Book 1 (2006)

(add picture of cover)

(link to Elsevier's website (The Publisher where books can be bought)

Introduction

(as per current website)

Layout

(as per current website)

Supporting data for each chapter

- Chapter 1:
  (as per the current website, but not the purchasing sentence)
- Chapter 2:
  (as per the current website, but not the purchasing sentence)
- Chapter 3:
  (as per the current website, but not the purchasing sentence)
- Chapter 4:
  (as per the current website, but not the purchasing sentence)
- Chapter 5: GOAL/FAILURE BASED APPROACH
  In absence of clearly defined goals, we become strangely loyal to performing daily acts of trivia.
  Introduction
  An acceptable level of safety for aviation is normally defined in terms of an acceptable aircraft accident rate. There are two primary causes of aircraft accidents:
  - operational (such as pilot error, weather and operating procedures) an
  - technical (such as design errors, manufacturing errors, maintenance errors and part failures).

  Historical accident rates indicate that technical cause factors will account for 40 to 50 per cent of the total accidents. When certifying a new (or modified) system, designers concentrate on the technical integrity of the system which has been designed around an operational requirement. Now, for a number of years, aeroplane systems were evaluated to specific requirements, to the "single fault" criterion, or to the "fail-safe design" concept (see Chapter 7).
  As later-generation aeroplanes were developed, more safety-critical functions were required to be performed. This generally resulted in an increase in the complexity of the systems designed to perform these functions. The likely hazards to the aeroplane and its occupants that could arise in the event of loss of one or more functions (provided by a system or that system's malfunction) had to be considered, as also did the potential interaction between systems performing different functions.
  The application of the Fail-Safe concept thus had to be supplemented by some sort of safety target (i.e. goal) against which the integrity of the system architecture could be evaluated

  Useful links not included in the text
  You may find the following additional sites of relevance when reading the above chapter:
  - TBD
  - TBD

- Chapter 6: HAZARDS
  Imagine a world with no hypothetical situations…..

Introduction:

Safety is the freedom from accidents. Accidents are caused by hazards. But what exactly do we understand the term "hazard" to mean?

The term "hazard" goes by many (often confusing) definitions

Note that the presence of a hazard does not make an accident inevitable. From the discussions in this chapter, it is proposed that an all-encompassing definition might thus rather be:

"A hazard is a prerequisite condition that can develop into an accident through a sequence of failures, events and actions in the process of meeting an objective".

There is a causal chain from causes to hazards to accidents. Rhys (2002, page 4) defines an accident as: "*an unintended event or sequence of events which causes death, injury, environmental damage or material damage*". The accident is the undesired outcome, rather than the initiating event or any intermediate state or hazard.

Useful links not included in the text

You may find the following additional sites of relevance when reading the above chapter:

- TBD
- TBD

- Chapter 7: THE FAIL-SAFE DIMENSION

The best car safety device is a rear-view mirror with a cop in it.

- Dudley Moore (1935 - 2002)

Introduction:

There are many reasons why systems may fail.

The first line of defence against hazardous failure conditions is avoidance in which design and management techniques should be applied to minimise the likelihood of faults arising from random or systemic causes (see Chapter 6).

The second line of defence is based on the provision of fault tolerance as a means of dynamic protection during system operation. Possible approaches include:

- Fault masking, where the system or component is designed to survive potential failures with full functionality,
- Graceful degradation (sometimes referred to as fail-soft), where the system or component is designed so that in the event of a failure its operation will be maintained but with some loss of functionality,
- Fail-safe, where in the event of a failure, the system or component automatically reverts to one of a small set of states known to be safe, and thereafter operates in a highly restricted mode. This may involve complete loss of functionality, or reverting to back-up/redundant features.

- Chapter 8: THE SYSTEM SAFETY ASSESSMENT

"Life can only be understood backwards, but it must be lived forwards"

- Soren Kierkegaard (1813 - 1855)

Introduction:

Lloyd and Tye (1995) recall that the airworthiness requirements (e.g. BCAR and FAR) of the mid 20th century "were devised to suit the circumstances. Separate sets of requirements were stated for each type of system and they dealt with the engineering detail intended to secure sufficient reliability". Where the system was such that its failure could result in serious hazard, the degree of redundancy (i.e. multiplication of the primary systems or provision of emergency systems) was stipulated. Compliance was generally shown by some sort of an FMEA .

