INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

PJ.14-W2-77 TRL6 Final TS/IRS - Part II - Safety Assessment Report

Deliverable ID:	**D5.1.120**
Dissemination Level:	**PU**
Project Acronym:	**PJ.14-W2 I-CNSS**
Grant:	**874478**
Call:	**[H2020-SESAR-2019-1]**
Topic:	**SESAR-IR-VLD-WAVE2-10-2022**
Consortium Coordinator:	**LEONARDO**
Edition Date:	**5 December 2022**
Edition:	**01.01.01**
Template Edition:	**00.00.04**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
EUROCONTROL	10 Oct. 2022
FREQUENTIS	15 Nov. 2022

Reviewers internal to the project

Beneficiary	Date
ENAIRE	22/11/202230
AIRBUS	22/11/202230
AIRTEL	22/11/202230
EUROCONTROL	22/11/202230
FREQUENTIS	22/11/202230
HONEYWELL	22/11/202230
INDRA	22/11/202230
INMARSAT	22/11/202230
LEONARDO	22/11/202230
THALES AIR SYSTEMS	22/11/202230

Reviewers external to the project

Beneficiary	Date

Approved for submission to the S3JU By - Representatives of all beneficiaries involved in the project

Beneficiary	Date
ENAIRE	24/11/20225
AIRBUS	24/11/20225
AIRTEL	24/11/20225
EUROCONTROL	24/11/20225
FREQUENTIS	24/11/20225
HONEYWELL	24/11/20225
INDRA	24/11/20225
INMARSAT	24/11/20225

EUROPEAN PARTNERSHIP

Co-funded by the European Union

LEONARDO	24/11/20225
THALES AIR SYSTEMS	24/11/20225

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	10 June 2022	DRAFT	EUROCONTROL	New document
00.00.01	27 Sept. 2022	DRAFT	FREQUENTIS	Internal review
00.01.00	10 Oct. 2022	FINAL	FREQUENTIS	Sent to Partners review and approval
01.00.00	15th Oct 2022	FINAL	FREQUENTIS	Submission to SJU
01.00.01	22nd Nov 2022	Candidate for update delivery	FREQUENTIS	Sent to Partners review and approval
01.01.00	24th Nov 2022	Final Delivery	FREQUENTIS	Submitted to SJU
01.01.01	5th Dec 2022	Final Delivery	FREQUENTIS	Implemented Mat Gate AI 09728 and submitted

PJ.14-W2 I-CNSS

PJ.14-W2 I-CNSS

This Safety Assessment Report is part of a project which has received funding from the SESAR Joint Undertaking under grant agreement No 874478 under European Union's Horizon 2020 research and innovation programme.

Abstract

In accordance with the relevant Safety Assessment Plan, this document aims at performing a Failure Mode and Effect Analysis (FMEA) and more generally a RAM (Reliability, Availability, Maintainability) analysis for the Future Communications Infrastructure (the FCI) in terms of safety design objectives.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Table of Contents

List of Tables

List of Figures

EUROPEAN PARTNERSHIP
Co-funded by the European Union

1 Executive Summary

The safety and security of a system is of primary concern for dependable systems in regulated industries such as aerospace, medical, nuclear, transportation, etc. As such hazards analyses due to inherent system failures and to external conditions is a requirement to show that a mission critical system meets its specified safety and security requirements. The failure conditions can be triggered by both unforeseen events such as procedural or installation and manipulation errors as well as malicious events provoked by directed malicious traffic.

In accordance with the relevant Safety Assessment Plan, ref. [1], this document aims at performing a Failure Mode and Effect Analysis (FMEA) and more generally a RAM (Reliability, Availability, Maintainability) analysis for the Future Communications Infrastructure (the FCI) in terms of safety design objectives.

The results of the FMEA/RAM analysis documented herein focus only on Availability, which is only one aspect of overall Safety and Performance it is to be noted that also an analysis on Continuity should be performed in future activities to complement this report.

In addition to the FMEA/RAM analysis, Solution 77 has also conducted performance measurements for all applicable Performance Requirements of EUROCAE ED-228A, ref. [4]. The results are documented in the TVALR, ref. [11].

