ARIBA

ATM system safety criticality Raises Issues in Balancing Actors responsibility

Final Report for Publication

WP8: Organisation and co-ordination between WPs
Final Report for Publication
Reference: ARIBA/NLR/WP8/FRFP

Contract No AI-97-SC.2033

Distribution List		
Bas VAN DOORN Henk BLOM Jasper DAAMS Herman NIJHUIS Mariken EVERDIJ	NLR	(NLR)
Eric ANDLAUER Françoise GIRARD	Sofréavia	(SOF)
Chris KELLY	DERA	(DERA)
Marc SOURIMANT	AIRSYS-ATM France	(Airsys)
Carl VANSTEELANDT	APTIME	(APT)
Billy JOSEFSSON	Swedish CAA	(SCAA)
Gavin BOUNDS	UKCAA SRG	(SRG)
Patrick HUDSON	Leiden University	(RUL)
Dominique VAN DAMME Jacques BEAUFAYS	EUROCONTROL	(EHQ)
Lars LÖNNBERG Gerald O'CONNELL	EC-DG VII	(DG7)

Edited by:	B.A. van Doorn	
Reviewed by:	H.A.P. Blom	
Approved by:	Lars Lönnberg, DG7	Date:

Document Change Log

Version #	Issue Date	Sections Affected	Relevant Information
1	03/12/99	All	New Document

Partnership

The ARIBA Consortium consists of:
- National Aerospace Laboratory NLR
- AIRSYS ATM France
- Sofreavia
- Defence Evaluation and Research Agency (DERA)
- Aptime
- UK CAA Safety Regulation Group
- Swedish Civil Aviation Administration
- Leiden University

Contact persons:

Lars Lonnberg (DG7 Project Officer)
European Commission, DG VII – Transport, Rue de la Loi 200, B-1049 Brussels, Belgium
tel: 32-2-296 72 76
fax: 32-2-296 83 50
E-mail: Lars.Lonnberg@dg7.cec.be

Henk Blom (Project Co-ordinator)
NLR, Anthony Fokkerweg 2, 1059 CM Amsterdam, The Netherlands
Tel: +31-20-511 3544
Fax: +31-20-511 3210
E-mail: blom@nlr.nl

Marc Sourimant
Airsys ATM France, P&D/LMCAS,19, Rue de la Fontaine, F-92221 Bagneux Cedex, France
tel: 33-1-40 84 18 66
fax: 33-1-40 84 18 79
E-mail: marc.sourimant@fr.airsysatm.thomson-csf.com

Chris Kelly
Defence Evaluation and Research Agency (DERA), ATC Systems Group (ATCSG), St. Andrews Road, Malvern, Worcs, WR14 3PS, UK
tel: 44-1684- 89 4684
fax: 44-1684-89 4109
E-mail: kelly@atc.dera.gov.uk

Eric Andlauer
Sofréavia, Carrefour de Weiden 3, 92441 Issy-les-Moulineaux, France
tel: 33-1-41.23.46.59
fax: 33-1-46.48.32.80
E-mail: andlauere@smtp.sofreavia.fr

Carl Vansteelandt
Aptime, Rue du Docteur Finlay 28, 75015 Paris, France
tel: 33-1-44 37 02 80
fax: 33-1-44 37 02 81
E-mail: vansteelandt@aptime.fr

Gavin Bounds
CAA Safety Regulation Group, Gatwick Airport South, Aviation House, West Sussex RH6 0YR, UK
tel: 44-1293-57
fax: 44-1293-57 39 74
E-mail: gavin.bounds@srg.caa.co.uk

Patrick Hudson
Leiden University, Wassenaarseweg 52, P.O Box 9555, 2300 RB Leiden, The Netherlands
tel: 31-71 527 3820
fax: 31-71 527 3619
E-mail: HUDSON@rulfsw.fsw.LeidenUniv.nl

Billy Josefsson, ASP100
Swedish Civil Aviation Administration, Vikboplan 11, S-601 79 Norrköping, Sweden
tel: 46-11 19 23 31
fax: 46-11 19 25 75
E-mail: billy.josefsson@ans.lfv.se

Jacques Beaufays
Eurocontrol Headquarters, Rue de la Fusée, 96, B-1130 Brussels, Belgium
tel: 32-2-729 37 32
fax: 32-2-729 91 08
E-mail: jacques.beaufays@eurocontrol.be

Executive Summary

ARIBA stands for "ATM system safety criticality Raises Issues in Balancing Actors responsibility". It is a project carried out on behalf of DGVII of the European Commission in 1998-1999 and addresses certification in ATM services.

Due to the competence of pilots and ATCo's, and the availability of appropriate technical systems and proven procedures, an ATM service provider is able to safely manage a certain traffic flow. In effect, ATM safety responsibilities end up with the human elements in the responsibility chain, i.e. the air traffic controllers and pilots. This forms an understandable reason for ATM service providers (and airlines) to have difficulties with accepting any new system, procedure or operation that potentially reduces the controllability of various non-nominally evolving traffic situations, while their responsibility increases with traffic volume. Currently, a major cost element of introducing advanced ATM operations is that the duration of the implementation period becomes uncontrollable when safety responsible actors become indecisive due to the lack of a systematic way to manage these paradoxical developments (lower controllability, higher responsibility). Consequently, potential investors know in advance that it might take decades before they receive any return on investments. Obviously, no commercial-like actor should invest under such condition. The aim of ARIBA is to make these situations manageable.

A recent FAA-initiated task force on certification [RTCA, 1999] has considered the question why the dynamic growth and globalisation of aviation have outpaced the existing certification framework in civil aviation. The time and cost required for implementing new operational capabilities has increased, while the translation of those capabilities into actually improved operations often asks for an unpredictable amount of time, cost and effort. This situation is further worsened by the existence of many differences between national certification processes and criteria. All together, the "certification" process from initial concept development to effective operational use has grown out of control. The RTCA task force on certification developed recommendations on how to make the regulatory oversight process more responsive to today's operational environment. These recommendations form a clear support for the ARIBA approach of studying the ATM safety certification problem not in isolation, but to focus in from the wider scope of the safety certification problem in civil aviation. In doing so, ARIBA has also introduced three key developments in certification:

- In Europe there already is a sound basis for thinking in terms of complementary responsibilities of various actor types, such as airports, ATM service providers, regulators and policy makers, where the RTCA task force on certification commonly refers to them as one actor type: authorities.
- Experience gained in other safety-critical domains (e.g. nuclear, petrochemical, rail transport) shows that safety management and Safety Case building are effective tools to combine business interests with safety interests.

- Advantage is taken of recent advancements in safety assessment methodology that overcome the serious limitations of established techniques, e.g. human controllers are capable solvers of non-nominal situations under various circumstances, while the established techniques rather represent them as error sources only.

The ARIBA project has used these key elements to develop significant improvements in safety certification for ATM. This is accomplished in two subsequent stages.

Stage 1: In-depth studies.

During the first stage, all effort was directed to the following five parallel in-depth studies:

1. ATM certification perceptions of various actor types and around Europe have been identified through enquiries. These results have been analysed and subsequently synthesised into ATM certification recommendations.
2. Existing certification practices have been analysed for the following applications: airborne software, systems in military aviation, automation systems in finance, equipment for nuclear industry, safety-critical systems for railways.
3. The ATM certification problem has been studied on the basis of the successful results obtained through the development and introduction of safety management approaches in the off-shore petrochemical industry.
4. For a basic ATM operational example it has been shown possible and effective to combine models from cognitive psychology with high level models of ATM systems, and subsequently assess accident risk and human controllability.
5. It was shown that there is a large variety in possible safety cases, and that an advanced methodology for building safety case for complex technical systems is not really capable of building safety cases for advanced ATM operations.

Stage 2: Consolidation

The aim of the consolidation stage of ARIBA has been to develop a safety certification framework and recommend supporting methodologies that enable an effective implementation of ATM advancements by the responsible actors. The safety certification framework is documented in Part I, the recommended methodologies are documented in Parts II and III for ATM service providers and manufacturers of ATM automation methodology respectively.

- Part I develops a new safety certification framework in ATM, using experience gained in other safety-critical domains. Three things will become clear: 1) for safety-critical domains safety management and Safety Case building are a matter of good business practice, 2) the complexity of ATM advancement asks for a dedicated safety validation methodology, and 3) enforcement of safety certification by authorities is most effective if it supports good business practices. Following these findings, Part I develops good safety business practices for the various commercial-like actors in ATM, identifies the particular safety driven collaboration needs of various commercial actors in ATM, and subsequently identifies how authorities could support the best business practices approach through appropriate enforcement of formal survey and approval.

- Part II outlines safety validation of changes to systems or operations in ATM. The central theme is safety validation by building Modern and Joint Safety Cases for changes in ATM operations, that are aimed to incorporate various types of human involvement, and in contrast with Classical Safety Case, that take safety management approach into account. In addition, it covers all kinds of hazards and not just failure modes. Part II outlines how several complementary state-of-the-art approaches allow to build Modern and Joint Safety Cases for ATM. These approaches are: 1) development of suitable risk criteria, 2) dependability techniques for the assessment of technical (sub)systems, 3) task load analysis for pilots and controllers, 4) fast-time simulation to assess air traffic network characteristics, 5) hazard identification and classification techniques, 6) accident risk assessment techniques in ATM, 7) providing feedback to advanced operation, and 8) technique to identify pro-active and reactive safety improvements of the operation/service. Part II concludes with guidelines to support the further development and application of these methodologies.

- Part III outlines safety validation of ATM automated systems by a manufacturer. From dependability experience in various domains, including certification of airborne systems, several complementary approaches have been identified as being of key importance to safety validation by ATM/CNS system manufacturers: systematic building of a safety case, usage of development standards (especially for software development), dependability assessment feedback during design, and reverse engineering. Part III presents how these approaches can best be combined in support of an effective safety validation for ATM automated systems from conceptual design up to site acceptance, and presents guidelines to develop further standardisation in support of the proposed methodology, and its implementation at manufacturers.

In conclusion, in order to realise an effective safety management of implementing ATM advances, ARIBA addresses the need and development of a safety-certification framework that leaves the responsibilities with the key commercial actors involved, and that promotes an active collaboration between airlines, airports and ATM service providers in projects that are dedicated to effectively introduce advanced ATM operations.

Table of Contents

1. Introduction

1.1 Background

The European collaborative project known as ARIBA (ATM system safety criticality Raises Issues in Balancing Actors responsibility) carried out in behalf of DGVII of the European Commission within its Transport Research and Technological Development Work Programme 1994-1998. This Programme invited proposals in three main air transport domains: Air Traffic Management, Air Transport Safety and Environment, and Airports. The project [ARIBA, 1997] was selected following submission in response to Research Task 4.1.3/25 in the ATM domain, the full title of which is 'Analysis of the safety criticality of the different system components to identify suitable methods for certification of ATM systems deriving from other areas, such as aeronautics or nuclear power plants'.
As such the objective used by the ARIBA project is "To develop a certification framework and supporting safety validation methodologies that enable an effective safety management of the implementation of ATM advancements by the responsible actors".

1.2 ARIBA project

The key resources of an ATM service provider are competent ATCo's, appropriate technical systems and proven procedures. Due to the competencies of ATCo's and pilots, an ATM service provider is able to provide safe services up to a certain level of traffic flow. In effect, ATM safety responsibilities end up with the human elements in the responsibility chain, i.e. the air traffic controllers and pilots. This forms an understandable reason why ATM service providers (and airlines) have difficulties with accepting any new system, procedure or operation that potentially reduces their ATCo's and pilots controllability of various non-nominally evolving traffic situations, while at the same time their responsibility increases with traffic volume. The key issue is how this paradoxical development can be managed.

Currently, a significant cost element of introducing advanced ATM operations is that, because of the lack of a systematic way to manage safety related changes, the duration of the implementation becomes uncontrollable, while a safety responsible actor has to stay indecisive. Consequently, the potential investors often know in advance that it might take decades before they receive any return on investments. Obviously, no commercial-like actor should invest under such conditions. The aim of ARIBA is to make these situations manageable by two complementary approaches:

- Developing a harmonisation approach towards 'system safety criticality related responsibility issues' including a practical, effective framework for operational introduction of ATM enhancements. This should include recommendations for the implementation and further development of this framework, in relation to existing practices and ideas. Since ATM makes part of civil aviation, these focused

objectives are studied within the wider scope of safety certification in civil aviation.

- Identifying a cost-effective methodology for ATM safety validation throughout all life-cycles, by means of building on the results from earlier safety and validation methodology studies (e.g. [DAAS, 1995]; [APATSI, 1996, 1997]; [MUFTIS, 1996]; [SECAM, 1996]; [VAPORETO, 1996]; [FRAIS, 1996]; [GENOVA, 1997]; [CASCADE, 1998] and [RHEA, 1998]) and those from other safety-critical domains, with particular attention paid to their usability for validating forthcoming technological enhancements in ATM, such as Space-based navigation and surveillance, Advanced ATC automation support tools, Flight plan data exchange through air-ground data link.

1.3 Complementing RTCA's certification task force study

A recent FAA-initiated international task force on certification [RTCA, 1999] has considered the question why the dynamic growth and globalisation of aviation have outpaced the existing certification framework in civil aviation. The time and cost required for implementing new operational capabilities has increased, while the translation of those capabilities into actually improved operations often asks for an unpredictable amount of time, cost and effort. This situation is further worsened by the existence of many differences between national certification processes and criteria. All together, the "certification" process from initial concept development to effective operational use has grown out of control. In order to see this unhealthy situation improved, the international RTCA Task Force identified 15 specific recommendations on how to make the regulatory oversight process more responsive to today's operational environment.

The RTCA recommendations form a clear support for the ARIBA approach of studying the ATM safety certification problem not in isolation, but to focus in from the wider scope of the safety certification problem in civil aviation. There are also three complementary developments that will be covered by ARIBA:

- The study of the ATM safety certification is based on the experience gained in other safety-critical domains (e.g. nuclear, petrochemical, rail transport).
- In Europe there already is a clear basis for thinking in terms of complementary responsibilities from various actor types, such as airports, ATM service providers, regulators and policy makers, where the RTCA report commonly refers to them as one actor type: authorities.
- Advantage is taken of recent advancements in safety assessment methodology that overcome the serious limitations of established techniques, e.g. human controllers are capable solvers of non-nominal situations under various circumstances, while the established techniques rather represent them as error sources only.

In effect ARIBA is aimed at getting better hold on the responsibility problem in safety certification in the multi-actor environment of ATM. This is achieved in two stages:

- Stage 1: In-depth studies
- Stage 2: Consolidation

Both stages are shortly explained in the next two subsections. Eventually, the consolidated ARIBA findings will be communicated to the ATM community by means of a World Wide Web site and presentations at an appropriate symposium.

1.4 In-depth studies

During the first stage, in-depth studies have been conducted within the following five parallel streams of work:

1. This has produced an inventory of the ATM certification perception around Europe. Although there is some common belief that there is need for ATM certification, there also is a certain level of detail where significant differences in the various certification views appear. It is at this level where ARIBA should develop a rationale for harmonising the different views. The identified level of detail, the main differences in views and the resulting recommendations have been described in [ARIBA-WP1].
2. This has produced an assessment of existing certification practices in other domains. A large variety of risk-critical areas have been studied where it is common practice to apply specific forms of certification. For each domain, use has been made of experts with broad and deep knowledge in that field. The findings are documented in [ARIBA-WP2].
3. This has analysed the ATM certification problem. In order to avoid the need for jumping to conclusions in a complex field, the scientific approach was first to elaborate the problem statement, and next to solve the problem. Following this principle, the identification of the specific problems formed an important result of this analysis. The findings of this are documented in [ARIBA-WP3].
4. This has demonstrated how to objectively assess the human operator performance in providing ATM safety by following an adequate stochastic modelling approach. It has been shown that by means of this approach it becomes possible to design future developments in ATM such that for a human operator the balance between controllability and responsibility for ATM safety evolves in a proper direction. This study has been documented in [ARIBA-WP4].
5. This has studied the development of a safety case for an advanced design of ATM automation equipment, with the aim to relate performance settings on automation sub-systems to the safety targets of the overall ATM design. The WP5 work has resulted in new insight into Safety Case thinking for ATM, but has also shown that a system engineering directed safety case approach is not really capable of connecting the safety targets settings at the top level with those at the equipment level. [ARIBA-WP5] provides further details.

1.5 Consolidation

Since the five main studies of the first stage have largely been conducted independently of each other, and since there also are complementary external sources, there is a clear need for an integration and consolidation of these results into recommendations and guidelines on safety validation and safety certification in ATM. During this consolidation it is not the task of ARIBA researchers to enforce decisions

on issues for which an objective rationale is missing. Rather, the aim of ARIBA is to provide insight into the problem, and identify possible directions for its solution.

The certification objective used during the ARIBA consolidation is "To develop a certification framework that enables an effective safety management of the implementation of ATM advancements by the responsible actors". The consolidated results are documented in the following three self-contained final report parts:

- Part I develops an improved safety certification framework in ATM. From experience gained in other safety-critical domains three things will become clear: 1) for safety-critical domains safety management and Safety Case building is a matter of good business practice, 2) the complexity of ATM advancement asks for dedicated safety validation methodology, and 3) enforcement of safety certification by authorities is most effective if it supports good business practices. Following these findings, Part I develops good safety business practices for the various commercial-like actors in ATM, identifies the particular safety driven collaboration needs of various commercial actors in ATM, and subsequently identifies how authorities could support the best business practices approach through appropriate enforcement of formal survey and approval.
- Part II outlines safety validation of changes to systems or operations in ATM. The central theme is safety validation by building Modern and Joint Safety Cases for changes in ATM operations that are aimed at incorporating various types of human involvement, and in contrast with Classical Safety Case, that take safety management approach into account. In addition, it covers all kinds of hazards and not just failure modes. Part II outlines how several complementary state-of-the-art approaches allow to build Modern and Joint Safety Cases for ATM. These approaches are: 1) development of suitable risk criteria, 2) dependability techniques for the assessment of technical (sub)systems, 3) task load analysis for pilots and controllers, 4) fast-time simulation to assess air traffic network characteristics, 5) hazard identification and classification techniques, 6) accident risk assessment techniques in ATM, 7) providing feedback to advanced operation, and 8) technique to identify pro-active and reactive safety improvements of the operation/service. Part II concludes with guidelines to support the further development and application of the proposed methodologies.
- Part III outlines safety validation of ATM automated systems by a manufacturer. From dependability experience in various domains, including certification of airborne systems, several complementary approaches have been identified as being of key importance to safety validation by ATM/CNS system manufacturers: systematic building of a safety case, usage of development standards (especially for software development), dependability assessment feedback during design, reverse engineering, etc. Part III presents how these approaches can best be combined in support of an effective safety validation for ATM automated systems from conceptual design up to site acceptance, and presents guidelines to develop further standardisation in support of the proposed methodology, and its implementation at manufacturers.

In conclusion, ARIBA identifies the need for goal setting safety management approaches by ATM service providers and airports, and the adoption of three types of

Safety Cases: 1) Classical Safety Case for an ATM automation system by a manufacturer, 2) Modern Safety Case, for a change that involves the safety management by a single service provider, and 3) Joint Safety Case, for a change that involves the safety management by more than one actor. A Classical Safety Case may form supporting evidence in a Modern Safety Case by an ATM service provider or an airport, while Modern Safety Cases form supporting evidence in a Joint Safety Case. The required type of supporting evidence has been identified in earlier stages.

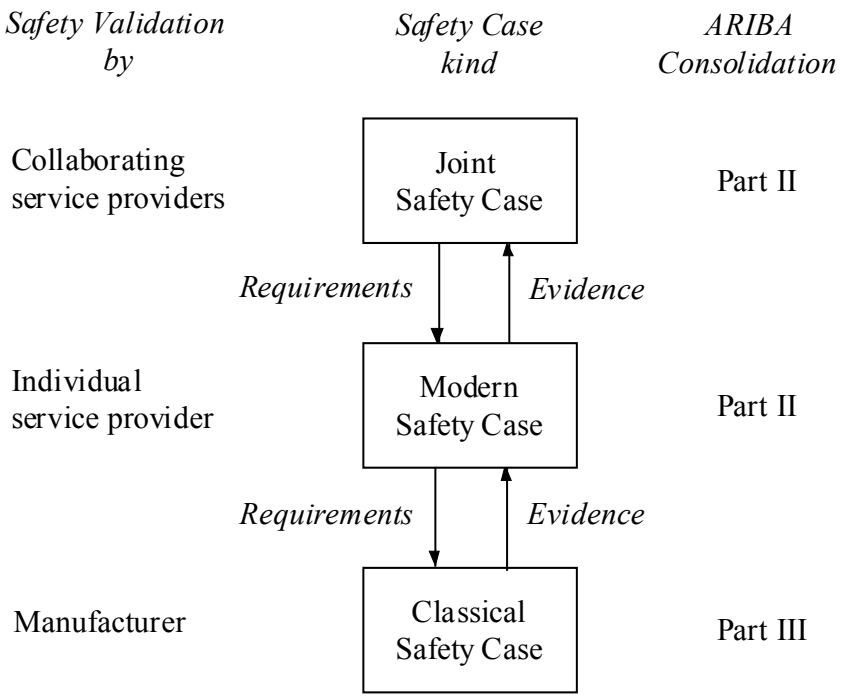


Figure 1. Complementary Safety Cases by various actors.

1.6 Organisation of this document

This document is ARIBA's Final Report for Publication. It presents the results of the consolidation stage of the project, which are also documented in [ARIBA-WP6-I], [ARIBA-WP6-II] and [ARIBA-WP6-III].

Part I present the safety certification framework in ATM. Part II presents the safety validation of changes to a system or operations in ATM. Part III presents the safety validation of ATM automated systems by a manufacturer.

Throughout this document, ISO terminology definitions ([ISO8402, 1994]; [ISO/IEC, 1996]) are adopted. The motivation for this is that they form the European Normalisation standard in the area of certification [EC, 1997] and they have appeared to be fit for the purpose of safety certification in ATM.

Part I - Safety certification framework in ATM

Authors: H.A.P. Blom and H.B. Nijhuis (NLR)

Part I of the ARIBA consolidation report is aimed at developing an argued recommendation on how to improve the safety certification framework in ATM. In doing so, we take into account that such framework should complement the certification framework in civil aviation. Part I focuses on the analysis of direction(s) for change in ATM safety certification, including guidelines on how to get things implemented into such recommended direction(s). This analysis is organised as follows:

- Section 2 gives an analysis of the existing certification framework in civil aviation. Considered are the certification processes on airborne avionics and ground/satellite systems, how this impacts the relations between commercial-like actors and places shortcomings on the standardisation process.
- Section 3 shows that experience in other safety critical domains implies that the adoption of goal-setting safety management approaches by airlines, airports and ATM service providers is a matter of good business practices. Obviously, the goal-settings have to be in line with applicable standards and regulations. Subsequently it is shown that an implementation of these good business practices by the majority of airports and ATM service providers would strengthen safety assurance in routine ATM operation.
- Section 4 shows that due to the distributed nature of ATM, airlines, airports and ATM service providers have various business needs to actively collaborate with each other on the development and (safety) validation of automation requirements, actor's safety goal settings and advanced ATM operations, and to actively involve manufacturers and Other service providers. Unfortunately, there hardly are opportunities to learn from other domains.
- Section 5 analyses the minimal need for enforcement of elements of a certification regime by regulatory authorities. This analysis is applied to the safety management and Modern Safety Cases from individual commercial-like actors and the Joint Safety Cases due to collaborations on advancing ATM. The baseline approach is that certification enforcement should support good business practices.
- Section 6 summarises the obtained results in the form of guidelines on safety certification in ATM, and suggestions on how to collect support around Europe to start with the implementation of these guidelines.

2. Existing framework

This section gives an analysis of the existing certification framework in civil aviation. Emphasis is on the roles played by the various actors.

2.1 Regulatory oversight

Historically, national and international regulatory authorities have established aviation policies to accommodate different aircraft users, various types of aircraft, and their different operational objectives and diverse capabilities. These policies include regulatory oversight in the operation of aircraft, the provision of aviation services and the manufacturing of aviation products within national airspace, across national borders and within international airspace. This regulatory oversight is commonly referred to as “certification” in civil aviation, and it is generally being recognised as the framework that has supported the safe introduction of new products, operational capabilities, and operations in civil aviation [RTCA, 1999]. The realised high safety levels in civil aviation show that this certification framework has been successful.

For the ECAC states, regulation and standardisation in civil aviation are coming in many forms from many bodies, e.g.:
- European Union (laws)
- National governments (laws)
- European Commission (mandates)
- ICAO (SARPS, PANS, SUPPS)
- JAA (JARs & TSOs)
- EUROCONTROL (directives and standards)
- National CAAs (AIP's)

Under the lead of the European Commission [EC, 1998a], activities are ongoing to bring the regulatory parts of the last three types of bodies together under the umbrella of a European Aviation Safety Authority (EASA). In addition to this, there are industrial standardisation bodies (CEN, CENELEC, ETSI, RTCA, EUROCAE, ARINC, etc.) and support for harmonisation in Europe, e.g. [EC, 1998b].

2.2 Approval of systems and operations

When incorporating a new functionality, requirements generally are derived consistent with a new or revised concept of operations. This is based on the intended role of the new functionality in improving operations. Figure 2 [RTCA, 1999] shows the idealised path for development and deployment of new CNS/ATM equipment, and associated procedures. In this path, the equipment is designed based on requirements related to the concept of operation. Following design and testing (according to JAR & FAR), the new equipment is integrated with other elements and deployed. By means of this process, operational experience and (hopefully) operational advantages consistent with the original concept of operations are gained.
Concentrating on the airborne avionics systems, installation generally requires airworthiness certification, which is part of its "type certificate" (TC) or "supplemental

type certificate" (STC). The equipment that supports CNS may meet a standard specification of a "technical standard order" (TSO), which is a form of certification for a particular type of equipment. Figure 2 illustrates that individual airworthiness certification of a particular piece of equipment for each operational use is not typically required. Based on innovative application of operational experience, the equipment can follow the approval path that bypasses the airworthiness approval step. In that case, it goes directly from design and test to operational approval. On the other hand, operational review or approval is nearly always required before implementation of new operational concepts.

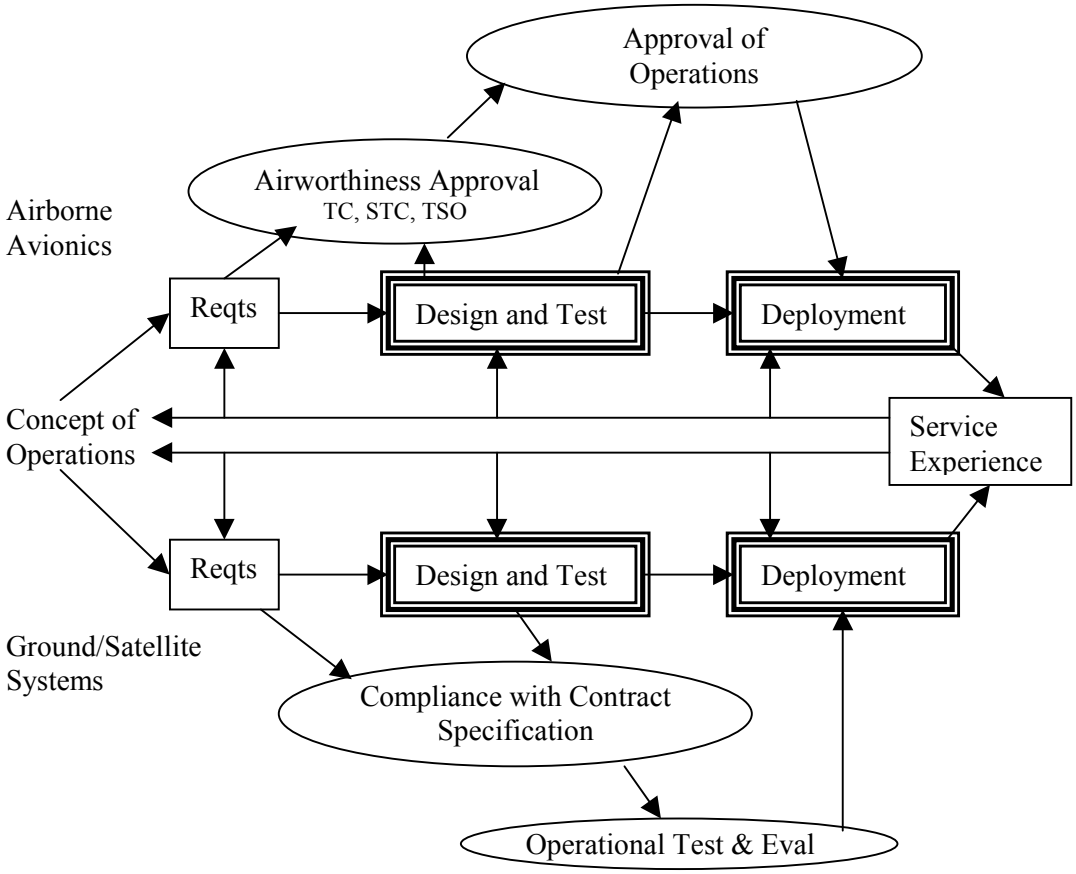


Figure 2. Similarities in development and deployment for airborne avionics and ground/satellite systems [RTCA, 1999]

In case of the development and deployment of ground-based and satellite equipment, certification generally represents two similar steps. First, the air traffic service provider's acceptance of the equipment is generally required through a contract. Second, there is usually some form of independent operational test and evaluation with controllers to assess the functioning, before it is deployed. The deployment criteria form the weakest links in both chains [Amalberti et al, 1998]. An important difference is that the level of international standardisation is less developed for ground/satellite systems than for airborne systems (both design / testing and deployment). In the following sections further differences will become clear, which are due to “commercial” relations between actors.

2.3 Feedback to survey

It has been recognised for decades that there is a need to receive feedback on the operation. This has led to the development of several accident and incident reporting systems (see Table 1). An overview of some key ones is given in the next table. The paradigms underlying these reporting systems are quite different. Some of them are publicly available.

