EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

TLS Apportionment Method

Edition	:	V0.7
Edition Date	:	2003-07-30
Status	:	Draft
Class	:	EATMP

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

PAGE INTENTIONALLY LEFT BLANK

DOCUMENT IDENTIFICATION SHEET

DOCUMENT DESCRIPTION		
Document Title **TLS Apportionment Method**		
PROGRAMME REFERENCE INDEX:	**EDITION:**	0.7
	EDITION DATE:	2003-07-30

Abstract

This document presents a method for apportioning the ESARR 4 TLS (for events of severity category 1) to ATM systems and setting numerical safety objectives to events of severity categories 2 to 4.

Keywords

TLS
ESARR4
Quantitative Safety Objective
Safety Assessment Methodology

CONTACT PERSON:	Patrick MANA (HQ) Eric PERRIN (ERC) B.KIRWAN (ERC)	**TEL:**	**PROGRAMME:**

DOCUMENT STATUS AND TYPE			
STATUS		**CLASSIFICATION**	
Working Draft	☐	General Public	☐
Draft	☑	EATMP	☑
Proposed Issue	☐	Restricted	☐
Released Issue	☐		

ELECTRONIC BACKUP		
INTERNAL REFERENCE NAME:		
HOST SYSTEM	**MEDIA**	**SOFTWARE**
Microsoft Windows	Type: Hard Disk	**MS Office Word 97**
	Media Identification:	**MS Windows 95**

PAGE INTENTIONALLY LEFT BLANK

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION	DATE	REASON FOR CHANGE	SECTIONS PAGES AFFECTED
0.1	2002-09-30	Working draft.	All
0.2	2002-11-15	Working draft.	All
0.3	2002-12-04	Draft for review within Contracting Company.	All
0.4	2002-12-10	Provisional issue following review within Contracting Company.	All
0.5	2003-02-14	Provisional issue following the application of the guidance to a Vertical Separation example and to GBAS Cat-I	All
0.6	2003-04-14	Provisional issue updated following review by EUROCONTROL.	All
0.7	2003-07-30	Provisional issue as SAM-FHA Guidance Material	All

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In many industry sectors including ATM, safety regulation has traditionally been carried out prescriptively, with the resulting problem of the regulator effectively inheriting safety responsibility from the regulatee. European ATM has adopted the recent trend towards objective-based safety regulation, in which safety, and the proof thereof, is more clearly the responsibility of the service provider. EUROCONTROL's ESARR 4 [Ref 2] enshrines this approach, defining a numerical Target Level of Safety (TLS) representing acceptable risk for ATM in its entirety.

The introduction of a numerical TLS has raised the problem of how to apportion the target within and between individual ATM systems. This document addresses this problem and is intended to become an Acceptable Means of Compliance with the TLS apportionment aspect of ESARR 4.

1. INTRODUCTION

1.1 Background

Traditionally, in many industries including ATM, safety regulation has been carried out prescriptively – ie the regulator defined the rules and standards to be followed, and used audit and inspection to check compliance with them. In so doing, the regulator implicitly (if not explicitly) inherited a substantial part of the responsibility from the regulatee. Furthermore, that approach required a great deal of specialist resource on the part of the regulator and was often over-constraining for the regulatee, particularly in the introduction of new processes and technologies.

In European ATM, recognition of these difficulties has led to an **objective-based** approach to safety regulation, in which safety is much more clearly the responsibility of the ATM service provider, the regulator's role being mainly to ensure that the service provider discharges his responsibilities properly. The regulator sets objectives for the achievement and demonstration of safety and the service provider has to show (by argument and evidence) that he has met those objectives – ie the *burden of proof* rests primarily with the service provider. The use of standards may still be appropriate but the service provider has to show that the standards he chooses to use are appropriate – rather than merely claim compliance with them.

This objective-based regime is encapsulated by EUROCONTROL regulations ESARR 3 [Ref 1] and ESARR 4 [Ref 2].

In objective-based safety regulation, appropriate top-level safety objectives for demonstrating that a system is *tolerably safe* would be to show that both of the following are true:

- a set of **safety requirements**[1] has been **specified**, sufficient to enable the *required level of safety*;
- those **safety requirements** have been **satisfied** in the implementation of the system.

The practical realisation of those two fundamental assurance principles can vary substantially. There has been a view that safety is largely a matter of reliability and that safety can be delivered largely by adherence to prescribed processes, especially in relation to software development.

However, theory and experience have shown this to be too narrow a view of safety. ESARR 4, in particular, defines very specifically what is meant by *tolerably safe* and *required level of safety* and demands a more complete and rigorous approach to the specification and satisfaction of safety requirements.

[1] The term "safety requirements" is used generically here. However, Stage 3 of the Method (in line with ESARR 4 terminology) uses safety requirements in a very specific sense

1.2 Applicability of ESARR 4

The numerical Target Level of Safety (TLS) specified in ESARR 4 requires that the probability of ATM directly contributing to an accident (Severity Category 1 event) shall not exceed 1.55×10^{-8} per flight hour. Interpretation of a *direct ATM contribution* is broader than might be thought at first sight, and guidance on the scope of application of ESARR 4 is therefore given herein.

The TLS applies at the level of ATM service provision and is of relevance to the entire system lifecycle from definition, through operational service, to decommissioning, and impacts to some degree on all safety management activities.

The TLS of not more than 1.55×10^{-8} accidents per flight hour was the target prevailing at the time at which this guidance material was prepared, and will be fixed at that level until 2015. It should be borne in mind that there is a long-term goal to improve safety levels, so it can be expected that the TLS will be progressively reduced in subsequent years. However, the method described herein will still be applicable, provided that the particular value of the TLS prevailing at the time of application is used.

Consequently, if any ANS Service Provider uses this method, he can decide to add a safety margin on top of ESARR4 TLS value without impacting the usability and applicability of the method described here after.

1.3 Purpose

This document presents a method for:

- Apportioning the ESARR 4 TLS (for events of severity category 1) to ATM systems
- Setting numerical safety objectives to events of severity categories 2 to 4.

1.4 Intended Users

This guidance is intended for use by anyone participating in the process of apportioning the ESARR 4 TLS to ATM systems.

It is assumed that users of this method are familiar with the underlying safety engineering techniques invoked – for example, Fault Tree Analysis, Event Tree Analysis and Functional Failure Analysis.

1.5 Structure

As indicated above, the introduction of ESARR 4 will in most cases require some changes to current safety practices. **Section 2,** therefore, introduces a number of safety engineering concepts that are key to the success of the application of this guidance.

Sections 3, 4, 5 and 6 give a step-by-step description of the method itself. The detailed guidance is preceded by a high-level overview.

Sections 7 and 8 list the references and present a glossary of acronyms.

Appendix A presents guidance on setting safety targets.

Appendix B presents a generic ATM safety model which is used during the process.

2. KEY CONCEPTS AND TERMINOLOGY

2.1 Introduction

In section 3 of this Guidance, it will be seen that, because the ESARR 4 TLS is specified at the level of ATM service provision, safety analysis has to start at this level. Furthermore, in order to correctly specify the safety attributes of the ATM system, and its component parts, in relation to the TLS, an understanding of the nature of safety-related systems (SRSs) and the principles of requirements determination is necessary; and a clear distinction needs to be made between accidents, hazards and causes. These aspects are discussed below.

2.2 Safety Related Systems

In broad terms, safety-related systems (SRSs) may be defined as either:

- Those whose primary purpose is to reduce pre-existing risk and thereby improve the safety of their environment - all safety protection systems (eg a fire alarm system) fall into this category [Ref 3]; or

- Those which do not serve a primary safety purpose but which would cause a safety hazard to their environment if they fail – a chemical processing plant, for example, would fall into this category.

Of course any SRS that meets the first definition would also cause a safety hazard to their environment if they fail. It is very important to note that ATM falls into the first category since its primary purpose is to maintain safe separation between aircraft.

The safety requirements of SRSs, at all levels in the system hierarchy, must be expressed in two complementary forms [Ref 3]:

- the *safety functions* and performance required of them, since it is these aspects which determine how effective a system will be in reducing risk.

- the *integrity* (eg the reliability) required of those safety function, since it is this aspect which determines the risk to the systems environment should the system fail to perform to specification.

A model which takes into account both the functional and the integrity aspects of safety is illustrated in Figure 2-1 below.

In this model, the influences of functionality and integrity are shown separately, such that:

- R_u represents the level of risk present before taking into account the SRS.

- R_m represents the minimum achievable risk assuming hypothetically that the SRS always functions to its specified performance, without failure.

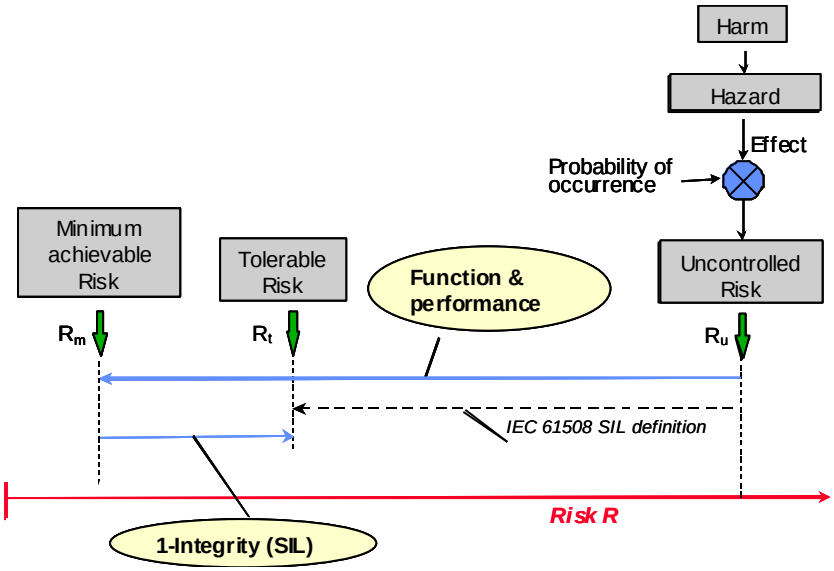


Figure 2-1

- R_t represents the tolerable level of risk – ie the TLS in the terms used in this document. [2]

In consequence, the risk margin $R_t - R_m$ determines the *integrity* required of the system and it is clear that if the SRS functionality and performance is insufficient to achieve the *necessary risk reduction* (ie if R_m is greater than the TLS, R_t) then, no matter how reliable an SRS was, it would not be tolerably safe!

It follows therefore that before the integrity required of an SRS can be specified it has to be shown that the level of risk reduction in the absence of failure (R_m) lies well below the minimum overall tolerable level (R_t). This is a key feature of the method described in sections 3 to 6 below.[3]

2.3 Requirements Determination

Figure 2-2 is a simple requirements determination model, and defines three principal levels for the development of safety requirements, as follows:

[2] Note that this is a more sophisticated model than that presented in [Ref 3] where the required integrity is equated directly to $R_u - R_t$, and the effects on the specified functionality and performance is masked.

[3] A full discussion of the model shown in Figure 2-1 can be found in [Ref 5]. The EUROCONTROL RVSM Programme is a good example of how the model has been applied [Ref 4].

