Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 17 (2011) 358 – 368

Procedia Engineering

www.elsevier.com/locate/procedia

The 2nd International Symposium on Aircraft Airworthiness (ISAA 2011)

Do safety cases have a role in aircraft certification?

SUN Linling[a]*, ZHANG Wenjin[b], Tim KELLY[a]

[a]*Department of Computer Science, University of York, York, YO10 5GH, UK*
[b]*School of Reliability and Systems Engineering, Beihang University, Beijing, 100083, P.R.China*

Abstract

Safety cases, as a means of demonstrating system safety, have been increasingly used as the basis for system assurance, especially in safety or mission-critical systems in fields such as offshore installation, railway operations, nuclear plants, and air traffic control. Despite the increased adoption of safety cases in the aforementioned areas, the usage of safety arguments is still limited in the certification of a civil aircraft design. This paper provides 1) a brief overview of the key regulations and guidelines in support of aero-system certification especially at the development stage; 2) a review of the history, the essence, and the practice of safety cases; 3) an analysis of the role of processes and safety arguments in aircraft certification; and 4) recommendations on the future work in terms of further application of safety cases in aircraft certification.

Keywords: Airworthiness; Certification process; Safety arguments; Safety case; Safety analysis

1. Introduction

Certification [1], as the 'legal recognition' of the level of intended functions and other attributes of a system, is important for regulatory bodies, developers, and end-users. In the aerospace domain, formal certification has long been required and practiced for aircraft and systems that implement the aircraft functions to confirm that their design, maintenance and operation are acceptably safe.

With the driver of more capable systems and the development of new technologies, modern aero-systems are becoming increasingly complex, e.g. digital engine control, Integrated Modular Avionics. As

* Corresponding author. Tel.: +44 -1904 325428; Fax: +44- 1904325599.
E-mail address: linling.sun@cs.york.ac.uk.

doi:10.1016/j.proeng.2011.10.041

a result, it is an increasingly challenging task to demonstrate the achieved level of aircraft/ system safety and show compliance with applicable requirements with an adequate degree of confidence.

There are many standards and guidelines, formulated, accepted and practiced in the area of safety and aircraft certification, e.g. FAR Part 25/ EASA CS-25, ARP 4754A, ARP 4761, MIL-STD-882D, MIL-STD-516B, MIL-HDBK-514, DS 00-56, and DS 00-970. They are strong in that they provide the high-level generic requirements and guidance for all aircraft systems and they represent auditable processes and encourage systematic system modeling and analysis.

However, these standards and guidelines leave implicit some issues of argumentation, which are necessary to provide the rationale, context and backing for the results being used for certification judgments. People may have thought about these issues, but most of them exist as informal (internal or private) dialogues that are implicit and undocumented. Without systematic and explicit justifications for the certification activities and certification data, our confidence in the certification results cannot be sufficiently established and improved.

In this paper, we will describe the notion of a ‘safety case’, which is increasingly adopted in a number of fields in which system safety is of paramount concern, such as air traffic control, military aviation, offshore installation, railway operations, and nuclear plants. The purpose of a safety case is to “communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context” [2]. This argument should be appropriately supported by evidence. Ideally, the argument is communicated in an orderly, structured, and transparent fashion by means of documenting clearly the pertinent set of safety objectives, supporting claims and evidence, and the inferential links between them. We will also explain the way in which safety cases can be used to support the certification process and to alleviate problematic issues in certification and the potential pitfalls and difficulties associated with the application of safety cases in the context of aircraft certification.

The rest of the paper is structured as follows. Firstly, a brief review of the key standards and guidance used for aero-system certification (and their interrelationships and change history are) is presented. Secondly, the importance of the ‘process’ element in aircraft certification and the issues related to the processes are discussed. Thirdly, the history, the essence and the practice of safety cases are reviewed. Finally, the potential benefits and pitfalls of applying safety cases and recommendations for future work are presented.

2. Standards and Guidelines

There are a series of certification specifications and guidance in the civil and military aviation domain in different countries. They share a common core part and each has its own specific features. Here we only present the most typical ones to describe the key frame of current regulations and guidance and their intended usage in aircraft certification.