Table 1. Main accident/incident reporting systems

Name	By	Since	Type	Reporters	Public
ADREP	ICAO	1970	Mandatory	States	Yes
ASRS	NASA	1975	Autonomous	Human operator	Yes
MORS	UK-CAA	1976	Mandatory	Human operator	Yes
CHIRP	UK-CAA	1982	Autonomous	Human operator	No
CAIR	BASI	1988	Autonomous	Human operator	No
BASIS	BA	1990	Autonomous	Airlines	No
ECC-AIRS	DG7	2002	Mandatory	States	No

In general, the problem is to avoid commercial conflicts when making information on incidents publicly available. It often is believed that mandatory incident reporting systems show only a part of the safety-relevant problems. For example, only one third of ICAO's ADREP consists of reports on incidents (of which about 80% is human factor related). In all autonomous reporting systems, the confidentiality of the human operators involved is guaranteed, and the competitive advantage is not jeopardised. Embarrassment for the commercial actor(s) involved definitively is a negative issue, however not a valid excuse for not participating. A truly severe problem is that for some states there are legal constraints in the way they are able to participate in incident and accident reporting. The general picture is that, with its ASRS, NASA has the lead in providing the necessary autonomous reporting feedback by pilots on incidents to the international standardisation process. An interesting observation is that less than 5% of these ASRS reports are made by controllers. There is clear evidence that this deserves significant improvement.

Both in Europe and in North America aviation safety improvement programmes are ongoing to improve this feedback:
- JSSI (Joint Safety Strategy Initiative) in Europe
- CAST (Commercial Aviation Safety Team) in North America

The aim of these programmes is to keep the number of fatalities in civil aviation at the current low levels by reducing the fatality risks per flight by at least as much as the number of flights increases. There is widespread agreement that the priorities for these safety improvement programmes are the CFIT and aircraft loss of control type of accidents, approach and landing phases, and human factors [FSF, 1999]. ATM induced fatality risks largely fall under the last category.

2.4 Commercial relations

In order to give a high level representation of the existing certification framework in civil aviation, we outline the situation for the passenger servicing actors:
- Civil aircraft operators, or for short Airlines in the sequel,
- Airport operators, or for short Airports in the sequel.

and outline their relation (see Figure 3) with other commercial-like actors in civil aviation:
- ATM service providers
- Manufacturers
- Satellite-based navigation service providers
- Telecommunication service providers
- Weather service providers.

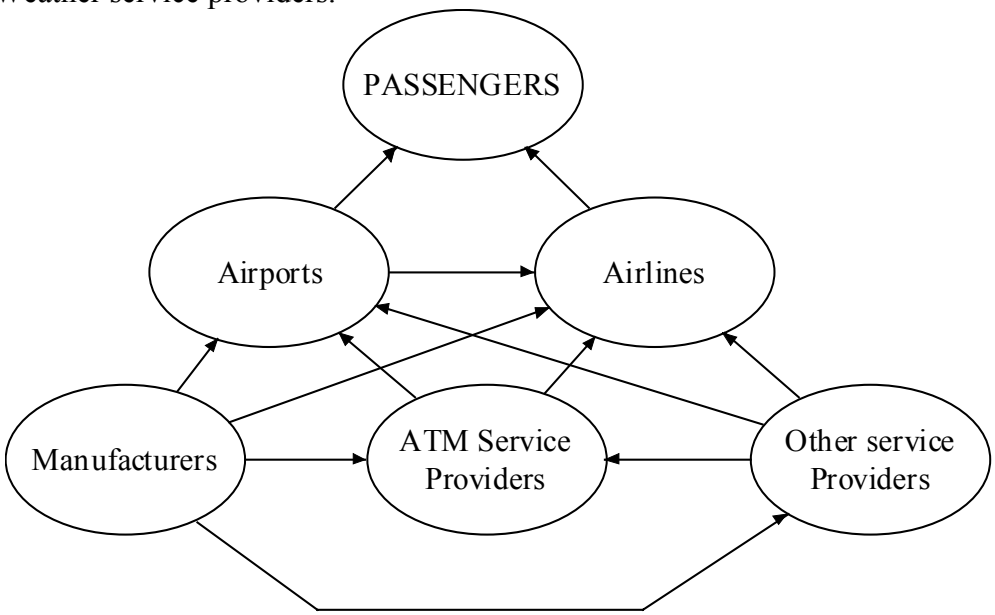


Figure 3. Relations between main commercial-like actors in civil aviation and passengers. Arrows represent products or services. Closest to passengers are airlines and airports. Manufacturers, ATM and Other service providers are at the next level.

Airlines

The core business of a civil aircraft operator (for short airline) is to transport passengers and/or cargo, both nationally and internationally. In general, each airline operates in line with internationally established operational standards and recommendations through ICAO (SARPs, PANS and SUPPS), JAA/FAA (JARs and FARs) and national regulators (e.g. AIPs). These operational recommendations are of a prescriptive nature, and address systems, procedures, and how the crew should make use of those systems and procedures under some typical conditions. In addition, an airline is responsible for maintenance of its aircraft to the prescribed safety standards, and to follow the manufacturer's advice on the maintenance of these standards. The enforcement of recommendations on national airlines is in hands of national civil aviation authorities, on the basis of applicable regulation. By ICAO conventions, common practice is that, by means of agreements between individual nations, each

state accepts to be responsible for the certification of its own airlines against the applicable standards and recommendations.

Airports
For airport operators (for short airports), the business role is to provide services to passengers and airlines. There are airports that are paid by the state to provide these services. There are three safety critical services to be considered: security checks of passengers and their belongings, service provision to aircraft on the airport, and protecting the environment (3rd party accident risk). For the last, national rules have been established, which may vary significantly from nation to nation, and vary from prescriptive to goal-setting. For the other two, international recommendations have been established by ICAO. These international rules are of a prescriptive nature and may concern systems, procedures and staff.

2.5 Products and services to airlines and airports

In Figure 3, manufacturers, ATM service providers, and several other service providers appear one level further from passengers than airlines and airports. Obviously, this does not mean that their safety-related role in civil aviation is less important. Only their distinct impacts on safety for passengers are brought into the process through their relation with airlines and airports. For each of these actors, an impression of these relations is shortly described below.

ATM service providers
With the growth of ATM service provider corporations during the last decade, the business role of ATM service provision has become clearly visible, providing effective services to airlines. Traditionally, ATM service provision within a nation's airspace was performed by its civil aviation authority, in line with ICAO standards and recommendations. As such there still are ATM service providers that are paid by the state (e.g. USA) to provide these services. Within ECAC states there is a steadily increasing impact by the harmonisation efforts of EUROCONTROL. Also here, the operational requirements are of a prescriptive nature and address how to organise air traffic within national boundaries, and how the ATM ground crews should make use of particular new procedures and systems under some typical conditions. National authorities are internationally obliged to assure the provision of adequately safe ATM services. This implies that some form of certification is presently enforced upon ATM service providers (see Figure 4).

Manufacturers
The business role of manufacturers is to deliver and integrate systems (consisting of hardware, software and related services) to airlines, airports, ATM service providers, etc. Due to the international nature of air transport, the need for world-wide interoperability of airborne systems has resulted into a well developed chain of standardisation organisations, which runs from ICAO (SARPs) through JAA/FAA (JARs/FARs) and EUROCAE/RTCA/SAE (MASPS, MOPS) to ARINC (interface specifications). The resulting requirements are of a prescriptive nature. In several countries, the national civil aviation authorities are capable of controlling and

certifying that the development of new airborne products is being done in line with these standards. For non-airborne ATM/CNS applications, the tendency is that the development of standards follows a similar route with involvement of EUROCONTROL. This is particularly the case for telecommunication developments. Currently there is not a kind of certification process enforced upon manufacturers of non-airborne equipment; this would be a problem anyway for COTS products [ARIBA-WP3].

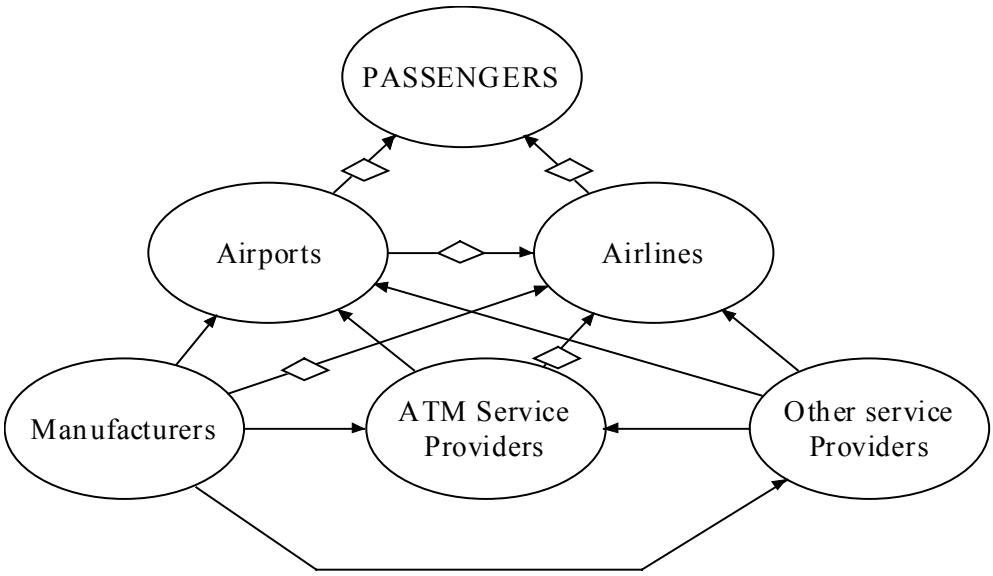


Figure 4: The products/services that fall under some existing form of certification by the provider are identified by white diamonds.

Satellite-based navigation service providers

The existing satellite systems are property of a few states, with military applications as primary objective. The services provided by those satellite-based systems can be used freely. This means there is no possibility to place extra requirements on these services themselves. What can be done, however, is to put requirements upon the providers of augmentation services, e.g. WAAS, EGNOS, which are aimed at enabling wide-spread civil aviation use of the military systems. For these services, standards are being developed by RTCA and EUROCAE, e.g. [EUROCAE, 1998].

Telecommunication service providers

Provision of telecommunication services occurs on a contractual basis, through which quality requirements on service performance are in principle accessible and negotiable. For example, INMARSAT provides validated dependability characteristics of their services. Obviously, civil aviation has become very dependent of telecommunication services. Notable examples are Airline Operational Centres that communicate with their aircraft all over the world. There is one particular area where the use of these telecommunication services has not found introduction yet. This is the area of communication between pilots and air traffic controllers.

Weather service providers.

Provision of weather service occurs on a contractual basis. As such, quality requirements on the service provision can be negotiated.

2.6 Standardisation

In civil aviation there is the internationally recognised need for civil aircraft that can operate world-wide in a predictable way. This has resulted in the evolution of an international standardisation process. It is this international standardisation process that provides the basis for national authorities to arrange through bi-lateral or multi-lateral agreements that the internationally accepted standards on aircraft, airborne systems, flying procedures and aircraft crew are being enforced by all states. The relations between the main actors involved with this international standardisation process are presented in Figure 5. In addition to these actors, there are the more general standardisation bodies like CEN, CENELEC and ETSI.

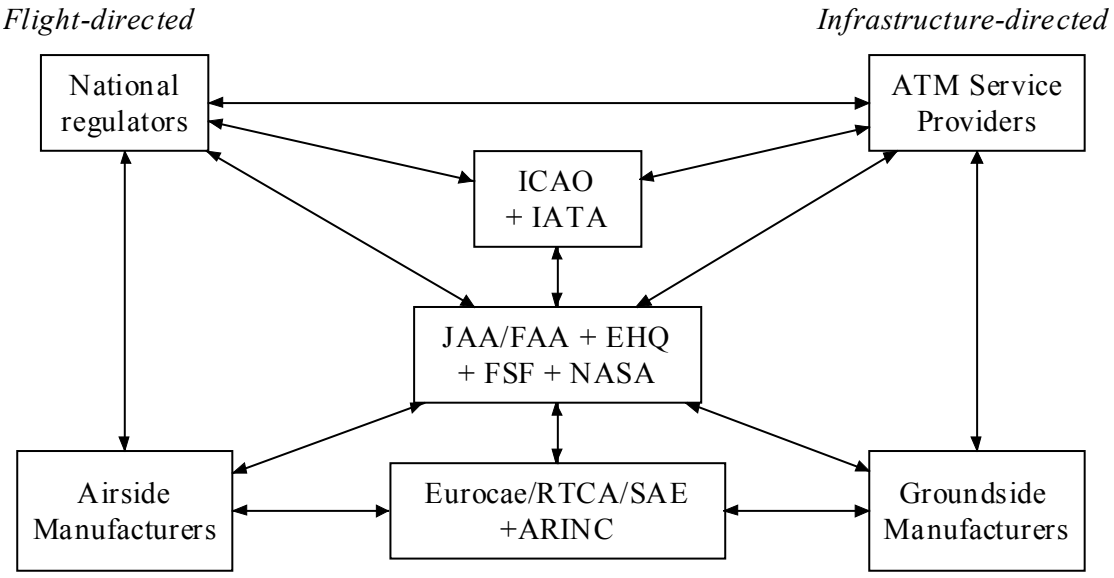


Figure 5. Impression of main relations in current standardisation for civil aviation.

The actors situated at the left-hand side in Figure 5 are involved in the flight-directed standardisation, while the actors situated at the right-hand side are concerned with the standardisation of the infrastructure. It should be noted that the National regulators and the ATM service providers often are both within the national civil aviation authority. Traditionally, the regulatory authorities mainly direct their attention to the flight-directed side of the standardisation process, while they often transfer infrastructure-directed standardisation activities for a large part to ATM service providers, for the simple reason that the necessary expertise is with them. As such, ATM service providers often have to represent the interests of other actors in the infrastructure standardisation process. The international standardisation process forms the cornerstone of the existing certification paradigm in civil aviation [O'Neill, 1998]. At first sight, one might suggest to copy the approach in use at the left-hand side to the right-hand side. Unfortunately, the standardisation process in use at the left-hand side is particularly weak on issues that are crucial for the infrastructure:

- The current standardisation process is so much directed to technical systems that there is insufficient place for an elaboration of standards from a human controlled mission perspective.

- The existing standardisation process appears to fall short for quite a number of new technology based services for which the paying customer(s) largely come from outside civil aviation, such as Telecommunication services and Satellite-based navigation services.
- The active participation of the actors that are closest to the passengers, i.e. airlines and airports, is rather limited. The likely explanation for this situation is the classical belief that national authorities are well capable of protecting the interests of the different types of actors.
- The development of a new concept of operations is currently largely done on the basis of existing service experiences. This places severe limitations on the timely acceptance of advanced operations.

3. Good business practices in routine operation

As far as safety assurance can be arranged on the basis of the best business practices that are known from other safety critical domains, this should be done. As such, it is quite logical to adopt good business practices first. In this section, routine operation is considered. The next section considers advancing ATM operations.

3.1 Safety Management

If the safety criticality of a product, an operation or a service concerns human society, then it is quite common that national regulation enforces some form of safety assurance for that product, operation or service. Typical examples are Pharmaceutical products, Nuclear plant operation and Ground transportation services, e.g. [ARIBA-WP2]. During the last two decades, the safety management thinking has rapidly evolved by positive experiences in various safety critical domains. This can best be understood by summarising the experience gained in the petrochemical offshore industry, as described in [ARIBA-WP3]. The classical safety assurance by an operator of an offshore petrochemical plant was aimed at maintaining adherence to the prescribed requirements to systems, procedures and crew. Thus, to put a new or changed petrochemical plant into operation, the operator of that plant had to show that all prescriptive requirements on the operations were satisfied, and that the operator showed to be capable of maintaining that situation, in order to receive a certificate from the national authorities. It was the report by Lord Cullen [Cullen, 1990] on the Piper-Alpha accident of 1988 that made clear that for complex safety critical operations there was a need to introduce two major improvements: 1) replace the prescriptive requirements by goal-setting ones (e.g. in terms of risk), and 2) implement appropriate safety feedback loops at all management levels. Quite rapidly, these recommendations for change have successfully been put into practice, first within the UK for the petrochemical industry, and subsequently also elsewhere (e.g. Australia, The Netherlands, Malaysia) and for other safety critical operations, such as ground transportation and nuclear plants.

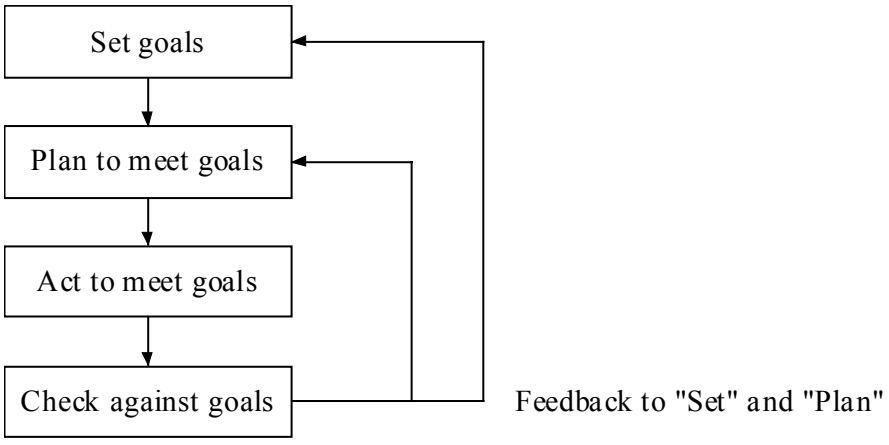


Figure 6. Safety Management process.

3.2 Airlines, airports and ATM service providers

Airlines, airports and ATM service providers are all logical candidates to adopt a goal-setting safety management approach, for the simple reason that they are the commercial actors that are directly responsible for the provision of safety in civil aviation. Based on experience in other domains, the implementation of adequate safety management approaches by airlines, airports and ATM service providers simply is a matter of following good business practices. As such, it is really important that all airlines, airports and ATM service providers are becoming convinced as soon as possible that the very positive practical experiences seen in other domains are no artefacts, but typical results of implementing goal-setting safety management for a complex safety critical operation. It should become clear that it is good business for airlines, airports and ATM service providers to take the hurdles in adopting a goal-setting safety management approach. Some airports, ATM service providers and airlines have already started to take these hurdles (e.g. [Overall, 1995]; [Profit, 1995]; [UK-CAA, 1999]; [SAPCOM, 1998]; [Wood, 1997]; [Mayes, 1997]). During recent years the safety management implementation development has received widespread attention in ATM (e.g. [EHQ-SYMP, 1997]). As a result of this, it has now widely been recognised that the implementation of Safety Management by ATM service providers is a major step in a harmonisation approach towards improving safety.

The main hurdles to be taken are the development of safety goal settings that are in line with national and international standards and requirements, to create a safety awareness culture at all levels of their organisation, and to develop ATM directed incident monitoring facilities. An important contribution from policy makers is to actively support those actors in taking the safety management implementation hurdles. By developing management goals that are not in conflict with national and international standards and requirements, the ATM service providers and airports might even have the opportunity to guide the international standardisation process (and thus stay ahead of it). It should also be realised that safety management is complementary to quality management and Crew / Team Resource Management. Moreover, safety management is much more demanding than quality management.

For airports and ATM service providers, their safety management approach would imply to contractually require (dependability) validation for the private sector products and services from their telecommunication service providers, their manufacturers or their weather service providers. The main limitation would be that this can not immediately be arranged in case competition is insufficient (e.g. telecommunication services). In view of the rapid developments in the telecommunication area, one could expect that these limitations would disappear over the coming years.

Unfortunately, a similar contractual approach does not work for the main providers of products and services to airlines:

- Requesting more than the JAR/FAR certificates from aircraft directed manufacturers should be done by means of the national authorities, and they are rather limited in effectuating such requests.

- Requesting special services from ATM service providers and airports is also rather limited for the very reason that the service provision often is provided on the basis of international agreements rather than contracts.
- Satellite-based navigation service providers are currently not interested in offering contractual services.

3.3 Impact on Other service providers and ATM/CNS manufacturers

The best business practices for individual actors can be summarised as follows:

1. The use of modern safety management approaches should be adopted by the main air traffic services directed operators like airlines, ATM service providers and airports.
2. Goal-setting standards should be developed that are not in conflict with the international standards.
3. ATM service providers and airports should contractually demand and survey a sound safety validation from crucial manufacturers and service providers.
4. If possible, airlines should contractually demand and survey a sound dependability validation from other service providers.

Application of these good business principles to Figure 2, leads to the improved situation, depicted in Figure 7.

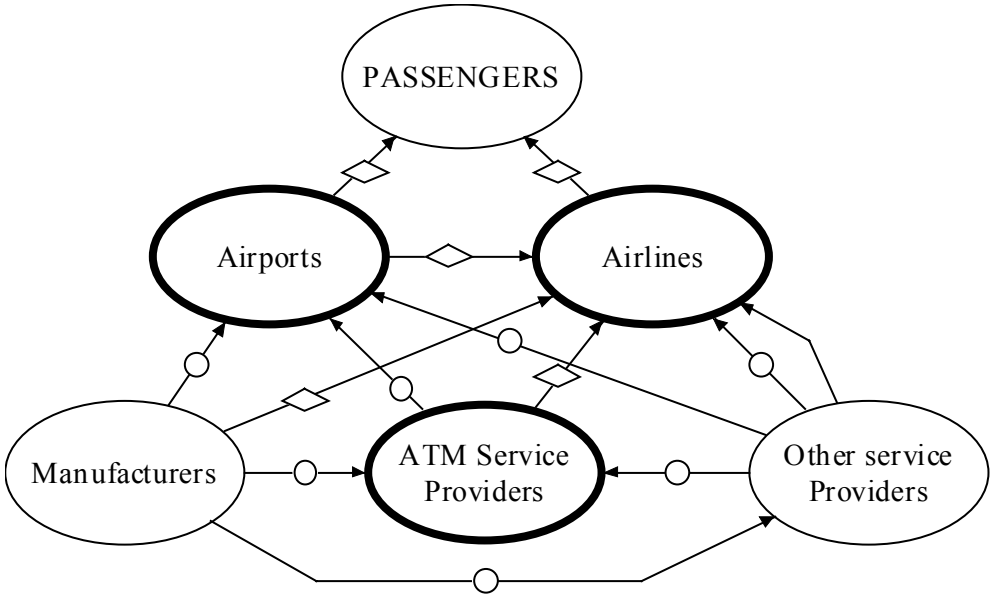


Figure 7. Following good business practices. Actors who have a good business reason to adopt a modern safety management approach are in bold ovals. The potential products/services for a contractually arranged safety validation during the procurement of a product or service are marked with circles. The products/services under some existing form of certification are marked with white diamonds.

Figure 7 shows that with the introduction of modern safety management approaches the safety assurance in civil aviation would be improved significantly. However,

significant weak areas still exist, in particular where airlines receive services from Other service providers.

3.4 Proactive Safety Management

Having realised the evolution from a prescriptive approach to a goal-setting safety management approach, the next major improvement in safety management thinking has been promoted by top management of the petrochemical industry [ARIBA-WP3]. Upon having a goal-setting safety management approach in place, it was noticed by top management that the remaining accidents were mainly due to "strange" causes. Thereupon, top management set up a program in order to first understand the problem, and subsequently to develop an adequate approach to capture such undesired situations. The "strange" causes appeared to be latent hazardous conditions [Reason, 1990], [Reason, 1995] which could reasonably not have been imagined before. Subsequently, this problem has been alleviated by the development and subsequent incorporation of proactive safety feedback loops, e.g. [Hudson, 1994], that are aimed at identifying latent hazardous conditions during routine operation, without the need to first await an induced incident or accident. Being completely in line with good business practices, these proactive extensions could be developed even if there is no certification requirement for doing so. It is very likely that once goal-setting safety management is in place, then top management of airlines, airports and ATM service providers will also support the extension of their safety management with pro-active feedback loops. With some airlines this has already started.

In order to illustrate the significant differences between a prescriptive safety assurance philosophy and a pro-active safety assurance philosophy, in the next table some typical characteristics of both are given for civil aviation, following [Pariès, 1996]. Additional information can be found in [ICAO, 1996] and [Hudson, 1996 & 1997]. As we have mentioned before, it takes significant efforts from airlines, airports and ATM service providers to evolve from a prescriptive approach to a well working reactive safety management approach. From then on it is another significant development to evolve further towards embedding pro-active safety feedback loops within a reactive management approach. In [ARIBA-WP3] it has been analysed that significant benefits could be expected for e.g. air-ground and ground-ground voice communication, Commercial Off-The-Shelf software and air-ground data-link.

Table 2 Two fundamental philosophies in the safety paradigm [Pariès, 1996]. The first philosophy supports a prescriptive safety assurance approach. The second philosophy supports a pro-active safety assurance approach. The baseline goal-setting safety assurance approach falls somewhere in between these two.

Philosophy #1	**Philosophy #2**
Aviation operations can be entirely specified through standardised procedures, programs, schedules, rules, nominal tasks, certification, selection, norms, etc.	Aviation operations cannot be entirely specified through standardised procedures, programs, and the like. One reason is that they include humans.

Safety results from the nominal (i.e. as specified) operation of the system	Safety results from the dynamic stability of the system.
Safety improvement will result from more specification (more extensive, comprehensive, and detailed procedures, etc.) and more discipline	Safety improvement will result from a better respect of the "ecology" of the system and a better acknowledgement of its auto-control processes.
Deviations from nominal operation are both a cause of lower performance, and the main threat for safety.	Deviations from nominal operation are both a necessity for adaptation to random dimension of real life, and a potential threat for safety.
Human operators are ultimately the only unpredictable and unspecifiable components of the system. They are the main source of deviation.	Human operators are up to now the only intelligent, flexible and real time adaptable component of the system. They are a deposit of safety.
Automation, whenever feasible and reliable, will decrease deviation rate and therefore improve both performance and safety	Automation will increase reliability, improve performance, make the operation more rigid, and create new problems in man-machine coupling.
Errors are non-intentional deviations from standard actions. Errors are inevitable	Errors are deviations from intentions, but at the same time they participate in the normal process of achieving intentions. Errors are necessary.
Errors are just as negative for safety as any other deviation. Any effort should be made to reduce the number of errors.	Uncorrected errors may be a threat for safety. Self-error awareness is a critical governor of operator's behaviour and risk management.
Incidents are a sub-set of accidental sequences. As such, they are accident precursors. Prevention based on incidents is reactive.	Incidents are normal episodes of local instability in complex systems operation. They blow up into accidents when they are not dampened and start resonating with local circumstances.
The system is a set of "black-boxes" coupled through inputs (perceptive data) which are transformed into outputs (actions) according to specified targets (goals) using adequate transfer functions (procedures, skills, etc.)	The system is a network of auto-organised structures, coupled through recursive processes of self-reproduction, and ultimately governed by their internal attractors.
Feedback is a deviation detector allowing for system operation corrections with reference to an external target.	Feedback leads to short and long term dynamic stability through adjustment of internal "goals" and "self-representations", learning process and immunisation.

4. Good business practices in advancing ATM

By its very nature, ATM is an activity that is highly distributed over multiple commercial actors (airlines, airports and ATM service providers), and multiple human controllers (a flight crew in each aircraft and controllers in each ground centre). In this section we will show that good business practices ask from the commercial actors to collaborate on the development and validation of advances in ATM. For this, a learning path from best practices in other safety-critical domains is not available.

4.1 Advancing product line development

The advances in ATM/CNS development lead to significant opportunities and challenges for the manufacturers. The challenge is to timely anticipate the evolving needs of their potential customers with their product line development. From the manufacturer's management perspective there are potentially three ways to satisfy the needs of the potential customers:

- The customer needs can be satisfied by the manufacturer's existing product-line and validation facilities.
- The customer needs can not be satisfied by the existing product-line and validation facilities, but there is objective evidence through prototypes that can be accommodated by the newly planned product-line and validation facilities.
- There is no prototype-based evidence that the customer needs can be satisfied by the newly planned product-line and validation facilities. However, technologically it is believed feasible to extend the prototypes and validation facilities developments such that the required needs are satisfied. Obviously, this involves an investment risk for the manufacturer.

Obviously, manufacturers are in need of a healthy balance in the frequencies at which risky and non-risky procurements are requested, otherwise the lifetime of a newly developed product-line would become too short to even balance the investments. Currently, the uncertainties in the future needs of airlines, airports and ATM service providers are such that manufacturers tend to be reactive in their development of new products. It is the joint interest of manufacturers, airlines, ATM service providers and airports to see this situation improved. Manufacturers also would like to receive a certificate from a third party for a successfully procured system.

It is sometimes believed that this could be realised just by developing MASPS and MOPS for ground systems, in a way similar to how this is done for airborne systems. Experience with airborne equipment, however, shows that much standardised functionality stays unused by civil aviation as long as there is no joint view on the practical use by the key actors involved. It is also important to realise that the same problem exists in the USA; in spite of its large civil aviation market with one FAA and one unified ATM system [RTCA, 1999]. The key explanation is that the flight-directed side of the standardisation process currently in use is particularly weak on issues that are crucial for the infrastructure-directed side, and that the improvement of this situation largely falls outside the reach of manufacturers alone. Thus, the best

business practice is that airborne-directed and ground-directed manufacturers collaborate on this with each other and with the actors who play a key role in infrastructure-directed developments.

4.2 Advancing automation requirements

Airports and ATM service providers should contractually require (dependability) validation from their manufacturers during procurement of a new system. Although this might suggest everything might run smoothly, in practice it too often happens that the procured system does not perform to the satisfaction of the client. There are many possible reasons for such dissatisfaction:

- the system does not fully satisfy the requirements, or
- the requirements appeared to be inconsistent or incomplete, or
- are in unbalance with the capabilities of the human controllers, or
- the requirements do not support the needs of the operation
- the available validation facilities appeared to fall short in performing the required types of performance assessments.

In any case, the client then has three options:

- The manufacturer gets more time to satisfy the client needs.
- The client can no longer wait, and therefore accepts the system as it is.
- The client cancels the whole project with this manufacturer.