In agreement with Project 19 of SESAR2020, ref. [6], this constitutes the Safety Assessment Report (SAR) representing Part II of the TS/IRS document and presents the assurance that the Safety Requirements for the TRL2-TRL6 phases are complete, correct and realistic, thereby providing all material to adequately complement the Solution TS/IRS Part I.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

In accordance with the relevant Safety Assessment Plan, ref. [1], this document aims at performing a Failure Mode and Effect Analysis (FMEA) and more generally a RAM (Reliability, Availability, Maintainability) analysis for the Future Communications Infrastructure (the FCI) in terms of safety design objectives.

In agreement with Project 19 of SESAR2020, ref. [6], this constitutes the Safety Assessment Report (SAR) representing Part II of the TS/IRS document and presents the assurance that the Safety Requirements for the TRL2-TRL6 phases are complete, correct and realistic, thereby providing all material to adequately complement the Solution TS/IRS Part I. In the EUROCONTROL Safety Assessment Methodology, ref. [8], this corresponds to the Preliminary System Safety Assessment (PSSA) Phase.

2.2 General Approach to Safety Assessment

The objective of this report is to document that FCI solution, as designed, implemented, and integrated will achieve a reasonably acceptable level of safety.

This report describes the result of the second step of the safety assessment process: Preliminary System Safety Assessment (PSSA), and in particular the bottom-up approach and does not include the top-down approach nor the SWAL analysis parts of the PSSA. The top-down approach, including Fault-Tree Analysis, is documented in ref. [2]. The objective of a PSSA is defined in EUROCONTROL's Air Navigation System Safety Assessment Methodology [8] as:

> *Preliminary System Safety Assessment (PSSA) is a mainly top-down iterative process, initiated at the beginning of a new design or modification to an existing design of an Air Navigation System. The objective of performing a PSSA is to demonstrate whether the assessed system architecture can reasonably be expected to achieve the Safety Objectives specified in the FHA.*
>
> *The PSSA process apportions Safety Objectives into Safety Requirements allocated to the system elements, i.e., specifies the risk level to be achieved by the system elements. PSSA also identifies an Assurance Level per system element.*
>
> *The system architecture can only achieve the Safety Objectives established during the FHA, provided the architecture elements meet their Safety Requirements."*

Thus, the objective of the PSSA activities is to define such safety requirements for FCI Solution, which will ensure that the Network Solution can fulfil the safety objectives determined during the FHA activity.

The FHA elements that have been used in the report are coming from Hazards as identified in the reference ED228A document, ref. [4].

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2.3 Scope of the Safety Assessment

The Safety Assessment Plan, ref. [1], describes activities agreed with PJ19, ref. [6], and sufficient to carry out the current activity. They are repeated here and constitute the scope of the current work:

- Analyse the Wave 1 baseline safety assessment, ref. [2], and identify gaps and needs for complementary developments
    - No gaps were identified in the current analysis
- Identify any issues/aspects that need to be addressed by standardisation
    - ATS-B3 applications mentioned in 6.2.8 will need to be standardised in due time, meanwhile the Safety and Performance Requirements used here are documented in EUROCAE ED228A, ref. [4].
    - The only related document known to these authors is ref. [9] as an initial set of Quality of Service set of requirements of future ATS-B3, which have neither been validated nor criticized at the time of writing.
- Top-Down approach: taking Operational Hazards from relevant standards and build Fault Trees for mono and multi-link scenarios
    - Ref. [2] has provided an approach to this requirement, which is used as a basis of the current work. Additional more detailed analysis on the specific case of Iris Precursor is available in ref. [7].
    - Within the limits of available resources and time, the current report is using available work to develop the missing part in the bullet below.
- Bottom-Up approach: this is the main focus of this report, i.e. work not performed before and being a strong gap in current safety analyses. A Failure Mode Effect and Criticality Analysis (**FMECA**) and a **RAM** analysis (Reliability Availability Maintainability) are proposed in the next chapters.

Note that software assurance is provided through Software Assurance Levels (SWAL). These SWALs shall be derived in relation to the guidelines in ED-153 but are out of scope of the present study.

2.4 Layout of the Document

Section 1 is the Executive Summary.

Section 2 provides an introduction and defines the scope of the document.

Section 3 reminds the FCI system description.

Section 4 describes the Methodology followed in the report.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Section 5 recalls the Main aspects of the Top-Approach.

Section 6 is the core of the document with the detailed FMECA/RAM study.

