AEROMACS - Safety Analysis

Document information	
Project Title	Airport Surface Datalink
Project Number	15.02.07
Project Manager	INDRA
Deliverable Name	AEROMACS - Safety Analysis
Deliverable ID	D08.1
Edition	00.01.00
Template Version	03.00.00
Task contributors	
AENA, AIRBUS, DSNA (TASK LEADER), EUROCONTROL, INDRA, SELEX ES, THALES	

Abstract

This deliverable has been developed by SESAR Project 15.2.7 "Airport Surface Data Link within WA8 "Safety and Security Analysis" that aims at performing an extensive analysis to identify the impact on security and safety issues of the new IEEE 802e/aero datalink.

This document consist of part 1 of the deliverable, addressing safety and performance analysis defining the requirements to be considered to implement and operate AeroMACS service.

Authoring (D08-Part1)

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] ALTRAN for DSNA/DTI	[redacted]	17/02/2014
[redacted] ALTRAN for AIRBUS		17/02/2014
[redacted] AIRBUS		17/02/2014
[redacted] DSNA/DTI		17/02/2014

Document History (D08-Part1)

Edition	Date	Status	Author	Justification
00.00.01	04/07/2011	Draft	DSNA/DTI	Draft deliverable submitted to WA08 contributors
00.00.02	07/10/2011	Draft	DSNA/DTI	New version addressing partners comments
00.00.03	03/05/2012	Draft	DSNA/DTI	New version including functional description of ground system and requirements apportionment
00.00.04	11/05/2012	Draft	DSNA/DTI + AIRBUS	New version including apportionment of requirements to Airborne system and implementing update of WG78/Sc214 changes
00.00.05	15/05/2012	Draft	DSNA/DTI	Draft deliverable submitted to WA08 contributors and WG82
00.00.06	21/06/2012	Draft	DSNA/DTI	Draft deliverable addressing partners and WG82 comments
00.00.07	06/12/2012	Draft	DSNA/DTI	Draft deliverable addressing change in WG78/Sc214 additional requirements
00.00.08	17/02/2014	Draft	DSNA/DTI	Final draft submitted to WA08 partners and ICAO
00.00.09	26/03/2014	Draft	DSNA/DTI	Final version for handover addressing comments
00.01.00	28/03/2014	Final	INDRA	Final version for Hand-Over

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

AeroMACS is a new aviation-dedicated transmission technology, based on the WiMAX IEEE 802.16e standard, and aiming at supporting Datalink communications. This document is the safety and performance analysis defining the requirements to be considered to implement and operate AeroMACS service.

Methodology applied for this analysis consists in three main steps:

First, the WG78/SC214 safety and performances requirements applicable to ACSP and aircraft, and suitable for AeroMACS, are defined. To that purpose, a bottom-up analysis, based on possible failures of the AeroMACS, considering the different context of use and external mitigation means, is carried-out.

Then, AeroMACS ground system requirements are declined from ACSP safety and performance requirements identified during the first step. The functional architecture of the ACSP, including the AeroMACS ground system, is defined and requirements are apportioned on the different parts of this architecture.

In the same way, AeroMACS airborne system requirements are declined from aircraft safety and performance requirements identified during the first step. The functional architecture of the aircraft, including the AeroMACS airborne system, is defined and requirements are apportioned on the different parts of this architecture.

The apportionments on AeroMACS ground system are based on assumptions regarding the architecture and the reliability of the ACSP components. Consequently, this analysis defines recommendations rather than requirements on AeroMACS ground system (only allocations coming from WG78/SC214 are considered as requirements). These recommendations are qualitative and quantitative and relates to availability, transaction time, software assurance level, monitoring and alert.

The apportionments on AeroMACS airborne system are qualitative and quantitative requirements relating to development assurance level, availability, likelihood of corruption, misdirection or loss of message, transaction time, monitoring and alert.

1 Introduction

1.1 Purpose of the document

AeroMACS is a new aviation-dedicated transmission technology based on the WiMAX IEEE 802.16e standard. The aim is to support safety and regularity of flight communications with mobile (aircraft and airport vehicles) at the airport surface. The AeroMACS technology allows MSs (Mobile Stations) such as aircraft or surface vehicles to communicate with airline operators and airport staff at three different surface zones: RAMP (where the aircraft is at the gate before departure), GROUND (the aircraft is taxing to the runway), and TOWER (until the aircraft takes-off).

NOTE: In some countries, AeroMACS can be used for communication with fixed subscribers for ATC and Airport operations.

Using a WiMAX-based technology standard is profitable for the aviation industry for many reasons. First, the standardization and deployment processes are fast and cost-effective at the opposite of a newly developed standard for the sake of airport communications. Moreover, the scientific community has been working on IEEE 802.16 standards since many years. Highly qualified certification agencies such as the WiMAX Forum are continuously looking after interoperability and technical issues related to the standard. The AeroMACS standard is currently a hot topic in datalink communications and many tests are already running their way for a future deployment. For instance, an AeroMACS profile was recently developed jointly by the RTCA SC-223 and EUROCAE WG-82 and intended to provide performance requirements for the system implementation.

This document presents an analysis of safety and performances requirements which could be applicable to the AeroMACS system as an enabler for ATC related Datalink services. This analysis is done in the frame of the SESAR project P15.2.7 which aims at developing and validating the AeroMACS system.

In order to derive safety and performances requirements or recommendations, a detailed analysis of Safety and Performance Requirements draft documentation developed by the joint Eurocae/RTCA group WG78/SC214 has been done. The requirements identified are then further apportioned to the different boxes taking part to the AeroMACS system.

NOTE: The present safety and performance analysis for AeroMACS started before P16 issued its conclusions. At that time, only two sources of information were available: COCR and WG78 draft deliverables. It was decided to base D08 of P15.2.7 on WG78 draft deliverables since it was the most complete documentation: detailed safety and performance analysis of DATALINK services were being under development. In addition, WG78/SC214 developped documentation based on EUROCAE ED-78A/ RTCA DO-264 which has also been recognized as an appropriate methodology to develop ED-120 (reference SPR for IR on DLS) and ED-122.

1.2 Document Structure

Chapter 1 is the introduction of the document

Chapter 2 is the preamble of the document, presenting the system, the environment and the Datalink services considered in the analysis

Chapter 3 presents the methodology of the safey and performance analysis.

Chapter 4 presents the results of the definition of safety and performance requirements. Particularly, paragraph 4.1 presents the results of the definition of safety requirements, paragraph 4.2 presents the results of the definition of performance requirements and paragraph 4.3 summarizes the safety and performance requirements applicable to aircraft and ACSP.

Chapter 5 presents the allocation of safety requirements on AeroMACS ground components

Chapter 6 presents the allocation of safety requirements on AeroMACS airborne components

Chapter 7 presents the list of assumptions considered during the analysis

Chapter 8 presents the references of the analysis

Appendix A present the hazard classification matrix considered for the severity classification of the operational hazards

Appendix B contains the Excel file allowing the identification of operational hazards

Appendix C lists the differences between Issue I and Issue M of WG78/SC214 documents

1.3 Intended readership

This document can be used by manufacturers developing AeroMACS system and service providers who could operate such system. Since AeroMACS can be used for ATC Datalink services, manufacturers shall pay attention to the Safety and Regularity of flight objectives which are inherent to such type of services. In this document, manufacturers and service provider will get a list of ATC Datalink services which could be supported by the AeroMACS system and derived Safety and Performance recommendations.

1.4 Background

This section identifies previous work on the subject covered by the document. A special emphasis on what is reused from another project or from past-project will be appreciated.

1.5 Acronyms and Terminology

Term	Definition
AC	Aircraft
ACSP	Air Ground Communication Service Provision
AE	Abnormal Event
APR	AeroMACS Performance Requirement
AR	AeroMACS Requirement
ASN	Access Service Network
ASR	AeroMACS Safety Requirement
ATM	Air Traffic Management
ATSU	Air Traffic Service Unit
CR	Component Requirement
CU	Context of Use
DM	Downlink Message (message from the aircraft to the ground)
EMM	External Mitigation Means

Term	Definition
E-ATMS	European Air Traffic Management System
OH	Operational Hazard
PR	Performance Requirement
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency.
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SO	Safety Objectives
SOH	Sector Operational Hour
SR	Safety Requirement
UM	Uplink message (message from the ground to the aircraft)
WG78	Working Group 78 : Standards for Air Traffic Data Communication Services

2 Preamble

The AeroMACS system should be able to support the following types of services at the airport's surface:

- ATC communication between Aircraft and ATC centers
- AOC/AAC communication between Aircraft and Airlines operation centers
- Communication between Airport operator and Ground vehicles to optimize surface operation.

The following analysis focus on the Safety and Performance requirements related to ATC services provided to Aircraft. AOC, AAC services and communication with ground vehicles are not addressed for the following reasons:

- It is assumed that Safety (if any) and Performance requirements related to AOC and AAC services are less stringent than those related to ATC Datalink services. This assumption seems to be validated with regards to the result of the AOC Communication Study done in the frame of SESAR.
- For communication with ground vehicles, there is no clear operation concept at this moment in time, it is thus very difficult to derive any Safety and Performance requirements related to such type of services.

2.1 System in its environment

The following figure presents the CNS/ATM system as it is defined in Working Group 78 documents. It includes the following elements:

- Flight Crew
- Aircraft System
- Air Ground Communication Service Provision (ACSP): Base stations + ASN Gateway + AAA server + routing infrastructure…
- Air Traffic Service Unit (ATSU)
- Controller

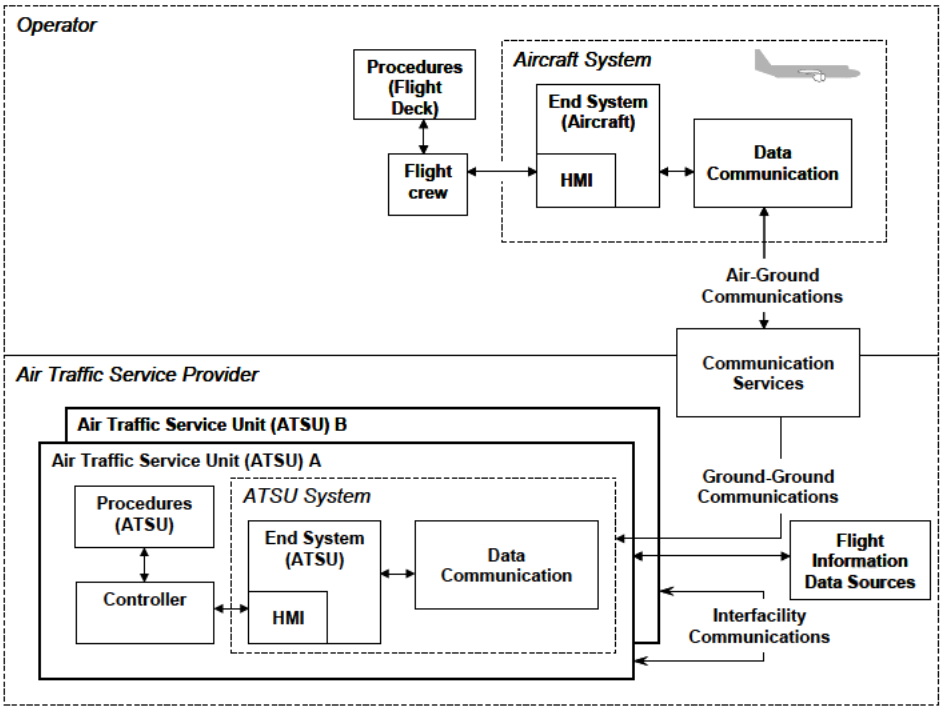


Figure 1 : Overview of CNS/ATM System as defined by WG78

The AeroMACS system is part:

- on the airborne side of the data communication domain : Antenna + AeroMACS mobile system
- on the ground side of the communication service domain (ACSP): Base stations + ASN Gateway + AAA server…

NOTE: The COCR presents the following model for the Air-Ground communication infrastructure. It defines Future Radio System (FRS) as the physical implementation of the radio components of a communication system. The FRS is part of the overall Future Communication Infrastructure (FCI), which includes all the components needed for the Air Navigation Service Provider and aircraft to communicate with each other.

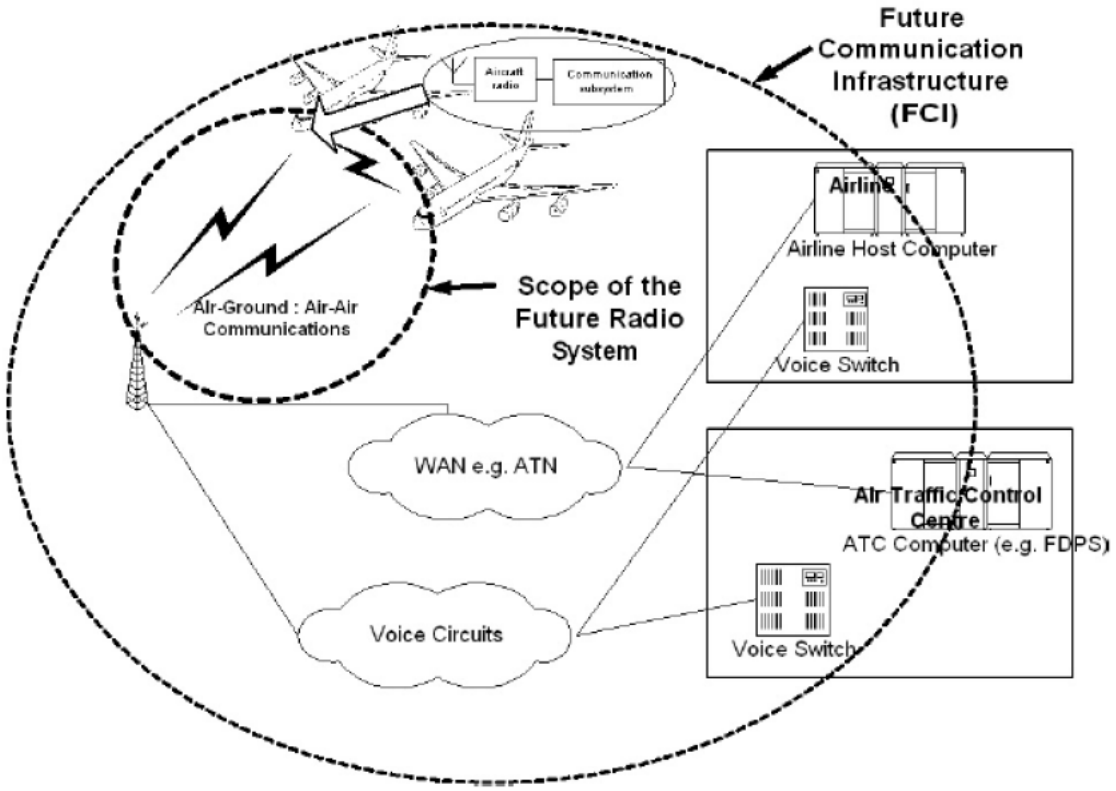


Figure 2 : Overview of CNS/ATM System as defined in COCR

To follow such model, AeroMACS is one of the Airport Component of this Future Radio System.

2.2 Considered environment

As presented in chapter 3, this document is based on the safety and performance analysis performed by the joint group WG78/SC214.

The reference documents that are used for this analysis are:

- CPDLC Operational Safety Analysis Issue I: document "PU-10_SPR-I_AnnexB-CPDLC-OSA_1-Feb_2012"
- ADS-C Operational Safety Analysis Issue I: document "PU-10_SPR-I_AnnexC-ADS-C-OSA_1-Feb_2012"
- D-FIS Operational Safety Analysis Issue H: document "SPR-H-AnnexD-FIS-OSA_Feb3"
- Operational Performance Analysis Issue I: document "PU-10_SPR-I-AnnexesEFGH-OPA-1-Feb_2012"

NOTE: New issue of WG78/SC214 documents is available. Differences between this issue of the documents and the current issue (issue M) are presented in Appendix C.

"WG78 environment" for Airport domain is described in WG78 documents. The main characteristics of this environment are described below:

	Characteristics in Airport Domain
Data communication	75% of aircraft are equipped with data communications

	Characteristics in Airport Domain
equipage	
Aircraft flight duration per sector	20.5 minutes
Average aircraft count per sector (during busy hour)	61 (19 Ramp, 31 Ground, and 11 Tower
Peak instantaneous aircraft count per sector	96 (30 Ramp, 48 Ground, and 18 Tower)
Aircraft handled per sector hour	179

Table 1: Characteristics of WG78 Environment

From a safety point of view it is important to note that this environment considers the existence of **sophisticated automation tools for problem detection, resolution advisories and prioritization** to assist the controller.

2.3 Datalink services considered for the analysis

Aeronautical Operational Control (AOC) and AAC services are not considered in the present safety and performance analyses for the following reasons:

- AOC services are mainly used to exchange information between the aircraft and the airlines (for example to prepare / optimize the maintenance of the aircraft). They are not considered in Working Group 78 documents,
- From a safety point of view, AOC services are usually deemed less critical than ATS services. So safety requirements defined by considering the ATS services should be more stringent than safety requirements that could be defined by considering AOC services,
- From a performance point of view, it is considered that performance requirements defined in WG78 document for ATS services are sufficient to use AOC services efficiently.

WG78 documents define the following Air Traffic Services (ATS) services at the airport's surface:

- **DLIC** (DataLink Initiation)
  - Definition: This service exchanges information between an aircraft and an ATSU to identify the data link services that are supported. The DLIC service is also used to establish a unique identity address for each aircraft initiating the connection process. It provides version and address information for all data link services including itself.
  - Airport utilization: The DLIC service is executed prior to any other addressed data link service.
  - Application: This service uses CM application.
- **ACM** (ATC Communication Management)
  - Definition: This service provides automated assistance to the flight crew and current and next controllers for conducting the transfer of ATC communications.
  - Airport utilization: The ACM service is intended to be used in all phases of flight and surface operations
  - Application: This service uses CPDLC application.
- **CRD** (Clearance Request and Delivery)
  - Definition: This service supports operational ATC data communication (clearance request, delivery and response) between the flight crew and the ground system/controller of the current data authority ATSU.

- Airport utilization: This service is intended to be used in all phases of flight and surface operations
- Application: This service uses CPDLC application.

- **IER** (Information Exchange and Reporting)
  - Definition: This service provides the capability for the controller and flight crew to exchange information (reports/confirmation messages, automatic report provided by aircraft, request for information on expected clearances...).
  - Airport utilization: This service can be used in all flight phases. In practise, it is not sure that it is really used in Airport.
  - Application: This service uses CPDLC and ADS-C application.
- **AMC** (ATC Microphone Check)
  - Definition: This service provides controllers with the capability to uplink an instruction to an aircraft in order for the flight crew to check that the aircraft is not blocking a given voice channel.
  - Airport utilization: The ACM service is intended to be used in all phases of flight and surface operations
  - Application: This service uses CPDLC application.
- **PR** (Position Reporting)
  - Definition: This service provides the controller with the capability to obtain position information from the aircraft. PR is intended only for position reports. When the aircraft sends reports associated with re-routing, these reports are sent via IER.
  - Airport utilization: This service can be used in all flight phases. WG78 specifies that “typically, position reports are sent when passing waypoints on oceanic tracks”. So this service is not considered as used in Airport domain.
  - Application: This service uses CPDLC and ADS-C application.
- **DCL** (Departure Clearance)
  - Definition: This service provides automated assistance for requesting and delivering departure clearances.
  - Airport utilization: The DCL service is intended for use during the surface departure phase of operation.
  - Application: This service uses CPDLC application.
- **D-TAXI** (DataLink Taxi)
  - Definition: This service provides communications between the flight crew and the ATSU system/controller during ground operations, and while the aircraft is approaching the airport. This service is not used to provide clearances related to active runways and take off clearances, which are provided by voice.
  - Airport utilization: The D-TAXI service is intended for use during ground operations, and while the aircraft is approaching the airport.
  - Application: This service uses CPDLC application.
- **4D-TRAD** (4-Dimensional Trajectory Data Link)
  - Definition: The 4DTRAD service enables the negotiation and synchronization of trajectory data between ground and air systems. This includes the exchange of 4-dimensional clearances and intent information such as lateral, longitudinal, vertical

and time or speed (including uplinked constraints specified as cleared speed / time constraints which can be issued as a part of a route clearance).

- Airport utilization: During the pre-departure, the 4D-TRAD trajectory is loaded in the Flight Management System automatically. The proposed 4-D trajectory portion will be used later in the flight to facilitate negotiation of the aircraft's final 4-D trajectory
- Application: The 4DTRAD service uses CPDLC for exchange of 4D clearances; and ADS-C for estimated trajectory downlink, from the aircraft to the ground.

- **IM** (Interval Management)
  - Definition: Currently, this service is not clearly defined in WG78.This service provides automated assistance to perform ITP (In Trail Procedures), Merging and Spacing (M&S), Crossing and Passing (C&P) or Paired Approach (PAIRAPP). , delegated separation services.
  - Airport utilization: All these procedures are only performed during En Route. This service is not used in Airport domain.
- **OCL** (Oceanic Clearance)
  - Definition: This service provides the capability to request and obtain oceanic clearances from ATSUs that are not yet in control of the aircraft.
  - Airport utilization: This service is not used in Airport domain (only used in En Route environment).
  - Application: This service uses CPDLC application.
- **D-OTIS** (DataLink Operational Terminal Information)
  - Definition: This service provides flight crews with compiled meteorological and operational flight information for aerodromes comprised of ATIS (Automatic Terminal Information Service), NOTAM (Notice To Airmen), and VOLMET (including Aerodrome Routine Meteorological (METAR), Aerodrome Special Meteorological (SPECI), Terminal Aerodrome Forecasts (TAF) and Significant Meteorological Forecast (SIGMET)).
  - Airport utilization: The overall service is available in all phases of flights including pre-departure. For the landing, "Operational Terminal Information" is necessary before the beginning of the approach procedure. The service is only used in Airport before takeoff.
  - Application: This service uses FIS application.
- **D-RVR** (DataLink Runway Visual Range)
  - Definition: This service provides flight crews with Runway Visual Range (RVR) information for aerodromes during periods of low visibility.
  - Airport utilization: The D-RVR service is available in all phases of flights, including pre-departure. For the landing the visual range information is necessary before the beginning of the approach procedure. This service is only used in Airport before takeoff.
  - Application: This service uses FIS application.
- **D-HZWX** (DataLink Hazardous Weather)
  - Definition: This service provides flight crews with flight critical weather information which may affect the safety of aircraft operations. The D-HZWX service includes the following report types: Data Link Wind Shear (D-WS), Data Link Micro Burst (D-MB), Data Link Special Air Reports (D-SAR), Data Link Significant Meteorological Information (D-SIGMET), Data Link Wake Vortex Reports (D-WVR).

- Airport utilization: The overall service is available in all phases of flights, including pre-departure. For the landing the weather information is necessary before the beginning of the approach procedure. This service is only used in Airport before takeoff.
- Application: This service uses FIS application.

Services that are not used in Airport are: IM, OCL and PR. All the other services will be considered in the present safety and performance analysis.

In consistence with WG78 document, the safety analysis is performed at application level: consequences of AeroMACS failures are linked to hazards at application level instead of hazards at services level.

The following assumptions are related to application/services considered in safety analysis:

- **ASSUMP-AEROMACS_01**: Context Management (CM) application is not considered during the identification of Operational Hazards.

  Justification: Consistent with WG78/SC214 approach: a failure during Datalink initiation doesn't have direct operational effects. However it can have effects during the use of the others applications (CPDLC, ADS-C and FIS). So the safety requirements concerning CM messages are determined by studying all the other applications.

- **ASSUMP-AEROMACS_02**: No specific safety analysis is carried out for 4D-TRAD service.

  Justification: 4D-TRAD uses both CPDLC and ADS-C applications. It is considered that 4D-TRAD do not drive more stringent requirements on CPDLC and ADS-C applications than other CPDLC and ADS-C services. This assumption will be validated when 4D-TRAD OSA will be published.

- **ASSUMP-AEROMACS_03**: Services D-RVR and D-HZWX are not taken into account when considering the FIS application in the safety analysis.

  Justification: WG78 OSA concerning FIS application only considers D-OTIS service. Other OSA are currently in process concerning services D-RVR and D-HZWX.

  These services could be added later if necessary.

Based on these considerations, following table presents the applications that are taken into account in the present document and the related services.

Application		Services considered in safety analysis		Used in APT domain	Covered by WG78	Addressed in present document
CM	Context Management	DLIC	DataLink Inititation	X	X	X
CPDLC	Controller Pilot DataLink Communication	ACM	ATC Communication Management	X	X	X
		CRD	Clearance Request and Delivery	X	X	X
		AMC	ATC Microphone Check	X	X	X
		DCL	Departure Clearance	X	X	X
		D-TAXI	DataLink Taxi	X	X	X
		4DTRAD	4-Dimensional Trajectory Data Link	X		X
		IER	Information Exchange and Reporting	X	X	X
		PR	Position Reporting		X	
		IM	Interval Management		X	
		OCL	Oceanic Clearance		X	
ADS-C	Automatic Dependent	4DTRAD	4-Dimensional Trajectory Data Link	X		X
		IER	Information Exchange and Reporting	X	X	X

Application		Services considered in safety analysis		Used in APT domain	Covered by WG78	Addressed in present document
	Surveillance	PR	Position Reporting			
		IM	Interval Management			
FIS	Flight Information Service	D-OTIS	DataLink Operational Terminal Information	X	X	X
		D-RVR	DataLink Runway Visual Range	X		
		D-HZWX	Data Link Hazardous Weather	X		

Table 2: Application considered for the safety analysis in WG78 environment

NOTE: More precisions regarding Datalink applications and services can be found in WG78/SC214 documentation.

3 Methodology

The methodology to derive Safety and Performance requirements applicable to the AeroMACS system is described below:

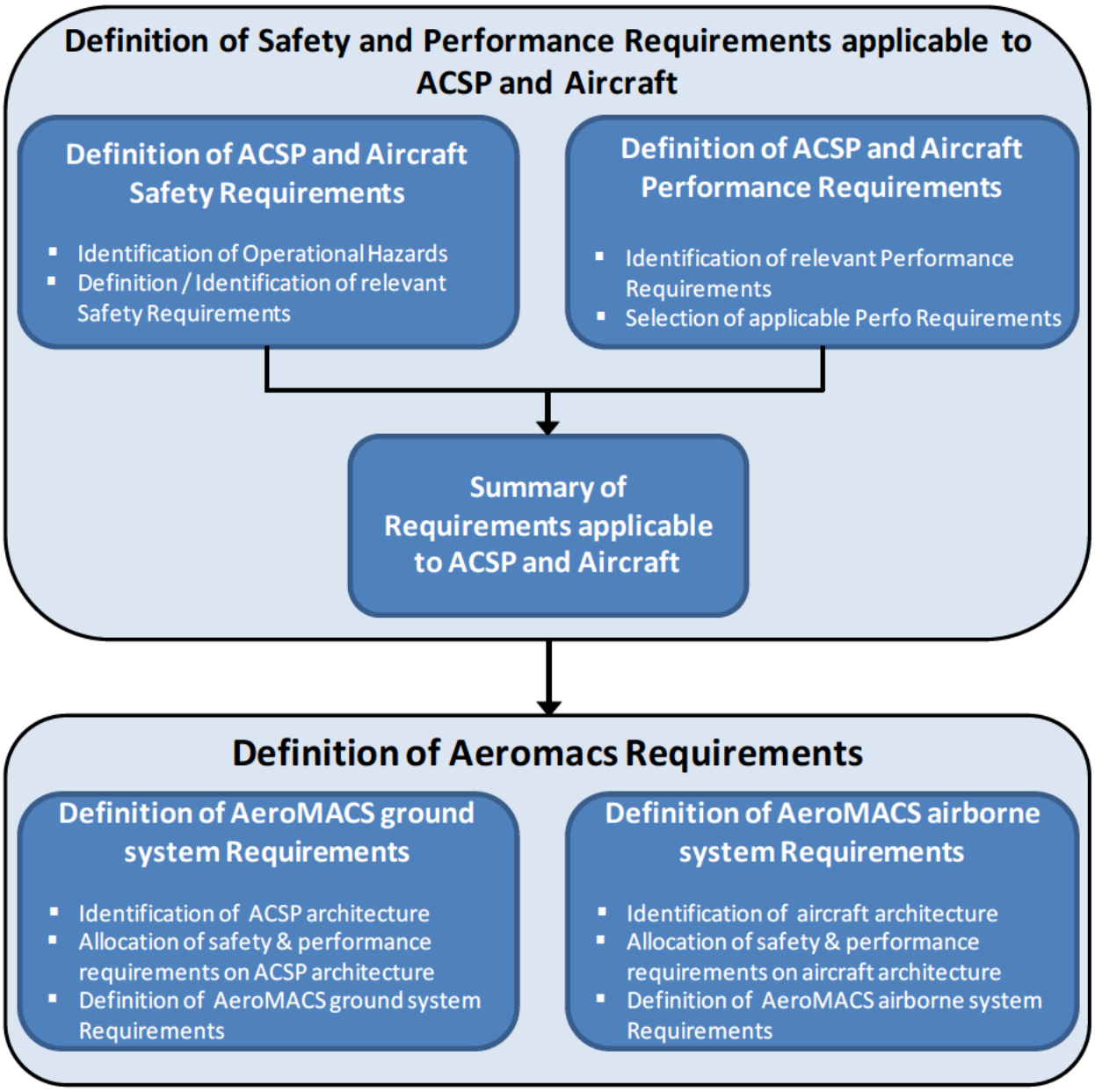


Figure 3 : Methodology for Safety and Performance analysis

As it appears on this figure, this analysis includes two main tasks:

- The Identification of requirements applicable at Aircraft and ACSP level (since these two domains contain parts of the AeroMACS). This task consists in a safety and performance analysis, based on WG78/SC214 draft documentation, aiming at determining the suitable list of requirements for the AeroMACS. The detailed methodology of this task is presented in § 3.1.