Experience shows that for automation projects in core ATM areas, these undesired situations do happen even with very capable manufacturers and clients. Structural problems of this kind have affected several major ATC renewal projects and different suppliers on both sides of the pond.

To avoid such undesired situation, a procurement contract should be based on validated requirements for the human controller's qualification/training aspects, the procedures, the automated systems and the maintenance. It should be noticed that, in this context, (dependability) validation of requirements has four meanings:

1) In the sense that the requirements have shown to be in conformance with the goals of the operational improvements.
2) In the sense that the requirements assumed on human controller performances are realistic (can be learned by adequate human resource management).
3) In the sense that the requirements are sufficiently measurable with help of validation facilities.
4) In the sense that the requirements have shown to be complete and consistent.

Potentially, there are three ways to get such validated requirements:

- The client needs can be satisfied by an already validated operational system. In that case it is sufficient to procure the same system.
- The client needs can be satisfied by a validated prototype system. In this case it is possible to adopt the validated requirements that are known from the validation reports on the prototype.
- The client needs can not be satisfied by a validated operational or prototype system. In that case there is need to set up a prototype development, an overall

validation of that prototype against the client goals, and a translation of the resulting prototype in objectively measurable requirements.

The current practice is that the client needs for many ATM service providers and airports in the core of Europe and North-America are so demanding that the last situation applies. This means there is a definitive need for these clients to join forces on the timely development of validated requirements for airlines, airports and ATM service provision and validation facilities, prior to any procurement by one of the participating clients. For example, by supporting developments of new operations, technology and validation methodology (e.g. [MacLeod & Taylor, 1994], [Maurino & Galotti, 1994], [Javaux et al., 1994], [Wickens et al., 1997], [Josefsson, 1999]) and by the simultaneous development of appropriate benchmarking processes to allow an objective comparison of the various performances realised. Such learning experience will also contribute significantly to the timely development of industrial standards and their product lines by the manufacturers and provide a sound basis for manufacturers to ask for a "voluntary certification".

4.3 Advancing actors' goal settings

The introduction of safety management thinking by airlines, airports and ATM service providers may easily create an increasing tension between individual actors due to the desired evolution in goal-settings and operational solutions. It is for example quite important that the safety targets aimed for within Europe do not vary significantly from one nation to another. At this moment, different proposals for setting safety targets co-exist in different ECAC states [EHQ-SAM, 1999], although they are all based on the same JAR severity/frequency requirements. The explanation is that these JAR requirements leave an order of magnitude ambiguity both in severity and in frequency (see e.g. [Lloyd and Tye, 1982], and have not been developed for human controlled operations (e.g. [Klompstra and Everdij, 1997]; [RTCA, 1999]).

In order not to jeopardise the valuable world-wide standardisation process, airlines, airports and ATM service providers should also be actively involved in the harmonised evolution of both individual and joint actor's goals at the national, regional and international levels, such as depicted in Figure 8.

Even at the national level, the co-ordination between air traffic operation directed actors already involves the policy makers, regulators, airlines, airports and ATM service providers. The same variety of actors should also be involved at the regional and international levels, since pilots from various countries have to collaborate with controllers all over the world. The airlines, airports and ATM service providers should collaborate on the joint identification of their actor goals under various operational concepts and against jointly elaborated high level objectives for various air traffic demands and environments. To support such collaboration the following recommendations can be made:

- The safety management approaches by the commercial actors should be integrated, and be made transparent to relevant organisations.
- Operational goal setting should be co-ordinated between policy makers, regulators, airlines, ATM service providers and airports.

- An approach should be developed to significantly improve the operational goal-setting and collaborative feedback process at regional and international levels (e.g. [Fron, 1998]).
- For advanced operations it may be required to redefine responsibilities spread over various actors.
- Collaborate on the further development and integration of Crew/Team Resource Management approaches.
- Collaborate on the development and application of proactive feedback loops, embedded within safety management.

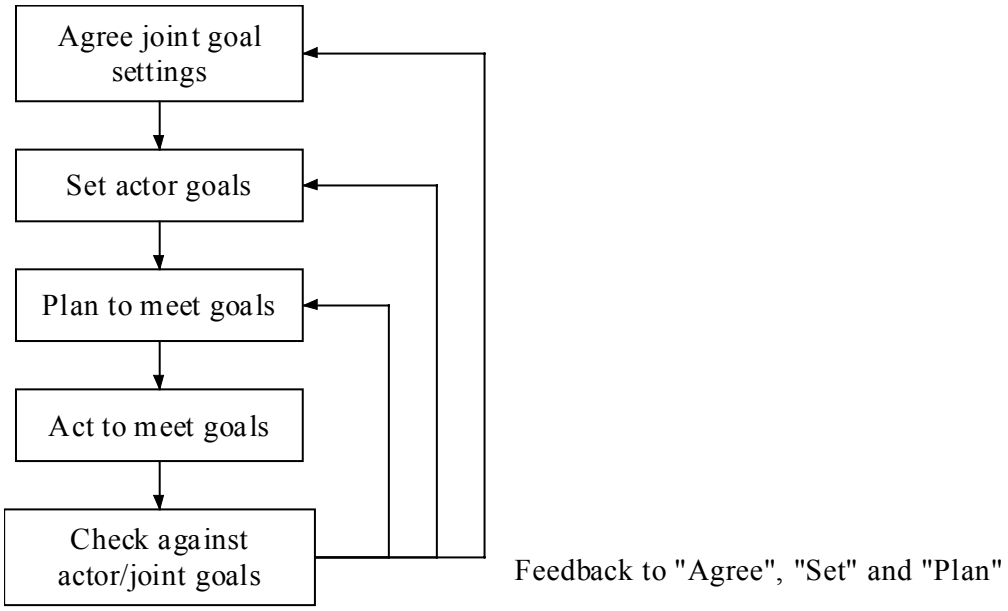


Figure 8. Integration of Safety Management processes in air traffic is enabled by goal-setting co-ordination at national, regional and international levels, and by the exchange between collaborating actors of adequate safety feedback at all management levels.

4.4 Advancing operational concepts

Major decisions to be made in civil aviation are concerned with how to best exploit technological enablers to improve air traffic operations for various types of air spaces, in terms of the high level objectives such as Safety, Capacity, Efficiency, Economy, Uniformity, National security, Environmental impact and Human factors. These high level objectives can not be reached as the sum of the improvements by individual actors; they ask for some joint optimisation and validation of new operations and individual actor goals for various air traffic demands and environments. Such joint optimisation starts already with handling the problem to jointly develop metrics for each of the high level objectives. As depicted in Figure 9, there is a clear need for interaction between advancing operational concepts, defining commercial actor goals, developing automation requirements, developing product lines, and with Crew/Team Resource Management as key connecting issue (e.g. [Helmreich, 1996], [Barbarino et al., 1999]).

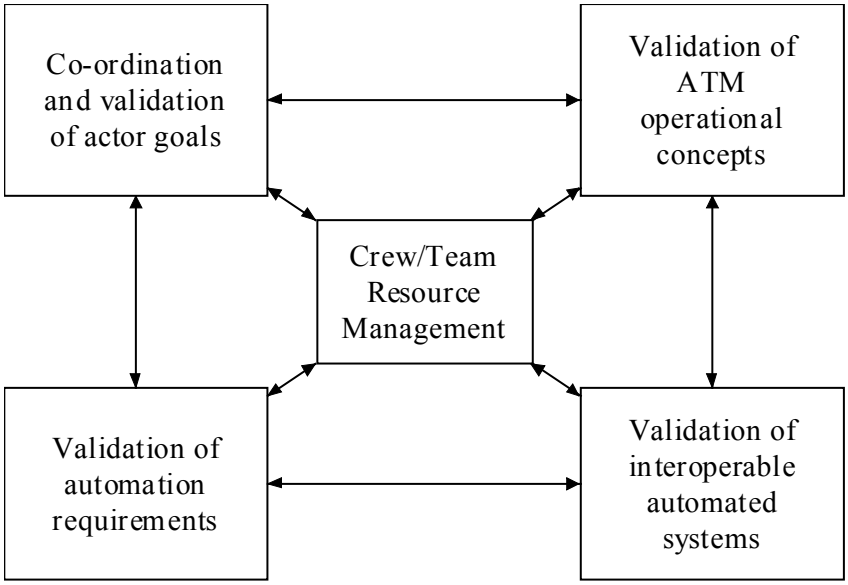


Figure 9. ATM advancements that ask for collaboration in the area of validation, and with human controller capabilities (for pilots and ATCo's) as a key connecting issue. There is no best practices learning path available from other domains.

With the current regulatory oversight, the emphasis is on bottom-up approaches at the right-hand side of the figure. For the development and validation of actor goals and automation requirements at the left-hand side it definitively would be preferable to do so in parallel with the development and validation of new operational ATM concepts, automation requirements and technological advances (e.g. [Wise & Wise, 1994], [Koelman, 1994], [Amalberti & Wibaux, 1994]). To illustrate this, consider a new operational concept that initially may be safely put into practice with the current, relatively large spacing between individual aircraft, thus initially not allowing any traffic load increase. Later on, when the new operation and safety management for that operation has been sufficiently further developed, then the applied spacing between aircraft might be safely reduced. This means that validation of a new operational concept, which is introduced to accommodate relatively high traffic demands, is inevitably related to the establishment of safe spacing standards.

Top management of airlines, airports and ATM service providers have a joint interest in the availability of decision-support tools to pro-actively manage the joint development of advanced ATM operations (e.g. [MUFTIS, 1996]; [Haraldsdottir, 1997]; [Odoni et al., 1997]; [ICAO, 1998]). In view of the complexity of ATM operations, a pro-active type of approach towards safety is to apply a safety assessment that is able to show how the various distributed entities in ATM could interact in non-nominal behaviour, and that is able to model the human capabilities and limitations such as identified in the right-hand-side column of Table 2. In addition, appropriate decision-support tools for other high level objectives of various actor types should be incorporated (e.g. [EHQ-EVAS, 1998]).

5. Modernising safety certification

In this section, an analysis is made of the needs to enforce elements of a safety certification regime on actors in civil aviation.

5.1 Safety Certification process

For various safety critical products, services or operations, the safety judgement is in general based on a series of documents describing the results of a safety **validation** process (ISO terms are bold printed; see Annex A for their definition). Such a series of documents is often referred to as a Safety Case, with the top level documents providing the argumentation and with the other documents providing the supporting evidence. Inherent to the general definition of a Safety Case, there is a whole spectrum of possible Safety Cases. As is explained in [ARIBA-WP5], it is quite well possible to build different safety cases for a single product, service or operation. Each of these safety cases is then valid under particular conditions, which may depend on e.g. site, operation, life-cycle phase, etc.

From experience in other safety critical domains [ARIBA-WP2], the various entities who participate in the certification process can be identified as follows:

- There often is an International organisation (e.g. ICAO, JAA, EUROCONTROL)[1] which harmonises the **regulations** and **standards**.
- There is a higher authority (e.g. national regulator, EUROCONTROL)[1] which has by law the responsibility to approve and further elaborate **regulations** and **standards**
- There is a **certification body** (a legal or administrative entity accredited by a higher authority) that provides a formal approval (or certificate) in case a product, service or operation conforms to **regulations** and **standards**.
- There is a safety auditing body (a third party accredited by a certification body) that conducts a safety **qualification process,** on the basis of the available Safety Case, in order to evaluate whether the product, service or operation is capable of fulfilling specified requirements.
- There is an applicant (e.g. a manufacturer, ATM service provider or airline) who wants to receive a formal approval (or certificate) for a product, service or operation that falls under a safety **certification** regime.
- There are safety and domain experts (e.g. specialised institutes or consultants) to support the applicant in the building of the Safety Case for a product, service or operation through an effective safety **validation** process.

The safety related certification process proceeds according to the following steps:

1. On request of the applicant, the Higher authority launches a certification process for a new or changed product, service or operation, and tasks a certification body to guide the certification process.

[1] EASA could play key roles in the future.

2. The applicant tasks safety and domain experts with the building of an appropriate Safety Case.
3. The certification body tasks a safety auditing body to conduct a qualification process on the basis of the Safety Case provided by the applicant. Some iteration may be needed to improve or modify the product, service or operation and the Safety Case before the qualified status is reached. The safety auditing body sends a qualification process report to the certification body.
4. The certification body judges the Safety Case and the qualification process report, and delivers a formal approval for a limited period (or asks for more informaton).

5.2 Modern Safety Case

The Safety Case thinking has evolved in parallel with the safety management and certification thinking. This can best be explained by looking again at the petrochemical offshore industry example considered in [ARIBA-WP3]. The original certification regime for an operator of an offshore petrochemical plant posed requirements to the systems, procedures and crew, which were of a prescriptive nature. To put a new or changed petrochemical plant into operation, the operator of that plant had to build a Safety Case for approval by the national authorities. This Safety Case had to provide the high level arguments and the supporting evidence that for each normal and failure mode of that plant, the combination of frequency of occurrence and severity of effects was acceptable.

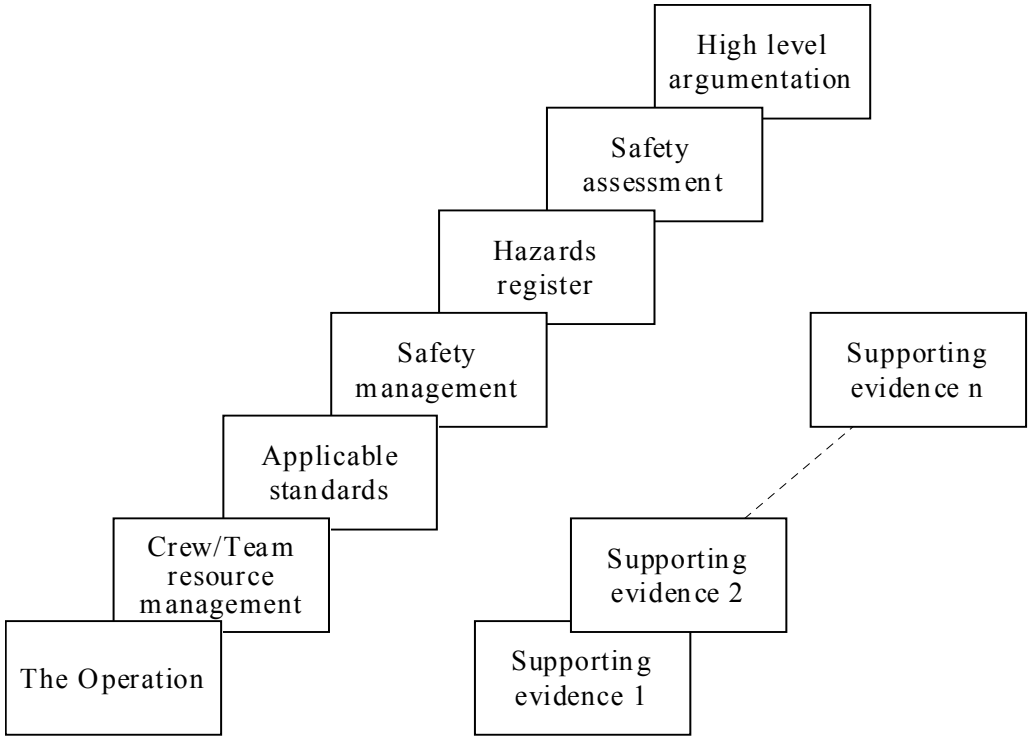


Figure 10. Modern Safety Case under a goal-setting certification regime takes Safety Management and Crew/Team Resource Management into account.

The adoption by the petrochemical industry of a goal setting safety management approach has had a major impact on Safety Cases. While under the prescriptive regime, a Safety Case tends to provide a instantaneous picture of the possible failure modes and their effects, under a goal-setting certification regime the scope of a Safety Case is much wider: 1) it is aimed to cover all hazards, rather than failure modes, and 2) it takes the impact of the safety management approach of the responsible actor into account. Thus, as outlined in Figure 10, a Modern Safety Case incorporates the description of the safety management approach and a hazard register. An additional extension for civil aviation is that it should take into account Crew/Team Resource Management.

A Modern Safety Case is a living document that is being updated on a regular basis, for example when new hazards have been identified and assessed. The coverage of hazards rather than failure modes is particularly important if human operators are in the loop of safety critical services or operations, since in those cases most hazards are not of the failure mode type. It should be remembered that a safety case should serve as a guide in improving safety at the physical level. This means continually updating and verification of its application.

A complementary recent development is that top level management has recognised the Modern Safety Case as a valuable decision-support management tool during all life cycle stages of a safety critical operation [e.g. Short, 1998]. For example, during the conceptual development stage of a new safety critical operation, top level management may have to make a decision with respect to further improving the design first, or starting the preparation and procurement for the operational implementation of a new or improved operation. In order to be fully informed, top level management rather needs the complete picture provided by a Modern Safety Case, than the partial picture provided by several technical evaluations. A related development is that, for a safety-critical operation, insurance companies reduce the insurance premium if a Modern Safety Case is available, e.g. in Petrochemical industry.

5.3 Enforcement on commercial actors

The next question is if safety management and Modern Safety Case approaches should be enforced by national authorities and upon which commercial actors. Similar enforcement often exists for other safety-critical operations such as in the nuclear industry and railway transportation [Short, 1998]. Since national authorities have the international obligation to support the provision of safe services to civil aircraft within their airspace (e.g. [Henaku, 1998]), they also have good reasons to improve the certification regime for airports, ATM service providers and Other service providers, where possible and useful. Since safety management is a matter of good business practice, it would be logical for national authorities to enforce adequate safety management approaches by their national airports and ATM service providers. Enforcement means (e.g. [UK-CAA, 1999]) that the national regulatory authority conducts in-depth surveys of their safety management approaches and how these are

used in practice. For the other service providers this might be unrealistic if their core business is outside civil aviation.

With respect to enforcing Modern Safety Cases from airports and ATM service providers for a change in equipment or internal procedure, however, the situation is less straightforward for several reasons:

- National regulators should first develop/agree safety goals for the individual actors. This issue deserves urgent attention anyway.
- National regulators have limited resources to conduct (or to let conduct) an objective **qualification process** on the basis of a Modern Safety Case, while they do become responsible once an accident could have been prevented by timely identification of a flaw in the Safety Case.

In order to avoid the major effects of all these complications, initially Modern Safety Cases could be enforced on airports and ATM service providers as a safety management tool, and where the responsibility of the regulator might initially be limited to:

1. Evaluating the conformity of the goal settings and operational standards used in the Safety Case against the goal settings and operational standards in use by other actors involved.
2. Verifying that the Safety Case documentation is complete and consistent.
3. Verifying that all methodology used while building the Safety Case has been accepted as part of the Safety Management system.
4. Verifying that the automation requirements placed on the human controllers have been validated in the sense of being within the scope of a well-trained human controller.
5. Regularly conducting an in-depth survey of the safety management approach, and verifying that all safety cases are kept up to date and are truly used as a guide to put things into practice.

In practice the above means a kind of “self-certification” of a Modern Safety Case by ATM service providers and airports. It is currently not clear if this “self-certification” of Modern Safety Cases is sufficient on the longer term.

It is not impossible that economic drive causes operations to be pushed to the legal limits. Therefore, public authorities should retain the right to determine the degree of mandatory requirements in key economic sectors where public safety assurance is important. In [UK-CAA, 1999] such is arranged for. This is a pre-requisite for policy makers to develop a more liberalised approach in the ATM sector, which facilitates competition. “Self-certification” of a Modern Safety Case may be appropriate for some functions, but safety regulators will need oversight and qualification powers to investigate further if they feel there are public interests to assure survey (failure examples of self-regulation scenarios on the other domain exist, unfortunately). Thus, it might be needed that national authorities collaborate on the development and application of a harmonised **qualification process**, in order to accomplish that the initial “self-certification” of Modern Safety Cases could evolve to the full certification process of Subsection 5.1. Obviously, the Modern Safety Case approach is able to serve any certification form.

In conclusion, airports and ATM service providers are good candidates to enforce a Modern Safety Case for a change of equipment or a procedure. Best would be to adopt this enforcement for all ECAC states. The effects of enforcing Modern Safety Case regime on airports and ATM service providers are depicted in Figure 11.

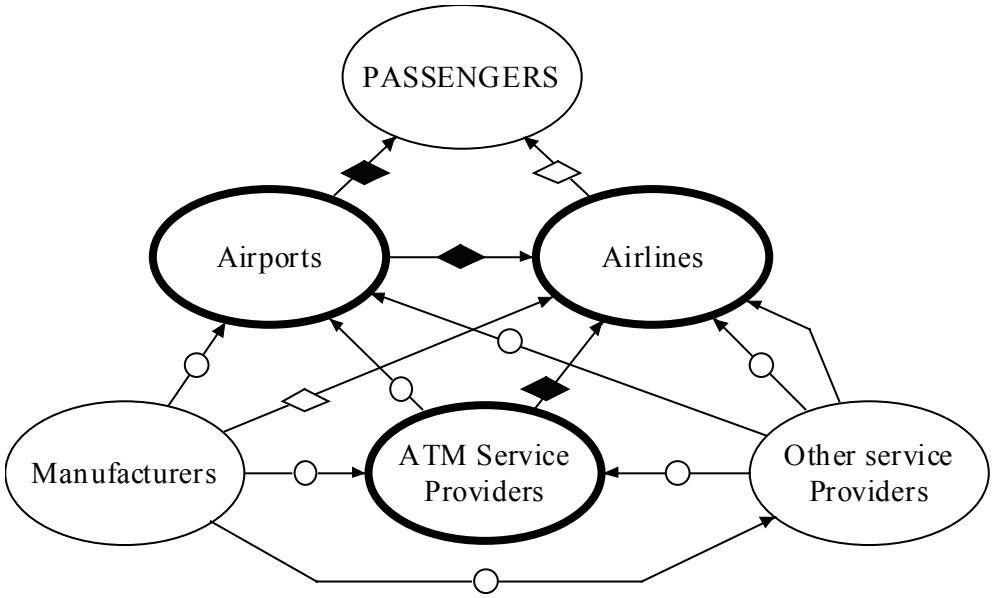


Figure 11. Actors who have a good business reason to adopt a modern safety management approach are in bold ovals. It would be logical to enforce a modern safety management approach on airports and ATM service providers. The services that are candidate for enforcing a Modern Safety Case regime are marked with black diamonds. The products/services that are candidates for a contractually arranged safety validation are marked with circles. The products/services staying under the existing certification form are marked with white diamonds.

The figure also shows that once an adequate safety management approach has been enforced upon airports and ATM service providers, within a sufficiently large collection of states, then there would be no need anymore to enforce certification regimes on ATM/CNS-ground equipment manufacturers. The procurement contracts should require them to perform a sound validation, and classical safety case documentation. The airport or ATM service provider should survey whether the manufacturer's (safety) validation is well executed, or should ask a qualified 3rd party (e.g. EUROCONTROL) to do so. The building of a classical safety case by a manufacturer is covered in Part III of the ARIBA consolidation report. Alternatively, a manufacturer is free to ask such 3rd party to conduct a survey and provide a certificate stating that a survey has been accomplished successfully for a particular safety validation of a particular piece of equipment. This is named voluntary certification.

5.4 Joint Safety Case

From Figure 11, it also becomes clear that, even with the best practices from other safety-critical domains, weak links in the safety assurance chain still exist between

Other service providers and Airlines. Basically, the problem is that it is difficult to require a certification regime from an Other service provider that has developed its core business for applications outside safety critical applications in civil aviation. In such case, it would be logical to require the building of a Joint Safety Case by the commercial actors involved. This could be done on the basis of an (occasionally) established collaboration between interested actors (e.g. an airline, its home-airport and its national ATM service provider), all under the approval of a certification authority.

This is just one example of a situation that needs a Joint Safety Case. In Section 4, it has already been identified that there are other needs too for which no good practices are available from other safety-critical domains. Due to the distributed organisation of air traffic, there is ample need for collaboration on validation which creates many more situations for which a Joint Safety Case is the only way out. Many advanced ATM concepts are aimed at increasing capacity (without loss of safety). These advances often have impacts on multiple commercial actors. Examples are:

- Introduce a new final approach procedure, or a wake vortex warning system that aims to reduce the wake vortex separation criteria. The advantage is that the capacity of the airport may be increased on the short term. Disadvantages are that pilots and ATCo's have to learn and train for another new procedure. The crucial question is by how much the separation criteria can be safely reduced. Many commercial actors are involved: at least an airport, an ATC service provider and a few airlines.
- Introduce ASAS in a situation of closely spaced runways. The advantage is that the capacity of the airport may be increased on the short term. Disadvantages are that pilots and ATCo's have to learn and train for using ASAS for this. The crucial question is by how much the separation criteria can be safely reduced. The commercial actors involved are at least an airport, an ATC service provider and a few airlines.
- Introduce direct routing at higher flight levels. An advantage is that this gives more flexibility to the airlines to control their flights between airports. A disadvantage is that pilots and ATCo's have to learn and train for applying this new operation. The crucial question is how the existing separation criteria should be adapted in order to allow a significant and safe increase of traffic flow due to this new operation, and such that it compares favourably to other options. The commercial actors involved are many airlines, and at least an ATS provider.

For each of these examples, the setting of new separation criteria and the feasibility of their safe application by pilots and ATCo's makes part of the problem and thus these aspects should be covered within their Joint Safety Case. As such, the Joint Safety Case should at least show that the concept upon which a forthcoming new or changed operation should be based, provides a sound enough basis to manage all flights sufficiently safe, and without causing significant delay as long as the traffic demands do not go beyond the required capacity. This means that the development of a Joint Safety Case can only be done by taking into account the various high level objectives of the commercial-like actors involved (e.g. C/AFT, 1999). In view of the complexity of this operational concept development process, there is need to do so iteratively:

each re-design is followed by an assessment against the high level objectives, and by a feedback to the operation development design team and their management. On the basis of adequate feedback it will be possible to develop the new operation such that all high level objectives, including safety, are satisfied. This corresponds with the situation of having reached an overall validated operational concept (e.g. [EHQ-EVAS, 1998]) and Business Cases for each of the commercial-like actors involved.

Obviously, the "self-approval" approach that works for a Modern Safety Case built by a single commercial actor does not work in case of a Joint Safety Case. As such, the building and approval of a Joint Safety Case should better be done according to the full certification scheme of Section 5.1. If all actors that build the Joint Safety Case are from the same state, then the national regulator could for example launch the certification process. If all actors are not from the same state, then it would be more logical that the certification process is launched by a collaboration between national regulators (e.g. through EUROCONTROL).

5.5 Availability to the civil aviation community

There are several arguments in favour to make certified Safety Cases in ATM available to the civil aviation community:

1. Without openness, local authorities easily could apply quite different judgements when approving safety management and safety cases of ATM service providers. Leaving this to a central body only (e.g. EUROCONTROL) could become far more effective when openness is required.
2. ATM service provision will stay a public service (privatised or not) to which airlines pay large amounts, while they can not pick themselves one of the service providers. Expecting openness is kind of minimum airlines could ask from them in return.
3. Each non-performing ATM service provider is also putting the airlines/passengers from other countries at risk. If you let the choice to those airlines/passengers from other countries, then they definitively would recommend those non-performing ones could timely learn from the safety knowledge of their own state ATM service provider.
4. It definitively is in the interest of airlines/passengers that ATM service providers effectively collaborate on ATM improvements, and in particular on the development of safe practices. Unfortunately, a direct enforcing of collaboration on advanced developments often works counter-productive. A much better alternative is to enforce publication of ATM developments that are in the interest of airlines/passengers (safety developments definitively are).
5. If service providers are afraid of publishing self-developed/invested IPR then they should seek protection through patents (if they like, this can be done jointly with a manufacturer). This would automatically mean that the new results are becoming publicly known. This way of working is a world wide established practice to promote the cross-fertilisation of advanced developments. In the ATM industry the patent seeking approach seems currently not fully exploited.

In conclusion, there are many advantages for human society of enforcing publication of certified Safety Cases in ATM. Misuse of such safety information can be remedied by agreeing upon a proper code of conduct.

If the certified Safety Cases in ATM are made available to the civil aviation community then there will be an increasing collection of widely available documents describing:

- Certified operational ATM concepts for various traffic demands and environments
- Certified actor goal settings per operational concept under various traffic demands and environments
- Certified automation requirements (human centred) per actor type and operational concept under various traffic demands and environments

These documents might become new regional, national, European or international references if the certification body is recognised respectively at regional, national, European or international level. For all such references applies that if they are valuable, then it is possible that they will be used by actors in other regions/nations and may form a basis for European or International standardisation.

6. Guidelines on safety certification in ATM

6.1 Good business practices

In Part I of the consolidation report, a safety motivated analysis has been accomplished for how to arrange safety certification in ATM. Providing safe ATM service is the responsibility of the ATM provider. The key resources of an ATM service provider to do so are competent ATCo's, appropriate technical systems and proven procedures. Due to the ATCo's competence he/she is able to provide safe services up to a certain level of traffic flow. In effect, ATM safety responsibilities end up with the human elements in the responsibility chain, i.e. the air traffic controllers and pilots. This forms an understandable reason for pilots and controllers to be reluctant to accept any new system or procedure which potentially reduces their controllability of various non-nominally evolving traffic situations, while at the same time their responsibility increases with traffic volume. ARIBA has developed a practical framework to handle this paradoxical development.

The approach taken for this development is the paradigm that enforcing certification can only be effective if it supports good business practices. As such the larger part of the analysis has been directed to the development of an argued framework for improving best business practices in safety by commercial-like actors in civil aviation. This has led to the following findings:

- Airlines, airports and ATM service providers have a healthy commercial interest to adopt goal-setting safety management approaches, and to use Modern Safety Cases for changes in services or operations as an effective safety management tool. For this, much can be learned from other domains.
- Airlines, airports and ATM service providers have a commercial interest to collaborate on the development, validation and integrated safety management of ATM advanced operations, and to develop and apply Joint Safety Cases as an effective tool to manage their collaborative developments. No learning from other domains.
- As much as is possible, airlines, airports and ATM service providers should contractually require and survey (dependability) validation as part of a procurement of a product or a service. Much can be learned from other domains.
- Airlines, airports and ATM service providers have a commercial interest to collaborate with each other and with manufacturers and other service providers on the development and (dependability) validation of advanced automation requirements in ATM. No learning from other domains.