The European Aviation Safety Agency (EASA) Certification Specifications (CSs) and Federal Aviation Regulations (FARs), prescribed by the Federal Aviation Administration (FAA), are the predominant rules governing the activities in the civil aviation domain. For example, for large aircraft the relevant requirements are defined in CS-25 and Part 25. They are designed to promote safe design, maintenance, and operation of aero-systems/aircraft and to protect the public from avoidable risks.

SAE ARP 4754A [1] (an up-issue of the previously issued version ARP 4754 [2]) provides the overall development guidance of civil aircraft and systems in the context of Part 25 and CS-25. It defines the safety assessment process, Development Assurance Levels (DALs), and deliverables required along with the aircraft/system development process and other integral processes, taking into account the overall aircraft operating environment and functions. Requirement validations and implementation verification are stressed for certification and product assurance in ARP 4754A: “It provides practices for showing compliance with the regulations and serves to assist a company in developing and meeting its own internal standards by considering the guidelines" [1].

Software development is addressed in RTCA document DO-178B, "Software Considerations in Airborne Systems and Equipment Certification" (the EUROCAE counterpart is ED-12B). The electronic hardware development is covered by RTCA document DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware". The design and certification issues of integrated modular avionics (IMA) are considered in RTCA/EUROCAE document DO-297/ED-124. In addition, ARP 4761 serves as guidance of the detailed techniques that can be adopted in safety assessment processes and ARP 5150/ ARP 5151 provide in-service safety assessment guidance. Figure 1 from [1] depicts the interrelationships between these guidance documents.

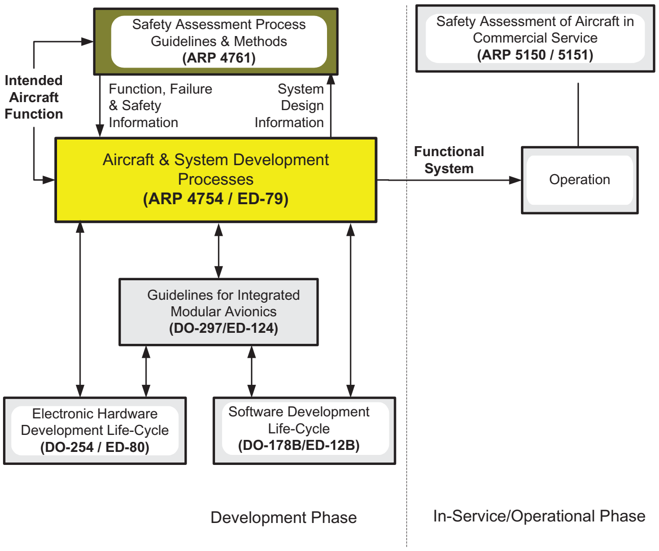
Safety Assessment Process Guidelines & Methods (ARP 4761)
Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
Aircraft & System Development Processes (ARP 4754 / ED-79)
Functional System
Operation
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
Electronic Hardware Development Life-Cycle (DO-254 / ED-80)
Software Development Life-Cycle (DO-178B/ED-12B)
Development Phase
In-Service/Operational Phase

Fig. 1 Guideline Documents Covering Development and In-Service/Operational Phases (from [1])

There are also standards and guidance for certification and safety used in military aviation, such as the US military standards and handbooks MIL-STD-882D, MIL-STD-516B, MIL-HDBK-514, and the UK Defence Standards 00-56 and 00-970, but we will not discuss these in this paper.