- The apportionment of requirements applicable to the Aircraft and ACSP domain to the AeroMACS system. This task aims at deriving hardware, software and operation requirements applicable at AeroMACS level. The detailed methodology of this task is presented in § 3.2.

3.1 Definition of Safety and Performance Requirements applicable to ACSP and Aircraft

As presented on figure 3, two analyses are performed in order to determine ACSP and Aircraft Requirements: safety analysis and performance analysis. These two analysis are carried out independently to determine Safety Requirements and Performance Requirements.

The following sections presents the methodology for the definition of Safety Requirements (§ 3.1.1) and Performance Requirements (§ 3.1.2).

3.1.1 Definition of Safety Requirements

The safety analysis includes two sub-tasks:

- Identification of Operational Hazards,
- Definition of relevant Safety Requirements

The principle of these two sub-tasks is presented in the following chapters.

3.1.1.1 Identification of Operational Hazards

This task is a qualitative bottom up analysis with the purpose to identify all the Operational Hazards associated to AeroMACS. Operational Hazards are consequences, on the global ATM system, of the AeroMACS failures (Abnormal Events). Abnormal Events can have different consequences depending on the Context of Use (CU) and on the success or failure of external mitigations means (in others systems).

The principle of this task is presented on the following figure.

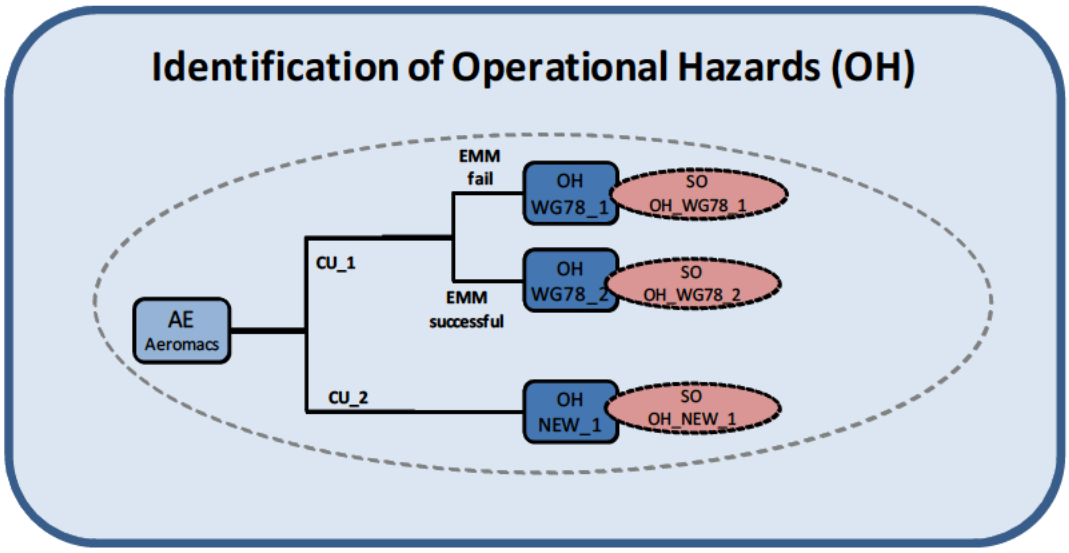


Figure 4 : Methodology for the identification of Operational Hazards

This identification is composed of five main sub-tasks:

- Identification of Abnormal Events at AeroMACS Level
- Identification of all Contexts of Use and External Mitigation Means associated to each Abnormal Event
- Identification of all Operational Hazards associated to each Abnormal Event
- Evaluation of severities associated to new Operational Hazards

- Definition of safety objectives associated to new Operational Hazards

The detailed methodology and the results associated to these different sub tasks are presented in § 4.1.1.

3.1.1.2 Definition / Identification of relevant ACSP and A/C Safety Requirements

Safety Requirements can be defined for the different components of the ATM system (Controller, Flight Crew, Aircraft System, Air Ground Communication System or Ground System) from the Operational Hazards / Safety Objectives identified during the previous task.

As presented in paragraph 2.1, AeroMACS is split between Aircraft System and ACSP. So, only the requirements applicable to the Aircraft system (AC) and to the Air Ground Communication System (ACSP) are considered as relevant for the AeroMACS.

The definition of the relevant ACSP or AC Safety Requirements is different depending on the kind of Operational Hazard:

- for “WG78 OH”, an allocation has already been performed by WG78. So ACSP and AC safety requirements are directly extracted from WG78 documents.
- for “NEW OH”, the complete allocation must be performed from the Operational Hazard to the different causes including ACSP or AC.

Then, for a given failure mode (eg: Loss of message or corruption of message), only the most stringent safety requirements are selected as being the applicable safety requirements.

The principle of this task is presented on the following figure.

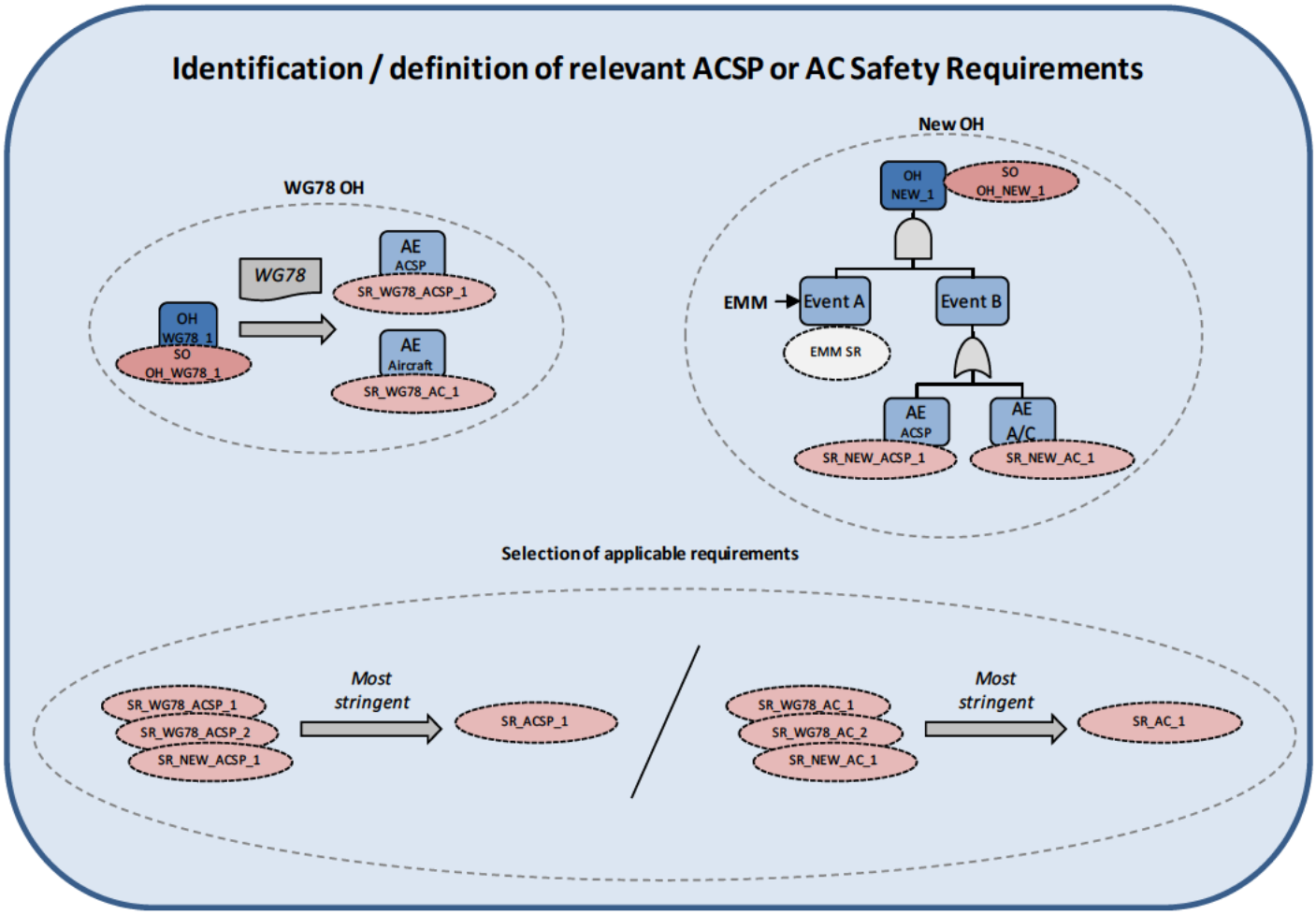


Figure 5 : Methodology for the definition / Identification of relevant ACSP or AC safety requirements

The detailed methodology and the results of this task are presented in § 4.1.2.

3.1.2 Definition of Performance Requirements

The performance analysis includes two sub-tasks:

- Identification of relevant Performance Requirements,
- Selection of applicable Performance Requirements

The principle of these two sub-tasks is presented on the following figure. More details are given in the following chapters.

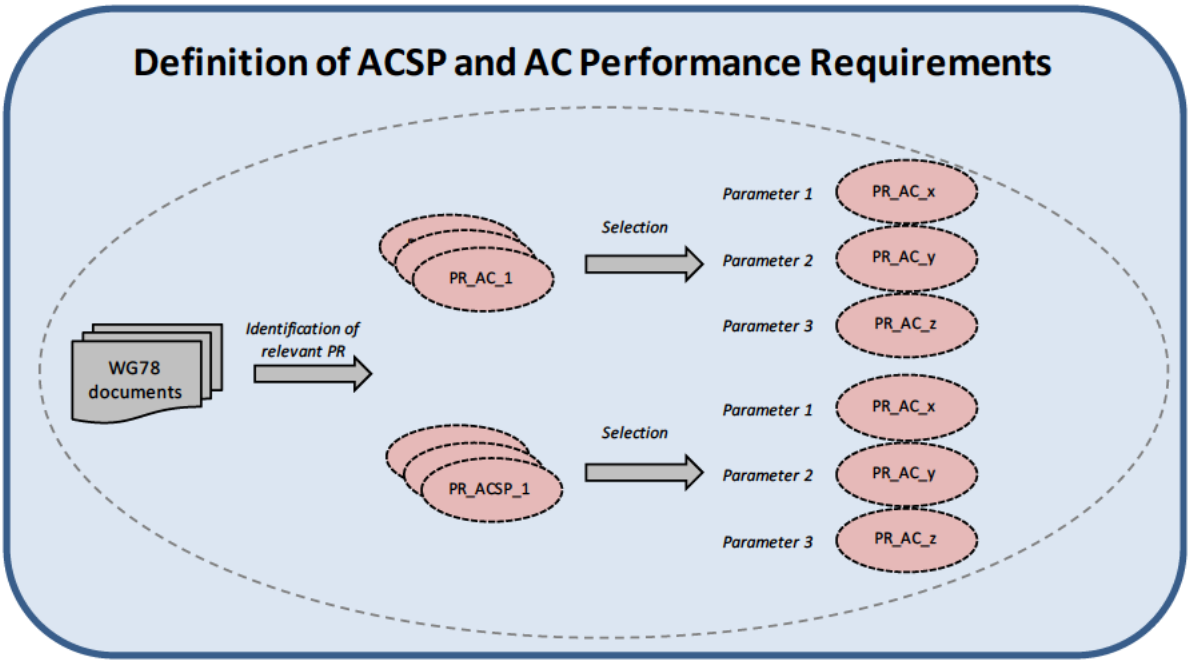


Figure 6 : Methodology for the definition of ACSP and AC Performance Requirements

3.1.2.1 Identification of relevant Performance Requirements in WG78 documents

WG78 has defined Performance requirements for the different components of the ATM system: Controller, Flight Crew, Aircraft System, Air Ground Communication System (ACSP) and Ground System.

As presented in paragraph 2.1, AeroMACS is split between Aircraft System and ACSP. So, only the performance requirements applicable to the Aircraft system (AC) and to the Air Ground Communication System (ACSP) are considered as relevant for AeroMACS.

This task consists in identifying, in the WG78 documents, all the performance requirements allocated to the Aircraft system or to the ACSP and concerning the transmission of messages between ground and aircraft or vice versa.

The results of this task are presented in § 4.2.1.

3.1.2.2 Selection of applicable ACSP and AC performance requirements

Different performance requirements can be defined, in the WG78 document, for a same performance parameter (for example continuity of service) and identified in the previous task. Consequently, this task consists in selecting, for each parameter, the most stringent performance requirement, that is the applicable performance requirement for this parameter.

The results of this task are presented in § 4.2.2

3.1.3 Selection of ACSP and AC Requirements

When a safety requirement (SR) and a performance requirement (PR) have been defined for a same parameter (e.g. availability) a comparison is performed between these two requirements and the most

stringent is selected as being the applicable Requirement for this parameter. This principle is presented on the following figure:

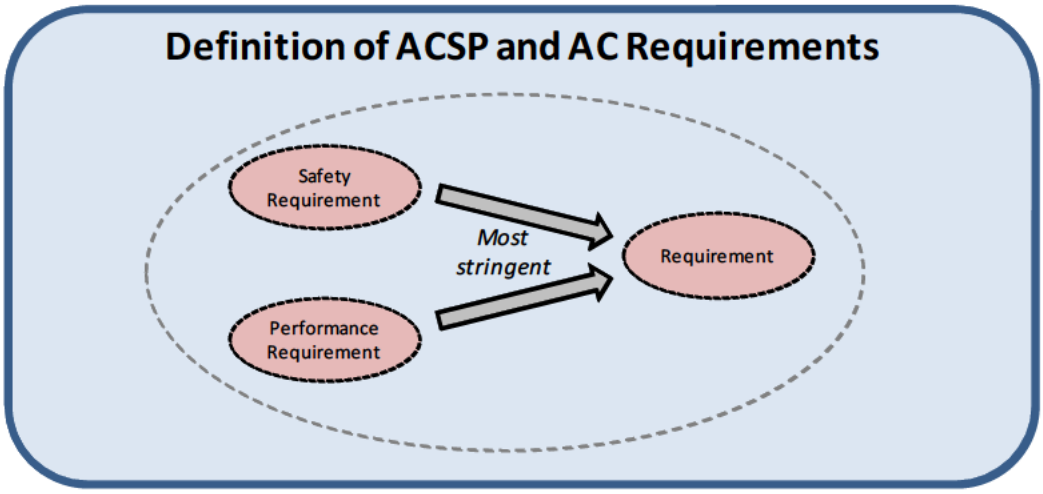


Figure 7 : Methodology for the selection of ACSP and AC Requirements

The results of this task are presented in § 5.

3.2 Definition of AeroMACS Requirements

The definition of AeroMACS Requirements is carried out independently for AeroMACS ground and airborne system: ACSP requirements drive requirements on AeroMACS ground system and Aircraft requirements drive requirements on AeroMACS airborne system.

For each part (airborne and ground), the same sub-tasks are performed:

- Identification of ACSP (or Aircraft) architecture
- Allocation of ACSP (or Aircraft) requirements on the different parts of ACSP (or Aircraft), including AeroMACS ground system (or AeroMACS airborne system)
- Definition of AeroMACS ground system Requirements

The principle of these three sub-tasks is presented on the following figure. More details are given in the following chapters.

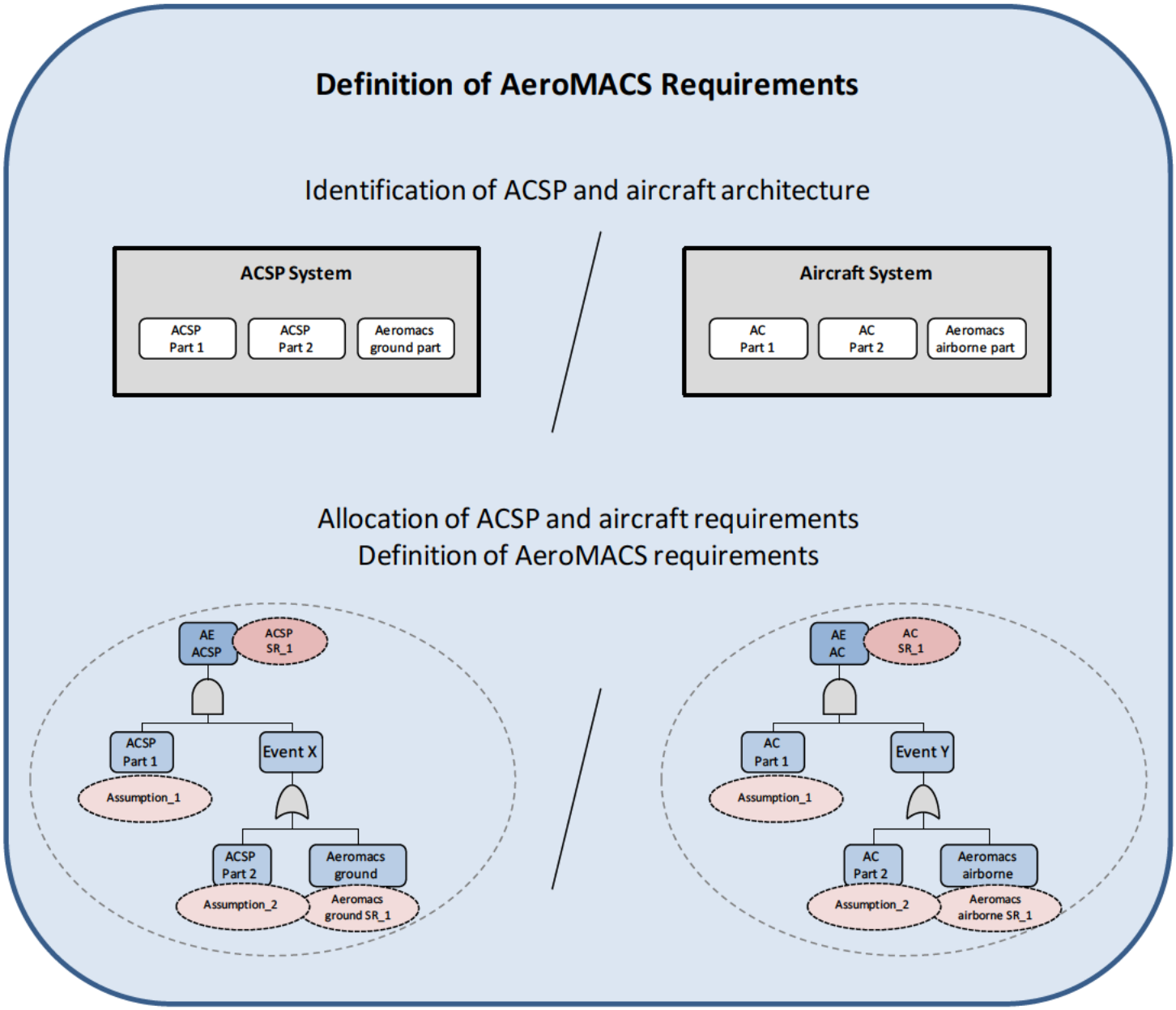


Figure 8 : Methodology for the definition of AeroMACS Requirements

3.2.1 Description of ACSP and aircraft architecture

As presented on the previous figure, this task consists in identifying the architecture of classical aircraft and ACSP systems. This identification should include:

- Presentation of aircraft and ACSP sub-systems, including AeroMACS airborne sub-system and AeroMACS ground sub-system
- Presentation of the function of each sub-system

This task will be a basis for the identification of sub-systems involved in the different Abnormal Events. The detail level of this architecture must be commensurate with the desired detail-level of the AeroMA CS Requirements.

The description of ACSP architecture is presented in § 5.1.

The description of aircraft architecture is presented in § 6.1.

3.2.2 Identification of components involved in Abnormal Events

As presented on Figure 8, this task consists in identifying for each Abnormal Event:

- the different sub-systems failures that could lead to this Abnormal Event
- the combination of failures that must occur to lead to this Abnormal Event

The failures are identified on the sub-systems defined previously.

3.2.3 Allocation of Components Requirements

This task consists in performing the allocation of requirements on the different sub-systems identified previously.

In order to perform this allocation, fault tree can be constructed, for each Abnormal Event, presenting all potential contributors for this Abnormal Event (potential contributors have been identified during the previous task). Then, assumptions are made regarding the failure of others sub-systems and requirements are allocated on AeroMACS. These requirements can be:

- Quantitative requirements on AeroMA CS sub-system. These requirements are derived from the ACSP and aircraft Requirements. If these quantitative requirements seem impossible to reach, design requirements could be defined (redundancies…)
- Assurance Level on AeroMA CS sub-system. These requirements are derived from the severity of the Operational Hazard to which the Abnormal Events contributes. The methodology for the allocation of Assurance Level will be detailed later.
- Requirements regarding the transaction time in AeroMACS sub-system
- Qualitative requirements regarding the functions of the system

The results of this allocations are presented in § 5.2 for AeroMACS ground system and § 6.2 for AeroMACS airborne system.

4 Definition of Safety and Performance requirements applicable to the ACSP and Aircraft

4.1 Definition of ACSP and Aircraft Safety Requirements

In this section, first are identified the different failure cases which can be encountered at AeroMACS level.

Then, mainly based on WG78/SC214 documentation (see [1], [2], [3], [4]), the Operational Hazards to which each Abnormal Event leads are identified, depending on the Context of Use and on success or failure of the External Mitigations Means.

NOTE: This bottom-up approach aims at reviewing the draft WG78/SC214 documentation in a different way they are developed which is beneficial since some problems could pop-up.

4.1.1 Identification of Operational Hazards

4.1.1.1 Identification of Abnormal Events

This sub-task consists in identifying all the failures (Abnormal Events) that can occur at AeroMACS level. Abnormal Events are directly linked to the main function of AeroMACS ("Transmit messages between ground and airborne systems in order to perform data link services").

The AeroMACS Abnormal Events are referenced as follow: "*AE_XX: xxxx*"

- *XX* : reference number of the AE
- *xxxx* : title of the AE

The identification of Abnormal Events is based on classical failures modes that can occur in a network. These failures modes are:

- Loss of message
- Corruption of message
- Misdirection of message
- Delay of message
- Generation of spurious message

These classical failures modes can apply to:

- One message
- All messages associated to one aircraft
- All messages associated to more than one aircraft

Failure concerning the "messages associated to one aircraft" can occur in case of failure in the airborne part of AeroMACS.

Failures affecting some messages are not considered because they are considered as equivalent to a succession of failure concerning one message.

The application of this systematic methodology leads to the following preliminary list of Abnormal Events which can be encountered at AeroMACS level:

Ref	Failure mode	Number of messages concerned	Abnormal Events
AE_temp_01	Loss	One message	Loss of one message

Ref	Failure mode	Number of messages concerned	Abnormal Events
AE_temp_02	Loss	Messages associated to one aircraft	Loss of messages associated to one aircraft
AE_temp_03	Loss	Messages associated to more than one aircraft	Loss of messages associated to more than one aircraft
AE_temp_04	Corruption	One message	Corruption of one message
AE_temp_05	Corruption	Messages associated to one aircraft	Corruption of messages associated to one aircraft
AE_temp_06	Corruption	Messages associated to more than one aircraft	Corruption of messages associated to more than one aircraft
AE_temp_07	Misdirection	One message	Misdirection of one message
AE_temp_08	Misdirection	Messages associated to one aircraft	Misdirection of messages associated to one aircraft
AE_temp_09	Misdirection	Messages associated to more than one aircraft	Misdirection of messages associated to more than one aircraft
AE_temp_10	Delay	One message	Delay of one message
AE_temp_11	Delay	Messages associated to one aircraft	Delay of messages associated to one aircraft
AE_temp_12	Delay	Messages associated to more than one aircraft	Delay of messages associated to more than one aircraft
AE_temp_13	Spurious	Messages associated to more than one aircraft	Generation of one spurious message
AE_temp_14	Spurious	Messages associated to more than one aircraft	Transmission of spurious messages to one aircraft
AE_temp_15	Spurious	Messages associated to more than one aircraft	Transmission of spurious messages to more than one aircraft

Table 3: Preliminary list of abnormal events

Some Abnormal Events of this list lead to the same Operational Hazards. So, the following assumptions were made in order to reduce the number of Abnormal Events to consider for the identification of operational hazards.

- **ASSUMP-AEROMACS_04**: Abnormal Events concerning all the messages at AeroMACS level associated to one aircraft are always detected. These events are grouped as single event: “permanent failure to communicate with one aircraft" (Availability of use).

  Justification: A failure on a message at AeroMACS level (corruption, loss…), is detected thanks to the external mitigation means such as time stamps, checksum… at upper layers. A systematic failure of the external mitigations means for all AeroMACS messages is very unlikely (the period of failure allocated by WG78 is one failure every 100 000 hours). The detection of this failure induces a clarification between controllers and flight crew. Then, following messages will be carefully watched; controllers will detect that there is a permanent failure on Datalink communication chain with the aircraft.

  ➔ AE_temp_02, AE_temp_05, AE_temp_08, AE_temp_11 and AE_temp_14 are grouped together: AE_05 “Permanent failure to communicate with one aircraft”

- **ASSUMP-AEROMACS_05**: Abnormal Events concerning all messages at AeroMACS level associated to more than one aircraft are always detected. These events are grouped as single event:”permanent failure to communicate with more than one aircraft” (Availability of provision).

Justification: A failure on an AeroMACS message (corruption, loss…), is detected thanks to the external mitigation means such as time stamps, checksum… A systematic failure of the external mitigations means for all message is very improbable (the period of failure allocated by WG78 is one failure every 100 000 hours). The detection of this failure induces a clarification between controllers and flight crew. Then, following messages will be carefully watched; controllers will detect that there is a permanent failure on Datalink communication chain.

➔ AE_temp_03, AE_temp_06, AE_temp_09, AE_temp_12 and AE_temp_15 are grouped together: AE_06 "Permanent failure to communicate with more than one aircraft"

So the final list of Abnormal Events that will be considered for the identification of Operational hazards is:

Ref	Abnormal Events
AE_01	Loss of one message at AeroMACS level
AE_02	Corruption of one message at AeroMACS level
AE_03	Misdirection of one message at AeroMACS level
AE_04	Delay of one message at AeroMACS level
AE_05	Generation of one spurious message at AeroMACS level
AE_06	Permanent failure to communicate with one aircraft (availability of use)
AE_07	Permanent failure to communicate with more than one aircraft (availability of provision)

Table 4: List of Abnormal Events considered for the identification of Operational Hazards

4.1.1.2 Identification of all Contexts of Use and External Mitigation Means associated to each Abnormal Event

4.1.1.2.1 Identification of "Context of Use"

This subtask consists in identifying all the "Contexts of Use" associated to each Abnormal Event. "Context of Use" reflects the operational environment in which the system can be used.

The Contexts of Use are referenced as follow: "*CU_XX: xxxx*"

- *XX* : reference number of the CU
- *xxxx* : title of the CU

The identification of "Context of Use" is based on the context of utilization of the AeroMACS which includes:

- Application related to the message transmitted via AeroMACS
- kind of message (uplink or downlink message). *Uplink messages are messages from the ground to the aircraft and downlink messages are messages from the aircraft to the ground. This definition is consistent with WG78/SC214, but not with the others deliverables of 15.2.7 (e.g. SRD).*
- kind of failure (corruption of a message into another existing message or corruption into an un-existing message)

The following table presents all the Contexts of Use identified for the AeroMACS

Ref	Context of Use
CU_01_a	Message is related to CPDLC application
CU_01_b	Message is related to ADS-C application

Ref	Context of Use
CU_01_c	Message is related to FIS application
CU_02_a	Message is an uplink message
CU_02_b	Message is a downlink message
CU_03_a	Downlink message is corrupted into an existing other downlink message
CU_03_b	Downlink message is corrupted into an unexisting downlink message
CU_04_a	Uplink message is corrupted into an existing other uplink message
CU_04_b	Uplink message is corrupted into an unexisting uplink message

Table 5: List of Contexts of Use considered for the identification of Operational Hazards

4.1.1.2.2 Identification of External Mitigation Means

This subtask consists in identifying all the External Mitigation Means associated to each Abnormal Event. Mitigation means are means that may help to reduce the effects of an Hazard related to Abnormal Event once it has occurred. External Mitigation Means are mitigations means outside the scope of the system under assessment, in our case it is thus outside AeroMACS system.

