ARIBA

ATM system safety criticality Raises Issues in Balancing Actors responsibility

WP6 Final Report Part III
Safety validation of ATM automated systems by manufacturer

WP6: Consolidation of results for safety certification in ATM
Part III: Safety validation of ATM automated systems by manufacturer
Final Report Part III (FR-III)
Reference: ARIBA/AAF/WP6/FR-III

Contract No AI-97-SC.2033

Distribution List		
Bas VAN DOORN Henk BLOM Jasper DAAMS Herman NIJHUIS	NLR	(NLR)
Eric ANDLAUER Françoise GIRARD	SOFREAVIA	(SOF)
Chris KELLY Clive PYGOTT Richard Furze	DERA	(DER)
Marc SOURIMANT Luc MALTIER	AIRSYS ATM S.A.	(AAF)
Carl VANSTEELANDT Pascal LEPROVOST	APTIME	(APT)
Billy JOSEFSSON	SCAA	(SCA)
Bounds GAVIN	UKCAA SRG	(SRG)
Patrick HUDSON	Leiden University	(RUL)
Jacques BEAUFAYS	EUROCONTROL	(EHQ)
Lars LÖNNBERG	DG VII	(DG7)

Authored by:	M. Sourimant, L. Maltier	
Reviewed by:	NLR, SCAA, SRG, DERA, APT, EUROCONTROL, DG7	
Approved by:	Lars Lönnberg (DG7)	Date: 19 November 1999

Document Change Log

Version #	Issue Date	Sections Affected	Relevant Information
0.1	31/3/99	All	First draft of consolidated document
0.2	07/05/99	All	Integration of comments from progress meeting
1.0	04/06/99	All	Integration of comments from partners
1.1	03/08/99	Executive summary, 1.2, 2.1, 2.2, 2.3, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.4, 6	Integration of comments
1.2	02/09/99	Executive summary, 1.1 to 1.6, 2.1 to 2.3, 3.1; merge of sections 2 and 3, 4.2, 4.3, 4.3.2.1, 4.3.2.4, 4.3.2.6, 4.3.3, 4.4.2, 5.2	Integration of a few late comments
1.3	13/09/99	3.2, 3.3 , Addition of appendix (7)	Integration of a comparison with EUROCONTROL safety assessment methodology
FINAL	29/10/1999	Executive Summary, 1, 3, 6, 7	Renumbering of WP6 parts + integration of comments on the appendix + few other minor changes

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 international RTCA Task Force on certification 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.

The current report forms Part III of the ARIBA consolidation report.

Table of Contents

Executive Summary

1. INTRODUCTION 7

1.1 BACKGROUND 7
1.2 ARIBA PROJECT 7
1.3 COMPLEMENTING RTCA'S CERTIFICATION TASK FORCE STUDY 8
1.4 IN-DEPTH STUDIES 9
1.5 CONSOLIDATION 10
1.5 ORGANISATION OF PART III 12

2. SAFETY VALIDATION OF AN ATM AUTOMATED SYSTEM 13

2.1 THE PROBLEM TO BE SOLVED 13
2.2 SAFETY VALIDATION CRITERIA 13
2.3 BUILDING A SAFETY CASE FOR AN AUTOMATED SYSTEM BY A MANUFACTURER 14
2.3.1 Introduction 14
2.3.2 Organisation of the safety case 15

3. METHODOLOGY 17

3.1 BASIC PRINCIPLES 17
3.2 STRUCTURE OF THE METHODOLOGICAL FRAMEWORK 17
3.3 COMPARISON WITH OTHER METHODOLOGIES 18
3.4 INDIRECT SAFETY ASSURANCE, THROUGH THE DEVELOPMENT PROCESS 19
3.4.1 Rationale 19
3.4.2 Case of newly developed parts 20
3.4.3 Special case: use of COTS software, or of already-developed software 24
3.5 SPECIFIC SAFETY ASSURANCE 25
3.5.1 Introduction 25
3.5.2 Initial safety assessment 26
3.5.3 Assessment of safety activities to be performed 27
3.5.4 Planning of safety programme 27
3.5.5 Identification of hazards, risk assessment and specification of mitigation solutions 28
3.5.6 Monitoring and tracking of hazard and safety issues 29
3.5.7 Verification that the system complies with safety requirements 29
3.5.8 Safety-related support during installation, commissioning, overall validation, transition, operation 30