Standards and guidance are the products of common concerns and established best practice. Over the past thirty years, many safety standards have been evolving, and continue to do so. They start with an initial version and have been updated periodically to address the improvement of technologies and lessons learnt from accidents, incidents and real practice. For example, the Part 25 has been refined and expanded over time, with the support of a large number of Advisory Circulars (ACs) and Technical Standard Orders (TSOs). There are other examples. We can trace initial systematic safety analysis consideration in [4] published in 1982, then the release of ARP 4754 in 1996 in which the system development and safety assessment processes for increasing integration and complexity of aircraft electronic systems are clearly defined, then the release of ARP 4754A in 2010 which introduce integral processes and put more emphasis at the development and synthesis of the overall aircraft. In terms of software certification, the evolving history of DO-178 [5] is that: DO-178 was first published in 1982, then revised as DO-178A in 1985, then updated into DO-178B in 1992 which focuses documentation integration, system issues, software verification, configuration management, software quality assurance etc. Another revision DO-178C will be issued shortly in order to better accommodate modern technological issues such as object-oriented technology, model-based design and verification, formal methods, and tool qualification [6]. There is also a planned update to ARP 4761 which will provide improved support to the application guidance of some of safety assessment methods and incorporate new safety assessment practice such as Model-Based Safety Assessment (MBSA). The evolution of these standards and guidelines reflect the advances in technological solutions and the continuous efforts to strengthen weak points in the development and certification of safety-critical aerospace systems.

3. Processes in Certification

3.1. Role of Processes

Processes are important elements in aircraft certification. Firstly, certification is a process itself which is to substantiate the compliance of applicable requirements by an aircraft and its systems. With the recommended processes which are intended to support certification, it is easy and clear for duty-holders to organize and plan activities and resources in the development lifecycle.

Many standards and guidance in aircraft certification are organised around processes, e.g. ARP 4754A, DO-178B, MIL-HDBK-514. The integration of the various processes is emphasized and usually core deliverables from these processes are recommended in these standards and guidance. In this paper, we use ARP 4754A below as an example to show the importance of processes in certification.

The newly released ARP 4754A present a series of interrelated processes. Comparing to the previous issue of ARP 4754, there are some important changes and improvements.

- The planning process of aircraft/systems development is more explicitly elaborated with a diagram.
- The aircraft or system development process is presented with key steps of the aircraft/system development cycle which is not explicitly represented in a flow diagram previously.
- The interaction between the system safety process and the system development process is more extensively described than that in the previous version.
- The aircraft function implementation process has been strengthened with two additional components – the DAL assignment process and the requirements capture process – and the subordinate role of the supporting processes is changed and is now described as integral processes.
- The safety assessment process model has been modified mildly, with PASA (Preliminary Aircraft Safety Assessment) and ASA (Aircraft Safety Assessment) explicitly stated which highlights the importance of safety synthesis.
- The FDAL (Functional Development Assurance Level) / IDAL (Item Development Assurance Level) assignment process is elaborated and examples have been provided.
- Both the requirement validation process model and the verification process model have been updated, but only with minor changes.
- The configuration management process is now more extensively explained.

3.2. Required Artefacts

To accompany the recommended processes, necessary certification data/ artefacts are usually suggested or required by guidance documents. We use the certification data described in ARP 4754A as an example of the required artefacts from integral processes. The certification data suggested in ARP 4754A is shown in Table 1.

Table 1 Certification Data (from [1])

Certification Data	
Certification Plan	Preliminary Aircraft / System Safety Assessment
Development Plan	Aircraft / System Safety Assessment
Design Description	Common Cause Analysis
Validation Plan	Validation Data
Verification Plan	Verification Data
Configuration Management Plan	Evidence of Configuration Management
Process Assurance Plan	Evidence of Process Assurance
Configuration Index	Certification Summary / Compliance Report
Functional Hazard Assessment	

The artefacts described are almost unchanged from the previous version of guidance. But the updated guidance indicates clearly that "all certification data in the above table should be generated as required" [1], although not all of the data is necessarily to be submitted to the certification authorities. There are no specific constraints on the forms of the certification data other than that it should be possible to provide "efficient retrieval and review". Previously, there were some indications as to the minimum required data items for certification in the data list; however, the new version has removed these indications as they were often misinterpreted and led to a misunderstanding that no possible queries and potential required submission of further details on specific topics under concern.

The certification data recommended above is important evidence for the decision-making processes of certification authorities. However, presenting them as the process 'outcomes' in the ARPs does not put enough emphasis on the fact that the developers should carefully contextualize and justify the data, and show how they fit together to form the overall justification of system safety. It is stated that 'any analysis is only as accurate as the assumptions, data, and analytical techniques it uses' (a quote from AMC25.1309 – the aerospace standard that describes acceptable means for showing compliance with the requirements of CS 25.1309 [7]). However, current requirements or guidance for the justification of evidence for its 'fitness for purpose' is insufficient and the analysis/model validation activity is usually not explicitly shown as a part of the integral safety assessment and system development processes.