Section 7 provides conclusions and pointers to further work.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 System description

3.1 Introduction

Europe's future aeronautical communications will need to support an increased number of aircraft, including new types such as unmanned aircraft systems, as well as military air traffic. This demands higher datalink communication capacity and better performance than any existing communication system. SESAR is focused on developing an air-ground communication infrastructure capable of supporting future air traffic services in addition to flight operations centres (or military wing operations centres). A key part of resilient air-ground communications is the development of a future communications infrastructure (**FCI**) network infrastructure to support future service concepts and the migration towards internet protocol. The extension of a common, shared, integrated and resilient network infrastructure is necessary to enable SWIM applications and interfaces between all parties, including the military.

Timely access to airspace management data and information services is the first step towards enabling real-time sharing of trajectories in 4D. The SESAR research includes completion of specifications for the FCI network infrastructure, in order to support multilink capability and complete mobility between different datalink systems such as satellite communications (SatCom), LDACS, or AeroMACS (see Figure 1). It also addresses civil-military interoperability requirements for ground/ground network interfaces, safety and security requirements. The candidate solution will improve safety and security, enhancing the efficiency and flexibility of the overall datalink system through the provision of resilient multilink and mobile communications capabilities to the aircraft.

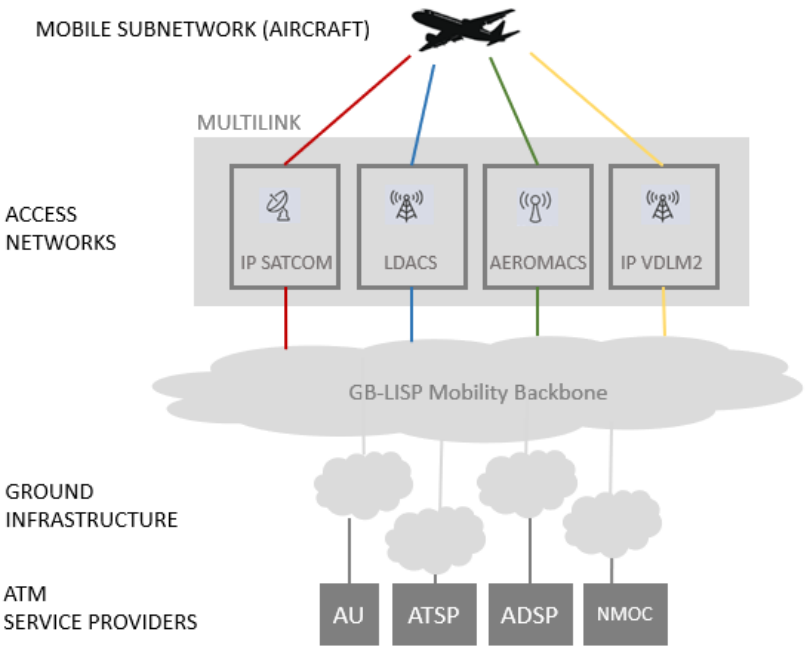


Figure 1. Future Communication Infrastructure high level architecture

Some intended benefits of the FCI are the following:

EUROPEAN PARTNERSHIP
Co-funded by the European Union

- Improved capacity, efficiency, performance, safety and resilience of the current CNS infrastructure
- It will enable the implementation and deployment of ATN-IPS in Europe and will support interoperability of the OSI and IPS networks
- Limited need for airborne changes to support multilink and mobility concepts, thanks to well-designed ground IP infrastructure
- Improved civil-military interoperability
- Positive economic impact on the deployment of the overall future communications system

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4 Methodology

4.1 Introduction

In agreement with Project 19 of SESAR2020 defining the scope of the current work, ref. [6], this document constitutes the Safety Assessment Report (SAR) for solution 77. In order to reach the assigned goals, this report follows EUROCONTROL's Safety Assessment Methodology (SAM), ref. [8], and EUROCAE ED-78A Guidelines, ref [5], which provide the expected results. According to the SAM method, a safety assessment comprises three phases:

- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA).

FHA shall identify and classify the hazards associated with the system and derive safety objectives for the system (objective for the safety of the system). This analysis is performed in the ED228 A document, refs. [4], [5].

