EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

CHAIN
Preliminary Safety Case

CHAIN

Controlled and Harmonised
Aeronautical Information Network

CHAIN/0135

Edition Number	**:**	**0.4**
Edition Date	**:**	**24 Oct 2006**
Status	**:**	**Proposed Issue**
Intended for	**:**	**Restricted audience**

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
CHAIN Preliminary Safety Case		
	EATMP Infocentre Reference:	
Document Identifier	**Edition Number:**	0.4
CHAIN/135	**Edition Date:**	24 Oct 2006

Abstract

The ultimate objective of the CHAIN Safety Case is to provide the argument and evidence to support the outputs of the CHAIN Activity and provide States with a generic safety assessment framework that can be used to support national AIS improvement activities.

This Preliminary Safety Case thus aims to provide guidance to States and to substantiate, with respect to safety requirements derivation, the claim that CHAIN will deliver a net ***safety benefit*** to ATM and other users.

Keywords

Contact Person(s)	Tel	Unit
M. UNTERREINER	3038	DAP/AIM/CHAIN

STATUS, AUDIENCE AND ACCESSIBILITY

Status		Intended for		Accessible via	
Working Draft	☐	General Public	☐	Intranet	☐
Draft	☐	EATMP Stakeholders	☐	Extranet	☑
Proposed Issue	☑	Restricted Audience	☑	Internet (www.eurocontrol.int)	☐
Released Issue	☐	*Printed & electronic copies of the document can be obtained from the EATMP Infocentre (see page iii)*			

ELECTRONIC SOURCE

Path:	C:\Efi's Folders\Projects\DataChain - P05007\20\P05007.20.3 - Preliminary Safety Case\Issue 1.0 Final\300306 Version On EBENI-LT-005	
Windows_NT	Microsoft Word 11.0	2104 Kb

EATMP Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS
Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Please make sure that the EATMP Infocentre Reference is present on page ii.		
Ebeni Ltd	E. RAILI A. SIMPSON	24 October 2006
EUROCONTROL DAP/SAF	D. FOWLER	24 October 2006
EUROCONTROL CHAIN Manager	M. UNTERREINER	24 October 2006

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	Oct 2005		Working draft version	All
0.2	Dec 2005		Draft for comment	All
0.3	Mar 2006		Updated to address comments	All
0.4	Oct 2006		Review of Final draft; SC Checklist assessment by DAP/SAF; Creation of proposed issue	All

CONTENTS

EXECUTIVE SUMMARY

Current and future navigation and other ATM systems are data dependent and reliant upon the provision of timely, accurate and correct Aeronautical Information. However, it is well known that the integrity of Aeronautical Information in use today does not provide the level of quality required and does not always conform to either the requirements laid down by ICAO Annex 15 or the needs of the users.

The EUROCONTROL Controlled & Harmonised Aeronautical Information Network (CHAIN) Activity has a high level aim to enable interoperability in the Aeronautical Information Services (AIS) environment. CHAIN's primary objective is to improve the accuracy and quality of the originated data and its management from the point of origination through publication to States' distribution of Aeronautical Information Publications (AIPs) and to subsequently enable enhanced processing throughout the entire Aeronautical Data Chain.

CHAIN has and will propose a series of improvements to the Upstream Data Chain aimed at addressing ICAO Annex 15 compliance issues, improving data integrity and providing users in the ATM domain with the data quality they require for current and future needs. States can choose which improvements to implement to support their Data Chain enhancement activities.

The ultimate objective of the CHAIN Safety Case is to provide the argument and evidence to support the outputs of the CHAIN Activity and provide States with a generic safety assessment framework that can be used to support national AIS improvement activities.

This Preliminary Safety Case captures the safety argument, available evidence and current shortfalls in the substantiation of the argument to support the claim that CHAIN will deliver a net ***safety benefit***[1] to ATM and other users. The CHAIN Safety Argument is based on four principal arguments as they apply to the scope of the CHAIN activity.

- Safety Requirements are defined to ensure the ***safety benefit*** is achieved.
- Guidance is provided on their implementation and the changes required.
- States show that the Safety Requirements are met in the implementation of the changes to Upstream Data Chain.
- Safety monitoring is in place to ensure that the ***safety benefit*** is maintained in the ongoing operation of Upstream Data Chain.

This Safety Case focuses on the evidence for the first two arguments and thus the conclusions are subject to full satisfaction of the other two arguments by individual States who implement CHAIN improvements. However, based on the evidence that is currently available and considering the number of open safety issues, it is concluded that the first two arguments are not yet fully substantiated.

[1] ***safety benefit*** is defined as:
- significantly reduces the probability of critical, essential or routine data errors in published AI;
- increases the confidence that the required level of integrity in published AI is achieved; and
- further reduces the probability of data errors as far as reasonably practicable (AFARP)

As the proposed CHAIN improvements are still under development, the Preliminary Safety Case should be revisited and updated to provide the additional evidence to support specific CHAIN improvements, resolve the outstanding issues allocated to CHAIN and incorporate any implications of the Aeronautical Data Integrity Mandate.

The Safety Argument and supporting Safety Assessment provides a framework in which a State can develop its own Safety Case(s) for improvements to the Data Chain. The States will need to take the material herein along with the supporting Safety Assessments, adapt as necessary to their particular operational processes and develop evidence concerning the implementation of the CHAIN improvements or other Data Chain improvements, for which they are responsible.

1. INTRODUCTION

1.1 Background

Current and future navigation and other ATM systems are data dependent and reliant upon the provision of timely, accurate and correct Aeronautical Information. However, it is well known that the integrity of aeronautical information in use today is not sufficient for the needs of the users and does not always conform with the requirements laid down by ICAO.

In addition, the ATM 2000+ Strategy states that Aeronautical Information Services (AIS) will be improved and developed within ECAC to provide a harmonised, co-ordinated service delivering quality-assured information for all phases of flight. This will be achieved through the increased use of automation, the introduction of quality management, and the evolution of aeronautical information provision to meet the interoperability requirements of system-wide information management.

EUROCONTROL has recognised this as a major issue and is undertaking a number of activities and programmes to improve the current situation. One of these activities is the pan-European, “Controlled & Harmonised Aeronautical Information Network – CHAIN”. The vision of CHAIN is to establish a data supply chain to support regulators, service providers and other stakeholders and also to enable system-wide interoperability. The primary objective is to improve the accuracy and quality of the originated data and its management for the Upstream Data Chain – ie from (but not including) the point of origination to the point of publication – and to enable subsequent enhanced processing throughout the entire data chain.

1.2 Development of the Preliminary Safety Case

As part of the CHAIN Activity a Preliminary Safety Impact Study [8] was carried out that identified a number of mechanisms whereby a safety benefit to the ATM environment could potentially be achieved. The results of this work and work carried out on the European Aeronautical Database (EAD) provided input into the development of a Preliminary Safety Case, with the objective of substantiating the claim that CHAIN will deliver a net safety benefit.

A Functional Hazard Assessment/Preliminary System Safety Assessment (FHA/PSSA) was conducted to provide an independent assessment of the hazards and risks related to the current Aeronautical Upstream Data Chain within the scope of CHAIN and to derive CHAIN Safety Requirements. The output of this activity forms the basis of this Preliminary Safety Case and is documented in [9].

1.3 Aim

The aim of this document is to set out the safety argument, and present the supporting evidence currently available, to show that CHAIN will deliver a net safety benefit, i.e.:

- significantly reduce the probability of critical and essential data errors in published AI (Note: Although formally out of scope for CHAIN a positive effect on routine data is expected as well);
- increase the confidence that the required level of integrity in published AI is achieved; and
- further reduce the probability of data errors as far as reasonably practicable (AFARP).

1.4 Purpose

The purpose of the preliminary CHAIN safety activity is two-fold:

1. to document the safety argument, available evidence and identified shortfalls in substantiation of the claim that CHAIN will deliver a net safety benefit; and
2. to provide the basis for each State to develop its own Safety Case(s) for the CHAIN improvements to the Upstream Data Chain and to facilitate that process by carrying out much of the required safety analysis, although on a generic basis.

States can take the material herein and in the supporting FHA/PSSA, adapt it as necessary to their particular operational environment and develop evidence concerning the implementation of their Data Chain improvements, for which they are responsible, but must take the implications of the identified safety issues (see section 6.2.2) into account. Guidance for States on the adaptation of the material presented in this Safety Case will be provided in a future edition.

1.5 Scope

This Preliminary Safety Case presents the results of the safety assessment activity carried out for the current Upstream Data Chain as scoped by CHAIN.

The analysis and conclusions presented herein cover the current Upstream Data operation (see Appendix B), i.e. from the point of origination (excluding Data Origination and its processes but including the transfer of Aeronautical Information (AI) from Data Origination to Data Publication) through to the publication and distribution of the Integrated Aeronautical Information Package (IAIP) by the State.

The analysis does not consider:

1. Origination of Raw Data or Procedures;
2. Downstream Data Chain activities, i.e. Data Application/Integration and Data End Use.
3. The regulation of Data Chain, although the impact that regulation could have on the achievement of a net safety benefit is considered. The issues raised in relation to regulation are to be considered as part of the development of the Aeronautical Data Integrity (ADI) Mandate.
4. Security aspects of the Data Chain, where they do not relate to safety.

It is recognised that the integrity of aeronautical data can only be fully addressed by considering the whole of the Data Chain from source origination through to

application integration and end use. As such the safety assessment has identified but not addressed those issues that can only be dealt with holistically such as the apportionment of Data Integrity Levels.

1.6 General Approach

The approach adopted complies with the general (qualitative) requirements of ESARR 4 [3], to the extent shown in Appendix J. Safety Requirements were derived for CHAIN based on:

- identifying issues in the Upstream Data Chain regarding compliance with the 'output requirements'[2] of Annex 15;
- identifying the means of correcting those inadequacies and expressing them as Safety Requirements;
- deriving Safety Requirements that will be addressed by CHAIN and devising a strategy for addressing those not addressed by CHAIN;
- providing 'Backing' evidence that sound processes were correctly applied, by competent people in deriving the Safety Requirements.

The safety assessment was bound by the same scope as the CHAIN Activity as discussed in section 1.5, but was not limited to the improvements being proposed by CHAIN nor the specific issues identified in the previous Safety Impact Study [8]. In addition, the assessment of data integrity was not restricted to just the maintenance of integrity as defined in ICAO Annex 15.

The derived safety requirements were rationalised with ICAO Annex 15 and EUROCAE ED76 requirements to identify gaps or issues of compliance. Where issues and/or gaps are identified, actions are recorded for the CHAIN or ADI Mandate activities to resolve.

1.7 Layout

Section 1 Introduction – presents an overview of the Preliminary Safety Case, its background, aim and scope.

Section 2 Context for the Preliminary Safety Case – presents the overall context for the Preliminary Safety Case.

Section 3 CHAIN Description – presents a description of the improvements to the Data Chain as proposed by the CHAIN Activity.

Section 4 Overall Safety Argument – presents the top level safety argument, including safety criteria and assumptions.

Section 5 Derivation of CHAIN Safety Requirements – presents the principal Safety Argument that CHAIN improvements realise a safety benefit together with supporting evidence.

[2] The integrity level classification for data items in Appendix 7.

Section 6 Conclusions and Recommendations – presents the conclusions and recommendations the Preliminary Safety Case.

Appendix A Definition of Data quality Properties – provides the definition of data quality properties based on ICAO Annex 15 and EUROCAE ED-76.

Appendix B Data Chain Functional and Logical Models – contains a series of diagrams presenting the Data Chain functional and logical models.

Appendix C Detailed Evidence for Arg 1.1 – provides detailed evidence from the FHA/PSSA activity to substantiate Arg 1.1.

Appendix D FHA/PSSA Relationship diagram – the diagram presents the components of the FHA/PSSA process and the input/output relationship between these components.

Appendix E Identified Current Data Chain Problems – presents a list of identified problems with current Data Chain.

Appendix F Upstream Data Chain (UDC) Safety Requirements – presents the derived UDC Safety Requirements defined in three levels.

Appendix G CHAIN Safety Requirements – provides the derived CHAIN safety requirements.

Appendix H CHAIN Safety Argument – presents the complete safety argument of the CHAIN improvements to the Upstream Data Chain.

Appendix I Goal Structuring Notation (GSN) – presents a guide to understanding the Safety Argument notation.

Appendix J ESARR 4 Process compliance - shows the degree and extent to which the approach taken in undertaking the safety analysis is compliant with the analysis process requirements of ESARR 4.

Appendix K Abbreviations and Acronyms - presents a table of abbreviations and acronyms used throughout the document.

Appendix L References.

2. CONTEXT FOR THE PRELIMINARY SAFETY CASE

2.1 Safety Policy

The EATMP Safety Policy [4] defines four Policy Statements for the management of ATM safety:

1. **Safety Management** – The ECAC States participating in EATMP should adopt an explicit, pro-active approach to safety management in the Air Navigation Services.
2. **Safety Responsibility** – Everyone has an individual responsibility for their own actions and managers are responsible for the safety performance of their own organisations.
3. **The Priority of Safety** – The achievement of satisfactory safety in the Air Navigation Services should be afforded the highest priority over commercial, operational, environmental or social pressures.
4. **The Safety Objective of Air Navigation Services** – While providing an expeditious service, the principal safety objective is to minimise the Air Navigation Services' contribution to the risk of an aircraft accident as far as reasonably practicable.

The purpose of the CHAIN Activity is to specify improvements within the upstream Data Chain activities, in keeping with Policy Statement 4, by:

- assessing the safety benefit from identifying improvements that will address issues within the current Data Chain offered by CHAIN or not;
- developing generic material for assessing the safety benefit of future improvements;
- informing the development of CHAIN Procedures and Guidelines in respect of achieving the safety benefits.

2.2 Relevant Standards and Regulatory Requirements

2.2.1 ICAO Requirements

Section 3.1.7 of ICAO Annex 15 [5] requires that the Aeronautical Information Services (AIS) of each Contracting State are required to:

"*…receive and/or originate, collate or assemble, edit, format, publish/store and distribute aeronautical information/data concerning the entire territory of the State as well as areas in which the State is responsible for air traffic services outside its territory*".

2.2.2 ESARR

The regulatory context for the CHAIN Preliminary Safety Case is captured within the EUROCONTROL Safety Regulatory Requirements (ESARR) and ICAO Annex 15 [5].

The ESARR most relevant to CHAIN improvements to Upstream Data Chain is ESARR 4 [3], which identifies the requirements for the structured assessment and mitigation of risk.

Although, currently, ESARR 3 [14] and ESARR 6 [15] are not applicable to AIS activities, it is considered that adoption of the principal objectives of these regulations is good practice.

Of particular interest in ESARR 3 is the requirement on ANSPs to reduce risk *as far as reasonably practicable* – this is the basis of one of the Safety Criteria discussed in section 4.3 below.

2.2.3 EUROCAE ED-76 / ED-77

The “Standards for Processing Aeronautical Data” document (EUROCAE ED-76 / RTCA DO-200A) [6] provides a recommended minimum standard for the processing of aeronautical data that are used for navigation, flight planning, terrain awareness, flight simulators and for other applications. It is applicable to all phases of the aeronautical data process, from origination through acceptance and application by the end-user. The standard provides requirements that should be used to develop, assess change, and support implementation of data processing quality assurance and data quality management.

The “Industry Requirements for Aeronautical Information” (EUROCAE ED-77 / RTCA DO-201A) [7] provides aeronautical information requirements of the aviation industry with emphasis on Area Navigation (RNAV) operations in Required Navigation Performance (RNP) airspace. The standard discusses the needs for standards that will accommodate the requirements for aeronautical data elements including accuracy, resolution, calculation conventions, naming conventions, and the timely dissemination of the finished data. It also describes specific operational requirements that civil aviation authorities, procedure designers and airspace planners should consider when developing procedures in the en route, arrival, departure, approach, and aerodrome environments and proposes standards where appropriate. The requirements and associated standards presented in ED-77 are not all inclusive but represent those of immediate concern to RNAV and RNP operations. This standard is applicable to this Safety Case in that it contains updated data integrity level assignments to the data integrity levels contained in ICAO Annex 15 [5].

3. CHAIN DESCRIPTION

3.1 Overview

The Aeronautical Data Chain is a conceptual representation of the path that a set, or an element, of aeronautical data takes from its creation through to the end use. As in a physical chain, each link is connected to its adjacent links, however, unlike a chain there may be many adjacent links. The symbolic links in the Aeronautical Data Chain can range from organisations and departments, to individuals and specific equipment. Many different Aeronautical Data Chains may contribute to a collection of data or Integrated Aeronautical Information Package (IAIP) that is used by an end user.

Each link in the Aeronautical Data Chain provides a function which facilitates the origination, transmission or use of aeronautical data for a specific purpose.

The Upstream Data Chain[3] includes the following functions:

- **Data origination** – origination of raw data (surveyed) and derived data (e.g. procedure design data).
- **Data transmission** – whereby data is moved from one physical location to another. It is performed by all chain participants in a variety of ways (e.g. electronically or paper).
- **Data publication** – whereby aeronautical data are collected prepared and issued into the public domain by the AIS of each Contracting State.
- **Data distribution** – this involves the delivery of the formatted data sub-set to users using various delivery media. The full distribution network involves many actors.

The Downstream Data Chain[4] includes the following functions:

- **Data application / integration** – whereby data, in an application specific configuration and format, is made available to the target application (e.g. filing a chart in a manual or processing data for FMS, for use in flight).
- **Data end-use** – a functional link for accessing and acting upon the output of an application. Aeronautical data end-users are typically aircraft operators, airline planning departments, air traffic service providers, flight simulation providers, airframe manufacturers, systems integrators and regulatory authorities.

Each of these functions is described in more detail in [9].

CHAIN covers the parts of the Upstream Data Chain for which States are responsible and encompasses the EUROCONTROL CHAIN Activity and Data Chain improvement activities of individual States although the latter remains the responsibility of States.

[3] Term used to refer to the Data Chain functions from the point of origination to the point of publication.
[4] Term used to refer to the Data Chain functions from Application/Integration to End-Use.

3.2 CHAIN Boundary and Scope

The boundary of CHAIN thus covers the upstream activities of the Data Chain, from (but not including) the point of origination through to the publication and distribution of the Integrated Aeronautical Information Package (IAIP) by States. Core functions of Data Origination (e.g. Surveying and Procedure Design) are outside the CHAIN boundary although the transfer of aeronautical information from Data Origination to Data Publication is within the scope of CHAIN. The regulation of the Upstream Data Chain (UDC) is also not within the scope of the CHAIN Activity; however, CHAIN seeks to identify regulation that would support the aims of CHAIN (see Figure 1). The diagram also shows the relationship with the Aeronautical Data Integrity (ADI) Mandate, which is currently under development, and will consider regulation issues (at a high level) as part of its development.

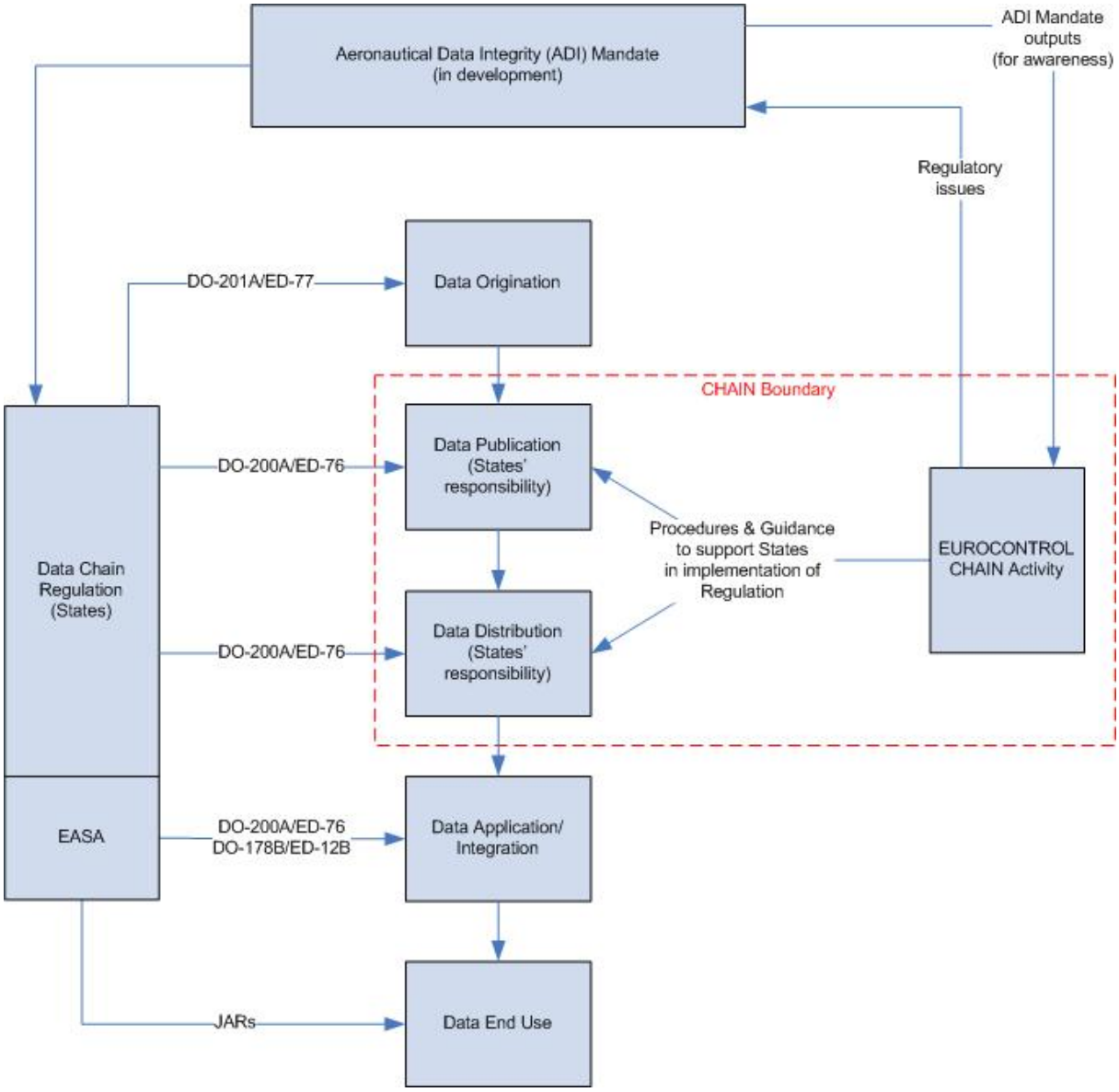


Figure 1: Data Chain Regulation and CHAIN Relationship Diagram

3.3 EUROCONTROL CHAIN Activity

CHAIN Activity is EUROCONTROL's component of CHAIN. It supports States by proposing and developing improvements to Data Chain.