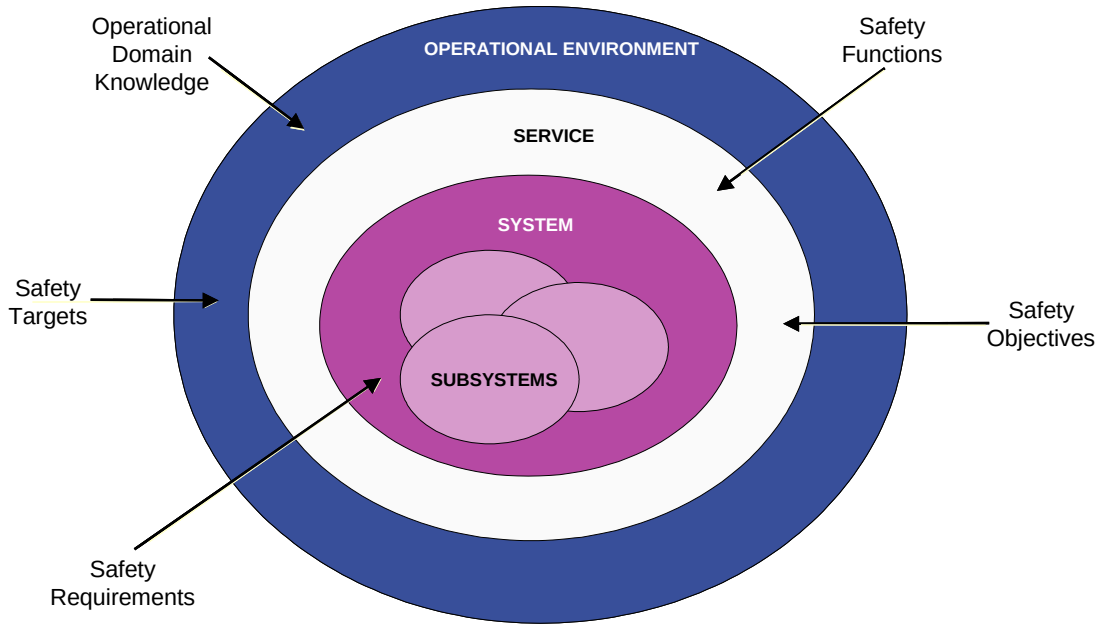


Figure 2-2

- The *operational environment* (or domain) into which the ATM system provides (safety-related) services. The airspace, and users[4] of the ATM service, for example, exist at this level.

- The level at which the safety properties of the (ATM) *service* are defined, in abstract terms – ie entirely independent of the physical aspects of the eventual system implementation.

- The core-*system* level comprising the physical sub-systems, implemented typically in equipment, people (ie operators) and procedures.

The products of the requirements determination process maps on to this model, as follows:

- *Safety targets* are what we want to make happen in the operational environment. *Safety targets* may be quantitative - eg "the probability of a Severity Category 1 event shall not exceed 1.5 x 10^{-8} per flight hour" - or qualitative – eg "the risk of collision shall be reduced to a level that is as low as reasonably practicable".

- *Safety functions* specify **what** the ATM service has to provide into the operational environment – including the level of **performance** required of the service - in order that the *safety targets* can be met.

- *Safety objectives*[5] are derived from a (service-level) functional hazard assessment and, in effect, specify the **integrity** required of the safety functions.

[4] Users are not the same as operators; the former sit outside the system boundary - the latter sit within it.

- Operational domain knowledge covers those pre-existing properties of the operational environment, which either are known to be true or have to be assumed to be true, and which determine whether the service-level safety functions and safety objectives are sufficient to meet the safety targets. For example, it would not be possible to say what accuracy would be required of a Surveillance safety function in order to meet a specific safety target, without knowing what separation criteria apply in the airspace concerned – those separation criteria would therefore be an essential item of operational domain knowledge.

- Safety requirements are the safety properties required of the physical system that necessary in order to provide the (service-level) safety functions and meet the safety objectives. They are expressed in terms of the functionally, performance and integrity required of each subsystem – ie including people, procedures and equipment[6].

The distinction and relationship between safety targets, objectives, domain knowledge, and requirements are not merely academic concepts but provide the essential foundations for developing systems that do, and can be shown to do, everything that is required of them.

2.4 Accidents, Hazards Risks, and Mitigations

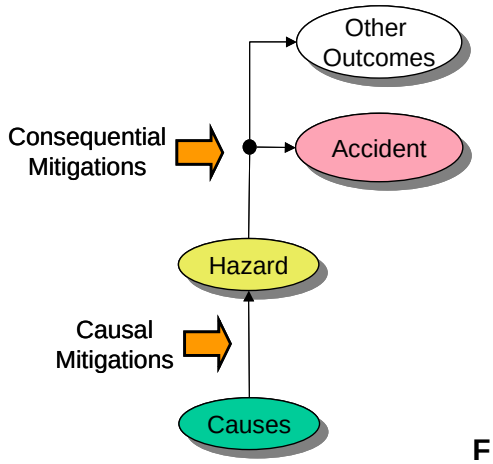


Figure 2-3

[5] The terms *safety objectives* and *safety requirements* are defined in ESARR 4. The descriptions given herein do not seek to redefine those terms, but rather seek to explain how the terms are applied to the TLS Apportionment Method.

[6] System domain knowledge may also be specified at this level.

An *accident* is an unintended event that results in death or serious injury. *Accidents* occur in the *operational domain*.

In general, a *hazard* is a state that could lead to an accident - whether it does or not, depends on the availability of *mitigations* to break the sequence of events that would otherwise lead to an accident, as shown in Figure 2-3.

Such mitigations are called *consequential* (since they relate to the consequences of a hazard, and can be either deliberately provided or circumstantial (ie purely a matter of chance).

The likelihood of an accident is also dependent on the likelihood that the hazard would occur in the first place. This in turn is dependent on the frequency of occurrence of the underlying *cause(s)* of the hazard and on the availability of (*causal*) *mitigations* to break the sequence of events between the causes and the hazard itself.

An SRS may provide either causal or consequential mitigations – for example, in the context of ATM, ATC systems usually provide the former and FIS systems the latter. A representation of consequential mitigation is shown in Figure 2-4. Of course, from the definition of an SRS (see paragraph 2.2 above), account has to be taken of the fact that the SRS may itself introduce risk by either:

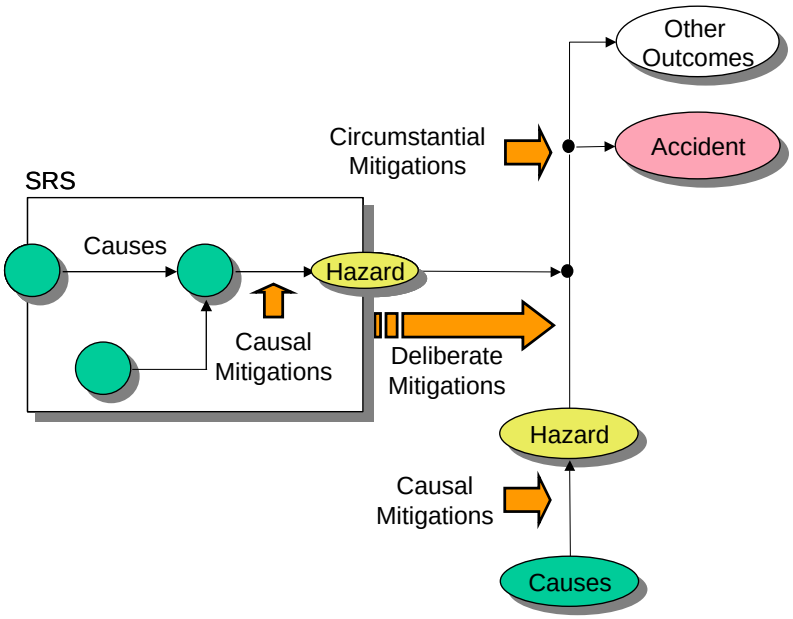


Figure 2-4

- Failing to deliver the functionality required to mitigate pre-existing hazards; or
- Delivering incorrect functionality / data (or delivering it at the wrong time) and thereby introducing a new hazard.

It should be noted that the hazard introduced by the SRS in Figure 2-4 is described at the boundary of the SRS, and causes are internal to the system. This is important since it

provides a general distinction in the way that hazards and their causes are handled, as follows:

- Safety Functions provide (deliberate) mitigations of the **consequences** of hazards.
- Safety Objectives are used to set the maximum **frequency of occurrence** of a hazard, at the ATM service level.
- Design is used to control the **causes** of a hazard such that the Safety Objectives are met.

Where a system is made up of a number of subsystems, hazards can also be defined at the boundary of each subsystem, as discussed in the detailed guidance which follows.

2.5 The "Bow-Tie" Model

The so-called the "Bow-tie" model, illustrated in Figure 2-5, is a convenient way of modelling risk by linking the causes of a hazard (modelled using Fault Tree Analysis (FTA)) and the consequences of a hazard (modelled using Event Tree Analysis (ETA)).

The point in the Fault Tree (FT) hierarchy at which the link to an Event Tree (ET) is established is known as a *pivotal event*.

The *pivotal events* typically correspond with the main system and or subsystem hazards. One FT/ET pair is constructed for each hazard and values are ascribed both to the probability of occurrence of each casual factor in the FTs and to the probability of success or failure of the outcome mitigations represented by the branches of the ETs. Using the facilities of a mature FTA / ETA tool, the overall probability of an accident from all causes can be determined and compared to the safety target(s).

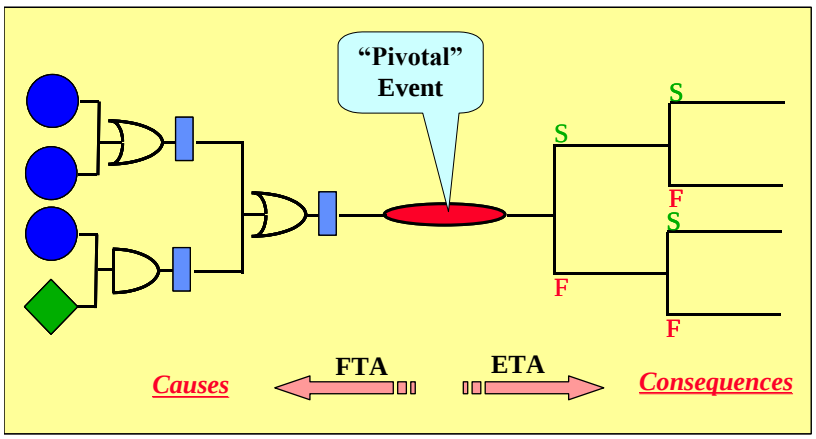


Figure 2-5

In terms of the EATMP Safety Assessment Methodology [Ref 8] the ETA side of the model relates to an FHA, and the FTA side relates to the subsequent PSSA and SSA.

Note that, in this model, hazards should be categorised according to probability that an accident will result given that the hazard has occurred. This contrasts with the EATMP

hazard classification scheme [Ref 8] which should be applied to only to the *outcomes* of a hazard.

3. TLS APPORTIONMENT METHOD – OVERVIEW

This chapter outlines the process to be followed to apportion the TLS to the system under analysis. The detailed process stages are presented in the subsequent chapters.

3.1 Service-level Safety Functions and Objectives

Figure 3-1 illustrates the process of getting from safety targets, to a set of service-level safety functions and objectives.