3.3. Process-Related Issues

Processes play an important role in system development and certification. However, there are potential issues need to be considered for in-depth and pragmatic understanding of these processes and effective implementation of these processes. Four major issues are discussed below concerning the imperfectness of merely process-oriented certification.

First of all, the rationale underlying the processes recommended or processes from best practice are often implicit and exist only as hidden knowledge. For example, ARP 4754A provides significant guidance on the derivation and demonstration of safety requirements through safety assessment. Historically, the reasons of doing so in a certain way have been considered or been done implicitly. The underlying reasoning is not typically documented in a systematic form and not included as a part of the certification document.

Secondly, the role and the treatment of evidence (the outputs of process activities) are not adequately emphasised. Although recommended deliverables are usually required and supplied with processes, evidence items are often managed as separate artefacts, which can provide a scattered/ fragmented view of the overall system. The review of evidence is required but with little guidance on how to do this in the existing standards and guidance. The review activities are often not systematically or explicitly documented. In addition, the links between the safety requirement hierarchy and different pieces of evidence are often difficult to comprehend, and the interrelationships between various pieces of evidence are again not always systematically addressed.

Thirdly, the safety process/activities planned and the enactment of a planned process are different. The traditional recommended safety assessment process is derived from industrial best practice and has been adopted and practiced for a long time. It allows us to tailor and provides us flexibility over the choice of activities. However, the recommended process or planned activities do not guarantee the quality of results generated from the enactment of a specific process. The safety of a system needs to be justified with outputs from the 'as-performed process', not just from the promise of the 'as-intended process'.

Finally, the interfaces of different processes are sometimes overlooked and they are not easy to manage and not well-managed in practice. For example, the certification process study for commercial airplanes [8, 9] initiated by FAA following a number of aviation accidents, found that the interfaces between the design certification and the maintenance and operation of aircraft are not well-connected. The study also identified many weak points in currently implemented certification processes and previously missing sub-processes in an aircraft/system life cycle.

In summary, processes are not perfect by themselves and the confidence in the eventual system attributes of the delivered system cannot be derived from processes alone. The issues discussed in this section must be considered and properly handled by both the regulators and the developers in order to provide assurance that the aircraft or systems are designed, maintained and operated in a safe manner.

4. Safety Cases

4.1. Overview of Safety Cases

The concept of presenting safety-related information and arguments in a formal report initially came from the nuclear industry, but the notion of 'safety cases' is originated in major industrial accident control regulations introduced in the process sector in the UK in 1984 [10]. Lord Cullen, in his report on the Piper Alpha accident [11] in 1990, recommended the introduction of a safety case regime as part of the regulation of oil and gas facilities and operation. The philosophy of a safety case is to construct a clear, structured, compelling argument to demonstrate the safety of a system in a particular operational context.

The definition from Defence Standard 00-56 [12] is that 'a Safety Case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment'.

The core of a 'safety case' is the safety argument. A safety argument communicates how the overall objectives and claims of the safety case can be shown to be supported by the available evidence (such as the safety analysis results). A safety argument is generally composed of a hierarchy of safety claims and evidence, together with the inferential steps that are believed to connect the claims to the evidence. By requiring the explicit presentation of a safety argument it encourages rigorous thinking and questioning that is more suitable for demonstrating the outputs of novel products and novel methods [13, 14].

Confidence in the validity of safety judgments comes not only from the sufficiency and validity of the evidence element of an argument, but also from the structure of a safety argument and the sufficiency and strength of the safety argument in linking the elements together. Argument and evidence go 'hand in hand' to provide the overall case. "Argument without supporting evidence is unfounded, and therefore unconvincing. Evidence without argument is unexplained – it can be unclear that (or how) safety objectives have been satisfied.”[2]

