Book 1 (2016)

(add picture of cover)

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

Introduction

This book follows on from the author's previous work[1], which set the broad scene of the regulatory environment, the approach, tools and techniques used in the assessment of aircraft system safety. In this book the author presents a practical user guide (for both the novice safety practitioner and their managers) in the more specific area of conducting and managing SSA's to satisfy the requirements of FAR/CS25.1309. This book is written to supplement (not substitute) the content of advisory material (e.g. AMC25.1309) or their principal supporting reference standards (i.e. SAE ARP 4761, SAE ARP 4754A, RTCA/DO-178, RTCA/DO-154). In summary, this book strives to amalgamate these documents into a consolidated strategy, supported by simple process maps to aid the user in their understanding and subsequently to allow the more experienced to optimise their efficient use.

Chapter 1 provides an introduction to the SSA concept and overall approach. A Case Study is defined therein, for which a safety strategy is derived in Chapter 2 to support the Safety Programme Plan. Chapters 3 to 11 then employ this strategy (see Figure 2.5) to explore the theory of the most commonly used safety assessment techniques required to execute the Safety Assessment. Each chapter then concludes by applying the theory to the Case Study. This Case Study thus provides continuity throughout each chapter, and enables the reader to bring the Safety Assessment together in a logical and efficient manner. The three last chapters of this book are of specific interest to those wishing to understand some of the potentially more esoteric disciplines used in assessing system safety:

- Chapter 9 addresses the systematic causes of failures or unanticipated system behaviours and provides guidance on Development Assurance Levels (DALs) to the Safety Assessor who may not be expert in the fields of software(S/W) or complex hardware (H/W).
- Chapter 10 addresses the assessment of the ability flight crew to cope with unsafe system failure conditions identified during the SSA process. As with Chapter 9, this chapter is written to assist the Safety Assessor in understanding system approaches to minimising crew error, the role of the operator, and how or when specialist Human Factors (HF) input and engagement might be required.
- Chapter 11 looks beyond the "Certification Phase" and provides a high level discussion of the SSA interface with the Safety Case and/or Safety Management System (SMS) in the "Continuing Airworthiness Phase". Note: The scope of this chapter is restricted to the Initial and Continued Airworthiness obligations of the relevant approval holders only, and not specific Continuing Airworthiness activities.

Layout

(as per current website)

Supporting data for each chapter

- **<u>Chapter 1:INTRODUCTION</u>**

  "If we slide into one of those rare moments of military honesty, we realize that the technical demands of modern warfare are so complex a considerable percentage of our material is bound to malfunction even before it is deployed against a foe. We no longer

[1] Kritzinger, D.E. *Aircraft System Safety: Military and Civil Aeronautical Applications*, Woodhead Publishing Ltd, 2006

waste manpower by carrying the flag into battle. Instead we need battalions of electronic engineers to keep the terrible machinery grinding."- Ernest K. Gann, The Black Watch

Synopses

When certifying a new (or modified) system, designers conduct a thorough assessment of potential failures to show that there is an inverse relationship between the probability of occurrence and the severity of consequence inherent in its effect [AMC25.1309]. The designers also consider whether the design is such that it can lead unnecessarily to errors (during manufacture, maintenance or operation) or whether the system is vulnerable to foreseeable variations in the operating environment. The vehicle to report this assessment is commonly known as the System Safety Assessment and it needs to consider ransom failure of system components as well as systematic errors which might be introduced during the development process.

- Chapter 2: SAFETY ASSESSMENT STRATEGY (WITH GOAL STRUCTURING NOTATION)
  "Strategy is a style of thinking, a conscious and deliberate process, an intensive implementation system, the science of insuring future success" - P. Johnson

  Synopses

  Many traditionally compiled Safety Assessments/Cases are inadequately planned resulting in a report which is disjointed, often poorly expressed, and generally not easily understood by the developer and any stakeholders who have to subsequently read or use it. Many readers of a comprehensive report are often overwhelmed by the bulk of effort, but left with a lingering feeling of "what has been missed?" Goal Structuring Notation (GSN) provides a useful tool to plan and scope a safety assessment strategy.

  In this chapter we define a simple process model of the GSN process and then apply this to define a safety assessment strategy for the case study defined in Chapter 1. This strategy is then executed in each of the remaining chapters of this book.

- Chapter 3: FUNCTIONAL HAZARD ANALSYSES
  "Our will is a function regulated by reflection; hence it is dependent on the quality of that reflection." - author unknown

  Synopses

  Every system has a function to achieve. When that function goes wrong (or is absent), then it may have a negative effect on aircraft safety. The Functional Hazard Analysis does two things: Before the system architecture is defined, the FHA systematically explores each function failure mode in the required solution. Upon finally defining the system architecture the FHA is updated to prove the functional integrity of the system under consideration.

  In this chapter we define a simple process model of the FHA process and then apply this model to the case study defined in Chapter 1.

- Chapter 4: FAULT TREE ANALYSIS

  "The greatest of faults, I should say, is to be conscious of none

  - Thomas Carlyle (1795 – 1881

  Synopses

  Any sufficiently complex system is subject to failure as a result of one or more subsystems failing. The aim of the FTA is to use deductive logic to understand all the underlying causes of a particular failure so that the likelihood of failure can be reduced through improved system design.

  In this chapter we define a simple process model of the FTA process and then apply this model to the case study defined in Chapter 1.