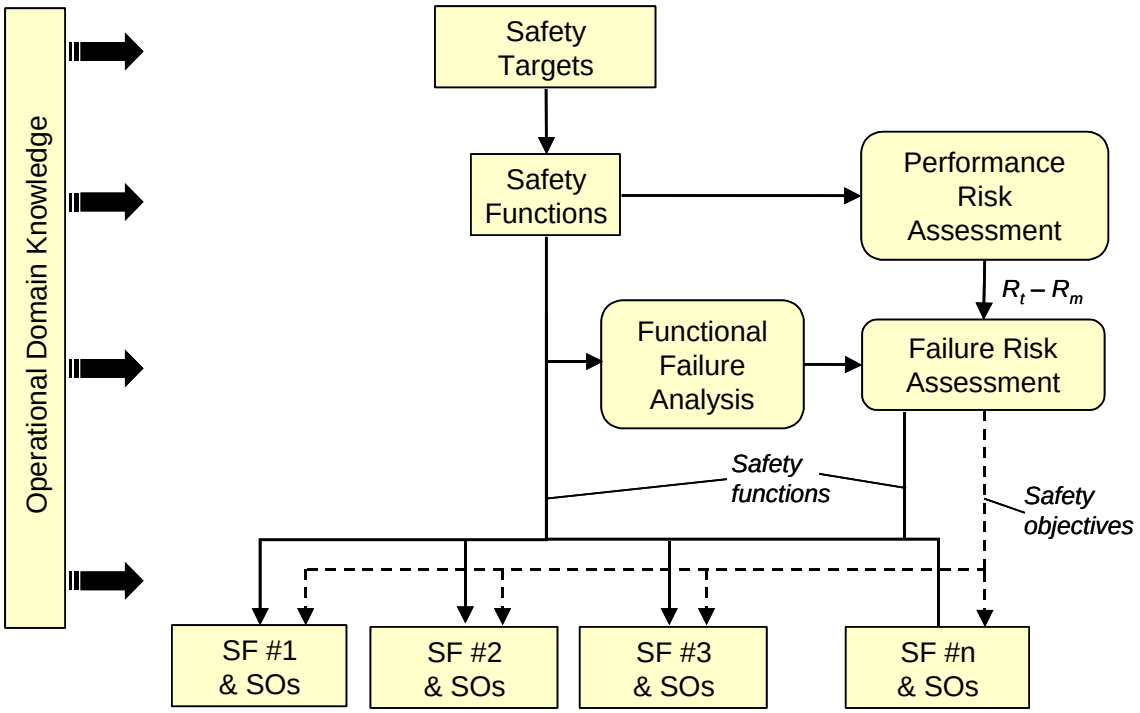


Figure 3-1 – Service-level Process

The first step is to determine what safety functions need to be provided at the service level, and to specify the performance required of them (eg accuracy, capacity, timeliness etc, but excluding integrity), in order for safety targets to be met. It is necessary at this stage to carry out some form of performance-risk assessment in order to show that specified safety functions are sufficient to reduce the risk to a level (R_m) well below the TLS (R_t).

R_t-R_m therefore represents that portion of the TLS which can be allocated to (functional) failure – clearly it must be positive, otherwise there is no point in proceeding further! Safety objectives are obtained from hazard and risk analysis at the service level, and limit the allowable rate of occurrence of each function failure mode (hazard) such that the total

risk associated with the identified hazards is within the value of R_t-R_m, taking account of any mitigations that are identified during the process.

All mitigations must be captured as either:

- Additional safety functions, and corresponding safety objectives, for the provision of "deliberate" mitigations of the consequences of the identified hazards.
- Operational domain knowledge for any "circumstantial" mitigations (ie those arising as a matter of pure chance).

At this point, it needs to be shown that that the (service-level) safety functions and safety objectives are sufficient to satisfy the (operational-level) safety targets, given the operational domain knowledge.

3.2 System-level Design and Safety Requirements Specification

The specification of safety requirements follows from an architectural design of the system, as illustrated in Figure 3-2.

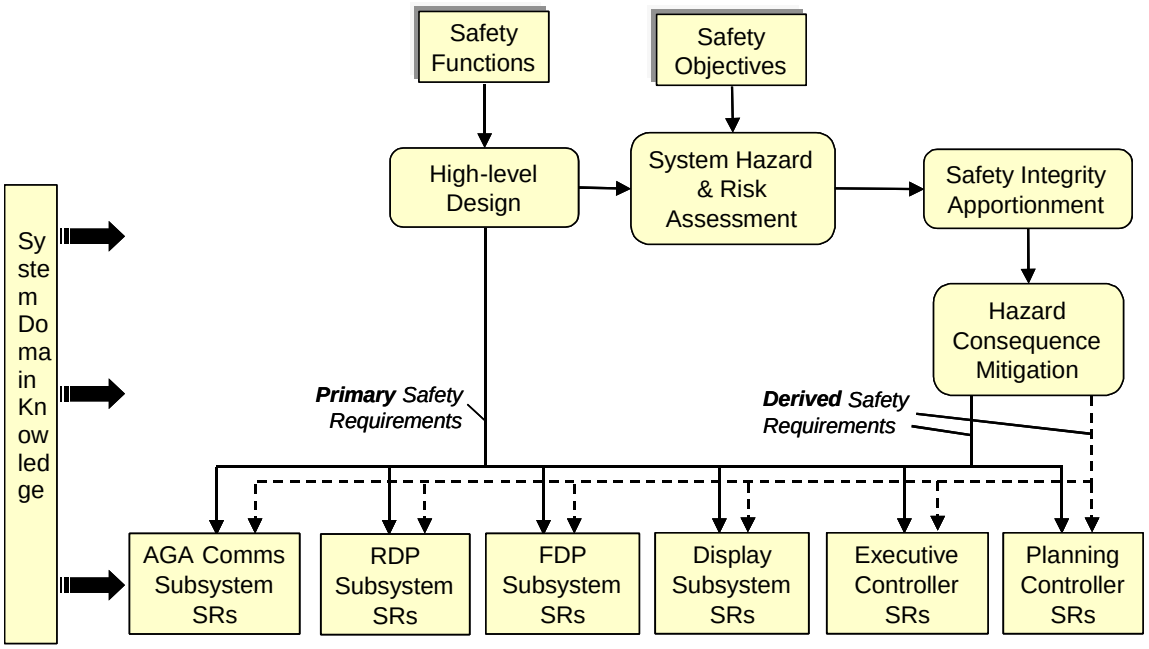


Figure 3-2 – System Architectural Design Process

The **primary** safety requirements stem from an allocation of the service-level safety functions (and their performance attributes) the subsystem(s) on which they are implemented. The illustration in Figure 3-2 shows four equipment-based sub-systems (air-ground communications, radar data processing, flight data processing, and display) and two human-based subsystems (executive and planner controllers).

The hazards and risks associated with failure of each subsystem (defined at the subsystem boundary) are assessed, any mitigations (of the consequence of failure) are identified and allocated (as assumptions or additional safety functions, as appropriate), and the safety integrity requirements for each subsystem determined – the additional safety functions and the safety integrity requirements are known collectively as **derived** safety requirements.

The outputs from this stage are therefore:

- The safety functions implemented by each subsystem, including the performance required of the safety functions.
- The safety integrity requirements for each subsystem.
- The interactions and interfaces between the subsystems.

Those three perspectives must be addressed for each subsystem irrespective of whether it is hardware-based, software-based or human-based.

Finally, it necessary to show that each service-level safety function and safety objective is met by the subsystem safety requirements, given the system domain knowledge.

3.3 Process Structure

The three main stages in the TLS allocation process are outlined in Figure 3-3.

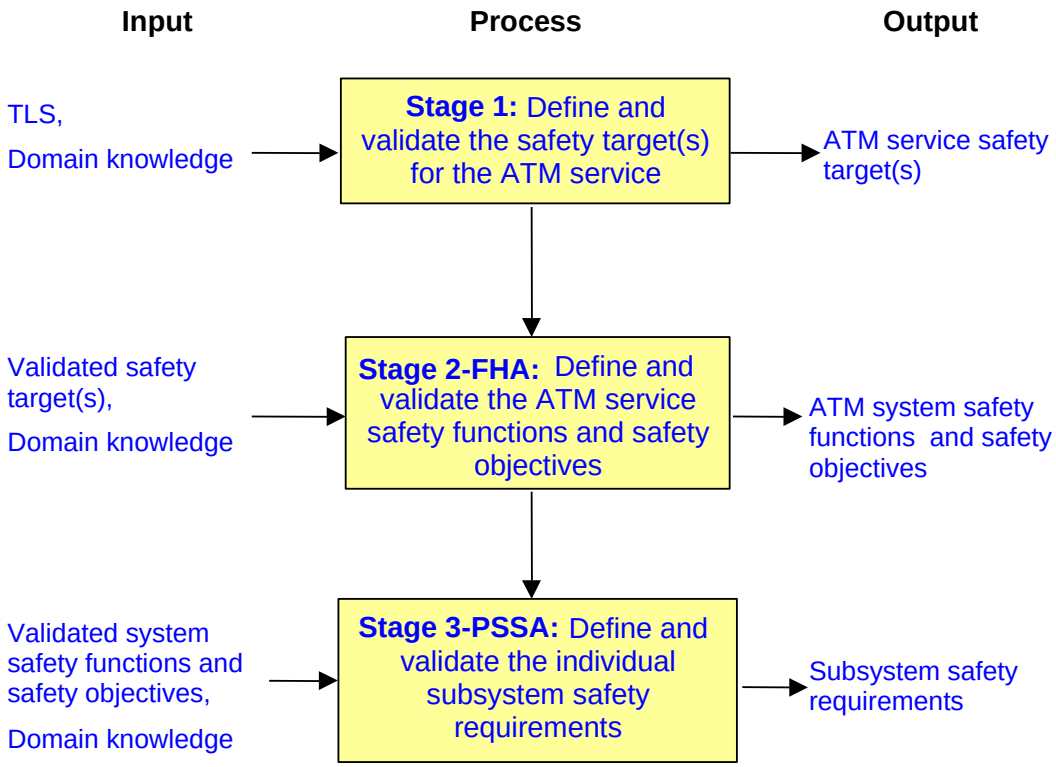


Figure 3-3 – Overall Process

The objective for **Stage 1** is to define the *safety targets* that apply to the ATM service. In keeping with the definitions provided in section 2.3 above, these safety targets specify what we are trying to achieve in terms of safety in the operational environment (ie in the airspace under consideration), without saying (other than in general terms) how that is to be achieved. The safety targets should reflect the ESARR 4 TLS, and any other TLSs, as applicable to the particular airspace under consideration. Safety targets may be quantitative (eg maximum probability of collision per flight or per unit of time) or qualitative (eg that the risk of collision shall be as low as reasonably practicable).

Stage 1 also includes a validation of the safety targets against the ESARR 4 TLS, and against any other TLS applicable to the airspace under consideration.

Details on Stage 1 are provided in **chapter 4** herein.

The objective of **Stage 2** is to produce a set of *safety functions* and *safety objectives* (see section 2.3 above, for definition) for the ATM service, by specifying the functions to be provided and the performance and integrity required of them, in order to satisfy the safety targets produced in Stage 1. [7]

It is important that this work is kept at an abstract, functional level without any regard for how those safety functions might be implemented in a physical system – the latter is done later, in Stage 3. By taking this approach, the task of defining the safety targets, safety functions and safety objectives need only be performed once per ATM service unit,

[7] Stage 2 maps directly on to the Functional hazard Assessment (FHA) of the EUROCONTROL Safety Assessment Methodology [ref 8]

provided that there is no subsequent fundamental change in the manner in which the service is provided.

Details on Stage 2 are provided in **chapter 5** herein.

Stage 3 represents the highest level of design of the ATM system and the allocation of the ATM service-level safety functions and safety objectives to the physical elements of the system – including equipment, people and procedures. The main output is a validated set of *safety requirements* (in the form of *safety functions* and *safety integrity requirements*) for each subsystem that together are shown to be sufficient to satisfy the ATM service-level safety functions and safety objectives. [8]

Although the overall process is shown in Figure 3-3 and in the subsequent detailed flowcharts as being linear, some iteration will be necessary if the output from any particular stage indicates that any apportionment, assumption or decision taken earlier needs to be modified. In particular, it should be noted that the introduction of any system (or subsystem) has the potential to change the properties of the operational domain, and may thereby lead to the potential for new safety functions (or safety objectives).

Details on Stage 3 are provided in **chapter 6** herein.