Safety case development and acceptance has been adopted and practiced systematically in a wide number of industries, especially in Europe, such as railway, air traffic control, maritime, and defence, for more than twenty years. The mandatory requirements for safety cases in some industries (e.g. UK Defence Standard 00-56, EUROCONTROL’s Safety Assessment Methodology) show that the role of safety arguments is acknowledged. The recent releases of international standards such as the ISO/IEC15026 (Part 1 and Part 2) [15, 16], ISO26262 [17], and a FDA guidance [18] also indicate increasing adoption and interest in the application of an argument-based approach for system assurance. The central theme of using arguments for justification of the achievement of system attributes has now been transferred and expanded beyond the area of safety engineering. There are security cases, reliability cases, dependability cases, trust cases, survivability cases, and assurance cases. Some aviation-related systems have adopted this approach for system safety assurance, for example, integrated modular avionics [19], air traffic control [20, 21] and aircraft operational hazard control [22]. In MISSA [23] project, the argument-based approach has been applied for justification of safety assessment models. The approach has also been suggested for some aerospace software certification [24].

A safety-case argument can be documented in either a textual form or a graphical form. A number of graphical notations are available to support structured documentation of safety arguments, such as Goal Structuring Notation (GSN) [25] and Claims-Arguments-Evidence (CAE) [26]. The construction and management of safety cases are also supported by commercial software tools, such as GSN Modeler [27] and ASCE [26]. An exemplar safety argument represented in GSN from [28] is shown in Figure 2. In the example, the top-level safety goal is “Control System Logic is fault free”. The top safety goal is supported by lower-level sub-goals indirectly through two argument strategies. At the lowest level, the sub-goals need not to be decomposed and can be clearly supported by reference to items of safety evidence, such as a system analysis model or the results of system testing. In Europe, safety cases have been practiced for the safety justification of a number of aviation systems [28] (in development stages or in operational stages), e.g. Eurofighter Aircraft Avionics, Hawk Trainer Aircraft, Eurocontrol Air Traffic Management.

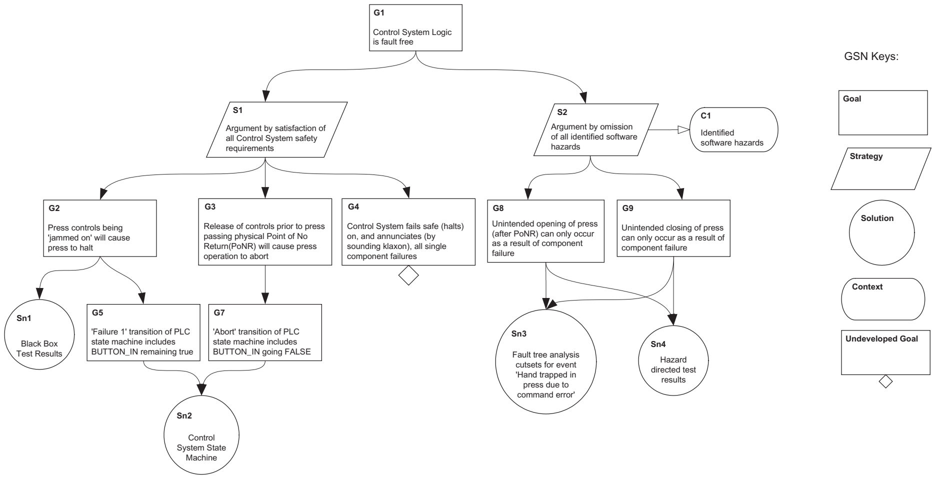
G1
Control System Logic is fault free
GSN Keys:
S1
Argument by satisfaction of all Control System safety requirements
S2
Argument by omission of all identified software hazards
C1
Identified software hazards
Goal
Strategy
G2
Press controls being 'jammed on' will cause press to halt
G3
Release of controls prior to press passing physical Point of No Return(PoNR) will cause press operation to abort
G4
Control System fails safe (halts) on, and annunciates (by sounding klaxon), all single component failures
G8
Unintended opening of press (after PoNR) can only occur as a result of component failure
G9
Unintended closing of press can only occur as a result of component failure
Solution
Context
Sn1
Black Box Test Results
G5
'Failure 1' transition of PLC state machine includes BUTTON_IN remaining true
G7
'Abort' transition of PLC state machine includes BUTTON_IN going FALSE
Sn3
Fault tree analysis cutsets for event 'Hand trapped in press due to command error'
Sn4
Hazard directed test results
Undeveloped Goal
Sn2
Control System State Machine

Fig. 2 An example safety argument represented in GSN (from[28])

4.2. Role of Arguments in Certification

Rushby has stated, in [29], that the high-level assurance for aircraft safety 'has much in common with the notion of a safety case', although not explicitly described or presented as a safety case. From the existing experience of safety case research and practice, we identify that the use of safety cases within the aircraft certification can potentially bring about the following benefits.