4. GUIDELINES FOR IMPLEMENTATION OF THE METHODOLOGICAL FRAMEWORK 31

4.1 SUMMARY OF WHAT NEEDS TO BE STANDARDISED 31
4.2 IMPLEMENTATION AT MANUFACTURERS 31
4.3 FURTHER WORK 32
4.4 POSSIBLE SCHEDULE FOR IMPLEMENTATION 32

5. CONCLUSIONS 34

6. REFERENCES 35

7. ACRONYMS 36

8. APPENDIX:
COMPARISON OF THIS DOCUMENT WITH EUROCONTROL SAFETY ASSESSMENT METHODOLOGY A1

1. Introduction

1.1 Background

The Parts I, II and III of this consolidation report have been produced as the final deliverables of a 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 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 certification objective used by the ARIBA project is "To develop a certification framework that enables an effective safety management of the implementation of ATM advancements by the responsible actors". This report forms Part III of the ARIBA consolidation report, and is aimed at developing an effective approach towards safety validation of ATM automated systems by manufacturers.

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, APATSI, MUFTIS, SECAM, VAPORETO, FRAIS, GENOVA, CASCADE and RHEA) 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 RTCA Task Force on certification 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 (listed in Annex C of Part I) 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 the 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.

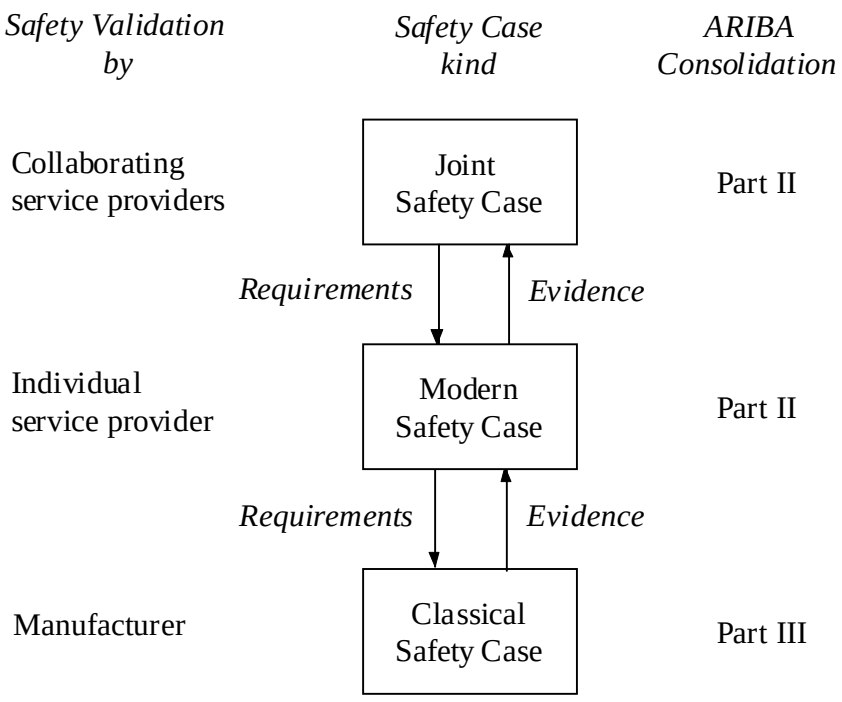


Figure 1. Complementary Safety Cases by various actors.

1.5 Organisation of Part III

The present document forms Part III of the ARIBA consolidation report. The aim of Part III is to consolidate a cost-effective safety validation methodological framework for manufacturers of ATM automation systems.

After the present introduction, the report first discusses the problem of safety validation for an automated ATM system, and the organisation of resulting data into a safety case (section 2). Then, in section 3, it presents the proposed methodological framework for safety validation of an automated system. A few guidelines for actual implementation of this framework are presented in section 4, and conclusions in section 5.

As the other parts of this report, this document adopts ISO terminology definitions.

2. Safety validation of an ATM automated system

2.1 The problem to be solved

In 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

2.2 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 4).

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.

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

2.3.1 Introduction

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 3.4.1.