[8] Stage 3 maps on to the first level of Preliminary System Safety Assessment (PSSA) of the EUROCONTROL Safety Assessment Methodology [ref 8]

4. STAGE 1: ATM SERVICE SAFETY TARGETS

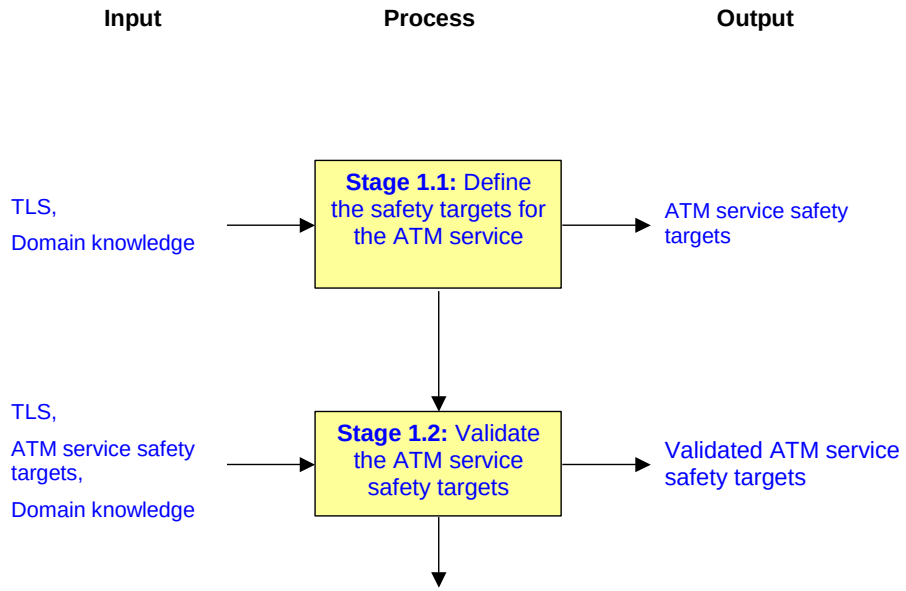


Figure 4-1 – Process Breakdown, Stage 1

Stage 1 is outlined in the flowchart in Figure 4-1, and described in sections 4.1 and 4.2.

4.1 Stage 1.1: Define the Safety Targets for the ATM Service

4.1.1 Objective:

To derive the safety targets to be met by the ATM service, for the airspace and phase of flight under consideration.

4.1.2 Process:

- Ascertain if any other TLSs (ie in addition to ESARR 4) apply to the service under consideration.
- The primary safety targets are then specified, in terms of the maximum acceptable frequency of an SC1 event, such that all TLSs are satisfied by the safety targets.
- Additional safety targets may be specified, in terms of the maximum frequency of less severe (SC2 to 4) events.
- Additional safety targets may also be specified in order to place qualitative limits on the level of risk.

- Record all domain knowledge that is associated with the service / airspace under consideration and is relevant to the safety targets.

4.1.3 Output from this Stage:

- Set of safety targets for the ATM service under consideration
- Set of relevant operational domain knowledge.

4.1.4 Considerations:

- The safety targets define what we want to achieve in the operational environment (the airspace). Quantitative targets are an interpretation of the TLSs that apply to the airspace / phase of flight under consideration. Qualitative targets should reflect applicable safety policy – eg the ATM 2000+ Safety Objective [Ref 9].
- Guidance on setting targets is given in Appendix A.
- It is necessary to consider if the ATM service, or components of it, is subject to a TLS additional to that specified in ESARR 4[9]. From a practical point of view, it is helpful to the subsequent analysis, if the TLSs applicable to a particular phase of flight / service can be reduced to a single safety target that satisfies them all[10].
- Under normal circumstances it will be necessary to consider the scope of the entire ATM service at this stage. However, it is possible that, in some cases, the TLS has to be apportioned to a particular subsystem in advance of a full analysis at the ATM service level[11]. In such cases, particular care should be taken with regard to the issue of operational domain knowledge and assumptions about those parts of the ATM service / system that are not being considered in the analysis.
- Relevant domain knowledge is essential during this stage, as it is throughout the entire process. At this stage, an understanding of the properties of the operational environment (ie the airspace under consideration) is required, and must be recorded alongside the safety targets.
- A thorough understanding of the basic concepts of modern requirements engineering is essential for the success of this stage. An overview is presented in section 2 above.

---

[9] For example, precision approaches are subject to a separate TLS for accidents related to *all* causes (ie not only to ATM causes).

[10] This is done in the case of the Vertical Separation example provided with this Guidance

[11] This is the case with the Vertical Separation example provided with this Guidance.

4.2 Stage 1.2: Validate the ATM Service Safety Targets

4.2.1 Objective:

To demonstrate that the ATM service safety targets are necessary, complete and correct.

4.2.2 Process:

The objective will be met by a *satisfaction argument* which demonstrates that the ATM service safety targets are sufficient to maintain the risk associated with the ATM service at a level below the ESARR 4 TLS, and any other relevant TLSs.

4.2.3 Output from this Stage:

- Satisfaction argument with supporting evidence which validates the claim that we have a set of ATM service safety targets that is sufficient to meet the TLS(s) and other, qualitative constraints.

4.2.4 Considerations:

The specific form of the argument will depend on the nature of the safety requirements themselves but, in general, should show that:

- The numerical safety targets will meet the TLS(s).
- The qualitative targets fully satisfy the applicable safety policies etc.
- The operational domain knowledge is complete and correct.

The form of the evidence will also depend on the particular safety targets concerned. In general, however, it will usually be the case that:

- The primary safety target will be the TLS itself, or some portion / derivation thereof. Showing that this safety target meets the TLS should be either trivial or a matter of showing that the apportionment of the TLS is valid. Wherever possible, the latter should be based on historical evidence (or at least an assumption[12]) that the portion of the TLS that is not the subject of the further analysis will be met by whatever service / system it has been allocated to.
- The validity of other safety targets would in most cases be demonstrated by straightforward traceability techniques.

[12] Such assumptions are to be validated.

5. STAGE 2: SPECIFICATION OF SAFETY FUNCTIONS AND SAFETY OBJECTIVES

Stage 2 is outlined in the flowchart in Figure 5-1, and is described in sections 5.1 to 5.7.

NOTE: As Stage2 maps directly SAM-FHA, the text here under does not intend to propose a new version of SAM-FHA, but aims at proposing an application of FHA stages in the light of the needs of the quantification method.

5.1 Stage 2.1: Functional Design of the ATM Service

5.1.1 Objective:

To produce a functional design of the ATM service to address the safety targets, for the airspace under consideration.

5.1.2 Process:

A generic ATM functional model, to facilitate the process, is presented in Appendix B, and consists of six functional groupings (Tactical Separation, Flight Directing, Strategic Separation, Co-ordination and Transfer, Traffic Management, and Aeronautical Information), which are decomposed into specific functions.

The model, as presented, is designed to cover all aspects of ATC in the En-route phase of flight, and to be adaptable to other flight phases. For example:

- Removal of Strategic Separation would provide the basis for modelling the Approach phase.
- Removal of Tactical Separation would provide the basis for modelling the Oceanic phase.

Consideration also needs to be given to non-ATC components of ATM - eg FIS and navigation aids.

5.1.3 Output from this Stage:

- A functional design model of the ATM service, for the airspace under consideration.

5.1.4 Considerations:

- The analysis must be performed in the context of relevant operational domain knowledge. Any additional domain knowledge identified during the functional design process must be recorded.
- If the ATM service provided applies to more than one flight phase (en-route, approach

or tower) then it may be necessary to define a separate model for each of the flight phases to take account of design differences between them.

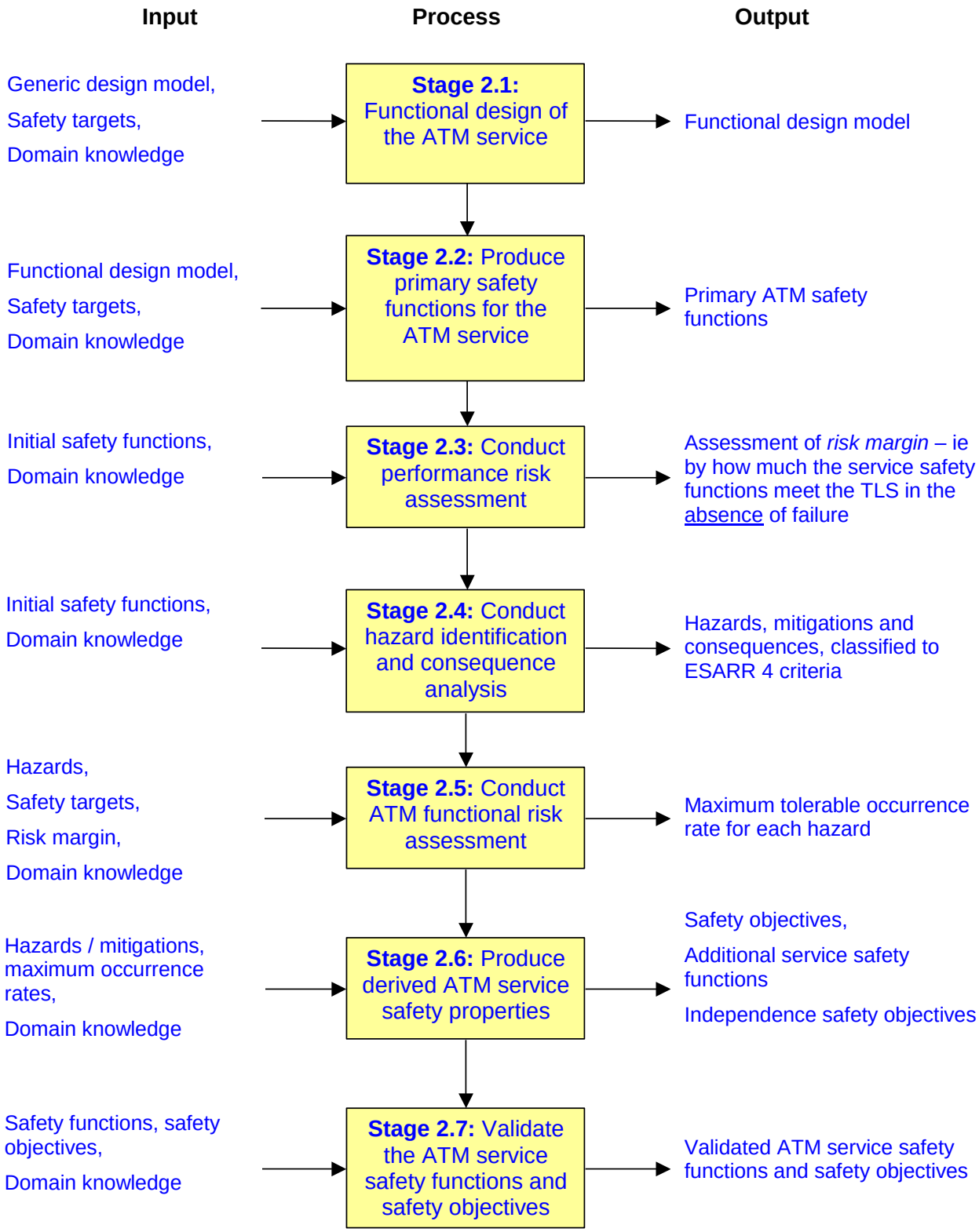


Figure 5-1 – Process Breakdown, Stage 2- FHA

- The generic functional model has been prepared so as to be sufficiently general to encompass all ATM safety functions. If there should appear to be a mismatch between the model of the system under analysis and the generic model, it is important to investigate the reasons and to reconcile the conflict before proceeding further.

- Normally, this stage (indeed the whole of Stage 2) is intended to be a one-off activity for each ATM service unit, and its outputs should be largely independent of the implementation of the safety functions and safety objectives in the physical ATM system. However, the outputs should be reviewed periodically, and whenever a change is introduced at the ATM service level, in order to ensure that they remain valid.

- If this analysis is being conducted for the first time with the short-term aim of allocating the TLS to a subsystem associated with a specific function, then it may be possible, with caution, to proceed by restricting the scope of the model and the analyses to a subset of the overall service.[13]

5.2 Stage 2.2: Primary Safety Functions for the ATM Service

5.2.1 Objective:

To specify the primary safety functions [14] for the ATM service modelled in Stage 2.1 above.