Subsequently, a certification framework has been developed where safety responsibilities are as much as possible arranged according to good business practices. In order to leave the safety responsibilities with the commercial-like actors, the enforced and surveyed safety certification process in ATM could stay rather limited. Obviously, authorities should reserve the right to strengthen their survey when necessary. The main elements of this safety certification process are:

- Enforce and survey Safety Management from airports and ATM service providers.
- Enforce Modern Safety Case from airport or ATM service provider for single actor change.
- Enforce and survey Joint Safety Case for ATM advances affecting multiple actors.
- Make certified Safety Cases available to the civil aviation community.

For each of these certification framework elements, guidelines are summarised below.

6.2 Enforce and survey safety management by airports and ATM service providers

During the last two decades, the safety management thinking has rapidly evolved due to positive experience in various safety critical domains. Since national authorities have the international obligation to support the provision of safe services to civil aircraft within their airspace, they have good reasons to enforce and survey an adequate safety management approach on their airports and ATM service providers (see Subsection 5.3). The main hurdles are the development of safety goal settings that are in line with national and international standards and requirements, to create a safety awareness culture at all levels of an organisation, and to develop ATM incident monitoring facilities (see Subsection 3.2). An important contribution from policy makers is to actively support those actors in taking the safety management implementation hurdles. As soon as an ATM service provider or airport has an appropriate safety management approach working, a follow-up challenge is to incorporate pro-active feedback loops (Subsection 3.4). The development of the methodology to realise such pro-active extension should be done in advance.

For airports and ATM service providers, their safety management approach implies to contractually require and survey a sound dependability validation, documented by a classical safety case, from their crucial manufacturers and service providers, if this is possible. In Part III an outline is given of the methodology for building such a classical safety case by a manufacturer for an ATM automation system. In principle there is no safety need for authorities to enforce a certification regime on ATM/CNS-ground equipment manufacturers (see Subsection 3.3). It should however be possible for ATM/CNS equipment manufacturers to voluntarily request for a safety certification of a product, for a specified operational usage, by a capable 3rd party. The advantage for ATM service providers and airports is that the development risks and costs are better controlled if the safety case is largely known at the time of signature of the contract. Industrial policy makers should support the development of such voluntary certification programmes.

6.3 Enforce and survey Modern Safety Cases from airports and ATM service providers

A Safety Case is a series of documents describing the results of a safety validation process for a change of equipment, process or operation. A Modern Safety Case has a wider scope than a classical one: it aims to cover all hazards, rather than failure

modes, and it explicitly takes the impact of the safety management system of the responsible actor into account (see Subsection 5.2).

For a change of equipment or procedure by an airport or an ATM service provider, the use of a Modern Safety Case should initially be enforced as a safety management tool. In that case the approval of a Modern Safety Case stays the responsibility of the ATM service provider or airport, while the survey by the regulator stays limited to:

1. Evaluating the conformity of the goal settings and standards used in the Safety Case against the goal settings and operational standards in use by other actors involved.
2. Verifying that the Safety Case documentation is complete and consistent.
3. Verifying that all methodology used while building the Safety Case has been accepted as part of the Safety Management System.
4. Verifying that the automation requirements placed on the human controllers have been validated in the sense of being within the scope of a well-trained human controller.
5. Regularly conducting an in-depth survey of the safety management approach, and verifying that the safety case is kept up-to-date and is truly used as a guide to put things into practice.

Presently it is not clear whether this kind of "self-approval" of Modern Safety Cases will work well on the long run for all ATM service providers and airports, regulatory authorities should keep the right to enforce a more rigid certification regime upon Modern Safety Cases of under-performing ATM service providers or airports.

6.4 Enforce and survey Joint Safety Cases to advance ATM

Due to the distributed nature of ATM, many changes might affect multiple actors. This makes it good business practice to collaborate with other commercial actors on ATM advancements like (see Subsections 4.2-4.4):

- Jointly developing and validating advanced automation requirements.
- Jointly developing, co-ordination and validation of actors goal-settings.
- Jointly developing and validation of advanced operational ATM concepts.

Most of these advanced changes have potential safety implications for multiple actors. In that case a Joint Safety Case should be enforced by the regulatory authorities upon the actors that may be affected by the developed change. Joint Safety Cases should clarify how the responsibilities of the various actors are arranged, and how this is taken into account through the safety management systems and safety cases of the various actors (see Subsection 5.5). Since a Joint Safety Case does not fall under the Safety Management System of one particular actor, there is need for a full certification cycle (see Subsection 5.1). For this, opportunities to learn from other domains are not really available.

In Part II, an outline is given of how to build Modern and Joint Safety Cases. Obviously, there is need for safety and industrial policy makers to support the further development and application in building Safety Cases in ATM; and Joint Safety Cases in particular.

6.5 Availability to the civil aviation community

There are several advantages for human society that certified Safety Cases are being made available to the civil aviation community:

- Enables comparison of applied safety criteria
- Airlines see what they pay for
- Allows ATM service providers and airports to learn from each other
- Spreading of relevant advances
- Patent seeking becomes more relevant

The minor disadvantages can be avoided by adopting a code of conduct, and by making use of patent seeking approaches. The positive effect is that for the civil aviation community there is an increasing collection of publicly available reference documents describing:

- Certified operational ATM concepts for various traffic demands and environments.
- Certified actor goal settings per operational concept under various traffic demands and environments
- Certified automation requirements (human centred) per operational concept under various traffic demands and environments
- Benchmarks from procured systems

For all these reference documents applies that when they are considered as being valuable enough by a sufficient large number of actors in other regions/nations, then they may be used as a basis for European or world-wide standardisation.

6.6 Collecting support around Europe

It is obvious that the practical implementation of any of these safety certification guidelines will ask for significant efforts. Fortunately, it is possible to simultaneously work on the practical implementation of each of the main certification elements. It has also become clear that the challenging problems are due to the distributed nature of ATM, since there is no best practice learning material available from other domains. It is recommended to invest here with highest priority.

The guidelines developed by ARIBA are based on the principle that safety management is adopted as good business practice by the various types of actors involved. A crucial condition for safety management to work is that safety responsibilities and accountabilities should be clearly identified. This also means that the success of making these guidelines accepted largely depends on the support being collected from those actors around Europe and also world-wide. The first positive tests for this have been accomplished by comparing the above guidelines with the mainstream certification perceptions around Europe, as identified in [ARIBA-WP1]. The result is given in Annex B of [ARIBA-WP6-I]. Obviously, there is follow-up work required in communicating the findings to relevant actors, and to further elaborate on the standardisation in ATM.

Part II - Modern safety cases for a new ATM operation

Authors: H.A.P. Blom, M.H.C. Everdij and J. Daams (NLR)

Part II of the ARIBA consolidation report is aimed at developing a consolidated view on an effective approach towards safety validation for a new or changed operation in ATM. Part II starts with the building of Safety Cases for an advanced ATM operation, as identified in Part I, goes through various complementary safety-related assessment types and a state-of-the-art accident risk assessment methodology for advanced ATM. For this consolidation ample use is made of [ARIBA-WP1], [ARIBA-WP2], [ARIBA-WP3], [ARIBA-WP4], [ARIBA-WP5] and several other ATM and safety validation related literature sources.

Section 7 outlines the building of two relevant types of modern safety cases for a change in an ATM operation: the Modern Safety Case and the Joint Safety Case (see Part I), and explains the role of building a Classical Safety Case by a manufacturer (see Part III), as part of a procurement contract. The motivation for using the Modern and Joint Safety Case concepts towards the safety validation of changes is that they unambiguously specify (e.g. for project leader, top management, certifying authority, other actors, etc.) how far a particular new operation has evolved along its life cycle.

Section 8 gives an overview of the safety-related techniques and their combined usage, in order to allow for an effective safety feedback during the ATM operation design. The following four safety-related techniques are considered in more detail:
- Accident types and severity assessment
- Assessment of tolerable accident frequencies
- Evaluation of encounter types, frequencies and pilot/ATCo task loads
- Dependability analysis for given technical systems.

Accident risk assessment methodology is claimed to form an effective means to integrate these different types of evaluation results.

Section 9 gives an overview of the state-of-the-art accident risk evaluation techniques that apply to advanced ATM operations. Techniques such as hazard identification, human reliability analysis and identifying risk-mitigating measures stem from developments in other safety critical domains. In addition, it is shown that some key areas ask for dedicated ATM modelling developments, such as:
- pilot and ATCo cognition modelling,
- pilot and ATCo co-ordination and control,
- conflict avoidance and collision risk modelling,
- wake vortex induced risk modelling.

Finally, Section 10 draws conclusions in the form of guidelines for further development and application of the safety validation of advanced ATM operations.

7. Safety validation of a change in operation

When introducing a new or a changed operation in air traffic, there is a definitive need to accomplish a safety validation first. The aim of this section is to outline the elements and the organisation of such safety validation.

7.1 Safety feedback needs

Safety is a general notion, which deserves attention from three different ATM perspectives:

- Safety perception (e.g. by pilot, controller, passenger, human society, etc.). An ATM design that is perceived as being unsafe will not easily be accepted by the pilots and controllers involved. Fact is that their positive perception about the safety of an ATM design is a training and deployment critical requirement. By its very nature, however, safety perception is a subjective notion, and therefore insufficient to really guide the approval of safety-critical changes in ATM. Moreover, the safety perception by passengers and human society can not be identified on the basis of an ATM design.
- Dependability of a technical system (e.g. an automation support system, an aircraft navigation system, a satellite based communication system) stands for a collective term used to describe the availability performance and its influencing factors, reliability performance, maintainability performance and maintenance-support performance [ISO8402, 1994]. Metrics for dependability elements have been widely studied in literature for technical systems (e.g. [Laprie, 1995]; [DAAS, 1995]) and are in use e.g. by the JAA [JAR 25.1309] and EUROCONTROL [EHQ-SAM, 1999].
- Accident risk, e.g. for 1st (crew), 2nd (passengers) and 3rd parties (external persons) in air transport. Accident risk metrics are commonly in use for human controlled safety-critical operations in chemical and nuclear industries, and in civil aviation. Two well known ICAO-adopted accident risk metrics are for an aircraft to collide either with another aircraft during en-route phase, or with fixed obstacles during landing. Risk may also be expressed in economic terms (e.g. [Jones-Lee & Loomes, 1995]) or societal risk (e.g. [Milloy, 1998]). For recent reviews of various accident risk metric possibilities in air transport see [Moek et al., 1997]; [ICAO, 1998].

First of all, well trained pilots and ATCo's should be able to perceive the new operation as being safe; otherwise it would be impossible for them to carry responsibility for the safe execution of the advanced ATM operation. A minimal requirement for this is that the cognitive workloads of pilots and ATCo's stay within reasonable bounds. Another trivial requirement is that all safety critical technical systems shall adhere to high levels of dependability. In addition to this, there is the requirement that the accident risk of the advanced operation stays at tolerable levels. Therefore, the design of an advanced ATM operation has to be such that all three safety views are adhered to. To guide the design process adequately, there is need for feedback from safety related assessments of design versions.

For existing operations, a lot of safety feedback can be obtained by means of safety monitoring, by keeping records of actual safety related events, and analysing this data statistically. For an advanced operation, however, such records of actual safety related events do not exist during the design phase. The alternative is to predict safety characteristics of an advanced design, and to provide safety feedback (e.g. [MUFTIS, 1996], [Odoni, 1997]; [Haraldsdottir, 1997]; [Blom et al., 1998]) for several purposes, such as:

- Safety management decisions. Based on the outcome of a safety evaluation, the safety management strategy will be implemented. Typically, the decisions involved concern the safety issues that ask for improvement of the operation and/or its future monitoring, or whether there is a need to assess safety issues in more detail.
- Feedback to the designers of the advanced operation. If the operation is still in a conceptual design phase, or if changes in the design are considered, then the outcomes of a safety evaluation provide valuable support; either for further development of the advanced operation and the safety monitoring approach, or for consolidation of the advanced design.
- Contributing to the process of building a modern Safety Case for the advanced operation including its safety monitoring and management, with the aim to receive approval from the responsible safety authority to operate according to the newly designed advanced operation.

There is a definite need for a systematic approach to organise the various safety assessments, and to co-ordinate their progress and feedback with the progress of the design of the operation. In Part I we have identified the Safety Case concept to provide appropriate means to guide the development and safety validation of that change, and to make the progress visible to others (e.g. project management, safety management, top management, other actors, certifying authority).

7.2 Modern and Joint Safety Cases

Significant changes in air traffic operations commonly involve more than one air traffic service provider (i.e. airline, ATM service provider or airport). In Part I it has been argued that for such situation three types of Safety Cases would be needed to support safety management:

1) Classical Safety Case for the safety requirements posed on a technical system.
2) Modern Safety Case for the service provision by a single service provider.
3) Joint Safety Case for the safety of the overall operation.

The type 1) safety case could be produced by the manufacturer of a technical system as part of a procurement process. How this could effectively be achieved by a manufacturer of non-airborne systems is outlined in Part III. The types 2) and 3) safety cases could best be produced by the service providing actors involved with the new operation. The type 2) has been well developed by UK-CAA under the name of Change Safety Case [UK-CAA, 1999]. The type 3) is complementary to type 2) and has been introduced for the first time in Part I to fill the gap when safety responsibility for a changed or new operation belongs to more than a single service provider.

The Joint Safety Case should provide the high level argumentation and evidence for the total operation, while each Modern Safety Case should provide the evidence and the high level argumentation for that part of the operation that falls under the responsibility of one specific service provider. For the Joint Safety Case there are multiple approaches to setting up a useful high level argumentation. Three typical approaches, which might also be used in combination, are:

- Integration approach. This approach means that the Modern Safety Cases are being built first. Next, a Joint Safety Case is being built through integration of the material available from the Modern Safety Cases.
- Hierarchical approach, in which the Joint Safety Case is being built first. On the basis of such a Joint Safety Case, the service requirements to be fulfilled by each of the service providers involved can be identified. Subsequently, each of these service providers has to develop a Modern Safety Case to show that the requirements, posed by the Joint Safety Case on his own operation, are satisfied.
- Negotiation approach, in which the Joint Safety Case and the Modern Safety Cases are all being built in parallel, and compared to each other. If there are gaps and/or overlap between the various resulting Modern Safety Cases and the Joint Safety Case, then through negotiations between the collaborating partners adequate improvements should be identified.

Obviously, it is up to the collaborating actors to choose the approach that is judged to be most effective in realising their collaboration objective.

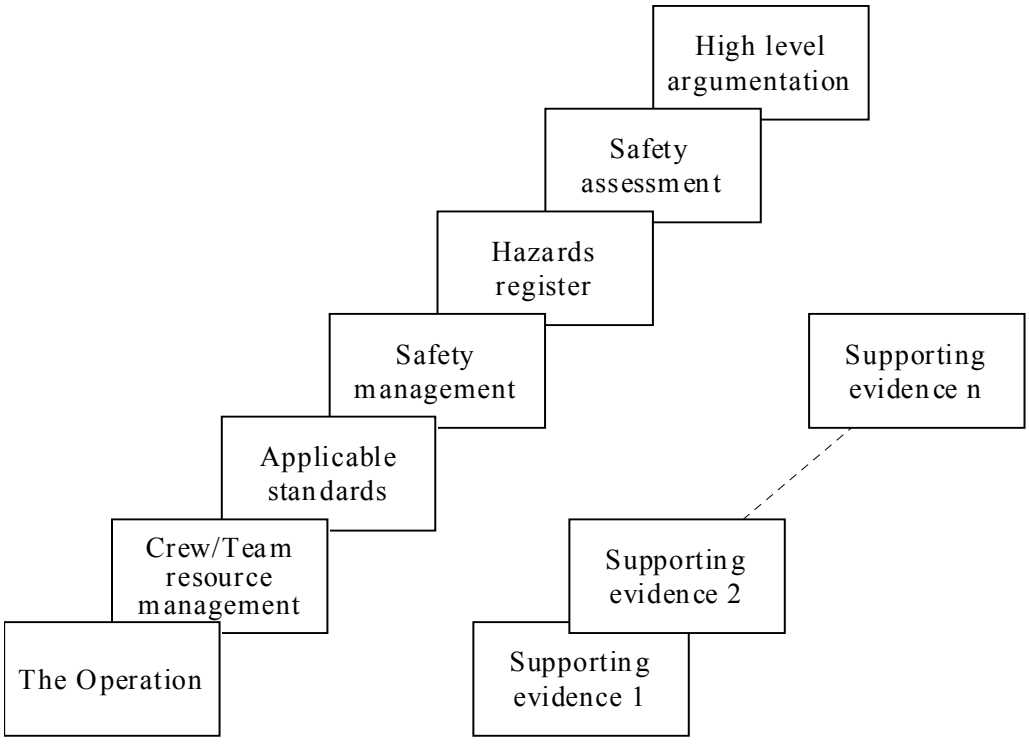


Figure 12. Contents of modern safety case; this applies to both a Modern Safety Case and a Joint Safety Case.

7.3 Complementary contributions

The Joint Safety Case considers the complete operation, including all commercial actors involved, while a Modern Safety Case considers that part of the operation for which a particular commercial actor is responsible. The implications of this can best be explained in terms of the modern safety case contents as depicted in Figure 12.

The operation: The Joint Safety Case considers the total operation, while each Modern Safety Case considers that part of an operation that concerns a particular actor only. This implicitly means that Modern Safety Cases often go into more detail than the Joint Safety Case, while the Joint Safety Case should explicitly cover issues like responsibilities and accountabilities of the various commercial-like actors, including the interfaces/boundaries between the actors. In order to prevent any confusion, in particular for hazardous situations, it is necessary that all Safety Cases refer to the same description of the advanced operation.

Crew/Team Resource Management: A Modern Safety Case takes into account the Crew or Team Resource Management approach by the particular service providing actor. The Joint Safety Case brings into account how the collaboration between Crews/Teams from different commercial actors is arranged.

Applicable standards: The Joint Safety Case should maintain a joint listing of all applicable (international and national) standards, while each Modern Safety Case should receive a copy of this, and should contribute to the completion of the joint listing.

Safety Management: Each Modern Safety Case relies on the Safety Management of its responsible actor. As an illustration, Annex C gives an outline of the Safety Management approach proposed by UK-CAA for an ATM service provider [UK-CAA, 1999]. The Joint Safety Case relies on how Safety Management responsibility and co-ordination is arranged for the total operation under consideration.

Hazards register: Since hazards that start under the responsibility of one service provider often affect the operation for another service provider, it is very important that the Joint Safety Case makes a joint hazard register which is as complete as is possible, while all Modern Safety Cases have a copy of this joint hazard register. This also means that hazard identification and development of safety improvement measures per hazard should be done both at the level of a Joint Safety Case, and at the level of each Modern Safety Case.

Safety assessment: The Joint Safety Case should assess the safety of the complete operation, while each Modern Safety Cases should assess the safety of that part of the operation that falls under the responsibility of the particular service provider. In effect this often means that within a Joint Safety Case it is necessary to perform a safety assessment for the operation, while within a Modern Safety Case the aim is to perform a safety assessment for the contribution by a single actor. Any assumptions about the operation that have been made during the assessment should be clearly stated and

justified; however obvious these assumptions may be, the implications for others involved with the project cannot always be predicted.

Supporting evidence: The Modern Safety Cases may provide safety supporting evidence for the Joint Safety Case. A Joint Safety Case, however, may only provide supporting evidence for a Modern Safety Case if it is shown that this does not lead to a vicious circle. For procured equipment, a manufacturer's Safety Case (see Part III) may form supporting evidence both for a Modern Safety Case and for a Joint Safety Case.

Both a Modern Safety Case and a Joint Safety Case must be developed in a way that allows for modifications, extensions or revisions, making them living documents that can be updated when, for example, new hazards have been identified and assessed during the development of the new or changed operation.

7.4 Safety Cases building phases

The Modern and Joint Safety Cases should be built in parallel with the lifecycle of the new or changed operation. As such, these Safety Cases usually take the form of several parts, each produced to document a distinct phase of the lifecycle of the change. Following [UK-CAA, 1999], these parts may represent the phases depicted in Figure 13, and shortly described below. Each change will be different, and normally each part will need to be completed before progressing to the next phase. Obviously, for simple changes, it would be logical to skip one or more of these phases.

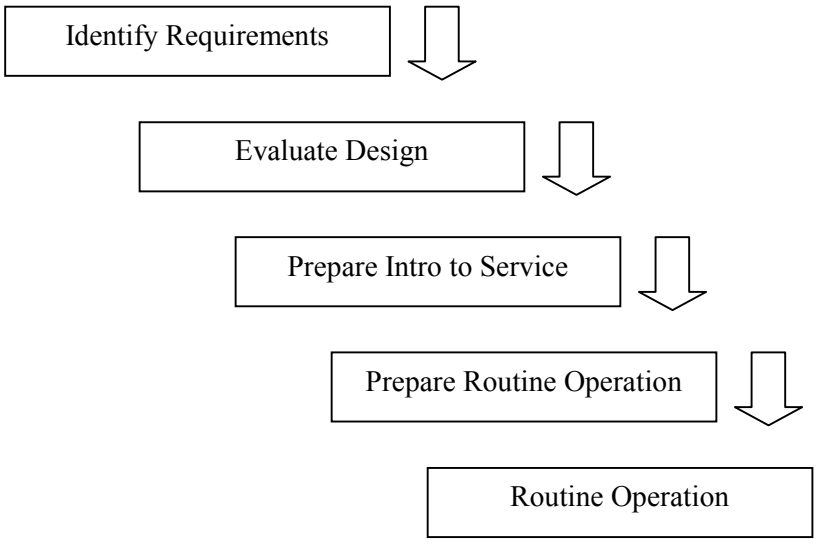


Figure 13. Typical lifecycle phases in building Joint and Modern Safety Cases.

Identify Requirements
The change in operation for which the Joint and Modern Safety Cases are to provide assurance should be clearly defined at the outset. This includes the reason why the

change in operation is developed, the identification of any changes in responsibilities of the service providers involved, including the interfaces/boundaries between them, the identification of the operational and functional requirements, the identification of pilot/ATCo's roles and crew/team resource requirements, the identification of implementation/transition requirements, the identification of performance monitoring requirements and the identification of the safety objectives and regulatory requirements which must be satisfied. This requirements identification phase should not seek to specify the design, even if the design solution is thought to be obvious, but should simply state the objective.

Safety assessment should be carried out to identify hazards associated with the change and assess their impact. This may result in additional safety requirements which will mitigate the identified hazards. This process may need to be repeated at a later stage if the design solution does not satisfy all requirements that have been identified.

Evaluate Design

In selecting a design solution, and its stepwise implementation path, evaluations have to be carried out to verify if and how all identified requirements will be satisfied. In addition, evaluations should be carried out to identify any further features that are not yet included in the requirements but may still affect the safety of the operation. Any related hazards will need to be mitigated. If possible, it would be beneficial for the service provider(s) to obtain assurance from equipment manufacturers that all assumptions made are valid. Part III presents a manufacturer's Safety Case approach to provide such assurance. Otherwise, evidence for such assurance should be gathered by the service provider(s) during the design evaluation parts of the Modern and Joint Safety Cases.

The Joint and Modern Safety Cases should document the safety-related aspects of this evaluation. It is possible that some of the identified requirements cannot be satisfied by the designed operation. This also should be clearly indicated, and mitigating measures need be identified by the designers. It may be necessary to complete further safety assessments that take all safety-related changes into account. It even may be necessary for the collaborating actors to decide that other high level objectives (e.g. capacity, flexibility, etc.) need to be relaxed in order to succeed in building the safety cases for the new operation. Since such a relaxation weakens the Business Cases for the commercial-like actors involved, the result could be that the further development of the operation is even stopped.

Prepare Introduction to Service

The Joint and Modern Safety Cases should consider any risks relating to the (stepwise) introduction of the new or changed operation. In many cases it may be necessary to include reversion procedures to be followed if some unforeseen problem prevents the introduction from being completed. The Joint and Modern Safety Cases should also demonstrate that any requirements that have not been satisfied by the design solution have been satisfactorily mitigated in some other way. It should also be evaluated that the crew/resource management requirements have been satisfied. The

Joint and Modern Safety Cases should provide the assurance prior to the introduction of the operation to service, and should contain a summary showing that all phases of the safety assessment have been implemented successfully.

Prepare Routine Operation
Before it can be decided that the changed operation has matured to the level of routine operation, it should have been demonstrated that organisational, operational and maintenance staff is able to run the operation according to the assessments and high level argumentation provided by the Joint and Modern Safety Cases. In case of any identified mismatch, mitigating measures should be developed and the Joint and Modern Safety Cases should be adapted accordingly. Finally, each commercial-like actor incorporates the Joint Safety Case and its own Modern Safety Case within its Safety Management System.

Routine Operation
Having reached the status of Routine Operation, the Safety Cases have to be maintained by each commercial-like actor as part of its Safety Management System. Following Part I, this means that if new hazards are identified (either due to proactive monitoring, or due to incident or accident reporting) mitigating measures for the operation and corresponding updates of the Safety Cases would be necessary.

7.5 Safety-related feedback needs

Having arrived at the point where both the relevant safety feedback types and the relevant Safety Case building phases have been outlined, it can be clarified how these combine. In order to do so, Table 3 summarises which safety-related operation design issues should be covered during which life-cycle phase.

Table 3. Typical operation design issues during life-cycle phases. The bold printed issues are introduced in consolidation report Part I.

Design issues	Identify Require ments	Design & Evaluation	Prepare Intro to Service	Prepare Routine operation	Routine operation
Safety goals/policy	Yes	-	-	-	-
Traffic scenarios	Yes	-	-	-	-
Applicable standards	Yes	-	-	-	-
Responsibilities	Yes	Update	Update	-	-
Human roles	Yes	Update	Familiarize	-	-
Technical systems	Yes	Yes	Integrate	Update	Updates
Procedures	Yes	Yes	Yes	Update	Updates
Human resources	Yes	Yes	Yes	Yes	Yes
Mitigate hazards	Yes	Yes	Yes	Yes	Yes
Safety management	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Safety feedback	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

Table 3 reflects that service provider's responsibilities and human roles can not easily be changed anymore once the Requirements identification life-cycle phase has been

closed, while it stays relatively easy to adapt human resources and procedures during later life-cycle phases. Technical systems fall in between these two extremes. This forms a logical reason why pilots and ATCo's easily end up with all kinds of procedures that are just developed to mitigate system design shortcomings from earlier life-cycle phases. The only way to avoid this is that the operation design definition and validation should be done thoroughly already during the first life-cycle phase. In order to allow for such validation there is need for feedback from adequate safety-related evaluations that can effectively be applied from the first life-cycle phase on.

An overview of various kinds of safety-related evaluations that are considered by the ARIBA consolidation report is given in Table 4. Obviously, some of them apply to later phases only. The last column of Table 4 refers to the Part and Section of the ARIBA consolidation report where the evaluation type has been considered.

Table 4. Kinds of safety-related evaluations that might provide effective safety feedback during various life-cycle phases.

Kind of safety-related evaluation	Identify Requirements	Evaluate Design	Prepare Intro to Service	Prepare Routine operation	Routine operation	Part & Section
Task load analysis	Yes	Update	Update	Update	Updates	Part II, S8
Accident risk evaluations	Yes	Update	Update	Update	Updates	Part II, S9
Dependability evaluations	Yes	Yes	Update	Update	Updates	Part III, S14 Part II, S8
Identify potential hazards	Yes	Yes	Yes	Yes	Yes	Part I, S3 Part II, S9
Identify mitigating measure candidates	Yes	Yes	Yes	Yes	Yes	Part II, S9
Human-in-the-loop evaluations	Yes	Yes	Yes	Yes	Yes	Part I, S2
Incident/accident report evaluation	-	-	Yes	Yes	Yes	Part I, S2
Traffic monitoring and evaluation	-	-	-	Yes	Yes	Part I, S3

Table 4 contains eight kinds of safety-related evaluations, six of which can be applied from the first life-cycle phase on. Of these, the human-in-the-loop evaluations are best known and most commonly in use for ATM. During the early life-cycle phases this comes down to real-time simulation based human-in-the-loop evaluations. Unfortunately, these are so demanding that it is difficult to assess the large variety of non-nominal situations that actually determine the safety of a new operation. As such, the other five kinds of safety-related evaluations remain as candidates to provide effective safety feedback from the first life-cycle phase on.

For all evaluations, the approach evolves significantly with the life-cycle phases, in particular for hazard identification. During the implementation phases, the hazard identification is done with the help of systematic brainstorming with experts from various domains; this is covered in the remainder of this Part II. As discussed in Part I, during the operation phase there also are the possibilities to make use of:

- Incident and accident report evaluations
- Traffic monitoring based evaluations
- Evaluation of human precursors to identify latent conditions.

For dependability evaluations, a differentiation has to be made between a technical system to be procured from a manufacturer according to specified requirements, and a given or existing technical system (or network of technical systems). The latter type of dependability evaluation should be done by service provider(s) and is covered in this Part II. The former type of dependability evaluation should be done by the manufacturer, and is covered in Part III.

8. Safety of an advanced operation

8.1 Safety-related assessment types

For an advanced operation, several complementary safety-related assessment types exist, and are useful. This is shown in Figure 14. The boxes at the top represent the advanced ATM operation being designed, together with the safety and capacity goals. The four boxes at the second level represent the various safety-related assessments that are necessary in addition to accident risk assessment. The box at the third level represents the accident risk assessment. The boxes at the bottom form the outputs of accident risk assessment. The accident risk assessment box and its outputs are detailed in Section 9, the four boxes at the second level are described in Subsections 8.2 through 8.5. The input boxes are shortly described below the figure.