The External Mitigation Means are referenced as follow: "*EMM_XX: xxxx*"

- *XX* : reference number of the EMM
- *xxxx* : title of the EMM

This identification of External Mitigation Means is based on the WG78/SC214 documentation (see [1], [2], [3], [4]): External Mitigation Means appear in Allocation of Safety Objectives and Requirements (ASOR) part of the OSAs. The mitigation means applicable to this safety analysis are mainly those related to the ACSP failures.

The result of this identification is that it exists external mitigation means for all the classical failures of a network:

- Loss of message (AE_01)
- Corruption of message (AE_02)
- Misdirection of message (AE_03)
- Delay of message (AE_04)
- Generation of a one spurious message at AeroMACS level (AE_05)

The following table presents all the External Mitigation Means that could apply and the failures that they mitigate (this list doesn't include the mitigation means inside the ACSP that could mitigate AeroMACS failures):

Ref	External Mitigation Means	Concerned AE
EMM_01	Flight Crew detects uplink message is inappropriate	Corruption : AE_02 Misdirection : AE_03 Delay : AE_04
EMM_02	Aircraft system detects and rejects corrupted uplink messages	Corruption : AE_02
EMM_03	Ground system detects and rejects corrupted downlink messages.	Corruption : AE_02
EMM_04	Ground system detects that a message has not been responded to within the expected time	Loss : AE_01 Misdirection : AE_03 Delay : AE_04

Ref	External Mitigation Means	Concerned AE
EMM_05	Aircraft system time stamps downlink messages Ground system checks the time stamp of a delayed downlink message and rejects it	Delay : AE_04
EMM_06	Ground system time stamps uplink messages Aircraft system checks the time stamp of a delayed uplink message and rejects it	Delay : AE_04
EMM_07	Aircraft system detects and rejects misdirected uplink messages	Misdirection : AE_03
EMM_08	Ground system detects and rejects misdirected downlink messages	Misdirection : AE_03
EMM_09	Controller detects downlink message is inappropriate	Corruption : AE_02 Misdirection : AE_03 Delay : AE_04
EMM_09	Controller waits Flight Crew response before sending other clearances	Delay : AE_04
EMM_10	Aircraft system checks UM/DM association and rejects spurious uplink messages	Spurious : AE_05
EMM_11	Ground system checks UM/DM association and rejects spurious downlink messages	Spurious : AE_05

Table 6: List of External Mitigation Means considered for the identification of Operational Hazards

4.1.1.3 Identification of all Operational Hazards associated to each Abnormal Event

This sub-task consists in identifying all the Operational Hazards to which each Abnormal Event leads, depending on the Context of Use and on the External Mitigations Means success or failure. Operational Hazards are identified by systematically applying the different Contexts of Use to the Abnormal Events and evaluating the associated consequences depending on External Mitigation Means success or failure.

A list of Operational effects has been established by Working Group 78 for the different data link application (CM, CPDLC, FIS and ADS). This list was established through expert consensus.

An Abnormal Event can lead to some of these WG78 Operational Hazards and eventually to new Operational Hazards that were not identified by WG78.

The list of Operational Effects will be referenced as follow: "*OH_XX_YY_ZZ: xxxx*"

- XX identify the kind of OH "*WG78*" for the OH already identified in WG78 and "*NEW*" for the new OH
- YY identify the application concerned by the OH: "*CPDLC*", "*ADSC*", "*FIS*", "or "*ALL*" if all the application are involved simultaneously in an OH.
- *ZZ* reference number of the OH. For the WG78 OH, the same number than in WG78 documents is used.
- *xxxx* title of the OH

The table associated to this systematic methodology is presented in Appendix B .

The results of this methodology are:

- AeroMACS failures can lead to 19 "**WG78 Operational Hazards**"

- 5 **CPDLC** Operational Hazards
  - OH_WG78_CPDLC_01: Loss of CPDLC capability [single aircraft]
  - OH_WG78_CPDLC_02: Loss of CPDLC capability [multiple aircraft]
  - OH_WG78_CPDLC_03 : Reception of a corrupted CPDLC message [single aircraft]
  - OH_WG78_CPDLC_04 : Unexpected interruption of a CPDLC transaction [single aircraft]
  - OH_WG78_CPDLC_05 : Reception of an unexpected CPDLC message [single aircraft]
- 9 **FIS** Operational Hazards
  - OH_WG78_FIS_1d : D-OTIS service unavailable for one aircraft (detected)
  - OH_WG78_FIS_2d : D-OTIS service unavailable for more than one aircraft (detected)
  - OH_WG78_FIS_3d : Incorrect D-OTIS report received (detected)
  - OH_WG78_FIS_3u : Incorrect D-OTIS report received (undetected)
  - OH_WG78_FIS_4d : D-OTIS report not received (detected)
  - OH_WG78_FIS_4u : D-OTIS report not received (undetected)
  - OH_WG78_FIS_5u : D-OTIS report is misdirected (undetected)
  - OH_WG78_FIS_6d : Spurious / unexpected D-OTIS report received (detected)
  - OH_WG78_FIS_6u : Spurious / unexpected D-OTIS report received (undetected)
- 5 **ADS-C** Operational Hazards
  - OH_WG78_ADSC_01 : Loss of ADS-C capability [single aircraft]
  - OH_WG78_ADSC_02 : Loss of ADS-C capability [multiple aircraft]
  - OH_WG78_ADSC_03 : Reception of incorrect ADS-C report [single aircraft]
  - OH_WG78_ADSC_05 : Reception of an unexpected ADS-C report [single aircraft]
  - OH_WG78_ADSC_07 : Loss of an ADS-C report [single aircraft]

- AeroMACS failure can lead to 2 "**New Operational Hazards**"
  - OH_NEW_ALL_01 : Failure to exchange any message with a single aircraft (detected)
  - OH_NEW_ALL_02 : Failure to exchange any message with more than one aircraft aircraft (detected)

For the WG78 Operational Hazards, definition of associated Safety Objective has already been performed by WG78. For the new Operational Hazards, the evaluation of the severity related to the effect and the definition of associated safety objective are performed in the two following paragraphs.

4.1.1.4 Evaluation of severity associated to new Operational Hazards

This sub-task consists in evaluating the effects associated to new Operational Hazards and in proposing a severity for these Operational Hazards. Consistent with WG78 analysis, the ED-78 Hazards Classification Matrix (see Appendix A) is used to evaluate the severities.

This sub-task is carried out in comparison with the severities that have been attributed by WG78. If a "new OH" has the same effects than a "WG78 OH" and the same mitigation means, the same severity is attributed to this OH. If a "new OH" has the same effect than a "WG78 OH" and if it hasn't the same mitigation means, a more severe classification might be allocated on this "new OH".

Two new hazards have been identified during the previous task:

- OH_NEW_ALL_01 : Failure to exchange any message with a single aircraft (detected)
- OH_NEW_ALL_02 : Failure to exchange any message with more than one aircraft (detected)

- **OH_NEW_ALL_01 : Failure to exchange any message with a single aircraft (detected)**

This Operational Hazard is a combination of three Operational Hazards:

- OH_WG78_CPDLC_01 : Loss of CPDLC capability [single aircraft] (SC5)
- OH_WG78_FIS_1d : D-OTIS service unavailable for one aircraft (SC5)
- OH_WG78_ADSC_01: Loss of ADS-C capability [single aircraft] (SC5)

Severities of all these Operational Hazards have been determined by evaluating their effects on the overall ATM system.

ASSUMP-AEROMACS_06: Simultaneous loss of all applications (CPDLC, D-OTIS and ADS-C) for one aircraft is not more critical that independent failure of each application for one aircraft.

Justification: This assumption seems coherent because Datalink application has never been considered as a reduction mean to mitigate the loss of another application. For example, OH_WG78_CPDLC_01 (failure to exchange CPDLC messages with a single aircraft) is not mitigated by the utilization of ADS-C or FIS.

For unavailability of short duration, the failure may remain **undetected**. This has no impact to pilot or controller workload and has a minimal safety impact: **SC5**.

For **CPDLC** messages, in case of unavailability of longer duration, when initiating a message, the initiator **detects** the system fails to send the message. At the time of detection, the initiator reverts to voice communication in order to settle the open dialogue. All subsequent dialogues will be initiated by voice.

This leads to a slight, but still tolerable increase in controller and flight crew workload. The flight crew may need to perform a manual re-logon: **SC5**.

For **ADS** messages, when initiating an ADS-C contract request, the controller **detects** that the ground system fails to send the message. In case of a demand or periodic contract, if the aircraft system fails to send ADS-C report(s), the controller will detect it. For an event contract, the controller may detect the loss of ADS-C capability depending on the type of event.

The loss of ADS-C capability leads to a slight, but still tolerable increase in controller workload: **SC5**.

For **FIS** messages, before contacting the approach or tower controller, the flight crew **detects** the unavailability of the D-OTIS service (due to report. There is no safety impact for all requested report types.

No increase of flight crew workload: **SC5**.

➔ This new operational hazard has a severity class 5 (**SC5**).

- **OH_NEW_ALL_02 : Failure to exchange any message with more than one aircraft (detected)**

This Operational Hazard is a combination of three Operational Hazards:

- OH_WG78_CPDLC_02 : Loss of CPDLC capability [multiple aircraft] (SC4)
- OH_WG78_FIS_2d : D-OTIS service unavailable for more than one aircraft (SC5)
- OH_WG78_ADSC_02: Loss of ADS-C capability [multiple aircraft] (SC4)

ASSUMP-AEROMACS_07: Simultaneous loss of all applications (CPDLC, D-OTIS and ADS-C) for multiple aircraft is not more critical that independent failure of each application for multiple aircraft.

Justification: This assumption must be validated by working group 78. However, this assumption seems coherent because Datalink application has never been considered as a reduction mean to mitigate the loss of another application.

For unavailability of short duration, the failure may remain **undetected**. This has no impact to pilot or controller workload and has a minimal safety impact: **SC5**.

For **CPDLC** messages, in case of unavailability of longer duration, when initiating a message, the initiator **detects** the system fails to send the message. At the time of detection, the initiator reverts to voice communication in order to settle the open dialogue. In the worst case of non-employment of a Standby System, all subsequent dialogues with the effected aircraft are exchanged using voice.

This may lead to a significant increase in controller workload due to reversion to voice communication and number of impacted aircraft and a slight increase in flight crew workload. It may have a slight effect on operations: **SC4**.

For **ADS** messages, when initiating an ADS-C contract request, the controller **detects** that the ground system fails to send the message. In case of a demand or periodic contract, if two or more aircraft systems fail to send ADS-C reports, the controller will detect it. For event contracts, the controller may detect the loss of ADS-C capability depending on the type of event.

From the ground viewpoint, the IER service cannot be used with two or more aircraft. Less predictability, using EPP, is causing for several aircraft an extra burden for the controller because in normal circumstances he relies on the EPP to obtain better predictability crosschecking or route conformance checking.

This may lead to a significant increase in controller workload as more checking is now required on the trajectory: **SC4**.

For **FIS** messages, before contacting the approach or tower controller, the flight crew **detects** the unavailability of the D-OTIS service (due to report. There is no safety impact for all requested report types.

No increase of flight crew workload: **SC5**.

➔ This new operational hazard has a severity class 4 (**SC4**).

4.1.1.5 Definition of Safety Objectives associated to new Operational Hazards

This sub-task consists in defining the safety objectives associated to “new OH”. In order to perform the allocation of AeroMACS Safety Requirements (cf. § 3.1.1.2), it is necessary to determine the safety objectives associated to all Operational Hazards, even those not identified by WG 78.

The same methodology than in WG78 is applied for this definition: the Safety Objective is linked to the severity attributed to the Operational Hazard.

- **OH_NEW_ALL_01 : Failure to exchange any message with a single aircraft**

This new Operational Hazard is classified with a severity 5 (SC5). In consistence with WG78 documents, no safety objective is defined from SC5 Operational Hazard.

- **OH_NEW_ALL_02 : Failure to exchange any message with more than one aircraft**

This new Operational Hazard is classified with a severity 4 (SC4).

As described previously, this severity is mainly driven because this hazard can lead to a "loss of CPDLC and ADS-C capability for more than one aircraft" (OH_WG78_CPDLC_02 and OH_WG78_ADSC_02).

The following safety objectives are allocated in WG78 Safety Analysis

- OH_WG78_CPDLC_02 – Safety Objective : $2.0*10^{-5}$ /FH
- OH_WG78_ADSC_02 – Safety Objective : $1.9*10^{-5}$ /FH

Consequently, the most stringent of these two safety objectives is used for a failure to use any application.

➔ **Safety Objective for OH_NEW_ALL_02 is $1.9*10^{-5}$ /FH**

4.1.2 Identification / definition of relevant ACSP and AC Safety Requirements

4.1.2.1 Identification of relevant ACSP and AC Safety Requirement from WG78 Operational Hazards

As mentioned previously, for all Operational Hazards identified by the WG78, the group has already performed an allocation of safety requirements on the different components of the ATM system: Controller, Flight Crew, Aircraft System, Air Ground Communication System (ACSP) and Ground System. Consequently, this task consists in identifying, in the allocation fault tree of the WG78, all the safety requirements that are relevant for the AeroMACS.

The AeroMACS is split between Aircraft System and ACSP. So, the relevant Safety Requirements are the requirements allocated to Aircraft system or ACSP and that concerns the exchange of message between ground and aircraft.

The list of relevant WG78 Safety Requirements will be referenced as follow: "*SR_WG78_XX_YY_ZZ: xxxx*"

- XX_YY_ZZ constitutes the reference of the cause in the WG78 fault tree
  - XX: identify the part on which the safety requirement is allocated : "*CP*" for ACSP or "*AC*" for Aircraft System
  - YY: identify the application associated to the fault tree : "*ADSC*", "*CM*", "*CPDLC*" or "*FIS*"
  - *ZZ* : is a reference number of safety requirement
- *xxxx* title of the WG78 Safety Requirement

The following chapters present the relevant safety requirements defined from each WG78 OH identified in § 4.1.1.3.

4.1.2.1.1 OH_WG78_ADSC_02

The safety objective to be met for this Operational Hazard is extracted from WG78 ADS-C Operational Safety Assessment (see [3]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $2*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_ADSC_02	4	2.00E-05	WG78_CP_ADSC_01	ACSP	Unavailable	Any	7.60E-06	*No ref*	The likelihood that the ACSP is unavailable shall be less than 7.6E-06/FH
			WG78_AC_ADSC_01	AC	Unavailable	Any	3.00E-03	*No ref*	The likelihood that the AC system is unavailable shall be less than 3E-03/FH
								SR-AC-ADSC-01	The aircraft system shall provide to the ATSU an indication when it rejects an ADS-C service request initiated by the ATSU at the application layer.
								SR-AC-ADSC-02	The aircraft system shall indicate to the flight crew a detected loss of ADS-C service.

Table 7: Relevant ACSP and AC safety requirements allocated from OH_WG78_ADSC_02

4.1.2.1.2 OH_WG78_ADSC_03

The safety objective to be met for this Operational Hazard is extracted from WG78 ADS-C Operational Safety Assessment (see [3]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $2.1*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_ADSC_03	4	2.10E-05	WG78_CP_ADSC_02	ACSP	Corruption	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_ADSC_02	AC	Corruption	Downlink	7.00E-05	SR-AC-ADSC-03	The likelihood that the aircraft system corrupts an ADS-C report shall be less than 7.0E-05/FH

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
			WG78_AC_ADSC_03	AC	EMM 02 - Corruption	-	3.50E-05	SR-AC-ADSC-04	The likelihood that the aircraft system fails to detect the corrupted ADS-C report shall be less than 3.5E-5/FH

Table 8: Relevant ACSP and AC safety requirements allocated from OH_WG78_ADSC_03

4.1.2.1.3 OH_WG78_ADSC_05

The safety objective to be met for this Operational Hazard is extracted from WG78 ADS-C Operational Safety Assessment (see [3]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $2*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
OH Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_ADSC_05	4	2,10E-05	WG78_CP_ADSC_03	ACSP	Spurious	Downlink	1,00E+00	*No SR*	*No SR*
			WG78_AC_ADSC_04	AC	Spurious	Downlink	1,00E+00	SR-AC-ADSC-5	The likelihood that the aircraft system generates a spurious report shall be less than 1.0E-05/FH .
			WG78_GD_ADSC_04	GD	EMM 11 - Spurious	Downlink	1,00E-05	SR-AC-ADSC-10	The aircraft system shall indicate in each report to which contract number it is referring
			WG78_CP_ADSC_04	ACSP	Delay	Downlink	1,00E+00	*No SR*	*No SR*
			WG78_AC_ADSC_06	AC	Delay	Downlink	1,00E-05	*No SR*	*No SR*

OH			Cause					WG 78 Safety Requirement	
OH Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
			WG78_AC_ADSC_05	AC	EMM 05 - Delay	-	1,00E-05	SR-AC-ADSC-6	The likelihood that the aircraft system incorrectly time stamps the report shall be less than 1.0E-05/FH
								SR-AC-ADSC-7	The aircraft system shall time stamp each report to within one second UTC when it is released for onward transmission.
			WG78_CP_ADSC_05	ACSP	Misdirection	Downlink	1,00E+00	*No SR*	*No SR*
			WG78_AC_ADSC_07	AC	Misdirection	Downlink	1,00E+00	SR-AC-ADSC-8	The aircraft system shall transmit messages to the designated recipient.
								SR-AC-ADSC-9	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits
			WG78_CP_CM_01	ACSP	Corruption	Downlink init	1,00E+00	*No SR*	*No SR*
			WG78_AC_CM_01	AC	Corruption	Downlink init	1,00E-05	SR-AC-CM-01	The likelihood that the aircraft system sends incorrect DLIC initiation data shall be less than 1.0E-05/FH
								SR-AC-CM-02	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, used for data link initiation correlation and ADS-C network address mapping, shall be unique and unambiguous
			WG78_CP_CM_02	ACSP	Corruption	Uplink init	1,00E+00	*No SR*	*No SR*
			WG78_AC_CM_02	AC	Misdirection	Uplink init	1,00E+00	*No SR*	*No SR*

Table 9: Relevant ACSP and AC safety requirements allocated from OH_WG78_ADSC_05

4.1.2.1.4 OH_WG78_CPDLC_02

The safety objective to be met for this Operational Hazard is extracted from WG78 CPDLC Operational Safety Assessment (see [2]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $1.9*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_CPDLC_02	4	1.90E-05	WG78_CP_CPDLC_01	ACSP	Unavailable	Any	7.60E-06	No ref	The likelihood that the ACSP is unavailable shall be less than 7.6E-06/FH
			WG78_AC_CPDLC_01	AC	Unavailable	Any	2.50E-03	No ref	The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH
								SR-AC-CPDLC-01	The aircraft system shall provide to the ATSU an indication when it rejects a CPDLC service request initiated by the ATSU at the application layer.
								SR-AC-CPDLC-02	The aircraft system shall display the indication provided by the ATSU when a DSC service request initiated by the flight crew is rejected at the application layer.
								SR-AC-CPDLC-03	The aircraft system shall indicate to the flight crew a detected loss of data link service.

Table 10: Relevant ACSP and AC safety requirements allocated from OH_WG78_CPDLC_02

4.1.2.1.5 OH_WG78_CPDLC_03

The safety objective to be met for this Operational Hazard is extracted from WG78 CPDLC Operational Safety Assessment (see [2]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $1.8*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_CPDLC_03	3	1.80E-05	-	ACSP	Corruption	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_01	AC	Corruption	Downlink	1.00E-05	SR-AC-CPDLC-13	The likelihood that the aircraft system corrupts a downlink message shall be less than 1.0E-05/FH
			WG78_AC_CPDLC_02	AC	EMM 02 - Corruption	-	1.00E-05	SR-AC-CPDLC-07	The likelihood that the aircraft system fails to detect the corrupted downlink message shall be less than 1.0E-05/FH
			WG78_CP_CPDLC_01	ACSP	Corruption	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_03	AC	Corruption	Uplink	1.00E-05	SR-AC-CPDLC-17	The likelihood that the aircraft system corrupts an uplink message shall be less than 1.0E-05/FH
								SR-AC-CPDLC-11	The aircraft system shall prohibit operational processing by flight crew of corrupted messages.
								SR-AC-CPDLC-05	The aircraft system shall execute the route clearance per the route clearance received from the ATS via data link
								SR-AC-CPDLC-06	The aircraft system shall ensure the correct transfer into or out of the aircraft's FMS of route data received/sent via data link,in support of the conditions in section 2.4.1.1.
			WG78_AC_CPDLC_04	AC	EMM 02 - Corruption	-	1.00E-05	SR-AC-CPDLC-08	The likelihood that the aircraft system fails to detect the corrupted uplink message shall be less than 1.0E-05/FH
								SR-AC-CPDLC-09	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.
								SR-AC-CPDLC-17	The aircraft system shall prohibit operational processing by flight crew of corrupted messages.

Table 11: Relevant ACSP and AC safety requirements allocated from OH_WG78_CPDLC_03

4.1.2.1.6 OH_WG78_CPDLC_04

The safety objective to be met for this Operational Hazard is extracted from WG78 CPDLC Operational Safety Assessment (see [2]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $1.8*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_CPDLC_04	3	1.80E-05	WG78_CP_CPDLC_10	ACSP	Delay	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_CP_CPDLC_10	ACSP	Loss	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_14	AC	Delay	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_14	AC	Loss	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_CP_CPDLC_06	ACSP	Misdirection	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_12	AC	EMM 07 - Misdirection	-	1.00E-05	SR-AC-CPDLC-19	The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH
								SR-AC-CPDLC-09	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.
								SR-AC-CPDLC-12	The aircraft system shall only accept uplink messages intended for it.
								SR-AC-CPDLC-21	The aircraft system shall be able to determine the message initiator.
								SR-AC-CPDLC-22	Once an aircraft accepts operational CPDLC messages from an ATSU, it shall reject operational CPDLC messages from any other ATSU until the first ATSU terminates CPDLC with that aircraft.

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
								SR-AC-CPDLC-35	Only the ATSU that has control of the aircraft shall be permitted to send a Next Data Authority (NDA) message to the aircraft.
			WG78_CP_CM_01	ACSP	Corruption	Downlink init	1.00E+00	*No SR*	*No SR*
			WG78_AC_CM_01	AC	Corruption	Downlink init	1.00E-05	SR-AC-CM-01	The likelihood that the aircraft system sends incorrect initialisation data shall be less than 1.0E-05/FH
								SR-AC-CM-02	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, and used for data link initiation correlation and CPDLC network address mapping, shall be unique and unambiguous
			WG78_CP_CPDLC_07	ACSP	Delay	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_CP_CPDLC_07	ACSP	Loss	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_15	AC	Delay	Downlink	1.00E+00	SR-AC-CPDLC-24	The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted
			WG78_AC_CPDLC_15	AC	Loss	Downlink	1.00E+00	SR-AC-CPDLC-24	The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted
			WG78_CP_CPDLC_05	ACSP	Misdirection	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_10	AC	Misdirection	Downlink	1.00E+00	SR-AC-CPDLC-10	The aircraft system shall transmit messages to the designated recipient.
								SR-AC-CPDLC-04	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits

Table 12: Relevant ACSP and AC safety requirements allocated from OH_WG78_CPDLC_04

4.1.2.1.7 OH_WG78_CPDLC_05

The safety objective to be met for this Operational Hazard is extracted from WG78 CPDLC Operational Safety Assessment (see [2]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $1.8*10^{-5}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_CPDLC_05	3	1.80E-05	WG78_CP_CPDLC_03	ACSP	Spurious	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_07	AC	Spurious	Downlink	1.00E+00	SR-AC-CPDLC-14	The aircraft system shall prevent release of a report/operational response without flight crew action.
			WG78_CP_CPDLC_04	ACSP	Delay	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_09	AC	Delay	Downlink	1.00E-05	*No SR*	*No SR*
			WG78_AC_CPDLC_08	AC	EMM 05 - Delay	-	1.00E-05	SR-AC-CPDLC-18	The likelihood that the aircraft system incorrectly time stamps the DM shall be less than 1.0E-05/FH
								SR-AC-CPDLC-16	The aircraft system shall time stamp to within one second UTC each message when it is released for onward transmission.
			WG78_CP_CPDLC_05	ACSP	Misdirection	Downlink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_10	AC	Misdirection	Downlink	1.00E+00	SR-AC-CPDLC-10	The aircraft system shall transmit messages to the designated recipient.
								SR-AC-CPDLC-04	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits
			WG78_CP_CM_01	ACSP	Corruption	Downlink init	1.00E+00	*No SR*	*No SR*

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
			WG78_AC_CM_01	AC	Corruption	Downlink init	1.00E-05	SR-AC-CM-01	The likelihood that the aircraft system sends incorrect initialisation data shall be less than 1.0E-05/FH
								SR-AC-CM-02	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, used for data link initiation correlation and CPDLC network address mapping, shall be unique and unambiguous
			WG78_CP_CM_02	ACSP	Corruption	Uplink init	1.00E+00	*No SR*	*No SR*
			WG78_CP_CM_03	ACSP	Misdirection	Uplink init	1.00E+00	*No SR*	*No SR*
			WG78_CP_CPDLC_02	ACSP	Spurious	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_06	AC	EMM 10 - Spurious	-	1.00E-05	SR-AC-CPDLC-25	Upon receipt of an UM, containing an MRN, the likelihood of the aircraft system, not rejecting that does not match a DM MIN shall be less than 1.E-5/FH.
								SR-AC-CPDLC-20	The aircraft system shall indicate in each response to which messages it refers
								SR-AC-CPDLC-26	Each downlink message shall be uniquely identified for a given aircraft-ATSU pair, following a sequential order
			WG78_CP_CPDLC_01	ACSP	Delay	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_02	AC	Delay	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_01	AC	EMM 06 - Delay	-	1.00E-05	SR-AC-CPDLC-09	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
								SR-AC-CPDLC-15	When a received message contains a time stamp that indicates the Latency Time Check value, set at equal or less than ETTRN, has been exceeded, the aircraft system shall a) discard the message and send an indication to the Ground System for display to the controller or b) provide the message to the flight crew with an appropriate indication.
								SR-AC-CPDLC-16	The aircraft system shall time stamp to within one second UTC each message when it is released for onward transmission
			WG78_CP_CPDLC_06	ACSP	Misdirection	Uplink	1.00E+00	*No SR*	*No SR*
			WG78_AC_CPDLC_11	AC	Misdirection	Uplink	1.00E-05	SR-AC-CPDLC-12	The aircraft system shall only accept uplink messages intended for it.
								SR-AC-CPDLC-06	The aircraft system shall ensure the correct transfer into or out of the aircraft's FMS of route data received/sent via data link, in support of the conditions in section 2.4.1.1.
								SR-AC-CM-01	The flight crew shall perform the initiation data link procedure again with any change of the aircraft identifiers (e.g. the Flight Identification and either the Registration Marking or the Aircraft Address)
			WG78_AC_CPDLC_12	AC	EMM 07 - Misdirection	-	1.00E-05	SR-AC-CPDLC-19	The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH

OH			Cause					WG 78 Safety Requirement	
Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
								SR-AC-CPDLC-09	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.
								SR-AC-CPDLC-12	The aircraft system shall only accept uplink messages intended for it.
								SR-AC-CPDLC-21	The aircraft system shall be able to determine the message initiator.
								SR-AC-CPDLC-22	Once an aircraft accepts operational CPDLC messages from an ATSU, it shall reject operational CPDLC messages from any other ATSU until the first ATSU terminates CPDLC with that aircraft.
			WG78_FC_CPDLC_01	FC	-	-	-	SR-AC-CPDLC-23	The aircraft system shall provide to the flight crew an indication of the ATSU that has established CPDLC (CDA) service.

Table 13: Relevant ACSP and AC safety requirements allocated from OH_WG78_CPDLC_05

4.1.2.1.8 OH_WG78_FIS_3u

The safety objective to be met for this Operational Hazard is extracted from WG78 FIS Operational Safety Assessment (see [4]): in Airport domain, the probability of occurrence of this hazard shall be no greater than $2.7*10^{-6}$ per flight hour.