PSSA shall demonstrate that the system can be designed and developed in a manner, which will ensure that the safety objectives derived from the FHA can be achieved. The PSSA shall establish the failures that may cause each of the hazards identified in the FHA and shall assess whether these failure events meet the hazard safety objectives.

The assessment approach combines two methods: Top down and bottom up. The Top down starts from the hazard potentially incurred by FCI datalink and establish an apportionment of its contributing sources of failures whereas the bottom up starts from the source of failures that could occur in any component of the FCI and causes the considered hazard to show its rate of occurrence is reasonably acceptable and meets the hazard safety objective set in the FHA.

The top-down failure analysis used is the Fault Tree Analysis (**FTA**); whereas the bottom-up failure analysis used is a combination of the Reliability Block Diagram (**RBD**) and Failure Modes, effects & Criticality Analysis (**FMECA**). Based on the method of assessment and the frequency by which each failure may occur, it can be assessed whether the safety objectives for a particular hazard can be met. Where this is not the case, additional risk mitigation needs to be introduced, resulting in the definition of additional Safety requirements.

Software assurance is provided through Software Assurance Levels (SWAL). These SWALs shall be derived in relation to the guidelines in ED-153 but are out of scope of the present study.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4.2 Stakeholders' expected benefits with potential Safety impact

4.2.1 Objective and process

The objective of the PSSA is to demonstrate that the system as specified and designed is compliant with the required safety objectives for all hazards derived from the FHA and as collected in ED228A.

This is done by identifying the type of failures that might lead to a given hazard and analyse, how often the failures are likely to occur and which mechanisms in the system that can rectify or compensate for the effect of the failure. The effects of failures are depicted per FTA i.e., the hazard apportionment whereas the failures are identified by FMECA and RBD methods to illustrate the relationship between the individual failures and these hazards and to analyse whether the safety objectives can reasonably be expected to be met.

If this is not the case, risk mitigation means must be introduced. They may include:

- Adjustments to the system functionality (e.g., new system requirements)
- Adjustments to the system design (e.g., additional redundancy)
- Adjustments to the expected use of the system (e.g., change in operational procedures)
- Adjustments external to the system (at the local equipment)
- Adjustment of the safety objectives if deemed unreasonably set.

Risk mitigation means, introduced in the specification or design, are defined as Safety requirements.

4.2.2 Hazards and Safety Objectives

ATS data communications services are documented in DO-350A/ED-228A [1] & DO-351A/ED-229A [2] (or future revision B currently addressed in EUROCAE/RTCA WG78/SC214).

The implementation of the Air Traffic Service (ATS) applications supporting the Baseline 2 data link services defining the Context Management (CM) application, the Controller-Pilot Data Link Communications (CPDLC) application and the Automatic Dependent Surveillance Contract (ADS-C) application.

Operational Safety Assessment for ATS datalink Services, based on CPDLC and ADS-C, is described in ED-228A/DO-350A. The document assigns a Security Class to each hazard. Derived from ED-78A/DO-264A, five Severity Classes (SC) are defined in terms of their impact on Operations, (aircraft) Occupants, Flight Crew, and the Air Traffic Service. SC5 is little more than a "don't care" category, while SC1 hazards relate to the total loss of an airframe and is not expected to apply to Air Traffic Services.

From the Hazard classification and safety objectives relationship of ED-78A/DO-264A, it is possible to identify that the occurrence of:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

- Severity class 5 (SC5) has no minimum safety objective,
- Severity class 4 (SC4) is shown to be no more likely than probable (equivalent to MINOR: 10E-3),
- Severity class 3 (SC3) is shown to be no more likely than remote (equivalent to MAJOR :10E-5),
- Severity class 2 (SC2) is shown to be no more likely than extremely remote (equivalent to HAZARDOUS: 10E-7),
- Severity class 1 (SC1) is shown to be no more likely than extremely improbable (equivalent to CATASTROPHIC: 10E-9) and is also subject to the "no single failure" criteria.

Table 1 lists (in a simplified summarizing form) the results of ATS data communications operational hazard assessment documented in Appendix B and Appendix C of DO-250A/ED-228A.