5.2.2 Process:

A set of generic ATM safety functions is presented in Appendix B, in order to facilitate the process.

A subset of the generic safety functions should be produced appropriate to the ATM service / phase of flight under consideration; these should be customised and, if necessary, additional safety functions defined so as to address fully the related ATM safety targets produced in Stage 1.

5.2.3 Output from this Stage:

- Set of primary safety functions, for the ATM service, whose specified performance, in the absence of failure, is sufficient for the risk in the operational domain to be substantially within the safety target(s).

[13] Justification for taking this approach would need to be provided

[14] The *primary* safety functions are the direct design response to the safety targets. They specify what the safety functions the service will execute and the performance required of them – in Stage 2.6, these will be supplemented by *derived* safety properties, specifying any additional safety functions required to mitigate against service failures, and the *integrity* required of all the safety functions.

- Any additional operational domain knowledge identified in the production of the primary safety functions.

5.2.4 Considerations:

- The analysis must be performed in the context of relevant operational domain knowledge.

- A thorough understanding of the basic concepts of modern requirements engineering is essential for the success of this stage. An overview is presented in section 2 above.

- If a safety function provided by the ATM service is used during more than one flight phase (en-route, approach or tower) then safety functions specific to all relevant flight phases may need to be defined separately.

- The generic safety functions have been prepared so as to be sufficiently general to encompass all ATM safety services. If there should appear to be a mismatch between the service under analysis and the generic model, it is important to investigate the reasons and to reconcile the conflict before proceeding further.

- The safety functions must consider the following *attributes* for each ATM system function; this list is not necessarily exhaustive:

    1. Functionality – what has to be done;

    2. Accuracy – fundamental precision and resolution of the output of the function;

    3. Timing – when, how often and how quickly the function has to be performed;

    4. Capacity – instantaneous capacity (eg number of simultaneous flights handled) and throughput rate (eg number of flights per hour);

    5. Overload tolerance – ability of function to respond to short-term capacity overload;

    6. Robustness – ability of function(s) to cope with failures external to it (or them);

  Where a particular attribute is not addressed in the safety function specifications, its omission must be justified in the satisfaction argument (see Stage 2.7 below).

5.3 Stage 2.3: Performance Risk Assessment

5.3.1 Objective:

To determine by how much the safety functions specified in Stage 2.2 would, in the absence of failure, reduce the risk of accident below that required by the safety targets.[15]

5.3.2 Process:

The ideal way to address the above objective would be to construct a performance model of the ATM service, based around the above safety functions and the operational domain knowledge identified in Stage 1, in order to predict what the risk of an SC1 event would be in the absence of failure in the service. The difference between this value and that required by the safety targets would then be carried forward (to Stage 2.5) as a target for the service safety objectives.

However, it is recognised that, in the short / medium term at least, an appropriate collision-risk model (CRM) is unlikely to be available to support such analysis, and therefore the following alternatives need to be considered.

Where the ATM service and operational domain knowledge (including, inter alia, separation minima) have remained substantially unchanged for a significant period of time, it may be possible to make use of appropriate historical data. Because of the required low frequency of an SC1 event, it is unlikely that enough data would be available from which to deduce an actual value for that frequency. However, in ATM it is usual to set separation standards such the normal operating risks (ie risk in the absence of failure) to a very low level - therefore, the absence of accidents in historical data could be used to argue **qualitatively** that the risk is negligible compared with the risk due to service failure.

Where the ATM service has changed, then any historical data would have to be interpreted in the context of the new situation before it could be used to deduce that the risk is negligible. The argument then becomes much more tenuous and might be difficult to substantiate, in which case some form of original performance modelling will probably be required. [16]

5.3.3 Output from this Stage:

- A prediction of the level of risk that would prevail in the operational domain in the presence of the specified safety functions but in the absence of any failure associated

[15] The rationale for this activity is provided by paragraph 2.2. If it cannot be shown that the system will perform (well) below the TLS in the absence of failure then there would be no point in proceeding further since the integrity required of the system would be unrealistically high (in the limit, infinite!)

[16] It is for this reason, for example, that extensive height-monitoring / collision-risk modelling has been used on the EUR RVSM Programmes to estimate the vertical collision risk resulting from the reduction in vertical separation minima.

with those functions – ie R_m as per Figure 2-1 of section 2 above.

5.3.4 Considerations:

- The analysis must be performed in the context of operational domain knowledge relevant to the phase of flight under consideration.

- Any potential dysfunctional interactions within the service - ie situations where the collective behaviour of the safety functions has an undesired effect[17] – must be taken into account. Such situations could occur, for example, where safety functions are mutually inconsistent, where different safety functions make different assumptions about common factors and / or data, or where there are inconsistencies between multiple instances of the "same" data in different parts of the system[18].

- Although in most cases the level of risk in the absence of failure will be low compared to the required frequency of an SC1 event, that may not always be the case and in future developments (eg the use of ADS for surveillance) the performance limitations of the system may become a more significant factor in the ability to meet the safety targets.

5.4 Stage 2.4: Hazard Identification and Consequence Analysis

5.4.1 Objective:

To identify the **hazards** presented by functional failure within the system, and their potential **consequences,** including possible mitigations.[19]

5.4.2 Process:

A functional failure analysis (FFA) should be performed in order to identify the hazards associated with the operation of the system, and a consequence analysis should be carried out to identify mitigations and the associated outcomes. The analysis should identify all credible outcomes, and each outcome should be classified according to the classification criteria defined in ESARR 4[20].

---

[17] Such behaviour would not be considered a failure of any particular function and may well be overlooked during conventional, static integrity analysis.

[18] Eg different versions of the aircraft's flight plan.

[19] The safety benefits of providing a system to reduce ATM risk can be significantly undermined if the system should fail to perform as specified. The rational for of this stage and Stage 2.5, therefore, is to understand the increase in risk which system failures represent.

[20] Note that some current safety practices attempt to classify hazards rather than the outcomes of hazards. That is illogical since all hazards (by definition) have some potential to cause an SC1 event, and would have to be categorised as SC1 !

The FFA and consequence analysis processes are well established and are not expanded upon further in this document. If further guidance is required, refer, for example, to [Ref 6].

5.4.3 Output from this Stage:

- Description of hazards presented by a failure of the service to perform as intended.
- A description of the possible mitigations and consequences (outcomes) of each hazard
- A classification of each possible outcome of each hazard, in accordance with the ESARR 4 severity classification criteria.

5.4.4 Considerations:

- The analysis must be performed in the context of relevant operational domain knowledge.
- It is essential to ensure that the concept of a hazard as a state on the boundary of a function / system is well understood. Refer to the overview of related concepts and terminology in Section 2.3.
- The most appropriate form of the model will depend on the particular circumstances. Often, a tabular form of FFA will suffice; however, where more than one mitigation is involved in a hazard, or if time sequence is important, Event Trees are usually more effective in modelling the potential outcomes of a hazard.
- Failure of data must also be considered, especially where such data are not produced by system functions.
- The possibility of dysfunctional interactions between different functions and data inconsistencies should again be considered during this stage.

5.5 Stage 2.5: Functional Risk Assessment

5.5.1 Objective:

To carry out a functional risk assessment, in order to determine the acceptable frequency of occurrence of each hazard, such that the safety target(s) are still met taking into account the possibility of such failures.

5.5.2 Process:

The functional risk assessment consists of the following steps:

- Assess the likelihood that each hazard mitigation will be successful;

- Hence calculate the probability that each hazard will lead to an SC1 event;

- Allocate the available risk budget from the safety targets to the individual hazards identified during the previous stage, taking into account the probability that each hazard will lead to an SC 1 outcome, and thence deduce the maximum acceptable frequency of occurrence of each hazard.

- Given the maximum acceptable frequency of occurrence of each hazard, check the corresponding frequency of occurrence of SC2 to 4 events against the global requirements of ESARR4, and decrease, as necessary, the maximum acceptable frequency of occurrence of the affected hazards.

- For any undeveloped events (eg increased workload) that have the potential to lead to a more severe (developed) outcome, assess the probability that such an outcome would arise. Multiply that probability by the corresponding frequency of occurrence of the undeveloped event and add the result to the frequency of occur of the more severe outcome. Decrease, as necessary, the maximum acceptable frequency of occurrence of the affected hazards such that the overall targets for SC1 to 4 outcomes are met.

5.5.3 Output from this Stage:

- Provisional determination of the maximum acceptable frequency of occurrence of each hazard.

5.5.4 Considerations:

- Tool support for the analysis may be required during this stage, so as to ensure that the SC 1 outcomes related to each hazard are correctly aggregated into a single overall frequency of the occurrence of an SC 1 event. Alternatively, it may be useful to produce a simple risk tolerability scheme to assist in this process, so as to allow an initial coarse allocation of risk budget. [21]

- For any given system, there exist potentially an infinite number of combinations of hazard occurrence frequencies that would allow the safety targets to be met. Consideration should be given at this stage to the potential achievability of those frequencies, since some potential solutions may be easier to implement than others. It may be necessary to iterate from later stages of the process back to this stage if the chosen frequencies are found during specification or design to be difficult to achieve.

- A completeness check should be performed. Have all hazards and consequences identified during the FFA been carried forward to this phase? Mapping the hazards on to the system functional model is often helpful in ensuring that the hazards are complete and have been properly described.

---

[21] This is done in the case of the Vertical Separation example provided with this Guidance.

- The analysis must be performed in the context of relevant operational domain knowledge.

5.6 Stage 2.6: Derived System Safety Properties

5.6.1 Objectives:

To express the outputs of Stage 2.5 as *derived* safety properties for the ATM service.

5.6.2 Process:

- Specify the safety objectives in accordance with the maximum acceptable frequencies of occurrence of each hazard, as determined in Stage 2.5.

- Identify any requirements for independence between functions – eg if a failure of function A is mitigated by function B, then we should ensure that function B is sufficiently independent of function A as to be unaffected by its failure.

- Record, as additional safety functions and safety objectives, the nature and probability of any *deliberate* mitigations identified in Stage 2.5.

- Record, as operational domain knowledge, the nature and probability of any *circumstantial* mitigations identified in Stage 2.5.

- Identify any safety monitoring requirements, so that the achieved level of safety may be measured against the safety targets and safety objectives. Using the achieved frequency of occurrence of SC1 outcomes would be both retrospectively unacceptable (because of the consequences) and statistically inadequate (because of the low frequency of occurrence), so it is necessary to select safety indicators which occur more frequently. The SC2 to SC4 outcomes identified in the event trees produced earlier can be used as indicators of occurrence of a hazard, because they are more frequent than SC1 outcomes (and are therefore more statistically useful) and we already have predicted frequencies of occurrence for them as a result of the earlier analysis.[22]

5.6.3 Output from this Stage:

- Safety objectives in the form of target frequencies for each hazard such that the overall risk of an SC1 event (and SC2 to SC4 events) is within the safety targets.

- Any additional safety functions and corresponding safety objectives necessary to provide deliberate mitigations of the hazards presented by the service failure.

[22] Safety indicators identified at this stage would necessarily be based on observing the occurrence and/or outcomes of hazards. Additional indicators, based on the causes of hazards, may emerge during the subsequent causal analysis, in Stage 3.3.

- Any additional operational domain knowledge assumed to provide circumstantial mitigations of the risk presented by service failure.

- Any safety objectives for independence between safety functions necessary to ensure that any failure is mitigated in the predicted manner.

- Requirements for the in-service safety monitoring of the system.

5.6.4 Considerations:

- All mitigations must be captured either as additional safety functions, including their required probability of success, or as operational domain knowledge.