The following table presents the relevant ACSP and AC requirements identified in WG78 Safety Analysis for this Operational Hazard (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					WG 78 Safety Requirement	
OH Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kind of message	Value (/FH)	SR Ref	Title
OH_WG78_FIS_3u	3	2.70E-06	WG78_CP_DOTIS_01	ACSP	Corruption	Downlink	2.80E-03	SR-CP-DOTIS-01	The likelihood that the ACSP corrupts a request shall be less than 2.8E-03/FH
			WG78_AC_DOTIS_01	AC	Corruption	Downlink	2.80E-03	SR-AC-DOTIS-01	The likelihood that the aircraft system corrupts the request without detecting it before the request is sent shall be less than 2.8E-03/FH
			WG78_AC_DOTIS_02	AC	Corruption	Downlink	2.80E-03	SR-AC-DOTIS-02	The likelihood that the aircraft HMI does not display data as inserted by the flight crew shall be less than 2.8E-03/FH
			WG78_CP_DOTIS_02	ACSP	Corruption	Uplink	2.80E-03	SR-CP-DOTIS-02	The likelihood that the ACSP corrupts a report shall be less than 2.8E-03/FH
			WG78_AC_DOTIS_05	AC	Corruption	Uplink	2.80E-03	SR-AC-DOTIS-05	The likelihood that the aircraft system corrupts the report when it receives it and does not detect it shall be less than 2.8E-03/FH
			WG78_AC_DOTIS_04	AC	EMM 02 - Corruption	-	2.80E-03	SR-AC-DOTIS-04	The likelihood that the aircraft system fails to detect and reject a corrupted report shall be less than 2.8E-03/FH
			WG78_AC_DOTIS_03	AC	Corruption	Uplink	1.30E-03	SR-AC-DOTIS-03	The likelihood that the aircraft system corrupts the report after having checked the end to end integrity shall be less than 1.3E-03/FH

Table 14 : Relevant ACSP and AC safety requirements allocated from OH_WG78_FIS_3u

4.1.2.1.9 Others WG78 OH

The others WG78 Operational Hazard identified in § 4.1.1.3 are:

- OH_WG78_CPDLC_01

- OH_WG78_ADSC_01
- OH_WG78_ADSC_07
- OH_WG78_FIS_1d
- OH_WG78_FIS_3d
- OH_WG78_FIS_3u
- OH_WG78_FIS_4d
- OH_WG78_FIS_4u
- OH_WG78_FIS_5u
- OH_WG78_FIS_6d
- OH_WG78_FIS_6u

These Operational Hazards are classified with a severity 5 (SC5) and no Safety Objectives has been defined from these hazards. Consequently there is no Safety Requirement derived from these hazards.

4.1.2.2 Definition ACSP and AC Safety Requirement from NEW Operational Hazards

This sub-task consists in performing the allocation of the Safety Objectives associated to NEW Operational Hazards on the different contributors.

This allocation includes two steps:

- For each NEW Operational Hazard, a fault tree is constructed identifying all potential contributors for this Operational Hazard (including ACSP and AC failures). Safety Requirements are defined by allocating the Safety Objective on the different contributors. Working Group documents are used as references to determine the values that can reasonably be allocated on the different contributors.
- For each New Operational Hazard, relevant Safety Requirements are identified amongst all the safety requirements The AeroMACS is split between Aircraft System and ACSP. So, the relevant Safety Requirements are the requirements allocated to Aircraft system or ACSP and that concerns the exchange of message between ground and aircraft.

The list of New relevant Safety Requirements are referenced as follow: "*SR_NEW_XX_YY_ZZ: xxxx*"

- XX: identify the part on which the safety requirement is allocated: "*CP*" for ACSP or "*AC*" for Aircraft System
- YY: identify the application associated to the fault tree : "*ADSC*", "*CM*", "*CPDLC*" or "*FIS*"

- *ZZ* : is a reference number of the safety requirement
- *xxxx* title of the NEW Safety Requirement

The following chapters present the relevant safety requirements defined from each New OH identified in § 4.1.1.3.

4.1.2.2.1 OH_NEW_ALL_01

This Operational Hazard is classified with a severity 5 (SC5) and no Safety Objective has been defined from this hazard. Consequently there is no Safety Requirements derived from this hazard.

4.1.2.2.2 OH_NEW_ALL_02

This new operational hazard consists in an impossibility to exchange any data link message with more than one aircraft. The Safety Objective to be met shall be no greater than $1.9*10^{-5}$ /FH

In order for this hazard to occur:

a) All the ground system are unavailable or

b) The ACSP is unavailable or

c) More than one aircraft system is unavailable.

The following assumption is made for the unavailability of the ground systems

- **ASSUMP-AEROMACS_08**: The probability that all the ground systems are unavailable is assumed to be less than $7*10^{-6}$ per flight hour.

  Justification: WG78 CPDLC OSA has defined a safety requirement of $7*10^{-6}$ for the unavailability of the CPDLC ground system. A failure of all the ground system should be lower than this requirement (multiple failure should occur to induce a failure of all ground systems).

The following figure presents the fault tree of OH_NEW_ALL_02 :

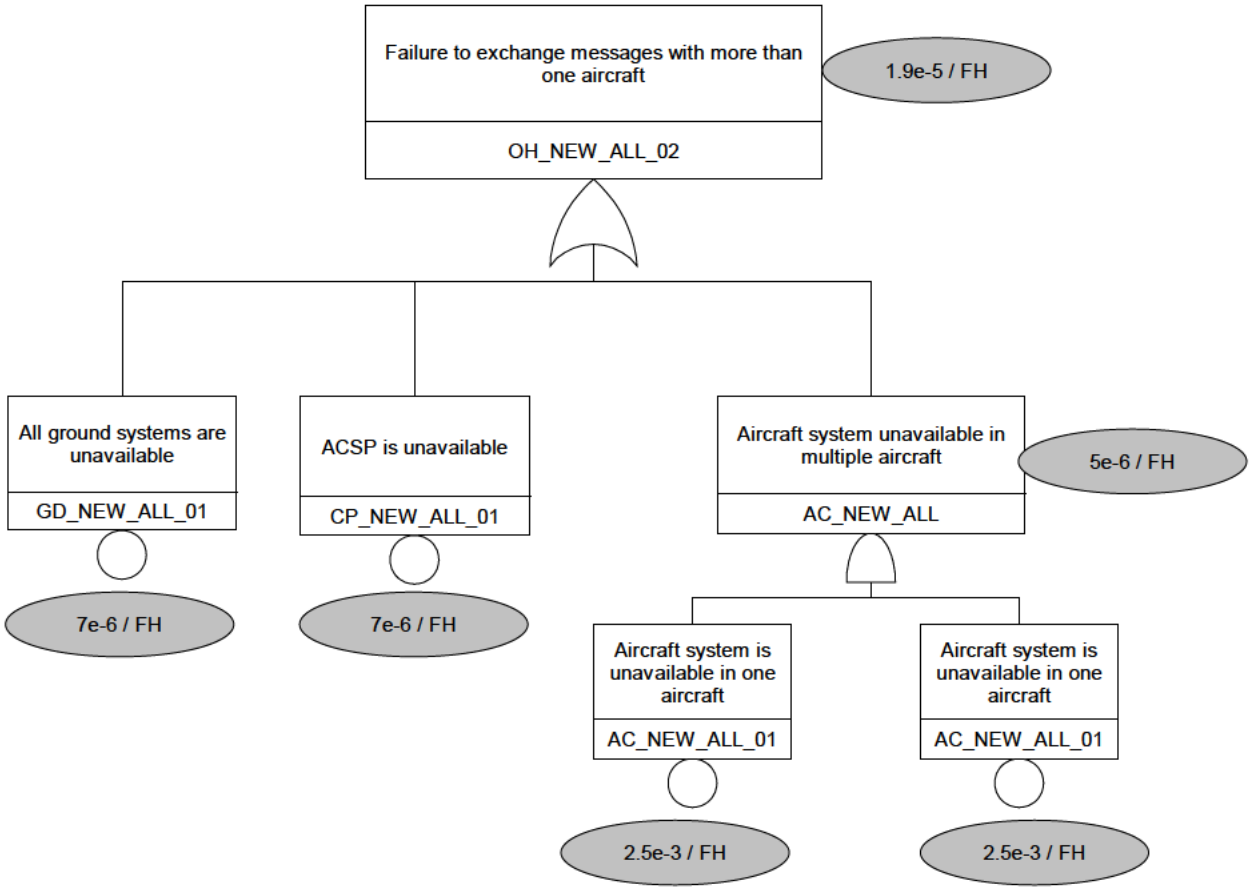


Figure 9 : OH_NEW_ALL_02 – Fault tree

The following table presents the causes identified on ACSP and AC for this OH, the values allocated on these causes and the associated Safety Requirements (in red: quantitative requirement, in green : qualitative requirements).

OH			Cause					SR	
OH Ref	Severity	SO (/FH)	Cause Ref	Part	Failure	Kinf of message	Value (/FH)	SR Ref	Title
OH_NEW_ALL_02	4	1,90E-05	NEW_CP_ALL_01	ACSP	Unavailable	Any	7.00E-06	SR-NEW-CP-ALL-01	The likelihood that the ACSP is unavailable shall be less than 7E-06/FH
			NEW_AC_ALL_01	AC	Unavailable	Any	2.50E-03	SR-NEW-AC-ALL-01	The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH

Table 15 : ACSP and AC safety requirements allocated from OH_NEW_ALL_02

4.1.2.3 Selection of applicable ACSP and AC Safety Requirements

Several Safety Requirements have been defined in the previous chapters on ACSP and AC system. Different Safety Requirements could have been defined for the same abnormal events (loss of message, corruption of message...).

Consequently this task consists in listing all the Safety Requirements that have been determined for each failure mode. Then the most stringent Safety Requirement is selected as being the applicable requirement for this failure mode.

The list of applicable Safety Requirements will be referenced as follow: "*SR_XX_YY: xxxx*"

- XX: identify the part on which the safety requirement is allocated: "*CP*" for ACSP or "*AC*" for Aircraft System
- YY: is a reference number of the applicable safety requirement
- *xxxx* title of the applicable safety requirement

NOTE: As defined in § 4.1.1.2.2, External Mitigation Means (EMM) are «means that may help to reduce the effects of an Abnormal Event once it has occurred". Consequently, the failure of an EMM can contribute to an operational hazard and safety requirements can be defined for EMM.

Following table presents for each abnormal events, all the Safety Requirements that have been identified or defined in the previous chapters (in red: quantitative requirement, in green: qualitative requirements).

AE		Selected SR					
Ref	Failure mode	Ref	Part	Value	Title	Source	Severity
AE_01	Loss of message	*No SR*	ACSP	-	*No SR*	-	-
		No SR	AC	-	*No SR*	-	-
		No SR	ACSP	-	*No SR*	-	-
		SR_AC_08	AC	-	The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted	OH_WG78_CPDLC_04	3
AE_02	Corruption of message	SR_CP_01	ACSP	2,80E-03	The likelihood that the ACSP corrupts a message (downlink or uplink) shall be less than 2.8E-03/FH	OH_WG78_FIS_3u	3
		SR_AC_01	AC	1,00E-05	The likelihood that the aircraft system corrupts a message (downlink or uplink) shall be less than 1.0E-05/FH	OH_WG78_ADSC_05 OH_WG78_CPDLC_03 OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	4 3 3 3
		No SR	ACSP	-	*No SR*	-	-
		SR_AC_09	AC	-	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, used for data link initiation correlation and ADS-C network address mapping, shall be unique and unambiguous	OH_WG78_ADSC_05 OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	4 3 3
		SR_AC_10	AC	-	The aircraft system shall prohibit operational processing by flight crew of corrupted messages.	OH_WG78_CPDLC_03	3

AE		Selected SR					
Ref	Failure mode	Ref	Part	Value	Title	Source	Severity
		SR_AC_11	AC	-	The aircraft system shall execute the route clearance per the route clearance received from the ATS via data link	OH_WG78_CPDLC_03	3
		SR_AC_12	AC	-	The aircraft system shall ensure the correct transfer into or out of the aircraft's FMS of route data received/sent via data link,in support of the conditions in section 2.4.1.1.	OH_WG78_CPDLC_03	3
AE_03	Misdirection of message	*No SR*	ACSP	-	*No SR*	-	-
		No SR	AC	-	*No SR*	-	-
		No SR	ACSP	-	*No SR*	-	-
		SR_AC_13	AC	-	The aircraft system shall transmit messages to the designated recipient.	OH_WG78_ADSC_05 OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	4 3 3
		SR_AC_14	AC	-	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits	OH_WG78_ADSC_05 OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	4 3 3
		SR_AC_15	AC	-	The aircraft system shall only accept uplink messages intended for it.	OH_WG78_CPDLC_05	3
		SR_AC_16	AC	-	The flight crew shall perform the initiation data link procedure again with any change of the aircraft identifiers (e.g. the Flight Identification and either the Registration Marking or the Aircraft Address)	OH_WG78_CPDLC_05	3
AE_04	Delay of message	*No SR*	ACSP	-	*No SR*	-	-
		No SR	AC	-	*No SR*	-	-
		No SR	ACSP	-	*No SR*	-	-
		No SR	AC	-	*No SR*	-	-
AE_05	Spurious	*No SR*	ACSP	-	*No SR*	-	-

AE		Selected SR					
Ref	Failure mode	Ref	Part	Value	Title	Source	Severity
	message	SR_AC_02	AC	1,00E-05	The likelihood that the aircraft system generates a spurious report shall be less than 1.0E-05/FH .	OH_WG78_ADSC_05	4
		No SR	ACSP	-	*No SR*	-	-
		SR_AC_17	AC	-	The aircraft system shall prevent release of a report/operational response without flight crew action.	OH_WG78_CPDLC_05	3
AE_06	Availability Use	*No SR*	ACSP	-	*No SR*	-	-
		No SR	AC	-	*No SR*	-	-
		No SR	ACSP	-	*No SR*	-	-
		No SR	AC	-	*No SR*	-	-
AE_07	Availability provision	SR_CP_02	ACSP	7,60E-06	The likelihood that the ACSP is unavailable shall be less than 7.6E-06/FH	OH_WG78_ADSC_02 OH_WG78_CPDLC_02 OH_NEW_ALL_02	4 4 4
		SR_AC_03	AC	2,50E-03	The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH	OH_WG78_ADSC_02 OH_WG78_CPDLC_02 OH_NEW_ALL_02	4 4 4
		No SR	ACSP	-	*No SR*	-	-
		SR_AC_18	AC	-	The aircraft system shall provide to the ATSU an indication when it rejects an ADS-C service request initiated by the ATSU at the application layer.	OH_WG78_ADSC_02	4
		SR_AC_19	AC	-	The aircraft system shall indicate to the flight crew a detected loss of ADS-C service.	OH_WG78_ADSC_02	4
		SR_AC_20	AC	-	The aircraft system shall provide to the ATSU an indication when it rejects a CPDLC service request initiated by the ATSU at the application layer.	OH_WG78_CPDLC_02	4

AE		Selected SR					
Ref	Failure mode	Ref	Part	Value	Title	Source	Severity
		SR_AC_21	AC	-	The aircraft system shall display the indication provided by the ATSU when a DSC service request initiated by the flight crew is rejected at the application layer.	OH_WG78_CPDLC_02	4
		SR_AC_22	AC	-	The aircraft system shall indicate to the flight crew a detected loss of data link service.	OH_WG78_CPDLC_02	4
EMM_01	Detection of inappropriate messages by the crew	SR_AC_33	AC		The aircraft system shall provide to the flight crew an indication of the ATSU that has established CPDLC (CDA) service.	OH_WG78_CPDLC_05	3
EMM 02	Detection of corrupted messages	SR_AC_04	AC	1,00E-05	The likelihood that the aircraft system fails to detect the corrupted message shall be less than 1.0E-05/FH	OH_WG78_CPDLC_03	3
		SR_AC_23	AC	-	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.	OH_WG78_CPDLC_03 OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	3 3 3
EMM_05	Detection of delayed downlink messages	SR_AC_05	AC	1,00E-05	The likelihood that the aircraft system incorrectly time stamps a message shall be less than 1.0E-05/FH	OH_WG78_ADSC_05 OH_WG78_CPDLC_05	4 3
		SR_AC_24	AC	-	The aircraft system shall time stamp each report to within one second UTC when it is released for onward transmission.	OH_WG78_ADSC_05	4
		SR_AC_25	AC	-	The aircraft system shall time stamp to within one second UTC each message when it is released for onward transmission.	OH_WG78_ADSC_05	4

AE		Selected SR					
Ref	Failure mode	Ref	Part	Value	Title	Source	Severity
EMM_06	Detection of delayed uplink messages	SR_AC_26	AC	-	When a received message contains a time stamp that indicates the Latency Time Check value, set at equal or less than ETTRN, has been exceeded, the aircraft system shall a) discard the message and send an indication to the Ground System for display to the controller or b) provide the message to the flight crew with an appropriate indication.	OH_WG78_CPDLC_05	3
EMM_07	Detection of misdirected uplink messages	SR_AC_06	AC	1,00E-05	The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH	OH_WG78_CPDLC_04	3
		SR_AC_27	AC	-	The aircraft system shall be able to determine the message initiator.	OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	3 3
		SR_AC_28	AC	-	Once an aircraft accepts operational CPDLC messages from an ATSU, it shall reject operational CPDLC messages from any other ATSU until the first ATSU terminates CPDLC with that aircraft.	OH_WG78_CPDLC_04 OH_WG78_CPDLC_05	3 3
		SR_AC_29	AC	-	Only the ATSU that has control of the aircraft shall be permitted to send a Next Data Authority (NDA) message to the aircraft.	OH_WG78_CPDLC_04	3
EMM_10	Detection of spurious uplink messages	SR_AC_07	AC	1,00E-05	The likelihood to accept a message out of context of the current transaction shall be less than 1.E-5/FH.	OH_WG78_CPDLC_05	3
		SR_AC_30	AC	-	The aircraft system shall indicate in each response to which messages it refers	OH_WG78_CPDLC_05	3
		SR_AC_31	AC	-	Each downlink message shall be uniquely identified for a given aircraft-ATSU pair, following a sequential order	OH_WG78_CPDLC_05	3

AE		Selected SR					
Ref	Failure mode	Ref	Part	Value	Title	Source	Severity
EMM_11	Detection of spurious downlink messages	SR_AC_32	AC	-	The aircraft system shall indicate in each report to which contract number it is referring	OH_WG78_CPDLC_05	3

Table 16 : List of Safety Requirements defined from WG78 and NEW Operational Hazards

Based on this table the applicable Safety Requirements for this study are (this table also presents the Operational Hazard that drives the Safety Requirements and its severity):

Applicable Safety Requirements					
Ref	Part	Failure mode	Value	Title	Source
SR_CP_01	ACSP	Corruption of message	2,80E-03	The likelihood that the ACSP corrupts a report shall be less than 2.8E-03/FH	OH_WG78_FIS_3u (severity 3)
SR_CP_02	ACSP	Availability	7,60E-06	The likelihood that the ACSP is unavailable shall be less than 7.6E-06/FH	OH_WG78_ADSC_02 (severity 4) OH_WG78_CPDLC_02 (severity 4) OH_NEW_ALL_02 (severity 4)
SR_AC_01	AC	Corruption of message	1,00E-05	The likelihood that the aircraft system corrupts a message (downlink or uplink) shall be less than 1.0E-05/FH	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_03 (severity 3) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_02	AC	Spurious message	1,00E-05	The likelihood that the aircraft system generates a spurious report shall be less than 1.0E-05/FH .	OH_WG78_ADSC_05 (severity 4)
SR_AC_03	AC	Availability	2,50E-03	The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH	OH_WG78_ADSC_02 (severity 4) OH_WG78_CPDLC_02 (severity 4) OH_NEW_ALL_02 (severity 4)

Applicable Safety Requirements					
Ref	Part	Failure mode	Value	Title	Source
SR_AC_04	AC	Detection of corrupted messages	1,00E-05	The likelihood that the aircraft system fails to detect the corrupted message shall be less than 1.0E-05/FH	OH_WG78_CPDLC_03 (severity 3)
SR_AC_05	AC	Detection of delayed downlink messages	1,00E-05	The likelihood that the aircraft system incorrectly time stamps a message shall be less than 1.0E-05/FH	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_05 (severity 3)
SR_AC_06	AC	Detection of misdirected uplink messages	1,00E-05	The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH	OH_WG78_CPDLC_04 (severity 3)
SR_AC_07	AC	Detection of spurious uplink messages	1,00E-05	The likelihood to accept a message out of context of the current transaction shall be less than 1.E-5/FH.	OH_WG78_CPDLC_05 (severity 3)
SR_AC_08	AC	Loss of message	-	The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted	OH_WG78_CPDLC_04 (severity 3)
SR_AC_09	AC	Corruption of message	-	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, used for data link initiation correlation and ADS-C network address mapping, shall be unique and unambiguous	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_10	AC	Corruption of message	-	The aircraft system shall prohibit operational processing by flight crew of corrupted messages.	OH_WG78_CPDLC_03 (severity 3)
SR_AC_11	AC	Corruption of message	-	The aircraft system shall execute the route clearance per the route clearance received from the ATS via data link	OH_WG78_CPDLC_03 (severity 3)
SR_AC_12	AC	Corruption of message	-	The aircraft system shall ensure the correct transfer into or out of the aircraft's FMS of route data received/sent via data link,in support of the conditions in section 2.4.1.1.	OH_WG78_CPDLC_03 (severity 3)

Applicable Safety Requirements					
Ref	Part	Failure mode	Value	Title	Source
SR_AC_13	AC	Misdirection of message	-	The aircraft system shall transmit messages to the designated recipient.	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_14	AC	Misdirection of message	-	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_15	AC	Misdirection of message	-	The aircraft system shall only accept uplink messages intended for it.	OH_WG78_CPDLC_05 (severity 3)
SR_AC_16	AC	Misdirection of message	-	The flight crew shall perform the initiation data link procedure again with any change of the aircraft identifiers (e.g. the Flight Identification and either the Registration Marking or the Aircraft Address)	OH_WG78_CPDLC_05 (severity 3)
SR_AC_17	AC	Spurious message	-	The aircraft system shall prevent release of a report/operational response without flight crew action.	OH_WG78_CPDLC_05 (severity 3)
SR_AC_18	AC	Availability	-	The aircraft system shall provide to the ATSU an indication when it rejects an ADS-C service request initiated by the ATSU at the application layer.	OH_WG78_ADSC_02 (severity 4)
SR_AC_19	AC	Availability	-	The aircraft system shall indicate to the flight crew a detected loss of ADS-C service.	OH_WG78_ADSC_02 (severity 4)
SR_AC_20	AC	Availability	-	The aircraft system shall provide to the ATSU an indication when it rejects a CPDLC service request initiated by the ATSU at the application layer.	OH_WG78_CPDLC_02 (severity 4)
SR_AC_21	AC	Availability	-	The aircraft system shall display the indication provided by the ATSU when a DSC service request initiated by the flight crew is rejected at the application layer.	OH_WG78_CPDLC_02 (severity 4)
SR_AC_22	AC	Availability	-	The aircraft system shall indicate to the flight crew a detected loss of data link service.	OH_WG78_CPDLC_02 (severity 4)

Applicable Safety Requirements					
Ref	Part	Failure mode	Value	Title	Source
SR_AC_23	AC	Detection of corrupted messages	-	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.	OH_WG78_CPDLC_03 (severity 3) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_24	AC	Detection of delayed downlink messages	-	The aircraft system shall time stamp each report to within one second UTC when it is released for onward transmission.	OH_WG78_ADSC_05 (severity 4)
SR_AC_25	AC	Detection of delayed downlink messages	-	The aircraft system shall time stamp to within one second UTC each message when it is released for onward transmission.	OH_WG78_ADSC_05 (severity 4)
SR_AC_26	AC	Detection of delayed uplink messages	-	When a received message contains a time stamp that indicates the Latency Time Check value, set at equal or less than ETTRN, has been exceeded, the aircraft system shall a) discard the message and send an indication to the Ground System for display to the controller or b) provide the message to the flight crew with an appropriate indication.	OH_WG78_CPDLC_05 (severity 3)
SR_AC_27	AC	Detection of misdirected uplink messages	-	The aircraft system shall be able to determine the message initiator.	OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_28	AC	Detection of misdirected uplink messages	-	Once an aircraft accepts operational CPDLC messages from an ATSU, it shall reject operational CPDLC messages from any other ATSU until the first ATSU terminates CPDLC with that aircraft.	OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_29	AC	Detection of misdirected uplink messages	-	Only the ATSU that has control of the aircraft shall be permitted to send a Next Data Authority (NDA) message to the aircraft.	OH_WG78_CPDLC_04 (severity 3)

Applicable Safety Requirements					
Ref	Part	Failure mode	Value	Title	Source
SR_AC_30	AC	Detection of spurious uplink messages	-	The aircraft system shall indicate in each response to which messages it refers	OH_WG78_CPDLC_05 (severity 3)
SR_AC_31	AC	Detection of spurious uplink messages	-	Each downlink message shall be uniquely identified for a given aircraft-ATSU pair, following a sequential order	OH_WG78_CPDLC_05 (severity 3)
SR_AC_32	AC	Detection of spurious downlink messages	-	The aircraft system shall indicate in each report to which contract number it is referring	OH_WG78_CPDLC_05 (severity 3)
SR_AC_33	AC	Detection of inappropriate messages by the crew	-	The aircraft system shall provide to the flight crew an indication of the ATSU that has established CPDLC (CDA) service.	OH_WG78_CPDLC_05 (severity 3)

Table 17 : List of applicable ACSP and AC Safety Requirements

4.2 Definition of ACSP and Aircraft Performance Requirements

4.2.1 Identification of relevant Performance Requirements in WG78 documents

This task consists in identifying, in the WG78 Performance Analysis, the performances requirements, that could be relevant for the AeroMACS (that means requirements allocated to Aircraft or ACSP and that concerns the exchange of message between ground and aircraft).

WG78 identify performances requirements in terms of:

- Integrity: WG78 Performance Analysis defines end-to-end integrity requirements, for each data link application. These requirements are directly extracted from WG78 Safety Analysis. There is no specific integrity requirement from a purely performance point of view.

  Consequently, these integrity requirements have already been considered during the safety analysis (cf. § 4.1) and it is not necessary to consider them again.

- Availability. WG78 Performance Analysis defines end-to-end availability requirements, for each data link application. These availability requirements are expressed in terms of "availability of use" and "availability of provision".

  WG78 Performance Analysis then derives these end-to-end availability requirements on the different CNS/ATM components (Aircraft, ACSP and ATSU) using the following formula:

$$A_{ACSP} = A_{ATSU} = \sqrt{A_{Provision}}$$

And $A_{Aircraft} = \frac{A_{Use}}{A_{ACSP} * A_{ATSU}}$

  Availability is defined for each ATM component as the following ratio $A = \frac{MTSO}{MTSO+MTSR}$, expressed in percentage with MTSO: Mean Time to Service Outage and MTSR: Mean Time to Service Restoral.

- Transaction Time (TT). WG78 Performance Analysis defines end-to-end timing requirements, for each data link application. These timing requirements are expressed in terms of:
  - Normal Transaction time (TT95): it defines the time at which 95 percent of all transactions, that are initiated, are completed
  - Transaction Time at 99.9% (TT99.9): it defines the time at which 99.9 percent of all transactions, that are initiated, are completed. This duration is closely linked to the continuity requirement (cf. below)

  Timing requirement are defined for each function of each application: a RCP-Type (Required Communication Performance) is defined for each function with a specific end-to-end timing requirement, expressed in seconds.

  WG78 Performance Analysis then derives these end-to-ends timing requirements on the different CNS/ATM components (Composition by the pilot, recognition by the controller, Aircraft, ACSP and ATSU), using statistical allocation. This allocation methodology leads to larger duration on the different components than the classical arithmetic allocation.

- Continuity: WG78 Performance Analysis defines end-to-end continuity requirements, for each data link application. Continuity is associated with the required level of efficiency or usability of the data communications system. It is defined as the probability that a transaction completes within the expiration time. Consequently, continuity is closely linked to transaction time.

WG78 Performance Analysis then derives these end to end continuity requirements on the different CNS/ATM components (Aircraft, ACSP and ATSU). In this allocation, continuity remains fixed over all ATM components: the allocation is made purely by the transaction time, allocated to each component.