A number of improvements proposed by the CHAIN Activity, which are currently under development, are as follows:

1. The development and distribution of process improvements and enhanced guidance material, related training and education covering the definition of:
    a. "Principles and Data Quality Management" providing the high level overview and describing the effective data management and quality management processes and procedures which must support a data process to ensure that the integrity and quality objectives of such a process are achieved;
    b. "Data Origination" setting out the minimum requirements for the origination navigation-related data applying to all organisations involved in the data origination process (created by NAV domain; integral part of awareness campaign and implementation support);
    c. "Data Publication" sets out the minimum requirements for the process involved in the provision of aeronautical data publication and applies to all organisations involved in the publication process for Aeronautical Information. The requirements cover the publication by traditional paper-based, methods as well as through use of electronic publication (e.g. eAIP);
    d. "Service Level Agreement (SLA) package" to support agreements between Originators, AIS Providers and Regulators;
    e. "Detailed data process mapping" for critical and essential data;
    f. "Standard Input Forms (SIF)" to assist data originators and AIS providers, in the absence of other means, to streamline the data capture and provision during an intermediate operation phase, until automated processes are implemented or developed by the States.";
    g. "Abbreviations and Definitions".
2. The "development of an automated Data Integrity process", to address and facilitate the automation of manual processes[5] - A problem for the Data Chain is when tasks are performed by multiple actors based on manual processes with the existence of numerous transaction points. At each of these points data may leave a semi-electronic or even a fully manual environment and are transferred in paper form rather than in electronic form, then re-entered in electronic form by the receiving actor. This is an error prone process. On the other hand, double and often triple entry of data is performed to reduce and detect errors.

[5] For example, the use of EUROCONTROL Data Quality Tool Set (DQTS) and the development and implementation of an 'automated process tool' based on the concept demonstrator called Data Integrity Tool (DIT).

3.4 Definition of CHAIN for the Safety Assessment

The FHA/PSSA activity was based on the scope and definition of CHAIN as described in section 3.2 of this report. The relationship between the scope and definition elements and the safety assessment activities is depicted in the diagram in Appendix D.

The definition and scope of CHAIN for the safety assessment has been captured in a series of models as described in sections 3.4.1 and 3.4.2 below along with a number assumptions captured in section 6.2.1.

3.4.1 UDC/CHAIN Functional Model

The functional links in the Data Chain are depicted in Figure 4 in Appendix B.1 and are described in more detail in [9].

The Data Chain should be viewed as a circular flow of information, with feedback loops – the end users of the data also feed back to determine the data that is needed at the origination stage. Each of the functional links in the chain may be performed by a single organisation, or distributed among various separate organisations. For example, a State could originate, prepare, and integrate aeronautical information for a specific application prior to end use.

3.4.2 UDC/CHAIN Logical Models

The Logical models for the Upstream Data Chain are shown in Appendix B.2. The models are drawn for:

- **Data Origination** presented in Figure 5. The Data Origination and its processes are outside the CHAIN Activity's boundary and the scope of the safety assessment activity, however the transfer of AI from Data Origination to Data Publication is within scope. For this reason the diagram was drawn to capture the transmission points where raw data is provided to Data Publication.
- **Data Publication** presented in Figure 6, Figure 7 and Figure 8. The Data Publication logical entities were drawn based on [18] and input provided by the FHA/PSSA workshop participants. The three diagrams capture two major logical tasks carried out by Data Publication, namely the Initial Check of Raw Data and Data Preparation. A detailed description of these two logical entities is provided in [9].
- **Data Distribution** presented in Figure 9. A detailed description of the model is provided in [9].

4. OVERALL SAFETY ARGUMENT

4.1 Objective

The objectives of this section are to:

- outline the current top-level safety argument for CHAIN;
- define any supporting context and justifications;
- explain the decomposition of the safety argument.

The overall safety argument structure is set out using Goal-structuring Notation (GSN) and is presented in Appendix H. Appendix I presents a guide to GSN.

The top-level safety argument is contained in Figure 2 below.

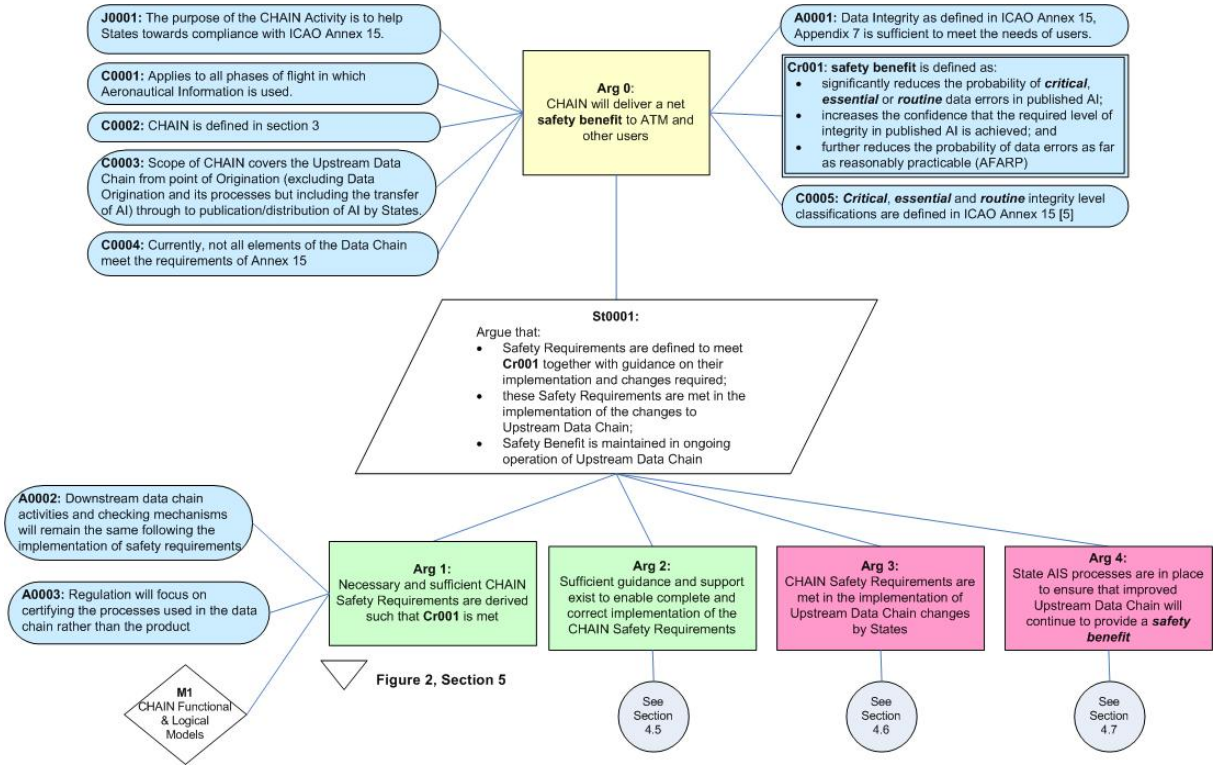


Figure 2: Overall Safety Argument

4.2 Principal Safety Argument

The purpose of the CHAIN Activity is to help States towards compliance with ICAO Annex 15 [5] (**J0001**), as currently not all elements of the Data Chain meet the requirements of ICAO Annex 15 (**C0004**). This assumes that ICAO Annex 15 and especially Appendix 7 is sufficient to meet the needs of users (**A0001**), in all phases of flight in which Aeronautical Data is used (**C0001**).

The Preliminary Safety Case makes the Claim (**Arg 0**) that CHAIN, as defined in section 3 (**C0002**), will deliver a net ***safety benefit*** to ATM and other users in terms of the contribution from the Upstream Data Chain as scoped by CHAIN (**C0003**).

4.3 Safety Criteria

In general, a ***safety benefit*** is an improvement in the level of safety in the ATM domain (as opposed to, say, the AIS domain) and could be either explicit, ie a tangible reduction of one or more risks of an accident, or implicit, ie increased confidence that the required level of safety will be/has been achieved.

In the case of the Data Chain the safety benefit to ATM of any change can be defined in terms of the reduction in the probability of errors being present in AI or increased confidence in the integrity of this information. To achieve a risk reduction changes to the Data Chain must either reduce the probability of an error being introduced to the AI or increase the probability that errors will be found, or both.

Given Assumption **A0001** the safety criteria for the Data Chain should be to demonstrate compliance with ICAO Annex 15. However, there are many significant issues with achieving this compliance at present (as are explained later in section 5.4) and the process of improving the Data Chain is likely to be lengthy and evolutionary due to its size, complexity and the number of actors involved.

Hence the criteria **Cr001** for CHAIN are based on a relative approach[6] to determining that a ***safety benefit*** is realised, i.e.:

- the probability of critical, essential (or routine) data errors in published AI is significantly reduced (where critical, essential and routine data are defined in ICAO Annex 15 [5] (**C0005**));
- the confidence that the required level of integrity in published AI is achieved is increased; and
- the probability of data errors is further reduced As Far As Reasonably Practicable (AFARP), within the scope of CHAIN.

4.4 Decomposition of Arg 0

Evidence gathered during the previous CHAIN safety study [8] as well as the reported non-compliances in the supplement to ICAO Annex 15 [5], identifies that some actors of the current Data Chain do not meet all of the requirements of ICAO Annex 15 (**C0004**) and thus any improvement to the current Data Chain that brings about compliance or reduces the gap would provide a ***safety benefit***[7].

Therefore the strategy for decomposing **Arg 0** is to argue that Safety Requirements and implementation guidance have been specified for CHAIN, which will be satisfied such that a ***safety benefit*** is realised, and processes are in place to ensure that the Safety Requirements continue to be satisfied in operation.

[6] The SCDM [2] provides an explanation of a relative approach to risk assessment.
[7] Note that changes to the Data Chain do not need to provide a ***safety benefit*** where the main purpose of the change is to provide an operational benefit such as improved efficiency. In this case it would still be of benefit if the change could reduce the risk as far as reasonably practicable.

This strategy is reflected in **Arg 1** to **Arg 4** in Figure 2. Note that it is assumed (**A003**) that regulation of Data Chain actors and their activities will focus on the assurance of processes followed rather than the review and approval of Aeronautical Data and thus providing a safety benefit in relation to the second criterion (**Cr001**) only.

One issue identified during the safety assessment related to the continued efficacy of Downstream Data Chain activities when Upstream Data Integrity is improved. Given that Data Application /Integration is outside the scope of CHAIN, it was assumed that the Downstream Data Chain activities and checking mechanisms will remain the same following improvements to the Upstream Data Chain (**A0002**).

Since **Arg 1** is the main argument to be addressed in this Safety Case it is addressed in section 5; **Arg 2** to **Arg 4** are addressed in subsections 4.5 to 4.7 below.

4.5 Guidance for Implementation of the CHAIN Safety Requirements (Arg 2)

There is currently no specific evidence to support this argument; this is captured as **Safety Issue 1** in section 6.2.2.

Guidance material will need to be developed by EUROCONTROL, in support of the CHAIN Safety Requirements, to assist the States in implementing them.

The guidance should include, but not be limited to:

- safe application of specific CHAIN improvements such as specifications, procedures and process definitions and Standard Input Forms – this will require further specific safety assessment of these improvements;
- general guidance on the implementation of the CHAIN Safety Requirements for specific State improvements;
- recommendations for carrying out State specific FHA/PSSA/SSA activities using the CHAIN FHA/PSSA as a basis to identify issues, assess the risk from introducing the new changes, decompose **Arg 3** and derive any additional safety requirements. The functional, logical and bow-tie models can be used to assess new changes;
- recommendations for using this report as a template for States to develop their Preliminary Safety Cases to provide the argument and evidence that the new changes to the Data Chain will realise a safety benefit;
- recommendations as to the use of this report to States, identifying the need for States to provide the evidence for the satisfaction of **Arg 3** (discussed in section 4.6). The EUROCONTROL Safety Case Development Manual [2] should be used by States as a guide to provide the argument and evidence for satisfying **Arg 3**.

4.6 CHAIN Safety Requirements are met by States' Implementation of Changes (Arg 3)

A fundamental part of satisfying the safety argument presented in Figure 2 is for States to demonstrate that the CHAIN Safety Requirements are met in the

implementation of Upstream Data Chain changes by States. Generic guidance on satisfying this argument needs to be developed by CHAIN as detailed in the previous section (4.6).

Development of specific arguments and evidence to support **Arg 3** is the responsibility of the States and therefore substantiation of **Arg 3** is outside the scope of this Preliminary Safety Case.

4.7 CHAIN Safety Requirements continue to be met in Operation (Arg 4)

Ongoing safety monitoring and improvement will need to be considered by the States in the implementation of the CHAIN Safety Requirements to ensure that a safety benefit continues to be achieved. Therefore substantiation of **Arg 4** is outside the scope of this Preliminary Safety Case.

The safety assessment (specifically the consequence analysis) identified that it is possible that, as the level of confidence in the integrity of AI supplied by the Upstream Data Chain increases, the level of checking in the Downstream Data Chain may decrease (captured as **A0002** – see section 4.4). This situation should be monitored as part of any ongoing monitoring of the Data Chain (see **Safety Issue 2**, section 6.2.2).

5. DERIVATION OF CHAIN SAFETY REQUIREMENTS

5.1 Objective

The objective of this section is to show that a necessary and sufficient set of Safety Requirements for CHAIN has been defined such that Criterion **Cr001** will be met by the CHAIN Activity – i.e. **Arg 1** has been satisfied and:

- significantly reduces the probability of critical, essential (or routine) data errors;
- increases the confidence that the required level of integrity in published AI is achieved; and
- further reduces the probability of data errors As Far As Reasonably Practicable (AFARP).

5.2 Strategy

The above objective is achieved through the decomposition of **Arg 1** presented in Figure 3 below.

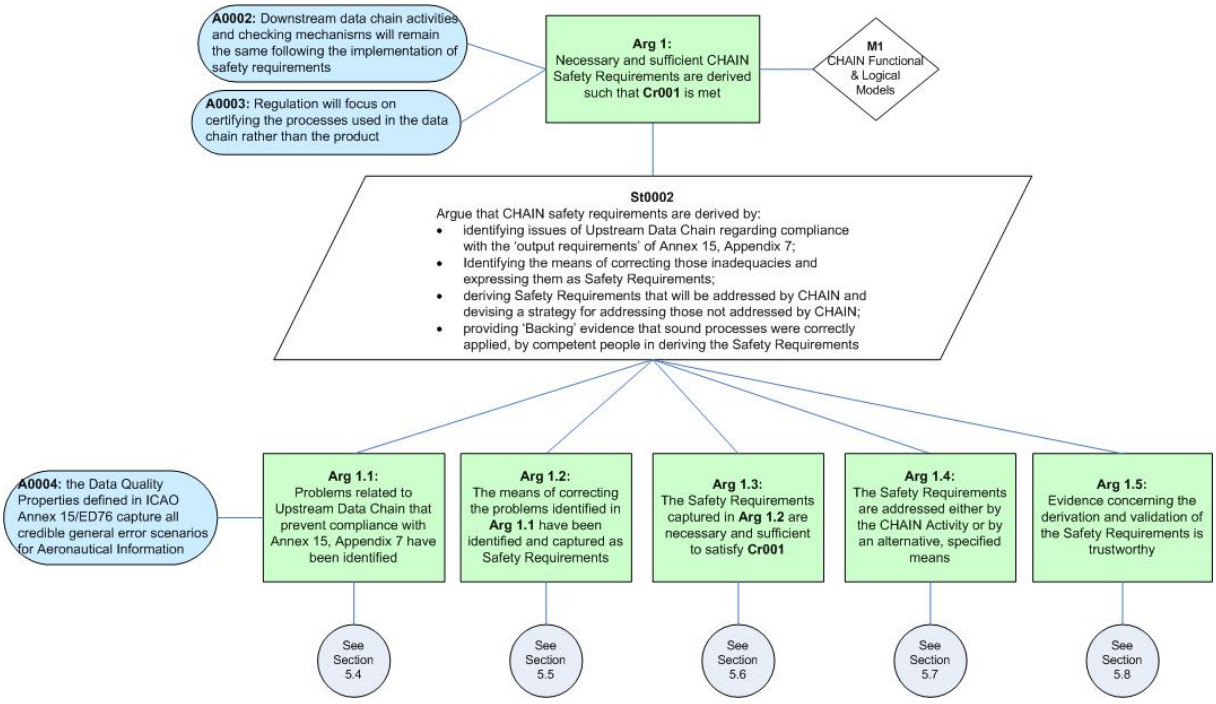


Figure 3: Necessary and Sufficient CHAIN Safety Requirements are Derived

5.3 Rationale for Arg 1

For CHAIN to deliver a net safety benefit it must identify a set of safety requirements that satisfy the safety criteria **Cr001** (**Arg 1.3**), which are then implemented by the States. However, stakeholder research, initial assessments for CHAIN [8] and the CHAIN FHA/PSSA workshop [12] made clear that there are several significant

issues currently facing the AIS community that prevent or undermine the AIS providers' compliance with the data integrity requirements of ICAO Annex 15.

To fully understand those issues in relation to the safety of data, the argument for CHAIN is based on performing an independent safety assessment of the current Data Chain hazards (FHA) and related causes (PSSA) to establish a baseline set of safety requirements for the current Upstream Data Chain (or UDC SRs). The assessment was performed using a set of validated functional and logical models for CHAIN (**M1**) which was developed based on the assumption that regulation of the Data Chain will focus on the certification of organisations and their processes rather than the certification of data products (**A0003**).

The UDC SRs were derived based on the assumption that the Data Quality property definitions in Annex 15 (see Appendix A) are necessarily and sufficiently complete to identify all credible data hazards (**A0004**). These requirements were then compared to the extant Data Chain requirements (as documented in ICAO Annex 15 and ED-76) to both identify gaps in those requirements and trace to the known problems in relation to satisfaction of the extant requirements (**Arg 1.1**).

CHAIN addresses these issues and gaps by identifying the means to resolve them, capturing the means as CHAIN Safety Requirements (or CHAIN SRs see **Arg 1.2**) and identifying those who should take action to address the CHAIN Safety Requirements. The CHAIN Activity intends to provide a series of guidelines, procedures and specifications that will support AIS providers in meeting the CHAIN Safety Requirements and thus improving their level of compliance with Annex 15.

Whilst the CHAIN Activity is not scoped to resolve all of the identified issues and gaps, achieving the ***safety benefit*** in **Cr001** will be as a result of addressing the issues within the scope of CHAIN and identifying the issues outside the scope of CHAIN (**Arg 1.4**)[8] to those responsible for their implementation (mainly AIS regulators).

The evidence in support of **Arg 1.1** to **1.4** is shown to be trustworthy in **Arg 1.5** by showing that the Safety Requirements were derived from the application by competent people of an ESARR 4 compliant process, based on the EUROCONTROL Safety Assessment Methodology [1].

5.4 Identification of Problems with Current Upstream Data Chain (Arg 1.1)

Problems related to current Upstream Data Chain that prevent compliance with Annex 15 have been identified as follows:

1. Comparing the results of an independent assessment of the Upstream Data Chain Safety Requirements with the extant Data Chain requirements and specifications contained in ICAO Annex 15 [5] and ED-76 [6].

   The independent safety assessment of the current Upstream Data Chain is described in Appendix C and was used to develop the UDC SRs. The UDC SRs are captured at three levels, which correspond[9] to:

[8] Identifying issues outside the scope of CHAIN Activity helps satisfy the safety criteria for reducing risks AFARP.
[9] Levels 1 and 2 also correspond approximately with the specification detail in Annex 15 and ED-76, although there is some cross-over.

- Level 1 – safety requirements at the boundary of CHAIN;
- Level 2 – safety requirements at the boundary of the major actors/logical processes within the Data Chain;
- Level 3 – safety requirements for the logical entities of the Data Chain as depicted in the logical models described in section 3.3.

The UDC SRs are captured in Appendix F by the first three columns of Table 3 (section F.1) for Level 1, Table 4, Table 5, and Table 6 (section F.2) for Level 2 and Table 7 (section F.3) for Level 3.

The results of the comparison with ICAO Annex 15 and ED-76 to check completeness of these requirements and identify any gaps that may exist within the standards themselves are captured by the column named "Existing Specification/Gap".

2. Capturing issues that the current Upstream Data Chain is facing including compliance issues with ICAO Annex 15. These problems were identified from a number of sources:
   - work carried out in the Preliminary Safety Impact Study [8] (a detailed list of all issues identified by the study can be found in Appendix E of the Preliminary Safety Impact Study Report [8]);
   - the CHAIN FHA/PSSA workshop [12], the logical diagrams in Appendix B.2 were annotated (as captured) and used by the FHA/PSSA participants to identify those parts of the process which are inconsistently applied across States or are not currently mandatory;
   - reported non-compliances in the supplement to ICAO Annex 15;

   A list of all identified problems and issues can be found in Appendix E.
3. Allocating known issues and problems (identified as described by step 2 above) to the identified UDC SRs as appropriate.

   The results of this allocation are captured by the column named "Implications/Known Issues" of Table 3, Table 4, Table 5, and Table 6 in Appendix F.

Whilst the identification of problems is comprehensive it cannot be considered to be exhaustive. Also, some of the problems need further research; for example, one of the most significant issues identified is the application and demonstration of the achievement of the data integrity levels stated in Annex 15 Appendix 7 (**Recommendation 1**). The resolution of this issue will either need further apportionment of numerical integrity within the Data Chain processes or identification of Assurance requirements for those processes dependent on the assigned data integrity levels. These issues do not prevent CHAIN from achieving its safety criteria[10] nor do they prevent the identification and capture of further problems as the CHAIN Activity continues. As such it is considered that the evidence satisfies the intent of **Arg 1.1** for this stage of the CHAIN Activity. However, it is recommended that a mechanism for capturing further problems is identified and implemented as part of CHAIN (see **Recommendation 2** in section 6.3).

[10] Only the extent to which it is achieved, eg how much risk reduction is achieved in the overall context of the Data Chain.

5.5 CHAIN Safety Requirements (Arg 1.2)

The identified problems and gaps with the satisfaction of Annex 15 / ED-76 were assessed for possible means of addressing them such that the safety criteria could be met either by:

- reducing the probability that data errors could be introduced;
- increasing the probability that data errors could be detected, or
- increasing the confidence in the integrity of Data Chain processes.

The means to correct each of the issues are captured by the column named “Means to Correct” of Table 3, Table 4, Table 5, and Table 6 in Appendix F. Note that the means to correct are generally identified at a level commensurate with the logical definition of the Data Chain to avoid being prescriptive about the implementation of any particular solution to address the issue or gap. The means to correct are given a unique identifier ‘Mxxx’ and may appear several times in the table where issues are common to more than one actor or more than one process.