For simple, self-contained systems this approach had its merits.

However, systems rapidly became more complex. Complex systems have a considerable amount of interfaces and cross/inter-connections between the electrical, avionic, hydraulic and mechanical systems . In addition, there are essential interfaces with the pilot, maintenance personnel and flight performance of the aircraft. The aircraft designer is thus faced not only with the analysis of each individual system independently, but needs to consider how these systems act in concert with other systems.

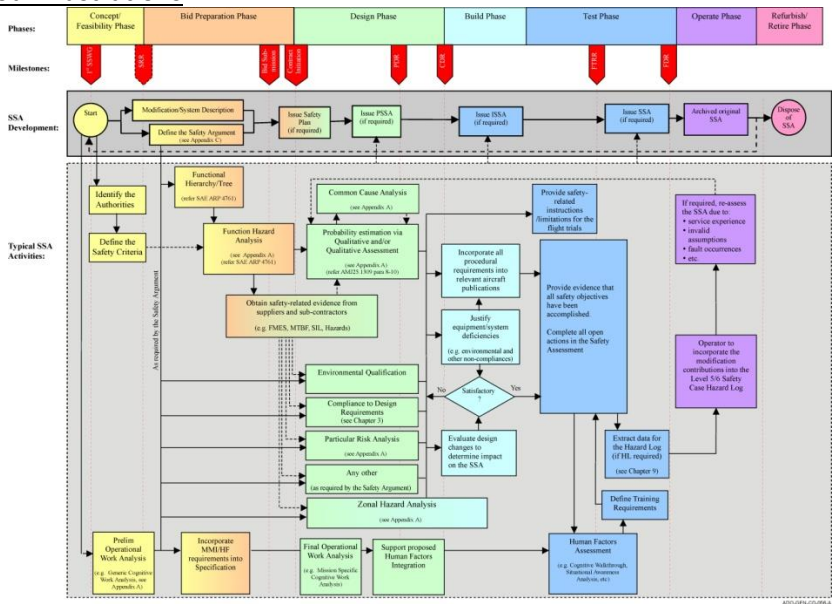
Airworthiness Authorities could thus not continue to issue detailed engineering requirements for each new application. Firstly, this would lead to a mountain of regulatory requirements and, secondly, this approach would inhibit innovation by leading designers into sub-optimum solutions.

It therefore became necessary to have some basic objective requirement (see Chapter 5 paragraph 2) related to an acceptable level of safety, which could be applied to the Safety Certification and Release To Service (RTS) of any system or function.
This new approach required that, for Safety Certification, the designers conduct a thorough assessment of potential failures and evaluate the degree of hazard inherent in the effect of failures. With complex critical systems and functions the designer has not only to consider the effect of single failures, but also the effects of possible multiple failures – particularly if some of these failures are passive (see Chapter 6). The designers need to show that there is an inverse relationship (see Chapter 5) between the probability of occurrence and the degree of hazard inherent in its effect.

The designers also need to consider whether the design is such that it can lead unnecessarily to errors during manufacture, maintenance or operation by the crew. Furthermore, the designer needs to consider the environment that the systems would be exposed to, which could involve large variations in atmospheric temperature, pressure, acceleration (e.g. due to gusts), vibration, and other hostile events such as lightning strikes and icing.

The vehicle to report this demonstration, for the purposes of Safety Certification and Release To Service (RTS), became known as the System Safety Assessment (SSA).

Colour Illustrations



- Chapter 9: THE SAFETY/RISK CASE

"The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come" Confucius (551-479BC)

Introduction:

The development of the Safety Case as an European approach to safety management can be traced though a series of major accidents (which are explored in this chapter)
Until quite recently only the people directly involved would have been held to blame for an accident. Now it is recognised that safety is everybody's concern. Key lessons learned for these disasters included :

- Engineering: Visibility is needed of decisions/assumptions that effect safety. However, it is also recognised that engineering alone cannot guarantee safety.
- Operations: Systems evolve, as do their operational application. Procedures and maintenance do affect safety. Frequent training can improve effectiveness.
- Management: Are responsible for the development of a safety culture in their organisations by defining safety policies and allocating resources in the development thereof.