- Chapter 5: FAILURE MODE & EFFECTS ANALYSIS

  "Failure is the rule rather than the exception, and every failure contains information

  - Steve Wozniak (Apple co-founder)

  Synopses

  An FMEA is a systematic "bottom-up" method of (a) Identifying single failure modes and failure probabilities of a system, item, function, or piece-part (i.e. smallest individual part or component); (b) Determining the effects of this failure mode on the next higher level of the design (if available to the assessor, i.e. an LRU supplier will not know how much redundancy the system integrator is going to build into his system); and (c) Classifying failure modes according to the worst case severity of the end effect

  In this chapter we define a simple process model of the FMEA process and then apply this model to the case study defined in Chapter 1.

- Chapter 6: COMMON MODE ANALASIS

  "A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools".

  - Douglas Adams (1952-2001)

  Synopses

  The acceptance of a qualitative or quantitative failure probability declaration is often based on the assumption that failures are independent. Although most critical systems employ redundancy techniques, it will be found on examination that many of them have a single cause" that could cause multiple failures. In most cases this single element is readily obvious, but this is not always the case. The Common Mode Analysis (CMA) purposefully looks for common cause failure in the system architecture (e.g. threats to full redundancy) as well as how that architecture is to be installed, operated and maintained.

In this chapter we define a simple process model of the CMA process and then apply this model to the case study defined in Chapter 1.

- Chapter 7: PARTICULAR RISK ANALYSIS

  "There is no reason to fly through a thunderstorm in peacetime"

  - Sign over squadron ops desk, Davis-Monthan AFB, AZ, 1970

  Synopses

  A Safety Analysis on a system cannot be complete without considering the robustness of that system to external events which that system will reasonably be exposed to. The PRA considers any events outside the immediate boundaries of the system which could cause system failures and impact aircraft airworthiness. Once identified, each particular event is subject to a specific study to examine and document its effect on the system and the aircraft.

  In this chapter we define a simple process model of the PRA process and then apply this model to the case study defined in Chapter 1.

- Chapter 8: ZONAL SAFETY ANALYSIS

  "There is no reason to fly through a thunderstorm in peacetime"

  - Sign over squadron ops desk, Davis-Monthan AFB, AZ, 1970

  Synopses

  The physical installation of systems, in terms of the act and the location, could significantly impair the assumed independence between systems, items and components. The Zonal Safety Analysis considers the proximity aspects of individual systems/items and the potential for mutual influence between several systems/items installed in close proximity. It ensures that independence in physical location can either be assured or, if not possible, deemed acceptable by incorporation into the probability declaration.

  In this chapter we define a simple process model of the ZSA process and then apply this model to the case study defined in Chapter 1.

- Chapter9: DEVELOPMENT ASSURANCE

  ""A program which does not work is undoubtedly wrong; but a program which does work is not necessarily right." - Michael A. Jackson [Principles of Program Design, Academic Press, 1975]

  Synopses

  Development Assurance is a methodology which provides confidence in the behaviours and properties of a system (or item). It is based on setting objectives and configuration control requirements for the life-cycle evidence (product and process). It also provides a process for establishing that the evidence satisfies the applicable objectives. The aim of this chapter is to describe the purpose and role of Development Assurance, and outline the general approach to satisfying the allocated FDAL or IDAL..

In this chapter we define a simple process model of how to apply and integrate the DAL logic of SAE ARP4754A, RTCA/Do-160C and RTCA/DO-254. We then apply this logic to the case study defined in Chapter 1, and a key enabler is the following spreadsheet:

- TBD link to spreadheet

- Chapter 10: CREW ERRORS IN THE SAFETY ASSESSMENT
  To err is human [Marcus Tullius Cicero,106-43BC]
  – and pilots, in spite of pretences, are only human

  Synopses

  Human errors continue to dominate as a contributing factor in aircraft accidents. In the design of systems it is thus important that we understand how operator errors (i.e. Incorrect actions or incorrect responses) are made and what can be done to prevent (or reduce the probability) of their occurrence. In this chapter we provide an overview of how errors are made and how their probability and/or impact can be reduced. A simple methodology is then proposed to consider flight crew error as another failure mode in the System Safety Assessment process.

  In this chapter we define a simple process model to mitigate crew errors and then apply this model to the case study defined in Chapter 1.

  Note that the scope of this chapter:

  - is limited to considering flight crew errors/mistakes only for the purposes of completing a typical CS25.1309 Safety Assessment.
  - does not extend to the full remit of Human Factors and excludes proving compliance to CS/FAR25.1302.
  - is restricted to unintentional errors only and does not extend to intentional errors or sabotage.
  - does not include system resilience provided by the fail safe design philosophy. See Chapter 7 in Kritzinger (2006) for more information on this

- Chapter 10: CONTINUING SAFETY
  "Serendipity should not be ignored" – Confucius
  .....but neither should vicissitudes

  Synopses

  Safety Assessment activities do not stop post certification. There needs to be a proper interchange of information between the aircraft manufacturer and operators, so that modes of failure and critical failure rates which occur in service can be checked against the predictions, unexpected failure modes or other system vulnerabilities can be assesses and mitigated (via re-design or via Service Bulletin action) and/or alterations can be made to

check and maintenance to support Continuing Airworthiness. The data and design familiarisation obtained during the certification process is critical to the success of the continuing airworthiness function. It enables the continual re-assessment to be made, action to be taken to ensure the continued fitness to fly of the aircraft, and feedback through to the original maintenance and design standards.

The aim of this chapter is to look beyond the Initial Airworthiness Phase (leading up to certification) and discuss the SSA interface with the Safety Management System (SMS) in the Continuing Airworthiness Phase.

)