A. Systematic, Holistic Thinking

Prior to the introduction of safety cases, many domains relied upon prescriptive safety regimes whereby regulators (through safety standards) dictated the specific measures to be adopted to ensure system safety. Safety cases provide a contrast to this approach. Firstly, adopting safety cases will shift more responsibility for the justification and demonstration of system safety to the primary developers and operators of systems. Secondly, safety cases often are introduced hand-in-hand with a 'goal-setting' approach whereby high-level objectives are provided by regulators, but developers and operators are given freedom in establishing suitable arguments and evidence to demonstrate the achievement of those objectives. Regulators will always struggle to be complete in prescribing regulations and requirements that are intended to apply to a large number and variety of applications. Regulators also inevitably struggle in writing regulations that engage in the specifics of the day-to-day operation of every system to which the regulation applied. This is why the shift towards requiring developers and operators to demonstrate their systematic thought-processes, and their systematic justification, is so important in regard of striving for a comprehensive and holistic account of safety.

B. Aiding Communication Amongst Stakeholders

In existing safety case practice, at minimum safety cases are developed by one organisation to be reviewed by another (i.e. a regulator). They enable the explicit documentation and communication of the beliefs and evidence as to why a system is acceptably safe. For most safety-critical and safety-related systems there are many stakeholders, e.g. there are designers, operators, maintainers, managers, evidence providers, and the public. Safety cases can act as a focus of discussion between these stakeholders. Each can provide input relating to their understanding and concerns. Each can query the resulting safety case to see how their issues have been addressed.

C. Encouraging Transparency and Clarity

As Petroski stated in [30], "it is the essence of modern engineering not only to be able to check one's own work, but also have one's work checked and to be able to check the work of others". It is not possible to demonstrate immediately and unequivocally the satisfaction of safety requirements by the evidence and artefacts that are currently required by aerospace safety standards. There will be assumptions behind any safety assessment models. These assumptions may or may not be reasonable. There will be leaps of logic that connect safety requirements with the outputs of safety analysis. The act of establishing and documenting a safety case can help expose existing implicit reasoning, assumptions and risk acceptance judgments explicit. Safety cases will represent clearly the structure and relationships between safety requirements and supporting evidence, more importantly with contextual information and associated relations included and with reasoning steps clarified. Having documented a case, it becomes easier to review the arguments, question the evidence, and challenge the adequacy of the approach presented.

D. Integration of Evidence Sources

It is commonplace in existing practice that a diversity of evidence sources and types are required to demonstrate system safety - such as trials, human factors analysis, testing, operational experience. However, this diversity and amount of evidence can create difficulties. It can be difficult to judge completeness. Is the evidence set comprehensive? Does it cover all the issues? It can also be difficult to understand the distinct role and purpose served by each form of evidence. Safety cases help in this regard, by presenting the argument that explains how the overall safety objectives can be seen to be addressed through the assembled items of evidence.

E. Aiding Safety Management and Governance

Without an explicit safety case that attempts to pull together all of the threads of the safety argument, and ensure that appropriate evidence has been presented, there is a significantly greater risk of safety issues 'falling down the cracks' that can exist between existing safety assessments, metrics, and arrangements representing the specific concerns of individual stakeholders, or addressing single issues. Without the 'big picture' of a safety case, it is also easy for wildly varying and disproportionate amounts of effort to be spent in risk management. In fact, the safety cases can provide links between operational safety management and the design safety risk analysis, especially with enough stress on the contextual information traditionally overlooked.

4.3. Potential Pitfalls and Difficulties

Besides the potential benefits, there are also potential risks in the application of safety cases. In [31], seven traps to avoid for safety-case practitioners are listed. This section discusses three examples of typical 'bad experience', and some difficulties that might hamper the intended usage of safety cases.