An approach was thus called for to supplement the regulatory shortcomings, and this was termed the Safety Case. The major push in the development of the Safety Case concept was the tri-partite (i.e. Government, Industry and Unions) Advisory Committee on Major Hazards (ACMH), which was formed after the Flixborough disaster. The most important and far reaching of their recommendations was that owners of major hazardous sites/facilities should develop a living Safety Case to identify and control hazards so as to prevent accidents.

- Chapter 10: NUMERICAL PROBABILISTIC APPROACH

Do not expect to arrive at certainty in every subject which you pursue. There are a hundred things wherein we mortals must be content with probability, where our best light and reasoning will reach no farther. - Isaac Watts

Introduction:

Amongst various requirements, the certification of an aircraft requires proof that any single failure, or reasonable sequence of failures, likely to lead to a catastrophe has a sufficiently low probability of occurrence. This has led (refer Chapter 4) to the general principle that an inverse relationship should exist between the probability of loss of function(s) or malfunction(s) (leading to a serious Failure Condition) and the degree of hazard to the aeroplane and its occupants arising therefrom.

It should go without saying that a low probability of occurrence equates with a high level of safety

Colour Illustrations

- Chapter 11: SAFETY MANAGEMENT SYSTEM

"Captain Lavendar of the Hussars, a balloon observer, unfortunately allowed the spike of his full-dress helmet to impinge against the envelope of his balloon. There was a violent explosion and the balloon carried out a series of fantastic and uncontrollable manoeuvres, whilst rapidly emptying itself of gas. The pilot was thrown clear and escaped injury as he was lucky enough to land on his helmet.
Remarks: This pilot was flying in full-dress uniform because he was the Officer of the Day. In consequence it has been recommended that pilots will not fly during periods of duty as

Officer of the Day. Captain Lavendar has subsequently requested an exchange posting to the Patroville Alps, a well known muleunit of the Basques." **- No2 Brief from Daedalian Foundation Newsletter (Dec 1917)**

Introduction:
A number of factors and inherent dangers exist that may influence the achievement of an acceptable level of system safety:

- Aircraft are very complex and highly integrated with a multitude of critical systems involving interfaces between hardware, software and operators. These configurations and interfaces are not stagnant and continue to evolve, introducing new situations and conditions;
- Aircraft, especially military, are required to operate in very demanding environments. Actual testing under realistic environmental conditions is not possible in all cases;
- weight restrictions require aircraft designs to be optimised with minimum margins of safety;
- redundancy is often considered an unaffordable luxury, especially for military aircraft types;
- design restrictions often place limitations on safety measures;
- during service life, the operational usage might change beyond that assumed in the original design and definition of the maintenance schedule;
- despite testing, unexpected hazardous conditions (such as flutter and stores separation problems) may occur;
- cost-cutting measures (e.g. extended maintenance intervals, less training, etc)
- other imperatives, such as mission accomplishment; available financial resources and schedule constraints may at times conflict with the technical airworthiness rules and standards.

As a result personnel associated with the design, manufacture, maintenance and material support of aeronautical products may be exposed to an evolving, ever-changing, level of risk.
Until quite recently only the people directly involved would have been held to blame for an accident. Now it is recognised that safety is everybody's concern. However, whilst individuals are responsible for their own actions, only managers have the authority and resources to correct the attitudes and organisational deficiencies which commonly cause accidents. An accident is an indication of a failure on the part of management. What is required is an ordered approach to manage safety throughout the system's lifecycle. This ordered approach is facilitated by the Safety Management System (SMS). This chapter provides some guidance on the philosophy and approach to a Safety Management System.

- Chapter 12: CONCLUDING OBSERVATIONS

" *Accidents are not due to lack of knowledge, but failure to use the knowledge we have*"
- Trevor Kletz

Introduction:
Aircraft flight has been transformed from an adventurous activity enjoyed by a selected few to a stable mass-market service industry which is largely taken for granted…… until things go wrong. The industry is then dominated by public perception of risk and the social amplification thereof. Accidents resulting in hull loss often result in fatalities and are almost always treated to extensive coverage in the national, if not world-wide, press. The aircraft industry is set to become more complex, the skies more crowded, and the budgetary

pressure will increase. A new impetus must be found in pro-safety activity if the high confidence of the public is to be maintained, let alone improved, through the impending doubling of traffic by 2020 and beyond. It will not be sufficient to increase the reliability of technical systems alone.