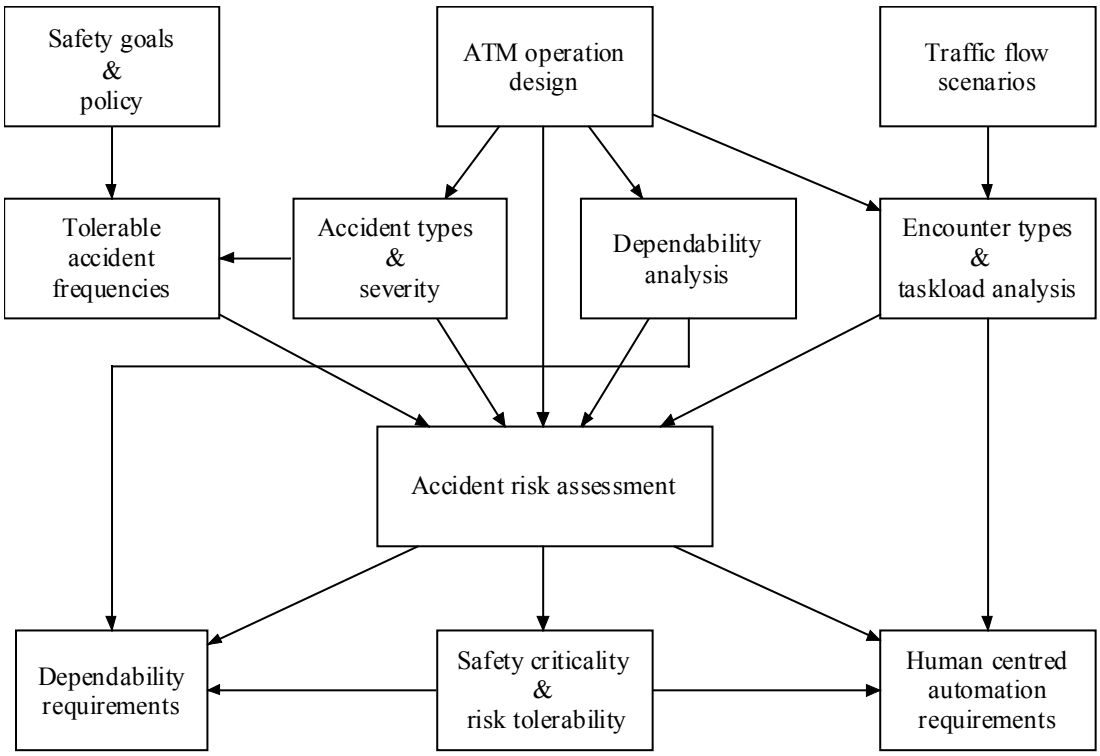


Figure 14. Overview of relations between safety related assessments of an ATM operation design.

The input boxes at the top of Figure 14 are:

- Safety goals and safety policy; these are the general principles that specify how safe the operation should be at a particular moment in time, e.g. following the ATM2000+ safety goals [EHQ-2000+, 1998] and the safety policy to realise those goals, e.g. [EHQ-POL, 1995].
- ATM operation design; this specifies the advanced operation to be assessed. This specification includes the scope of the operation considered, the airspace and airways structure (or airport structure), the pilot and controller roles, the

CNS/ATM systems, the service provider's responsibilities, a description of the procedures (e.g. separation criteria), the conditions under which the procedures are used, the frequency of operation, etc.

- Traffic flow and scenarios; capacity bottlenecks of the existing ATM operation often form the driving force for top management to start the design of an advanced ATM operation that would allow to increase the traffic flow up to certain higher levels. In order to arrive at useful results, the risk assessment has to be done for these higher levels of traffic flows.

8.2 Accident types and severity

Following [ICAO, Annex 13], an **accident** is defined as:
"an occurrence associated with the operation of an aircraft, which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which:

a) a person is fatally or seriously injured as a result of being in the aircraft, or of direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or of direct exposure to jet blast (except when the injuries are from natural causes, self-inflicted, or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passenger and crew); or
b) the aircraft sustains damage or structural failure which adversely affects the structural strength, performance or flight characteristics of the aircraft, and would normally require major repair or replacement of the affected component (except for engine failure or damage, when the damage is limited to the engine, its cowlings or accessories; or for damage limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin); or
c) the aircraft is missing or is completely inaccessible."

This definition covers various ATM related accidents during various flight phases, such as:

- Collision with another aircraft on ground (taxi, take-off, landing, go-around)
- Collision with another aircraft in flight (all airborne flight phases)
- Collision with ground (final approach, initial climb, etc.)
- Collision with other airborne object (e.g. bird, missile)
- Collision with other ground based object (e.g. physical structure, truck, car)
- Accident induced by an expedite escape manoeuvre (all airborne flight phases)
- Accident induced by an expedite deceleration (landing, take-off, taxi)
- Accident induced by a wake vortex (all airborne flight phases)
- Accident induced by a meteorological condition (all airborne flight phases)

For the particular advanced operation considered, all possible ATM related accident types should be identified. The next step is to assess the (expected) severity of the consequences of each accident type (per flight phase) in terms such as:

- the expected number of fatalities,
- the expected number of injuries, and

- the expected material damage.

Having identified the relevant accident types and having assessed the severities by using statistical accident data, the next step is to derive the tolerable frequencies per accident type.

8.3 Tolerable accident frequencies

In order to build an accident risk tolerability matrix for air traffic operations, we have to assess accident frequencies that complement the accident severity assessment. For some flight phases we use expected frequency per flight hour (e.g. en-route), while for some other phases we use expected frequency per flight phase (e.g. landing). Next, we determine tolerable frequencies per accident type, depending on the associated severity level. Obviously, requiring a zero accident frequency is not realistic and not necessary. For ATM, a practical way to incorporate the concept of tolerating some risk is to define for each accident type the frequency requirement by three regions (Figure 15) in the continuum of possible frequency values [HSE, 1995]:

- an intolerability region,
- a tolerability region, and
- a broadly acceptable region.

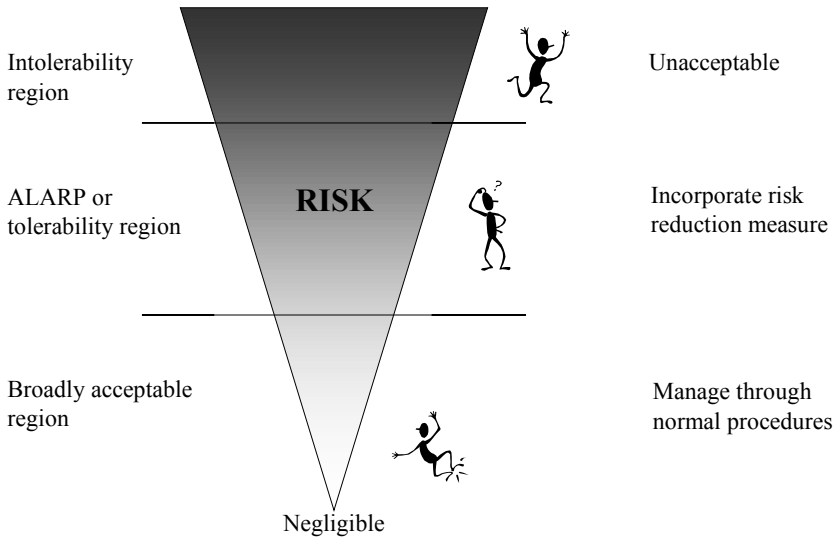


Figure 15. Risk regions: intolerability, ALARP and broadly acceptable.

It suffices to identify the boundaries of these regions per accident type. The tolerability region is also known as ALARP (As Low As Reasonably Practicable) region. For this region, specific safety management measures should be defined (e.g. safety monitoring, safety improvement projects, etc.) as long as such is reasonably practicable. Above a certain level, a frequency of a certain accident type is regarded as intolerable and cannot be accepted. An accident type frequency below the ALARP region is considered broadly acceptable in comparison with the existing operation and/or with other (perceived) risks to human society, e.g. [Evans, 1996]. Obviously, these risks still need to be managed through the normal procedures.

For the determination of the boundary levels of the ALARP region per accident type, combined use should be made of the severity of the consequences and the accident frequencies in current ATM and in comparison with other (perceived) risks to human society. For the determination of the boundary level between the tolerability and intolerability regions, additional use is made of the safety goal, the applicable safety management system (e.g. safety monitoring, safety policy, etc.), and the proven effectiveness of that safety management system for the accident type considered. Conversely, if no risk management is available then the ALARP principle should not be followed and the size of the ALARP region should become smaller, at the cost of an increase of the intolerability region. This also shows the need for developing proper rationales in order to assure that the ALARP principle is not misused to approve unacceptably risky operations.

The final step is to combine the accident severity classes and the accident frequency classes into an accident risk tolerability matrix (see Table 5 for an illustration).

Table 5: Illustration of a possible accident risk tolerability matrix.

Severity of accident		Frequency of accident				
Expected material damage	Expected injury or fatalities	1x / yr in civil aviation	>1x / yr in civil aviation	1x / yr per large airline	>1x / yr per large airline	1x / yr per aircraft
No damage	No injury					
Minor damage	Minor injury					
Serious damage	Major injury					
Major damage	Single fatality					
Hull loss	Many fatalities					
Hulls loss	Hundred(s) of Fatalities					

Manage through normal procedures

Incorporate risk reduction measures

Intolerable

8.4 Encounter types and task load analysis

The aim of the encounter types and task load analysis is to characterise the encounter types and frequencies, and the related controller and pilot tasks and workloads for the advanced ATM operation considered. To do so, first it is necessary to model the advanced operation in terms of airspace and airways structures, the roles and tasks for the pilots and ATCo's, their control/communication procedures, their automation supporting facilities, the CNS systems, etc. For the subsequent assessment of encounter types and frequencies it would suffice to use fast-time simulators like TAAM, NASPAC or RAMS [MUFTIS, 1995]. To do so, the advanced operation models are implemented in the selected fast-time simulator. Subsequently, traffic scenarios are defined, simulations are run, and results are analysed. [TOSCA-WP1, 1998]; [TOSCA-WP3, 1997]; [TOSCA-WP5, 1998]; [TOSCA-WP7, 1997].

In order to also assess the workload of pilots and ATCo's it is necessary to develop and integrate appropriate workload models in the fast-time simulation activities. For this it is necessary to perform a hierarchical task analysis of the advanced operation, and an analysis of pilot/controller tasks and subtasks, and to assess the workload involved with each subtask [EHQ-HUM, 1996]; [Buck et al., 1997]. It should be noticed that a choice has to be made with respect to the level of detail necessary in subtask modelling [AGARD, 1998] and the limitations posed by such a functional modelling approach, e.g. [MacLeod & Taylor, 1994], [Small & Rouse, 1994]. Relatively straightforward subtask models can be incorporated directly within fast-time simulators like TAAM and RAMS. If the subtasks should go down to the level of HMI interactions, then one could develop and run fast-time simulations, e.g. [Evans, 1994], [TOSCA-WP8, 1997], that are tuned to results obtained from observational task analysis.

Having arrived at this point it is important to realise that the problem of accident risk assessment can be seen as one of extending fast-time simulation models up to the level of accidents, and subsequently run simulations with those models in order to count all kinds of accidents. The challenge in realising such model extension, however, can be depicted as climbing to the top of the ATM 'safety iceberg' (Figure 16).

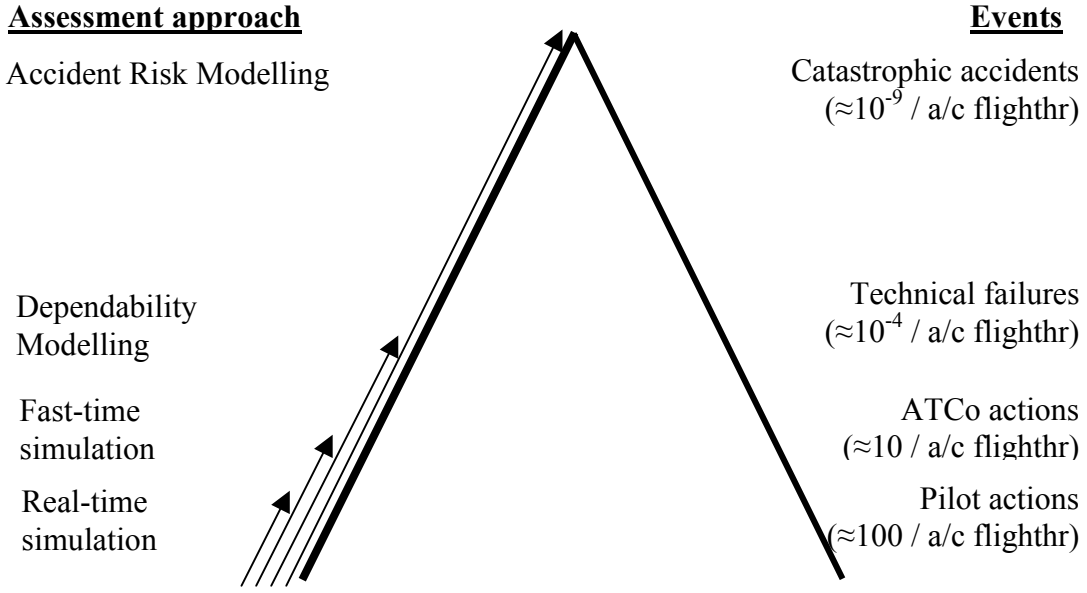


Figure 16: ATM 'safety iceberg'

Indeed, the established fast-time simulation models, e.g. used in TAAM, apply to assessments that address a broad scope in combination with a low level of non-nominal detail. In order to subsequently assess the catastrophic accident rate, one needs additional techniques which handle other combinations of scope (e.g. volume of airspace) and focus (i.e. level of model detail), in particular for dependability

assessment and accident risk assessment. The latter is addressed in Section 9, the former is addressed below.

8.5 Dependability analysis

In literature, dependability is studied as the ability of a technical system to perform one or several required functions under given conditions [Laprie, 1995]. Generally speaking, dependability is considered to be the science of failures and faults of systems. In [ISO8402, 1994] dependability is defined as a collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance performance. In order to indicate that reliance can justifiably be placed on the service delivered by a system, various metrics could be used, such as reliability, availability, maintainability, system safety, integrity, confidentiality, security, or combinations of these.

Dependability analysis is useful throughout the life-time (from design up to routine operation) of technical systems, including HMI's, in air traffic, such as Communication, Navigation, Surveillance and ATM automation systems. References [JAR 25.1309], [SAE, 1994], [DAAS, 1995] present related methodology, largely from a manufacturers point of view. More recently, EUROCONTROL has extended these approaches towards applications from an ATM service provider point of view, which means that the system life-time has been extended to include transition into operation, and routine operation [EHQ-SAM, 1999]; Annex C gives an outline of this methodology.

Often a dependability analysis for a technical system will be performed as part of a procurement contract by a manufacturer. This is outlined in more detail in Part III of the consolidation report. However, it should be realised that technical systems in ATM often are so distributed, that also service providers may be in need of dependability assessment methodology, in order to build Joint and Modern Safety Cases for the operational introduction of that system.

Table 6: Failure condition tolerability matrix based on JAR 25.1309 (Annex B).

	Severity			
Probability Level	Catastrophic	Hazardous	Major	Minor
Probable	***Intolerable***	***Intolerable***	***Intolerable***	***Tolerable***
Remote	***Intolerable***	***Intolerable***	***Tolerable***	***Negligible***
Extremely remote	***Intolerable***	***Tolerable***	***Negligible***	***Negligible***
Extremely improbable	***Tolerable***	***Negligible***	***Negligible***	***Negligible***

Common practice is that a dependability assessment methodology incorporates severity-frequency criteria for the tolerability of failure conditions for safety-critical technical systems. The criteria given by JAA (see Annex B) can be expressed in the form of a tolerability matrix, Table 6.

Each sector of the matrix represents a category in such a way as to prioritise the failure condition for review or further analysis. A failure condition can be placed in more than one sector if there is some uncertainty in the severity or probability of occurrence of that failure condition. Ignoring such uncertainty by placing the failure condition in a preferred sector definitely makes the outcome very subjective and, therefore, should be discouraged. Failure conditions in the *Negligible* sectors of the matrix do not need to be analysed further whereas failure conditions in the *Intolerable* sectors could need further quantification and possible elimination or reduction. The *Tolerable* sectors fall between the two other categories. Such situation is tolerated as long as its risk has been reduced to the lowest level practicable, bearing in mind the benefits resulting from its acceptance and taking into account the costs of further improvement.

The practicality of further technical improvements depends to a large extent on the impact the failure condition has on the accident risk of the operation. In order to assess this impact for ATM it often is not sufficient to perform a dependability assessment for technical systems only. It could be necessary to perform a risk assessment as described in Section 9. Then, it could turn out that some failure conditions are significantly less safety critical than as assessed during the initial severity classification, by which the tolerability of the failure condition might form no problem at all. In a recent paper on satellite navigation application such situation is explained [Benstead & Spriggs, 1998].

Several dependability techniques are available to assess failure conditions on their severity and their frequencies of occurrence [ΣΣ, 1993]. Well known examples are Failures Modes and Effects Analysis, Fault Tree Analysis, Event Tree Analysis, Dependence Diagrams, Reliability Block Diagrams, Particular Risk Analysis, Common Cause Analysis and Zonal Safety Analysis. Most of these techniques combine qualitative and quantitative approaches [Everdij et al., 1996]. For complex technical systems (e.g. Flight Planning systems, Satellite based navigation, etc.) it may be necessary to use more advanced approaches like Generalised Stochastic Petri Nets (GSPN) and Markov analysis techniques to assess dependability [Fota et al., 1997], and tools that support the building of a safety case for a technical system [ARIBA-WP5, 1999].

9. Accident risk assessment feedback

The aim of this section is to describe the remaining four boxes in Figure 14.

9.1 State of the art

For other safety-critical operations, such as in the nuclear and chemical industries, the accident risk assessment feedback problem has been widely studied, and numerous techniques and tools have been developed, e.g. [Aldemir et al., 1994]. A thorough study of the applicability of these techniques to safety assessment in ATM has been accomplished within the MUFTIS project [Everdij et al., 1996]. The key finding is that the stochastic dynamical behaviour over time for complex interactions of highly distributed ATM pose more demanding challenges to risk assessment than is needed in other safety critical domains. This is illustrated in Figure 17.

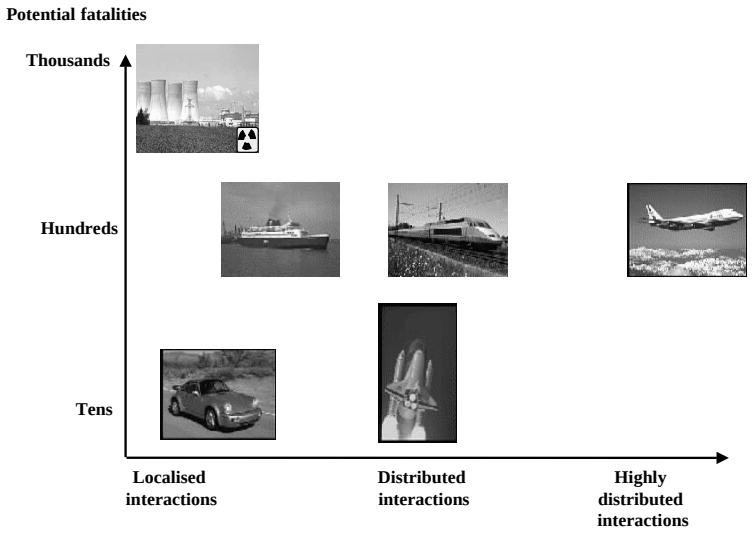


Figure 17: Potential fatalities and distribution level of ATM and other safety critical activities.

Due to the highly distributed interactions, the established safety assessment techniques fall short in handling several problems that are of crucial importance in performing accident risk assessment for ATM:

- Human performance is not strictly functional, and varies in practice with cognitive workload. This is clearly reflected by the characteristics of the pro-active safety philosophy paradigms in Table 2, and by the overview given by [RTCA, 1999], pp. 78-86. As such, established safety assessment techniques fall short in properly assessing the cognitive effects of the human controllers [ARIBA-WP3]; [ARIBA-WP4].
- ATM related accidents in civil aviation typically happen in an environment of decision-making feedback loops and with sequences of hazards. The established

safety assessment techniques fall short in properly assessing combinations of such situations [Everdij et al., 1996]; [ARIBA-WP3].

- For Joint and Modern Safety Cases it is important that both a forward and a backward reasoning is supported. These capabilities are required respectively to cover all hazards and to trace back the safety critical hazardous combinations, in order to provide effective information to the designers of means to control those hazards. The established techniques support either forward or backward reasoning [ARIBA-WP3].
- For ATM accident risk assessment it is necessary to have collision risk models and wake vortex induced risk models that can seamlessly be combined with the assessment of the occurrence of combinations of hazardous events (e.g. [ICAO, 1998]; [Everdij et al., 1996]).

Recently, by a joint effort of EUROCONTROL and FAA, in collaboration with some key developers (from USA and Europe), an overview has been established that outlines the key problems and the most relevant approaches currently under development and/or in use for the safe separation assessment of advanced procedures in air traffic [Cohen et al., 1998]. Based on the most relevant approaches identified in that study, together with the additional techniques identified in [ARIBA-WP3, 1999] and [ARIBA-WP4, 1999], it is possible to propose an advanced risk assessment methodology for advanced operations in ATM. The aim of this section is to outline the most important aspects of such methodology.

9.2 Identify and qualify hazards

A lot of information needs to be collected at the beginning of any safety analysis. First of all, it is very important to verify that the operation to be assessed has been defined well. The information already collected during any fast-time (or real-time) simulation and any dependability analysis of technical systems involved would also be very useful (Subsections 8.4 and 8.5).

Hazard identification

The aim is to identify all possible hazards, hazardous events and their causes and consequences, i.e. events, situations and effects that potentially cause the advanced operation to deviate from nominal behaviour. These hazards and hazardous events should be generated from various viewpoints. For example: an operational experience viewpoint (what went wrong in the past), a functional viewpoint (failure conditions, human errors), a cognitive viewpoint (operator internal states/strategies, experience/training issues), an organisational viewpoint (general working conditions, CRM issues, culture), and a safety management viewpoint (both proactive and reactive). Hazards may be obtained from incident/accident reports, existing hazard databases, dedicated brainstorm sessions, etc. Obviously, all information collected is to be documented, together with the sources.

Hazard brainstorming sessions can be run best in a structured way (e.g. by using HAZID or HAZOP techniques) and with a number of experts from relevant domains

(e.g. pilots, ATCo's, CNS experts, human factors experts in HMI and in human cognition). During the brainstorming stage, none of the suggested hazards or hazardous events should be dismissed based on their apparent remote probability of occurrence. In order to take maximal advantage of expert knowledge, it is best to distinguish two types of brainstorming sessions. One type is directed towards the identification of the hazards that are coupled to the existing operation. Another type is directed towards the identification of both new and reduced hazards due to the change in the operation. The findings are documented in a HAZID or HAZOP report. Existing hazard databases are valuable sources to identify additional hazards where necessary, and also to verify the exhaustiveness of the brainstorm.

A complementary activity is to identify sources of statistical information (literature and databases on incident and accidents) and expert opinion about the frequency of occurrence of the hazards and hazardous events identified. Obviously, this information is often available for particular groups of hazards or hazardous events only. Moreover, the information collected from different sources may be partially incomplete or partially different. For such cases it may be advantageous to make use of evidential reasoning techniques to objectively combine the various pieces of evidence.

Qualitative assessment

In general it may be useful to conduct a qualitative assessment prior to conducting a quantitative one. If the changes to the operation have a limited effect on accident risk, it might even be sufficient to conduct a qualitative assessment only. A qualitative risk assessment consists of a preliminary analysis of the hazards identified. If the existing operation is at least tolerably safe, then it is most effective to accomplish two qualitative assessments; one for the existing operation, and one for the new operation. Following [Blanker et al., 1997], such approach may work as follows:

1. All hazards that have similar adverse impact on the operation are aggregated under a single "adverse condition" class. This is done both for the existing operation, and for the proposed changes.
2. The failure condition tolerability matrix based on JAR (Table 6) is assumed to be also applicable as an effective "adverse condition" tolerability matrix.
3. For each of the "adverse condition" classes both the "severity" and the "frequency" are qualitatively identified by safety analysts and domain experts. This is done both for the existing operation and for the changes to the operation. One shall identify all sectors that are possible, thus not only the most likely one.
4. If the existing operation is at least tolerably safe for all "adverse conditions", then there are three situations possible:
    - All "adverse conditions" due to the change can be shown to be negligible; this means that to the best of knowledge the change appears to be sufficiently safe.
    - It can be shown that none of the "adverse conditions" due to the change are intolerable; this means that a change to the operation would ask for risk reducing measures to be applied to all relevant hazards (thus also to the ones of the existing operation).

- Some “adverse conditions” due to the change may be intolerable; this means that either the changed operation is unsafe, or a qualitative assessment leaves too much uncertainty.

9.3 Types of risk models

Often, a qualitative assessment does not provide a sufficiently clear insight into the safety of a new ATM operation. In such case a follow-up activity is to perform a quantitative accident risk assessment for an adequate model of the operation considered. An advanced ATM operation involves a large variety of entities that play a crucial role in its safety, and that thus have to be covered by complementary risk modelling approaches, the main of which are:
- Dependability and human reliability,
- Human operator cognitive models,
- Aircraft evolution, incident and accident models,
- Co-ordination and control.

The types of risk models necessary to cover each of these four are shortly discussed below. Models that allow incorporation of all four approaches are in general mathematically involved and therefore they have the disadvantage to be less transparent for non-specialists. This, however, must be considered as the price paid for being able to deal with the level of complexity of ATM operations.

Dependability and human reliability

For technical systems, the dependability techniques mentioned in subsection 8.5 form a useful starting point. However, the level of modelling required during such dependability analysis often is much more detailed than what is necessary for accident risk assessment. For the latter application it is therefore better to adopt a relatively simple model that captures the main characteristics assessed during the dependability analysis.

For human controlled operations in other safety critical domains, common practice is to apply dependability techniques in combination with Human Reliability Analysis (HRA) techniques that consider the human operator as performing functional tasks, the performance of which is limited due to failures of human information processing [Rasmussen, 1983]; [Reason, 1990]. Established HRA techniques are Action Error Analysis (AEA), Technique for Human Error Rate Prediction (THERP), Human Interaction Timeline (HITLINE), Human Error Assessment and Reduction Technique (HEART), Operator Action Trees (OATS), Human Cognitive Reliability model (HCR), Influence Diagram Approach (IDA), see [Everdij et al., 1996]. The effect is that, at functional level only, procedures and human functioning can be integrated with dependability assessment. Since these techniques are human task directed, they actually consider a human as a source of errors only, and not as a reliable source in dealing with unforeseen situations.

Human operator cognitive models

During the last decade it has become quite clear among cognitive psychologists that human cognitive facets such as human understanding, judgement and choice cannot be easily mapped onto a system function (e.g. [MacLeod & Taylor, 1994]. In line with this, the view on human reliability has started to evolve from a functional and error centred approach, towards a contextual and cognitive perspective, in which human actions are the product of human internal states, strategies, the environment and culture, e.g. [Jorna, 1991]; [Wickens, 1992], [Bainbridge, 1993]; [Hollnagel, 1993]; [Endsley, 1995]; [Westrum, 1995]; [Amalberti & Wioland, 1997]; [Shorrock & Kirwan, 1999], [EHQ-HER, 1999]. In parallel this has also led to the development of goal directed cognitive task analysis approaches, e.g. [Seamster et al., 1993]; [Seamster et al., 1997]; [EHQ-MOD, 1997]; [EHQ-TASK, 1998] and contextual performance type models that are based on generally-applicable human cognition and responsibility principles. As an example, situations should be covered where the operator chooses to let an even more urgent problem receive attention when the subjectively available time is short or when high workload requires the operator to make quick decisions, without bothering excessively about the quality of those decisions. These effects are inextricably bound up with human flexibility and the ability of humans to deal with unforeseen situations.

In order to take advantage of these new developments, in a sequence of ATM directed studies ([Biemans & Daams, 1997], [Daams et al., 1998], [ARIBA-WP4, 1999]) it has been demonstrated, by an effective collaboration between cognitive psychologists and stochastic analysts, that contextual cognitive modelling based approaches apply very well to ATM risk assessment. The benefits experienced with such approaches are that they enable better feedback to designers and that they remove the major need to use overly conservative individual sub-models for relevant operator actions that may blur understanding of how safety is achieved in ATM.

Aircraft evolution, incident and accident models

The aircraft evolution and incident models to be used should be able to represent in sufficient detail the performance and avoidance manoeuvre characteristics of aircraft. This often asks for a similar level of detail as being used by fast-time and real-time simulators like TAAM or NARSIM. Modelling areas not well covered by these traditional simulators are random meteorological conditions, and accident risk.

The random meteorological conditions affect the evolution of the various aircraft, and introduce an element of dependency between the evolutions of those aircraft. There is a need for models that adequately cover these effects, in particular under non-nominal meteorological conditions. Other key needs are realistic models for risk of collisions between aircraft and for ATM related accidents due to expedite escape manoeuvres and wake vortex encounters. For collisions the baseline is formed by the ICAO-adopted Reich model [ICAO, 1998]. A mathematically oriented overview of ATM relevant extensions over this Reich model is given in [Bakker & Blom, 1993]. Rather recent are the developments in wake vortex induced risk modelling, e.g. [Speijker et al., 1999].

Co-ordination and control
All entities described above do not yet form an advanced ATM system. To improve this situation, it is necessary to also model the interactions between these entities. For a complex operation in air traffic, the key interactions consist of co-ordination and control loops that are governed by humans at various levels and often across multiple commercial actors (managers, pilots, ATCo's, etc.). Only with these interactions an advanced operation can be modelled completely. This observation coincides with a similar observation that has been made in RTCA's certification study [RTCA, 1999]; there, it is explicitly mentioned that human operators not only perform their functionally defined tasks, but also play unique roles in integrating information coming from all kind of sources. For complex operations in air traffic, these roles are crucial contributions to safety, in particular when the situation to be controlled has evolved into a non-nominal situation. Thus, an advanced operation can only be modelled adequately if the key interactions provided by humans are incorporated.