The CHAIN Safety Requirements (CHAIN SRs) are presented in Appendix G and are derived directly from the “Means to Correct” derived as discussed above. As some of the CHAIN Safety Requirements relate to general issues such as the specification of automated tools, they are also traced to all related Level 3 UDC SRs, i.e. all the Level 3 UDC SRs that trace to the Level 1 or Level 2 “Means to Correct” from which the CHAIN safety requirement is derived.

The CHAIN SRs will need to be further developed for each proposed CHAIN improvement to ensure that the change specification captures all of the specific safety requirements to ensure that the CHAIN SRs are addressed. Thus to fully substantiate argument **Arg 1.2** it will be necessary to rationalise and/or further decompose the CHAIN SRs for each specific CHAIN improvement as and when they are specified. This is captured as **Safety Issue 3,** and **Safety Issue 4** for the changes that the CHAIN Activity currently proposes, namely the Process improvements and enhanced guidance material, related training and education and the automation of manual transfer as discussed in section 3.3.

These issues will remain open until such time as all CHAIN improvements specified by the CHAIN Activity have been addressed.

5.6 CHAIN Safety Requirements are Necessary and Sufficient to satisfy Cr001 (Arg 1.3)

To show that CHAIN will deliver a net safety benefit it is necessary to show that the CHAIN SRs address the safety criteria. This is achieved as follows:

- significantly reduce the probability of critical, essential (or routine) data errors in published AI;

  The CHAIN SRs that address this are identified by the acronym “RR” (for Risk Reduction) in the column name as “RR / IC” (Increased Confidence) in Table 8 of Appendix G. In each case the SR states qualitatively the need for the reduction in error generation/increase in error detection unless a quantitative improvement was identified as part of the FHA/PSSA workshop.

- increase the confidence that the required level of integrity in published AI is achieved;

  The CHAIN SRs that address this are identified by the acronym “IC” (for Increase Confidence) in the column name as “RR/IC” in Table 8 of Appendix G. In each case the SR captures what needs to be changed or addressed within the current Data Chain quality, management or regulatory processes, on the assumption that the regulatory approach will focus on certifying the processes used in the Data Chain rather than the product (see A0003, section 6.2.1).

- further reduce the probability of data errors as far as reasonably practicable (AFARP)

  This is addressed by identifying SRs for the Data Chain that falls within the boundary of CHAIN without restricting the safety assessment to just those issues that fall within the scope of the CHAIN Activity to address. The assignment of SRs is described in section 5.7.

Although there are issues with the completeness of problem identification the safety criteria for CHAIN is set such that it does not rely on this. In reality both CHAIN and States will continue to work together towards implementing an ever safer Data Chain until such time as Annex 15 and the needs of the Data User are shown to be met in full. However, this argument cannot be substantiated until the issues with the level of detail for some of the CHAIN SRs (see Safety Issue 3, and Safety Issue 4 raised in section 5.5) are resolved.

5.7 Safety Requirements are addressed by CHAIN or Others (Arg 1.4)

Each of the CHAIN SRs has been allocated an owner based on whether the requirement can be addressed entirely by the CHAIN Activity or is solely the responsibility of the States (either AIS or the regulators). The results of this process are captured in column “Owner” of Table 8 in Appendix G.

This argument is substantiated as far as possible for this stage of the CHAIN Activity, although the evidence will need to be updated to keep track of any new CHAIN SRs needed to fully satisfy **Arg 1.2** and **Arg 1.3**. It is recommended that all of the CHAIN SRs not allocated to CHAIN Activity in Table 8 of Appendix G are considered and addressed by the Aeronautical Data Integrity Mandate (see **Recommendation 3** in section 6.3).

5.8 Safety Requirements Derivation Process is Trustworthy (Arg 1.5)

The generic material provided in the FHA/PSSA was developed to support a safety assessment approach based on the EUROCONTROL Safety Assessment Methodology (SAM) [1] to facilitate compliance with ESARR 4. Specific Safety Requirements for CHAIN deliverables will need to be derived from an ESARR 4 [3] compliant relative safety assessment - i.e. using a qualitative comparison of the risk before and after the introduction of potential improvements to the Upstream Data Chain, SAM should be used as a guide to providing an acceptable means of compliance with ESARR 4. See section 4.5 for further discussion on the guidance material.

This safety assessment was undertaken independently from EUROCONTROL by individuals experienced in the field of safety engineering with extensive knowledge in the application of the EUROCONTROL Safety Assessment Methodology and ESARR4 to ATM and AIS domain systems including the European AIS Database.

Fundamental to validating the assumptions and models constructed for the safety assessment process was to obtain ‘buy-in’ from identified stakeholders at an appropriate forum. All the models were therefore presented for validation at an FHA/PSSA Workshop [11] held at EUROCONTROL Headquarters on 31 August to 1 September 2005. The Workshop was also used to identify an initial set of hazards along with associated causes and consequences for the current Upstream Data Chain (as scoped by CHAIN). The models presented in Appendix B incorporate all comments received both during and following the workshop.

The models were then used as input into the FHA/PSSA activity, which derived the safety requirements for CHAIN. The relationship between the scope definition elements and the safety assessment is depicted in the diagram in Appendix C.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Summary

This Preliminary Safety Case describes the safety argument, summarises the available supporting evidence and identifies shortfalls in the satisfaction of the overall Claim that CHAIN will deliver a net safety benefit for ATM and other Users. A number of Caveats to this Claim are identified in section 6.2 below. The Claim is founded on the following four principal Safety Arguments as applicable to the scope of the CHAIN activity.

1. Safety Requirements are defined to ensure the safety benefit is achieved – **Arg 1**.
2. Guidance is provided on their implementation and the changes required – **Arg 2**.
3. States show that the Safety Requirements are met in the implementation of the changes to the Upstream Data Chain – **Arg 3**.
4. Safety monitoring is in place to ensure that the safety benefit is maintained in the ongoing operation of Upstream Data Chain – **Arg 4**.

This Safety Case focuses on the evidence for the **Arg 1** and **Arg 2** and thus the conclusions are subject to full satisfaction of **Arg 3** and **Arg 4** by individual States who implement CHAIN improvements. However, based on the evidence that is currently available and considering the number of shortfalls (i.e. open safety issues), it is concluded that the first two arguments are not yet fully substantiated.

The proposed CHAIN improvements to the Upstream Data Chain are under development. As such, the Preliminary Safety Case should be revisited and updated throughout the CHAIN Activity to provide the evidence to support the claims of this Preliminary Safety Case.

The resolution of a number of the identified CHAIN SRs falls outside of the CHAIN Activity yet their satisfaction is very important to ensuring that Data Integrity is fully and holistically addressed. As such a number of recommendations (see section 6.3) are made but they do not affect the specific conclusions of the CHAIN Preliminary Safety Case.

6.2 Caveats

The above conclusions concerning CHAIN are subject to the following Assumptions, Limitations and Resolution of the outstanding Safety Issues.

6.2.1 Assumptions

The following table lists the assumptions that have been made during the construction of this Preliminary Safety Case and their associated validation statements.

ID	Description	Source	Validation
A0001	Data Integrity as defined in ICAO Annex 15, Appendix 7 is sufficient to meet the needs of users	CHAIN Preliminary Safety Case, section 4.2	ICAO Annex 15 is the de facto standard for AIS provision world-wide. Note, however, that an amendment has been tabled by EUROCONTROL and there is a revised assignment table provided by ED-77 [7].
A0002	Downstream Data Chain activities and checking mechanisms will remain the same following implementation of safety requirements	CHAIN Preliminary Safety Case, section 5.3	The experts participating at the FHA/PSSA Workshop [12], which included representatives of the Downstream Data Chain and the assessment carried out in the workshop confirmed that this assumption is valid for now. However, monitoring of the continued efficacy of Downstream Data Chain activities when data integrity delivered by Upstream Data Chain is improved should be part of the ongoing validation of this assumption – see discussion of Safety Issue 2 in section 4.7.
A0003	Regulation will focus on certifying the processes used in the Data Chain rather than the product[11]	CHAIN Preliminary Safety Case, Section 5.3	This is the current intention of the ADI Regulatory Approach [17] but will need to be confirmed once the Implementing Rule is complete (Safety Issue 5, section 6.2.2)
A0004	The Data Quality Properties defined in ICAO Annex 15 [5] and ED-76 [6] capture all credible general error scenarios for Aeronautical Information	CHAIN Preliminary Safety Case, Section 5.3	The experts participating at the FHA/PSSA Workshop [12] and the assessment carried out in the workshop confirmed that the data quality properties as defined in ICAO Annex 15 are sufficient for the purposes for which the aeronautical data will be used.

Table 1 – Assumptions made in Preliminary Safety Case

6.2.2 Safety Issues

The following Open Safety Issues were identified during the safety analysis activity. These Issues must be resolved, or the means of resolving them identified, before the Final Safety Case is issued.

[11] It is anticipated that regulation will focus on the certification of organisations and their processes for data preparation, rather than the certification of Data products.

Ref	Issue	Resolution	Status
1	No guidance material has been developed to support States– see section 4.5	CHAIN Activity to develop guidance material in support of the CHAIN Safety Requirements to assist States in implementing them.	**In progress**
2	Safety assessment identified that it is possible, as the level of confidence in the integrity of AI supplied by the Upstream Data Chain increases, the level of checking in the Downstream Data Chain may decrease as confidence in the reliability of AI increases. Although this has been captured as an assumption (see A0002, section 6.2.1) for this safety case, it will be necessary to ensure for future changes that the level of checking remains commensurate with the degree of integrity in the data supplied by the Upstream Data Chain – see section 4.7.	CHAIN Activity and States to monitor the continued efficacy of Downstream Data Chain activities when data integrity delivered by Upstream Data Chain is improved.	**Open**
3	CHAIN SRs assigned to CHAIN and the related Level 3 UDC SRs are not traced and rationalised with the 'automated process Specification' to ensure Safety Requirements are addressed – see section 5.5.	CHAIN Activity to trace and rationalise the CHAIN SRs and the related Level 3 UDC SRs with the specification to ensure that safety requirements are addressed.	**Open**
4	CHAIN SRs assigned to CHAIN and the related Level 3 UDC SRs are not traced and rationalised with the Procedures and Guidance Material to ensure Safety Requirements are addressed – see section 5.5.	CHAIN Activity to rationalise the CHAIN SRs and the related Level 3 UDC SRs with the Procedures and Guidance Material to ensure that safety requirements are addressed.	**Open**
5	It is not confirmed that Regulation will focus on certifying the processes of organisations rather than the data products – see A0003 in sections 5.3 and 6.2.1.	ADI Regulatory Approach to confirm its intention regarding certification of data processes versus data products.	**Open**

Table 2: Open Safety Issues

6.3 Recommendations

Based on the contents of this safety case the following recommendations have been made.

1. ADI Regulatory Approach should consider further apportionment of numerical integrity within the Data Chain processes or identification of assurance requirements for those processes dependent on the assigned

data integrity levels to resolve the issue of application and demonstration of the achievement of the data integrity levels as stated in ICAO Annex 15 Appendix 7 – see section 5.4.

2. CHAIN should identify and implement a mechanism for capturing further issues and problems with the Data Chain – see section 5.4.
3. All CHAIN Safety Requirements not allocated to CHAIN Activity (see Table 8 of Appendix G) should be considered and addressed by the ADI Mandate.

APPENDIX A DEFINITION OF DATA QUALITY PROPERTIES

The quality of data is defined by its ability to satisfy the requirements for its safe application in the end system. The quality of aeronautical information and the way that it is processed is characterized by the following (based on ICAO Annex 15 and EUROCAE ED-76/RTCA DO200A 'Standards for Processing Aeronautical Data') [6]:

- **Accuracy**; is the degree of conformity of a measured or calculated quantity to its actual, nominal, or some other reference, value. **Confidence level** in the accuracy is the probability that any single location in the data set is in error of the true position by less than the stated accuracy.

  The required accuracy of a particular data element should be based upon its intended use. Accuracy is usually specified for data elements that are derived from measured values, and are not specified for data elements which have a defined value. For example, the location of a VOR and the height of an obstacle are measured and should have an associated accuracy requirement. The identifier associated with that VOR is defined, and does not have an accuracy requirement.

- **Resolution**; the required resolution of a particular data element should be based on its intended use. Resolution only applies to data elements that are derived from measured values, and does not apply to data elements that are defined. Since the resolution may also affect the accuracy of the data, it must be considered in relation to the accuracy requirement.

- **Integrity**; is the degree to which data is complete and free from errors in respect to other data quality properties, whether errors are introduced at source or subsequent processes in the Data Chain.

- **Traceability**; user requirements for traceability are typically stated in terms of the duration of time that specific data elements must be traceable. Data traceability should be retained as long as the data is in use.

- **Timeliness**; many data elements have an identified period for which the data is valid. The period of validity may be based upon an update period from the supplier or the underlying characteristics of the data itself. An example of an update period is the 28 day AIRAC cycle.

- **Completeness;** includes defining any requirements that define the minimum acceptable set of data to perform the intended function. One minimum set may be defined at time of equipment approval, while a larger set may be identified by the end-user.

- **Format**; the format of delivered data must be adequate to ensure that the data, when loaded into the end application, is interpreted in a manner that is consistent with the intent of the data. The format of the data will also define the transmission resolution of data

APPENDIX B DATA CHAIN FUNCTIONAL AND LOGICAL MODELS

B.1 Data Chain Functional Model

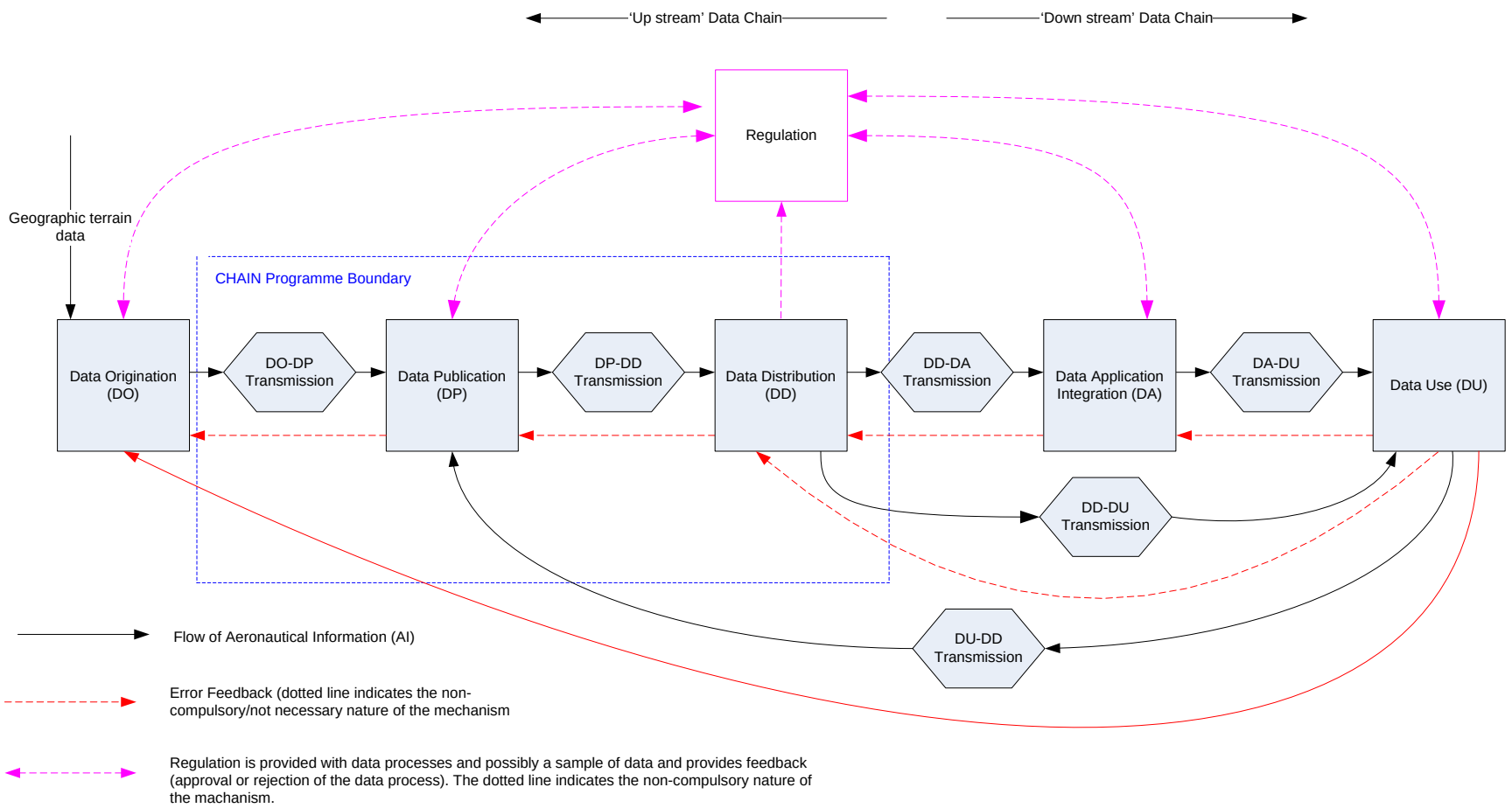
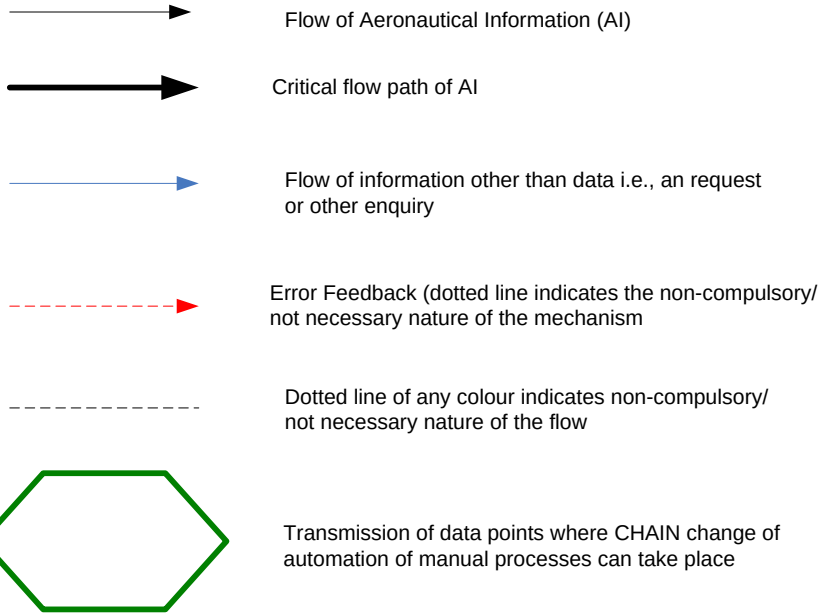


Figure 4: Data Chain Top Level Functional Model

B.2 UDC/CHAIN Logical Diagrams

The Key to diagrams in Figure 5 through to Figure 9 is presented below. Note that the green colour is used to highlight the areas in the current Upstream Data Chain that will be potentially affected by the change of automation of manual processes proposed by CHAIN