The following table presents the availability, continuity and transaction time requirements allocated by WG78, on ACSP and AC, for each application kind of message:

List of Performance Requirements						
Application	**RCP Type**	**Function**	**Part**	**TT 99,9% - one way (in seconds)**	**TT 95% - one way (in seconds)**	**Availability (in percent)**
CPDLC	RCP 120	*Taxi Clearance; ATC Comm; IM-S; 4DTBO*	ATSU	14	6	99,95%
			ACSP	18	8	99,95%
			AC	23	10	99,40%
	RCP400	*Departure Clearance*	ATSU	14	6	99,95%
			ACSP	18	8	99,95%
			AC	23	10	99,40%
ADS-C	RSP95	*4DTBO, ATC Comm periodic/event reports*	ATSU	7	3	99,95%
			ACSP	9	4	99,95%
			AC	11.5	5	99,40%
	RSP120	*4DTBO; ATC Comm single/1st periodic/baseline report*	ATSU	14	6	99,95%
			ACSP	18	8	99,95%
			AC	23	10	99,40%
D-FIS	RIP180	*ATIS, NOTAM, VOLMET, HZWX, RVR*	ATSU	155	67	99,90%
			ACSP	32	14	99,90%
			AC	74	32	99,90%

Table 18: Relevant ACSP and AC performance requirements (Availability, Continuity, and Transaction times)

4.2.2 Selection of applicable ACSP and AC performance requirements

Several relevant Performance Requirements have been identified in the previous chapters on ACSP and AC systems. This task now consists in identifying, for each parameter (availability, continuity and transaction time), the most stringent requirement (that is the applicable requirement):

- Availability: selection of the highest percentage among all values of document [5].
- Normal Transaction Time (TT 95 %): selection of the lowest TT 95% value in document [5].

  In facts this selection might be not totally exact if it exists different categories of messages, with different priority classes that could affect the transaction time. However, this is the requirement for transactions with the highest level of priority.
- Continuity / Transaction Time 99.9 %: The same continuity requirement is defined on all ATM components for all applications (see document [5]): 0.999 per transaction. This requirement defines the probability that the transaction completes within a given duration. If the continuity requirement is 0.999, this duration that all transactions shall respect is the Transaction Time at 99.9% (TT 99.9 %).

Consequently a common continuity / TT 99.9% requirement is defined specifying the delay that 99.9 % of all transactions shall respect. This requirement is the lowest TT 99.9% value in document [5].

The selected Performance Requirements are referenced as follow: "*PR_XX_YY: xxxx*"

- XX: identify the part on which the performance requirement is allocated: "*CP*" for ACSP or "*AC*" for Aircraft System
- YY: is a reference number of the selected performance requirement
- *xxxx* value of the performance requirement (expressed in percent for availability, and in seconds for transaction times).

The following table presents the selected ACSP and AC performance requirements (in red: quantitative requirement, in green: qualitative requirements).:

Selected Performance Requirement					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
PR_CP_01	ACSP	Transaction Time 99,9 % (in seconds)	9	The transaction time (one way) in ACSP shall be less than 9 seconds for 99.9% of the messages	Performance analysis ADS-C - RSP 95
PR_CP_02	ACSP	Transaction Time 95 % (in seconds)	4	The transaction time (one way) in ACSP shall be less than 4 seconds for 95% of the messages	Performance analysis ADS-C - RSP 95
PR_CP_03	ACSP	Availability (in percent)	99,95%	The availability of the ACSP shall be more than 99.95%	Performance analysis CPDLC - RCP 120 CPDLC - RCP 400 ADS-C - RSP 95 ADS-C - RSP 120
PR_CP_04	ACSP	Availability (in percent)	-	The ground system shall be capable of detecting ground system failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function.	Performance analysis
PR_CP_05	ACSP	Availability (in percent)	-	When the communication service no longer meets the requirements for the intended function, the ground system shall provide indication to the controller.	Performance analysis
PR_AC_01	AC	Transaction Time 99,9 % (in seconds)	11,5	The transaction time (one way)in aircraft shall be less than 11.5 seconds for 99.9% of the ADS-C - RSP 95 messages	Performance analysis ADS-C - RSP 95
PR_AC_02	AC	Transaction Time 95 % (in seconds)	5	The transaction time (one way)in aircraft shall be less than 5 seconds for 95% of the ADS-C - RSP 95 messages	Performance analysis ADS-C - RSP 95
PR_AC_03	AC	Availability (in percent)	99,40%	The availability of the ADS-C aircraft system shall be more than 99.40%	Performance analysis CPDLC - RCP 120 CPDLC - RCP 400 ADS-C - RSP 95 ADS-C - RSP 120

Selected Performance Requirement					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
PR_AC_04	AC	Availability (in percent)	-	The aircraft system shall be capable of detecting aircraft system failures or loss of air/ground communication that would cause the aircraft communication capability to no longer meet the requirements for the intended function.	Performance analysis
PR_AC_05	AC	Availability (in percent)	-	When the aircraft communication capability no longer meets the requirements for the intended function, the aircraft system shall provide indication to the flight crew.	Performance analysis

Table 19: Selected ACSP and AC performance requirements

4.3 Summary of Safety and Performance requirements applicable to ACSP and Aircraft

The following table is the detailed ACSP and AC requirement list:

Requirement list					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
PR_CP_01	ACSP	Transaction Time 99,9 % (in seconds)	9	The transaction time (one way) in ACSP shall be less than 9 seconds for 99.9% of the messages	Performance analysis ADS-C - RSP 95
PR_CP_02	ACSP	Transaction Time 95 % (in seconds)	4	The transaction time (one way) in ACSP shall be less than 4 seconds for 95% of the messages	Performance analysis ADS-C - RSP 95
PR_CP_03	ACSP	Availability (in percent)	99,95%	The availability of the ACSP shall be more than 99.95%	Performance analysis CPDLC - RCP 120 CPDLC - RCP 400 ADS-C - RSP 95 ADS-C - RSP 120
PR_CP_04	ACSP	Availability	-	The ground system shall be capable of detecting ground system failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function.	Performance analysis
PR_CP_05	ACSP	Availability	-	When the communication service no longer meets the requirements for the intended function, the ground system shall provide indication to the controller.	Performance analysis
SR_CP_01	ACSP	Corruption of message (per flight hour)	2,80E-03	The likelihood that the ACSP corrupts a report shall be less than 2.8E-03/FH	OH_WG78_FIS_3u (severity 3)
SR_CP_02	ACSP	Availability (per flight hour)	7,60E-06	The likelihood that the ACSP is unavailable shall be less than 7.6E-06/FH	OH_WG78_ADSC_02 (severity 4) OH_WG78_CPDLC_02 (severity 4) OH_NEW_ALL_02 (severity 4)

Requirement list					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
PR_AC_01	AC	Transaction Time 99,9 % (in seconds)	11,5	The transaction time (one way) in aircraft shall be less than 11.5 seconds for 99.9% of the ADS-C - RSP 95 messages	Performance analysis ADS-C - RSP 95
PR_AC_02	AC	Transaction Time 95 % (in seconds)	5	The transaction time (one way) in aircraft shall be less than 5 seconds for 95% of the ADS-C - RSP 95 messages	Performance analysis ADS-C - RSP 95
PR_AC_03	AC	Availability (in percent)	99,40%	The availability of the ADS-C aircraft system shall be more than 99.40%	Performance analysis CPDLC - RCP 120 CPDLC - RCP 400 ADS-C - RSP 95 ADS-C - RSP 120
PR_AC_04	AC	Availability	-	The aircraft system shall be capable of detecting aircraft system failures or loss of air/ground communication that would cause the aircraft communication capability to no longer meet the requirements for the intended function.	Performance analysis
PR_AC_05	AC	Availability	-	When the aircraft communication capability no longer meets the requirements for the intended function, the aircraft system shall provide indication to the flight crew.	Performance analysis
SR_AC_01	AC	Corruption of message (per flight hour)	1,00E-05	The likelihood that the aircraft system corrupts a message (downlink or uplink) shall be less than 1.0E-05/FH	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_03 (severity 3) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_02	AC	Spurious message (per flight hour)	1,00E-05	The likelihood that the aircraft system generates a spurious report shall be less than 1.0E-05/FH .	OH_WG78_ADSC_05 (severity 4)

Requirement list					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
SR_AC_03	AC	Availability (per flight hour)	2,50E-03	The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH	OH_WG78_ADSC_02 (severity 4) OH_WG78_CPDLC_02 (severity 4) OH_NEW_ALL_02 (severity 4)
SR_AC_04	AC	Detection of corrupted messages (per flight hour)	1,00E-05	The likelihood that the aircraft system fails to detect the corrupted message shall be less than 1.0E-05/FH	OH_WG78_CPDLC_03 (severity 3)
SR_AC_05	AC	Detection of delayed downlink messages (per flight hour)	1,00E-05	The likelihood that the aircraft system incorrectly time stamps a message shall be less than 1.0E-05/FH	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_05 (severity 3)
SR_AC_06	AC	Detection of misdirected uplink messages (per flight hour)	1,00E-05	The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH	OH_WG78_CPDLC_04 (severity 3)
SR_AC_07	AC	Detection of spurious uplink messages (per flight hour)	1,00E-05	The likelihood to accept a message out of context of the current transaction shall be less than 1.E-5/FH.	OH_WG78_CPDLC_05 (severity 3)
SR_AC_08	AC	Loss of message	-	The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted	OH_WG78_CPDLC_04 (severity 3)
SR_AC_09	AC	Corruption of message	-	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, used for data link initiation correlation and ADS-C network address mapping, shall be unique and unambiguous	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)

Requirement list					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
SR_AC_10	AC	Corruption of message	-	The aircraft system shall prohibit operational processing by flight crew of corrupted messages.	OH_WG78_CPDLC_03 (severity 3)
SR_AC_11	AC	Corruption of message	-	The aircraft system shall execute the route clearance per the route clearance received from the ATS via data link	OH_WG78_CPDLC_03 (severity 3)
SR_AC_12	AC	Corruption of message	-	The aircraft system shall ensure the correct transfer into or out of the aircraft's FMS of route data received/sent via data link,in support of the conditions in section 2.4.1.1.	OH_WG78_CPDLC_03 (severity 3)
SR_AC_13	AC	Misdirection of message	-	The aircraft system shall transmit messages to the designated recipient.	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_14	AC	Misdirection of message	-	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits	OH_WG78_ADSC_05 (severity 4) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_15	AC	Misdirection of message	-	The aircraft system shall only accept uplink messages intended for it.	OH_WG78_CPDLC_05 (severity 3)
SR_AC_16	AC	Misdirection of message	-	The flight crew shall perform the initiation data link procedure again with any change of the aircraft identifiers (e.g. the Flight Identification and either the Registration Marking or the Aircraft Address)	OH_WG78_CPDLC_05 (severity 3)
SR_AC_17	AC	Delay of message	-	The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted	OH_WG78_CPDLC_04 (severity 3)
SR_AC_18	AC	Availability	-	The aircraft system shall provide to the ATSU an indication when it rejects an ADS-C service request initiated by the ATSU at the application layer.	OH_WG78_ADSC_02 (severity 4)

Requirement list					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
SR_AC_19	AC	Availability	-	The aircraft system shall indicate to the flight crew a detected loss of ADS-C service.	OH_WG78_ADSC_02 (severity 4)
SR_AC_20	AC	Availability	-	The aircraft system shall provide to the ATSU an indication when it rejects a CPDLC service request initiated by the ATSU at the application layer.	OH_WG78_CPDLC_02 (severity 4)
SR_AC_21	AC	Availability	-	The aircraft system shall display the indication provided by the ATSU when a DSC service request initiated by the flight crew is rejected at the application layer.	OH_WG78_CPDLC_02 (severity 4)
SR_AC_22	AC	Availability	-	The aircraft system shall indicate to the flight crew a detected loss of data link service.	OH_WG78_CPDLC_02 (severity 4)
SR_AC_23	AC	Detection of corrupted messages	-	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.	OH_WG78_CPDLC_03 (severity 3) OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_24	AC	Detection of delayed downlink messages	-	The aircraft system shall time stamp each report to within one second UTC when it is released for onward transmission.	OH_WG78_ADSC_05 (severity 4)
SR_AC_25	AC	Detection of delayed downlink messages	-	The aircraft system shall time stamp to within one second UTC each message when it is released for onward transmission.	OH_WG78_ADSC_05 (severity 4)
SR_AC_26	AC	Detection of delayed uplink messages	-	When a received message contains a time stamp that indicates the Latency Time Check value, set at equal or less than ETTRN, has been exceeded, the aircraft system shall a) discard the message and send an indication to the Ground System for display to the controller or b) provide the message to the flight crew with an appropriate indication.	OH_WG78_CPDLC_05 (severity 3)

Requirement list					
Ref	**Part**	**Parameter**	**Value**	**Title**	**Source**
SR_AC_27	AC	Detection of misdirected uplink messages	-	The aircraft system shall be able to determine the message initiator.	OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_28	AC	Detection of misdirected uplink messages	-	Once an aircraft accepts operational CPDLC messages from an ATSU, it shall reject operational CPDLC messages from any other ATSU until the first ATSU terminates CPDLC with that aircraft.	OH_WG78_CPDLC_04 (severity 3) OH_WG78_CPDLC_05 (severity 3)
SR_AC_29	AC	Detection of misdirected uplink messages	-	Only the ATSU that has control of the aircraft shall be permitted to send a Next Data Authority (NDA) message to the aircraft.	OH_WG78_CPDLC_04 (severity 3)
SR_AC_30	AC	Detection of spurious uplink messages	-	The aircraft system shall indicate in each response to which messages it refers	OH_WG78_CPDLC_05 (severity 3)
SR_AC_31	AC	Detection of spurious uplink messages	-	Each downlink message shall be uniquely identified for a given aircraft-ATSU pair, following a sequential order	OH_WG78_CPDLC_05 (severity 3)
SR_AC_32	AC	Detection of spurious downlink messages	-	The aircraft system shall indicate in each report to which contract number it is referring	OH_WG78_CPDLC_05 (severity 3)
SR_AC_33	AC	Detection of inappropriate messages by the crew	-	The aircraft system shall provide to the flight crew an indication of the ATSU that has established CPDLC (CDA) service.	OH_WG78_CPDLC_05 (severity 3)

Table 20 : Selected ACSP and AC Requirements

5 Definition of Safety and Performance requirements applicable to the AeroMACS ground system

5.1 Functional description of the ground infrastructure – ACSP

5.1.1 Network Reference Model

The Wimax Forum (WMF) has developed a Network Reference Model which is a logical description of the communication infrastructure covering the AeroMACS system and the surrounding IP network enabling the provision of wireless connection between mobile user and application servers.

The following three sub-domains are defined in the WMF document (see [6]) as follows:

- the Mobile Station (MS): Generalized mobile equipment set providing connectivity between subscriber equipment and a base station (BS). The Mobile Station MAY be a host or a CPE type of device that supports multiple hosts,
- the Access Service Network (ASN): Access Service Network (ASN) is defined as a complete set of network functions needed to provide radio access to a WiMAX subscriber.
- the Connectivity Service Network (CSN): Connectivity Service Network (CSN) is defined as a set of network functions that provide IP connectivity services to the WiMAX subscriber(s).

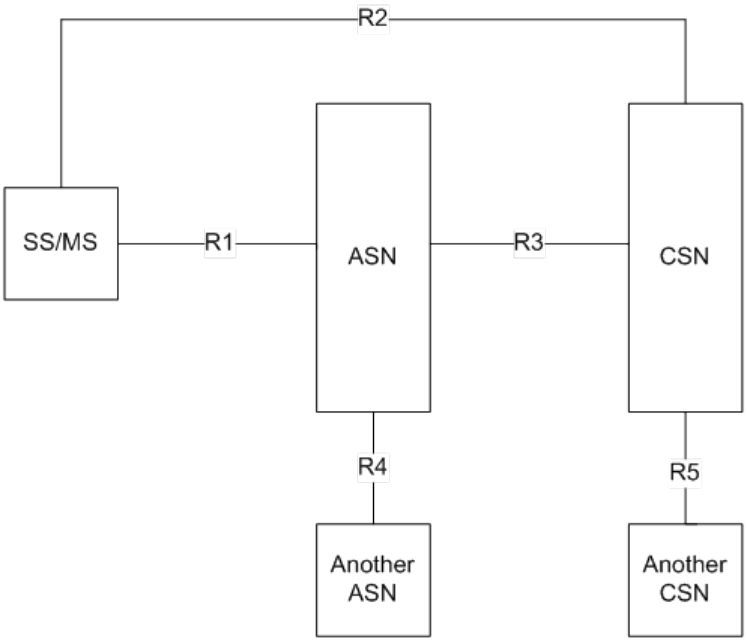


Figure 10: Network Reference Model

NOTE: Each of the entities, MS, ASN and CSN represent a grouping of functional entities. Each of these functions may be realized in a single physical functional entity or may be distributed over multiple physical functional entities.

According to these definitions:

- the avionics domain defined in WG78 is larger than the MS sub-domain since the latter covers only the physical layer up to the IP level.

- **the ACSP domain defined in WG78 is comparable to the aggregation of the ASN and CSN sub-domains, these two sub-domains are presented below (see § 5.1.2 and 5.1.3)**

5.1.2 ASN: the Access Service Network

The ASN reference model is illustrated in Figure 11. An ASN shares R1 reference point (RP) with an MS, R3 RP with a CSN and R4 RP with another ASN. The ASN consists of at least one instance of a Base Stations (BS) and at least one instance of an ASN Gateway (ASN-GW). A BS is logically connected to one or more ASN Gateways. The R4 reference point is the only RP for Control and Bearer Planes for interoperability between similar or heterogeneous ASNs. Interoperability between any types of ASNs is feasible with the specified protocols and primitives exposed across R1, R3 and R4 Reference Points.

NOTE: When ASN is composed of n ASN-GWs (where n > 1), Intra ASN mobility MAY involve R4 control messages and Bearer Plane establishment.

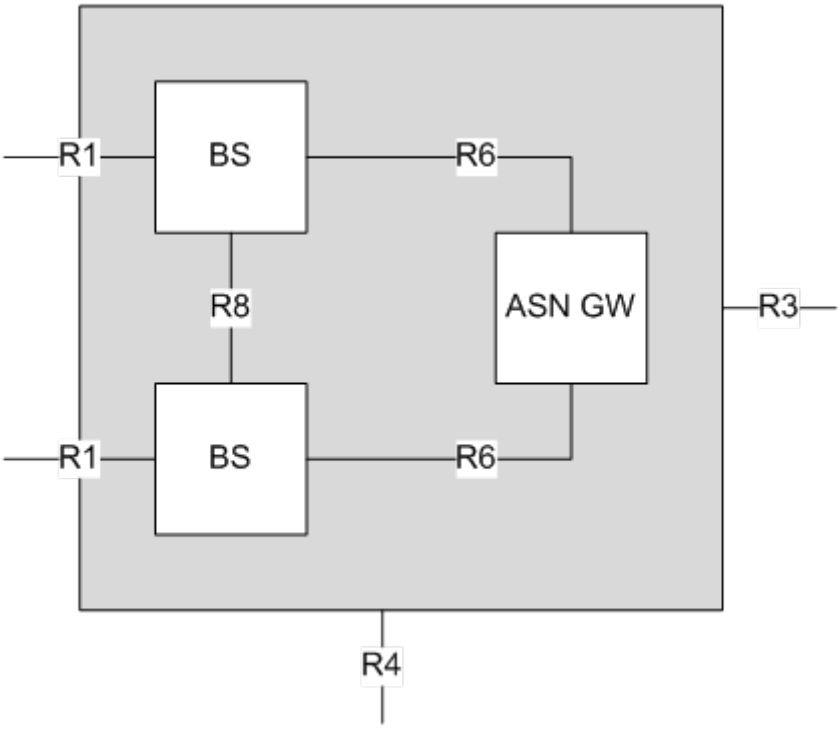


Figure 11: ASN Reference Model

5.1.2.1 Base Stations

The AeroMACS Base Station (BS) is a logical entity that embodies a full instance of the MAC and PHY layers in compliance with the AeroMACS Specifications and may host one or more access functions. A BS instance represents one sector with one frequency assignment. It incorporates scheduler functions for uplink and downlink resources. Connectivity (i.e., reachability) of a single BS to more than one ASN-GW may be required for load balancing or a redundancy option. BS is logical entity and one physical implementation of BS can have multiple BSs.
It incorporates HO Control and Radio Resource Management (RRM) functions.

5.1.2.2 ASN Gateways

The ASN Gateway (ASN-GW) is a logical entity that represents an aggregation of Control Plane functional entities that are either paired with a corresponding function in the ASN (e.g. BS instance), a

resident function in the CSN or a function in another ASN. The ASN-GW may also perform Bearer Plane routing or bridging function.
ASN-GW implementation may include redundancy and load-balancing based on radio parameters among several ASN-GWs. ASN-GW implementations shall include load-balancing based on SLA requirements of the MSs. For every MS, a BS is associated with exactly one default ASN GW. However, ASN-GW functions for every MS may be distributed among multiple ASN-GWs located in one or more ASN(s).

5.1.2.3 AeroMACS ASN Profile

A profile maps ASN functions into BS and ASN-GW so that protocols and messages over the exposed reference point are identified. This thus ensures interoperability between the physical entities forming part of the ASN.

The WMF has specified three profiles showing three possible implementations of the ASN features.

For the AeroMACS implementation, it was decided to implement **profile C** (see AeroMACS Functional Definition in document T32-002 (see [6]).

According to Profile C, ASN functions are mapped into ASN-GW and BS as shown in Figure 12: WMF ASN Profile C. Key attributes of Profile C are:

- HO Control is in the Base Station.
- RRC is in the BS that would allow RRM within the BS. An “RRC Relay” is in the ASN GW, to relay the RRM messages sent from BS to BS via R6.
- ASN Anchored mobility among BSs SHALL be achieved by utilizing R6 and R4 physical connections.

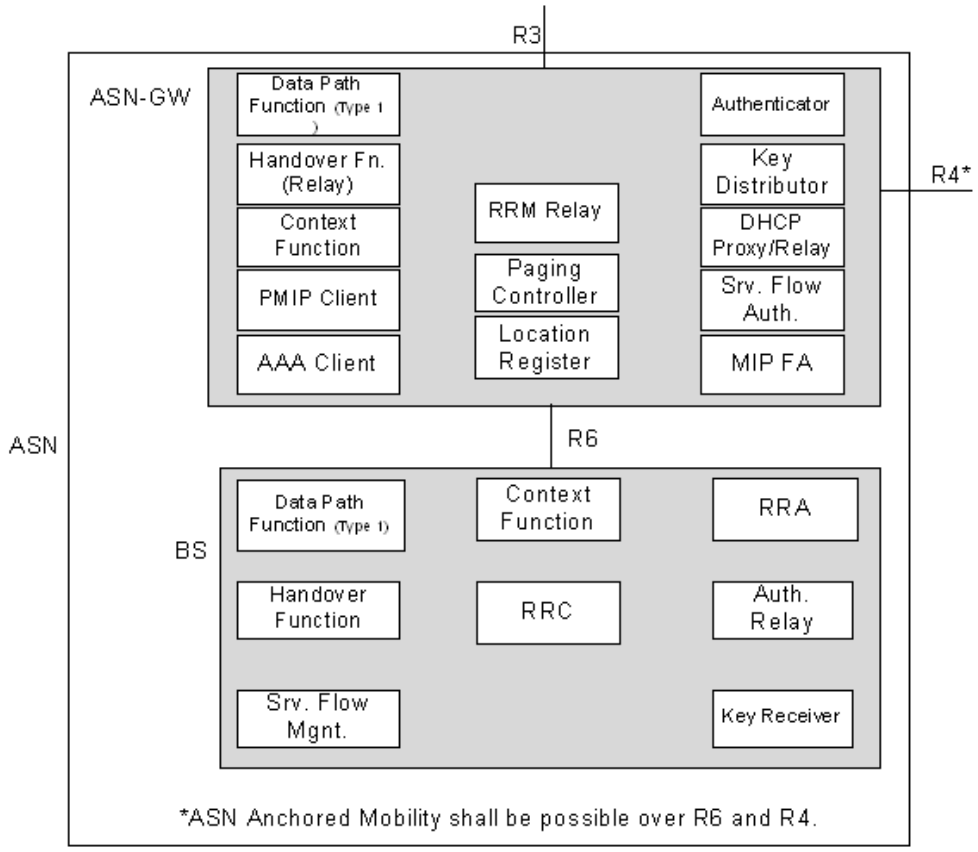


Figure 12: WMF ASN Profile C

NOTE: The depiction of a function on either the ASN GW or the BS in the figures below does not imply that the function exists in all manifestations of this profile. Instead, it indicates that if the function existed in a manifestation it would reside on the entity shown. For example, PMIP Client may not always be present in all manifestations of Profile C. However, if it is used, it shall reside on the ASN GW.

5.1.3 CSN: the Connectivity Service Network

In T32-002 (see [6]), Connectivity Service Network (CSN) is defined as follows: CSN is a set of network functions that provide IP connectivity services to the WiMAX subscriber(s). A CSN may provide the following functions:

- MS IP address and endpoint parameter allocation for user sessions,
- Internet access,
- AAA proxy and server,
- Policy and Admission Control based on user subscription profiles,
- ASN-CSN tunneling support,
- WiMAX subscriber billing and inter-operator settlement,
- Inter-CSN tunnelling for roaming,
- Inter-ASN mobility.

CSN MAY comprise network elements such as routers, AAA proxy/servers, user databases, Interworking gateway MSs. A CSN may be deployed as part of a Greenfield WiMAX NSP or as part of an incumbent WiMAX NSP.

5.1.4 Communication infrastructure (ACSP) model

The ACSP domain, as defined in WG78, covers all the functions related the communication service provided to the mobiles. The boundaries of this domain are:

- The RF interface towards the aircraft.
- The border router serving the ATSU domain hosting the terminal communicating equipment and the application server(s) interacting with the ATM system.

Based on the WMF functional description, the ACSP domain encompasses:

- **the ASN,**
- **the CSN including visited and home networks if any,**

To apportion the different requirements applicable to the ACSP domain, additional details are needed in the way the system is designed.

Nevertheless, it is not possible to describe really in detail the ground communication infrastructure since:

- Additional work is needed to further identify the different function implemented at CSN level. This work will be done in other SESAR projects (e.g. P15.2.4) and at ICAO level,

- The implementation of the various functions notably at CSN level will probably be very dependent upon manufacturers and service provider's choices.

A very high level functional architecture is thus presented in this section and the derived requirements can only be considered as recommendations.

The communication infrastructure is described as below:

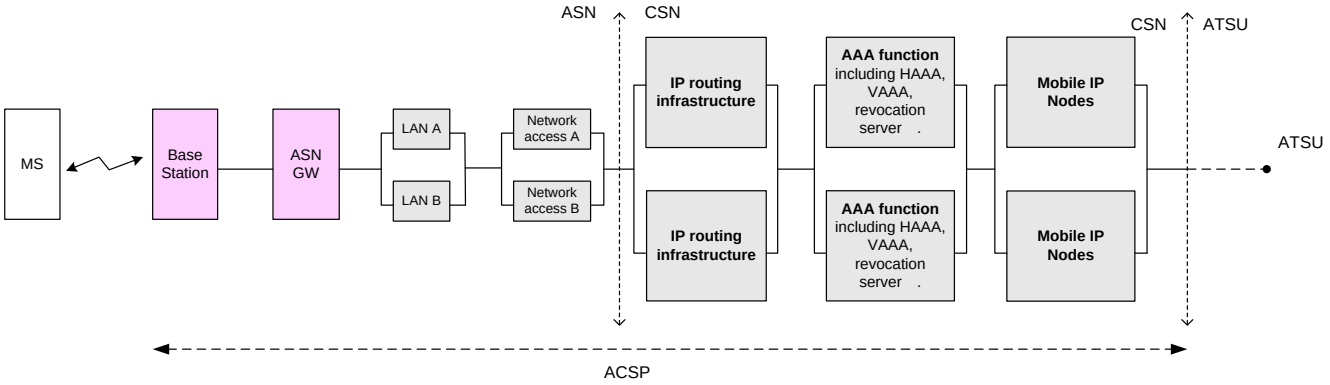


Figure 13 : Communication infrastructure model

The ASN is made of the following components with the associated assumptions (considering state of the art for implementation):

- The base station serving the whole or part of the airport surface:
  - no assumption is taken regarding the implementation of redundancy,
  - no assumption is taken regarding its MTBF
  - MTTR = 19 hours (5 days a week, H8 and Time to intervene = 4 hours),
  - the base station is in charge of the RF Media Access and the packet scheduling function. One can consider as reasonable to allocate a greater part of the transaction time to the Base Station compared to the other components of the communication infrastructure since their contribution to the transaction time will be mainly processing time,
- The ASN Gateway function:
  - no assumption is taken regarding the implementation of redundancy,
  - serving the whole airport and thus potentially connected to several Base Stations. The loss of the ASN Gateway will have a greater impact on the service than the loss of a Base Station
  - no assumption is taken in terms of MTBF
  - MTTR = 19 hours (5 days a week, H8 and Time to intervene = 4 hours),
  - The contribution of the ASN GW to the transaction time will be mainly due to its processing time,
- The Airport Local Network made of redundant LAN components
  - MTBF = 60 000 hours per component,
  - MTTR = 19 hours (5 days a week, H8 and Time to intervene = 4 hours),
  - The ASN Gateway and Base Station have a redundant attachment to the network

- The network access:
    - Redundant access: it is assumed that a redundant access will be available since a typical availability for single network access is 99,9% and thus less than the objective (99.95%).
    - The network access shall be independent.