- The safety indicators to be used for in-service safety monitoring rely on the correctness of the analysis carried out in Stage 2, and it is essential that this analysis is validated as part of the on-going safety monitoring process. If it is found that the measured frequency of occurrence of any safety monitoring event selected subsequently turns out to differ significantly from the predicted frequency, the cause should be investigated, as such a situation indicates either that the effectiveness of one or more of the mitigations is incorrect, or that the actual frequency of occurrence of the hazard differs from the predicted value. In either case, the predicted frequency of occurrence of any SC1 outcome related to the same hazard may also be incorrect.

- A completeness check should be performed. Have all hazards and consequences identified during the FFA been carried forward to this phase?

- The possibility of dysfunctional interactions between different functions and data inconsistencies should again be considered during this stage.

- The analysis must be performed in the context of relevant operational domain knowledge.

5.7 Stage 2.7: Validation of the Service Safety Functions and Objectives

5.7.1 Objective:

To show that the ATM service safety functions and safety objectives are necessary and sufficient to meet the ATM service safety targets produced in Stage 1.

5.7.2 Process:

A *satisfaction argument* needs to be presented to demonstrate that the ATM service safety functions and safety objectives are necessary and sufficient to meet the ATM service safety targets produced in Stage 1.1, having shown in Stage 1.2 that those safety targets are themselves necessary and sufficient to meet the TLS(s).

In general, the satisfaction argument will need to be supported by evidence from a variety of sources such as system functional modelling, simulation, collision-risk modelling, historical data, FMECA and Fault tree / Event Tree analysis.

It also needs to be shown that any additional operational domain knowledge, established during Stage 2, is complete and correct.

5.7.3 Output from this Stage:

- Satisfaction argument that validates the claim that we have a set of safety functions and safety objectives for the ATM service which will meet the ATM safety targets.

5.7.4 Considerations:

- It is most important to understand that the satisfaction argument is not simplify a matter of establishing traceability from the safety targets to the safety functions and safety objectives, but rather to show how the safety functions and safety objectives, individually and collectively, statically and dynamically, will achieve a level of risk in the operational environment that is within the limits set by the safety targets.

- The safety argument can only be established in the context of complete and correct operational domain knowledge.

- The satisfaction argument should be built upon both **direct evidence** – the most direct and tangible way of showing that a particular requirement has been achieved, and **backing evidence** – providing information about the quality of the direct evidence and the degree of confidence with which it can be used. In other words the backing evidence provides either a justification for the process by which the direct evidence was produced, or an independent (but less rigorous) way of showing that the main argument is valid.

- All attributes of the safety functions and safety objectives must be addressed – ie functionality, accuracy, timing, capacity, overload tolerance, robustness and reliability.

- Where the ATM service (including, *inter alia*, separation minima) itself has remained substantially unchanged for a significant period of time, the evidence of correct functionality (including the absence of any dysfunctional interactions) and adequate performance could be based on historical data. Even then it is likely that the argument will be largely qualitative – ie it would be argued that the absence of accidents indicates that the safety targets have been met – and it might be necessary to supplement the historical data with some of the techniques discussed under the next bullet point.

- Where the ATM service has changed, then any historical data would have to be interpreted in the context of the new situation. The argument then becomes much more tenuous and might be difficult to substantiate and it will probably be necessary to use, for example:

    1. System modelling and/or simulations to prove general functionality and to ensure that the system is free from dysfunctional interactions.

    2. Mathematical proof of more complex (and/or more critical) functionality.

    3. System modelling and/or simulations to prove timing; capacity; overload tolerance; and robustness.

4. Some form of collision-risk modelling to prove accuracy [23]

5. FTA / ETA to prove integrity.

- It is very important that the safety objectives are also achievable in the implemented system. If the initial safety objectives are not considered to be realistic, then further mitigations should be sought to reduce the consequences of the related hazards thus allowing the acceptable frequency of occurrence to be relaxed.

[23] It is recognised that, in the short / medium term at least, an appropriate CRM is unlikely to be available to support such analysis. Where this is the case, the consequential weakening of the satisfaction argument should be highlighted.

6. STAGE 3: SYSTEM SAFETY REQUIREMENTS DEFINITION

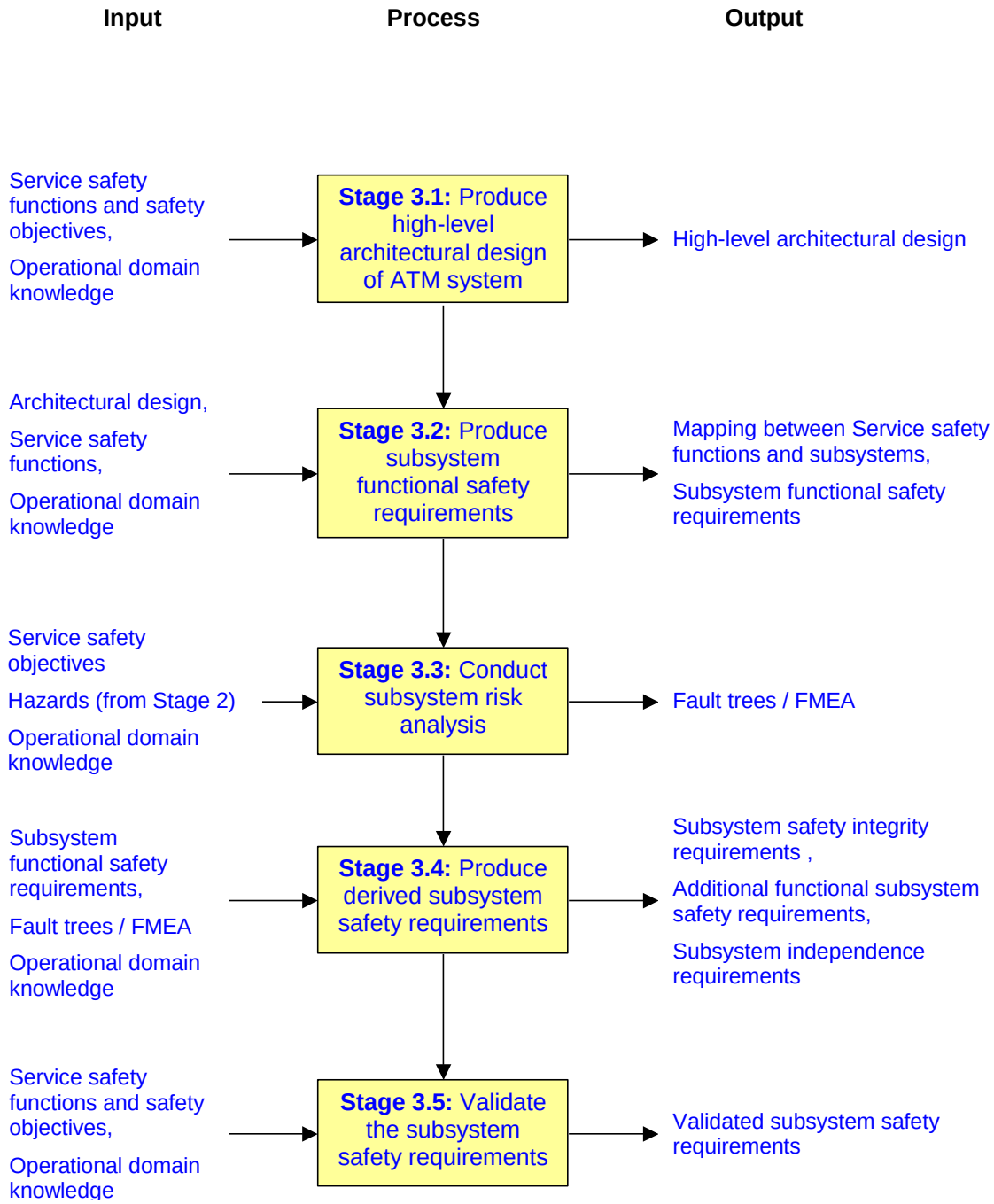


Figure 6-1 – Process Breakdown, Stage 3-PSSA

Stage 3 is outlined in the flowchart in Figure 6-1, and is described in sections 6.1 to 6.5.

NOTE: As Stage3 maps directly SAM-PSSA, the text here under does not intend to propose a new version of SAM-PSSA, but aims at proposing an application of PSSA stages in the light of the needs of the quantification method.

6.1 Stage 3.1: High-Level Architectural Design

6.1.1 Objective:

To produce a high-level system architecture capable of meeting the ATM service safety functions and safety objectives specified in Stage 2.

6.1.2 Process:

- Define the high-level system architecture in terms of the constituent subsystems, and the interactions between those subsystems.
- Describe the purpose of each subsystem, and interactions with other subsystems and the system's application domain, from a safety perspective.

6.1.3 Output from this Stage:

- High-level system architecture which includes all subsystems which comprise the system.

6.1.4 Considerations:

- The design at this level is moving towards a physical (rather than purely functional) view of the system.
- All elements of the system – ie equipment, people and procedural elements – must be included.
- The analysis must be performed in the context of relevant system domain knowledge.

6.2 Stage 3.2: Subsystem Functional Safety Requirements

6.2.1 Objective:

To determine the *primary* safety requirements[24] for the subsystem functions identified in Stage 3.1 above.

[24] The *primary* safety requirements describe only the subsystems safety functions and the performance required of them – in Stage 3.4, these will be supplemented by *derived* safety requirements, specifying any additional safety functions required to mitigate against subsystem failures, and the *integrity* required of all the safety functions.

6.2.2 Process:

- Allocate the service-level safety functions (the output from Stages 2.1 and 2.6) to the appropriate subsystems identified in Stage 3.1.

- Develop functional safety requirements for each subsystem so as to satisfy the allocation of service-level safety functions.

6.2.3 Output from this Stage:

- Mapping between service-level safety functions and subsystems.

- Functional safety requirements for each subsystem

- Any additional operational and/or system domain knowledge identified in the production of the (primary) functional safety requirements.

6.2.4 Considerations:

- Consideration must also be given to the interaction between the system and any non-ATM systems or subsystems, and to the implications of this on the system and non-ATM components.

- The functional safety requirements must address the attributes defined in paragraph 5.2.4 above; this list is not necessarily exhaustive:

    1. Functionality;
    2. Accuracy;
    3. Timing;
    4. Capacity;
    5. Overload tolerance;
    6. Robustness;

- An understanding of the interactions between subsystems may lead to a refinement of the independence requirements that were identified during Stage 2.6. The independence requirements may also be refined further during the next stage of the process (Stage 3.3).

- Relevant system (and subsystem) domain knowledge is essential at this stage.

6.3 Stage 3.3: Subsystem Risk Analysis

6.3.1 Objective:

To identify the risks presented by subsystem failure, for each of the hazards identified in Stage 2.

6.3.2 Process:

It is now necessary to allocate a risk budget to the subsystems so that the target frequency of occurrence for each hazard can be met, taking into account any mitigations available between subsystems. This can be achieved using either of the following techniques:

- Fault tree analysis – working top-down from the hazards identified in Stage 2.4, in effect producing a "bow-tie" fault tree / event-tree pair for each hazard. If this technique is adopted, the fault trees should not normally need to be developed further than the subsystem boundaries.

- Bottom-up consequence analysis, FMEA for example, working up from the subsystem boundaries to the ATM system boundary.[25]

6.3.3 Output from this Stage:

- A risk model of the causes of each of the hazards identified in Stage 2.

- Additional functional safety requirements and/or domain knowledge for all mitigations identified in the process.

6.3.4 Considerations:

- A completeness check should be performed: have all system hazards been taken into consideration – ie do any new hazards emerge at the subsystem level that have not been identified as causes of the hazards from Stage 2?

- All mitigations identified above must be captured either as additional functional safety requirements, including their required probability of success, or as system domain knowledge.

- Where mitigations at this level are complex, or sequencing is important, Event Tree Analysis could be used to supplement the Fault Tree Analysis.

- It is important to ensure that the result of any numeric analysis is expressed in the correct units. It may be appropriate at this stage to express the results in terms of accidents per system operating hour.