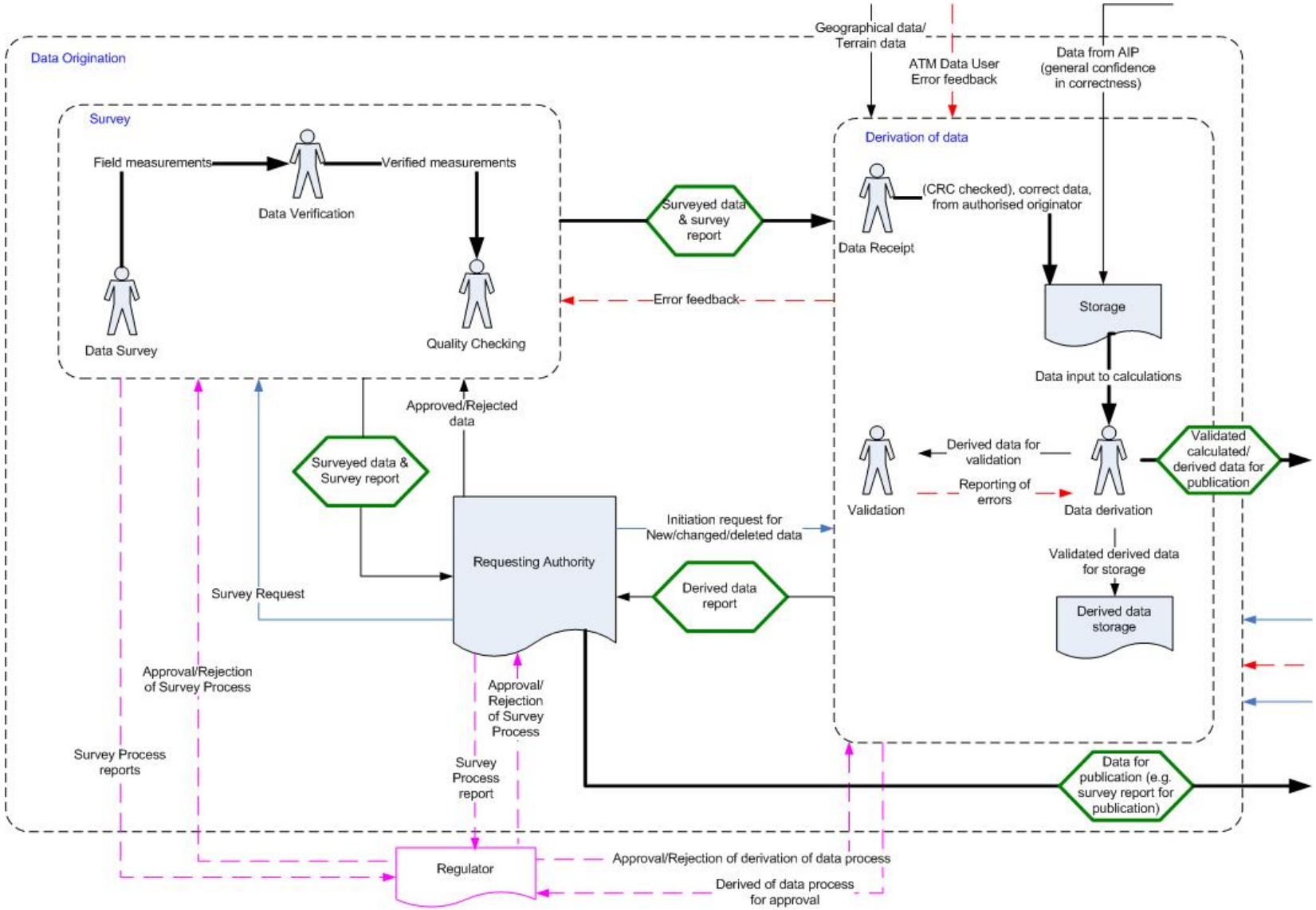


Figure 5: Upstream Data Chain Logical Model – Data Origination

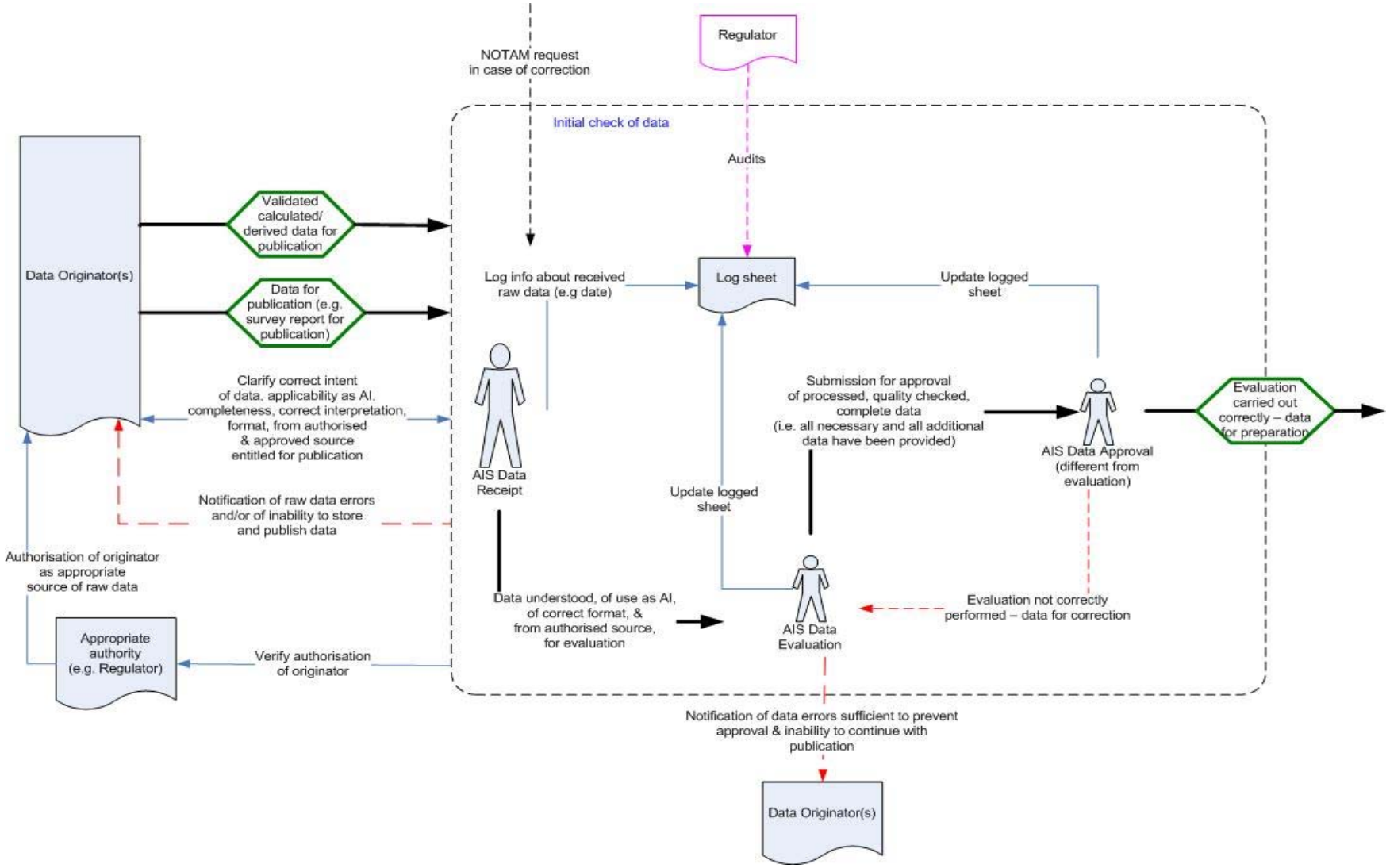


Figure 6 – Upstream Data Chain Logical Model – Initial Check of Raw Data

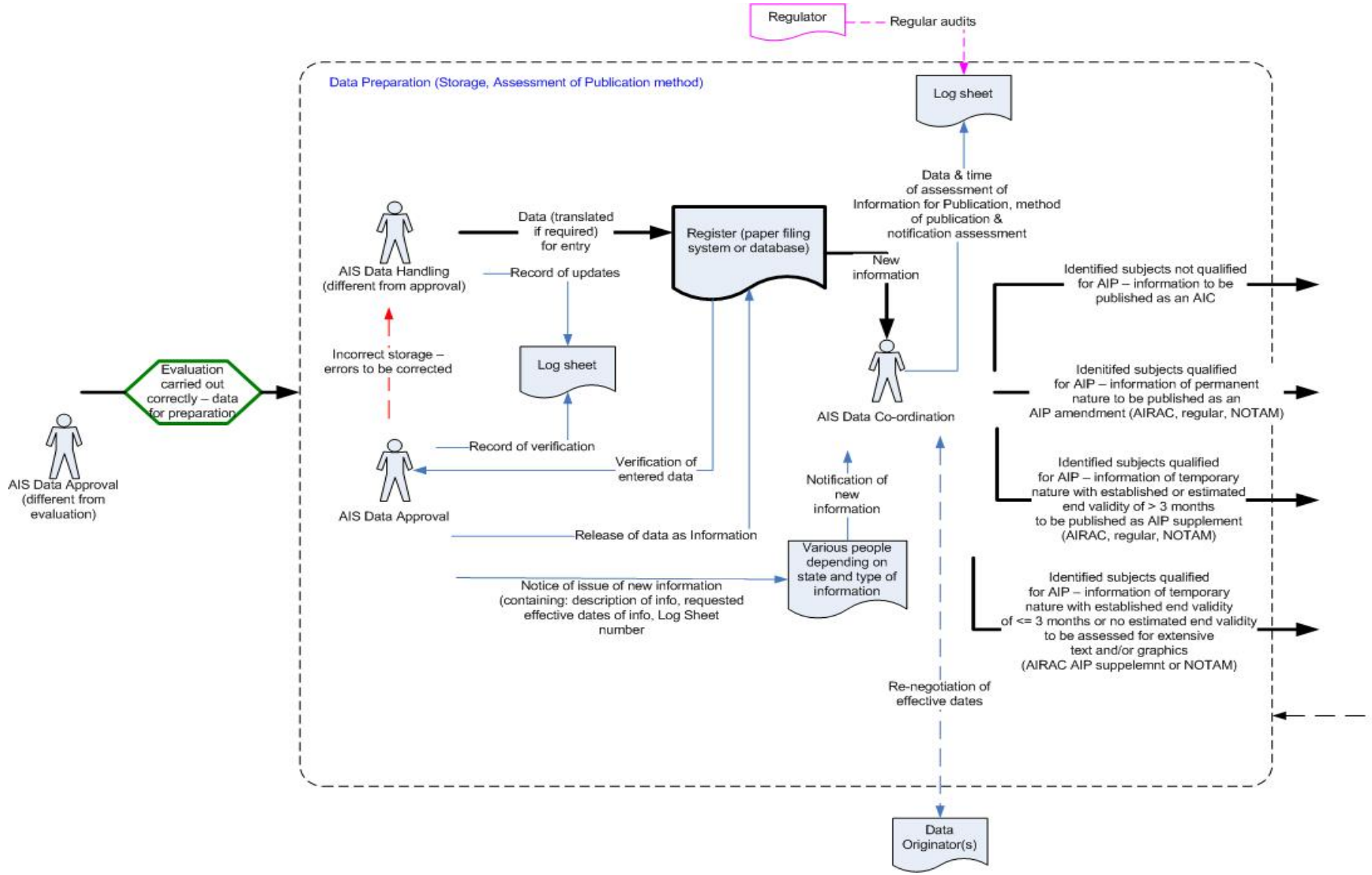


Figure 7 – Upstream Data Chain Model – Data Preparation

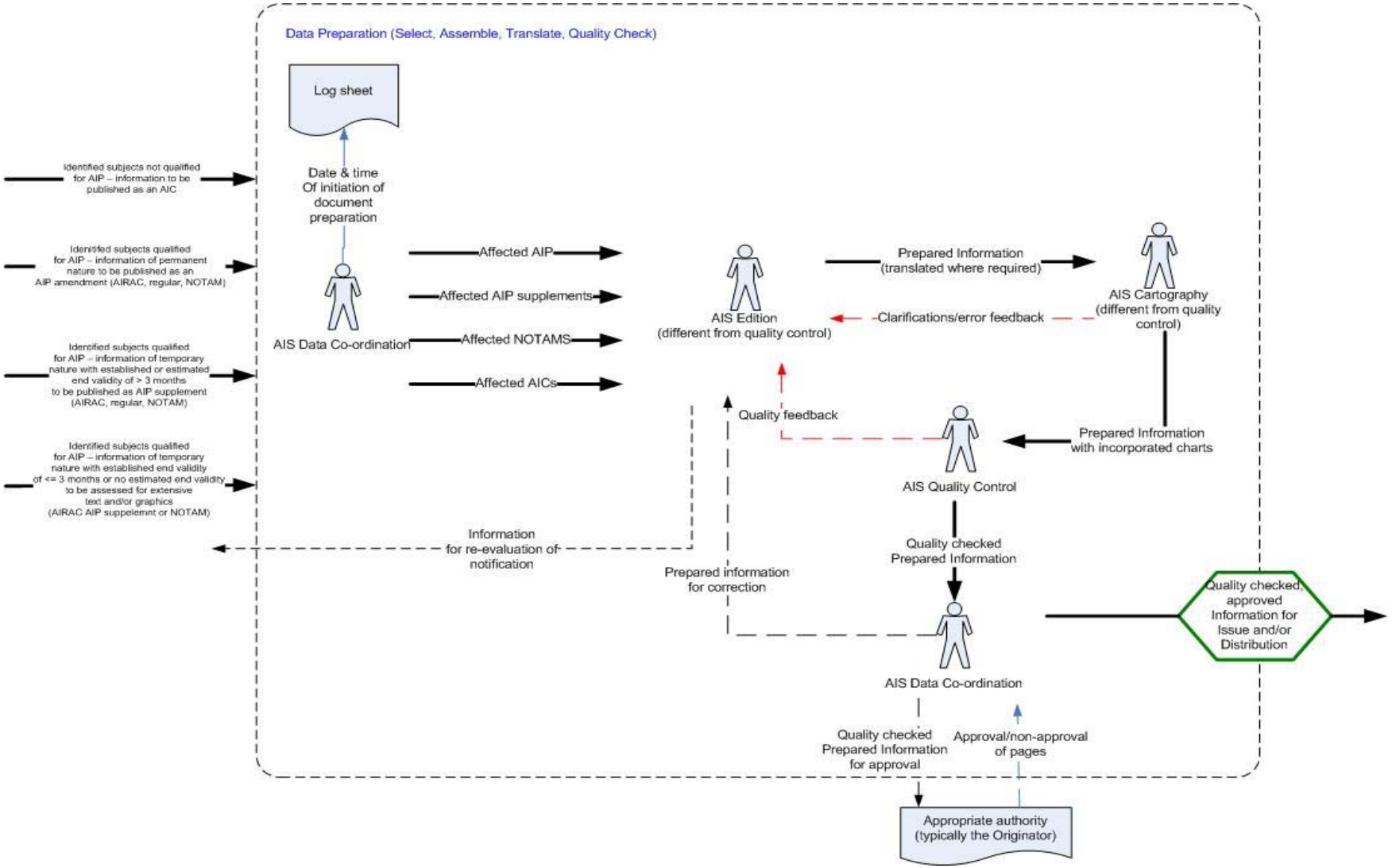


Figure 8 – Upstream Data Chain Logical Model – Data Preparation

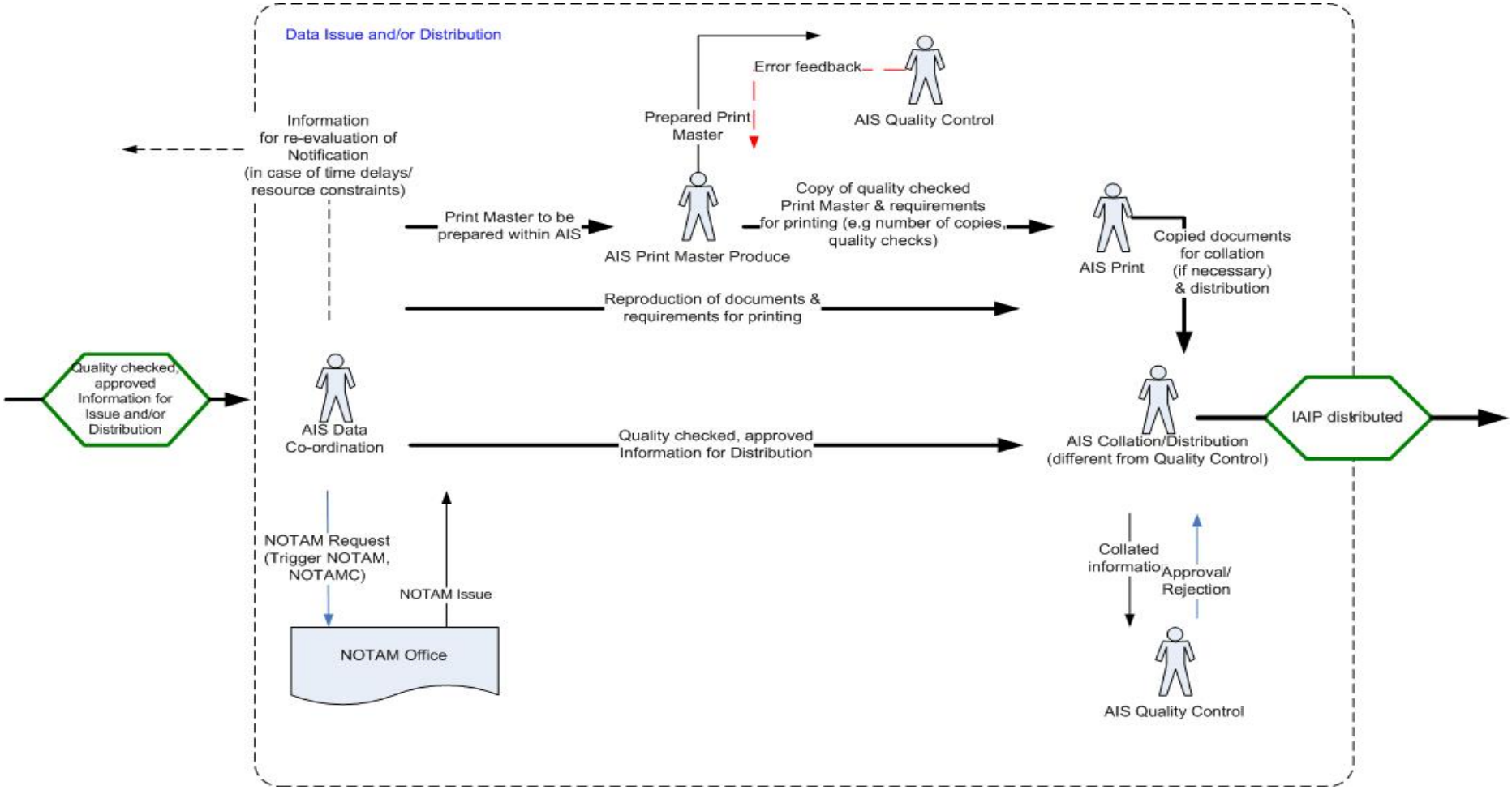


Figure 9 – Upstream Data Chain Logical Model – Data Issue and/or Distribution

APPENDIX C DETAILED EVIDENCE FOR ARG 1.1

C.1 Introduction

This section provides detailed evidence substantiating **Arg 1.1** discussed in section 5.4 of the main document.

Originally, the FHA aimed to identify the data hazards that could potentially lead to ATM or Airspace user hazards. However, this would have required an analysis of each data type and identification of all the potential errors for each data type that could lead to a hazard and the consequence across the entire ATM Domain. Such an analysis was not practicable within the scope of the CHAIN Activity. As such the FHA assumed that the Data Quality property definitions in Annex 15 were necessarily and sufficiently complete to identify data hazards (**A0004**).

The FHA/PSSA was performed using a defined and validated series of models, scoping statements and assumptions for the current Upstream Data Chain as scoped by CHAIN. Obtaining 'buy-in' from identified stakeholders at an appropriate forum was fundamental to validating the models, and was achieved by holding a workshop [12] to obtain feedback and generate discussions to support the safety assessment activity. The models were used as input into the FHA/PSSA activity.

The FHA/PSSA for the current Upstream Data Chain was undertaken to assess the current risk and thus derive a baseline set of appropriate Safety Requirements for the current Upstream Data Chain based on assurance that:

- necessary and sufficient identification of hazards as applicable to Aeronautical Information in the current Upstream Data Chain (within the bounds of CHAIN);
- assessment of the consequences of those hazards;
- assessment of the causes of those hazards developed to the level of detail commensurate with the scope and purpose of the safety assessment;
- the necessary risk mitigations to address the causes were identified;
- safety requirements are derived to achieve the risk mitigation.

The evidence in support of the above claims is described in sections C.2 to C.5. below.

C.2 Hazard Identification

The current Upstream Data Chain hazards were identified by examining potential failure scenarios associated with the functions of each major link in the Upstream Data Chain in the functional model and the Data Quality Properties. A series of functional failure guidewords was applied for each Upstream Data Chain function (working back along the data chain from the agreed CHAIN boundary), for each Data Quality Property as follows:

- Loss (partial/complete);

- Data Corruption;
- Inconsistency (with other Data Chain functions);
- Too early;
- Too late;
- Other (used as an open question as a completeness check).

The following hazards were identified for the current Upstream Data Chain (as scoped by CHAIN) and are defined in terms of the product of the Upstream Data Chain - ie IAIP:

- HAZ001 – Distributed IAIP contains valid but corrupt aeronautical data;-
- HAZ002 – Total Loss of Aeronautical Information;
- HAZ003 – Distributed IAIP is missing specific change(s) in Aeronautical Information (AI);
- HAZ004 – Inconsistent Aeronautical Information between actors of Downstream Data Chain.

C.3 Consequence Analysis

The consequence analysis in [9] showed that the introduction of improvements to Upstream Data Chain will not in itself affect the mitigations that are available in the Downstream Data Chain for any of the identified hazards; however, there is a concern that improvements in the Upstream Data Chain may be seen as a reason to reduce mitigations in the Downstream Data Chain in the future. This is captured as **A0002** and in section 4.2 and 6.2.1 of this Safety Case.

C.4 Causal Analysis

The causal analysis considered the causes of each identified hazard (as listed in section C.2 above) using the results of the FHA/PSSA workshop [12]. These causes were captured in a series of fault trees. The fault trees were based on a typical model for AIS as captured by the logical models of Appendix B.2, and thus the depth of the analysis stopped at the level of detail in the logical models[12].

The causal analysis showed how known issues and inconsistencies in the application of processes (identified as discussed in section 5.4) relate to each of the hazards. It thus highlighted the areas where reduction of risk may be required and enabled the allocation of issues to UDC SRs (also discussed in section 5.4).

C.5 Risk Assessment

The causal analysis showed that a ***safety benefit*** could be achieved by either:

Reducing the frequency of generated errors through:

[12] The models become less representative at the lower levels due to the specific logical variations in the processes between States.

- reducing the frequency of generated errors through:

automation of processes where possible, using qualified tools e.g. EAD;

more rigour in the definition of processes, manual or automated;

consistent application of the processes within an organisation and across States where required (independent of implementation).

- improving the error detecting processes through:

improving the effectiveness of the error detection (either the range of detectable errors or the probability of successful detection);

enforcement of the independence of the error detection process from the process potentially generating the error;

enforcement and clear definition of a feedback mechanism and resolution for the detected errors.

The role of the human operator and thus the significance of human error is evident from study of the logical models. The analysis confirmed that the Data Chain is susceptible to human errors, which can be introduced due to not following processes, lack of or insufficient training in performing the process, lack of or insufficient experience in the task provided (particularly in checking for errors), or unclear or undefined roles causing confusion and resulting in errors. Therefore, improvements can be made by:

- clear definition and assignment of roles;
- guidance on the application of processes and the importance of following them;
- ongoing competency assessment and training of AIS staff.

It should be noted that the size of reduction in risk of error achieved by any one change to the process is dependent on what parts of the FTA the change will affect. The most effective would be:

- reducing errors during transmission of data;
- improving the range of errors detected by, or rigour of, error checking processes;
- reducing the number of generated data errors that are more difficult to detect.

C.6 Upstream Data Chain Safety Requirements Definition

The Safety Requirements for the current Upstream Data Chain were derived from the risk assessment (described in section C.5 above) and are captured at three levels:

- Level 1 Requirements are set at the CHAIN boundary of the Upstream Data Chain and relate to the hazards and the functions depicted in the functional model of Figure 4 within Appendix B.1.

  The Level 1 Requirements are presented in Table 3 in Appendix F, section F.1.

- Level 2 Requirements relate to the logical entities of Data Origination, Initial Check of Raw Data, Data Preparation, and Data Distribution depicted in the logical models of Figure 5 to Figure 9 in Appendix B.2.

  The Level 2 Requirements are presented in Table 4, Table 5, and Table 6 in Appendix F, section F.2.

- Level 3 Requirements relate to processes described within each logical entity in the logical models. The sources of these requirements are visible within the fault trees in the FHA/PSSA Report [9] as base events.

  The Level 3 Requirements and the base events associated with each Level 3 Requirement are presented in Table 7 in Appendix F.3.