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

2.3.2 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.

3. Methodology

3.1 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.

3.2 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:

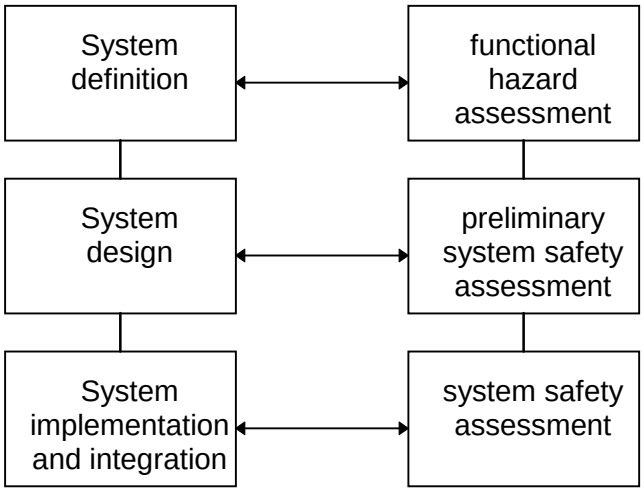
- to avoid mixing up the safety-specific part of the methodology, which is used only because the system is safety significant, with "normal" methods, which should be used even for systems which are not safety significant;
- to separate activities which a safety manager should more specifically manage.

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 (3.4 and 3.5), the methodological framework is presented chronologically.

3.3 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, at the end of the present document.

3.4 Indirect safety assurance, through the development process

3.4.1 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 3.5 (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.

3.4.2 Case of newly developed parts

3.4.2.1 Along the whole life cycle:

- **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.

3.4.2.2 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.

3.4.2.3 "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 3.4.2); 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.

3.4.2.4 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. 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 safety management plan (see section 3.4)

Also refer to section 3.4.5 for safety-management aspects.

3.4.2.5 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 safety management plan (see section 3.4)
- **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).

3.4.2.6 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 section 3.4.5 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 safety management plan (see section 3.4).

3.4.2.7 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.

3.4.3 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.

3.5 Specific safety assurance

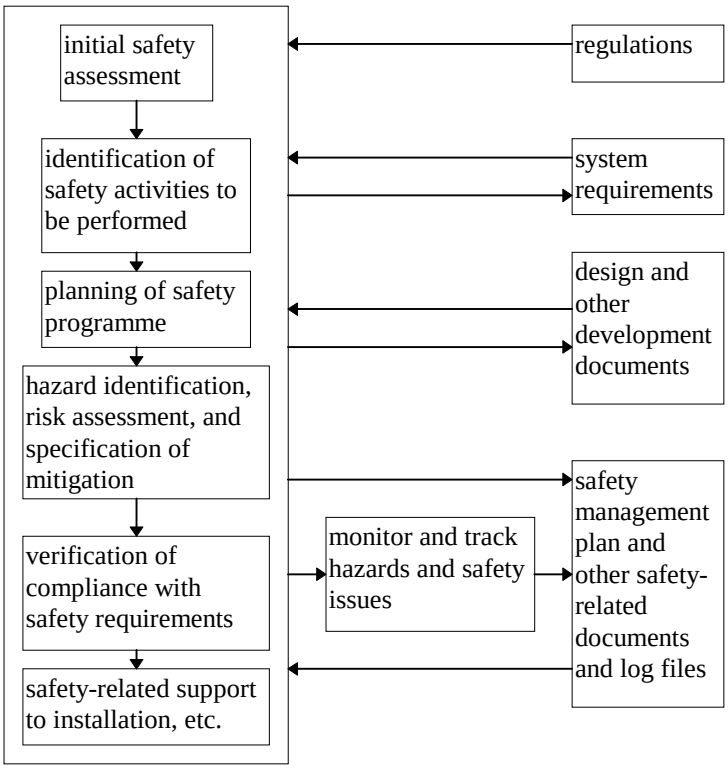
3.5.1 Introduction

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

3.5.2 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.

3.5.3 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.

3.5.4 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.

3.5.5 Identification of hazards, risk assessment and specification of mitigation solutions

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.

3.5.6 Monitoring and tracking of hazard and safety issues

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.

3.5.7 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.

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

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.