Hazard #	Hazard Description	Hazard Severity	Safety Objective
OH-DC-1	Loss of data link capability [single aircraft]	SC4	10E-3
OH-DC-2	Loss of data link capability [multiple aircraft]	SC3	10E-5
OH-DC-3	Reception of a corrupted data link message [single aircraft]	SC3	10E-5
OH-DC-4	Reception of corrupted data link messages [multiple aircraft]	SC3	10E-5
OH-DC-5	Reception of an unintended data link message [single aircraft]	SC3	10E-5
OH-DC-6	Reception of unintended data link messages [multiple aircraft]	SC3	10E-5
OH-DC-7	Unexpected interruption of a data link transaction [single aircraft]	SC3	10E-5
OH-DC-8	Unexpected interruption of data link transactions [multiple aircraft]	SC3	10E-5

Table 1: Operational Safety Hazards of ATS Data Communications

It is important to note that ED-228A/DO-350A Operational Hazard Assessment was performed in a 'single link' approach. To consider a multilink scenario, it is necessary to perform a RAM analysis where several A/G datalink technologies are considered independently in the corresponding FCI datalink functional block.

The multilink environment may be used to improve availability and reliability beyond that which can be achieved when only a single end-to-end path exists. It achieves this by being able to switch dynamically between each available path to overcome either persistent or transient problems on a given path.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

The hazards related to misdirection of messages and corruption of messages (OH-DC-3, OH-DC-4, OH-DC-5 and OH-DC-6) require a separate SWAL analysis that of out of scope of this initial RAM analysis and, for this reason, these hazards are marked in grey in the previous table.

Note that Design Assurance Levels (DAL) are also out of scope of this study.

When further reviewing OH-DC-7 compared to OH-DC-1, it is considered that OH-DC-7 materializes when OH-DC-1 materializes or when, even if multiple access networks are available and one subnetwork fails, the failover to another subnetwork takes too much time and creates an interruption of a datalink transaction because of some time-outs, even if the second subnetwork datalink capability is available. But this scenario can only happen if there is a software failure (such as a routing failure) which would need to be subject to a SWAL analysis and therefore is out of scope of the study. This means that OH-DC-7 will provide same results than OH-DC-1.

This situation is also happening when reviewing OH-DC-8 compared to OH-DC-2 where it is assumed that OH-DC-8 will provide same results than OH-DC-2.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 FCI SAFETY ASSESSMENT: TOP/DOWN APPROACH FAILURE ANALYSIS

According to the method used, one should, for each hazard, determine which failures in the FCI system, people and procedures could cause a hazard and what is the probability that such failures occur. Consequently, during the PSSA, a failure analysis is performed for each hazard and compared with the hazard's Safety Objective.

The detail of the hazards affecting the FCI service has been included in EUROCAE ED228A document.

Prior to the completion of fault trees for hazards concerning the FCI service, some previous issues have been addressed.

The description of the hazards that were determined during the previous FHA version development, as well as their effects, and the risk reduction measures that were detected in the initial phase have been revisited.

As a main result, these descriptions fundamentally describe equipment failures, so it has been necessary to deepen the involvement of personnel actions and the procedures established in the service provided. Information on these two factors has been identified in this PSSA, including the outcomes. In some cases, nuances and new barriers or mitigations have also been included. All this has been reviewed, validated, and improved by experts in FCI service, belonging to both the operational part and the technical exploitation of the ATC systems.

After this review process, , the following table summarizes the hazards related to the FCI services:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective before apportionment (/FH)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	1,00E-03
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	1,00E-03
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	1,00E-03
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	1,00E-05
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	1,00E-05
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	1,00E-05
OH-DC-7	Unexpected interruption of a data link transaction [single aircraft]	3	1,00E-05
OH-DC-8	Unexpected interruption of data link transactions [multiple aircraft]	3	1,00E-05

Table 2: Hazards and associated safety objectives

It is worth noting that due to the severity of their effects, only hazards which have a safety objective associated (severities from 1 to 4) are analysed in detail.

As another general consideration, the distribution of the safety objective among the different actors that may be causing the occurrence of a hazard, has been conducted considering the experience of different professionals specialized in technical and operational issues in relationship with the analysed service. This session initially started with general failure rates (at a high level) refinement, also completed with lower levels of fault trees (level with more details), obtaining the final distributions according to the opinion of above-mentioned experts. Both the system architecture, as well as the safety events and their distribution in the trees, were refined with the collaboration of the experts.

The distribution of the safety objective must take into consideration the potential FCI system failures as well as people and procedures failures.