APPENDIX D FHA/PSSA RELATIONSHIP DIAGRAM

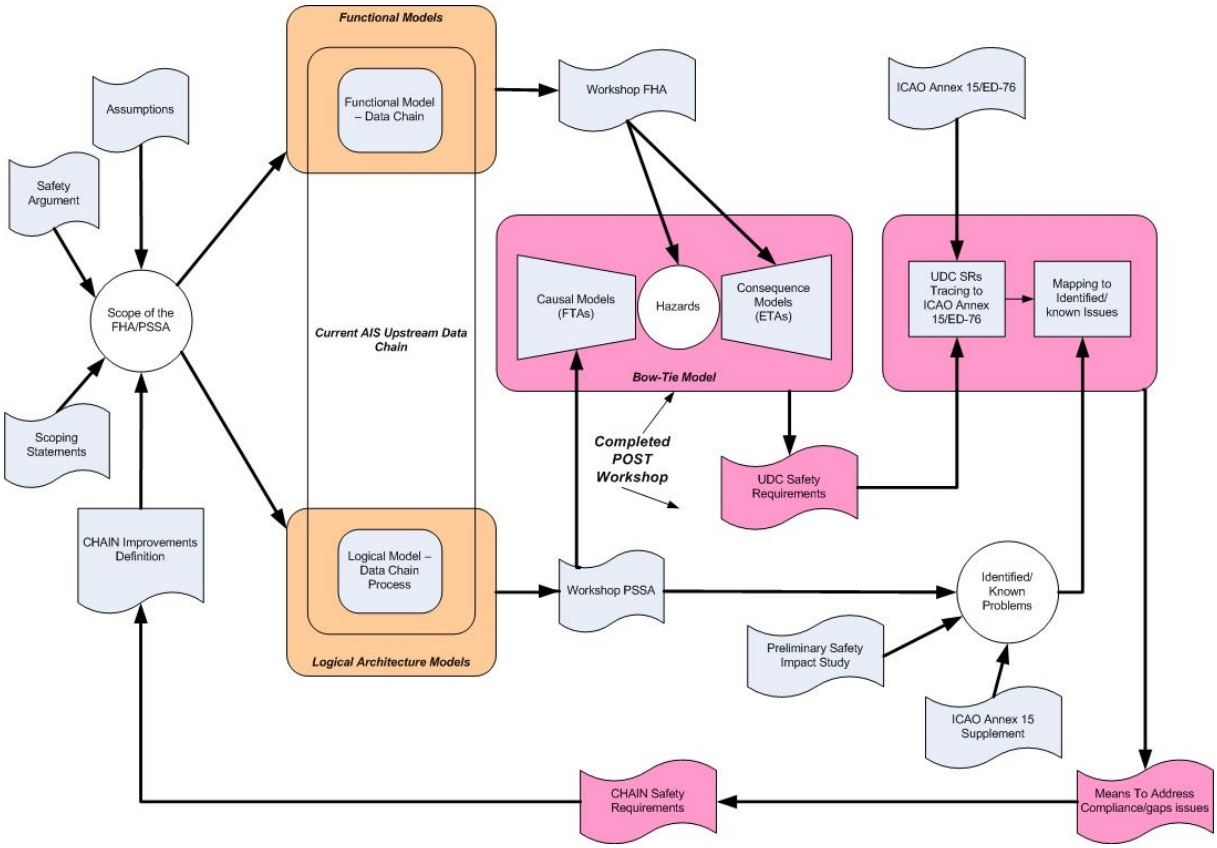


Figure 10: FHA/PSSA Relationship Diagram

APPENDIX E IDENTIFIED CURRENT DATA CHAIN PROBLEMS

A number of issues have been identified with the current Data Chain as a whole (i.e. Upstream and Downstream) from the sources mentioned in section 5.4.

A number of the issues relate to all stages of the Data Chain as follows:

- Evidence gathered during the previous CHAIN safety study [4] as well as the reported non-compliances in the supplement to Annex 15, suggests that components of the current Data Chain do not meet all of the requirements of ICAO Annex 15. In particular it is unclear if any AIS have demonstrated compliance with the integrity targets (Issues 1 and 8 in Appendix E.4 of Preliminary CHAIN Safety Impact Study [8]).
- There is the need to view Data Chain holistically (issue identified in FHA/PSSA Workshop, section 2.5.1, [12]), i.e. from Data Origination through to Data End Use.
- A key consistent issue is the need for regulation of the Data Chain with a common preference for regulation of the AIS process rather than certification of AI by the regulator (Issue identified in FHA/PSSA Workshop [3]. Regulation of data origination is seen as particularly important in recognition that some origination errors are very unlikely to be detected at later stages of the Data Chain, such as absolute errors in whole data sets, e.g. for an aerodrome (Issue identified in FHA/PSSA Workshop and Preliminary CHAIN Safety Impact Study [8], Section E.4, Issue 4).
- Within individual stages of the Data Chain, people are not necessarily familiar with the use of data at the other end, and therefore have limited understanding of the potential impact of data errors, or where their responsibility begins and ends with respect to the correctness of data (Issue identified in FHA/PSSA Workshop [3] and Preliminary CHAIN Safety Impact Study [8], Section E.4, Issue 25).

The following identified issues are relevant to Upstream Data Chain:

- Data Users do not always feedback data errors, but it is vital that the error is reported to the State AIS as detection of errors is not a sufficient mitigation on its own (Issue identified in FHA/PSSA Workshop [12]).
- Synchronisation of data is problematic as data has got wider use than just for publication purposes and there is lack of confidence regarding usage of the latest version of data amongst all users. There is a degree of cross checking between organisations, so it is possible to detect inconsistencies through regular communications, e.g. with State AIS. However, these checking activities are not mandated[13] (Issue identified in FHA/PSSA Workshop [3] and Preliminary CHAIN Safety Impact Study [8], Section E.4, Issue 11).
- Manual transfer of information introducing a high number of errors (identified in the FHA/PSSA Workshop (Section 2.5.1 of [12]) and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]).

[13] One of the benefits of pan-European use of EAD is that AI can be cross-checked at an international level.

- Processing of aeronautical data within current Upstream Data Chain can be manual or automated. In both cases, errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error; however, not all processes can be automated. (Issue identified in FHA/PSSA Workshop [12], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8] Section 4.1).
- State distributed IAIP having a different representation to the representation of data used by Data Application/Integration and Data Use is currently an issue, especially where the representation is paper-based (Issue identified in Preliminary CHAIN Safety Impact Study [8] Section E.4, Issue 19).
- There is a need for standardised format of electronic or paper representations of IAIP across States or management of different representations across States (for example due to current technical limitations like older versions of Flight Management Systems) (identified in FHA/PSSA Workshop Minutes [12], Section 2.6, Identified Issue 6).
- The timely delivery of data for preparation and publication is an issue. There are contingency procedures to deal with late publications, however the process is costly and errors can be introduced due to people working under pressure (identified in FHA/PSSA Workshop Minutes [12], Section 2.5.5, and in the Preliminary CHAIN Safety Impact Study [8], Section E.4, Issue 13).

APPENDIX F UPSTREAM DATA CHAIN (UDC) SAFETY REQUIREMENTS

This section presents the Upstream Data Chain Safety Requirements (UDC SRs), captured in a series of tables.

For each table:

- the first two columns capture, for each requirement, the requirement's ID and description;
- the column named "Owner" captures, for each Level 2 requirement, the Data Chain function to which the requirement applies to, i.e. to Data Distribution (DD), Data Publication (DP), and Data Origination (DO);
- the column named "Source" identifies the source from where the requirement was derived;
- the column named "Generic Event (pattern)" (only in Level 3 requirements) captures the generic event (e.g. Human Error) which is repeated as a number of distinct events in the FTA documented in the FHA/PSSA Report [9].
- the column named "Existing Specification/Gap" captures the results of the comparison with ICAO Annex 15 and ED-76 to check completeness of the requirements and identify any gaps that may exist within the standards themselves;
- the column named "Known Issues/Problems" captures known issues related with the requirement as appropriate, and records identification source of the issues;
- the column named "Means to Correct" captures the means to address the raised issues; and
- the last column contains, for Level 1 requirements, forward traceability to Level 2 requirements, for Level 2 requirements, traceability back to Level 1 requirements, and for Level 3 traceability back to Level 2 requirements.

Note that the Level 2 and Level 3 requirements exhibit a number of patterns either as a result of similar requirements imposed on different actors in the chain or related to the source of the error. In the former case the issues in achieving the SR may be different depending on the owner. Thus the level 2 requirements identify who the owner is so that the SRs and issues can be separately stated for that owner.

The Level 3 UDC requirements are indicative based on the generic models produced during the FHA/PSSA. The requirements should be rationalised when applying them to specific Data Chain improvements, ie verified as applicable to the scope of the improvement and where necessary further decomposed to the level of implementation and expanded to cover the functionality of the improvement (see Safety Issue 3, and Safety Issue 4 in section 6.2.2).

F.1 UDC Level 1 Safety Requirements

ID	Requirement	Source	Existing Specification or Gap	Implications/Known Issues	Means to Correct	Forward Traceability
L1-01	Published and Distributed Aeronautical Information shall meet defined criteria for Accuracy, Resolution and Format.	HAZ001 Data Quality Properties	Accuracy is defined by Annex 15 para 3.2.6	No known issues	N/A	L2-01, L2-03, L2-04, L2-05, L2-06, L2-07, L2-08, L2-09, L2-10, L2-11, L2-12, L2-13, L2-14, L2-15, L2-17, L2-18, L2-37
			Resolution is defined by Annex 15 para 3.2.7	No known issues	N/A	
			Traceability is required by Annex 15 para 3.2.4	This relates to the issue of authentication and validity status, i.e. if the source and the changer of any data are identified then authentication can be carried out by other users. The validity status of data was discussed at the workshop in terms of at which point in the Data Chain AI is considered valid. Some validation takes place within AIS but some validation (e.g. on terrain data) takes place as part of a flight test, which is outside the AIS boundary (issue identified at FHA/PSSA Workshop [12])	**M038** – Include information on the source and any amendments to data as well as the validity status of the data	
			Format is addressed by specific chapters of Annex 15 for each publication)	There is no standard format of electronic or paper representations of IAIPs particularly across States, or management of different formats, due to current technical limitations (e.g. older versions of Flight Management Systems.) (identified in FHA/PSSA workshop [12]) The issue of digitisation of data has been identified where a distinction should be made between digitisation (i.e. scanning a paper document) and a digital data (i.e. data captured in digital form, e.g. the digitisation of NOTAM which may contain different information to support digital environment).	**M001** - Mandate a standard digital format for AI interchange for AIS (eg, AIXM, eAIP)	

ID	Requirement	Source	Existing Specification or Gap	Implications/Known Issues	Means to Correct	Forward Traceability
				The digital data flow would need to be established (identified in Preliminary Safety Impact Study [8], section E.4, Issues 20 and 21)		
			Common Geospatial reference system defined in WGS-84	Not all States adhere to common geospatial referencing system	**M002** – Mandate a standard geospatial referencing system	
L1-02	The probability that Published or Distributed Aeronautical Information contains errors shall be less than the pre-CHAIN situation and further reduced as far as reasonably practicable (AFARP)[14].	Safety Criteria	No explicit requirement in Annex 15 for AFARP, however, is defined in ESARR 3	ESARR 3 does not apply to AIS	**M003** – Extend scope of ESARR3 to include AIS	L2-01, L2-02, L2-04, L2-05, L2-06, L2-08, L2-09, L2-10, L2-12, L2-14, L2-17, L2-18, L2-37, L2-19, L2-21, L2-23, L2-24, L2-29, L2-30, L2-31, L2-33, L2-35, L2-36, L2-38, L2-39, L2-41, L2-43, L2-47, L2-52, L2-53, L2-55
			ICAO Annex 15 para 3.2.8.Appendix 7	The integrity requirements for individual items of data stated in Annex 15 are not currently considered to be achieved. There is evidence that only Routine ($1x10^{-3}$) is met today and only Essential ($1x10^{-5}$) can be achieved in the near term. Extra procedures will be required for critical data ($1x10^{-8}$) Appendix 7 of ICAO Annex 15 is incomplete, ie it does not include all the data types that exist (as identified by ED77)	**M004** – Show that specific improvements meet the safety criteria **M005** - Consider the implications for non-achievability of current Data Integrity Levels within Data User applications **M006** - Show that regulatory implementing rules meet the safety criteria **M007** – Develop methodology for assigning and demonstrating Data Integrity Levels	

14 L1-02 is expressed as a relative target due to the known issues with achieving the absolute targets in ICAO Annex 15. It is also anticipated that future changes to the Data Chain needed to rectify this situation will happen gradually over time.

ID	Requirement	Source	Existing Specification or Gap	Implications/Known Issues	Means to Correct	Forward Traceability
L1-03	In all instances, information provided under the AIRAC system shall be published in paper copy form.	HAZ002	ICAO Annex 15 para 6.2.1	If AIS systems become purely electronic in the future, the issue of a comprehensive backup would need to be resolved in order to avoid the situation of total loss of AI.	**M008** - Define requirements for availability of publications, backups and lost data contingency planning	N/A
L1-04	Changes to Published AI shall be made available to Data Users prior to the effective date of the change	HAZ003	ICAO Annex 15 para 3.1.1.2, 6.2.1	The timely delivery of data for preparation and publication has been identified as an issue (identified in Preliminary CHAIN Safety Impact Study, Section E.4, Issue 13, FHA/PSSA Workshop Minutes, Section 2.5.5) There are contingency procedures to deal with late publications, however the process is costly and errors can be introduced due to people working under pressure, or due to lack of coordination between actors in the data chain. Further issues are stated against specific Level 2 requirements.	**M009** - Define and implement contingency management and co-ordination procedures in the event of resource overload	L2-19, L2-20, L2-22, L2-23, L2-24, L2-26, L2-29, L2-30, L2-31, L2-32, L2-33, L2-34, L2-35, L2-36, L2-38, L2-40, L2-41, L2-42, L2-43, L2-44, L2-45, L2-46, L2-47, L2-48, L2-49, L2-52, L2-53
L1-05	Measures shall be implemented to minimize the mechanisms through which inconsistency between States IAIPs can arise	HAZ004	No explicit requirement in Annex 15		**M010** – Include following requirement in Annex 15: Measures shall be implemented to minimize the mechanisms through which inconsistency between States IAIPs can arise	L2-39, L2-40, L2-41, L2-42, L2-43, L2-44, L2-45, L2-46, L2-47, L2-48, L2-49, L2-50, L2-51, L2-52, L2-53, L2-54, L2-55, L2-56, L2-58, L2-59

Table 3: UDC Level 1 Safety Requirements

F.2 UDC Level 2 Safety Requirements

This section presents the UDC Level 2 Safety Requirements derived as part of the FHA/PSSA activity (documented in the FHA/PSSA Report [9]). The Level 2 requirements are presented in three tables:

- Table 4 presents the UDC Level 2 safety requirements derived from HAZ001;
- Table 5 presents the UDC Level 2 safety requirements derived from HAZ002; and
- Table 6 presents the UDC Level 2 safety requirements derived from HAZ004.

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
L2-01	The integrity of IAIP shall be maintained during the transfer of IAIP from Data Distribution to subscribed Data Users	DD	FTA Gate L2-01, FTA page 5, in FHA/PSSA Report [9]	Para 3.2.8, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [5] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude[15].	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors[16]. **M029** - Mandate Service Level Agreements	L1-02
L2-02	The integrity of IAIP. shall be maintained in IAIP made available for unsubscribed Data Users unless otherwise clearly indicated [17]	DP	FTA Gate L2-02, FTA page 5, in FHA/PSSA Report [9]	ED-76 2.4.5	No known Issues.	N/A	L1-02
L2-03	Aeronautical Information issued for distribution	DD	FTA Gate L2-02, FTA	This is a re-statement of	o Internal processes within Data Distribution can be manual or automated. In both cases,	**M030** - Develop specifications for	L1-01

[15] Para 3.6.5, Annex 15 recommends that "Automation in AIS should be introduced with the objective of improving the speed, accuracy, efficiency and cost-effectiveness of aeronautical information services"
[16] Maybe outside the scope of the ADI mandate.
[17] Subscribed data users refers to data users that have requested published AIP or are mandatory recipients of published AIP.

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
	shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.		page 6, in FHA/PSSA Report [9]	L1-01 for Data Distribution	errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error. However, not all processes can be automated (Issue identified in FHA/PSSA Minutes [5], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8], Section 4.1] o Where internal Data Distribution processes are fully automated or where software tools are used to enhance the manual processes, systematic faults in such tools (e.g. software bugs) can credibly corrupt AI. The frequency of corruption by such tools is high (as assessed in FHA/PSSA Workshop) since often these tools are not subject to validation.	automated Data Distribution Procedures **M020** – Develop specifications for validation of automated tools	
L2-04	Data Distribution and Data Publication shall maximise the effectiveness of their checking mechanisms for data corruption in terms of absolute accuracy	DD	FTA Gate L2-04, FTA page 5, in FHA/PSSA Report [9]	**Gap:** Annex 15 does not specifically address this class of error detection, although it does specify the responsibilities of AIS with respect to ensuring the correctness of data - see para 3.2.12 of Annex 15.	Valid but corrupt absolute[18] accuracy in data introduced due to use of different co-ordinate systems by different originators is very unlikely to be detectable by the Upstream Data Chain (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.2) Incorrect but valid information entering CHAIN is one of the difficult things to detect. For example AIS can check the format and completeness of supplied data, but not the accuracy of it (issue identified in Preliminary Safety Impact Study [8], Appendix E.4, Issue 16, and in FHA/PSSA Minutes [12], Sections 2.5.1 and 2.6)	**M013** - Identify possible mechanisms for AIS to identify absolute accuracy errors.	L1-02
L2-05	Data Distribution shall provide independent mechanisms to detect	DD	FTA Gate L2-05, FTA page 10, in	Para 3.2.12, ICAO Annex	o It was not clear from the FHA/PSSA workshop whether visual checks are a standardised practice across States and are	**M014 –** Mandate application of visual	L1-02

[18] Small inaccuracies only. Relative inaccuracies within a data set (e.g. for an aerodrome) are more likely to be detected.

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
	corruption in received published AI for distribution		FHA/PSSA Report [9]	15: ED-76 2.3.4	explicitly required by defined procedures when receiving published AI for distribution or are at the discretion of each State. o Where visual checks are carried out, the probability of visual checks carried out at within Data Distribution processes to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [12], section 2.5.1)	checks by AIS **M028** – Develop training procedures for visual checking **M015** – Develop standard procedures for performing visual checks	
L2-06	The integrity of AI shall be maintained in the transfer of AI from Data Publication to Data Distribution	DP	FTA Gate L2-06, FTA page 11, in FHA/PSSA Report [9]	Para 3.2.8, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [5] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [2]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors.	L1-02
L2-07	Independent mechanisms shall be provided for detecting corruption in AI prior to its release for issue and distribution	DP	FTA Gate L2-07, FTA page 11, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 ED-76 2.3.4	Credibly corrupted data in published AI could be detected by review of the published AI prior to its release by Data Originators. However such a review is not mandated at the moment and is inconsistently applied if at all, particularly as some Data Originators are not interested in reviewing AIPs (Issue identified in FHA/PSSA Workshop Minutes [12], section 2.5.1).	**M016** - Mandate review of IAIP by Data Originators.	L1-02
L2-08	Data Preparation within Data Publication shall provide independent mechanisms to detect	DP (Data Preparation)	FTA Gate L2-08, FTA page 28, in FHA/PSSA	Para 3.2.12, ICAO Annex 15	o Application of business/integrity rules at Data Handling can be either manual or automated. Automated application of the rules increases the probability of detection of errors over	**M017** – Develop specification for automated business/integrity	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
	corruption in raw data received from Data Originators		Report [9]		manual by one order of magnitude from medium to high (Issue identified in FHA/PSSA Workshop Minutes [12], section 2.5.1) o The probability of visual checks carried out at various points in Data Preparation (at Data Handling, Data Co-ordination, Data Edition and Data Cartography) to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [5], Section 2.5.1)	checking tools **M015** – Develop standard procedures for performing visual checks **M028** – Develop training procedures for visual checking	
L2-09	Data Distribution and Data Publication shall maximise the effectiveness of their checking mechanisms for data accuracy errors and credibly corrupted effective dates provided by Data Origination	DP	FTA Gate L2-09, FTA page 11, in FHA/PSSA Report [9]	**Gap:** Annex 15 does not specifically address this class of error detection, although it does specify the responsibilities of AIS with respect to ensuring the correctness of data - see para 3.2.12 of Annex 15.	Valid but corrupt effective dates provided by Data Origination or data accuracy errors provided by Data Origination are very unlikely to be detectable by processes within Data Publication (Issue identified in FHA/PSSA Workshop Minutes [12], section 2.5.1and in Preliminary Safety Impact Report [8], Appendix E.4, Issue 16.	**M016** - Mandate review of IAIP by Data Originators.	L1-02
L2-10	Data Preparation within Data Publication shall provide independent mechanisms to detect corruption in approved evaluated raw data	DP (Data Preparation)	FTA Gate L2-10, FTA page 12, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15	o Application of business/integrity rules at Data Handling can be either manual or automated. Automated application of the rules increases the probability of detection of errors over manual by one order of magnitude from medium to high (Issue identified in FHA/PSSA	**M017** – Develop specification for automated business/integrity checking tools	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
	received from Initial Check of Raw Data phase of Data Publication.				Workshop Minutes [12], Section 2.5.1) o The probability of visual checks carried out at various points in Data Preparation (at Data Handling, Data Co-ordination, Data Edition and Data Cartography) to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [12], section 2.5.1) o Independent double entry of all data into storage and independent triple entry of critical data into storage (manual or automated) significantly increases the probability of detecting errors during the process of entering approved evaluated raw data into storage (identified in FHA/PSSA Workshop Minutes [5], Section 2.5.1). However, it was not clear from the workshop whether these practices are standardised across States and are explicitly required by defined procedures or are at the discretion of each State. For example, it was identified by the analysis that the Procedure for the Storage of Approved Data within the Operating Procedures for AIS Static Data defined in [8] does not explicitly identify the requirement for independent double and independent triple entry of data	**M015** – Develop standard procedures for performing visual checks **M028** – Develop training procedures for visual checkin**g** **M018** – Develop robust procedures for manual transfer of AI using double or triple checking	
L2-11	Approved Evaluated Raw data provided to Data Preparation shall be correct, i.e. shall be accurate, of correct resolution and of correct format.	DP (Initial Check of Raw Data phase)	FTA Gate L2-11, FTA page 24, in FHA/PSSA Report [9]	As in L1-01	o Initial Check of Raw Data processes (within Data Publication) can be manual or automated. In both cases, errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error. However, not	**M019** - Develop specifications for automated initial checking of Raw Data	L1-01

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					all processes can be automated (Issue identified in FHA/PSSA Minutes [5], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8], Section 4.1] o Where Initial Check of Raw Data processes are fully automated or where software tools are used to enhance the manual processes, systematic faults in such tools (e.g. software bugs) can credibly corrupt AI. The frequency of corruption by such tools is high (as assessed in FHA/PSSA Workshop) since often these tools are not subject to validation.	**M020** – develop specifications for validation of automated tools	
L2-12	The integrity of AI shall be maintained in the transfer of AI from Initial Check of Raw Data to Data Preparation	DP (Initial Check of Raw Data phase)	FTA Gate L2-12, FTA page 24, in FHA/PSSA Report [9]	Para 3.2.8, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors[19].	L1-02
L2-13	Prepared Aeronautical Information for publication shall be correct, i.e. shall be accurate, of correct resolution, of correct format, and timeliness	DP (Data Preparation phase)	FTA Gate L2-13, FTA page 12, in FHA/PSSA Report [9]	As in L1-01	o Internal processes of Data Preparation (within Data Publication) can be manual or automated. In both cases, errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error. However, not all processes can be automated (Issue identified in FHA/PSSA Minutes [12], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8], Section 4.1] o Where internal processes are fully automated or where software tools are used to enhance	**M021** - develop specifications for automated Data Preparation Procedures **M020** – develop specifications for validation of	L1-01

[19] Maybe outside the scope of the ADI mandate.