4. Guidelines for implementation of the methodological framework

4.1 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.

4.2 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).

4.3 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.

4.4 Possible schedule for implementation

The schedule of implementation might be divided into three phases:

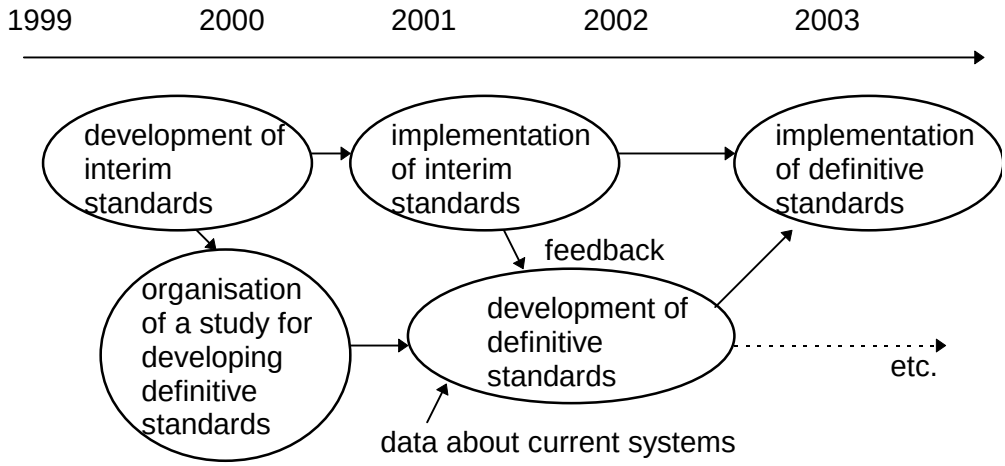
First phase:
- Development of an interim version of recommended standards, based on best current practices, and on improvements which can be implemented quickly.
- Organisation of a study to develop the second version of standards, including a first model for safety forecasting.

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.

5. Conclusions

This document 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.

6. References

This report took as main inputs the following references:

- ARIBA WP2, WP3, WP4 and WP5 reports
- EUROCONTROL Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01-00, Edition 0.5.
- RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification. RTCA Inc., December 1992.
- 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.
- Process used to assure safety at Airsys ATM (internal document).
- for the "phased inspections" technique: John C. Knight and E. Ann Myers. *An improved inspection technique.* Communications of the ACM. November 1993/Vol.36, No.11.
- N. Fota, M. Kaaniche and K. Kanoun, *A modular and incremental approach for building complex stochastic Petri net models*, Proc. 1st Int. Conf. on Mathematical methods in reliability, 1997.
- H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij and M.B. Klomstra, *Accident risk assessment for advanced ATM,* Proc. 2nd USA/Europe ATM R&D Seminar, Orlando, December 1998.
- J. Voas, *Certifying Software for High-Assurance Environments,* IEEE Software, July/August 1999, pp. 48-54.

7. Acronyms

AAF	Airsys ATM France
APT	Aptime
ARIBA	ATM system safety criticality Raises Issues in Balancing Actors responsibility
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATM	Air Traffic Management
CAA	Civil Aviation Authority
CEC	Commission of the European Communities
COTS	Commercial Off The Shelf
DAL	Development Assurance Level
DERA	Defence Evaluation and Research Agency
DG	Directorate General
DOD	Department Of Defense
EATCHIP	European Air Traffic Control Harmonisation and Integration Programme
E.C.	European Commission
EGNOS	European Geostationary Navigation Overlay Services
FAA	Federal Aviation Authority
FHA	Functional Hazard Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FR	Final Report
FTA	Fault Tree Analysis
GSN	Goal Structuring Notation
HAZOP	HAZard and OPerability Study
HMI	Human Machine Interface
ICAO	International Civil Aviation Organisation
ISO	International Standard Organisation
NLR	Nationaal Lucht- en Ruimtevaartlaboratorium
PSSA	Preliminary System Safety Assessment
R&D	Research and Development
RTCA	Requirements and Technical Concepts for Aviation
RUL	Rijksuniversiteit Leiden
SAM	Safety Argument Manager
SCAA	Swedish Civil Aviation Administration
Sofréavia	Société Française d'Étude et de Réalisation d' Équipements Aéronautiques
SRG	Safety Regulation Group
SSA	System Safety Assessment
TRTD	Transport Research and Technological Development
WP#	Numbered Work Package
WPR	Work Package Report

8. Appendix: Comparison of this document with EUROCONTROL Safety Assessment Methodology

This appendix identifies main differences between the methodological framework presented in this document, and the corresponding features of the EUROCONTROL safety assessment methodology.