NOTE: The airport power supply can be reasonably considered as redundant and offering a high quality of service.

NOTE: A 60 000 hour MTBF is deemed as a typical MTBF for a Network node.

NOTE : The network architecture for the ASN domain here above is quite simple and can be representative of the infrastructure deployed by an ACSP if this latter acts as ASN for a given airport.

In the case the ACSP outsources to the ASN operation to another entity (airport operator, local ATSP), it is likely that the ASN components will be integrated in the network of the ASN operator. The communication between the ASN and the CSN would be done through Security Gateway which would be redundant and thus would offer great QoS.

CSN is made of the following components:

AAA function and certificate revocation function:

- this function can be spread over several AAA nodes acting for a given aircraft as proxy or server,
- it is assumed that the failure of this function could have an impact at, at least, regional scale. Consequently, AAA operator will take necessary measures to ensure great availability and continuity of service for this function,
- the contribution of the AAA function to the transaction time will be mainly due to its processing time:

Mobile IP nodes:

- it is assumed that the failure of this function could have an impact at, at least, regional scale. Consequently, Mobile IP operator will take necessary measures to ensure great availability and continuity of service for this function,
- the contribution of this function to the transaction time will be mainly due to its processing time

IP routing infrastructure:

- this IP infrastructure ensures connectivity for an Aircraft at worldwide scale. It thus can interconnect Home and Visited Networks,
- it is made of routers, security components (e.g. firewall), connected by leased lines….
- it is assumed that the failure of this function could have an impact at, at least, regional scale. Consequently, the operator will take necessary measures to ensure great availability and continuity of service for this function,
- the contribution of this function to the transaction time will be much less than the ASN one.

The following more detailed assumptions are taken for the CSN **service**:

The CSN network is made of two redundant (and totally independent) chains of communication (including the power supply), each one having the following parameters:

- availability = 99,8%
- MTBF = 15 000 hours
- MTTR = MTTR = 19 hours (5 days a week, H8 and Time to intervene = 4 hours),

The 12 500 hour MTBF is derived considering 4 network nodes (e.g. Firewall, Firewall, Home Agent, AAA server), each having a 60 000 hour MTBF.

NOTE: It should be noticed that assuming the CSN functions are made redundant, the influence of the number of network nodes and the MTBF of each one is limited with regards to the availability objective, as shown in the table below:

Nbr_Net_components	MTBF_component	MTBF_chain	MTTR	A_chain	A_redundant_chain
3	60000	20000	19	0,99905	0,999999
4	60000	15000	19	0,99873	0,999998
5	60000	12000	19	0,99842	0,999998
6	60000	10000	19	0,99810	0,999996
7	60000	8571	19	0,99779	0,999995
8	60000	7500	19	0,99747	0,999994
9	60000	6667	19	0,99716	0,999992
10	60000	6000	19	0,99684	0,999990

Table 21: Variation of CSN availability with regards to the number of network nodes

5.2 Allocation of safety and performance requirements to the AeroMACS ground system

This section identifies the ACSP components which could be involved in the degradation of the performance and safety level with regards to the requirements identified previously.

Then, the ACSP safety and performance requirements are apportioned to the different parts of the ACSP, and notably the AeroMACS system.

5.2.1 Furthermore, requirements are apportioned to the various AeroMACS sub components based on different set of assumptions in terms of MTBF for ASN GW and BS being components of the ASN. Allocation of requirements regarding corruption

The following safety requirement applicable to the ACSP is identified:

- **SR_CP_01: The likelihood that the ACSP corrupts a report shall be less than 2.8E-03/FH**

NOTE: This requirement should disappear in the next update of working group 78 documents.

5.2.2 Allocation of availability requirements - Hardware

The following two availability requirements will be allocated:

Performance = PR_CP_03: The availability of the ACSP shall be more than 99.95%.

Safety = SR_CP_02: The likelihood that the ACSP is unavailable shall be less than 7.6E-06/FH.

The expression of Safety Requirements per flight hour (FH) is consistent with standards. However, in order to properly evaluate the safety risk for the ACSP, the quantitative safety requirements should be specified in units of probability per Sector Operational Hour (SOH).

The following table, extracted from WG78 Operational Safety Assessment, provides the conversion factor from safety requirements per flight hour to safety requirements per sector operational hours, in each domain (APT, TMA, and ENR).

UNIT CONVERSION		
Flight phase	**FH / SOH**	**Failure / SOH**
APT	61	Failure/FH x 61
TMA	16	Failure/FH x 16
ENR-1	26	Failure/FH x 26

Table 22: Unit Conversion Table

Consequently, the availability **safety** requirement, for ACSP, in Airport environment is:

SR_CP_01: The likelihood that the ACSP is unavailable shall be less than 4.3E-04/SOH

NOTE: 1 over 4.3E-04/SOH is equivalent of the MTBF of the ACSP service over AeroMACS.

NOTE: the availability requirement coming from the performance analysis for the ACSP service over AeroMACS is 99.95%.

According to the model previously presented contributors to unavailability of the ACSP service can be due to:

- **an ASN failure at :**
  - The Base Station
  - The ASN gateway
  - The Airport Local Network
  - The Network access
- **a CSN failure.**

NOTE:

- *it is assumed that the airport power supply availability is about 100%,*
- *it is assumed that failure at ASN and at CSN are independent.*

The following formulas are reminded:

$$A_i = \frac{MTBF_i}{MTTR_i + MTBF_i}$$

$$MTBF_{AND} = \frac{1}{\prod_{i=1}^{n}\frac{MTTR_i}{MTBF_i}\sum_{i=1}^{n}\frac{1}{MTTR_i}}, \quad MTTR_{AND} = \frac{1}{\sum_{i=1}^{n}\frac{1}{MTTR_i}}$$

$$MTBF_{OR} = \frac{1}{\sum_{i=1}^{n}\frac{1}{MTBF_i}}, \quad MTTR_{OR} = \frac{\sum_{i=1}^{n}\frac{MTTR_i}{MTBF_i}}{\sum_{i=1}^{n}\frac{1}{MTBF_i}},$$

5.2.2.1 SCENARIO 1: the ASN Gateway is not redundant

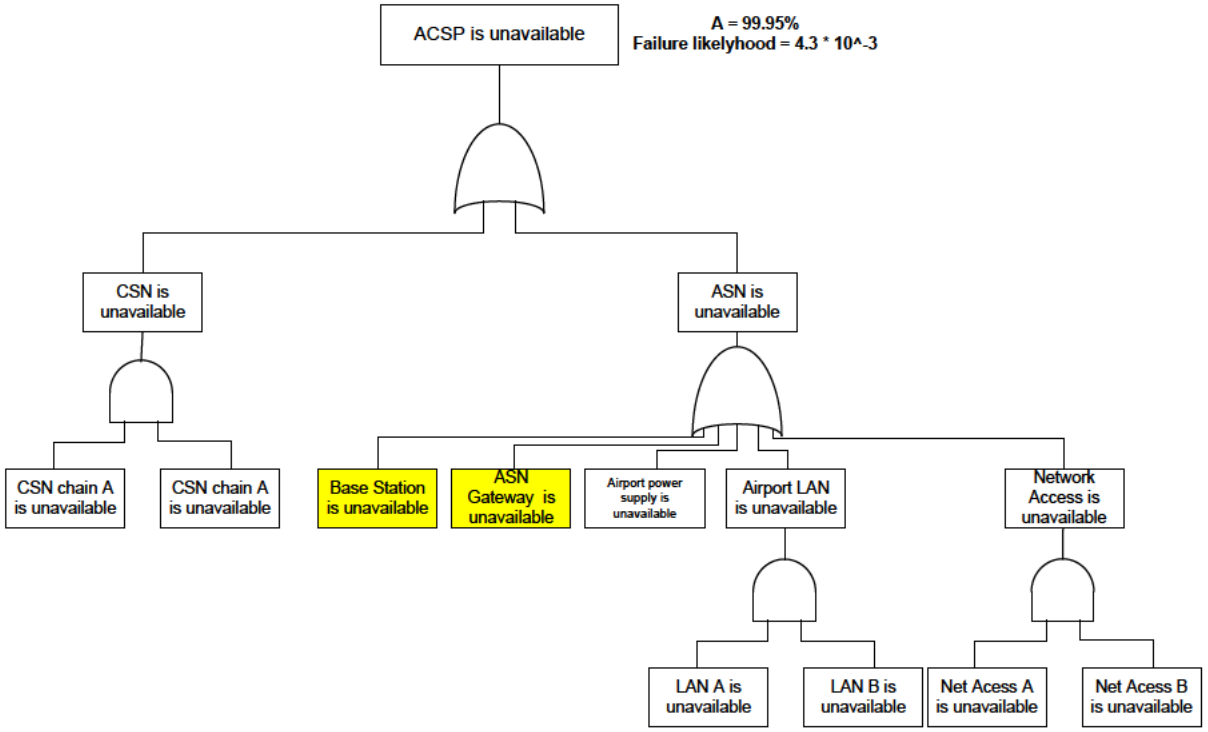


Figure 14 : ACSP availability fault tree - ASN Gateway & base station not redundant

First approach for the apportionment: the ASN gateway and the Base station have the same weight in the likelihood of unavailability of the service.

			MTBF	1/MTBF	MTTR	Availibility
ACSP		**Objectives**		**4,300E-04**		**0,999500**
	CSN					
		CSN chain A	*15000*		*19*	*0,99873*
		CSN chain B	*15000*		*19*	*0,99873*
		CSN chain A + B				*1,00000*
	ASN					
		Redundant Power supply				***1,00000***
		Network access A	*18981*		*19*	*0,99900*
		Network access B	*18981*		*19*	*0,99900*

		Network access A + B				***1,00000***
		LAN A	*60000*		*19*	*0,99968*
		LAN B	*60000*		*19*	*0,99968*
		LAN A + B				***1,00000***
		AeroMACS	***38192***	***2,618E-05***	*19*	***0,99950***
		ASN Gateway	*76384*	*1,30917E-05*	*19*	*0,99975*
		Base Station	*76384*	*1,30917E-05*	*19*	*0,99975*

Table 23 : Apportionment of reliability requirement on ASN Gateway and base Station with scenario 1 (ASN Gateway & base station not redundant) – Same allocation on ASN and base station

NOTE: compliance with Performance Availability requirement ensures compliance with the Safety Availability requirement.

Second approach for the apportionment: as mentioned previously, the failure of the ASN gateway will impact the whole service at the airport if it is not redundant. Consequently, it is proposed to allocate a more stringent requirement to the ASN gateway compared to the Base station.

This assumption is also relevant since the RF function is usually less reliable than "low power" function.

It is proposed to fix the MTBF of the Base Station to **50 000 hours**. Then:

			MTBF	1/MTBF	MTTR	Availibility
ACSP		**Objectives**		**4,300E-04**		**0,999500**
	CSN					
		CSN chain A	*15000*		*19*	*0,99873*
		CSN chain B	*15000*		*19*	*0,99873*
		CSN chain A + B				*1,00000*
	ASN					
		Redundant Power supply				***1,00000***
		Network access A	*18981*		*19*	*0,99900*
		Network access B	*18981*		*19*	*0,99900*
		Network access A + B				***1,00000***
		LAN A	*60000*		*19*	*0,99968*
		LAN B	*60000*		*19*	*0,99968*
		LAN A + B				***1,00000***
		AeroMACS	***38191***	***2,618E-05***	*19*	***0,99950***
		ASN Gateway	*161697*	*6,1844E-06*	*19*	*0,99988*
		Base Station	*50000*	*0,00002*	*19*	*0,99962*

Table 24: Apportionment of reliability requirement on ASN Gateway and base Station with scenario 1 (ASN Gateway & base station not redundant) – MTBF of base station is fixed at 65 000 hours

In relaxing the requirement applicable to the Base Station, the MTBF of the ASN Gateway becomes 161 697 hours. This requirement can not be met without implementing redundancy.

NOTE: The following table shows the variation of the MTBF for ASN Gateway with regard to the MTBF of the Base Station.

MTBF (hours)	
Base Station	ASN Gateway
75000	77820
70000	84049
65000	92601
60000	105074
55000	124966
50000	161697

Table 25: Apportionment of reliability requirement on ASN Gateway and base Station – Variation of the MTBF of ASN Gateway with regards to the MTBF of the Base Station

NOTE: without implementing redundancy at Airport LAN, one can release the need for double attachment at ASN GW and Base Station level. Even with a MTBF = 150 000 hours for the LAN component, the resulted MTBF for the Base Station and the ASN Gateway become very stringent (90 000 and 120 000 hours).

5.2.2.2 SCENARIO 2: the ASN Gateway is redundant at the airport

It is assumed:

- that the ASN gateway is redundant at the airport,
- all the Base Stations is connected to each ASN Gateway.

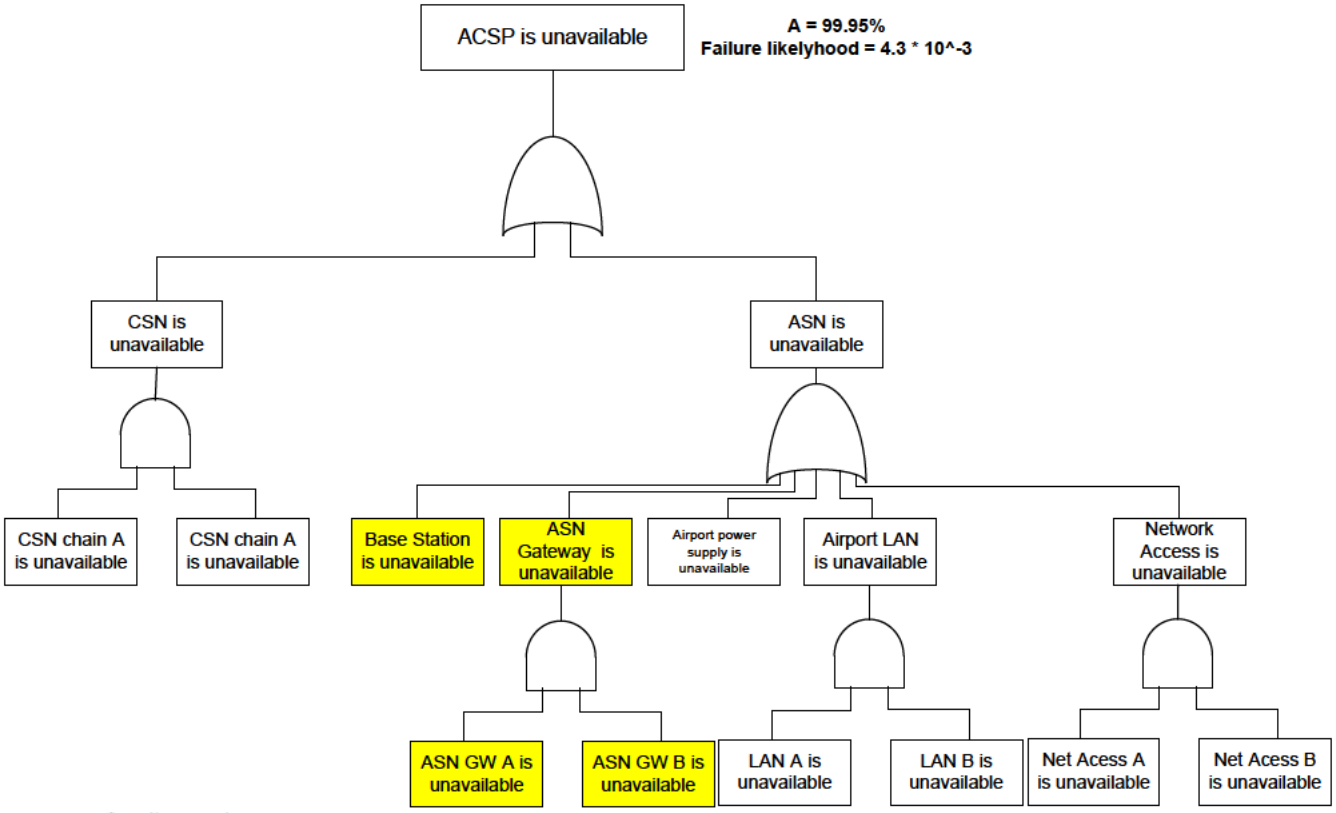


Figure 15 : ACSP availability fault tree - ASN Gateway is redundant & base station not redundant

Based on the analysis done in the SCENARIO 1 and state of the art, the following figure is proposed: MTBF ASN Gateway = 60 000 hours.

			MTBF	1/MTBF	MTTR	Availibility
ACSP		**Objectives**		**4,300E-04**		**0,999500**
	CSN					
		CSN chain A	*15000*		*19*	*0,99873*
		CSN chain B	*15000*		*19*	*0,99873*
		CSN chain A + B				*1,00000*
	ASN					
		Redundant Power supply				***1,00000***
		Network access A	*18981*		*19*	*0,99900*
		Network access B	*18981*		*19*	*0,99900*
		Network access A + B				***1,00000***
		LAN A	*60000*		*19*	*0,99968*
		LAN B	*60000*		*19*	*0,99968*
		LAN A + B				***1,00000***
		AeroMACS	***24000***	***4,167E-05***	*19*	***0,99953***
		ASN Gateway A	*60000*	*1,66667E-05*	*19*	*0,99968*
		ASN Gateway B	*60000*	*1,66667E-05*	*19*	*0,99968*
		ASN Gateway A + B				*1,00000*
		Base Station	*40000*	*0,000025*	*19*	*0,99953*
ACSP		**Derived**				**0,999522**

Table 26: Apportionment of reliability requirement on ASN Gateway and base Station with scenario 2 (ASN Gateway is redundant & base station not redundant)

Implementing redundancy at ASN Gateway:

- Improves significantly continuity of service offered per Base Station,
- Gives the opportunity to relax the MTBF requirement on Base Station with reasonable MTBF at ASN gateway level.

Consequently, it can be strongly recommended to make redundant this function notably for airports covered with several BS and/or with human intervention capability implying very high time to restore the service (e.g. no intervention during Week-End).

Redundancy (or load balancing strategy) at ASN gateway level can be implemented in different ways, for instance:

- Cold back-up: only one ASN gateway is UP at a given time. While experiencing a failure on the operational ASN Gateway, the other ASN gateway shall take over automatically the service:
  - connection between the Back-Up ASN GW and the Base Stations shall be re-established,
  - connection between the Back-Up ASN GW and the Base Stations shall be re-established,

  - the whole process to get access to the network (AAA, IP assignment…) shall be re-done.

- Static load balancing:
  - Several ASN Gateways are operational at the airport,
  - Base Stations are connected to only one ASN gateway,
  - If an ASN Gateway is Down, the service is loss for a part of the airport surface or/and overall bandwidth offered is reduced.
- Dynamic load balancing:
  - All instances of the ASN Gateways are Up at the same time,
  - All the Base Stations are connected to all the ASN Gateways,
  - The CSN function is connected to all the ASN Gateways,
  - Mobile connections are spread over the different ASN Gateways by the Base Stations.
  - While experiencing single failure, the whole process to get access to the network (AAA, IP assignment…) shall be re-done for the concerned mobiles,
- Hot back-up mechanism:
  - The context of connection is maintained in each instance of the ASN Gateway function,
  - Single failure at ASN Gateway level is fully transparent for the Mobiles.

5.2.2.3 SCENARIO 3: the ASN Gateway and the Base Stations are redundant at the airport

Both functions, ASN gateway and Base Station, are not impacted by single failure.

Such approach should improve the availability of the service at the airport.

Redundancy at Base Station level can be implemented in different ways, for instance:

- Cold back-up: only one Base Station is UP at a given time. While experiencing a failure on the operational ASN Gateway, the other ASN gateway shall take over automatically the service:
  - connection between the Back-Up Base Station and the ASN Gateway shall be re-established,
  - the whole process to get access to the network (AAA, IP assignment…) shall be re-done.
- Load balancing:
  - All the Base Stations are Up at the same time,
  - Base Stations operate on different channels,
  - All the Base Stations are connected to all the ASN Gateways,
  - While experiencing single failure, the whole process to get access to the network (AAA, IP assignment…) shall be re-done for the concerned mobiles on a different channel,
- Hot Back-Up mechanism:
  - The context of connection is maintained in each instance of the Base Station function,

- Only one transmit and receive at a given time,
- Single failure at Base Station level is fully transparent for the Mobiles, since the back-up station maintains the same context of connection and takes over the RF function.

5.2.2.4 Summary of availability requirements and recommendations

The table here below summarizes the applicable requirements or recommendations derived from the Safety and Performance requirements.

In the following table, only requirements coming from WG78/SC214 and applicable to the ACSP domain are considered as requirements (SHALL : G_Req_xx).

All other requirements are considered as recommendations (SHOULD : G_Rec_xx) since they are based on many assumptions on system design and/or maintenance organisation. Nevertheless, these assumptions are deemed reasonable with regards to the state of the art consequently manufacturers and Communication Service provider shall pay attention to them while implementing AeroMACS at a given airport.

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
ACSP	-	ACSP - all components	PC_CP_03 , SR_CP_02	G_Req_01	shall	The availability of the ACSP service shall be more than 99.95%
	-	ACSP - all components	PC_CP_03 , SR_CP_02	G_Req_02	shall	The likelihood that the ACSP service is unavailable shall be less than 4.3E-03/SOH
	-	ACSP - all components	PC_CP_03 , SR_CP_03	G_Rec_01	should	Depending on the implementation (type of redundancy), the Ground System should implement strategy to ease recovery of service in case of single failure at the following levels: -AAA, -Mobile IP, -ASN Gateway, -Base Station.
ACSP	CSN Operator	Power supply	PC_CP_03 , SR_CP_02	G_Rec_02	should	The power supply should be redundant.
		AAA function	PC_CP_03 , SR_CP_02	G_Rec_03	should	The CSN function should implement redundancy at AAA level. A hot back-up or load balancing strategy should be prefered.
		Mobile IP	PC_CP_03 , SR_CP_02	G_Rec_04	should	The CSN function should implement redundancy at Mobile IP level. A hot back-up or load balancing strategy should be prefered.
		Routing and level 2 infrastructure	PC_CP_03 , SR_CP_02	G_Rec_05	should	The CSN function shall implement redundancy at IP network level and Local Area Network. A hot back-up should be prefered.
		CSN	PC_CP_03 , SR_CP_02	G_Rec_06	should	The CSN operator should target an availability for the service greater than 99,9998%
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_07	should	The CSN operator should target a Mean Time to Repair a system less than 19 hours.
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_08	should	The CSN components should have the capability to be remotely monitored and controlled
ACSP	ASN Operator	Power supply	PC_CP_03 , SR_CP_02	G_Rec_09	should	The ASN operator should ensure that power supply is redundant for all ASN components

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
		Network access	PC_CP_03 , SR_CP_02	G_Rec_10	should	The ASN operator should implement a redundant network access
		Airport Local Network	PC_CP_03 , SR_CP_02	G_Rec_11	should	The ASN operator should implement a redundant Airport Local Network
		ASN Gateway	PC_CP_03 , SR_CP_02	G_Rec_12	should	The ASN Gateway MTBF should be greater than 60 000 hours
		ASN Gateway	PC_CP_03 , SR_CP_02	G_Rec_13	should	The ASN Gateway should have a redundant access to the network
		Base Station	PC_CP_03 , SR_CP_02	G_Rec_14	should	The Base Station should have a redundant access to the network
		Base Station	PC_CP_03 , SR_CP_02	G_Rec_15	should	The Base Station MTBF should be greater than 50 000 hours
		ASN	PC_CP_03 , SR_CP_02	G_Rec_16	should	The ASN operator should target an availability for the service greater than 99,95 %
		ASN - all components	PC_CP_03 , SR_CP_02	G_Rec_17	should	The ASN operator should target a Mean Time to Repair a system shall be less than 19 hours.
		ASN - all components	PC_CP_03 , SR_CP_02	G_Rec_18	should	The ASN components should have the capability to be remotely monitored and controled
		ASN Gateway	PC_CP_03 , SR_CP_02	G_Rec_19	should	The ASN Gateway should be implemented with redundancy. The redundancy mechanism shall not require human intervention
		Base Station	PC_CP_03 , SR_CP_02	G_Rec_20	may	The Base Station may be implemented with redundancy.

Table 27: Availability requirements on ACSP & Availability recommendations on AeroMACS Ground components

NOTE: in case, CSN is made of one or several Visited CSN in addition to the Home CSN, the requirements in the table above are applicable to the whole CSN function made on the different V-CSN plus the Home CSN. Contractual arrangements shall be establshed to ensure compliance to the safety and performance requirements.

The table below presents requirements applicable to Airborne system and related to the availability of the service.

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
Airborne system	-	-	PC_CP_03 , SR_CP_02	A_Rec_01	should	The airborne system shall implement a procedure for service recovery while experiencing failure at ASN (Base Station and ASN Gateway) and CSN ground system level
	-	-	PC_CP_03 , SR_CP_02	A_Rec_01	should	The service recovery procedure should be based on random mechanism to avoid avalanche of network access request
	-	-	PC_CP_03 , SR_CP_02	A_Rec_02	should	Unintended continuous transmission by the airborne system should be avoided

Table 28 : Requirements applicable to Airborne system and related to the availability of the AeroMACS service.

5.2.2.5 Additional recommendations from WG78/SC214 about maximum duration and number of outages

In draft deliverables version I of WG78/Sc214, the following additional requirements are mentioned concerning:

- Unplanned service outage duration,
- Maximum number of service unplanned outages,
- Maximum accumulated service unplanned outage time,
- Unplanned service outage notification delay.

List of Availibility Performance Requirements								
Application	**RCP Type**	**Function**	**Part**	**Availability (in percent)**	**Unplanned service outage duration (min)**	**Maximum number of service unplanned outages**	**Maximum accumulated service unplanned outage time(min/yr)**	**Unplanned service outage notification delay (min)**
CPDLC	RCP 120	*Taxi Clearance; ATC Comm;*	ATSU	99,95%	6	40	240	5
			ACSP	99,95%	6	40	240	5
			AC	99,40%	-	-	-	-
	RCP400	*Departure Clearance*	ATSU	99,95%	6	40	240	5
			ACSP	99,95%	6	40	240	5
			AC	99,40%	-	-	-	-
ADS-C	RSP95	*4DTBO, ATC Comm periodic/even*	ATSU	99,95%	6	40	240	5
			ACSP	99,95%	6	40	240	5
			AC	99,40%	-	-	-	-
	RSP120	*4DTBO; ATC Comm single/1st*	ATSU	99,95%	6	40	240	5
			ACSP	99,95%	6	40	240	5
			AC	99,40%	-	-	-	-
D-FIS	RIP180	*ATIS, NOTAM, VOLMET, HZWX, RVR*	ATSU	99,90%	6	40	240	5
			ACSP	99,90%	10	48	520	5
			AC	99,90%	-	-	-	-

Table 29: WG78/SC214 recommendations regarding maximum duration and number of outages

The following diagram, copied from WG78/Sc214, shows the relationships between these 4 parameters.