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					the manual processes, systematic faults in such tools (e.g. software bugs) can credibly corrupt AI. The frequency of corruption by such tools is high (as assessed in FHA/PSSA Workshop) since often these tools are not subject to validation	automated tools	
L2-14	Data Preparation shall provide independent mechanisms to detect corruption in prepared AI prior to its release as published AI for distribution.	DP (Data Preparation phase)	FTA Gate L2-13, FTA page 12, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.2.1, ICAO Annex 15	There are no specific known issues regarding quality control checks of prepared AI prior to its release as published AI for distribution other than that, as processes, they are subject to human error or to being ill-defined and the more manual the quality control process is, the higher the frequency of error omission.	**M022** – Develop standard data quality control procedures **M023** – Mandate standard AIS quality procedures	L1-02
L2-15	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.	DO	FTA Gate L2-15, FTA page 29, in FHA/PSSA Report [9]		The frequency of errors presented in data provided by Data Origination for publication was assessed as high by the participants at the FHA/PSSA Workshop (identified in FHA/PSSA Minutes [12], Section 2.5.1), with some errors very unlikely to be detectable.	**M024** – Introduce monitoring of data origination errors **M025** – Mandate use of authorised data originators only **M012** – Define Service Level Agreements between actors. **M029** - Mandate Service Level Agreements **M026** – Define rules for setting up as a data provider	L1-01
L2-16	Calculated/derived data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.	DO	FTA Gate L2-16, FTA page 28, in FHA/PSSA Report [9]		Use of unauthorised originators as sources of providing data to Data Publication increases the frequency of these errors. (Issue identified in Preliminary CHAIN Safety Impact Study Report [8] section E.4, Issue 4). In general, the interface of origination of data to AIS has been characterised as weak (identified in [8], section E.4, Issue 18). There is a need for regulation of the Data Providers in recognition of the safety-related nature of the information being provided. Due to lack of regulation, there are no rules for setting up as a data provider and the success of such an enterprise rests mostly on earned reputation. Also, there are no clearly defined boundaries of responsibility for correctness of data (Issue		L1-01

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					identified in FHA/PSSA Minutes [12], section 2.5.1)	**M027** – Define roles and responsibilities for Data Chain Actors	
L2-17	The integrity of AI shall be maintained in the transfer of AI from Data Origination to Data Publication	DO	FTA Gate L2-17, in FHA/PSSA Report [9]	Para 3.2.8, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors **M029** - Mandate Service Level Agreements	L1-02
L2-18	Initial Check of Raw Data within Data Publication shall provide independent mechanisms to detect corruption in raw data received from Data Origination and agree alterations with the Data Originator	DP (Initial Check of Raw Data phase)	FTA Gate L2-18, FTA page 28, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 ED-76 2.3.5 (3), ED-76 2.4.1 (6) and 2.4.2.	o The probability of visual checks carried out at Initial Check of Raw Data phase (ie at Data Receipt and Data Approval) to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [12], section 2.5.1) o Use of unauthorised originators as sources of providing data to Data Publication increases the frequency of these errors. (Issue identified in Preliminary CHAIN Safety Impact Study Report [8] section E.4, Issue 4). There is a need for regulation of the Data Providers in recognition of the safety-related nature of the information being provided. Due to lack of regulation, there are no rules for setting up as a data provider and the success of such an	**M015** – Develop standard procedures for performing visual checks **M028** – Develop training procedures for visual checking **M025** – Mandate use of authorised data originators only **M026** – Define rules for setting up as a data provider	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					enterprise rests mostly on earned reputation.		
L2-37	Data Distribution shall provide independent mechanisms to detect corruption in issued AI for distribution and report errors to Data Publication	DD	FTA Gate L2-37, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15, Para 3.2.1, ICAO Annex 15, ED-76 2.3.4	There are no specific known issues regarding quality control checks of issued AI prior to distribution other than that, as processes, they are subject to human error or to being ill-defined and the more manual the quality control process is, the higher the frequency of error omission.	**M022** – Develop standard data quality control procedures **M023** – Mandate standard AIS quality procedures	L1-02

Table 4: UDC Level 2 Safety Requirements derived from HAZ001

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
L2-19	Data Distribution shall make any changes to IAIP available to subscribed Data Users prior to the effective date of the changes.	DD	FTA Gate L2-19, FTA page 33, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors **M029** - mandate Service Level Agreements	L1-02
L2-20	Changes to issued AI shall be made available for distribution prior to the effective date of the change.	DD	FTA Gate L2-20, FTA page 34, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15 Para 6.2.1, ICAO Annex 15	o Internal processes within Data Distribution can be manual or automated. In both cases, errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error. However, not all processes can be automated (Issue identified in FHA/PSSA Minutes [12], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8], Section 4.1]	**M030** - develop specifications for automated Data Distribution Procedures	L1-04

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					o Where internal Data Distribution processes are fully automated or where software tools are used to enhance the manual processes, systematic faults in such tools (e.g. software bugs) can credibly corrupt AI. The frequency of corruption by such tools is high (as assessed in FHA/PSSA Workshop) since often these tools are not subject to validation.	**M020** – develop specifications for validation of automated tools	
L2-21	IAIP made available for unsubscribed distribution shall be up to date unless clearly otherwise indicated.	DD	FTA Gate L2-21, FTA page 33, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15	No known Issues.	N/A	L1-02
L2-22	Data Distribution shall provide independent mechanisms to detect missing changes in received published AI prior to the effective dates of the changes.	DD	FTA Gate L2-19, FTA page 38, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.1.1.2, ICAO Annex 15	o It was not clear from the FHA/PSSA workshop whether visual checks are a standardised practice across States and are explicitly required by defined procedures when receiving published AI for distribution or are at the discretion of each State. o Where visual checks are carried out, the probability of visual checks carried out at Data Distribution to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1)	**M014 –** mandate application of visual checks by AIS **M015** – develop standard procedures for performing visual check**s** **M028** – develop training procedures for visual checking	L1-04
L2-23	Data Publication shall make any changes to IAIP available to subscribed Data Users prior to the effective date of the changes.	DP	FTA Gate L2-23, FTA page 38, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	Agreements between actors	
L2-24	Data Distribution shall maximise the effectiveness of their checking mechanisms for detecting required changes that have not been made by Data Origination.	DD	FTA Gate L2-24, FTA page 39, in FHA/PSSA Report [9]	**Gap:** Annex 15 does not specifically address this class of error detection, although it does specify the responsibilities of AIS with respect to ensuring the correctness of data, see para 3.2.12 of Annex 15.	Changes to AI (isolated or driven by other changes) which should have been made by Data Originators but haven't, are very unlikely to be detectable by the Upstream Data Chain (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.3).	**M012** – Define Service Level Agreements between actors **M029** - mandate Service Level Agreements	L1-02
L2-25	Independent mechanisms shall be provided for detecting missing changes to published AI prior to its release for issue and distribution.	DP	FTA Gate L2-25, FTA page 39, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 ED-76 2.3.4	Changes missing from the published AI could be detected by review of the published AI prior to its release by Data Originators. However such a review is not mandated at the moment and is inconsistently applied if at all, particularly as some Data Originators are not interested in reviewing AIPs (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1and 2.5.3)	**M016** - mandate review of IAIP by Data Originators. **M031** – implement sequence numbering of changes	L1-04
L2-26	Data Publication shall maximise the effectiveness of their checking mechanisms for detecting isolated changes that have been	DP	FTA Gate L2-24, FTA page 39, in FHA/PSSA Report [9]	**Gap:** Annex 15 does not address anywhere not easily detectable	Changes to AI that are made in isolation (i.e., not part of a set of changes) and are not notified by Data Origination for publication are very unlikely to be detectable20 by processes of Data Publication and Data Distribution (Issue identified in FHA/PSSA Workshop Minutes [12], Section	**M016** - mandate review of IAIP by Data Originators.	L1-04

[20] AIS would not normally notice missing single data item changes or whole sets of data items not notified by the Data Originator, although experienced actors could know about the changes from the AIS grapevine!

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
	made but not provided for publication by Data Origination.			errors.	2.5.3).		
L2-27	Changes in surveyed data shall be made available to Data Publication prior to the effective date of change.	DO	FTA Gate L2-27, FTA page 56, in FHA/PSSA Report [9]	Para 3.2.6, ICAO Annex 15 Para 3.1.4, ICAO Annex 15	The frequency of errors presented in data provided by Data Origination for publication was assessed as high by the participants at the FHA/PSSA Workshop (identified in FHA/PSSA Minutes [12], Section 2.5.1), with some errors very unlikely to be detectable. Use of unauthorised originators as sources of providing data to Data Publication increases the frequency of these errors. (Issue identified in Preliminary CHAIN Safety Impact Study Report [8] Section E.4, Issue 4). In general, the interface of origination of data to AIS has been characterised as weak (identified in [8], Section E.4, Issue 18). There is a need for regulation of the Data Originators in recognition of the safety-related nature of the information being provided. Due to lack of regulation, there are no rules for setting up as a data originator and the success of such an enterprise rests mostly on earned reputation. Also, there are no clearly defined boundaries of responsibility for correctness of data (Issue identified in FHA/PSSA Minutes [12], Section 2.5.1)	**M024** – introduce monitoring of data origination errors **M025** – mandate use of authorised data originators only **M012** – define Service Level Agreements between actors. **M029** - mandate Service Level Agreements **M032** – define rules for setting up as a data originator **M027** – define roles and responsibilities for Data Chain Actors	L1-04
L2-28	Changes in calculated/derived data shall be made available to Data Publication prior to the effective date of change.	DO	FTA Gate L2-28, FTA page 56, in FHA/PSSA Report [9]	Para 3.2.6, ICAO Annex 15 Para 3.1.4, ICAO Annex 15			
L2-29	Data Origination / Data Publication shall verify the	DO	FTA Gate L2-29, FTA	Para 3.1.1.2, ICAO Annex	The issue of manual transfer introducing a high number of errors was identified both in the	**M011** – Produce specification for	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
	successful transfer of any changes in raw/surveyed data to Data Publication.		page 56, in FHA/PSSA Report [9]	15	FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	automated transfer of AI between actors **M012** – Define Service Level Agreements between actors	
L2-30	Initial Check of Raw Data shall provide independent mechanisms to detect missing changes in received raw data prior to the effective date of the changes	DP (Initial Check of Raw Data phase)	FTA Gate L2-30, FTA page 56, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.1.1.2, ICAO Annex 15	The probability of visual checks carried out at Initial Check of Raw Data phase (i.e. at Data Receipt and Data Approval) to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [5], Section 2.5.1)	**M015** – develop standard procedures for performing visual check**s** **M028** – develop training procedures for visual checking	L1-02
L2-31	Data Preparation shall provide independent mechanisms to detect missing changes in received raw data prior to the effective date of the changes.	DP (Data Preparation phase)	FTA Gate L2-31, FTA page 57, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.1.1.2, ICAO Annex 15	o Application of business/integrity rules at Data Handling can be either manual or automated. Automated application of the rules increases the probability of detection of errors over manual by one order of magnitude from medium to high (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1) o The probability of visual checks carried out at various points in Data Preparation (at Data Handling, Data Co-ordination, Data Edition and Data Cartography) to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA	**M017** – develop specification for automated business/integrity checking tools **M015** – develop standard procedures for performing visual check**s** **M028** – develop	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					Workshop Minutes [12], Section 2.5.1) o Independent double entry of all data into the register and independent triple entry of critical data into the register (manual or automated) is a mechanism that can significantly increase the probability of detecting missing changes in AI during the process of storing approved evaluated raw data (identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1). However, it was not clear from the workshop whether these practices are standardised across States. For example, it was identified by the analyst that the Procedure for the Storage of Approved Data within the Operating Procedures for AIS Static Data defined in [18] does not explicitly identify the requirement for independent double and independent triple entry of data.	training procedures for visual checking **M018** – develop robust procedures for manual transfer of AI using double or triple checking	
L2-32	Changes in prepared AI shall be made available for publication prior to the effective date of the change.	DP (Data Preparation phase)	FTA Gate L2-32, FTA page 40, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15 Para 6.2.1, ICAO Annex 15	o Internal processes of Data Preparation (within Data Publication) can be manual or automated. In both cases, errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error. However, not all processes can be automated (Issue identified in FHA/PSSA Minutes [12], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8], Section 4.1] o Where internal processes are fully automated or where software tools are used to enhance the manual processes, systematic faults in such tools (e.g. software bugs) can credibly corrupt AI. The frequency of corruption by such tools is high (as assessed in FHA/PSSA Workshop) since often these tools are not subject to validation	**M021** - develop specifications for automated Data Preparation Procedures **M020** – develop specifications for validation of automated tools	L1-04

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
L2-33	Data Preparation shall provide independent mechanisms to detect missing changes in prepared AI.	DP (Data Preparation phase)	FTA Gate L2-33, FTA page 40, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.2.1, ICAO Annex 15	There are no specific known issues regarding quality control checks of prepared AI prior to its release as published AI for distribution other than that, as processes, they are subject to human error or to being ill-defined and the more manual the quality control process is, the higher the frequency of error omission.	**M022** – develop standard data quality control procedures **M023** – mandate standard AIS quality procedures	L1-02
L2-34	Changes in approved evaluated raw data shall be made available to Data Preparation prior to the effective date of the changes.	DP (Initial Check of Raw Data phase)	FTA Gate L2-34, FTA page 52, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15 Para 6.2.1, ICAO Annex 15	o Initial Check of Raw Data processes (within Data Publication) can be manual or automated. In both cases, errors can be generated by human error or ill-defined processes, however the more manual the process, the higher the frequency of error generation due to human error. However, not all processes can be automated (Issue identified in FHA/PSSA Minutes [12], Section 2.5.1, and in Preliminary CHAIN Safety Impact Study [8], Section 4.1] o Where Initial Check of Raw Data processes are fully automated or where software tools are used to enhance the manual processes, systematic faults in such tools (e.g. software bugs) can credibly corrupt AI. The frequency of corruption by such tools is high (as assessed in FHA/PSSA Workshop) since often these tools are not subject to validation.	**M019** - develop specifications for automated initial checking of Raw Data **M020** – develop specifications for validation of automated tools	L1-04
L2-35	Data Publication shall verify the transfer of approved, evaluated raw data changes from Initial Check of Raw Data to Data Preparation.	DP (Initial Check of Raw Data phase)	FTA Gate L2-35, FTA page 52, in FHA/PSSA Report [9]	Para 3.1.1.2, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
					magnitude.		
L2-36	Data Preparation shall provide independent mechanisms to detect missing changes in received approved evaluated raw data	DP (Data Preparation phase)	FTA Gate L2-36, FTA page 52, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.1.1.2, ICAO Annex 15	o Application of business/integrity rules at Data Handling can be either manual or automated. Automated application of the rules increases the probability of detection of errors over manual by one order of magnitude from medium to high (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1) o The probability of visual checks carried out at various points in Data Preparation (at Data Handling, Data Co-ordination, Data Edition and Data Cartography) to detect errors depend on the knowledge and experience of the people performing them. The probability of success of the check carried out by an experienced person over the probability of success of the check carried out by a less experienced person increases by one order of magnitude (Issue identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1) o Independent double entry of all data into the register and independent triple entry of critical data into the register (manual or automated) is a mechanism that can significantly increase the probability of detecting missing changes in AI during the process of storing approved evaluated raw data (identified in FHA/PSSA Workshop Minutes [12], Section 2.5.1). However, it was not clear from the workshop whether these practices are standardised across States. For example, it was identified by the analyst that the Procedure for the Storage of Approved Data within the Operating Procedures for AIS Static Data defined in [18] does not explicitly identify the requirement for independent double and independent triple entry of data.	**M017** – develop specification for automated business/integrity checking tools **M015** – develop standard procedures for performing visual check**s** **M028** – develop training procedures for visual checking **M018** – develop robust procedures for manual transfer of AI using double or triple checking	L1-02

ID	Requirement	Actor	Source	Existing Specification / Gap	Known Issues/Problems	Means to Correct	Trace to Level 1
L2-38	Data Distribution shall provide independent mechanisms to detect missing changes in issued AI for distribution prior to the effective dates of the changes.	DD	FTA Gate L2-38, FTA page 52, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 3.1.1.2	There are no specific known issues regarding quality control checks of issued AI prior to distribution other than that, as processes, they are subject to human error or to being ill-defined and the more manual the quality control process is, the higher the frequency of error omission.	**M022** – develop standard data quality control procedures **M023** – mandate standard AIS quality procedures	L1-02

Table 5: UDC Level 2 Safety Requirements derived from HAZ003

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
L2-39	Transfer of IAIP from Data Distribution to Data Application/Integration shall not introduce inconsistencies in IAIPs	DD	FTA Gate L2-39, in FHA/PSSA Report [9]	No specific requirement	The issues with this requirement combine the issues related to the maintenance of data transfer during transfer and the successful notification of changes. These sources should thus be assured with reference to the related requirements under HAZ001 and HAZ003. However, there are a number of issues that could still lead to this situation: 1. diverse interpretation of NOTAM – due to the current nature of NOTAM some distributors add or alter NOTAM data to "clarify" the meaning. This can introduce different interpretations by downstream actors 2. Inconsistent resolution of resource loading issues. See issue discussed under L2-42.	**M033** – mandate that where NOTAM are amended the original NOTAM must also be included **M009** - define and implement contingency management and co-ordination procedures in the event of resource overload	L1-02
L2-40	Data Distribution shall distribute regulated IAIP to subscribed Data Users in accordance with the AIRAC cycle	DD	FTA Gate L2-40, FTA page 60, in FHA/PSSA Report [9]	Para 6.1.1, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define	L1-05

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
					Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	Service Level Agreements between actors **M029** - mandate Service Level Agreements	
L2-41	Data Publication shall distribute regulated IAIP to subscribed Data Users in accordance with the AIRAC cycle..	DP	FTA Gate L2-41, FTA page 61, in FHA/PSSA Report [9]	Para 6.1.1, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors	L1-02
L2-42	Data Distribution shall implement measures to minimise time delays in internal processes resulting in non-adherence of regulated IAIP to AIRAC cycle	DD	FTA Gate L2-42, FTA page 62, in FHA/PSSA Report [9]	Para 6.2.1, ICAO Annex 15 Para 6.3.2, ICAO Annex 15	The timely delivery of data for preparation and publication is an issue (identified in FHA/PSSA Workshop Minutes [12], Section 2.5.5, and in the Preliminary CHAIN Safety Impact Study [8] Section E.4, Issue 13). There are contingency procedures to deal with late publications, however the process is costly and errors can be introduced due to people working under pressure. Increased workload, insufficient resources and information provided by originators too late are the main causes that have been identified in the workshop.	**M035 –** develop AIS procedures that are more efficient **M009** - define and implement contingency management and co-ordination procedures in the event of resource overload	L1-04, L1-05
L2-43	Data Distribution shall implement measures to check for late changes in prepared AI for publication to AIRAC cycle	DD	FTA Gate L2-43, FTA page 61, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15	Lack of co-operation or co-ordination between different departments in Data Publication and Data Preparation within a State or across States Lack of awareness among Data Originators of the importance of adhering to AIRAC rules is also one of the reasons (issue identified in FHA/PSSA Workshop [12], and Preliminary Safety Impact Study [8],	**M012** – Define Service Level Agreements between actors **M029** - mandate Service Level Agreements **M034** – improve	L1-02

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
						awareness of Data Originators to AIRAC cycle	
L2-44	Initial Check of Raw Data within Data Publication shall implement measures to minimise time delays of its internal processes resulting in non-adherence of regulated IAIP to AIRAC cycle	DP (Initial Check of Raw Data)	FTA Gate L2-44, FTA page 64, in FHA/PSSA Report [9]	Para 6.2.1, ICAO Annex 15 Par 6.3.2, ICAO Annex 15	The timely delivery of data for preparation and publication is an issue (identified in FHA/PSSA Workshop Minutes [5], Section 2.5.5, and in the Preliminary CHAIN Safety Impact Study [8] Section E.4, Issue 13). There are contingency procedures to deal with late publications, however the process is costly and errors can be introduced due to people working under pressure. Increased workload, insufficient resources and information provided by originators too late are the main causes that have been identified in the workshop.	**M035 –** develop AIS procedures that are more efficient **M009** - define and implement contingency management and co-ordination procedures in the event of resource overload	L1-04, L1-05
L2-45	Data Preparation shall implement measures to minimise time delays of its internal processes resulting in non-adherence of prepared AI for publication to AIRAC cycle	DP (Data Preparation phase)	FTA Gate L2-45, FTA page 64, in FHA/PSSA Report [9]	Para 6.2.1, ICAO Annex 15 Para 6.3.2, ICAO Annex 15	The timely delivery of data for preparation and publication is an issue (identified in FHA/PSSA Workshop Minutes [12] Section 2.5.5, and in the Preliminary CHAIN Safety Impact Study [8] Section E.4, Issue 13). There are contingency procedures to deal with late publications, however the process is costly and errors can be introduced due to people working under pressure. Increased workload, insufficient resources and information provided by originators too late are the main causes that have been identified in the workshop.	**M035 –** develop AIS procedures that are more efficient **M009** - define and implement contingency management and co-ordination procedures in the event of resource overload	L1-04, L1-05
L2-46	Data Preparation shall implement measures to check for late changes in prepared AI for publication to AIRAC cycle	DP (Data Preparation phase)	FTA Gate L2-46, FTA page 64, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15	Lack of co-operation or co-ordination between different departments in Data Publication and Data Preparation within a State or across States	**M012** – Define Service Level Agreements between actors	L1-04, L1-05
L2-47	Data Originators shall distribute raw / prepared AI sufficiently in advance of the AIRAC cycle, in which the data is effective, to	DO	FTA Gate L2-47, FTA page 64, in FHA/PSSA Report [9]	Para 6.1.1, ICAO Annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define	L1-02

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
	allow for Data Publication				Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	Service Level Agreements between actors **M029** - mandate Service Level Agreements	
L2-48	Data Origination shall implement measures to minimise time delays in providing raw data to Data Publication too late for AIRAC adherence	DO	FTA Gate L2-48, FTA page 64, in FHA/PSSA Report [9]	Para 6.2.1, ICAO Annex 15 Para 6.3.2, ICAO Annex 15	The timely delivery of data for preparation and publication is an issue (identified in FHA/PSSA Workshop Minutes [12] Section 2.5.5, and in the Preliminary CHAIN Safety Impact Study [8] Section E.4, Issue 13). Lack of awareness among Data Originators of the importance of adhering to AIRAC rules is also one of the reasons (issue identified in FHA/PSSA Workshop [5], and Preliminary Safety Impact Study [8],	**M035 –** develop AIS procedures that are more efficient **M034** – improve awareness of Data Originators to AIRAC cycle	L1-04, L1-05
L2-49	Initial Check of Raw Data shall identify originated data that is too late for publication and agree appropriate action with Data Originator21	DP (Initial Check of Raw Data phase)	FTA Gate L2-49, FTA page 64, in FHA/PSSA Report [9]	Para 6.2.1, ICAO Annex 15 Par 6.3.2 ED-76 2.4.2 applies to alteration of data There is also specific guidance on making alterations and avoiding last minute	There are error feedback inconsistencies in the AIS co-ordination with Data Origination (inconsistent feedback identified in FHA/PSSA Workshop [12]).	**M012** – Define Service Level Agreements between actors **M029** - mandate Service Level Agreements	L1-04, L1-05

[21] Such action may for example include issuing a NOTAM or delaying the effective date of the change.