[25] It is advisable to apply both techniques, and to use the results of one to validate the other – thus providing input for the satisfaction argument which will be produced in Stage 3.5.

- Tool support for any fault tree analysis is important to ensure that the results of the numerical analysis are correctly aggregated.

- The analysis must be performed in the context of relevant system and sub-system domain knowledge.

6.4 Stage 3.4: Derived Subsystem Safety Requirements

6.4.1 Objective:

To express the outputs of Stage 3.3 as *derived* safety requirements for the subsystems.

6.4.2 Process:

Identify the subsystem safety integrity requirements, and any additional functional safety requirements, taking the results of the previous stage as input.

6.4.3 Output from this Stage:

- Subsystem safety integrity requirements – such that the service-level safety objectives are met.

- An identification of any additional functional safety requirements and/or domain knowledge which may be required to mitigate the risk presented by each subsystem.

- A refinement of the requirements for independence between subsystems.

- Identify any safety monitoring requirements additional to those identified in Stage 2.6.

6.4.4 Considerations:

- Consideration should be given to the potential achievability of the safety integrity requirements – some potential solutions may be easier to implement than others.[26]

- All mitigations must be captured either as additional functional safety requirements / safety integrity requirements or as assumptions.

[26] If necessary, the architectural design and/or system-level safety integrity requirements should be revised until a satisfactory result is obtained.

6.5 Stage 3.5: Validation of the Subsystem Safety Requirements

6.5.1 Objective:

To show that the subsystem safety requirements are necessary and sufficient to meet the service-level safety functions and safety objectives produced in Stage 2.

6.5.2 Process:

Produce a satisfaction argument to validate the claim that each service-level safety function and corresponding safety objective(s) is met collectively by the related subsystem safety requirements[27].

The validation must take into account functional correctness, performance and integrity.

The complete set of satisfaction arguments (from Stages 1.2, 2.7 and the current stage) must be of sufficient detail to provide *rich traceability*[28] from the subsystem safety requirements, through the service-level safety functions and safety objectives, and safety targets, back to the TLS). In other words, the satisfaction arguments will demonstrate that, the subsystem safety requirements are collectively sufficient to meet the overall TLS(s).

6.5.3 Output from this Stage:

- Set of satisfaction arguments, validating the claim that each service-level safety function / safety objective is met by the subsystem safety requirements.

6.5.4 Considerations:

- The satisfaction argument should be built upon both **direct evidence** and **backing evidence**.
- Functional correctness could be validated against a system functional model, simulation or prototyping.
- Performance could be validated through simulation or prototyping.
- If a top-down approach (eg FTA) was used to generate safety integrity requirements during Stages 3.3 and 3.4, it would be appropriate to validate this through a bottom-up approach (eg FMECA) – or vice versa.
- Verification activities could be used to support the validation argument, as backing evidence.

---

[27] Ie the subsystem *functional safety requirements* and *safety integrity requirements.*

[28] Rich traceability means that both traceability and satisfaction are demonstrated.

- The validation process should check that all analysis was consistent in the use of numerical units.
- The validation activity should check that the interaction between subsystems – including non-ATM subsystems – has been fully taken into account.
- People and procedures issues must be included in the validation.
- Achievability should be taken into account – ie is it likely to be possible to implement the specified system safety requirements?
- All domain knowledge must be validated.

7. REFERENCES

Ref. 1 Use of Safety Management Systems by ATM Service Providers, ESARR 3

Ref. 2 Risk Assessment and Mitigation in ATM, ESARR 4

Ref. 3 Functional Safety of Safety Related Systems, International Electrotechnical Commission, IEC 61508

Ref. 4 Nancy G Leveson, The Role of Software in Recent Aerospace Accidents, Proceedings of the 19th International System Safety Conference, Huntsville, Alabama, USA Sep 01

Ref. 5 A J Simpson and J. Stoker, Will it be Safe? An approach to Engineering Safety Requirements, Safety Critical Systems Club Symposium, February 2002.

Ref. 6 Guidance and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE, ARP 4761, December 1996

Ref. 7 Aircraft Accidents/Incidents and ATM Contribution, SRC DOC 2

Ref. 8 EUROCONTROL EATMP Air Navigation System Safety Assessment Methodology (FHA Edition 1.0, PSSA Edition 1.0).

Ref. 9 EUROCONTROL, Air Traffic Management Strategy for 2000+ (November 1999).

8. ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used in this document.

AIS	Aeronautical Information Service
AMC	Acceptable Means of Compliance
APP	Approach
ATC	Air Traffic Control
ATM	Air Traffic Management
CFIT	Controlled Flight Into Terrain
CRM	Collision Risk Modelling
EATMP	European Air Traffic Management Programme
ESARR	EUROCONTROL Safety Regulatory Requirement
ET	Event Tree
ETA	Event Tree Analysis
FFA	Functional Failure Analysis
FHA	Functional Hazard Assessment
FMECA	Failures Modes Effects and Criticality Analysis
FT	Fault Tree
FTA	Fault Tree Analysis
PSSA	Preliminary system Safety Assessment
RVSM	Reduced Vertical Separation Minima
SC	Severity Category
SR	Safety Requirement
SS	Subsystem
SSA	System Safety Assessment

TLS	Target Level of Safety

APPENDIX A: GUIDANCE ON SAFETY TARGETS

A.1 Note on the Scope of Applicability of ESARR4

As shown in the body of this Guidance, the first two levels of satisfaction of the safety target(s) are achieved through:

- Firstly, the specification of ATM service-level Safety Functions and Safety Objectives, and the related Operational Domain Knowledge.

- Secondly, the functional design and Safety Specification (including related Domain Knowledge) of an ATM system that is capable of meeting those safety requirements.

It is essential that both the scope of the ATM service and the boundary of corresponding ATM system are not only clearly defined but also that they relate exactly to the scope of the TLS that they are intended to satisfy.

In the case of ESARR4, the TLS of 1.55×10^{-8} SC1 events per flight hour represents the maximum tolerable probability (sic) of ATM directly contributing to an accident of a commercial air transport aircraft.

In general, ATM may directly contribute to an accident by either:

- **commission** - ie causing (or significantly contributing to the cause of) an accident that would not have otherwise occurred;

- or **omission** - ie failing to prevent an accident from occurring, when ATM could reasonably have been expected to prevent it (or significantly help to prevent it).

Each case has to judged on its merits but in general the risk of an accident can be said to be within the scope of the ESARR4 TLS if the cause (or significant contribution to the cause) of an accident either:

1. Lies within the ATM system loop – irrespective as to whether the problem is in the ground, air or space segment of that loop.

2. Or lies outside of the ATM loop but ATM could reasonably have been expected to mitigate the initiation or consequence of the causal event.

Determination of what lies within, and outside, the ATM system will depend on, *inter alia*, the phase of flight and type of service under consideration. For example:

- For en-route control, the aircraft altimetry system would be considered to be an integral part of the ATM (Vertical Separation) system, since the ATM system was deliberately designed to make full use of altimetry data.

- For final approach using, say, ILS, the aircraft altimetry system[29] would not be considered to be an integral part of the ATM system, since in this case vertical separation is a pilot-interpreted system.

Wherever practicable and appropriate, the parameters of every element of the ATM system should be included within the Safety Specification; where it not practicable or appropriate, the appropriate parameters must be included as assumptions in the Domain Knowledge, so that full account is taken of them in determining whether the TLS is satisfied. The relevant parameters associated with causal events that lie outside of the ATM loop (for example, the expected frequency of occurrence of such events) must always be included within the Domain Knowledge.

A.2 Units of Measurement

Because the TLS is expressed in units of incidents per flight hour, the value of 1.55×10^{-8} specified in ESARR 4 can be applied unchanged to any part of the airspace and any phase of flight irrespective of the size of the airspace, number of sectors, traffic levels, flight duration, etc.

During the apportionment process, any numerical analysis should be conducted in the units most appropriate to the specific failures under consideration. Experience has shown that it more convenient to work in units of incidents per flight hour as far as possible through the process. It is recognised that it will be necessary to convert to units of incidents per system hour at some stage before the system can be implemented because, for example, equipment reliability is usually expressed in such units. However, this point will normally occur during subsystem design – a later stage in the development process later than is covered by the scope of this document.

Where additional TLS have to be met and are expressed in different units - eg for the approach and landing flight phases, units of incidents per landing are specified – it is recommended that they be converted to units of incidents per flight hour (according to average duration of the flight phase) for comparison with the ESARR 4 TLS. .

A.3 Weighting the TLS

Although the value of 1.55×10^{-8} accidents per flight hour can be applied universally, it may be desirable in certain circumstances to weight the TLS more heavily towards one phase of flight as opposed to another, taking into account the relative level of risk and the exposure time in the specific phases. Historic data, for example from [Ref 7] can be useful in this respect.

A.4 Target Setting for SC2 to SC4 Events

The following guidance should be applied when determining appropriate target frequencies of occurrence of SC2 to SC4 events.

[29] Note however, that the provision of correct QFE / QNH data would be considered to be part of the ATM system.

From an **a priori system design** point of view, the number of predicted fully developed[30] SC2 to SC4 events would have no bearing on the probability of occurrence of an accident (SC1 event) and therefore is not related to system safety in the strict meaning of the term safety. However, it would be inappropriate to design a system such that the permitted rate of SC2 to SC4 events would lead to the perception that the system was unsafe. Therefore, a global limit should be placed on the rate of such events, and the system design must therefore ensure that the target for all categories of event are met, not just those for SC1 events. Ideally, ESARR 4 should specify global targets for fully developed SC2 to SC4 events based on historical acceptability or equivalence values (applying a factor of, say, 100 between one severity level and the next[31]); the current lack of historical data would suggest that such an equivalence approach is needed in the short term.

From an **a posteriori safety monitoring** perspective, the situation is more complex, and two questions need to be asked:

- Firstly, whether the system is perceived to be safe, based on the number of actual SC2 to SC4 events compared with the ESARR 4 targets – this is equivalent to the above a priori analysis.

- Secondly, whether the rate of occurrence of SC2 to SC4 events is an (indirect) indication that the system is actually safe (ie whether the likelihood of an SC1 event is higher or lower than would be acceptable[32]). For this analysis, the actual number of SC2 to SC4 events over a defined period must be compared with the expected number[33], not with the limit prescribed by ESARR 4. This is the basis of the safety monitoring approach described in section 5.6 and illustrated in the En-route Airspace example which accompanies this guidance.

[30] A fully developed event is one which has reached a final conclusion – ie there is no potential for further consequences. Undeveloped events, such as those relating to increased workload, have the potential to lead on to more serious consequences (including an SC1 outcome) – the Method provides the means for handing these.

[31] Such that, for example, the *a priori* safety target for SC2 events would be 1.55×10^{-6} per flight hour.

[32] It is assumed that the rate of occurrence of SC1 events would be so low as to render statistically inconclusive any analysis based on direct observations of such events.

[33] The expected number as determined during the risk assessment conducted during Stage 2.5 of the Method.

APPENDIX B: GENERIC ATM SERVICE SAFETY MODEL

B.1 Generic Model

This appendix presents an initial generic model of the safety functions provided by the air traffic management service for the en-route flight phase. The model is intended to assist in the process of identifying functional safety specifications specific to the service under analysis during Stage 2.1 of the apportionment method.

Six functional areas are identified:

- Tactical separation
- Flight directing
- Strategic separation
- Co-ordination and transfer
- Traffic management
- Aeronautical information

These six functional areas are further decomposed into specific safety functions[34]. The safety functions are then developed into more detailed generic safety specifications.