A. Being Simply a 'Paper Exercise'

Safety cases must not become just another 'filed return'. The production of a safety case is an opportunity for gaining greater understanding of the current picture of safety, and for potentially making safety improvements. However, to do this it is important to ensure that appropriate time and effort is budgeted for the development and review of safety case. It is particularly important that safety case review is thorough and systematic.

B. Being Removed from Everyday Practice

Safety cases are supposed to address the realities of everyday system operation. It is important that they don't become a desk exercise that relates only dimly to the actual design or operating practice. The primary concern of a safety case should lie in demonstrating safety, rather than being an exercise in attempting to shift liability, or in merely demonstrating compliance with 'due practice'.

C. Being produced by the Wrong People

It is important that safety case development involves all of the relevant stakeholders with a understanding of, and involvement in, what actually makes systems safe (or unsafe).

A prerequisite of introducing safety cases is that there are (sufficient numbers of) suitably qualified and experienced personnel in place to help develop and review safety cases. In addition, the review and maintenance of safety cases need to be effectively policed.

4.4. Recommendations

On the basis of the review of current aircraft certification guidance and safety case practice, we suggest the following topics for future work.

A. Integration of a safety case regime with existing regulation and practice in aircraft certification

It is important that a clear and distinct role be defined for any safety case regime in order that it is not seen as nugatory or a duplication of existing efforts. The approach will not be well-accepted unless there is a pragmatic way to integrate and merge the practice of safety cases within existing practice of the aircraft development and certification.

B. Guidance in context of the aviation domain

Practical guidance will be required as to how to formulate safety case arguments, appropriately select evidence and critically review safety cases. Similar to the suggestion in [32], the regulators in aircraft certification also need to define a goal-structured safety case approval process, covering issues such as “How much evidence is enough?” and “How the evidence is to be used?”.

C. More trials of applying safety cases

With more real practice by those with first-hand experience in the aircraft certification domain, the benefits and difficulties can be more extensively identified.

5. Conclusions

This paper discusses the role of arguments in the certification of aviation systems, especially from the system safety assessment and synthesis perspective. An important observation is that there is insufficient emphasis (i.e. limited guidance and informal practice only) in existing guidance and practice concerning the explicit reasoning that connects claims of overall safety to the available evidence, and the adequacy of the safety analyses performed in existing guidance and practice. A review has been presented, focusing on the latest updates of safety assessment standards, the trends in system and software assurance and the historical background and the essence of safety cases. We understand that the existing standards and guidelines are widely adopted and accepted, and have served the regulatory authorities and industrial practitioners well. However, to increase rigor, more scrutiny is necessary and arguments must be constructed and presented to support the demonstration and justification of system safety at an adequate level of confidence. In addition, it is important to acknowledge that a safety case is not a ‘silver bullet’. It cannot be a substitute for current safety analysis or safety review practice, but plays a complementary role that encourages explicit documentation, critical and systematic reasoning and rigorous safety demonstration in system development, maintenance and operation. It is the people that work on safety and their way of thinking and implementation that determine the level of safety delivered and the degree of confidence in a claimed safety level.

Acknowledgements

This work has been partially supported by the MISSA project which is funded by the European Commission 7th Framework Program (ACP7-GA-2008-212088). The authors would like to thank Dr Katrina Attwood and the anonymous reviewers for their suggested improvements to the draft of this paper.

References

[1] SAE (Society of Automotive Engineers). ARP (Aerospace Recommended Practice) 4754A, Guidelines for Development of Civil Aircraft and Systems, 2010.

[2] Kelly TP. Arguing Safety: A Systematic Approach to Managing Safety Cases: Univ. of York, Dept. of Computer Science; 1998.

[3] SAE (Society of Automotive Engineers). ARP (Aerospace Recommended Practice) 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems. 1996.

[4] Lloyd E, Tye W, Great B. Systematic Safety: Safety Assessment of Aircraft Systems: Civil Aviation Authority; 1982.

[5] Kornecki A, Zalewski J. Software Certification for Safety-Critical Systems: A Status Report. Computer Science and Information Technology, IMCSIT 2008 International Multiconference on: 20-22 Oct. 2008.