Based on operational experience, the following apportionment of failures for all the FCI hazards has been considered:

- FCI system failure: 80%
- People failure: 10%
- Procedure failure: 10%

For each of the hazards with severities from 1 to 4, the corresponding top-down analysis has been performed to define an apportionment of safety objectives among FCI system, people and procedures failures identifying the corresponding FCI safety objectives including apportionment.

The safety assessment against the safety objectives of the FCI system is summarized in the following table:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective before apportionment (/FH)	Apportionment to FCI system	Safety Objective including apportionment (/FH)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	1,00E-03	80%	8,00E-04
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	1,00E-03	80%	8,00E-04
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	1,00E-03	80%	8,00E-04
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	1,00E-05	80%	8,00E-06
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	1,00E-05	80%	8,00E-06
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	1,00E-05	80%	8,00E-06
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	1,00E-03	80%	8,00E-04
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	1,00E-03	80%	8,00E-04
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	1,00E-03	80%	8,00E-04
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	1,00E-05	80%	8,00E-06
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	1,00E-05	80%	8,00E-06
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	1,00E-05	80%	8,00E-06

Table 3: Hazards and associated safety objectives including apportionment

A bottom-up safety assessment approach will be performed in the next section running a RAM (Reliability/Availability/Maintainability) analysis using RBD (Reliability Block Diagrams) method to demonstrate that FCI system meets the safety objectives identified in this high-level top-down analysis.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

6 FCI SAFETY ASSESSMENT: BOTTOM/UP APPROACH FAILURE ANALYSIS

6.1 OBJECTIVE

The objective of this chapter is to perform the Reliability/Availability/Maintainability Analysis (RAM) of the FCI datalink solution as specified in ED228A document. The RAM analysis aims to demonstrate that the FCI datalink solution is compliant with the required safety objectives for each of the hazards identified in the FHA.

The RAM approach used is the Reliability Bloc Diagram (RBD) method with the goal to demonstrate whether the safety objectives for each hazard can be met when various network path components failures inducing these hazards occur. The RBD method depicts the FCI datalink path blocks which composes the provision of the end-to-end datalink services.

6.2 RAM ANALYSIS

As stated in section the safety objectives defined at the functional level of the system correspond to Tolerable Hazard Occurrence Rates (THORs).

The methodology applied under IEC EN 61508 refers to safety being related to dangerous failures, dangerous being either loss of network service or corruption of network service causing the loss or corruption of the ATM IP flow and preventing it from running error free.

6.2.1 RAM ANALYSIS MODEL

This RAM analysis uses 2 complementary analysis methods, the RBD and FMECA combined with the Markov chain modelling techniques to assess the solution services in scope of the RAM and their failure rates and their risks of failures for to the applicable hazards. The approach derives the estimated services availability and verifies whether the solution contains any unacceptably safe single points of failures.

These techniques use a bottom-up approach and consider one failure event occurring at a time. It checks its effects at the unit level, node level and network path level, which in turn impacts the service path level. The RBD and FMECA at the node level is readily available from the FCI components design data. Indeed, RBD and FMECA is applied on all FCI datalink solution at the design and verification stages of the FCI datalink solution development cycle to estimate their Reliability and fault coverage and verify they meet their Reliability design requirements.

6.2.2 FAILURE ANALYSIS STRATEGY.

The goal of this chapter is to present the reliability model and provide reliable information about the expected reliability of the ATM critical data flows as defined by FHA.

Availability of the critical paths is impacted by:

EUROPEAN PARTNERSHIP

Co-funded by the European Union

- availability of FCI datalink elements of which data flow is consisted,
- interdependence of network elements,
- and common cause of failure (CCF) where same types of elements are used.

FMEA has been conducted on FCI datalink building systems element level by ED228A document.

MTBF values and calculations have been provided and taken as source values for building FTA models and calculating MU. Detailed information regarding the FTA calculation process can be found in section 6.2.3 “DETAILS OF THE RAM CALCULATION PROCESS “.

Per the method used, one should, for each hazard, determine which failures in the FCI datalink solution components or the use hereof could cause any of the hazards and what is the probability that such failures occur.