The challenge is how to model those interactions unambiguously, and such that the resulting overall model is of a form for which appropriate risk evaluation methods exist. The most generally applicable approach that the authors are aware of is a stochastic modelling and analysis framework which supports a large variety of modelling approaches (e.g. Monte Carlo simulations, Hybrid-state Markov processes and Dynamically Coloured Petri Nets) and which always allows that one particular form of model is being transformed into any of the other forms [TOSCA-WP4, 1999]. Due to the support of a large variety of modelling approaches, the resulting framework supports both a forward and a backward reasoning. The backward reasoning starts from accidents, and shows which hazards provide the key contribution to that accident. The forward reasoning starts from the base hazards, and shows how frequent and how various accidents may evolve from it. The dual capability is required to take into account all identified hazards and trace back the safety critical hazardous combinations. Both capabilities are valuable to the designers of means to control those hazards.

9.4 Accident risk evaluation

The accident risk evaluation consists of two subsequent steps. First, develop an appropriate model using all information collected. Second, use the model to evaluate the accident risks involved with the various encounter types of the advanced operation.

Model development
After all relevant information is identified, a specific risk model is developed. This specific risk model shall cover all types of encounters and accidents that are possible within the advanced ATM operation considered, taking into account the collected information and the hazards identified. The risk model is developed iteratively; each iteration consists of a model synthesis step and a model verification step:

- Model synthesis. Using the initial description of the various entities that play a role in the advanced operation, for each of them a high level performance model is instantiated. Obviously, this includes the development of the interaction models and a valid parameterisation. This model development should be done incrementally, starting from a high level, until all relevant encounters, accident types and the possible effects of all hazards are covered. If information is missing, additional information is collected from statistical analysis of available data, domain experts.
- Model verification; During this step, it is verified whether the operational procedures, the humans, the technical systems and the identified hazards and accident types are properly covered by the model developed thus far. For each hazard (or hazardous event) it is verified how it is taken into account by the model. If relevant hazards (or hazardous events) are not appropriately covered yet then a next iteration is necessary. If all hazards are sufficiently covered then the model is frozen, and valid hazard aggregations can be made.

Model based evaluation

This is the process in which to evaluate, in a quantitative way, the frequencies of various accidents happening during particular flight phases and for particular encounter classes on the basis of the model developed. Although it definitively is possible to realise Monte Carlo[2] simulations with the developed model, this will not be really effective for the assessment of catastrophic risks in aviation. In order to develop an effective approach to the numerical evaluation, the model should first be analysed by safety analysts with the appropriate background in stochastic analysis, with the aim to decompose the accident risk estimation into an effective sequence of conditional evaluations, each of which can be accomplished through Monte Carlo simulations and/or analytical evaluations. To be more specific, the risk evaluation can be done in the following steps, which are performed for each encounter type separately:

- Decomposition of risk evaluation. Because of the extremely low probability of accidents, and the very large number of possible adverse event sequences, the idea is to evaluate the risks not for each adverse combination of events, but only for particular classes of event sequences per accident type (think of them as potential scenarios per accident type). In addition it is necessary to evaluate the probability of the occurrence of an accident conditional on the occurrence of an arbitrary event sequence of that particular class. Following this idea, the risk decomposition problem asks for analysing which classes of event sequences are particularly useful for an effective decomposition. For complex and new operations these event sequence classes are identified with the help of feedback from Monte Carlo simulations.

2 Monte Carlo simulation involves running a fast-time simulation many times, each run of which uses randomly drawn input samples.

- Evaluation of the probability distribution for the identified classes of event sequences. This step is performed by Monte Carlo simulation of the risk model, in combination with verification through analytical model evaluations.
- Evaluation of the conditional accident probabilities. For each particular class of event sequences, the probability densities of the relevant aircraft state components are evaluated. This is done by Monte Carlo simulations and fitting the resulting histograms by analytical probability density functions. The resulting density fits form the input of appropriate accident risk and/or wake vortex induced risk models.
- Combination of risk results. Using the law of total probability, the results of the previous steps are first combined into accident risks per encounter/accident type, and subsequently into total risks per accident type for the operation considered.

A crucial issue concerns the validation that a risk assessment exercise is performed to an acceptable degree, without the need to first employ very expensive large scale real-time simulations of new concepts. There are three types of validation/corroboration possible [TOSCA-WP4, 1999]:

- Judge the level of conservatism of the assumptions adopted for the development of the stochastic model instantiation for the situation considered. This should be done with active involvement of operational and design experts.
- Let ATCo's and pilots (subjectively) judge the outcomes of risk assessments executed for existing operations, and count for these operations relevant incident types for which statistical information has been collected in the past.
- Perform dedicated model based evaluations to compare the outcomes with empirical data available from dedicated real-time experiments.

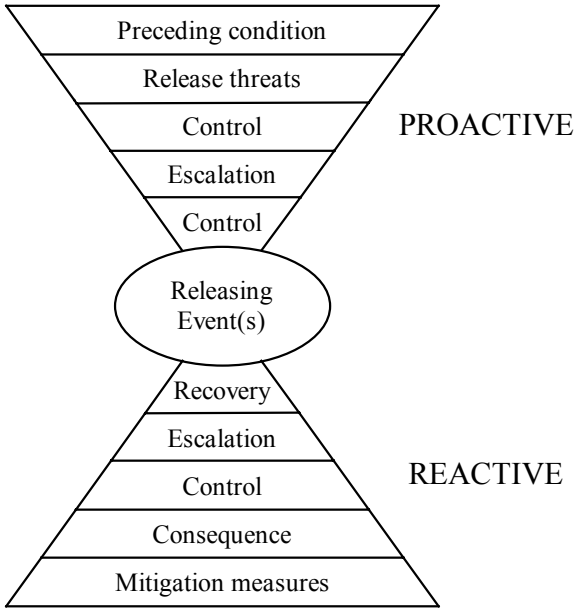


Figure 18: An adapted version of the Bow-Tie in [Edwards, 1999]. The original bow tie shape has been rotated by 90 degrees:

9.5 Potential proactive and reactive measures

If the "adverse conditions" are classified as being broadly acceptable, then the normal procedures suffice from a safety perspective. However, if there are "adverse conditions" classified as being "Tolerable" or "Intolerable" then it is necessary to develop risk reducing measures for these "adverse conditions". In [ARIBA-WP3, 1999] it has been identified that petrochemical industry has made significant methodological advances in the development of safety increasing measures during the design of and Safety Case building for an operation. In support of the risk assessment methodology discussed so far, the key complementary element of these methodological advances is an approach to structure brainstorming sessions, with experts of the advanced operation, that are aimed to collect potential risk reducing measures for the operation considered [Edwards, 1999]. The enabling paradigm for this is named the Bow-Tie, which is depicted in Figure 18.

Figure 18 actually presents a generalised version of the Bow-Tie approach that is aimed at a better support of the more demanding complexity of ATM. The objective of the Bow-Tie approach is to collect for each key "adverse condition" two types of measures:

- Proactive measures; to improve the chances to avoid entering the adverse condition at all,
- Reactive measures; to improve the chances to escape from the adverse condition prior to its escalation.

The Bow-Tie in Figure 18 depicts the sequence of steps along which the brainstorm sessions have to be guided for each of the "adverse conditions".

To collect proactive measures, brainstorm sessions pass the following steps:

- Identification of the condition that precedes the "adverse condition" considered.
- Identification of the Threats that could release the "adverse condition".
- Assessment of the Threat Controls already in place and the identification of additional controls that may be necessary to manage the threat effectively.
- Identification of the Escalation Factors that are conditions that prevent a threat control being effective.
- Assessment of Escalation Controls which are further measures needed to maintain control of the escalation factors.

To collect reactive measures, brainstorm sessions pass the following steps:

- Identification of the event(s) that could release the "adverse condition" considered.
- Assessment of Recovery Measures that would be appropriate to return the situation to as near to normal as possible.
- Identification of the Escalation Factors, which are conditions that prevent a recovery measure being effective.
- Assessment of the Escalation Controls, which are further measures needed to maintain control of the escalation factor.
- Assessment of the Consequences that may be incurred if controls fail.

- Identification of the Mitigation Measures that must be taken to reduce the effect of the consequences to a minimum.

The outcomes of these brainstorm sessions are documented, and the effects of the proactive and reactive measures are initially analysed in a qualitative way, with support from advanced operation experts. The particular usage of this feedback depends of the particular life cycle phase of the advanced operation. It is evident that during the conceptual phase more reactive and proactive measures are still feasible than during later phases in the life cycle. This implies that the development of those measures could be significantly more cost-effective if this is done during the early phases.

9.6 Feedback to advanced ATM operation

Risk tolerability of the operation can now be assessed by comparing the accident risk results with the risk criteria. To do so, the risk estimation figures can be placed in the applicable accident risk tolerability matrix (e.g. Table 4). If the risks are negligible, the normal safety management approach would be sufficient. If the risks fall in the ALARP region, additional risk reduction measures should be incorporated. The safety criticality analysis determines which elements in the operation are most critical with respect to safety, i.e. it analyses which hazards can be alleviated best to reduce risk. The information provided by the risk evaluation has far more uses than the straightforward application of risk values. In particular, since the risk is decomposed into several classes of event sequences, the risk associated with each class of event sequence is available. By identifying those classes of event sequences that have an associated risk of the order of magnitude of the total risk (of the accident type), safety criticality at the level of event sequences is identified. The risk can also be traced back further by identifying the ATM entities whose performance is critical for the occurrence of the most risky event sequences.

In addition to this, safety analysts should subsequently extract the main “adverse conditions” from the safety critical event sequences, and classify them in the JAR-based tolerability matrix (Table 3). In general, there is now less uncertainty than during the qualitative hazard analysis, for two reasons: 1) a more objective identification of the key “adverse conditions”, and 2) more precision in the classification of the key “adverse conditions” according to their severity and frequency in the “adverse condition” tolerability matrix.

The results of these risk tolerability and safety criticality assessments provide feedback at the three levels of advanced operation design, depicted in figure 14:

- Safety management of the advanced operation. The risk tolerability specifies how well the advanced ATM operation considered satisfies the Safety goals if it satisfies the Capacity goals. It typically is a safety management responsibility to decide to continue with the next phase of the life cycle of an operation, or to decide to first improve the advanced operation before going to the next phase.
- Dependability requirements. During the accident risk assessment step particular assumptions with respect to the dependability of technical systems involved are

made. It is important to identify if and how far these contribute to the safety criticality. If they do not, the dependability assumptions form a useful basis for setting better requirements on the technical systems, and to feedback these findings to the designers/manufacturers of technical systems.

- Human centred automation requirements. If the safety criticality of the advanced operation is (partly) due to human cognitive workload, then it is important to identify for which classes of event sequences this is the case, and to feedback these findings to the designers of the advanced ATM operation. A complementary way to feedback the safety assessment findings to these designers is to use dedicated brainstorming sessions for the generation of possible measures to reduce the key safety critical event sequences.

10. Guidelines on safety validation of an operation

10.1 Key findings

When introducing a new or a changed operation in ATM, the Modern Safety Case concept provides an appropriate means to guide the development and safety validation of that change, and to make the progress visible to others (e.g. project management, safety management, top management, other actors, certifying authority). If a changed or new ATM operation involves safety responsibilities from multiple service providers, then two complementary types of safety cases have to be produced: a Joint Safety Case by all service providers together, and a Modern Safety Case by each of the service providers. The Joint Safety Case concept has been newly proposed during the ARIBA consolidation, while the Modern Safety Case concept has been well developed by UK-CAA for ATM changes that involve one service provider only. The building phases of the Modern Safety Cases appeared to be useful for the Joint Safety Case as well.

For the design of an ATM operation, safety should be considered from three complementary perspectives: Safety perception by pilots and ATCo's, Dependability of technical systems and Accident risk of the operation. Each of these safety perspectives may give rise to complementary requirements. For the safety cases this means that there is need for various safety-related evaluations, the application of which should be effective from the early life-cycle phases of the advanced ATM design on. For this purpose, an outline of state-of-the–art safety-related evaluation techniques has been developed. This leads to guidelines in the following four areas:

- Joint and Modern Safety Cases,
- Dependability assessment methodology,
- Accident risk assessment methodology,
- Integration with other ATM evaluation developments.

The specific guidelines are given in the next four subsections.

10.2 Building Joint and Modern Safety Cases

So far, the elaboration of Joint and Modern Safety Cases has been done at a high level only. Thus a lot of details still need to be developed. Issues that deserve particular attention are the co-ordination of responsibilities and safety management for the new or changed operation by the air traffic service providers and other commercial-like actors involved.

A question that could easily arise is what should be implemented first, a modern safety case, or a safety management system. It is important to recognise that the modern safety case assumes that there is an adequate form of safety management arranged for the advanced operation only. Thus there is no obligation that all service providers involved have a fully working Safety Management System (e.g. Annex C of [ARIBA-WP6-II]). What should be arranged, however, is that an appropriate

integrated safety management for the new or changed operation is agreed jointly by the service providers involved.

The further development of Joint and Modern Safety Cases can best be done on the basis of some concrete and relevant ATM operation changes that involve safety responsibilities from more than one service provider. It would also be logical that this is done with active involvement of EUROCONTROL.

10.3 Dependability assessment methodology

For technical systems that are designed from scratch, proven dependability techniques are available from the aviation industry. These have been used as a basis to develop EUROCONTROL's initial safety assessment methodology [EHQ-SAM, 1999]. For a given (e.g. compilers) or an existing technical system (e.g. external networks) these techniques do not suffice. For those technical systems alternative approaches have to be developed that can be applied by manufacturers and by service providers. For manufacturers this is also identified in Part III. For service providers, however, this need also applies; e.g. in ATM the various technical systems often make part of a much larger network that extends beyond the borders of the national service providers. Examples are telecommunication systems, satellite based navigation and surveillance systems, flight planning systems, etc. With the growth of these networks the dependability problem may grow unnoticed. The established dependability techniques such as CCA, FMEA and FTA fall short to bring the dynamic performance of these networks of systems into account. In order to prevent any surprise it definitively is necessary to develop advanced evaluation techniques for the provision of dependability feedback during the further extension of the usage of these networks by air traffic service providers.

10.4 Accident risk assessment methodology

The safety validation of a change to an ATM operation often is relatively simple if traffic demand is relatively low. Since the motivation for introducing changes to ATM operations often stems from the need to increase capacity in a safe way, there also is often a safety validation need. The implication is that feedback from accident risk evaluations is coming into the picture although nobody ever asked for it explicitly. Due to the highly distributed nature of ATM, the techniques established in other safety-critical domains appeared to fall short in performing an adequate risk assessment for ATM operations. Fortunately, a lot of developments in this challenging area have already been accomplished, even for the notoriously difficult ones like wake vortex induced accident risk, collision risk, human cognitive behaviour and interactions between human, procedures and technical systems. In view of this, there are good reasons to continue the further development of accident risk methodology for ATM firmly. Best would be to do so for particular advanced ATM operations, with support from the service providing actors involved with that operation, and with active participation of:

- Safety analysts,
- Cognitive psychologists,

- Designers of the operation,
- Licensed pilots,
- ATCo's,
- Air traffic operation experts,
- Cockpit automation experts,
- ATM automation experts,
- CNS domain experts.

One should be aware that for accident risk modelling and evaluation, it is necessary to involve the active participation of mathematicians with background in stochastic analysis. The motivation for this, largely stems from the complexity that is due to the interactions between the humans, procedures and technical systems. For many other state-of-the-art techniques this does not apply, and a widespread use by air traffic service providers could therefore be arranged as part of implementing safety management.

With respect to the further development and application of advanced risk assessment in ATM, several research projects are ongoing or are planned, such as:
- Elaborate accident risk assessment methodology for EUROCONTROL (TOSCA)
- Development of System-wide safety models for NASA
- Assess wake vortex induced accident risk for DFS (HALS)
- Development of risk assessment supporting tools for NLR (TOPAZ)
- Human cognitive models and stochastic analysis techniques for NLR (DYNAMO)
- Assess impact of air derived data on safety/capacity for EC-DGXIII (DADI)
- Modelling of wake vortex induced accident risk for EC-DGXII (S-WAKE)
- Assess ADS-B impact on safety/capacity for EC-DGVII (EMERTA)
- Modelling of airport accident risk for EC-DGVII (OPAL)

10.5 Integration with other evaluation methodologies.

For accident risk assessment the operation to be evaluated should be specified in nominal and non-nominal detail. Many of the nominal details are also necessary as input to a task load analysis or a fast time simulation with e.g. TAAM or RAMS. As such, it seems logical to look for an approach that enables the integration of the modelling and simulation for accident risk assessment, with those for task load analysis and those for fast time simulation.

Another relevant connection is that the development of cognitive models for the pilots and the ATCo's could also serve other important applications, such as human cognitive/error based evaluations [EHQ-HER, 1999] of traffic monitoring data, incidents and accidents, and latent hazardous conditions. It would be most effective to arrange for an integration of these developments. In general, these models are quite complex and of a dynamic and stochastic nature. As such, it could be recommended to accomplish these model developments through a collaboration of cognitive psychologists and stochastic analysts. The results obtained in [ARIBA-WP4] illustrate the use of such collaboration.

Another area for integration is to develop a co-ordination between safety validation and overall validation [EHQ-EVAS, 1998]. Without a systematic co-ordination there easily grows a Babylonian communication problem. A sound framework for such co-ordination could be obtained by using Business Cases in combination with the Joint and Modern Safety Cases as a blue print for an effective organisation. This could also provide an additional basis for the classification of particular validation activities within a Validation Data Repository.

Part III - Safety validation of ATM automated systems by manufacturer

Authors: M. Sourimant and Luc Maltier (Airsys ATM France)

The aim of Part III is to consolidate a cost-effective safety validation methodological framework for manufacturers of ATM automation systems.

This part first discusses the problem of safety validation for an automated ATM system, and the organisation of resulting data into a safety case (section 11). Then, in sections 12, 13 and 14 the proposed methodological framework for safety validation of an automated system is presented. A few guidelines for actual implementation of this framework and conclusions are presented in section 15.

11. Safety validation of an ATM automated system

11.1 The problem to be solved

In Part III of this document, we are concerned with the question: How do we meet the requirements stemming from general principles and operational concept, regarding the automated system (i.e. the automated part of the advanced ATM system, but keeping in mind that it is to be used by human beings). More precisely, the problem addressed is the following:

An automated ATM system, or an update to an automated system, has to be developed. A list of requirements is available, including some requirements related to safety or impacting on safety. **What methodology should be used to validate safety of this system?**

Needs raised by this question may be classified into:
- need of assessable safety validation criteria for the automated system
- need of safety validation methods to assess performance against these criteria

11.2 Safety Validation Criteria

Safety criteria must be translated into metrics before safety can be assessed. However it is impossible to **prove** rigorously that an ATM system will have some level of **safety** in the future. So direct safety metrics, such as the number of fatalities by passenger-kilometre, have to be ruled out, except possibly for already operational systems.

The only way to assess safety is to find factors that have a (more or less direct) impact on safety, and then, when possible, to define metrics for each of these factors. Such safety factors are, for example, reliability or availability of the automated system.
But even for such metrics, it is often difficult to get figures. Therefore practical metrics often has to be still more indirect, and this analysis must be iterated until measurable indicators are found. For example, such measurable indicators may be test coverage, code complexity (measured through standard metrics), methods used for development and for ensuring safety and to what degree they were used, etc. Feedback from operational systems is required for this analysis (see Section 15).

Then, different **methods** have to be used for assessing safety of the system, depending on chosen criteria and metrics. The methodological framework proposes a number of methods to be used for ensuring safety.

Some characteristics which make safety validation of ATM automated systems very difficult are as follows:
- ATM automated systems are always complex, because the problems they deal with are complex, as are nuclear power plants, oil production platforms, etc.

- this complexity makes the development of complete systems from the beginning very costly; therefore, most systems are based on previous systems, and also use already developed COTS products, which has a strong impact on safety validation
- the system is used by human controllers, and the "man-machine coupling" is difficult to validate for safety, although it has a major impact on safety
- interfacing of the automated system with the external world is complex, due to the variety of current systems and people involved.
- proving rigorously that an ATM system has some safety characteristics is impossible (e.g. it is impossible to prove that there will be no accidents, or less than 1 accident every 15 years, in traffic controlled by this system). However it is possible to express the system safety requirements and assess the system against them. Therefore, the way of expressing safety requirements is of the utmost importance, and it is currently very heterogeneous.

Throughout the whole report, priority has been given to practicality, and to methods experimented in the ATM domain, in order to ensure that what is proposed is actually applicable, based on experience and feedback available.

11.3 Building a safety case for an automated system by a manufacturer

A safety case is a consistent and coherent set of arguments and evidence that the system meets or exceeds the system safety standard or target, used to justify the safety of a system.
The safety case proposed in this part is of the classical type, as opposed to the "modern" safety case, to be built by the ATM service provider, and which is more based on the operational use and operational conditions of use of the system.

WP5 recognises three approaches for obtaining evidence for justifying this safety:

- Approach 1 : Use of development standards
- Approach 2 : Independent assessment
- Approach 3 : Reverse engineering

The methodology proposed in this report is based on all of those three approaches: use of development standards, assessment, and reverse engineering (as this document does not deal with responsibility issues, it is not concerned with the independence of assessment).

The major output in the methodological framework is the safety case. Inputs to the safety case are outputs of activities recommended in the methodology, which make it possible to get the required set of arguments. Inputs of these activities are very variable. Some important inputs and outputs are summarised in the figure of section 13.1.

This section briefly discusses how to organise this set of arguments into a coherent safety case.

Organisation of the safety case

The safety case proposed, after WP5, is based on a safety argument that describes:

- the safety requirements,
- the evidence available and
- the justification why the evidence should be accepted as meeting the requirements.

The first point (safety requirements) is provided by the higher level safety management of the system, and complemented by new safety requirements found necessary during analysis of these requirements for development of the automated system.

The second point (evidence) includes:

- the safety management plan and other safety-related documents and hazard and safety log files.
- log documents showing that activities required by the safety plan have been performed.
- design documents and other documents produced during development, and which can impact on the safety of the system; this especially includes test reports and review reports

It is important to define the structure of the safety case at the beginning of the programme, so that the process is organised in such a way that the required evidence emerges from activities. The general structure should be standard.

The third point (justification from evidence that safety requirements are satisfied) often proves very difficult or even impossible to really achieve (e.g. it cannot be proven that the accident rate will be inferior to a threshold, or that the average time between failures is above some value). However, evidence should be available to determine whether the controls and mitigation measures required to meet the safety requirements are in place and operating correctly. Therefore, the recommended contents includes:

- justification using standard documents providing equivalence between the kind and level of supporting evidence and resulting safety characteristics. These standard documents should be based on experience and describe what evidence is deemed necessary to justify each kind and each level of safety requirements. Of course, this kind of justification is possible only if safety requirements are always expressed in a standard way. This method should be the main way to justify safety, as it is the most objective and most standard one.
- specific arguments in the cases:
    - ♦ when the above method is not applicable (e.g. when no standard is available for this case (standard not generic enough, or too generic, or not available at all),
    - ♦ or when methods stated in the standard have not been applied for whatever reason, but good other means were possible in this specific case, etc.

12. Methodology

12.1 Basic principles

A few principles must be kept in mind by organisations in charge of the system development and safety validation:

1. safety must be ensured, even when some clear safety requirements are not explicit in the initial list of requirements. The need for new safety requirements must be reported, in order to add them when necessary.
2. no requirement should require that a system is 100% safe (all complex systems have some probability, however small, of falling into an unexpected state).
3. safety requirements (including those added) should be verifiable, and should be traced through the whole development.
4. safety assurance should be an integral part of the development life cycle from the start.
5. similarity with previous operational systems, which already are "safety-validated", is a very important factor for validating the new system; outputs from safety validation of these previous systems must be reused wherever possible, so that experience gained is not lost. Of course, they should be reused only where possible (differences in context of use often make this impossible).
6. all safety-related activities should be formally recorded, for justification reasons.

12.2 Structure of the methodological framework

This framework is composed of two complementary parts:

- indirect safety assurance, dealing with the system development process: methods are not specifically dedicated to safety, but improve safety when used;
- specific safety assurance, dealing with methods specifically addressing safety (for the automated system).

The main reasons for separating them are:

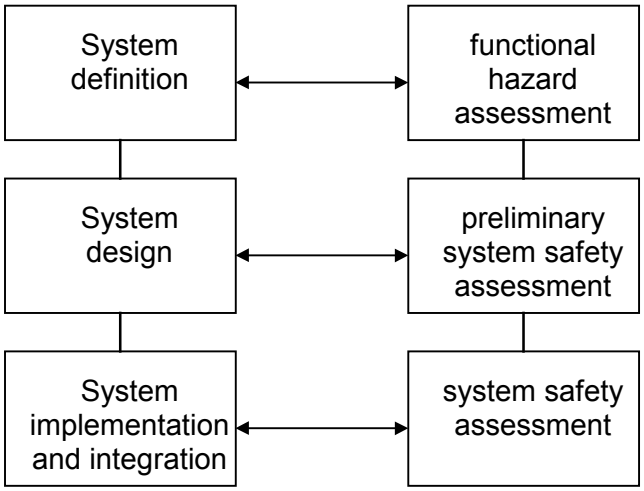
- to avoid mixing up the safety-specific part of the methodology, which is used only because the system is safety significant, with "normal" methods, which should be used even for systems which are not safety significant;
- to separate activities which a safety manager should more specifically manage.

But both parts are complementary and have to be used together in order to ensure safety. Also note that the Safety Plan described in the second part impacts on activities described in the first part. This implies that the separation made is convenient, but that all activities linked to system development should be integrated in a single system engineering process, taking into account safety issues. In both parts (13 and 14), the methodological framework is presented chronologically.

12.3 Comparison with other methodologies

This general approach to safety assurance is similar to the one recommended by ARP4754 document for aircraft development: this document states that the system development process and the safety assessment process **should interact**, and that **both should be used** for the aircraft certification process.

This approach is also consistent with the one used by EUROCONTROL Safety Assessment Methodology, as presented in the following figure:



Coverage of the life cycle in EUROCONTROL methodology

However, in order not to duplicate lots of works already or planned to be done, ARIBA focussed on aspects felt important and not or little dealt with within EUROCONTROL document:

- unlike the EUROCONTROL methodology, the present document includes a part on "indirect safety assurance" (i.e. methods to be followed all along the development cycle and which, even though not specific to safety are felt to impact the level of safety very much);
- ARIBA tries to keep a specific focus on practical issues (i.e. recommendations about how to do the work practically, e.g. for COTS);
- in ARIBA, there is also a focus on the need (felt very important) for international standardisation about the way of expressing and assessing safety requirements and rules for ensuring safety, specific to the ATM domain. (EUROCONTROL document began work on this issue, e.g. risk classification scheme).

An identification of main differences between EUROCONTROL methodology and ARIBA one is presented as an appendix in [ARIBA-WP6-III].

13. Indirect safety assurance, through the development process

13.1 Rationale

ATM systems are software-based complex systems. In such systems, although hardware failures can occur, most events with a negative impact on safety are caused by software bugs or, more generally, insufficient quality of specification, or design or implementation of the system.

Therefore, all methods used to improve and assure this quality favourably impact on safety, either directly or indirectly (through improved dependability), and are a key element of a safety case. This should not be underestimated, and this is recognised by guideline documents such as ED-12B/DO-178B, used in aircraft development. Many of the requirements stated in these guidelines are related to this kind of issue, such as the emphasis put on test coverage and partitioning.

Experience shows that, for ATM, it could be considered as a set of guidelines, with some adaptations, but that taking it as a standard to be strictly applied to ATM without any adaptation is impossible, due to specific ATM characteristics:

- very large systems
- very complex systems; this complexity sometimes makes partitioning difficult
- wide use of COTS products, both during development and in operations (including compilers, operating systems, COTS libraries, etc.)
- wide use of components already developed, either adapted or not for use in the new system (actually, new developments generally relate to a part of the system, the other parts remaining largely unchanged).

To develop these systems, a specific life cycle model is not required (this is easily adaptable to variant life cycles). However, due to main characteristics of these systems, specifying and applying reference processes covering all activities in the spirit of quality assurance standards such as ISO 9001 is recommended. Furthermore, taking into account safety aspects when specifying these processes is also recommended. In the following sections, practical methods adapted to the characteristics of ATM systems and so recommended to be used while applying these processes are described. The reader will considered them together with methods described in section 14 (Specific Safety Assurance) to get a more complete view of what is proposed as safety assurance and validation of automated systems by manufacturers).

Adaptation according to safety criticality

Not all parts of an ATM system have the same safety-criticality. The relation to safety of some of them is very remote (for example, this is the case of long term assessment

of demand to forecast the traffic level long in advance). The description assumes that the system of concern is one with direct impact on safety, such as ATC automated systems. When the safety criticality is lower, the development assurance level may also be lower. Nonetheless, it should be considered that the following recommendations apply to all parts of an advanced ATM system, except when explicitly stated.

13.2 Case for newly developed parts

Along the whole life cycle

Along the whole life cycle of safety-critical systems, the following should be used:

- **Documentation management plan:** A documentation management plan should specify documents needed and their contents, and provide templates. This is required to make information easily accessible to everybody needing it (availability or not of needed information is an important quality factor). Standard references such as DOD-STD-2167A, or a similar standard, are recommended.
- **Configuration management:** configuration management techniques are necessary to control the complexity of the system and of its successive changes (an uncontrolled system is often unsafe).
- **Requirement traceability**: A tool managing requirements traceability should be used all along the life cycle (the number of requirements usually makes manual management very tedious or even nearly impossible). Requirement traceability, including of course dependability and safety requirements, is essential to safety assurance.
- **Tools**: All tools used should be either suitably certified or proven in use. This does not apply to parts of the system that are not safety-critical.

Operational use definition

Note that this work has generally been done when specifying requirements. It can be skipped, or simply checked, in this case.

It consists in defining how its operational users will use the system. This use must be consistent with applicable operational procedures.

