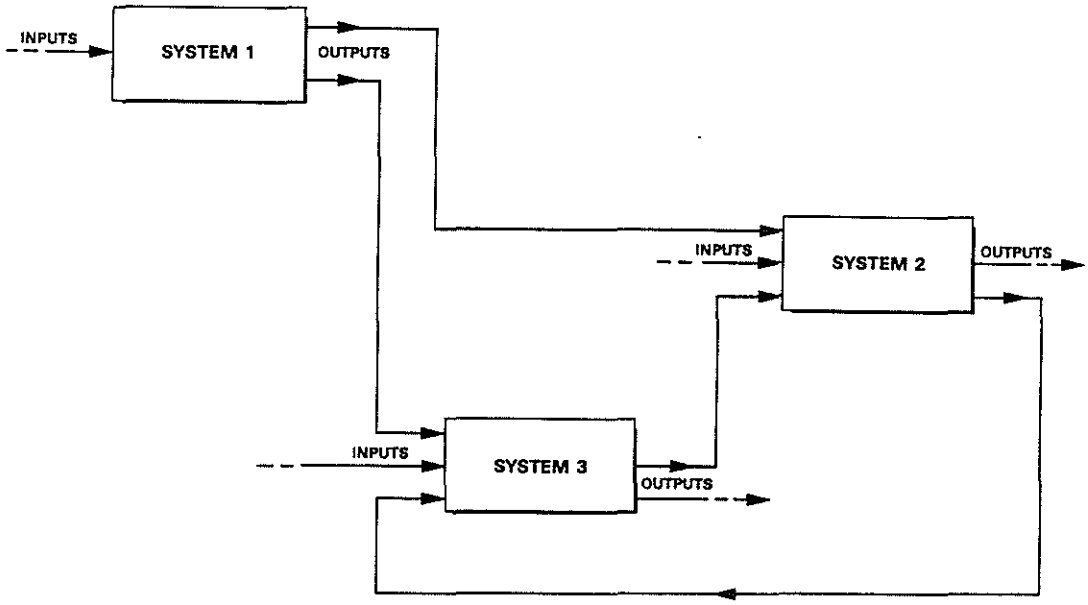

FIGURE 5 - System interfaces

Aircraft:
System:
Reference Drawing:

SUMMARY OF FAILURE CONDITIONS
(HAZARD ASSESSMENT)

Date
Sheet of
Compiled by:

Function	Functional Failure	Most Critical Operational Phase	Effect of Functional Failure on other systems	Failure Condition	Failure Condition Classification	Remarks

FIGURE 6 - Hazard Assessment tabular format

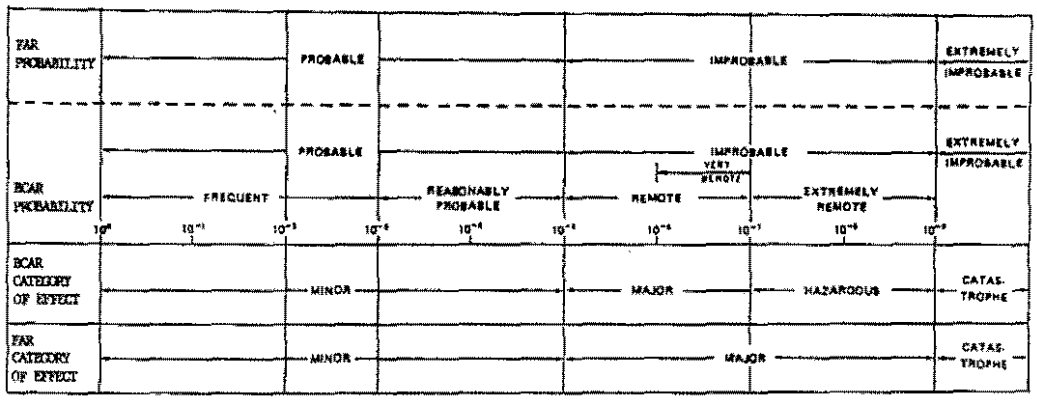

FIGURE 7 - Relationship between probability and severity of effects

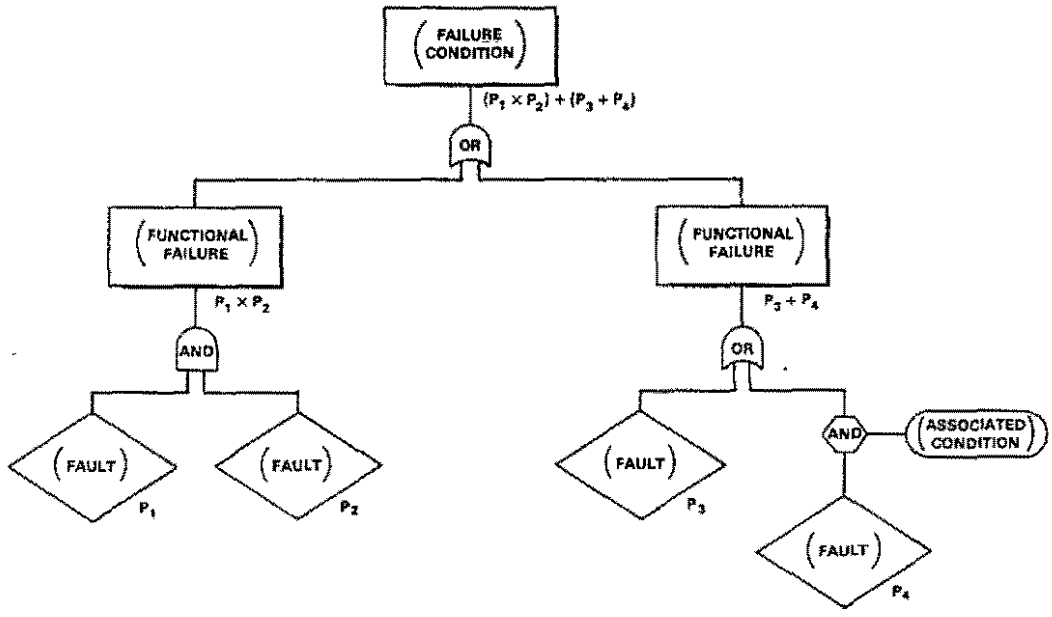

FIGURE 8 - Example of Fault Tree

SYSTEM DESCRIPTION

- includes: physical description,
  system schematics,
  functional block diagrams,
  input/output lists,
  safety features,
  warnings etc.

FAILURE RATE DERIVATIONS

- origins of quoted failure rates to be explained. Cases for similarity to existing systems to be explained.

STATEMENT OF CONFORMITY TO THE REQUIREMENTS

- will include a summary of the analyses carried out and references to the details.

SAFETY CHECKS AND INSPECTIONS

- a list of those checks/inspections required to meet the Safety Objectives.

FIGURE 9 - Typical Contents of The Safety Assessment Report