6.2.3 DETAILS OF RAM CALCULATION PROCESS.

6.2.3.1.1 Term definition and formulas

Availability (A): Inherent Availability is defined as the probability that a system or equipment, when used under specified conditions, not considering delays due to the support environment (i.e., readily available tools, spares, maintenance personnel, etc.), will operate satisfactorily at any point in time, as required. Operational Availability is defined as the probability that a system or equipment, when used under specified conditions, in a real support environment (i.e., a specific amount of time is required to have tools, spares, maintenance personnel, etc. on site), will operate satisfactorily at any point in time, as required. In this document the term availability always refers to operational availability.

Failure Rate (λ): The Failure Rate is the number of failures per time unit. For the reason, when the electronic equipment is operated within the specified useful life, the failure rate is assumed to be constant. Therefore, the failure rate is equivalent to the reciprocal of MTBF.

Mean Time Between Failure (MTBF): The Mean Time Between Failure is defined as the sum of SST and SOT divided by the numbers of failures. As continuously operational items are assumed, the MTBF value is equal to the Mean Up Time (MUT). This definition is termed Mean operating Time Between Failure in [IEC 61703]

Mean Time To Repair (MTTR): The Mean Time To Repair only concerns the time necessary for repairing the equipment, including failure identification. It is defined as the ratio of the sum of corrective maintenance times and the total number of failures. This definition is termed Mean Repair Time in [IEC 61703]. By simplification, it is considered that MTTR parameter also includes:

- Mean Logistic Down Time (MLDT): The Mean Logistic Down Time is directly linked to the logistic environment of the system. It is dependent on stock level, the probability of non-interruption of spare part delivery from stock and provision times between considered levels.
- Mean Travel Time (MTT): The Mean Travel Time is the mean time necessary to get spare parts in a considered site stock (i.e., administrative time). This value is usually very low and in general negligible. This definition is termed Mean Administrative Delay in [IEC 61703].

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Repair Rate (μ): The Repair Rate is defined as the ratio of the sum of all failures and the sum of all times spent on failure correcting maintenance, i.e., the reciprocal of MDT.

When performing the calculations for the Fault tree analysis, typical MTBF values provided by the equipment manufacturer (for instance Cisco or Nokia) have been considered. Different values of MTTR parameters were taken into consideration to be applied to FCI network nodes.

Abbreviation	Meaning
FTA	Fault tree analysis
MTBF	Mean time between failures (measured in hours)
MTTR	Mean time to repair (measured in hours)
FR	Failure rate, measured in 10^{-6} hours
Q mean	Mean unavailability

The Mean unavailability is calculated using the following calculation parameters:

The failure of a network component (namely a router) is treated as a repairable event – where MTBF and MTTR are taken into consideration according to the following formula:

Q mean =λ/(λ + μ),

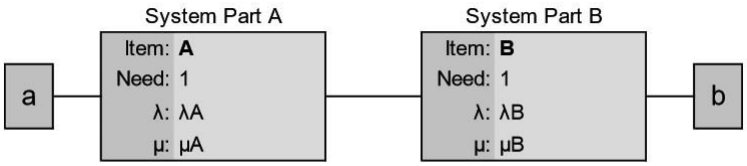
where FR= λ, μ=1/MTTR

The FR (Failure rate) is derived from the general formula MTBF= 1/FR,

where we express FR as =1/MTBF.

For an initial calculation of FCI RAM analysis, an initial MTTR/MDT (time necessary for repairing the equipment) value of 4 hours for FCI ground systems and A/G access networks and an initial MTTR/MDT value of 24 hours in the case of airborne systems are going to be considered.

Formulas in use for a serial structure:



Co-funded by the European Union

Failure rate (λ_S):

$$\lambda_S = \lambda_A + \lambda_B = \frac{MTBF_A + MTBF_B}{MTBF_A \cdot MTBF_B}$$

Repair rate (μ_S):

$$\mu_S = \frac{MTBF_A + MTBF_B}{MTBF_A \cdot MDT_B + MTBF_B \cdot MDT_A + MDT_A \cdot MDT_B}$$