It is now recognised that this phase is particularly tricky, and many problems in later phases have their origin in the lack of objective data collected.

Work analysis techniques are recommended to complete the operational needs expression by objective data, which can support (or not) some of the requests. These techniques can also help to identify the tasks to be realised, data used by the operators, constraints in the work activity.

When defining the operational concept, work analysis techniques are recommended during simulations running experiments, for test of operational concepts, by explaining how operators work with the proposed operational concept. Questions are:

- What is the performance, which can be ensured using this solution?
- What does it change for the operator in terms of mental demands, required skills, and risk of error?

The recommended work analysis techniques depend on the objective or on data already available:

- **Before writing down requirements related to operational use,** knowledge-elicitation techniques (interviews with operators and more sophisticated techniques...) are recommended when there is a need to fully understand how operators work and how they take decisions. Such information is needed for validating their needs.
- **Once requirements have been written down**, they should be reviewed. This is useful for checking their completeness, consistency, ambiguities, testability, etc. The favoured technique is the **"phased inspections"** technique (see references for details). Phased inspections have the objective of guaranteeing (almost) 100% problem detection while saving much time and money. A very high problem detection rate is achieved by:
  - ♦ performing several iterations with different goals and different people (chosen according to goals),
  - ♦ using check lists and computer tools designed for assisting inspectors in their work,
  - ♦ and verifying the rigour of inspectors' work (statistics about the use of the assistance tools, questionnaires they should be able to answer...).
- **For HMI assessment,** the following **methods are recommended:**
  - ♦ As a first step, and when there it is felt that there is a high risk that the HMI will not do, HMI modelling is recommended for formal description of an HMI before implementing it, and its assessment from this description.
  - ♦ Then, fast prototyping is recommended to implement HMI requirements (at least those which involve most risk), in order to validate them with operators. A prototype is recommended whenever a new HMI is developed, in order to:
    - ⇒ make requirements "visible", so that they are more easily assessed
    - ⇒ confront involved parties to the consequences of their wishes,
    - ⇒ make sure that ATM developers understand requirements correctly.
  - ♦ Human factor techniques: once a prototype has been built, these techniques, which include such specialised work analysis methods as electrocardiograms, or eye-tracking, may be used as a complement, when equipment and experienced staff is available, to assist in validation of HMI usability requirements.

"Bid" phase

As a call for tender is usually issued for developing the new system, manufacturers have to prepare a bid, and must take safety into account during this preparation in two ways:

- analysis of safety requirements, and of the impact of other requirements on safety (see section 13.2); it is important to detect any safety-related problem in the call for tender during this phase, to be aware of possible changes which would be required;
- analysis of methods for ensuring safety required in the call for tender, when they are methods not usually used by the manufacturer, and their possible impact (on cost, duration, etc.);
- and description of the proposed safety case.

13.3 Newly developed parts

System specification
This is the phase translating operational requirements used as inputs, including dependability and safety requirements, into system requirements.
The main problem is to ensure that during this translation, safety-related requirements are considered, and that none of them get lost. This also refers to subsection 14.5 for hazard management aspects. Besides normal requirement traceability, it is useful to use the following method:

– **Definition of standard system specification rules** (especially rules intending to ensure dependability). These rules should be referred to in the specific safety assurance plan (see section 14)

Design
Methods recommended are those useful for improving the design (for all aspects of the design, and especially safety-related aspects):

- **Definition of standard design rules** (especially rules intending to ensure dependability); as a simple example, such a rule can be "always monitor periodic input, and raise an alarm when input is missing"). These rules should be referred to in the specific safety assurance plan (see section 14)
- **Prototyping**
  - ♦ before committing to the choice of a new technology during the design phase, it is important to ensure that this technology is fully understood, assessed, and mastered by ATM developers. There is always a risk in adopting new technologies, new methods, new tools, new approaches, etc. (either really new or new in the ATM domain). **Exploratory prototyping** is recommended in this case, as it is usually the best way to achieve these objectives.
  - ♦ when some difficult design choice must be done, or when an alternative must be chosen, exploratory prototyping is also recommended.
- **Dependability-related techniques**: Design choices must be validated relatively to dependability; the recommendation is that all techniques aiming at assessing dependability may be used here, but first at a high level only: input data required generally are missing, or are too unreliable to make a low level study worthwhile; only when some experience is available, providing a good feedback and reliable data, it is recommended to try these techniques at a lower level, for new systems with the same kind of design;
- when requirements imply the development of new algorithms, new protocols, etc., automated **theorem "provers"** may help to prove their correctness (thus mitigating one of the risk factors).
- **Performance modelling and simulation**: In simple cases, it is recommended to validate design choices, relatively to performance requirements, by modelling and simulating the system through specialised tools. Results should be later refined all along the life cycle, as more precise data become available, and especially when

considering the development of successive releases of the same system (or the same family of systems).

- **Reviews**: again, reviews are strongly recommended for design documents: studies show that the design phase is a major source of errors. The **"phased inspections"** technique is favoured (see above).

Software coding

- **Programming rules** are required and must have the following objectives:
  - ♦ ensuring robustness; for example, the policy to be used for dealing with exceptions should be defined. The robustness property is essential to dependability assurance, as not all situations are foreseeable.
  - ♦ ensuring correctness and readability; for example, using different variables with about the same meaning and almost the same name may lead to errors difficult to detect; programming rules should prevent this kind of errors;
- **Testing**: testing is a requirement, and is the traditional way to remove dependability risks linked to programming errors; testing groups many techniques which aim to discover errors in programs (i.e. non-conformance to specification). These techniques are well known, and do not require further development in this report; the following points are part of the methodological framework.
  - ♦ It must be kept in mind that a 100% test coverage is impractical in such complex systems.
  - ♦ Nonetheless, (not too high) test coverage objectives have to be defined, and checked. These objectives should be defined according to the safety impact of the component (higher in components impacting much on safety, in accordance with subsection 14.6 below).
  - ♦ Tests should be reusable (for use as regression tests); test programs can be used for that. Commercial tools are available and are recommended here for producing reusable HMI tests. Generally speaking, it is recommended to automate testing to the maximum extent.
  - ♦ Failure modes must be tested.
  - ♦ Orthogonal testing (i.e. testing that unwanted things do not happen) should not be forgotten.
  - ♦ Another technique must be used to make up for the incomplete test coverage.
- **Reviews**: This is a good complement to testing, as there is no better method to detect errors not detected by testing. The "phased inspections" technique, aiming at 100% default detection, is favoured (see above). This technique is very appropriate, as software programming is its primary field of application. It is recommended to use automated tools to the maximum extent to assist this work, and to develop them if needed. A complete coverage of source code, especially for all components likely to impact on safety, is possible and recommended (except for code generated by code generators). This has to be done as part of an optimised strategy describing tests and reviews and their relative scopes, and mentioned in the specific safety assurance plan (see section 14).

Integration

- **Reviews** are recommended: the main interest of reviews (especially "phased inspections") for integration is the verification that their integration will cause no error. Interfaces between the current system and the new component must be checked with a special care. Such inspections must be automated to the maximum extent (through internal or standard tools; e.g., as a simple example, many checks on C programs interfacing may be automated by using the *lint* tool)
- **Integration testing** is required; this may use all techniques aiming at discovering errors which can appear only after integration, especially in interfacing, and in functions which use both new components and other parts of the system. Recommendations about testing given above also apply.
- **Regression testing**: this is a check that changes to the existing system have not introduced errors in previously tested parts. Its application is very simple if all tests already run have been carefully recorded. It is recommended that their use should be automated and systematic.

13.4 Special case: use of COTS software, or of already-developed software

This section addresses COTS (commercial off the shelf) software, either included as part of the system (e.g. software libraries), or used to produce the system (e.g. code generators). It mainly applies to software potentially impacting on safety (tools such as text editors are not considered here).

Most of the above recommendations cannot be applied to COTS software. The method recommended in such as case is:

- assess the safety criticality of the product, according to its intended use
- then, gather all possible information on:
  - the way this product has been developed,
  - and/or statistics on its reliability, from past experience in its use,
  - and, if an international, inter-domain, certification scheme, with specified safety levels, has been defined *(see WP2 report)*, the certified safety level of this product (if certified), together with the defined meaning of this level.
- If data gathered provide enough evidence that the product is unsafe for its intended use, discard it.
- Test this product; this is always useful to get practical experience on its use, and to evaluate it. If data gathered in the previous phase were not sufficient to provide the required trust in the product reliability, test coverage should be as wide as practicable. However, testing for ultra-high reliability requirements is not practicable.
- One of the techniques used should be fault injection to test the reaction of the COTS product and to test the robustness of the system in case of a COTS failure (see e.g. [Voas, 1999]).
- If neither available data, nor testing, provide required evidence, reverse engineering tools should be used to justify dependability. In this case, there should be a focus

on safety-related characteristics, to limit costs, as this method may be very costly (see: *ARIBA WP2 and WP5 final reports).*

- If after using above methods, there is still no sufficient evidence that using this product in this context would be safe, discard the product and find another solution. As an alternative, when missing evidence is limited, it may possible in some cases to write a "wrapper" for inclusion between the COTS product and the remaining of the system, this wrapper providing missing guarantees through appropriate checks.

Note that this work does not have to be done again, if the same product was already used for the same usage in a previous system. Available data may be used in this case, with a check that they are still valid for the new system. For data no longer valid, e.g. because of a different usage environment, the process has to be repeated.

It is good practice to write a software package to encapsulate the COTS item to only allow the propagation of wanted effects into the wider system.

14. Specific safety assurance

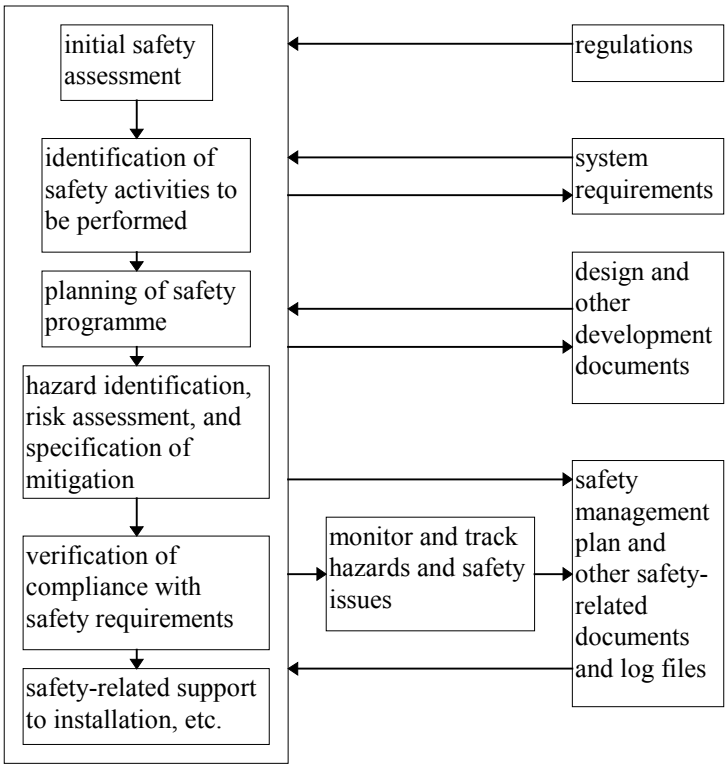
14.1 Introduction

This section applies to safety-critical parts of the system, i.e. most parts of a complete ATM system, excluding only some parts where the cost or performing recommended activities is obviously not justified by safety benefits, such as tools for long term assessment of traffic demand.

The following safety activities are recommended (excluding responsibility issues, which are dealt with in WP6.2):

- Initial safety assessment
- Assessment of safety-related activities to be performed for this system (they depend on several criteria.)
- Planning of safety programme
- Identification of hazards and specification of mitigation solutions
- Monitoring and tracking of hazards and safety issues
- Verification that the system complies with safety requirements
- Safety-related support during installation, commissioning, overall validation, and transition.

This is summarised in the following figure:



Specific safety assurance process

14.2 Initial safety assessment

This is an initial work to be performed on input data (especially requirements).
The objective is checking scope, completeness, consistency, ambiguities, testability, ...of stated safety requirements, and impact on safety of other requirements (especially identification of "unsafe" requirements).
New safety requirements may have to be added during this activity, either for legal reasons, or because of the safety policy of manufacturer involved, or simply because it is found that stated requirements are not sufficient to guarantee a safe system.
It is a recommended to use:

- a standard check list of rules that requirements specification must respect (for example: the allowed domain of input values must be specified, as well as the behaviour of the system in case of a value outside its domain);
- standard recommendations for hardware selection

Currently, one of the major problems is the great variety in the expression of safety requirements, and in levels of safety required, without any clear reasons for these differences. Therefore, the **generalised use of unique reference standards, adapted to the ATM domain, is recommended for description of safety requirements**. In these standards, numerical figures should not be the primary references, as assessment of numerical figures is often disputable.
More generally, this phase should be supported by **standard specification rules related to safety**, together with standard checklists to assist in the application of these rules.

The favoured method is reviews, and more specifically the **"phased inspections"** technique, already addressed above.

14.3 Assessment of safety activities to be performed

This is tailoring the recommended framework to actual needs and requirements, when needed.
This is needed in the cases below.

- The system (or more probably the considered component) does not have a significant impact on safety.
- The system is very similar to one for which safety activities have already been done; in this case, already available results may and should be reused, wherever possible.
- Stated requirements include the requirement that some other methodology should be used for this development, instead of, or in complement to, the recommended methodological framework. Parts of the framework impacted by this requirement should be adapted accordingly.

No technique is specifically recommended, but principles of inspections should be used, such as the use of checklists.

14.4 Planning of safety programme

This is the production of a Safety Plan, specifying all required activities related to safety. It should be based on a standard content, adapted to the system of concern, according to safety requirements and to above assessment, and agreed by the future user of the system.
The Safety Plan should include:

- references to other standards applicable (without duplicating them);
- safety-related activities to be performed (by all organisations participating in the development), when they must be performed, and which methods must be used;
- references to documents describing these methods;
- roles, and competence and organisational interfaces;
- deliverables from the safety programme;
- how and when information on safety-related activities should be recorded.

It should also describe required actions, and allowed or required adaptations to the methodology, in non-nominal situations. A typical case is the occurrence of large delays or budget problems during development. If these difficult situations have not been explicitly considered, they might have a negative impact on safety, in practice (although they should not, in theory).
The recommended approach is that the safety plan should keep all activities that are required, because activities had been specified to ensure safety in the most cost-effective way, and to very clearly explain why they are required. Some adaptations could however prove useful, either to make safety activities still more rigorous, and/or to lower the level of stress whilst maintaining effectiveness of the process (e.g. changes in organisation of work).

All members of the teams involved in development and safety assessment must receive appropriate briefing and training about the safety policy, including those not present at the beginning of the project.

14.5 Hazard management

The objective is to identify possible hazards and associated risks, and possible causes of these hazardous conditions, in order to produce a safe system.

This includes:

- Choice or definition of a Risk Classification Scheme, including:
  - ♦ severity categories, with precise definitions
  - ♦ classes of likelihood
  - ♦ classes of risk tolerability

  This should be done very early in the process, and should be based on a standard scheme, but with verification that this standard scheme is adapted to the system and context considered.
  This is not related to the automated system itself, but the resulting scheme is a necessary input to following activities.

- Identification of hazards and failure modes; several methods should be used concurrently to get a first list as complete as possible:
  - ♦ meetings with experts and experienced people, with the help of a structured method (e.g. structured brainstorming, for getting the results of brainstorming in a structured framework)
  - ♦ use of lists already available for similar systems, and from reference books, and from actual historical accident and incident logs,
  - ♦ FHA (Functional Hazard Analysis), at a level depending of the system complexity. Using this method at a very low level for a very complex system is not practicable.
  - ♦ Techniques such as FMECA (Failure Mode, Effects and Criticality Analysis). Their scope of application depends on the system complexity. For complex systems such as a complete ATC system, it can only be done, in practice, at a very high level (high-level components of the system, and communication between these components).

  Once this list of hazards is available, it should be reviewed (for completeness, relevance, consistency, etc.) The "structured inspections" technique is favoured for this review.
  - ♦ Assignment of a severity to each hazard: this depends on possible consequences of each hazard, and must follow the Risk Classification Scheme. This should be done through meetings with experts and experienced people, with the help of a structured method
- Estimation of hazard likelihood: this evaluates how often the hazard could happen (frequency of occurrence by hour and for the projected lifetime of the system). This evaluation should be based on the study of initiating events, contributing factors, and probability of failure of features aiming at removing this hazard. Techniques favoured are:
  - ♦ established techniques, such as Fault Tree Analysis, remaining at a rather high level, in the case of complex systems;
  - ♦ stochastic techniques when feasible; this requires availability of experienced specialists, necessary data and models, etc.; for example, refer to ARIBA WP4 report and to Fota's and Blom's papers (see references).
- Risk assessment; this combines hazard severity and hazard likelihood to estimate the risk produced by each hazard, and to compare this estimate with previously defined thresholds of acceptability and tolerability. This is the goal of practices such as PSSA (preliminary system safety assessment).
- Risk reduction; this activity defines the means to be used, adaptations to be done to the design, etc. in order to ensure that the system produced is at least tolerably safe. This may be through:
  - ♦ removal of all unacceptable hazards, where practicable;
  - ♦ mitigation of hazards not removed to an acceptable level.

  This may require:
  - ♦ re-specification
  - ♦ re-design
  - ♦ incorporation of safety features
  - ♦ incorporation of warning devices

♦ new operating and training procedures.

Techniques to be used depend much on the problem to be solved. All techniques aiming at improving reliability should very often be considered (e.g. replication of critical components).

Hazard likelihood and risk assessment should be updated once solutions have been defined. Where the risk cannot be reduced to an acceptable level, the activity should be stopped.

14.6 Verification that the system complies with safety requirements

This is part of the normal life cycle, which is not specific to safety (testing and reviews).

However:

- In the case of safety-related requirements, results of tests and reviews should be specifically reviewed and checked.
- Techniques used in other domains for System Safety Assessment may be used when practicable.
- When mitigating features have been added their efficacy should be specifically tested.

14.7 Safety-related support during installation, commissioning, overall validation, transition, operation

All identified hazards, their characteristics, the source of their identification, solutions chosen to solve safety risks they raise, and, generally speaking, everything concerning safety-related issues should be recorded in a safety log, augmented with new information all along the life cycle.

Safety may be impaired by the way a system is installed, operated or maintained. A support activity is often required in order that the (safe) system is used in a safe way.

It is especially important that system developers provide all information about the automated system, which is necessary for the operator of the system to organise operations in a safe way.

Of course, whenever it is intended to use the system in a different manner, or when changes are to be incorporated, additional safety analysis is essential.

15. Guidelines for implementation of the methodological framework

15.1 Summary of what needs to be standardised

The methodology proposed above recommends that some standards should be decided for ATM systems. They are summarised below.

- Standards related to expression and assessment of safety requirements. These standards should be international.
  - ♦ Standard way of expressing safety requirements (e.g. standard, and practical, metrics). This includes the definition of standard safety levels and a standard checklist of rules that these requirements must respect (including rules not specific to safety, such as consistency, and their verifiability).
  - ♦ When possible, standard recommended safety requirements for each high level function (e.g. communication between components of the system), in order to prevent too much heterogeneity in operational ATM systems.
  - ♦ Standard risk classification scheme.
  - ♦ Standard equivalence between safety characteristics (safety level, etc.) required and the kind and level of supporting evidence justifying these safety characteristics.
- Standards used for ensuring safety. These standards may be either international recommendations, or specific to each manufacturer. When they are referred to in the first category standards, they should have an international definition. In any case, they should not be made mandatory, as each manufacturer is responsible for techniques it uses for meeting requirements, and they must be free to use innovative and most appropriate techniques. Such "standards" mentioned in this documents are:
  - ♦ standard list of system specification rules, for ensuring safety;
  - ♦ standard list of design rules, for ensuring safety;
  - ♦ standard recommendations for hardware selection;
  - ♦ standard contents of a Safety Plan, and of a Safety Case.

15.2 Implementation at manufacturers

This document does not discuss responsibilities, but most activities recommended should obviously be undertaken by manufacturers.

As these activities have been designed to be as cost-effective as possible and they belong to the kind of activities normally performed by manufacturers, their implementation is considered realistic.

Of course, the effectiveness of the recommended activities is also dependent on the degree of commitment and collaboration with the buyers, users, and regulators, who should provide information required. Manufacturers also need to provide information about the limitations of use of the system supplied to the service provider so that they can make decisions ensuring the safety of their service provision.

However, some of the validation activities mentioned (such as eye-tracking) belong more to the field of activity of research institutes, and require availability of operational controllers, of specialists of the techniques, and specific equipment, which are not usually available at the manufacturers. Therefore, these activities normally are the responsibility of service providers.
As with other techniques, manufacturers should be left free to use them or not and, if they choose to use them, to perform relevant activities themselves or by collaborating with high-level external specialists.

In some cases, ATM service providers may also have to perform tasks described here because integration requires it (e.g. integration of technical subsystems that are property of different ATM service providers and delivered by different manufacturers).

15.3 Further work

Further work is mainly on the development of recommended standards.
The major challenge is the development of an objective correspondence between safety levels and supporting evidence that allows confidence that some safety level has been reached. This requires a safety forecasting model, using, as only inputs, indicators that are both measurable and available before this system is operationally used. To build and improve this model, data and feedback from operational systems is necessary.
Depending on the results of this study, the development of some new validation techniques could be required too.

15.4 Possible schedule for implementation

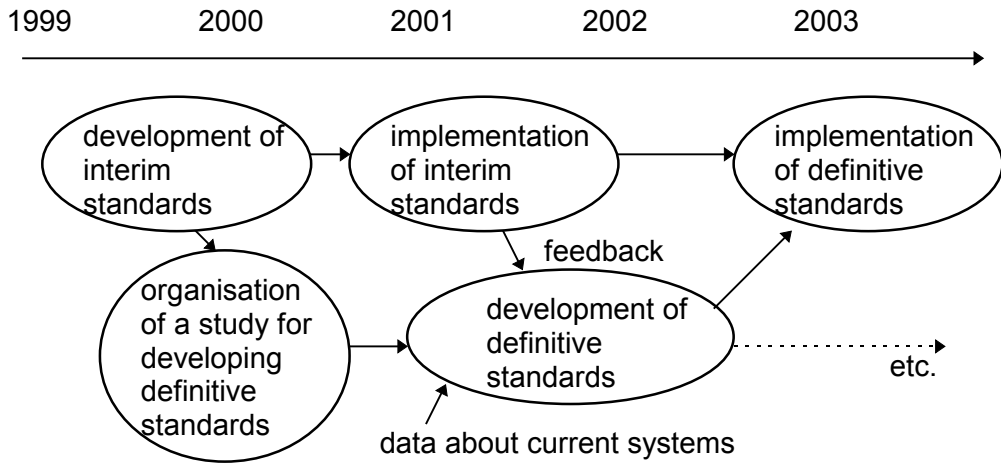
The schedule of implementation might be divided into three phases:

First phase:
- Development of an interim version of recommended standards, based on best current practices, and on improvements which can be implemented quickly.
- Organisation of a study to develop the second version of standards, including a first model for safety forecasting.

Second phase:
- Implementation of interim standards in relevant organisations.
- Collection of feedback information from this implementation.
- Development of the second, improved, version of standards.

Third phase:
- Implementation of definitive standards in relevant organisations.

The associated schedule might be:



However, this schedule is probably too optimistic for the definition of mandatory standards, given the delay generally required for standardisation by ICAO and other worldwide organisations.
Therefore, as a first step, it is proposed that standards should be developed and recommended, but not made mandatory, until the definitive international decisions.

15.5 Conclusions

Part III consolidated previous ARIBA results related to safety validation of ATM automation systems by providing a methodological framework.

The problem addressed is very complex, due to the complexity of systems themselves and the number of stakeholders, and the difficulty to assess safety of a system.

To address this complexity, the report makes the following main recommendations:

- use of some international standards related to safety validation, to be specifically developed for ATM;
- use of some cost-effective methods all along the development, both for ensuring safety through development activities, and through specific safety assurance;
- validation of safety of the automated system by measuring indirect safety factors, and making a correspondence with actual safety objectives in a safety case;
- permanent consideration of practicality when developing safety validation standards.

References

[Airsys] Process used to assure safety at Airsys ATM (internal document).

[AGARD, 1998] AGARD, A designer's guide to human performance modelling, AGARD Advisory report 356, December 1998.

[Aldemir et al, 1994] T. Aldemir, N.O. Siu, A. Mosleh, P.C. Cacciabue and B.G. Göktepe (Eds.) Reliability and safety assessment of dynamic process systems, Springer, 1994.

[Amalberti & Wioland, 1997] R. Amalberti and L. Wioland, Human error in aviation, Proc. Int. Aviation Safety Conf., VSP, Utrecht, 1997, pp. 91-108.

[Amalberti et al., 1998] R. Amalberti, J. Pariès, C. Valot, F. Wibaux, Human factors in aviation: an introductory course, Ed: K.M. Goeters, Aviation Psychology: a science and a profession, Ashgate, 1998, 19-43.

[Amalberti & Wilbaux, 1994] R. Amalberti and F.Wibaux, Advanced automated glass cockpit certification: being wary of human factors, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical Univ. Press, 1994, pp. 309-319.

[APATSI, 1996] ECAC/APATSI study on validation processes in ATC, A proposal for a harmonised validation methodology, PRAXIS, January 1996.

[APATSI, 1997] ECAC/APATSI, Guidance for the validation of ATC procedures and systems, PRAXIS, January 1997.

[ARIBA, 1997] ARIBA, ATM system safety criticality raises issues in balancing actors responsibility, Technical annex to the contract with the European Commission, NLR, 1997.

[ARIBA-WP1] ATM certification perception around Europe, M. Blaize, N. Fota, E. Andlauer, C. Vansteelandt, ARIBA-WP1 report + appendices, Sofréavia, 1999.

[ARIBA-WP2] Assessment of existing certification practices, P. Leprovost et al., ARIBA-WP2 report, APTIME, 1999.

[ARIBA-WP3] Analysis of the ATM certification problem, E. Andlauer, E. Chenevier, G. Gaudiere, F. Girard and P. Hudson, ARIBA-WP3 report, Sofréavia, 1999.

[ARIBA-WP4] Human operators controllability of ATM safety, J. Daams, H.B. Nijhuis and H.A.P. Blom, ARIBA-WP4 report, NLR, 1999.

[ARIBA-WP5] Safety case assessment approach for ATM, C. Pygott, R. Furze, I. Thompson and C. Kelly, ARIBA-WP5 report, DERA, 1999.

[ARIBA-WP6-I] Safety certification framework in ATM, H.A.P. Blom and H.B. Nijhuis, ARIBA-WP6 report Part I, NLR 1999.

[ARIBA-WP6-II] Safety Cases for a new ATM operation, H.A.P. Blom, M.H.C. Everdij and J. Daams, ARIBA-WP6 report Part II, NLR, 1999.

[ARIBA-WP6-III] Safety validation of ATM automated systems by manufacturer, M. Sourimant, L. Maltier, ARIBA WP6 report Part III, Airsys ATM France, 1999.

[Bainbridge, 1993] L. Bainbridge, The change of concepts needed to account for human behaviour in complex dynamic tasks, Proc. 1993 Int. Conf. on Systems, Man and Cybernetics, pp. 126-131, 1993.

[Bakker & Blom, 1993] G.J. Bakker and H.A.P. Blom, Air Traffic Collision risk modelling, In: Proceedings of the 32nd IEEE Conf. on Decision and Control, pp.,1464-1469, December 1993.

[Barbarino et al., 1999]Team Resource Management in European Air Traffic Control, Proc. Of the 4th ICAO Global Flight Safety and Human Factors Symposium, Chile, April 1999, pp. 97-105.

[Benstead & Spriggs, 1998] P.A. Benstead and T.J. Spriggs, Safety risk classification schemes for satellite navigation, Proc. Int. Conf of the Royal Institute of Navigation NAV98, Dec. 1998, paper 34, pp. 1-10.

[Biemans & Daams, 1997] M.C.M. Biemans and J. Daams, Human Operator Modelling to Evaluate Reliability, Organisation and Safety, NLR report TR 98073, 1997.

[Blanker et al., 1997] P.J.G. Blanker, G.W.H. van Es, E. Eveleens and M.A. Piers, A method for qualitative safety assessment of proposed new flight procedures at Amsterdam Airport Schiphol, TOMS report 96-078, NLR, 1997

[Blom et al., 1998] H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij and M.B. Klompstra, Accident risk assessment for advanced ATM, 2nd USA/Europe Air Traffic Management R&D Seminar, Orlando, December 1998.

[Buck et al., 1997] S. Buck, M.C.M. Biemans, B.G. Hilburn, P.T.L.M. van Woerkom, Synthesis of functions, NLR technical report TR 97054 L, Final report RHEA/NL/WPR/2/03, 1997.

[C/AFT, 1999] CNS/ATM Focused Team, Airline metrics concepts for evaluating air traffic service performance, Report of the ATS Performance Focus Group, C/AFT, February 1999.

[CASCADE, 1998] CASCADE, Contributing for Assessment of Common ATM Development in Europe, Final report for DG7, 1998.

[Cohen et. al., 1998] S. Cohen, S. Hockaday et. al., A concept paper for separation safety modelling, FAA/EUROCONTROL, May 1998.

[Cullen, 1990] Cullen, The Lord, Report on Piper Alpha accident, HMSO, London, 1990.

[Daams et al., 1998] J. Daams, H.B. Nijhuis and H.A.P. Blom, Accident risk assessment with a human cognitive model using TOPAZ, December 1998.

[DAAS, 1995] DAAS, Dependability Approach to ATM systems, Final report for EC-DG XIII, 1995.

[EC, 1997] EC, Accreditation and the Community's Policy in the Field of Conformity Assessment, Brussels, December 1997.

[EC, 1998a] EC, European Commission authorisation to negotiate establishment of a European Aviation Safety Authority (EASA), Executive Summary for CAA Board, European Commission, July 1998.