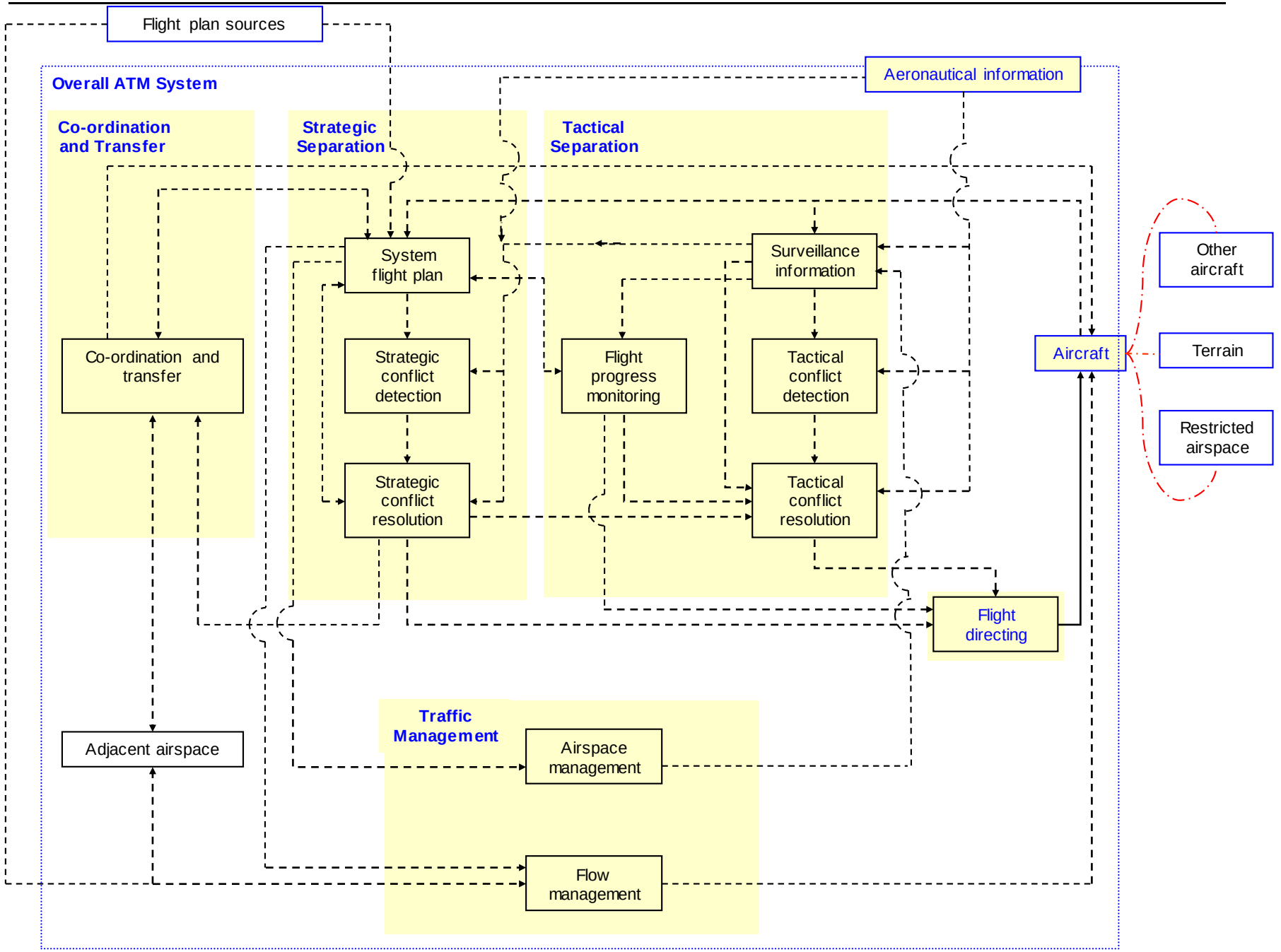
The diagram indicates the interaction of the safety functions which operate so as to maintain separation between any aircraft and other aircraft, terrain or restricted airspace. A solid line indicates control flow, and dotted lines indicate information flow.

The model, as presented, is designed to be applied directly to ATC in the En-route phase of flight, and to be adaptable to other flight phases. For example:

- Removal of Strategic Separation would provide the basis for modelling the Approach phase.
- Removal of Tactical Separation would provide the basis for modelling an Oceanic phase.

Note that the boundary of the overall ATM system has been placed so as to include an airborne component – for example, transponders and ADS.

[34] Although Flight Directing and Aeronautical Information do not logically decompose further.


Flight plan sources
Overall ATM System
Aeronautical information
Co-ordination and Transfer
Strategic Separation
Tactical Separation
System flight plan
Surveillance information
Other aircraft
Co-ordination and transfer
Strategic conflict detection
Flight progress monitoring
Tactical conflict detection
Aircraft
Terrain
Restricted airspace
Strategic conflict resolution
Tactical conflict resolution
Flight directing
Traffic Management
Adjacent airspace
Airspace management
Flow management

The safety functions are described in the tables below. Note that these tables are limited to a generic functional description; any application of this model will require attributes such as accuracy, resolution, timing, capacity, overload tolerance and robustness to be taken into account.

Functional Area: Tactical Separation

Safety Function	Description	Initiation
Surveillance information	The function shall provide: • Current identification, position, heading, altitude / flight level, track and groundspeed information for all Aircraft in the Airspace. • Airspace information – ie maps (including information on boundaries, obstacles and restricted Airspace / danger areas) for the Airspace. • Information on Airspace weather conditions - eg heavy precipitation	Near-continuous operation.
Tactical conflict detection	The function shall determine, in the near term, all potential erosions of required separation minima between each of the following: • any two aircraft; • any one aircraft and restricted / prohibited airspace; • any one aircraft and an active danger area; • any one aircraft and terrain / ground-based obstacle	Continual operation, based normally on information from the Surveillance Information safety function

Safety Function	Description	Initiation
Tactical conflict resolution	The function shall identify appropriate changes to an aircraft's heading, flight level or airspeed as necessary to resolve the conflict situation.	Whenever a potential erosion of required separation minima is detected by Tactical Conflict Detection.
Flight progress monitoring	The function shall check conformance between actual and cleared trajectories, and resolve any non-conformance through Tactical Conflict Resolution / Flight Directing and, where appropriate, an update to the System Flight Plan (see below).	Continuous operation.

Functional Area: Flight Directing

Safety Function	Description	Initiation
Flight directing	The function shall: • Issue clearances and/or other instructions as necessary to effect the necessary changes to the trajectory of the Aircraft involved; • Handle clearance requests and / or other information from Aircraft. • Provide directions for the orderly sequencing of traffic; • Provide airport and weather information relevant to the progress of the flight.	Whenever required by Tactical Conflict Resolution, Strategic Conflict Resolution, Flight Progress Monitoring (see below), or Aircraft.

Functional Area: Strategic Separation

Safety Function	Description	Initiation
System flight plan	The function shall provide for the creation, storage and maintenance of a system representation of aircraft flight plan information, including: • Callsign • Intended 4-D trajectory • RVSM status • R-NAV status • 8.33Khz status • Estimated time at (airspace) boundary	As required by (*inter alia*) external flight plan sources, Flight Progress Monitoring, Strategic Conflict Resolution, Co-ordination & Transfer, or Aircraft.
Strategic conflict detection	The function shall determine, in the medium term, all potential erosions of required separation minima between each of the following: • any two aircraft; • any one aircraft and restricted / prohibited airspace; • any one aircraft and an active danger area; • any one aircraft and terrain.	Continual operation, normally on information from System Flight Plan and Surveillance. Also, triggered by any proposed change to System Flight Plan.

Safety Function	Description	Initiation
Strategic conflict resolution	The function shall: • Identify appropriate changes to an aircraft's intended 4-D trajectory, as necessary to resolve the conflict situation. • Advise Co-ordination and Transfer, System Flight Plan and/or Flight Directing (as appropriate) accordingly. Where it is not possible to resolve a conflict strategically, the function shall advise Tactical Conflict Resolution, for the conflict to be resolved tactically.	Whenever a potential erosion of required separation minima is detected by Strategic Conflict Detection.

Functional Area: Co-ordination and Transfer

Safety Function	Description	Initiation
Co-ordination and transfer	The function shall: • By means of information exchange between the controlling authorities of adjacent Airspace, obtain agreement on 'boundary conditions' (position, altitude/ flight level, time etc.). • Issue clearances and instruction for transfer of control. • Effect the transfer of control of an Aircraft from one controlling authority Airspace, to the next. • Provide notification to Airspace controlling authorities, where a flight is in an area of common interest, or when the transit is close to a boundary of control.	Whenever an Aircraft is due to enter or leave the Airspace under consideration.

Functional Area: Traffic Management

Safety Function	Description	Initiation
Airspace Management	The function shall adjust the traffic capacity of the Airspace in anticipation of significant changes in traffic demand, so as to maintain a safe, orderly, expeditious and economic traffic flow.	When required.
Flow Management	The function shall adjust the flow of traffic within a portion of airspace so as to ensure that the present or predicted traffic demand does not exceed the safe capacity of the ATC service.	When the flow of traffic exceeds (or is likely to exceed) the sustainable capacity of the Airspace.

Functional Area: Aeronautical Information

Safety Function	Description	Initiation
Aeronautical Information	The function shall process and distribute essential aeronautical information including: • The nature, dimensions and timings of restricted Airspace. • Meteorological conditions (actual and forecast). • Airport information. • Status of services and systems. • Procedures and regulations.	Continuous operation.

B.2 Concept of Operations

B.2.1 En-route Operations

Progressively updated (strategic) information concerning the flight is exchanged by the ***Co-ordination and Transfer (C&T)*** function before the flight is planned to enter the receiving Airspace. Prior to the planned entry into the Airspace, the flight details will be checked by the ***Strategic Conflict Detection (SCD)*** function for conflicts anywhere along its route through the Airspace.

If there is a conflict, it may be resolved by the ***Strategic Conflict Resolution (SCR)*** function resulting in a request to the handing-over control authority, via the C&T function, to modify to the aircraft's trajectory. Where appropriate, the Aircraft's flight data will be updated by the ***System Flightplan (SFPL)*** function. If the conflict is irresolvable at that stage, it will be resolved by ***Tactical Separation (TSF),*** once the aircraft has entered the receiving Airspace.

Immediately prior to the Aircraft entering the receiving Airspace, the respective C&T function effect the handover of control responsibility from the adjacent control authority.

Short-term separation is maintained by ***TSF*** and in the medium term by the ***Strategic Separation function*** **(*SSF*)** – in both cases, resolution of the conflict will be effected via the ***Flight Directing function*** **(FDF).** The primary objective of the ***SSF*** is to remove from the system as many potential future conflicts as possible thus reducing the workload on ***TSF*** and reducing the risk of a potential conflict remaining undetected.

Airspace Management function **(*AMF*)** ensures (strategically) that the traffic capacity is matched to the expected pattern of short-term traffic demand economically, but without impairing the safe, orderly, and expeditious flow of traffic.

The ***Flow Management function*** **(*FMF*)** ensures that the traffic capacity and traffic demand are balanced tactically, such that overload of the other ATM functions does not exceed the declared capacity of the ATM service (for the current configuration).

The ***Aeronautical Information function*** **(*FMF*)** provides tactical /pre-tactical static/dynamic data service to ensure aircraft are managed according to the current rules and conditions.

Prior to the aircraft exiting the Airspace, the ***C&T*** function effects the handover of responsibility for control to the next block of Airspace, as described at the beginning of this section.

B.2.2 Approach Operations

The Approach service operates in the same way as for En-route except that:

- There is no Strategic Conflict Detection or Strategic Conflict Resolution function as such. However, outputs from the System Flight Plan function are used in the (strategic) planning of arrivals and departures traffic so that they are sequenced and spaced in order to maintain an expeditious flow and to smooth out the workload on Tactical Separation.

- The flow of traffic into APP airspace is regulated according to the prevailing weather, runway in use and runway configuration using Flow Management.

- Distribution of information on prevailing weather, runway in use and runway configuration, etc, forms part of the Aeronautical Information function for the Approach service.

END OF DOCUMENT