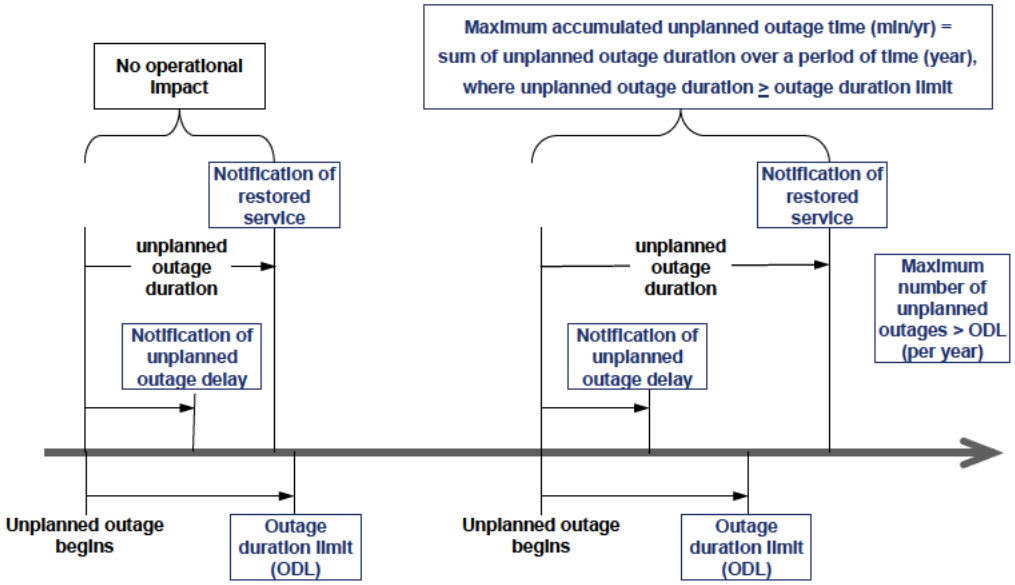


Figure 16 : Definition of availability concepts: Unplanned service outage duration, Maximum number of service unplanned outages, Maximum accumulated service unplanned outage time and Unplanned service outage notification delay

It should be noted that such additional requirements are quite dimensioning for the system compared to safety and performance requirements as presented before in the documents. Notably, the 6 minute maximum service outage requires:

- the implementation of redundancy at each single node of the ACSP domain and thus at ASN Gateway and Base Station level since human intervention to change a hardware component is impossible in less than 6 minutes,
- the implementation of the redundancy mechanism shall ensure service recovery (applicative data can be exchanged) while experiencing a single failure in less than 6 minutes.

NOTE: outage duration greater than 6 minutes will potentially impact regularity of flights but not safety (AeroMACS will only be used for surface non safety critical operation). Consequently, decision to implement redundancy at Base Station level should be analysed carefully.

NOTE: depending on the redundancy mechanism, service recovery does not only depend on the ground system. It may also depend on the Avionic service recovery strategy and traffic load since log-on procedure is based on a competitive access to the media.

NOTE: the 6 minute maximum service outage is based on the current Transport layer timer for the connection maintenance. Nowadays, in case no Transport message has been received for 6 minutes from the other commutating system, the Transport layer connection is down (event "Provider abort") and there is a need to re-establish the whole connection for the Avionics system. Such re-establishment can need a human action. It is thus desirable to limit as much as possible such disconnection.

The following requirements can be derived on the ACSP domain:

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
ACSP	-	ACSP - all components	PC CP 03 , SR_CP_02	G_Rec_43	should	The maximum unplanned service outage duration should be 6 minutes
	-	ACSP - all components	PC CP 03 , SR_CP_02	G_Rec_44	should	The maximum number of unplanned service outage should be less than 40
	-	ACSP - all components		G_Rec_45	should	The maximum accumulated service unplanned outage time should be 240 minutes / year
	-	ACSP - all components	PC CP 03 , SR_CP_03	G_Rec_46	should	The maximum unplanned service outage notification delay should be 5 minutes
ACSP	CSN Operator	CSN - all components	PC CP 03 , SR_CP_02	G_Rec_47	should	CSN service (AAA, MP…) should be single failure resilient.
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_48	should	While experiencing a single failure at CSN level, the interruption of service should not last more than 6 minutes, in case, the single failure is not transparent for mobiles (disconnection), these 6 minutes take into account time needed to re-establish the connection for all mobiles impacted
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_49	should	The ATC centre should be notified in less than 5 minutes by the CNS operator in case of interruption of service.
ACSP	ASN Operator	ASN - all components	PC CP 03 , SR_CP_02	G_Rec_50	should	ASN service (ASN GW, BS…) should be single failure resilient.
		ASN - all components	PC CP 03 , SR_CP_02	G_Rec_51	should	While experiencing a single failure at ASN level, the interruption of service should not last more than 6 minutes, in case, the single failure is not transparent for mobiles (disconnection), these 6 minutes take into account time needed to re-establish the connection for all mobiles impacted
		ASN - all components	PC CP 03 , SR_CP_02	G_Rec_52	should	The ATC centre should be notified in less than 5 minutes by the ANS operator in case of interruption of service.

Table 30 : ACSP recommendations regarding maximum duration and number of outages

NOTE: in case, CSN is made of one or several Visited CSN in addition to the Home CSN, the requirements in the table above are applicable to the whole CSN function made on the different V-CSN plus the Home CSN. Contractual arrangements shall be established to ensure compliance to the safety and performance requirements.

NOTE: for redundancy implementation, one can prefer to implement Hot Back-Up strategy to minimize the impact of single failure. In case cold back-up is implemented, the operator should ensure that the interruption of service (from users perspective) should be less than 6 minutes. These 6 minutes take into account the time to disconnect and reestablish the service for all mobiles impacted.

5.2.3 Allocation of transaction time requirements

The performance requirements regarding transaction time in ACSP are:

- **PR_CP_01: The one way transaction time in ACSP shall be less than 9 seconds for 99.9% of the messages**
- **PR_CP_02: The one way transaction time in ACSP shall be less than 4 seconds for 95% of the messages**

Non compliance with the transaction time figure can be due to:

- The ASN including :
    - Base Station: processing time + time to access to the media + “low” bit rate RF link
    - ASN Gate Way : processing time
    - Airport Local network : processing time
    - Network access : processing time + bit rate of leased line
- The CSN: processing time + bit rate of leased line

Transaction time is allocated on these different components using arithmetic allocations. Arithmetic allocations result in shorter individual allocation on each element than statistical allocations. However statistical allocation approach relies on the assumption that element delays are independent which cannot be easily verified in ACSP domain.

Based on the considerations presented in § 5.1.4, following rules have been applied for the apportionment of the safety requirement SR_CP_01:

- CSN : 20% of ACSP transaction time,
- AeroMACS : 80% of ACSP transaction time.

The following tables present the resulting requirements related to the transaction time requirements:

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
ACSP	-	ACSP - all components	PR_CP_01	G_Req_04	shall	The one way transaction time in ACSP shall be less than 9 seconds for 99.9% of the messages
	-	ACSP - all components	PR_CP_02	G_Req_05	shall	The one way transaction time in ACSP shall be less than 4 seconds for 95% of the messages
ACSP	CSN operator	CSN - all components	PR_CP_01, PR_CP_02	G_Rec_21	should	The various CSN components should be sufficiently sized to minimize the time to process data
		CSN - all components	PR CP 01, PR_CP_03	G_Rec_22	should	The CSN components should process data in less than 100 ms under all traffic conditions
		CSN - all components	PR CP 01, PR_CP_02	G_Rec_23	should	The CSN should be sufficiently sized to avoid congestion of the network.
		CSN - all components	PR_CP_01, PR_CP_03	G_Rec_24	should	The CSN operator should monitor the transit delay offered by its network and adapt its capacity to the demand
		CSN - all components	PR CP 01, PR_CP_04	G_Rec_25	should	The CSN components should have the capability to log exchanged traffic in order to derive statistics about network performance
		CSN - all components	PR_CP_01, PR_CP_02	G_Rec_26	should	The transaction time in the CSN should be less than 2 seconds for 99,9% of applicative messages
		CSN - all components	PR CP 01, PR_CP_02	G_Rec_27	should	The transaction time in the CSN should be less than 0,8 seconds for 95% of applicative messages
ACSP	ASN operator	ASN - all components	PR_CP_01, PR_CP_02	G_Rec_28	should	The various ASN components should be sufficiently sized to minimize the time to process data
		ASN - all components	PR CP 01, PR_CP_03	G_Rec_29	should	The ASN components should process data in less than 50 ms under all traffic conditions
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_30	should	The ASN should be sufficiently sized to avoid congestion of the network.
		ASN - all components	PR CP 01, PR_CP_03	G_Rec_31	should	The ASN operator should monitor the transit delay offered by its network and adapt its capacity to the demand

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
		ASN - all components	PR_CP_01, PR_CP_04	G_Rec_32	should	The ASN components should have the capability to log exchanged traffic in order to derive statistics about network performance
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_33	should	The transaction time in the ASN should be less than 7 seconds for 99,9% of applicative messages
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_34	should	The transaction time in the ASN should be less than 3,2 seconds for 95% of applicative messages
		Base Station	PR_CP_01, PR_CP_02	G_Rec_35	should	The scheduler should be optimized to minimize the number of AeroMACS channels to cope with a given demand
		Base Station	PR_CP_01, PR_CP_02	G_Rec_36	should	Coverage and capacity analysis to meet transaction time should be done per airport prior deploying Base Stations
		Base Station	PR_CP_01, PR_CP_02	G_Rec_37	should	Base Station deployment should ensure seamless operation from user point of view while experiencing hand-over
		Base Station	PR_CP_01, PR_CP_03	G_Rec_38	should	The transaction time in the ASN should be less than 3,2 seconds for applicative messages while experiencing hand-over procedure

Table 31 : Transaction Time requirements on ACSP & Availability recommendations on AeroMACS Ground components

NOTE: in case, CSN is made of one or several Visited CSN in addition to the Home CSN, the requirements in the table above are applicable to the whole CSN function made on the different V-CSN plus the Home CSN. Contractual arrangements shall be established to ensure compliance to the safety and performance requirements.

5.2.4 Allocation of Software Assurance Level Requirements

The allocation of software assurance level is performed using the SWAL allocation process of ED-153. The following table presents the SWAL allocation matrix:

Likelihood of generating such an effect (Pe x Ph) \ Effect Severity Class	1	2	3	4
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

Table 32: ED-153 SWAL Allocation matrix

- Allocation of Software Assurance Level considering “availability of use” Operational Hazards : “OH_WG78_CPDLC_01: Loss of CPDLC capability [single aircraft]”, “OH_WG78_FIS_1d: D-OTIS service unavailable for one aircraft (detected)”, “OH_WG78_ADSC_01: Loss of ADS-C capability [single aircraft]”
  - The effects of these Operational Hazards have a severity 5
  - AeroMACS failures directly contribute to these hazards ➔ likelihood of generating such an effect is “possible”
  - No SWAL is allocated on AeroMACS considering these operational hazards
- Allocation of Software Assurance Level considering “availability of provision” Operational Hazards: “OH_WG78_CPDLC_02: Loss of CPDLC capability [multiple aircraft]”, “OH_WG78_FIS_2d: D-OTIS service unavailable for multiple aircraft (detected)”, “OH_WG78_ADSC_02: Loss of ADS-C capability [multiple aircraft]”
  - The effects of these Operational Hazards have a severity 4
  - AeroMACS failures indirectly contribute to these hazards ➔ likelihood of generating such an effect is “possible”
  - **SWAL 4** is allocated on AeroMACS considering these operational hazards
- Allocation of Software Assurance Level considering “corruption, loss, spurious” Operational Hazards: “OH_WG78_CPDLC_03: Reception of a corrupted CPDLC message [single aircraft]”, “OH_WG78_CPDLC_04: Unexpected interruption of a CPDLC transaction [single aircraft]”, OH_WG78_CPDLC_05: Reception of an unexpected CPDLC message [single aircraft]” and “OH_WG78_FIS_3u: Incorrect D-OTIS report received (undetected)”
  - The effects of these Operational Hazards have a severity 3

- AeroMACS failures directly contribute to these hazards, these operational hazards occurs if AeoMACS and external protection mechanisms fails ➔ likelihood of generating such an effect is “very unlikely”
- **SWAL 4** is allocated on AeroMACS considering these operational hazards

AeroMACS systems shall be allocated a SWAL 4 which is equivalent to a Development Assurance Level equaled to AL5 according to ED-109 document.

5.2.5 Allocation of monitoring and alert requirements

The performance requirement regarding detection and alert in case of ACSP failures are:

- **PR_CP_04: The ground system shall be capable of detecting ground system failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function**
- **PR_CP_05: When the communication service no longer meets the requirements for the intended function, the ground system shall provide indication to the controller.**

These requirements are more or less directly applicable to the CSN and ASN:

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
ACSP	-	-	PR_CP_04	G_Req_06	shall	The ground system shall be capable of detecting ground system failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function
	-	-	PR_CP_05	G_Req_07	shall	When the communication service no longer meets the requirements for the intended function, the ground system shall provide indication to the operator.
ACSP	CSN operator	CSN - all components	PR_CP_04	G_Rec_39	should	The CSN nodes should be capable of detecting CSN failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function
		CSN - all components	PR_CP_05	G_Rec_40	should	When the CSN communication service no longer meets the requirements for the intended function, the CSN components should provide indication to the operator.
ACSP	ASN operator	ASN - all components	PR_CP_04	G_Rec_41	should	The ASN nodes should be capable of detecting ASN failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function
		ASN - all components	PR_CP_05	G_Rec_42	should	When the ASN communication service no longer meets the requirements for the intended function, the ASN components should provide indication to the operator.

Table 33 : Allocation of monitoring and alert requirements

5.3 Summary of Safety and Performance Requirements & Recommendations applicable to the AeroMACS Ground system

In the following table, only requirements coming from WG78/SC214 and applicable to the ACSP domain are considered as requirements (SHALL : G_Req_xx).

All other requirements are considered as recommendations (SHOULD : G_Rec_xx) since they are based on many assumptions on system design and/or maintenance organisation. Nevertheless, these assumptions are deemed reasonable with regards to the state of the art consequently manufacturers and Communication Service provider shall pay attention to them while implementing AeroMACS at a given airport.

Domain	Sub-domain	Component	Related Safety and Performance requirements	Ref	shall / should	Requirements/Recommendations
ACSP	-	ACSP - all components	PC_CP_03 , SR_CP_02	G_Req_01	shall	The availability of the ACSP service shall be more than 99.95%
	-	ACSP - all components	PC_CP_03 , SR_CP_02	G_Req_02	shall	The likelihood that the ACSP service is unavailable shall be less than 4.3E-03/SOH
	-	AeroMACS components	SR_CP_02	G_Req_03	shall	The AeroMACS ground component system shall be developped with the software assurance level AL 5 in compliance with ED-109
	-	ACSP - all components	PR_CP_01	G_Req_04	shall	The one way transaction time in ACSP shall be less than 9 seconds for 99.9% of the messages
	-	ACSP - all components	PR_CP_02	G_Req_05	shall	The one way transaction time in ACSP shall be less than 4 seconds for 95% of the messages
	-	ACSP - all components	PR_CP_04	G_Req_06	shall	The ground system shall be capable of detecting ground system failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function
	-	ACSP - all components	PR_CP_05	G_Req_07	shall	When the communication service no longer meets the requirements for the intended function, the ground system shall provide indication to the operator.
	-	ACSP - all components	PC_CP_03 , SR_CP_03	G_Rec_01	should	Depending on the implementation (type of redundancy), the Ground System should implement strategy to ease recovery of service in case of single failure at the following levels: -AAA, -Mobile IP, -ASN Gateway, -Base Station.
		ACSP - all components	PC_CP_03 , SR_CP_02	G_Rec_43	should	The maximum unplanned service outage duration should be 6 minutes
	-	ACSP - all components	PC_CP_03 , SR_CP_02	G_Rec_44	should	The maximum number of unplanned service outage should be 40
	-	ACSP - all components		G_Rec_45	should	The maximum accumulated service unplanned outage time should be 240 minutes / year

	-	ACSP - all components	PC_CP_03, SR_CP_03	G_Rec_46	should	The maximum unplanned service outage notification delay should be 5 minutes
	-	AeroMACS components	SR_CP_02	G_Req_03	shall	The AeroMACS ground component system shall be developped with the software assurance level AL 5 in compliance with ED-109
ACSP	CSN Operator	Power supply	PC_CP_03, SR_CP_02	G_Rec_02	should	The power supply should be redundant.
		AAA function	PC_CP_03, SR_CP_02	G_Rec_03	should	The CSN function should implement redundancy at AAA level. A hot back-up or load balancing strategy should be prefered.
		Mobile IP	PC_CP_03, SR_CP_02	G_Rec_04	should	The CSN function should implement redundancy at Mobile IP level. A hot back-up or load balancing strategy should be prefered.
		Routing and level 2 infrastructure	PC_CP_03, SR_CP_02	G_Rec_05	should	The CSN function shall implement redundancy at IP network level and Local Area Network. A hot back-up should be prefered.
		CSN	PC_CP_03, SR_CP_02	G_Rec_06	should	The CSN operator should target an availability for the service greater than 99,9998%
		CSN - all components	PC_CP_03, SR_CP_02	G_Rec_07	should	The CSN operator should target a Mean Time to Repair a system less than 19 hours.
		CSN - all components	PC_CP_03, SR_CP_02	G_Rec_08	should	The CSN components should have the capability to be remotely monitored and controled
		CSN - all components	PR_CP_01, PR_CP_02	G_Rec_21	should	The various CSN components should be sufficiently sized to minimize the time to process data
		CSN - all components	PR_CP_01, PR_CP_03	G_Rec_22	should	The CSN components should process data in less than 100 ms under all traffic conditions
		CSN - all components	PR_CP_01, PR_CP_02	G_Rec_23	should	The CSN should be sufficiently sized to avoid congestion of the network.
		CSN - all components	PR_CP_01, PR_CP_03	G_Rec_24	should	The CSN operator should monitor the transit delay offered by its network and adapt its capacity to the demand
		CSN - all components	PR_CP_01, PR_CP_04	G_Rec_25	should	The CSN components should have the capability to log exchanged traffic in order to derive statistics about network performance
		CSN - all components	PR_CP_01, PR_CP_02	G_Rec_26	should	The transaction time in the CSN should be less than 2 seconds for 99,9% of applicative messages

		CSN - all components	PR_CP_01, PR_CP_02	G_Rec_27	should	The transaction time in the CSN should be less than 0,8 seconds for 95% of applicative messages
		CSN - all components	PR_CP_04	G_Rec_39	should	The CSN nodes should be capable of detecting CSN failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function
		CSN - all components	PR_CP_05	G_Rec_40	should	When the CSN communication service no longer meets the requirements for the intended function, the CSN components should provide indication to the operator.
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_47	should	CSN service (AAA, MP…) should be single failure resilient.
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_48	should	While experiencing a single failure at CSN level, the interruption of service should not last more than 6 minutes, in case, the single failure is not transparent for mobiles (disconnection), these 6 minutes take into account time needed to re-establish the connection for all mobiles impacted
		CSN - all components	PC_CP_03 , SR_CP_02	G_Rec_49	should	The ATC centre should be notified in less than 5 minutes by the CNS operator in case of interruption of service.
ACSP	ASN Operator	Power supply	PC_CP_03 , SR_CP_02	G_Rec_09	should	The ASN operator should ensure that power supply is redundant for all ASN components
		Network access	PC_CP_03 , SR_CP_02	G_Rec_10	should	The ASN operator should implement a redundant network access
		Airport Local Network	PC_CP_03 , SR_CP_02	G_Rec_11	should	The ASN operator should implement a redundant Airport Local Network
		ASN Gateway	PC_CP_03 , SR_CP_02	G_Rec_12	should	The ASN Gateway MTBF should be greater than 60 000 hours
		ASN Gateway	PC_CP_03 , SR_CP_02	G_Rec_13	should	The ASN Gateway should have a redundant access to the network
		Base Station	PC_CP_03 , SR_CP_02	G_Rec_14	should	The Base Station should have a redundant access to the network
		Base Station	PC_CP_03 , SR_CP_02	G_Rec_15	should	The Base Station MTBF should be greater than 50 000 hours

		ASN	PC_CP_03, SR_CP_02	G_Rec_16	should	The ASN operator should target an availability for the service greater than 99,95%
		ASN - all components	PC_CP_03, SR_CP_02	G_Rec_17	should	The ASN operator should target a Mean Time to Repair a system shall be less than 19 hours.
		ASN - all components	PC_CP_03, SR_CP_02	G_Rec_18	should	The ASN components should have the capability to be remotely monitored and controled
		ASN Gateway	PC_CP_03, SR_CP_02	G_Rec_19	should	The ASN Gateway should be implemented with redundancy. The redundancy mechanism shall not require human intervention
		Base Station	PC_CP_03, SR_CP_02	G_Rec_20	should	The Base Station should be implemented with redundancy.
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_28	should	The various ASN components should be sufficiently sized to minimize the time to process data
		ASN - all components	PR_CP_01, PR_CP_03	G_Rec_29	should	The ASN components should process data in less than 50 ms under all traffic conditions
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_30	should	The ASN should be sufficiently sized to avoid congestion of the network.
		ASN - all components	PR_CP_01, PR_CP_03	G_Rec_31	should	The ASN operator should monitor the transit delay offered by its network and adapt its capacity to the demand
		ASN - all components	PR_CP_01, PR_CP_04	G_Rec_32	should	The ASN components should have the capability to log exchanged traffic in order to derive statistics about network performance
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_33	should	The transaction time in the ASN should be less than 7 seconds for 99,9% of applicative messages
		ASN - all components	PR_CP_01, PR_CP_02	G_Rec_34	should	The transaction time in the ASN should be less than 3,2 seconds for 95% of applicative messages
		Base Station	PR_CP_01, PR_CP_02	G_Rec_35	should	The scheduler should be optimized to minimize the number of AeroMACS channels to cope with a given demand
		Base Station	PR_CP_01, PR_CP_02	G_Rec_36	should	Coverage and capacity analysis to meet transaction time should be done per airport prior deploying Base Stations
		Base Station	PR_CP_01, PR_CP_02	G_Rec_37	should	Base Station deployment should ensure seamless operation from user point of view while experiencing hand-over

		Base Station	PR_CP_01, PR_CP_03	G_Rec_38	should	The transaction time in the ASN should be less than 3,2 seconds for applicative messages while experiencing hand-over procedure
		ASN - all components	PR_CP_04	G_Rec_41	should	The ASN nodes should be capable of detecting ASN failures and configuration changes that would cause the communication service to no longer meet the requirements for the intended function
		ASN - all components	PR_CP_05	G_Rec_42	should	When the ASN communication service no longer meets the requirements for the intended function, the ASN components should provide indication to the operator.
		ASN - all components	PC_CP_03 , SR_CP_02	G_Rec_50	should	ASN service (AAA, MP…) should be single failure resilient.
		ASN - all components	PC_CP_03 , SR_CP_02	G_Rec_51	should	While experiencing a single failure at ASN level, the interruption of service should not last more than 6 minutes, in case, the single failure is not transparent for mobiles (disconnection), these 6 minutes take into account time needed to re-establish the connection for all mobiles impacted
		ASN - all components	PC_CP_03 , SR_CP_02	G_Rec_52	should	The ATC centre should be notified in less than 5 minutes by the ANS operator in case of interruption of service.

Table 34: List of safety and performance requirements & recommendations applicable to the AeroMACS ground system

6 Definition of safety and performance requirements applicable to the AeroMACS airborne system

6.1 Functional description of the aircraft system

The aircraft system as referred to in this document includes all sub-systems associated with data communications on an aircraft.

For the purpose of this analysis, it will be considered that the aircraft system is made up of:

- End System, including HMI,
- Data Communication.

The End System part of the aircraft system considered for the purpose of this section includes:

- ATS applications (e.g. CPDLC) that support ATS functions (e.g. Departure Clearance) using datalink services,
- Air-Ground ATN router that supports Upper Layer Communications Service (ULCS) and ATN/IPS protocols (“AeroIP”).

This set of components is called “ATS End System” thereafter.

The Data Communication part of the aircraft system considered for the purpose of this section includes:

- RF antenna mounted on top of the aircraft fuselage,
- Mobile System (MS) that provides access to Air-Ground AeroMACS Subnetwork.

This set of components is called “AeroMACS” thereafter.

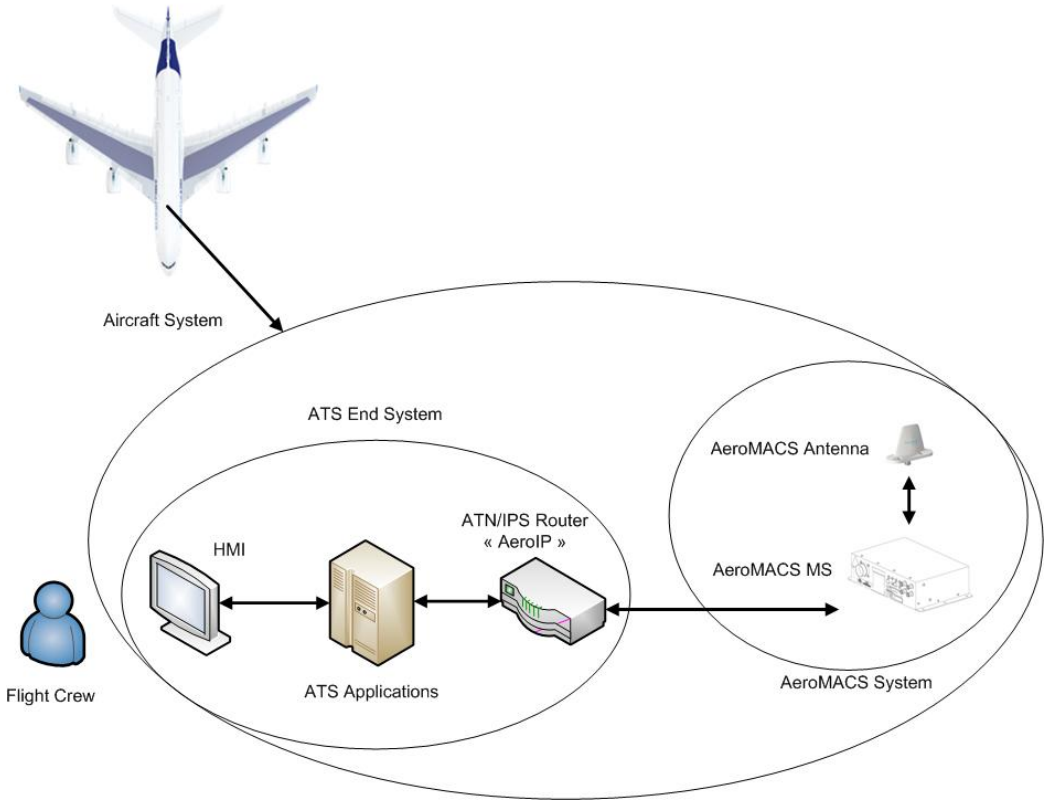


Figure 17: Aircraft System Components

6.2 Allocation of Safety and Performance Requirements to the aircraft system components

6.2.1 Introduction and assumptions

This section identifies the components which could be involved in the degradation of the performance and safety level with regards to the requirements identified previously.

Then, the safety and performance requirements are apportioned to the different parts of the aircraft system, including AeroMACS. Furthermore, recommendations are derived on the AeroMACS components in order to reach these requirements.

For the purpose of the analysis the following assumption related to aircraft system architecture is defined:

ASSUMP-AIRCRAFT-1 The end-to-end integrity checks are performed by the ATS applications within the ATS End System.

NOTE: The term "integrity" deals with the hazards assessed in the OSA (Operational Safety Analysis), leading to amongst other things:

a) Undetected corruption;

b) Undetected misdirection;

c) Undetected spurious;

d) Undetected delivery of a delayed message after expiration time;

e) Undetected loss of communication and user attempts to initiate a transaction.

The analysis will also make use of the following assumption, defined in SPR WG-78/SC-214:

ASSUMP-CPDLC-5 Datalink implementations within aircraft systems are expected to be at least ED12B/DO178B based Design Assurance Level C (DAL C)..