[EC, 1998b] EC, General guidelines for the co-operation between CEN, CENELEC and ETSI and the European Commission, Information note to the Senior Officials Group on Standardisation, September 1998.

[Edwards, 1999] C.J. Edwards, Developing a Safety Case with an Aircraft Operator, In Proc. Second Annual Two-day Conference on Aviation Safety Management, May 1999.

[EHQ-2000+, 1998] EUROCONTROL, Air Traffic Management Strategy for 2000+, Brussels, 1998.

[EHQ-EVAS, 1998] EVAS, EATMS Validation Strategy Document, Edition 1.1, EUROCONTROL, Brussels, June 1998.

[EHQ-HER, 1999] EUROCONTROL, Technical review of human performance models and taxonomies of human error in ATM, Draft version 0.1, Brussels, May 1999.

[EHQ-HUM, 1996] EUROCONTROL, Model for Task and Job Descriptions of Air Traffic Controllers. EHQ document HUM.ET.-ST01.1000-REP-01. Brussels, 1996.

[EHQ-MOD, 1997] EUROCONTROL, Model of the cognitive aspects of air traffic control, Brussels, 1997.

[EHQ-POL, 1995] EUROCONTROL, EHQ Safety policy, Brussels, 1995

[EHQ-SAM, 1999] EUROCONTROL, Air Navigation System Safety Assessment Methodology, EHQ, SAF.ET1.ST03.1000-MAN-01-00, Edition 0.5, Working Draft, Brussels, 30 Apr. 1999.

[EHQ-SYMP, 1997] EUROCONTROL, Safety Management Symposium, Brussels, 1997.

[EHQ-TASK, 1998] EUROCONTROL, Integrated Task and Job Analysis of air traffic controllers, Phase 1, Development of methods, Brussels, 1998.

[Endsley, 1995] M.R. Endsley, Towards a theory of situation awareness in dynamic systems, Human Factors, Vol. 37, 1995, pp. 32-64.

[EUROCAE, 1998] EUROCAE, List of publications from the European Organisation for Civil Aviation Equipment, Paris, 1998.

[Evans, 1996] A. Evans, Risk appraisal and the valuation of injury, Contributions to the Int. Conf. Passenger safety in European public transport, Brussels, May, 1996, pp. 26-30

[Evans, 1994] A.E. Evans, Human factors certification in the development of future Air Traffic Control system, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical University Press, 1994, pp. 87-96.

[Everdij et al, 1996] M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom and O.N. Fota, Evaluation of hazard analysis techniques for application to en-route ATM, MUFTIS Safety Model, Final Report Part I, European Union DGVII, 1996.

[FRAIS, 1996] FRAIS, Functional requirements for an airport ground movement control and management interconnection system, Final report for EC-DG7, 1996.

[GENOVA, 1997] GENOVA, Generic overall validation for ATM, Final report for DG7, 1997.

[Fota et al., 1997] N. Fota, M. Kaaniche and K. Kanoun, A modular and incremental approach for building complex stochastic Petri net models, Proc. First Int. Conf. on Mathematical Methods in Reliability, 1997.

[Fron, 1998] X. Fron, ATM performance review in Europe, Proc. 2nd USA/Europe Air Traffic Management R&D Seminar, Orlando, FAA/EUROCONTROL, December 1998.

[FSF, 1999] Flight Safety Foundation, Opening remarks by S. Matthews at the 44th Annual CASS, April 1999.

[Haraldsdottir, 1997] A. Haraldsdottir et al., Air Traffic Management Concept Baseline Definition, NEXTOR report RR-97-3, Boeing, 1997.

[Helmreich, 1996] R.L. Helmreich, The evolution of Crew Resource Management, Proc. IATA Human Factors Seminar, October 1996, Warsaw, Poland, 11 pages.

[Henaku, 1998] K. Henaku, Legal issues affecting use of navigation systems, Proc. Int. Conf. of the Royal Institute of Navigation NAV98, December 1998, paper 8, pp. 1-7.

[Hollnagel, 1993] E. Hollnagel, Human Reliability analysis, context and control. Academic Press, London, 1993.

[HSE, 1995] HSE-author: A.F. Ellis, Achieving safety in complex control systems, Proc. Safety-critical systems symposium, Eds: F. Redmill and T. Anderson, Springer, 1995, pp. 1-14.

[Hudson, 1994] P.T.W. Hudson et al., Tripod Delta: proactive approach to enhanced safety, J. of Petroleum Technology, Vol. 46 (1994), pp. 58-62.

[Hudson, 1996] P.T.W. Hudson, Establishing a safety culture in transport industries, Contributions to the Int. Conf. Passenger safety in European public transport, Brussels, May, 1996, pp. 31-41.

[Hudson, 1997] P.T.W. Hudson, Safety culture in the aviation industry: a system in search of perfection, Proc. Singapore Air, 1997.

[ICAO, 1996] ICAO, Production versus safety goals, in: Proc. 3rd ICAO global flight safety and human factors symp., ICAO Circular 266-AN/158, 1996, pp. 347-348.

[ICAO, 1998] ICAO, Manual on airspace planning methodology for the determination of separation minima, Doc 9689-AN/953, First Edition, 1998.

[ICAO Annex 13] ICAO, International standards and recommended practices, Aircraft accident and incident investigation, Annex 13 to the convention on international civil aviation, 8th edition.

[ISO8402, 1994] International Standard ISO 8402, Quality management and quality assurance – Vocabulary, 2nd edition, 1994.

[ISO/IEC, 1996] ISO/IEC Guide 2, Standardization and related activities – General vocabulary, 1996 [= EN 45020, 1998].

[JAR 25.1309] Joint Aviation Requirements JAR - 25, Large Aeroplanes, Change 14, 27 May 1994, and Amendment 25/96/1 of 19 April 1996, including AMJ 25-1309: System design and analysis, Advisory Material Joint, Change 14, 1994.

[Javaux et al., 1994] D. Javaux, M. Masson and V. De Keyser, Beware of agents when flying aircraft: Basic principles behind a generic methodology for the evaluation and certification of advanced aviation systems, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical Univ. Press, 1994, pp. 321-345.

[Jones-Lee & Loomes, 1995] M.W. Jones-Lee, G. Loomes, Measuring the benefits of transport safety, Proc. Safety-critical systems symposium, Eds: F. Redmill and T. Anderson, Springer, 1995, pp. 15-47.

[Josefsson, 1999] Integrating human factors in the lifecycle of ATM systems, Proc. Of the 4th ICAO Global Flight Safety and Human Factors Symposium, Chile, April 1999, pp. 91-97.

[Jorna, 1993] P.G.M. Jorna, Operator workload as a limiting factor in complex systems, Eds: J.A. Wise, V.D. Hopkin and P. Stager, Verification and validation of complex systems: human factors issues, Springer, Berlin, 1993, pp. 281-304.

[Koelman, 1994] H. Koelman, Certification of tactics and strategies in aviation, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical Univ. Press, 1994, pp. 53-75.

[Knight & Myers, 1997] John C. Knight and E. Ann Myers. An improved inspection technique, Communications of the ACM. November 1993/Vol.36, No. 11.

[Klompstra & Everdij, 1997] M.B. Klompstra and M.H.C. Everdij, Evaluation of JAR and EHQ risk assessment methodologies, Report CR 97678 L, National Aerospace Laboratory NLR, 1997.

[Laprie, 1995] Dependability – Its attributes, impairments and means, Eds: B. Randell et al., Predictably dependable computing systems, Springer, Berlin, 1995.

[Lloyd & Tye, 1982] E. Lloyd and W. Tye, Systematic safety - safety assessment of aircraft systems, CAA, London, 1982.

[MacLeod & Taylor, 1994] I.S. MacLeod and R.M. Taylor, Does human cognition allow human factors certification of advanced aircrew systems?, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical University Press, 1994, pp. 163-186.

[Maurino & Galotti, 1994] D. Maurino and V. Galotti, Integrating human factors knowledge into certification: the point of view of ICAO, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical University Press, 1994, pp. 263-273.

[Mayes, 1997] P. Mayes, Proactive air safety investigation, The Australian experience, Ed: H. Soekkha, Proc. Int. Aviation Safety Conf., VSP, Utrecht, 1997, pp. 109-118.

[Milloy, 1998] C. Milloy, An introduction to risk acceptance criteria, Eds: H. Gluver and D. Olsen, Ship collision analysis, Balkema, Rotterdam, 1998, pp. 97-102.

[Moek et al., 1997] G. Moek, J-P. Beaujard, C. Kelly, J. Mann, L. Clarke, D. Marsh, H.A.P. Blom and M.B. Klompstra, GENeric Overall Validation for ATM, WP 3 report: Methods and Techniques, EU-DGVII, NLR, 1997.

[MUFTIS, 1996] MUFTIS, Model Use and Fast-Time Simulation studies, Final reports for EC-DGVII, 1996.

[Odoni, 1997] A.R. Odoni et al., Existing and required modeling capabilities for evaluating ATM systems and concepts, Final report, MIT, March 1997.

[O'Neil, 1998] K. O'Neil, Developing a safety culture in a highly regulated environment, In: Aviation Safety Management "Partnering for Safety", IBC, 1998

[Overall, 1995] M. Overall, Managing safety and regulating aviation safety: a new emphasis and a new relationship, in: 48th Annual International Air Traffic Safety Seminar, Flight Safety Foundation, 1995.

[Pariès, 1996] J. Pariès, Evolution of the aviation safety paradigm: towards systematic causality and proactive actions, Proc. 3rd Australian Aviation Psychology Symp., eds: B.J. Haywars and A.R. Lowe, Ashgate Publishing, 1996, pp. 39-49.

[Profit, 1995] R. Profit, Systematic Safety Management in the Air Traffic Services, Euromoney, London, 1995.

[Rasmussen, 1983] J. Rasmussen, Skills, rules and knowledge: signals, signs and symbols, and other distinction in human performance models, IEEE Transactions on System, Man and Cybernetics, Vol. 13, pp. 257-266, 1983.

[Reason, 1990] J. Reason, Human error, Cambridge Univ. Press, 1990.

[Reason, 1995] J. Reason, A systems approach to organizational error, Ergonomics, Vol. 38 (1995), pp. 1708-1721.

[RHEA, 1998] RHEA, Role of Human in the Evolution of ATM systems, Final report for DG7, 1998.

[RTCA, 1992] RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification, RTCA Inc., December 1992.

[RTCA, 1999] RTCA, Certification Final report of RTCA Task Force 4, 1999

[SAE, 1994] SAE, ARP 4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, S-18 Committee, Society of Automotive Engineers, Inc., March 1994.

[SAE, 1995] SAE ARP 4754, *Certification considerations for highly-integrated or complex aircraft systems*, Systems Integration

Requirements Task Group AS-1C, Avionics Systems Division (ASD), Society of Automotive Engineers, Inc. (SAE), September 1995.

[SAPCOM, 1998] SAPCOM (Safety Program for Commercial Operators), Aviation Safety Management - An operator's guide to building a safety program, Civil Aviation Safety Authority, Australia, 1998.

[SECAM, 1996] SECAM, Safety, Efficiency and Capacity of ATM methodologies, Final report for EC-DGVII, 1997.

[Seamster et al, 1993] T.L. Seamster, R.E. Redding, J.R. Cannon, J.M. Ryder, J.A. Purcell, Cognitive Task Analysis of Expertise in Air Traffic Control. The International Journal of Aviation Psychology, 3, 257-283, 1993.

[Seamster et al., 1997] T.L. Seamster, R.E. Redding and G.L. Kaempf, Applied cognitive task analysis in aviation, 1997.

[Shorrock & Kirwan, 1999] The development of TRACEr: a technique for the retrospective analysis of cognitive errors in ATM, Ed: D. Harris, Engineering psychology and cognitive ergonomics, Volume 3, Transportation systems, medical ergonomics and training, Ashgate, 1999, pp. 163-171.

[Short, 1998] R. Short, Organisational accidents: managing safety, In: Aviation Safety Management "Partnering for Safety", IBC, 1998

[Small & Rouse, 1994] R.L. Small and W.B. Rouse, Certify for success: a methodology for human-centered certification of advanced aviation systems, Proc. Human Factors Certification of Advanced Aviation Technologies Conference, July 1993, Embry-Riddle Aeronautical Univ. Press, 1994, pp. 125-133.

[Speijker et al., 1999] L.J.P. Speijker, H.A.P. Blom and J. Kos, Assessment of Wake Vortex Safety to Evaluate Separation Distances, Proc. Research for Safety in Civil Aviation, Paris, October 21-22, 1999

[ΣΣ, 1993] System Safety Society, System Safety Analysis handbook 1993

[TOSCA-WP1, 1998] TOSCA-II WP1, Route Network Design Strategies, NATS, 1998.

[TOSCA-WP3, 1997] TOSCA-II WP3, Assessment of the TMA to TMA hand-over concept, CENA, 1997.

[TOSCA-WP4, 1999] M.H.C. Everdij and H.A.P. Blom, Explanatory document on TOPAZ, TOSCA-II WP4 Phase 2 report, April 1999.

[TOSCA-WP5, 1998] TOSCA-II WP5, The dynamics of strategies of route networks, DERA, 1998.

[TOSCA-WP7, 1997] TOSCA-II WP7, Airport capacity enhancement Interim report, NLR/EEC, 1997.

[TOSCA-WP8, 1997] TOSCA-II WP8, Workload assessment, NATS, 1997.

[UK-CAA, 1999] Safety Regulation Group, CAP 670, Part B, Air Traffic Services Safety Requirements, Civil Aviation Authority, London, March 1999.

[VAPORETO, 1996] VAPORETO, Validation Process for Overall Requirements in air Traffic Operation, Guidelines for the convergence of validation processes in Europe, Final report for EC-DGVII, NLR, 1996.

[Voas, 1999] J. Voas, Certifying Software for High-Assurance Environments, IEEE Software, Jul./Aug. 1999, pp. 48-54.

[Westrum, 1995] R. Westrum, Organisational dynamics and safety, Eds: N. Johnston and R. Fuller, Applications of psychology to the aviation system, 1995.

[Wickens, 1992] C.D. Wickens, Engineering, psychology and human performance, Merrill, 1992.

[Wickens et al., 1997] C.D Wickens, A.S. Mavor and J.P. McGee, Flight to the Future: Human Factors in Air Traffic Control, National Academic Press, Washington, 1997.

[Wise & Wise, 1994] M.A. Wise and J.A. Wise, On the use of the systems apporach to certify advanced aviation technologies, Proc. Human Factors Certification of Advanced Aviation Technologies Conf. 1993, Embry-Riddle Aeronautical University Press, 1994, pp. 15-23.

[Wood, 1997] R.H. Wood, Aviation safety programs, A management handbook, Jeppesen, 2nd ed., 1997.

Acronyms

AAF	Airsys ATM France
ADREP	Aviation Data Reporting Program
AIP	Aeronautical Information Publication
ARINC	Aeronautical Radio, Incorporated
APT	Aptime
ARIBA	ATM system safety criticality Raises Issues in Balancing Actors responsibility
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATM	Air Traffic Management
BA	British Airways
BASI	Bureau of Air Safety Investigation
BASIS	British Airways Safety Information System
CAA	Civil Aviation Authority
CAIR	Confidential Aviation Incident Reporting
CEC	Commission of the European Communities
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation ELECtronique
CHIRP	Confidential Human Factors Incident Reporting Programme
CNS	Communication, Navigation, Surveillance
COTS	Commercial Off The Shelf
DAL	Development Assurance Level
DERA	Defence Evaluation and Research Agency
DG	Directorate General
DOD	Department Of Defence
EASA	European Aviation Safety Authority
EATCHIP	European Air Traffic Control Harmonisation and Integration Programme
EATMS	European Air Traffic Management System
EC	European Commission
ECAC	European Civil Aviation Conference
ECC-AIRS	European Co-ordination Centre for the mandatory Aircraft Incident Reporting Systems
EGNOS	European Geostationary Navigation Overlay Service
ETSI	European Telecommunication Standardisation Institute
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FHA	Functional Hazard Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FR	Final Report
FSF	Flight Safety Foundation
FTA	Fault Tree Analysis
GSN	Goal Structuring Notation
HAZOP	HAZard and OPerability Study
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HSE	Health and Safety Executive
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IEC	International Electrotechnical Commission
INMARSAT	International Maritime Satellite Organisation
ISO	International Standard Organisation
JAA	Joint Aviation Authorities
JAR	Joint Aviation Requirement

JSSI	Joint Safety Strategy Initiative
MASPS	Minimum Aviation System Performance Standards
MOPS	Minimum Operational Performance Standard
MORS	Mandatory Occurrence Reporting System
NASA	National Aeronautics and Space Administration
NLR	Nationaal Lucht- en Ruimtevaartlaboratorium
PANS	Procedures for Air Navigation Services
PSSA	Preliminary System Safety Assessment
R&D	Research and Development
RTCA	Radio Technical Commission for Aeronautics
RUL	Rijksuniversiteit Leiden
SAE	Society of Automotive Engineers
SAM	Safety Argument Manager
SAPCOM	Safety Program for Commercial Operators
SARPs	Standards and Recommended Practices
SCAA	Swedish Civil Aviation Administration
Sofréavia	Société Française d'Étude et de Réalisation d' Équipements Aéronautiques
SRG	Safety Regulation Group
SSA	System Safety Assessment
STC	Supplemental Type Certificate
SUPPS	Supplementary Procedures
TC	Type Certificate
TRTD	Transport Research and Technological Development
TSO	Technical Standard Order
WAAS	Wide Area Augmentation Service
WP#	Numbered Work Package
WPR	Work Package Report
WAAS	Wide Area Augmentation Service

Annex A: Relevant ISO terminology

Accreditation	=	Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks [ISO/IEC, 1996]
Authority	=	Body that has legal powers and rights [ISO/IEC, 1996]
Body (responsible for standards/ regulations)	=	Legal or administrative entity that has specific tasks and composition [ISO/IEC, 1996]
Certification	=	Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements [ISO/IEC, 1996]
Certification body	=	Body that conducts certification [ISO/IEC, 1996]
Dependability	=	Collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance-support performance [ISO8402, 1994]
Normative document	=	Document that provides rules, guidelines or characteristics for activities or their results [ISO/IEC, 1996]
Objective evidence	=	Information which can be proved true, based on facts obtained through observation, measurement, test or other means [ISO 8402, 1994]
Organisation	=	Body that is based on the membership of other bodies or individuals and has an established constitution and its own administration [ISO/IEC, 1996]
Provision	=	Expression in the content of a normative document, that takes the form of a statement, an instruction, a recommendation or a requirement [ISO/IEC, 1996]
Qualification process	=	Process of demonstrating whether an entity is capable of fulfilling specified requirements [ISO8402, 1994]
Regulation	=	Document providing binding legislative rules, that is adopted by an authority [ISO/IEC, 1996]
Standard	=	Document, established by consensus and approval by a recognised body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context [ISO/IEC, 1996]
Supplier's declaration	=	Procedure by which a supplier gives written assurance that a product, process or service conforms to specified requirements [ISO/IEC, 1996]
Third party	=	Person or body that is recognised as being independent of the parties involved, as concerns the issue in question [ISO/IEC, 1996]
Validation	=	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled [ISO8402, 1994]
Verification	=	Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled [ISO8402, 1994]

Annex B: JAR failure condition tolerability matrix

This annex presents the classification criteria adopted by [JAR 25.1309] for tolerability criteria for any failure condition of a technical system under design. For this outline use is made of the description provided by [Klompstra and Everdij, 1997]. For background information see e.g. [Lloyd & Tye, 1982].

Failure mode severity classification
According to [JAR 25.1309] each failure condition is classified according to its severity. The Joint Aviation Authorities (JAA) qualitative definitions of severity are given in Table B.1. These definitions are commonly accepted in civil aviation.

Table B.1: Definitions of severity categories according to JAR AMJ 25.1309

Description	Definition
Catastrophic	Failure conditions, which would prevent continued safe flight and landing.
Hazardous	Failure conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be: • A large reduction in safety margins or functional capabilities, • Physical distress or higher workload such that the flight crew cannot be relied upon to perform their task accurately or completely, or • Serious injury or fatal injury to a relatively small number of the occupants.
Major	Failure conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example: • A significant reduction in safety margins or functional capabilities, • A significant increase in crew workload or in conditions impairing crew efficiency, or • Discomfort to occupants, possibly including injuries.
Minor	Failure conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example: • Slight reduction of safety margins, • Slight increase in crew workload, or • Some inconvenience to occupants.

Failure condition frequency classification
Next, for each failure condition a classification of its frequency or probability of occurrence is given. Qualitative definitions of probability according to the JAA standard are given in Table B.2. The absence of a quantitative (numerical) scale to the Table B.2 is intentional, since it avoids a lot of confusion presently created by such

numerical scales; e.g. all existing probability scales of classification matrices quantify the probability per hour, whereas for airport related hazards probabilities per approach/departure are required.

Table B.2: Definitions of frequency levels according to JAR AMJ 25.1309.

Description	**Estimate of frequency**
Probable	Anticipated to occur one or more times during the entire operational life of each aeroplane.
Remote	Unlikely to occur to each aeroplane during its total operational life but which may occur several times when considering the total operational life of a number of aeroplanes of the type.
Extremely Remote	Unlikely to occur when considering the total operational life of all aeroplanes of the type, but nevertheless, has to be considered as being possible.
Extremely Improbable	So unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type.

In JAR, the terms probable, remote, extremely remote and extremely improbable are also expressed in terms of acceptable numerical frequency ranges for each flight hour, as follows:

Probable	Failure condition frequency is more than 10^{-5} per aircraft flight hour
Remote	Failure condition frequency is between 10^{-7} and 10^{-5} per aircraft flight hour
Extremely remote	Failure condition frequency is between 10^{-9} and 10^{-7} per aircraft flight hour
Extremely improbable	Failure condition frequency is less than 10^{-9} per aircraft flight hour

Failure condition tolerability identification

JAR AMJ 25.1309 allows failure conditions with the following combinations of severity and frequency:

- Minor severity may be probable.
- Major severity must be no more frequent than remote.
- Hazardous severity must be no more frequent than extremely remote.
- Catastrophic severity must be extremely improbable.

The classified frequency and severity are usually (though not explicitly in JAR) combined in a failure condition tolerability matrix (also known as hazard risk-matrix). In such matrix, the above stated combinations are classified as *"Tolerable"*. Combinations with a higher level of severity and/or a higher frequency of occurrence are classified as *"Intolerable"*, the remaining combinations are classified as *"Negligible"*. The result is shown in Table 6 in Section 8.5.

Annex C: EATCHIP safety assessment methodology

This annex gives a short overview of the EUROCONTROL-adopted safety assessment methodology, at its current development status [EHQ-SAM, 1999]. A comparison of an earlier version (dated Nov. 1996) of the same methodology with JAR and SAE approaches is given in [Klompstra & Everdij, 1997].

The [EHQ-SAM, 1999] document 'Air navigation system safety assessment methodology' aims at presenting a general process for the safety assessment of Air Navigation Systems. The scope of the methodology is presented as the following:

- The safety assessment methodology applies to ground-based components of Air Navigation Systems in the first instance. Later issues will address the integration of airborne and satellite systems
- The methodology considers only the safety aspects of the Air Navigation System. Other attributes of the system, aiming, for example, to achieve capacity and/or efficiency objectives, are not addressed.
- The methodology does not address Air Navigation System certification issues. However, the application of the principles could prepare to and support a certification process.
- The methodology does not address organisational aspects related to safety assessment. For each project, organisational entities involved in the safety assessment process should be identified and their respective responsibilities should be specified.

[EHQ-SAM, 1999] presents a general overview of a system safety assessment from an engineering perspective. The safety assessment activities are sub-divided into:

- Risk Assessment activities, to identify hazards and failure conditions, and evaluate the associated risk tolerability,
- Safety engineering activities, to select, validate and implement counter measures to mitigate these risks, and
- Safety assurance activities, which involve specific planned and systematic actions that together provide confidence that all relevant failure conditions have been identified, and that all significant failures that could cause or contribute to those failure conditions have been considered.

The objective of the methodology is to define a means for providing assurance that an Air Navigation System is safe for operational use. It is an iterative process conducted throughout the system development life cycle, from initial system definition, through design, implementation, integration, transfer to operations, to operations and maintenance[3]. The iterative process consists of a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and a System Safety Assessment (SSA), see Figure C.1. During PSSA and SSA, a Common Cause Analysis is done.

[3] Note that the Operations and maintenance phase has been added to the system development process in reference [EHQ, 1999], with respect to the earlier version (dated Nov. 1996).

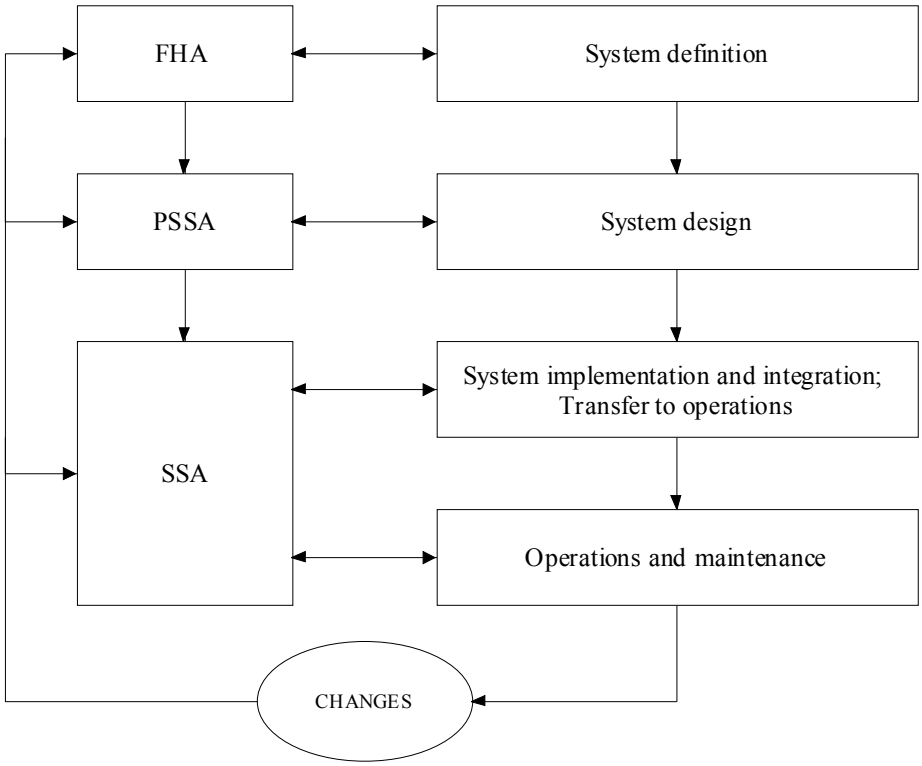


Figure C.1: Safety Assessment Methodology [EHQ-SAM, 1999]

The objectives of the FHA, the PSSA and the SSA are:

- Functional Hazard Assessment (FHA) analyses the potential consequences on safety resulting from the loss or degradation of system functions. Using service experience, engineering and operational judgement, the severity of each potential failure is determined qualitatively; each potential failure condition is placed in a class Catastrophic, Hazardous, Major, Minor or No safety effect. *Safety Objectives* determine the maximum tolerable probability of occurrence of a failure condition, in order to achieve a tolerable risk level (i.e. similar to JAR: see Annex B). The FHA is described in significantly more detail in [EHQ-SAM, 1999].
- Preliminary System Safety Assessment (PSSA) determines that the proposed system architecture is expected to achieve the safety objectives. PSSA examines the proposed system architecture and determines how faults of system elements and/or external events could cause or contribute to the hazards and failure conditions identified in the FHA. Next, it supports the selection and validation of mitigation means that can be devised to eliminate, reduce or control the hazards. System *Safety Requirements* are derived from Safety Objectives; they specify the potential means identified to prevent functional failure conditions or to reduce their effects to an acceptable level in combination with specific possible constraints or measures.
- System Safety Assessment (SSA) collects arguments, evidence and assurance to ensure that each system element as implemented meets its safety requirements and that the system as implemented meets its safety objectives throughout its lifetime.

It demonstrates that all risks have been eliminated or minimised as far as reasonably practicable, and subsequently monitors the safety performance of the system in service. The safety objectives are compared with the current performances to confirm that they continue to be achieved by the system.

In [EHQ-SAM, 1999], a very handy table is provided which gives an overview of the expertise required for each of these three assessment activities. This overview is copied in the table below.

Table C.1: Expertise required for FHA, PSSA and SSA activities

Expertise required	**FHA activities**	**PSSA activities**	**SSA activities**
Operational	Identification of hazard and failure condition	Evaluation of automation concepts	Design and validation of ATC procedures; Evaluation of HMI
Human factors	-	Identification of risk mitigation means related to human errors	Identification of risk mitigation means related to human errors
Ergonomic	-	Design of working position	Implementation of working position; Implementation of HMI
System engineering	Identification of hazard and failure condition	Identification, selection and validation of risk mitigation means	Verification and validation
Software / hardware engineering	-	Design methods	Software and hardware implementation
Quality assurance	Quality assurance of FHA process	Quality assurance of the design process	Quality assurance of implementation, integration, transfer to operations, operations and maintenance
Safety management	All activities	All activities	All activities

It can be noticed that human factors expertise and software/hardware engineering is not required during Functional Hazard Assessment. In addition, it can be noticed that human cognitive analysis is not required during any of the FHA, PSSA and SSA activities.

Annex D: List of Publications and Presentations

The results of the ARIBA project are published on the WWW:

http://www.nlr.nl/public/hosted-sites/ariba/index.html

ARIBA was presented at:

- DG7 (Brussels) - 16 September 1999
- EHQ-SRC meeting (Brussels) - 5 October 1999
- European Transport Research Conference (Lille) – 8/9 November 1999
- 3rd CAVA Workshop (Brussels) – 16 November 1999

In addition, two flyers have been produced, one in February 1999, which was distributed at the ATC '99 Exhibition in Maastricht, and one in November '99 containing a short overview of project results. The latter will be widely distributed e.g. at the ATC 2000 Exhibition in Maastricht.