This comparison is based on working draft 0.5 of EUROCONTROL document.

Readers should be aware that this short analysis might sometimes be disputable, due to:

- the differences in objective, scope and focus of both documents (not mentioning something in a document does not always mean that it has been rejected or forgotten, but often means that it has not been considered as relevant to the document),
- the fact that the edition of the EUROCONTROL document used (0.5) is still in a development stage.

In the present ARIBA document	Associated feature in EUROCONTROL methodology	Comments
1st part of the framework: "indirect" safety assurance, through the development process. (Not detailed in this table).	Not included. Sometimes a short mention such as "the absence of errors cannot be demonstrated by testing only" or the mention of five Development Assurance Levels. Engineering principles are considered, but always with the safety "filter".	Clearly not considered as in the scope of the EUROCONTROL document. ARIBA felt this point impacts very much the level of safety of the system and so needed to be addressed. .
How to deal with the use of COTS.	Not included.	It would be worth including it, for **practical** reasons.

In the present ARIBA document	Associated feature in EUROCONTROL methodology	Comments
2nd part of the framework: specific safety assurance	This is what the EUROCONTROL methodology focuses on.	
Initial safety assessment (to complete and finalise safety requirements, preferably in a standard way)	Meaningful only if considering that some organisation provides requirements to another one. This kind of problem is not considered (higher level).	Standardising the way of expressing safety requirements (e.g. criticality of services and functions, risk classification, etc.) is felt of high importance.
Assessment of safety activities to be performed. Before planning safety activities, it is important to identify what activities are necessary, according to the specific case.	The EUROCONTROL document addresses this in the "safety planning" section, and mentions only the required safety level as a criterion.	It could be interesting to discuss activities to be performed, in some important practical cases: various safety levels, but also use of COTS products, changes in an existing system, re-use of the same system in a different context, etc.
Planning of safety programme	More detailed in EUROCONTROL document. It mentions competency, but not briefing and training about the safety policy.	Discussing briefing and training about the safety policy could be useful, because important in practice.
Identification of hazards, risk assessment and specification of mitigation solutions: (a) risk classification scheme. A verification that the standard scheme is adapted to the system and context considered is mentioned.	The EUROCONTROL document proposes such a standard scheme. It also mentions NATS and CENA approaches, which deal with the adaptation of the scheme to ground systems through different definitions of severity.	Severity levels defined in the scheme are well adapted to aircraft, but their association of their **definitions** to a ground system needs further clarification.
(b) identification of hazards and failure modes	The EUROCONTROL document approach is to use FHA (described in detail, with an example).	Does not explain how to deal with practical application problems related to the complexity or the size of the system.

In the present ARIBA document	Associated feature in EUROCONTROL methodology	Comments
(c) estimation of hazard likelihood	Dealt with in PSSA (see below).	
(d) risk assessment (combining severity and likelihood). PSSA is mentioned as an example of risk assessment practice.	The EUROCONTROL document approach is to use PSSA (described in detail, with an example), including failure condition evaluation, common cause analysis, and zonal safety analysis. Then to use SSA (continuation of PSSA during the detailed design and implementation). Detailed descriptions (parts III and IV) are still missing.	Here too, practical application to specific cases (complex systems, very large systems, systems including COTS products, etc.) should be discussed in the next version, for practical reasons. Also, PSSA-like activities, which can impact the system, should continue the implementation phase.
(e) risk reduction	This is included in the SSA, which is an iterative process.	
Monitoring and tracking of hazard and safety issues.	This is dealt with in safety assurance principles.	
Verification that the system complies with safety requirements.	Addressed in SSA safety assurance activities.	
Safety-related support during installation, commissioning, overall validation, transition, operation.	Not addressed in EUROCONTROL document yet (unless it is considered to be addressed in SSA).	These points should be explicitly addressed in the missing detailed description parts.