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
				postponements in ED-77 2.4.3 and 2.4.4, respectively			
L2-50	Data Distribution shall implement measures to minimise the mechanisms through which inconsistency arises with IAIP distributed by others	DD	FTA Gate L2-50, FTA page 74, in FHA/PSSA Report [9]	**Gap:** No explicit requirement in ICAO Annex 15		**M010** – Include following requirement in Annex 15: Measures shall be implemented to minimize the mechanisms through which inconsistency between States IAIPs can arise	L1-05
L2-51	Data Distribution shall implement measures to minimise the mechanisms through which inconsistencies arise between distributed IAIP	DD	FTA Gate L2-51, FTA page 74, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15	No known issues, but this checking is not mandated with respect to inconsistencies	**M036** – develop processes that minimise inconsistencies between IAIP	L1-05
L2-52	Initial Check of Raw Data shall distribute regulated IAIP to Data Preparation sufficiently in advance of the AIRAC cycle, in which the data is effective, to allow for Data Publication	DP (Initial Check of Raw Data phase)	FTA Gate L2-52, in FHA/PSSA Report [9]	Para 6.1.1, ICAO annex 15	The issue of manual transfer introducing a high number of errors was identified both in the FHA/PSSA Workshop (Section 2.5.1 of [12] and in the Preliminary CHAIN Safety Impact Study (Issue 10 in Appendix E.4 of [8]). At the FHA/PSSA Workshop it was assessed, that the frequency of error in electronic transfer (low) of data is lower than the frequency of error in manual transfer (high) of data by approximately two orders of magnitude.	**M011** – Produce specification for automated transfer of AI between actors **M012** – Define Service Level Agreements between actors	L1-02
L2-53	Data Preparation shall identify checked data that is too late for publication and agree appropriate action with Data Originator	DP (Data Preparation phase)		Para 3.2.12, ICAO Annex 15	There are error feedback inconsistencies in the AIS co-ordination with Data Origination (inconsistent feedback identified in FHA/PSSA Workshop [12]).	**M012** – Define Service Level Agreements between actors	L1-02

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
L2-54	Data Distribution shall implement measures to minimise mechanisms through which inconsistencies between paper issued AI and electronically published AI can arise.	DD	FTA Gate L2-54, FTA page 73, in FHA/PSSA Report [9]	Para 6.3.1, ICAO Annex 15	Inconsistencies between issued AI and electronically published AI in Data Distribution can arise mainly by the use of different representations for data between paper and electronic system.	**M036** – develop processes that minimise inconsistencies between IAIP	L1-05
L2-55	Data Distribution shall check that there are no inconsistencies between paper and electronic version of published AI	DD	FTA Gate L2-55, FTA page 73, in FHA/PSSA Report [9]	Para 3.2.12, ICAO Annex 15 Para 3.2.1, ICAO Annex 15	Inconsistencies can be introduced by differences between paper and electronic versions of the same AI. Where a State issues both, reviewing the paper version against the electronic version of the published AI can reduce the frequency of inconsistencies between the two. It was not clear from the workshop or the AIS Data Process description [8] whether the final quality check of the issued AI for distribution would carry out this type of review.	**M037** – develop procedures for consistency checking of all paper and electronic IAIP	L1-02
L2-56	Data Preparation shall ensure that any last minute changes in published AI are communicated to subscribed Data Users	DP (Data Preparation phase)	FTA Gate L2-56, FTA page 73, in FHA/PSSA Report [9]	No explicit requirement in ICAO Annex 15	Co-operation/co-ordination between departments is very important in communicating any last minute changes in electronically published AI which need to be reflected in the paper version of AI at issuing	**M012** – Define Service Level Agreements between actors	L1-05
L2-57	Measures shall be implemented to minimise the mechanisms through which inconsistent representation of Aeronautical Information between States and Data Application/Integration and Data End Use can arise	DO, DP, DD	FTA Gate L2-57, FTA page 71, in FHA/PSSA Report [9]	No explicit requirement in Annex 15	State distributed IAIPs having a different representation to the representation of data used by Data Application/Integration and Data Use is currently an issue, especially where the representation is paper-based (Issue identified in Preliminary CHAIN Safety Impact Study [8] Section E.4, Issue 19). The issue is that downstream actors need to extract the data from the paper-based product and convert it to digital form in order to be able to use it; this is a process which results in data synchronisation problems and it is a source of errors as it is a process involving manual manipulation of data.	**M040** – develop specifications for automated transfer of IAIP to Data Application / Integration (e.g. automatic translation of AIXM to ARINC)	L1-05

ID	Requirement	Actor	Source	Existing Spec/Gap	Known issues/problems	Means to Correct	Trace to Level 1
L2-58	Measures shall be implemented to minimise the mechanisms through which inconsistent electronic IAIPs distributed from different AIS can arise	DD	FTA Gate L2-58, FTA page 72, in FHA/PSSA Report [9]	No explicit requirement in Annex 15	Standardised format of electronic representations of IAIPs across States or the management of different representations across States has been identified as an issue (FHA/PSSA Workshop Minutes, Section 2.6, Identified Issue 6) [22] Electronic representations of IAIPs across States are not standardised yet. The lack of a standard has led to divergent implementations, manifested through heterogeneous technical solutions, navigation structures and presentation formats.	**M001** - Mandate a standard digital format for AI interchange for AIS (e.g. AIXM, eAIP)	L1-05
L2-59	Measures shall be implemented to minimise the mechanisms through which inconsistent paper IAIPs distributed from different AIS can arise.	DD	FTA Gate L2-59, FTA page 72, in FHA/PSSA Report [9]	No explicit requirement in ICAO Annex 15	Standardised format of paper representations of IAIPs across States or the management of different representations across States has been identified as an issue (FHA/PSSA Workshop Minutes, Section 2.6, Identified Issue 6)	**M039** - Mandate a standard format for paper AI interchange for AIS	L1-05
L2-60	Data Distribution shall check that all subscribed recipients receive the same paper copy of IAIP.	DD	FTA Gate L2-59, FTA page 74, in FHA/PSSA Report [9]	Para 3.3.5, ICAO Annex 15	There is a general lack or inconsistency of feedback from Data Users (currently not mandated). This means that errors can go unreported (identified in Preliminary Safety Impact Study [8], section E.4, issue 2, and in FHA/PSSA Workshop [12]).	**M012** – Define Service Level Agreements between actors **M041** – Provide mechanism to facilitate and encourage error feedback from data users	

Table 6: UDC Level 2 Safety Requirements derived from HAZ004

[22] This issue could be addressed if AIS migrate to EAD as inconsistencies between digital State AIS data are checked for as part of the level C Static Data Checks in EAD.

F.3 UDC Level 3 Safety Requirement

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).	E3-13, E3-09, E3-17, E3-60, E3-56, E3-65, E3-35	Malfunction of tools (s/w)	Para 2.4.5, ED-76	L2-03, L2-11, L2-13, L2-20, L2-32, L2-34, L2-50
L3-02	Tool validation shall include the impact of hardware failure	E3-08, E3-12, E3-16, E3-36, E3-57, E3-61 E3-66	Hardware fault of tools	Para 2.4.5, ED-76	L2-03, L2-11, L2-13, L2-20, L2-32, L2-34
L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.	E3-37 E3-58, E3-62, E3-67, E3-142, E3-143, E3-144	Failure of hardware built-in tests of tool(s) used at various processes	Para 2.4.5, ED-76:	L2-03, L2-11, L2-13, L2-20, L2-32, L2-34
L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.	E3-06, E3-10, E3-14, E3-18, E3-21, E3-30, E3-33, E3-39, E3-42, E3-45, E3-46, E3-51, E3-54, E3-55, E3-59, E3-64, E3-68, E3-84, E3-87, E3-91, E3-145	Human Error	Para 3.2.3, ICAO annex 15 Para 3.6.7, ICAO Annex 15 Para 2.4.4, ED-76 Para 2.5.2, ED -76	L2-03, L2-05, L2-08, L2-10, L2-11, L2-13, L2-14, L2-18, L2-20, L2-22, L2-30, L231, L2-32, L2-
L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.				
L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.				
L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.				

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls				33, L2-34, L2-36, L2-37, L2-38, L2-43, L2-46, L2-49, L2-50, L2-51, L2-53, L2-54, L2-55, L2-56
L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process	E3-07, E3-11, E3-15, E3-19, E3-20, E3-22, E3-24, E3-31, E3-32, E3-34, E3-40, E3-41, E3-43, E3-44, E3-63, E3-69, E3-73, E3-76, E3-82, E3-85, E3-86, E3-88, E3-89, E3-90, E3-92, E3-103, E3-135, E3-138	Absence of/Incorrect process (various data process procedures)	Para 2.4.1, ED-76 (states what data processing procedures should define) Para 2.2, ED-76 (Quality Management)	L2-03, L2-05, L2-08, L2-10, L2-11, L2-13, L2-14, L2-18, L2-20, L2-22, L2-30, L2-31, L2-32, L2-33, L2-34, L2-36, L2-37, L2-38, L2-43, L2-46, L2-49, L2-50, L2-51, L2-53, L2-54, L2-55

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
L3-10	Aeronautical Information integrity checking rules shall comply as a minimum with the EUROCONTROL Business Integrity Rules	E3-75	Incomplete business/integrity rules		L2-08, L2-10, L2-31, L2-36
L3-11	Protection of electronic aeronautical data while stored or in transit shall be totally monitored by the cyclic redundancy check (CRC) as defined in Annex 15 para 3.2.10.	E3-01 E3-03 E3-71 E3-80	Credible corruption of data introduced by electronic transfer	Para 3.2.10, ICAO Annex 15	L2-01, L2-06, L2-12, L2-17
		E3-108	Inconsistencies in IAIP introduced by electronic transfer	None identified specific to this level	L2-39
L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.	E3-02 E3-04 E3-72 E3-81 E3-141	Credible corruption of data introduced by manual transfer	None identified specific to this level	L2-01, L2-06, L2-12, L2-13, L2-17, L2-32
		E3-109	Inconsistencies in IAIP introduced by manual transfer	None identified specific to this level	L2-39
		E3-50, E3-53	No requirement for independent double or triple entry of data	None identified specific to this level	L2-32
L3-13	Measures shall be employed to detect AI changes lost during electronic transfer between actors	E3-94, E3-96, E3-98, E3-26	Specific AI change lost in electronic transfer	None identified specific to this level	L2-19, L2-23, L2-29, L2-35
		E3-108	Inconsistencies in IAIP introduced by electronic transfer	None identified specific to this level	L2-39
L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors	E3-95, E3-97, E3-99, E3-27	Specific AI change lost in manual transfer	None identified specific to this level	L2-19, L2-23, L2-29, L2-35

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
		E3-109	Inconsistencies in IAIP introduced by manual transfer	None identified specific to this level	L2-39
L3-15	It shall be possible to trace the originator of any data item	E3-83	Data originator incorrectly identified as authorised source of data	Para 2.3.5, item (3) ED-76	L2-18
L3-16	Data Suppliers shall be RTCA-200A/EUROCAE ED-76 compliant				
L3-17	Raw Data shall be routinely re-surveyed at defined intervals to ensure that AI remains up to date	E3-101, E3-102	AI isolated required changes that have not been made at all by Data Originator	None identified specific to this level	L2-24
			AI required change(s) driven by other changes that have not been made at all by Data Originator	None identified specific to this level	
L3-18	Data Originators shall ensure that all AI changes are notified to the appropriate Data Publication authority	E3-100	Isolated changes that have been made but not provided to publication by DO	None identified specific to this level	L2-26
L3-19	Where multiple manual entry of AI is employed the data sets shall be cross-checked for non-matching entries	E3-38 E3-47	Paper-based register system does not flag unmatched entries	None identified specific to this level	L2-13, L2-32
L3-20	Tools used to cross check manually entered data shall be qualified	E3-48	Electronic-based register system does not flag unmatched entries	Para 2.4.5, ED-76	L2-13, L2-32
L3-21	Contingency procedures shall be defined for performing manual entry with reduced staffing levels to ensure that data integrity is not compromised	E3-49, E3-52, E3-133, E3-128	Lack of/Insufficient resources (to carry out double or triple entry of data into register, generally in a department)	None identified specific to this level	L2-13, L2-32, L2-42, L2-45

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
L3-22	The availability of communications between actors in the Data Chain shall be specified to ensure that AI changes are available prior to the related effective date	E3-114, E3-116, E3-118, E3-120, E3-136, E3-125	Failure of or slow electronic means of communication between (e.g. between DD and DAI, etc)	None identified specific to this level	L2-40, L2-41, L2-43, L2-46, L2-47, L2-52
L3-23	Contingency Procedures shall be in place to ensure critical AI changes are communicated to the next actor in the Data Chain	E3-115, E3-117, E3-119, E3-121	Failure of or slow paper means of communication (e.g. between DD and DAI etc)	None identified specific to this level	L2-40, L2-41, L2-47, L2-52
L3-24	Data Chain actors shall implement procedures to manage workload.	E3-123, E3-124, E3-130, E3-131, E3-132, E3-133, E3-127	Increased workload	None identified specific to this level	L2-42, L2-44, L2-45, L2-43, L2-46
L3-25	Contingency procedures shall be implemented to co-ordinate a reduction in the workload where it is likely to become excessive				
L3-26	Last minute cancellation of announced changes to AI shall be avoided wherever possible	E3-122 E3-134 (L2-42), E3-129 (L2-45)	Last minute changes	ED-76 2.4.2	L2-42, L2-44, L2-45
L3-27	AIS shall maintain an up to date list of subscriber recipients of IAIP	E3-106	Incomplete/corrupted recipients list	None identified specific to this level	L2-60
L3-28	Actors shall establish Service Level Agreements with all other interfacing actors (e.g. between DP and DD).	E3-126 (L2-46), E3-105 (L2-56) E3-137	Lack of co-ordination/co-operation between DD and DP	None identified specific to this level	L2-43, L2-46, L2-56
L3-29	Data Publishers shall state within their SLAs with Data Originators the required Data Quality properties including the timeliness of data.	E3-139	Lack of awareness among Data Originators of the importance of adhering to AIRAC rules	None identified specific to this level	L2-48

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
L3-30	AIS shall use a common geospatial reference system (WGS-84)	E3-104	Different representations of data are used between paper and electronic systems	None identified specific to this level	L2-54
L3-31	AIS shall use a common format for all digital electronic representation of AI[23]	E3-110	No standard electronic representation of IAIPs across States	AIXM [20] (e.g. used by many AIS including EAD) ARINC [19] (e.g. used to specify procedures for Flight Management Systems) eAIP [20] (e.g. used by some AIS)	L2-58
L3-32	States shall ensure that AIS use mandated common electronic IAIP formats	E3-111	States do not adhere to standard electronic representation of IAIPs	AIXM [20] ARINC [19] eAIP [20]	L2-58
L3-33	States shall produce paper copies of all IAIP in accordance with the formats defined in ICAO Annex 15	E3-112	No standard paper representation of IAIPs across States	ICAO Annex 15 provides the standard representation for a paper IAIP	L2-59
L3-34	States shall ensure that AIS use mandated common paper IAIP formats	E3-113	States do not adhere to standard paper representation of IAIPs	ICAO Annex 15 provides the standard representation for a paper IAIP	L2-59
L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.	E3-77	Valid but corrupt obstacle data	Para 2.3.4 item (1), Ed-76 (although not specific to surveyed data)	L2-15
		E3-05, E3-28	Aeronautical data corrupted in terms of absolute accuracy		L2-04, L2-09
L3-36	The probability of an error in any data item shall be less than or equal to the integrity level specified in ICAO Annex 15 Appendix 7	E3-78	Valid but corrupt terrain data	Para 3.2.8, ICAO Annex 15	L2-15
		E3-79	Valid but corrupt data for navigation-related facilities		
L3-37	The probability of an error in any meta data item shall be less than or equal to the integrity level specified for the associated data type in ICAO Annex 15 Appendix 7	E3-29	Credibly corrupted effective dates provided by DO	Para 3.2.8, ICAO Annex 15	L2-09

[23] This requirement is outside the scope of CHAIN, but should be considered as part of regulation.

ID	Requirement	Source FTA Event	Generic Event (pattern)	Existing Spec/Gap	Trace to Level 2
L3-38	Data recipients shall report identified omissions in AI change definitions or missing change definitions to the previous actor in the Data Chain	E3-107	Recipients do not report omitted AI	None identified specific to this level	L2-60
L3-39	Data survey requests shall stipulate deadlines for survey reports	E3-140	Data Origination processes suffer delays	None identified specific to this level	L2-48

F.3.1

Table 7: UDC Level 3 Safety Requirements

APPENDIX G CHAIN SAFETY REQUIREMENTS

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
CH-SR-001	A standard digital format[25] for AI interchange for AIS (e.g. AIXM, eAIP) shall be mandated.	M001	L1-01, L2-58	RR	Regulation	L3-31	AIS shall use a common format for all digital electronic representation of AI[2]
						L3-32	States shall ensure that AIS use mandated common electronic IAIP formats
CH-SR-002	A standard geospatial referencing system shall be mandated and enforced.	M002	L1-01	RR	Regulation	N/A	N/A
CH-SR-003	The scope of ESARR3 shall be extended to include AIS.	M003	L1-02	IC	Regulation	N/A	N/A
CH-SR-004	Specific improvements proposed by CHAIN shall be shown to meet the safety criteria.	M004	L1-02	IC	CHAIN Activity	N/A	N/A
CH-SR-005	The implications for non-achievability of current Data Integrity Levels within Data User applications shall be resolved by Data Users.	M005	L1-02	IC	Data Users	N/A	N/A
CH-SR-006	Regulatory implementing rules shall be shown to meet the safety criteria.	M006	L1-02	IC	Regulation	N/A	N/A
CH-SR-007	A methodology for assigning and demonstrating Data Integrity Levels shall be developed.	M007	L1-02	IC	Regulation	N/A	N/A
CH-SR-008	Requirements for availability of publications, backups and lost data contingency planning shall be defined.	M008	L1-03	RR	Regulation	N/A	N/A
CH-SR-009	Contingency management and co-ordination procedures in the event of resource overload shall be defined and implemented.	M009	L1-04	IC	CHAIN Activity	L3-11	Protection of electronic aeronautical data while stored or in transit shall be totally monitored by the cyclic redundancy check (CRC) as defined in Annex 15 para 3.2.10.
						L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.