6.2.2 Quantitative safety requirements

6.2.2.1 Introduction

The quantitative safety requirements applicable to the aircraft system are reminded hereafter:

Requirement list				
Ref	**Parameter**	**Value**	**Title**	**Classification (as per AMC 25.1309)**
SR_AC_01	Corruption of message (per flight hour)	1,00E-05	The likelihood that the aircraft system corrupts a message (downlink or uplink) shall be less than 1.0E-05/FH	Major (MAJ)
SR_AC_02	Spurious message (per flight hour)	1,00E-05	The likelihood that the aircraft system generates a spurious report shall be less than 1.0E-05/FH	Minor (MIN)
SR_AC_03	Availability (per flight hour)	2,50E-03	The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH	Minor (MIN)
SR_AC_04	Detection of corrupted messages (per flight hour)	1,00E-05	The likelihood that the aircraft system fails to detect the corrupted message shall be less than 1.0E-05/FH	Major (MAJ)
SR_AC_05	Detection of delayed downlink messages (per flight hour)	1,00E-05	The likelihood that the aircraft system incorrectly time stamps a message shall be less than 1.0E-05/FH	Major (MAJ)
SR_AC_06	Detection of misdirected uplink messages (per flight hour)	1,00E-05	The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH	Major (MAJ)
SR_AC_07	Detection of spurious uplink messages (per flight hour)	1,00E-05	The likelihood to accept a message out of context of the current transaction shall be less than 1.E-5/FH.	Major (MAJ)

6.2.2.2 Loss of datalink capability

The safety requirement regarding availability of aircraft system is:

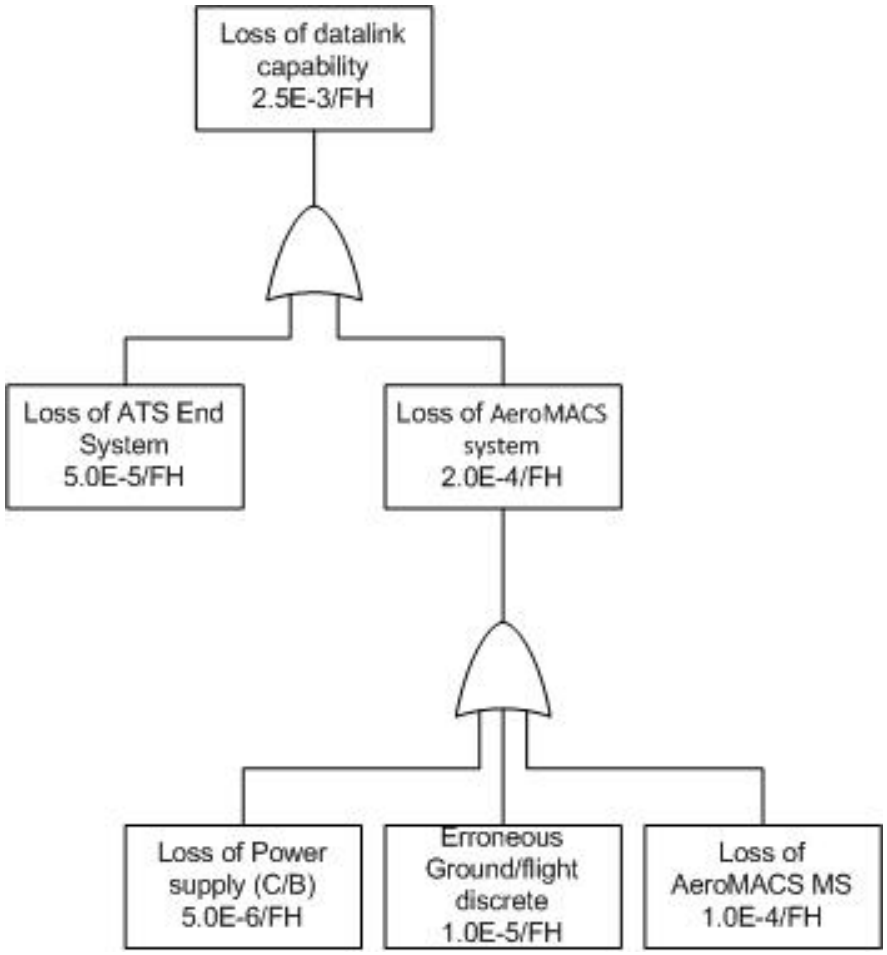
- SR_AC_03: The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH

The potential causes for this failure condition to occur are:

a) The ATS End System is unable to provide ATS functions, or

b) Dependant systems of AeroMACS make it inoperative, or
c) The AeroMACS MS itself is unable to provide datalink services

The figure below provides the fault tree for this failure condition and allocation to the system components:



NOTE: loss of AeroMACS system due to permanent reset (erroneous reset discrete input, if any) has not been taken into account (the estimated contribution of this event is 1.0E-6/FH).

The following Safety Requirement has been identified to be applicable to the AeroMACS airborne system:

- **A_Req_2**: The likehood that the AeroMACS system is unavailable shall be less that 1.0E-4/FH.

6.2.2.3 Erroneous datalink message

The safety requirements regarding corruption of message by aircraft system are:

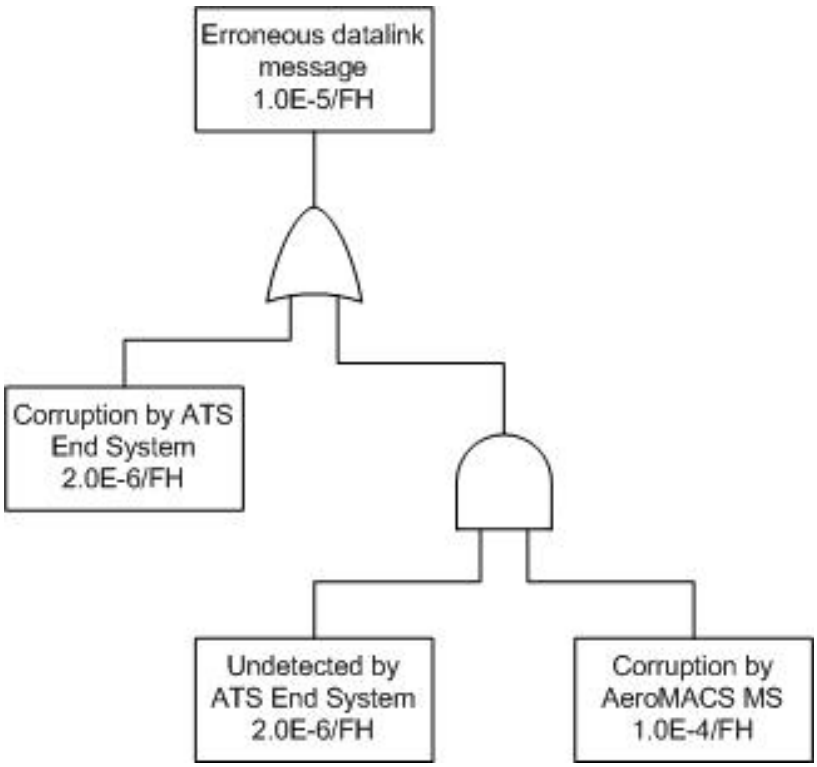
- SR_AC_01: The likelihood that the aircraft system corrupts a message (downlink or uplink) shall be less than 1.0E-05/FH

- SR_AC_04: The likelihood that the aircraft system fails to detect the corrupted message shall be less than 1.0E-05/FH

The potential causes for this failure condition to occur are:

a) The ATS End System corrupts the message, after having checked the end to end integrity, when processing it, or
b) The ATS End System is unable to detect a corrupted message

The figure below provides the fault tree for this failure condition and allocation to the system components:



The following Safety Requirement has been identified to be applicable to the AeroMACS airborne system:

- **A_Req_3**: The likehood that the AeroMACS system corrupts a message (downlink or uplink) shall be less that 1.0E-4/FH.

6.2.2.4 Unexpected datalink message

This failure condition covers most part of integrity requirements, with the exception of message corruption covered above, related to those potential causes:

- A system spontaneously generates a message (spurious), or
- The message is delayed, lost or misdirected on its way to its destination (potentially due to incorrect association or initialisation)

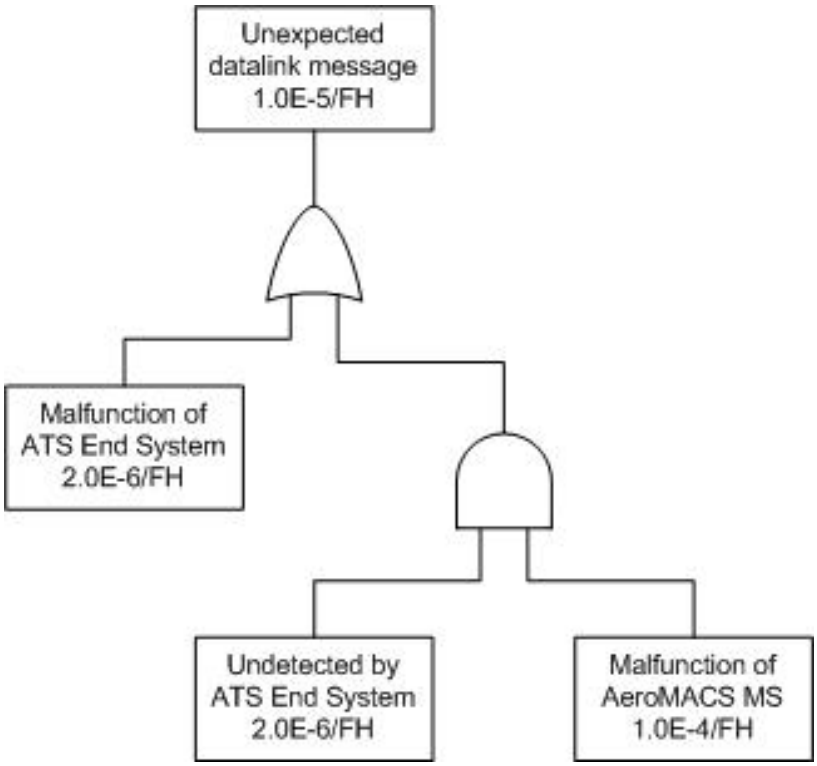
The safety requirements regarding spurious, delayed or misdirected message by aircraft system are:

- SR_AC_02: The likelihood that the aircraft system generates a spurious report shall be less than 1.0E-05/FH
- SR_AC_05: The likelihood that the aircraft system incorrectly time stamps a message shall be less than 1.0E-05/FH
- SR_AC_06: The likelihood that the aircraft system fails to detect and reject the misdirected uplink message shall be less than 1.0E-05/FH
- SR_AC_07: Upon receipt of an UM, containing an MRN, the likelihood of the aircraft system, not rejecting that does not match a DM MIN shall be less than 1.E-5/FH

The potential causes for this failure condition to occur are:

a) The ATS End System misbehaves, after having checked the end to end integrity, when processing it, or
b) The ATS End System is unable to detect an unexpected message

The figure below provides the fault tree for this failure condition and allocation to the system components:



The following Safety Requirement has been identified to be applicable to the AeroMACS airborne system:

- **A_Req_4**: The likehood that the AeroMACS system spontaneously generates, delays, losses or misdirects a message (downlink or uplink) shall be less that 1.0E-4/FH.

6.2.2.5 Development Assurance Level (DAL)

In the fault tree related to "Loss of datalink capability", taking into account:

- the failure condition is classified Minor, as per AMC 25.1309,
- and a single failure of any component can lead to the abnormal event,

the Development Assurance Level (DAL) of ATS End System and DAL of AeroMACS shall be at least "D", as per DO-178C.

In the fault trees related to "Erroneous datalink message" and "Unexpected datalink message", taking into account:

- the erroneous, spurious, delay, loss or misdirection of datalink message is classified MAJOR, as per AMC 25.1309,
- the assumptions **ASSUMP-CPDLC-5** and **ASSUMP-AIRCRAFT-1**.

the Development Assurance Level (DAL) of ATS End System should be "C" and DAL of AeroMACS should be "D", as per DO-178C.

The following Safety Requirement has been identified to be applicable to the AeroMACS airborne system:

- **A_Req_1**: The Development Assurance Level (DAL) of AeroMACS shall be at least be "D", as per DO-178C.

NOTE: Airborne Development Assurance Level (DAL) "D" is equivalent to Assurance Level (AL) 5 as per DO-278/ED-109 "Software Standard for Non-Airborne Systems".

6.2.3 Qualitative safety requirements

The qualitative safety requirements applicable to the aircraft system are reminded hereafter:

The lines in **bold** indicate the requirements allocated to AeroMACS system, provided that all requirements are applicable to the ATS End System part of the aircraft system.

Requirement list			
Ref	**Parameter**	**Title**	**Classification (as per AMC 25.1309)**
SR_AC_08	**Loss of message**	**The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted**	**Major (MAJ)**
SR_AC_09	Corruption of message	The flight and aircraft identifiers (either the Registration Marking or the 24-bit Aircraft Address) sent by the aircraft system, used for data link initiation correlation and ADS-C network address mapping, shall be unique and unambiguous	Major (MAJ)
SR_AC_10	**Corruption of message**	**The aircraft system shall prohibit operational processing by flight crew of corrupted messages.**	**Major (MAJ)**
SR_AC_11	Corruption of message	The aircraft system shall execute the route clearance per the route clearance received from the ATS via data link	Major (MAJ)

Requirement list			
Ref	**Parameter**	**Title**	**Classification (as per AMC 25.1309)**
SR_AC_12	Corruption of message	The aircraft system shall ensure the correct transfer into or out of the aircraft's FMS of route data received/sent via data link,in support of the conditions in section 2.4.1.1.	Major (MAJ)
SR_AC_13	Misdirection of message	The aircraft system shall transmit messages to the designated recipient.	Major (MAJ)
SR_AC_14	Misdirection of message	The aircraft system shall provide unambiguous and unique identification of the origin and destination of each message it transmits	Major (MAJ)
SR_AC_15	**Misdirection of message**	**The aircraft system shall only accept uplink messages intended for it.**	**Major (MAJ)**
SR_AC_16	Misdirection of message	The flight crew shall perform the initiation data link procedure again with any change of the aircraft identifiers (e.g. the Flight Identification and either the Registration Marking or the Aircraft Address)	Major (MAJ)
SR_AC_17	**Delay of message**	**The aircraft system shall indicate to the flight crew when a message cannot be successfully transmitted**	**Major (MAJ)**
SR_AC_18	Availability	The aircraft system shall provide to the ATSU an indication when it rejects an ADS-C service request initiated by the ATSU at the application layer.	Minor (MIN)
SR_AC_19	**Availability**	**The aircraft system shall indicate to the flight crew a detected loss of ADS-C service.**	**Minor (MIN)**
SR_AC_20	Availability	The aircraft system shall provide to the ATSU an indication when it rejects a CPDLC service request initiated by the ATSU at the application layer.	Minor (MIN)
SR_AC_21	Availability	The aircraft system shall display the indication provided by the ATSU when a DSC service request initiated by the flight crew is rejected at the application layer.	Minor (MIN)
SR_AC_22	**Availability**	**The aircraft system shall indicate to the flight crew a detected loss of data link service.**	**Minor (MIN)**
SR_AC_23	Detection of corrupted messages	Whenever a message is discarded by the aircraft system, it shall send an indication to the ground system for display to the controller.	Major (MAJ)
SR_AC_24	Detection of delayed downlink messages	The aircraft system shall time stamp each report to within one second UTC when it is released for onward transmission.	Minor (MIN)
SR_AC_25	Detection of delayed downlink messages	The aircraft system shall time stamp to within one second UTC each message when it is released for onward transmission.	Minor (MIN)

Requirement list			
Ref	**Parameter**	**Title**	**Classification (as per AMC 25.1309)**
SR_AC_26	Detection of delayed uplink messages	When a received message contains a time stamp that indicates the Latency Time Check value, set at equal or less than ETTRN, has been exceeded, the aircraft system shall a) discard the message and send an indication to the Ground System for display to the controller or b) provide the message to the flight crew with an appropriate indication.	Major (MAJ)
SR_AC_27	Detection of misdirected uplink messages	The aircraft system shall be able to determine the message initiator.	Major (MAJ)
SR_AC_28	Detection of misdirected uplink messages	Once an aircraft accepts operational CPDLC messages from an ATSU, it shall reject operational CPDLC messages from any other ATSU until the first ATSU terminates CPDLC with that aircraft.	Major (MAJ)
SR_AC_29	Detection of misdirected uplink messages	Only the ATSU that has control of the aircraft shall be permitted to send a Next Data Authority (NDA) message to the aircraft.	Major (MAJ)
SR_AC_30	Detection of spurious uplink messages	The aircraft system shall indicate in each response to which messages it refers	Major (MAJ)
SR_AC_31	Detection of spurious uplink messages	Each downlink message shall be uniquely identified for a given aircraft-ATSU pair, following a sequential order	Major (MAJ)
SR_AC_32	Detection of spurious downlink messages	The aircraft system shall indicate in each report to which contract number it is referring	Major (MAJ)
SR_AC_33	Detection of inappropriate messages by the crew	The aircraft system shall provide to the flight crew an indication of the ATSU that has established CPDLC (CDA) service.	Major (MAJ)

To summarize, the AeroMACS system shall:

a) Indicate a detected loss of datalink services (SR_AC_08, SR_AC_19, SR_AC_22)

b) Only accept uplink messages intended for the aircraft (SR_AC_15)

c) Prohibit operational processing of corrupted messages (SR_AC_10)

d) Indicate when a message cannot be successfully transmitted (SR_AC_17)

The following Safety Requirements have been identified to be applicable to the AeroMACS airborne system:

- **A_Req_5**: The AeroMACS system shall indicate a detected loss of datalink services.

- **A_Req_6**: The AeroMACS system shall only accept uplink messages intended for the aircraft.
- **A_Req_7**: The AeroMACS system shall prohibit operational processing of corrupted messages.
- **A_Req_8**: The AeroMACS system shall indicate when a message cannot be successfully transmitted.

6.2.3.1 RF interferences with other CNS systems

One particular case of malfunction of AeroMACS MS is the inadvertent activation during flight (due for example to erroneous Ground/Flight condition), in this situation:

- The minimum required isolation from AeroMACS transmission (fundamental emission) is 43 dB (refer to document "Aircraft installation & Operational aspects of the AeroMACS"), i.e. a minimum distance of 0.7 meter@5120 MHz
- The minimum required isolation from AeroMACS transmission (spurious & broadband noise emissions) is 118 dB. However, considering a minimum reduction of 70 dB below 2 GHz for AeroMACS emissions, the minimum required isolation is 48 dB, i.e. a minimum distance of 1.2 meter@5120 MHz

Taking into account that the minimum distance with the AeroMACS antenna will be 1.5 meter (5 feet), the inadvertent activation during flight of AeroMACS has no effect on others CNS systems.

6.2.4 Quantitative performance requirements

The quantitative performance requirements applicable to the aircraft system are reminded hereafter:

Requirement list			
Ref	**Parameter**	**Value**	**Title**
PR_AC_01	Transaction Time 99,9 % (in seconds)	11,5	The transaction time (one way) in aircraft shall be less than 11.5 seconds for 99.9% of the ADS-C - RSP 95 messages
PR_AC_02	Transaction Time 95 % (in seconds)	5	The transaction time (one way) in aircraft shall be less than 5 seconds for 95% of the ADS-C - RSP 95 messages
PR_AC_03	Availability (in percent)	99,40%	The availability of the ADS-C aircraft system shall be more than 99.40%

6.2.4.1 Transaction Time (Continuity)

The performance requirements regarding transaction time of message by aircraft system are:

- PR_AC_01: The transaction time (one way) in aircraft shall be less than 11.5 seconds for 99.9% of the ADS-C - RSP 95 messages
- PR_AC_02: The transaction time (one way) in aircraft shall be less than 5 seconds for 95% of the ADS-C - RSP 95 messages

Transaction time is allocated on the different components using arithmetic distribution. The following table presents the results of this allocation:

Objective (one-way transmission) (downlink or uplink)	ATS End System	Interface between ATS End System and AeroMACS	AeroMACS system
TT(95%): 5 sec	4 sec	500 msec	500 msec
TT (99.9%): 11.5 sec	10 sec	500 msec	1 sec

The following Performance Requirements have been identified to be applicable to the AeroMACS airborne system:

- **A_Req_9**: The delay introduced by the AeroMACS system for a one-way transmission (downlink or uplink) shall be less than 500 msec.

6.2.4.2 Availability

The performance requirement regarding availability of aircraft system is:

- PR_AC_03: The availability of the ADS-C aircraft system shall be more than 99.40%

With an average use of aircraft system of 2.5 hours/flight, the quantitative performance requirement is computed as follows:

Probability of loss of aircraft system = (1 - $A_{AIRCRAFT}$)/(flight duration) = (1 – 0.994)/2.5 = 2.4E-3/FH

This probability of loss of aircraft system is commensurate with the likelihood defined in SR_AC_03 (“The likelihood that the AC system is unavailable shall be less than 2.5E-03/FH”).

Thus the fault tree and allocations of section “Loss of datalink capability” remain valid, and Safety requirement A_Req_2 is still applicable for Performance.

The following Performance Requirements have been identified to be applicable to the AeroMACS airborne system:

- **A_Req_2**: The likehood that the AeroMACS system is unavailable shall be less that 1.0E-4/FH.

6.2.5 Qualitative performance requirements

The qualitative performance requirements applicable to the aircraft system are reminded hereafter:

Requirement list

Ref	Parameter	Title
PR_AC_04	Availability	The aircraft system shall be capable of detecting aircraft system failures or loss of air/ground communication that would cause the aircraft communication capability to no longer meet the requirements for the intended function.
PR_AC_05	Availability	When the aircraft communication capability no longer meets the requirements for the intended function, the aircraft system shall provide indication to the flight crew.

To summarize, the AeroMACS system shall:

a) Indicate a detected loss of datalink services

b) Indicate when a message cannot be successfully transmitted

The following Performance Requirements have been identified to be applicable to the AeroMACS airborne system:

- **A_Req_5**: The AeroMACS system shall indicate a detected loss of datalink services.
- **A_Req_8**: The AeroMACS system shall indicate when a message cannot be successfully transmitted.

6.3 Summary of Safety and Performance Requirements applicable to the AeroMACS airborne system

The following Safety and Performance Requirements have been identified to be applicable to the AeroMACS airborne system:

- **A_Req_1**: The Development Assurance Level (DAL) of AeroMACS shall be at least be “D”, as per DO-178C.
- **A_Req_2**: The likelihood that the AeroMACS system is unavailable shall be less that 1.0E-4/FH.
- **A_Req_3**: The likelihood that the AeroMACS system corrupts a message (downlink or uplink) shall be less that 1.0E-4/FH.
- **A_Req_4**: The likelihood that the AeroMACS system spontaneously generates, delays, losses or misdirects a message (downlink or uplink) shall be less that 1.0E-4/FH.
- **A_Req_5**: The AeroMACS system shall indicate a detected loss of datalink services.
- **A_Req_6**: The AeroMACS system shall only accept uplink messages intended for the aircraft.
- **A_Req_7**: The AeroMACS system shall prohibit operational processing of corrupted messages.
- **A_Req_8**: The AeroMACS system shall indicate when a message cannot be successfully transmitted.
- **A_Req_9**: The delay introduced by the AeroMACS system for a one-way transmission (downlink or uplink) shall be less than 500 msec.

7 List of assumptions

List of Assumptions			
Ref	**Phase**	**Assumption**	**Jutification**
ASSUMP-AEROMACS_01	Services / Application	Context Management (CM) application is not considered during the identification of Operational Hazards.	Consistent with WG78/SC214 approach: a failure during Datalink initiation doesn't have direct operational effects. However it can have effects during the use of the others applications (CPDLC, ADS-C and FIS). So the safety requirements concerning CM messages are determined by studying all the other applications.
ASSUMP-AEROMACS_02	Services / Application	No specific safety analysis is carried out for 4D-TRAD service	4D-TRAD uses both CPDLC and ADS-C applications. It is considered that 4D-TRAD do not drive more stringent requirements on CPDLC and ADS-C applications than other CPDLC and ADS-C services. This assumption will be validated when 4D-TRAD OSA will be published.
ASSUMP-AEROMACS_03	Services / Application	Services D-RVR and D-HZWX are not taken into account when considering the FIS application in the safety analysis.	WG78 OSA concerning FIS application only considers D-OTIS service. Others OSA are currently in process concerning services D-RVR and D-HZWX.

List of Assumptions			
Ref	**Phase**	**Assumption**	**Jutification**
ASSUMP-AEROMACS_04	Definition of AE	Abnormal Events concerning all the messages at AeroMACS level associated to one aircraft are always detected. These events are grouped as single event: “permanent failure to communicate with one aircraft" (Availability of use).	A failure on a message at AeroMACS level (corruption, loss…), is detected thanks to the external mitigation means such as time stamps, checksum… at upper layers. A systematic failure of the external mitigations means for all AeroMACS messages is very unlikely (the period of failure allocated by WG78 is one failure every 100 000 hours). The detection of this failure induces a clarification between controllers and flight crew. Then, following messages will be carefully watched; controllers will detect that there is a permanent failure on Datalink communication chain with the aircraft.
ASSUMP-AEROMACS_05	Definition of AE	Abnormal Events concerning all messages at AeroMACS level associated to more than one aircraft are always detected. These events are grouped as single event:”permanent failure to communicate with more than one aircraft” (Availability of provision).	A failure on an AeroMACS message (corruption, loss…), is detected thanks to the external mitigation means such as time stamps, checksum… A systematic failure of the external mitigations means for all message is very improbable (the period of failure allocated by WG78 is one failure every 100 000 hours). The detection of this failure induces a clarification between controllers and flight crew. Then, following messages will be carefully watched; controllers will detect that there is a permanent failure on Datalink communication chain.

List of Assumptions			
Ref	**Phase**	**Assumption**	**Jutification**
ASSUMP-AEROMACS_06	Evaluation of severity	Simultaneous loss of all applications (CPDLC, D-OTIS and ADS-C) for one aircraft is not more critical than independent failure of each application for one aircraft.	This assumption must be validated by working group 78. However, this assumption seems coherent because Datalink application has never been considered as a reduction mean to mitigate the loss of another application. For example, OH_WG78_CPDLC_01 (failure to exchange CPDLC messages with a single aircraft) is not mitigated by the utilization of ADS-C or FIS.
ASSUMP-AEROMACS_07	Evaluation of severity	Simultaneous loss of all applications (CPDLC, D-OTIS and ADS-C) for one aircraft is not more critical that independent failure of each application for one aircraft.	This assumption must be validated by working group 78. However, this assumption seems coherent because Datalink application has never been considered as a reduction mean to mitigate the loss of another application.
ASSUMP-AEROMACS_08	Allocation of SR	The probability that all the ground systems are unavailable is assumed to be less than 7*10-6 per flight hour.	WG78 CPDLC OSA has defined a safety requirement of 7*10-6 for the unavailability of the CPDLC ground system. A failure of all the ground system should be lower than this requirement (multiple failure should occur to induce a failure of all ground systems).
ASSUMP-AIRCRAFT-1	AeroMACS airborne system Allocation	The end-to-end integrity checks are performed by the ATS applications within the ATS End System.	Consistent with current architectures

Table 35: List of Assumptions

8 References

[1] **Data Communications Safety and Performance Requirements -** Annex A Operational Safety Analysis Approach – Issue I, 1st February 2012 – WG78/SC214

[2] **Data Communications Safety and Performance Requirements -** Annex B CPDLC Operational Safety Analysis – Issue I, 1st February 2012 – WG78/SC214

[3] **Data Communications Safety and Performance Requirements -** Annex C ADS-C Operational Safety Analysis – Issue I, 1st February 2012 – WG78/SC214

[4] **Data Communications Safety and Performance Requirements -** Annex D FIS Operational Safety Analysis – Issue H, 3rd February 2010 – WG78/SC214

[5] **Data Communications Safety and Performance Requirements -** Annex EFGH Operational Performance Analysis – Issue I, 1st February 2012 – WG78/SC214

[6] **WiMAX Forum Network Architecture – Stage 2 Architecture Tenets, Reference Model and Reference Points-** Ref T32-002 Release 1.0 Version 4 - February 03, 2009 T32-002 –

Appendix A : Hazard Classification Matrix (ED-78A)

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	Normally with hull loss. Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience.
Effect on Air crew	Fatalities or incapacitation.	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or slight reduction in air traffic control capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.

Appendix B : Identification of Operational Hazards table

The table associated to this systematic methodology is presented in the following file:

Identification of Operational Hazards

Appendix C : Differences between issue I and issue M of WG78/SC214 documents

The present safety and performance analysis is based on issue I of WG78/SC214 documents. At the moment this document is delivered, the current version of the WG78/SC214 document is issue M.

This appendix presents a brief analysis of the differences between the two issues and some first analysis of potential impact on AeroMACS design. It has to be noticed that WG78 deliverables have still to be reviewed in order to address merged European and US approach on ATN Baseline 2.

General remarks

Flight Information Services are no longer in the perimeter of the WG78 / SC214.

Remarks regarding the Safety Analysis

Severities of some Operational Hazards have been modified. Particularly, severities of hazards « Loss of ADS-C capability [multiple aircraft] - undetected » and « Loss of CPDLC capability [multiple aircraft] - undetected » have been reassessed from 4 to 3.

- For CPDLC hazard, “undetected loss of CPDLC capability for multiple aircraft”, the severity is 3 in release M (instead of 4 in release I) only for Separation Assurance function which is only used in En-Route Domain. AeroMACS being used only for airport operation, this modification should thus not impact on AeroMACS design.
- For ADS-C hazard, “undetected loss of ADS-C capability for multiple aircraft”, the severity is 3 in release M (instead of 4 in release I) only for 4D-TBO and for ATC Com function (for the effect *“Significant reduction in safety margins and separation”)*. ADS-C application supports the following services: 4-Dimensional Trajectory Data Link (4DTRAD), Information Exchange and Reporting (IER) and Position Reporting (PR). These services, apart from the establishment of the ADS-C contract, will likely not be used while the aircraft is on the ground. Consequently, this modification of effect severity should not impact AeroMACS design.

Safety Requirements are only derived on Aircraft System, ATS Provider and Operator: there is no longer safety requirements apportioned to the ACSP, it is considered as a part of ATS Provider.

Remarks regarding Performance Analysis

No significant modification for AeroMACS design.

-END OF DOCUMENT-