[6] Brosgol B, Comar C. DO-178C: A New Standard for Software Safety Certification. Available from: http://sstc-onlineorg/2010/pdfs/BMB2623pdf, 2010.

[7] EASA (European Aviation Safety Agency. CS-25 Certification Specifications for Large Aeroplanes. 2003.

[8] FAA (Federal Aviation Administration). Commercial Airplane Certification Process Study - An Evaluation of Selected Aircraft Certification, Operations, and Maintenance Processes. 2002.

[9] FAA (Federal Aviation Administration). Part 23 - Small Airplane Certification Process Study - Recommendations for General Aviation for the Next 20 Years. 2009.

[10] Control of Industrial Major accidents Aazards Regulations (CIMAH) 1984.

[11] Cullen THL. The Public Inquiry Into the Piper Alpha Disaster 2 Volumes: Her Majesty's Stationary Office; 1990.

[12] MoD. Defence Standard 00-56: Safety Management Requirements for Defence Systems, Part 1: Requirements, Issue 4. 2007.

[13] Conlin H, Brabazon PG, Lee K. Exploring the Role and Content of the Safety Case. Process Safety and Environmental Protection 2004;82:283-290.

[14] O'Connor P. Standards in Reliability and Safety Engineering. Reliability Engineering & System Safety 1998;60:173-177.

[15] ISO/IEC TR 15026-1:2010 Systems and Software Engineering – Systems and Software Assurance – Part 1: Concepts and Vocabulary. 2010.

[16] ISO/IEC 15026-2:2011 Systems and Software Engineering – Systems and Software Assurance – Part 2: Assurance Case. 2011.

[17] ISO/DIS 26262 Road vehicles – Functional Safety. 2011.

[18] FDA (Food and Drug Administration). Total Product Life Cycle: Infusion Pump - Premarket Notification Submissions (Draft Guidance). Available from: http://wwwfdagov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM209337pdf 2010.

[19] Jolliffe G. Producing a Safety Case for IMA Blueprints. Digital Avionics Systems Conference (DASC) 2005.

[20] CAA (Civil Aviation Authority). CAP 670 Air Traffic Services Safety Requirements, SW01 Regulatory Objectives for Software Safety Assurance. Civil Aviation Authority Safety Regulation Group 2009.

[21] Felici M. Modeling Safety Case Evolution – Examples from the Air Traffic Management Domain. In: Guelfi N, Savidis A, eds. Rapid Integration of Software Engineering Techniques: Springer Berlin / Heidelberg; 2006: 81-96.

[22] Edwards C. Aircraft Operators Have Built a Generic Hazard Model for Use in Developing Safety Cases. ICAO Journal 2000;55:12-14.

[23] MISSA Project. Details available at: http://www.missa-fp7.eu/.

[24] Jacklin SA. Closing the Certification Gaps in Adaptive Flight Control Software. Guidance, Navigation, and Control Conference. Honolulu, Hawaii, USA; 2008.

[25] Kelly T, Weaver R. The Goal Structuring Notation - A Safety Argument Notation. Dependable Systems and Networks 2004 Workshop on Assurance Cases; 2004.

[26] Adelard. The Adelard Safety Case Editor (ASCE). Product description available at: http://adelard.co.uk/software/asce/; 2003.

[27] Atego. Atego GSN Modeler. Available at: http://www.atego.com/products/atego-gsn-modeler/ Accessed on 21 May 2011.

[28] Kelly T. A Systematic Approach to Safety Case Management. SAE International, SAE World Congress. Detroit, USA; 2003.

[29] Rushby J. AIAA 2008-6799 How Do We Certify for the Unexpected? AIAA Guidance, Navigation and Control Conference and Exhibit. Honolulu, Hawaii, USA; 2008.

[30] Petroski H. To Engineer is Human: The Role of Failure in Successful Design: Vintage Books; 1992.

[31] Kelly T. Are Safety Cases Working? Safety Critical Systems Club Newsletter 2008;17:31-33.

[32] Weinstock CB, Goodenough JB. CMU/SEI-2009-TN-018 Towards an Assurance Case Practice for Medical Devices. 2009.