[24] Identifies which Safety Criteria is addressed by the requirement :- RR – Risk Reduction or IC Increased Confidence
[25] As opposed to *digitised* format although practicalities of implementation may require more

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
						L3-13	Measures shall be employed to detect AI changes lost during electronic transfer between actors
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
						L3-21	Contingency procedures shall be defined for performing manual entry with reduced staffing levels to ensure that data integrity is not compromised
						L3-24	Data Chain actors shall implement procedures to manage workload.
						L3-26	Last minute cancellation of announced changes to AI shall be avoided wherever possible
CH-SR-010	The following requirement shall be included in ICAO Annex 15: "Measures shall be implemented to minimize the mechanisms through which inconsistency between States IAIPs can arise".	M010	L1-05	IC	Regulation	N/A	N/A
CH-SR-011	Specifications for automated transfer of AI between actors shall include requirements for CRC checking and tool validation to ensure that the probability of data error is reduced by at least two orders of magnitude over triplicate manual transfer.	M011	L2-01, L2-06, L2-12, L2-17, L2-19, L2-23, L2-29, L2-35, L2-40, L2-41, L2-47, L2-52	RR	CHAIN Activity	L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).
						L3-02	Tool validation shall include the impact of hardware failure
						L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.
						L3-11	Protection of electronic aeronautical data while stored or in transit shall be totally monitored by the cyclic redundancy check (CRC) as defined in Annex 15 para 3.2.10.
						L3-13	Measures shall be employed to detect AI changes lost during electronic transfer between actors
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
						L3-22	The availability of communications between actors in the Data Chain shall be specified to ensure that AI changes are available prior to the related effective date
						L3-23	Contingency Procedures shall be in place to ensure critical AI changes are communicated to the next actor in the Data Chain
CH-SR-012	Service Level Agreements (SLAs) between actors shall be defined. (see also CH-SR-029)	M012	L2-60	RR	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-11	Protection of electronic aeronautical data while stored or in transit shall be totally monitored by the cyclic redundancy check (CRC) as defined in Annex 15 para 3.2.10.
						L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.
						L3-13	Measures shall be employed to detect AI changes lost during electronic transfer between actors
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
						L3-17	Raw Data shall be routinely re-surveyed at defined intervals to ensure that AI remains up to date
						L3-22	The availability of communications between actors in the Data Chain shall be specified to ensure that AI changes are available prior to the related effective date
						L3-23	Contingency Procedures shall be in place to ensure critical AI changes are communicated to the next actor in the Data Chain
						L3-25	Contingency procedures shall be implemented to co-ordinate a reduction in the workload where it is likely to become excessive
						L3-28	Actors shall establish Service Level Agreements with all other interfacing actors (e.g. between DP and DD).
						L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.
						L3-36	The probability of an error in any data item shall be less than or equal to the integrity level specified in ICAO Annex 15 Appendix 7

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
CH-SR-013	Any possible mechanisms for AIS to identify absolute accuracy errors shall be identified as far as reasonably practicable.	M013	L2-04	RR	CHAIN Activity	L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.
CH-SR-014	Application of visual checks by AIS shall be mandated.	M014	L2-05, L2-22	IC	Regulation	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
CH-SR-015	Standard procedures for performing visual checks shall be developed.	M015	L2-05, L2-08, L2-10, L2-18, L2-22, L2-30, L2-31, L2-36	IC	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-10	Aeronautical Information integrity checking rules shall comply as a minimum with the EUROCONTROL Business Integrity Rules [ref]
CH-SR-016	Review of IAIP by Data Originators shall be mandated.	M016	L2-07, L2-09, L2-25, L2-26	RR	Regulation	L3-18	Data Originators shall ensure that all AI changes are notified to the appropriate Data Publication authority
						L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
						L3-37	The probability of an error in any meta data item shall be less than or equal to the integrity level specified for the associated data type in ICAO Annex 15 Appendix 7
CH-SR-017	Specification for automated business/integrity checking tools shall be developed such that the probability of detection of data error by the automated application of the rules is increased by at least one order of magnitude or more over manual application of the rules.	M017	L2-08, L2-10, L2-31, L2-36	RR	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-10	Aeronautical Information integrity checking rules shall comply as a minimum with the EUROCONTROL Business Integrity Rules [ref]
CH-SR-018	Robust procedures for manual transfer of AI using double or triple checking shall be developed such that the probability of data error introduced during data entry shall be lower than the probability of errors introduced during single data entry.	M018	L2-10, L2-31, L2-36	RR	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-10	Aeronautical Information integrity checking rules shall comply as a minimum with the EUROCONTROL Business Integrity Rules [ref]
						L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
CH-SR-019	Specifications for automated initial checking of Raw Data shall be developed.	M019	L2-11, L2-34	RR	CHAIN Activity	L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).
						L3-02	Tool validation shall include the impact of hardware failure
						L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.
						L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
CH-SR-020	Specifications for validation of automated tools shall be developed such that the integrity of the tool is assured commensurate to the ICAO Annex 15 integrity level assignment.	M020	L2-03, L2-11, L2-13, L2-20, L2-32, L2-34	RR	CHAIN Activity	L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).
						L3-02	Tool validation shall include the impact of hardware failure
						L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.
						L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.
						L3-19	Where multiple manual entry of AI is employed the data sets shall be cross-checked for non-matching entries
						L3-20	Tools used to cross check manually entered data shall be qualified
						L3-21	Contingency procedures shall be defined for performing manual entry with reduced staffing levels to ensure that data integrity is not compromised
CH-SR-021	Specification for automated Data Preparation procedures shall be developed.	M021	L2-13, L2-32	RR	CHAIN Activity	L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).
						L3-02	Tool validation shall include the impact of hardware failure
						L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.
						L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.
						L3-19	Where multiple manual entry of AI is employed the data sets shall be cross-checked for non-matching entries

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
						L3-20	Tools used to cross check manually entered data shall be qualified
						L3-21	Contingency procedures shall be defined for performing manual entry with reduced staffing levels to ensure that data integrity is not compromised
CH-SR-022	Standard data quality control procedures shall be developed.	M022	L2-14, L2-37, L2-33, L2-38	IC	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
CH-SR-023	Standard AIS quality procedures shall be mandated.	M023	L2-24, L2-37, L2-33, L2-38	IC	Regulation	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
CH-SR-024	Monitoring of data error probabilities shall be introduced at each stage of	M024	L2-15, L2-27,	RR	Regulation	L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
	the Upstream Data Chain (i.e. at Data Origination, Data Publication and Data Distribution).		L2-28			L3-36	The probability of an error in any data item shall be less than or equal to the integrity level specified in ICAO Annex 15 Appendix 7
CH-SR-025	Use of authorised data originators shall be mandated.	M025	L2-16, L2-18, L2-27, L2-28	IC	Regulation	L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.
						L3-36	The probability of an error in any data item shall be less than or equal to the integrity level specified in ICAO Annex 15 Appendix 7
CH-SR-026	Rules for setting up as an aeronautical data provider shall be defined.	M026	L2-16, L2-18	IC	Regulation	L3-35	Surveyed data provided to Data Publication shall be correct, i.e. shall be accurate, of correct resolution, and of correct format.
						L3-36	The probability of an error in any data item shall be less than or equal to the integrity level specified in ICAO Annex 15 Appendix 7
CH-SR-027	Roles and responsibilities for Data Chain actors shall be clearly defined.	M027	L2-16, L2-27, L2-28	RR	Regulation	N/A	No related UDC Level 3 requirement
CH-SR-028	Training procedures for visual checking shall be developed such that the probability of success of carrying out the check by a less experienced but trained person increases by one order of magnitude or more. Develop training procedures for visual checking	M028	L2-05, L2-08, L2-10, L2-18, L2-22, L2-30, L2-31, L2-36	IC	CHAIN Activity	L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).
						L3-02	Tool validation shall include the impact of hardware failure
						L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.
						L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-10	Aeronautical Information integrity checking rules shall comply as a minimum with the EUROCONTROL Business Integrity Rules [ref]

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
						L3-15	It shall be possible to trace the originator of any data item
						L3-16	Data Suppliers shall be RTCA-200A/EUROCAE ED-76 compliant
CH-SR-029	Service Level Agreements shall be mandated. (see also CH-SR-012)	M029	L2-01, L2-15, L2-16, L2-17, L2-19, L2-24 L2-27, L2-28, L2-40, L2-43, L2-47, L2-49	RR	Regulation	L3-13	Measures shall be employed to detect AI changes lost during electronic transfer between actors
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
						L3-17	Raw Data shall be routinely re-surveyed at defined intervals to ensure that AI remains up to date
						L3-22	The availability of communications between actors in the Data Chain shall be specified to ensure that AI changes are available prior to the related effective date
						L3-23	Contingency Procedures shall be in place to ensure critical AI changes are communicated to the next actor in the Data Chain
CH-SR-030	Specifications for automated Data Distribution procedures shall be developed.	M030	L2-03, L2-20	RR	Regulation	L3-01	Tools used to support the preparation or checking of Aeronautical Information shall be validated against the intended use (e.g. as defined in DO-178B).
						L3-02	Tool validation shall include the impact of hardware failure
						L3-03	Tools shall provide internal checking to detect and warn of corruption of AI. Where CRC are applied this shall be in accordance with para 3.2.10 of ICAO Annex 15.
						L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained. 8
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
CH-SR-031	AI changes shall be separately numbered to assist with identification of missing changes.	M031	L2-25	RR	CHAIN Activity	N/A	N/A

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
CH-SR-032	Rules for setting up as a data originator shall be defined.	M032	L2-27, L2-28	IC	Regulation	N/A	N/A
CH-SR-033	It shall be mandated that where NOTAMs are amended the original NOTAM must also be included.	M033	L2-39	RR	Regulation	L3-11	Protection of electronic aeronautical data while stored or in transit shall be totally monitored by the cyclic redundancy check (CRC) as defined in Annex 15 para 3.2.10.
						L3-12	Manual transfer of Aeronautical Information shall be avoided wherever possible. Where deployed, manual transfer shall be sufficiently robust to meet the integrity level of the most critical data handled.
						L3-13	Measures shall be employed to detect AI changes lost during electronic transfer between actors
						L3-14	Measures shall be employed to detect AI changes lost during manual transfer between actors
CH-SR-034	Awareness of Data Originators to AIRAC cycle shall be improved.	M034	L2-43, L2-46, L2-48	IC	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-22	The availability of communications between actors in the Data Chain shall be specified to ensure that AI changes are available prior to the related effective date
						L3-25	Contingency procedures shall be implemented to co-ordinate a reduction in the workload where it is likely to become excessive
						L3-28	Actors shall establish Service Level Agreements with all other interfacing actors (e.g. between DP and DD).
						L3-29	Data Publishers shall state within their SLAs with Data Originators the required Data Quality properties including the timeliness of data.
						L3-39	Data survey requests shall stipulate deadlines for survey reports

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
CH-SR-035	AIS procedures shall be developed to ensure continued safe operation during reduced staffing levels or excessive workload.	M035	L2-42, L2-44, L2-45, L2-48	IC	CHAIN Activity	L3-21	Contingency procedures shall be defined for performing manual entry with reduced staffing levels to ensure that data integrity is not compromised
						L3-24	Data Chain actors shall implement procedures to manage workload.
						L3-26	Last minute cancellation of announced changes to AI shall be avoided wherever possible
						L3-29	Data Publishers shall state within their SLAs with Data Originators the required Data Quality properties including the timeliness of data.
						L3-39	Data survey requests shall stipulate deadlines for survey reports
CH-SR-036	Processes that minimise inconsistencies between IAIPs shall be developed.	M036	L2-51, L2-54	RR	Regulation	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process
						L3-30	AIS shall use a common geospatial reference system (WGS-84)
CH-SR-037	Procedures for consistency checking of all paper and electronic IAIPs shall be developed.	M037	L2-55	RR	CHAIN Activity	L3-04	The skills and knowledge required for each function shall be identified and personnel assigned to perform those functions shall be appropriately trained.
						L3-05	States shall ensure that personnel possess the skills and competencies required to perform specific assigned functions.
						L3-06	Appropriate records shall be maintained so that qualifications of personnel can be confirmed.
						L3-07	Initial and periodic assessments shall be established that require personnel to demonstrate the required skills and competencies.
						L3-08	Periodic assessments of personnel shall be used as a means to detect and correct shortfalls
						L3-09	Procedures shall be defined for all stages of the Data Origination, Publication and Distribution Process

ID	CHAIN Safety Requirement Description	Traces to MTC	Trace (L1/L2)	RR / IC[24]	Owner (who)	UDC L3 Req ID	UDC L3 Requirement
CH-SR-038	Meta-data shall include information on the source and any amendments to data as well as the validity status of the data.	M038	L1-01	RR	CHAIN Activity & Regulation	N/A	N/A
CH-SR-039	Standard format for paper AI interchange for AIS shall be mandated.	M039	L2-59	RR	Regulation	L3-33	States shall produce paper copies of all IAIP in accordance with the formats defined in ICAO Annex 15
						L3-34	States shall ensure that AIS use mandated common paper IAIP formats
CH-SR-040	Specification for automated transfer of IAIP to Data Application/Integration (e.g. automatic translation of AIXM to ARINC) shall be developed.	M040	L2-57	RR	Regulation, States	N/A	N/A
CH-SR-041	Mechanisms shall be developed to facilitate and encourage error feedback from data users.	M041	L2-60	RR	States	L3-27	AIS shall maintain an up to date list of subscriber recipients of IAIP
						L3-38	Data recipients shall report identified omissions in AI change definitions or missing change definitions to the previous actor in the Data Chain

Table 8: CHAIN Safety Requirements

APPENDIX H CHAIN SAFETY ARGUMENT

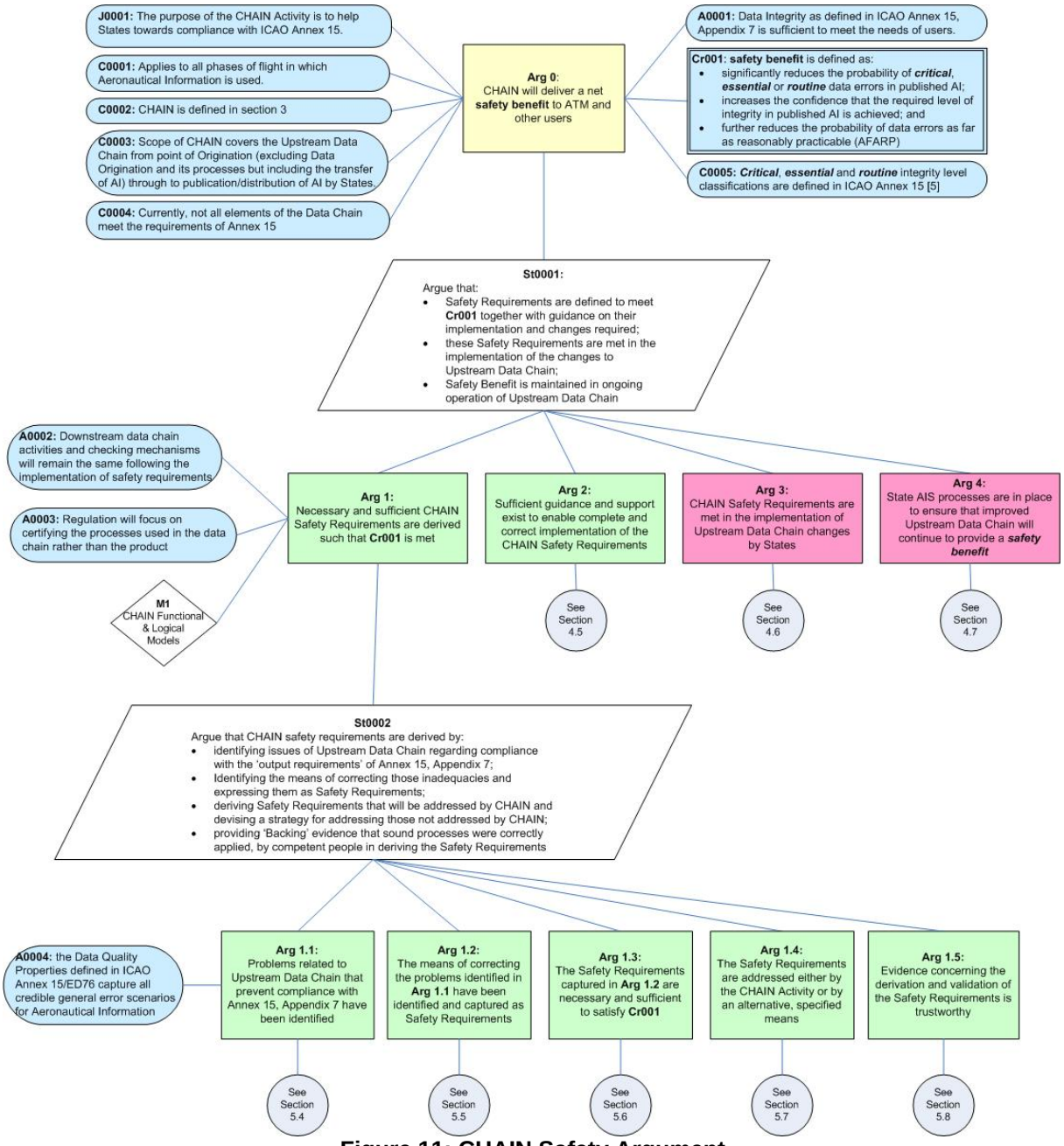
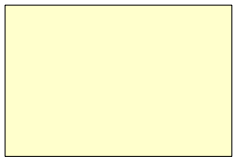


Figure 11: CHAIN Safety Argument

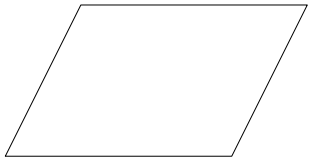
APPENDIX I GOAL STRUCTURING NOTATION (GSN)



Safety Argument Goal (Top level argument)

Safety Argument Goal (sub-argument)

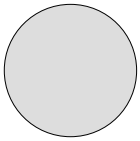
Safety Argument Goal (sub-argument – outside scope)



Safety Argument strategy for achieving the Goal

Criteria to support goal

Assumption/Context/Justification to support goal or strategy



Reference to supporting evidence

APPENDIX J ESARR 4 PROCESS COMPLIANCE

ESARR 4		Compliance Statement
Ref	**Requirement**	
4	Within the overall objective of ensuring safety, the objective of this requirement is to ensure that the risks associated with hazards in the ATM System are systematically and formally identified, assessed, and managed within safety levels, which as a minimum, meet those approved by the designated authority.	The approach satisfies the objective of ESARR 4, section 4, by following a rigorous and systematic safety process documented in the FHA/PSSA Report [9]. All risks associated with identified hazards have been identified, assessed and managed within the safety levels defined in relation to the existing system.
5	An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which:	
5.1a	addresses the complete life-cycle of the constituent part of the ATM System under consideration, from initial planning and definition to post-implementation operations, maintenance and de- commissioning;	Compliant with the lifecycle requirements, but limited, by the scope of the analysis and EUROCONTROL responsibilities as documented in [9], to safety requirements derivation.
5.1b	addresses the airborne and ground components of the ATM System, through cooperation with responsible parties;	Compliant with scope requirements and ATM systems. Cooperation with responsible parties covered during FHA/PSSA Workshop see section 5.8, references [11] and [12].
5.1c	addresses the three different types of ATM elements (human, procedures and equipment), the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM System.	Compliant within scope requirements and at the level of Upstream Data Chain Logical Models as it impacts on the ATM Domain. See section 4.4.
5.2	The hazard identification, risk assessment and mitigation processes shall include:-	
5.2a	a determination of the scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate;	Compliant with context requirements, a rigorous approach has been taken to defining the scope boundaries, interfaces, functions and operational environment. See section 3.4.
5.2b	a determination of the safety objectives to be placed on the constituent part, incorporating :- (i) an identification of ATM-related credible hazards and failure conditions, together with their combined effects, (ii) an assessment of the effects they may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme provided in Appendix A, and a determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects, in a manner consistent with Appendix A;	Compliant with safety objectives process. Identification of hazards together with combined effects documented in FHA/PSSA Report [9]; see also section 5. Cause consequence analyses undertaken using an assumption about the impact in the ATM domain, see assumption A0002 in section 6.2.1
5.2c	the derivation, as appropriate, of a risk mitigation strategy which :-	Compliant with risk mitigation strategy. All mitigations are stated as requirements at the

ESARR 4		Compliance Statement
Ref	**Requirement**	
	(i) specifies the defences to be implemented to protect against the risk bearing hazards, (ii) includes, as necessary, the development of safety requirements potentially bearing on the constituent part under consideration, or other parts of the ATM System, or environment of operations, and (iii) presents an assurance of its feasibility and effectiveness;	system level.
5.2d	verification that all identified safety objectives and safety requirements have been met (i) prior to its implementation of the change, (ii) during any transition phase into operational service, (iii) during its operational life, and (iv) during any transition phase till decommissioning.	Compliant in part with safety requirements satisfaction. The Preliminary Safety Case is limited to safety requirements specification and allocation and the guidance covering implementation by the States to satisfy the requirements.
5.3	The results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures:-	
5.3a	that correct and complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall ATM System are, and will remain, tolerably safe including, as appropriate, specifications of any predictive, monitoring or survey techniques being used;	Compliant with argument requirements. The approach uses Goal Structure Notation (GSN) to help frame a logically consistent and complete argument.
5.3b	that all safety requirements related to the implementation of a change are traceable to the intended operations/functions.	Compliant, traceability is a key feature of the supporting FHA/PSSA Report [9].
A-1	Before the risks associated with introduction of a change to the ATM System in a given environment of operations can be assessed, a systematic identification of the hazards shall be conducted. The severity of the effects of hazards in that environment of operations shall be determined using the classification scheme shown in Figure A-1.	A qualitative assessment has been undertaken and is defined within the FHA/PSSA Report [9]. A severity classification scheme was not used see assumption A0002 in section 6.2.1.
A-2	Safety objectives based on risk shall be established in terms of the hazards maximum probability of occurrence, derived both from the severity of its effect, according to Figure A-1 and from the maximum probability of the hazard's effect, according to Figure A-2.	No probabilistic risk assessment has been carried out for the identified hazards, due to the requirement to demonstrate, where possible, a risk improvement for a process which has had no previous safety assessments carried out.

APPENDIX K ABBREVIATIONS AND ACRONYMS

Acronym/ Abbreviation	Definition
ADI	Aeronautical Data Integrity
ADP	AIS Data Process
AFARP	As Far As Reasonably Practicable
AI	Aeronautical Information
AIC	Aeronautical Information Circular
AIP	Aeronautical Information Publication
AIRAC	Aeronautical Information Regulation And Control
AIS	Aeronautical Information Service
AIXM	Aeronautical Information Exchange Model
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Services
CHAIN	Controlled Harmonised Aeronautical Information Network
DIT	Data Integrity Tool
EAD	European Aeronautical Database
eAIP	electronic Aeronautical Information Publication
EATMP	European Air Traffic Management Programme
ECAC	European Civil Aviation Conference
ESARR	EUROCONTROL Safety Regulatory Requirements
ETA	Event Tree Analysis
FHA	Functional Hazard Assessment
FSR	Functional Safety Requirements
FTA	Fault Tree Analysis
GSN	Goal Structured Notation
IAIP	Integrated Aeronautical Information Package
ICAO	International Convention
NOTAM	Notice to Airmen
PSSA	Preliminary System Safety Assessment
RNAV	Area Navigation
RNP	Required Navigation Performance
SIR	Safety Integrity Requirements
SLA	Service Level Agreement
SRC	Safety Regulatory Commission
UDC	Upstream Data Chain

APPENDIX L REFERENCES

1. Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, 30 April 2004, Edition 2.0
2. EUROCONTROL Safety Case Development Manual, DAP/SAF/091, Edition 2.0 Proposed Issue, 12 September 2005
3. ESARR 4 Risk Assessment and Mitigation in ATM, ESARR4, 05-04-2001, Edition: 1.0
4. EATMP Safety Policy, SAF.ET1.ST01.1000-POL-01-00, Issue 2.0, 09 May 2001
5. International Standards and Recommended Practices – Aeronautical Information, ICAO Annex 15, Edition 12, July 2004
6. Standards for Processing Aeronautical Data, RTCA DO-200A/EUROCAE ED76
7. Industry Requirements for Aeronautical Information, RTCA DO-201A/EUROCAE ED-77
8. Preliminary Safety Impact Study of Controlled Harmonised Aeronautical Information Network – Final Report, AIM/AISD/DI/022, Edition 0.5
9. CHAIN Functional Hazard Assessment/Preliminary Safety Assessment (FHA/PSSA) Report, Issue 0.3, 16th December 2005, P05007.20.2
10. AIS Data Process, EUROCONTROL, AIM/AEP/ADP, Edition 1.0, 15th December 2002, Released Issue
11. Briefing Pack for the FHA/PSSA Workshop, P05007.10.3, 29th July 2005, Issue 1.0
12. Minutes of the FHA/PSSA Workshop (31/08/05 – 01/09/05), P05007.10.5, Issue 0.2, 12th September 2005
13. Aeronautical Information Services Manual, ICAO Doc 8126
14. Use of Safety Management Systems by ATM Service Providers, ESARR 3, Edition 1.0, 17 July 2000
15. Software in ATM Systems, ESARR 6, Edition 1.0, 06 November 2003
16. CHAIN Overview, Technical Note, EUROCONTROL, DAP/NET/CHAIN/007
17. Single European Sky (SES) Regulations, Regulatory Approach for the Aeronautical Data Integrity, EUROCONTROL, Released Edition 1.1, January 2006
18. AIS Data Process, EUROCONTROL, Edition 1.0, 15th December 2002, Released Issue
19. AEEC, ARINC Specification 424, Navigation System Data Base
20. European Organization for the Safety of Air Navigation – EUROCONTROL. AIXM XML Primer. 1.1 ed. EATMP-021001-01, January 10, 2002
21. European Organization for the Safety of Air Navigation – EUROCONTROL. eAIP (Electronic Aeronautical Information Publication), http://www.EUROCONTROL.int/eaip