Reliability (R_S):

$$R(t)_S = R(t)_A \cdot R(t)_B$$

Unreliability (UR_S):

$$UR(t)_S = 1 - R(t)_S$$

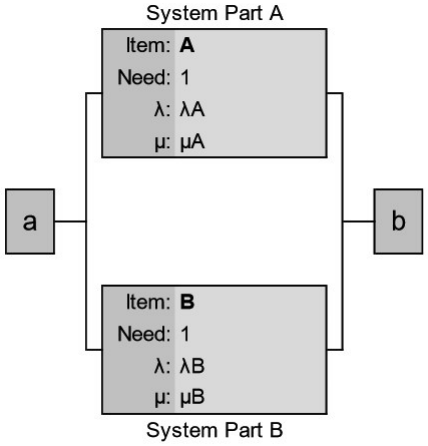
Availability (A_S):

$$A_S = A_A \cdot A_B$$

Unavailability (UA_S):

$$UA_S = 1 - A_S$$

Formulas in use for a parallel structure:



Co-funded by the European Union

Failure rate (λ_P):

$$\lambda_P = \frac{MDT_A + MDT_B}{MTBF_A \cdot MTBF_B + MTBF_A \cdot MDT_B + MTBF_B \cdot MDT_A}$$

Repair rate (μ_P):

$$\mu_P = \mu_A + \mu_B$$

Reliability (R_P):

$$R(t)_P = R(t)_A + R(t)_B - R(t)_A \cdot R(t)_B = 1 - UR(t)_A \cdot UR(t)_B$$

Unreliability (UR_P):

$$UR(t)_P = UR(t)_A \cdot UR(t)_B$$

Availability (A_P):

$$A_P = A_A + A_B - A_A \cdot A_B = 1 - UA_A \cdot UA_B$$

Unavailability (UA_P):

$$UA_P = UA_A \cdot UA_B$$

6.2.3.2 Initial considerations different FCI datalink solution components.

Following sections provide information about MTBF values and calculations per FCI system element.

The FCI system utilizes the following devices:

- A/G routers are mainly Cisco 4351 with MTBF: 566.310 hours.
- The G/G routers and the OSI/IPS GWs are Cisco 4331 with MTBF: 587.250 hours.
- Ground ATN/IPS End-System and ATN/OSI End-System are implemented with an estimated MTBF: 500.000 hours.
- Airborne ATN/IPS End-System and Airborne ATN/OSI End-System are implemented with an estimated MTBF: 500.000 hours.

ADS-C server has been considered collocated and integrated with the Ground ATN/IPS or ATN/OSI End system and not as a centralized Pan-European system.

Regarding NewPENS availability, the current SLA signed in the contract with the current NewPENS Service Provider has been considered. So, the following values are considered:

- Availability: 99,99%.
- MTTR NewPENS (h): 4.

A datalink Mandate (EC 310/2015) is in force today that claims for an availability of 99,99% for the VDLm2 A/G access network over FL285. As initial approach, it has been considered that all the potential A/G access networks (LDACS, SATCOM and AeroMACS) will provide the same availability figure of 99.99%.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Regarding Mean Time To Repair (MTTR) values, it has been assumed that the current experience of some ANSPs maintaining and operating other ground communications infrastructure will also apply to FCI infrastructure. The following initial values have been considered:

- MTTR ground systems (h): 4.
- MTTR airborne systems (h): 24.
- MTTR A/G access network (h): 4
- ADS-C serve

6.2.3.3 CCF (Common Cause Failures) groups used in calculations

FCI datalink solution elements and interconnections scheme show which system elements are used in FCI as well as the number of elements used to provide high availability. Interdependency between these elements is used to represent FCI datalink Functional models that will be used for evaluating the reliability of the FCI datalink solution.

To ensure availability calculations consider all relevant parameters, relying on MTBF data per single element is not sufficient.

Using multiple elements of the same type in the same system can result in the risk of simultaneous malfunctions of multiple elements based on the common weakness/vulnerability/cause. Relying on multiplication of the critical elements to achieve acceptable availability must consider the risk that all such elements can fail at the same time because they are designed, manufactured and used in a same way.

FCI datalink solution elements that are potentially vulnerable to CCF are:

- Duplicated FCI datalink solution components as per FCI datalink design.
- Unknown CCF that could impact independency of the A/G datalink subnetworks.

RAM analysis will perform an evaluation of the expected CCF rates for these FCI datalink solution elements which are to be used in FTA (Fault tree analysis) and is introduced in the FCI design as a corrective β factor.

Several corrective β factors are considered during RAM analysis:

- β1 factor between Ground ATN/IPS End systems: it is measuring the interdependency between two Ground ATN/IP End systems devices of the same model providing redundancy.
- β2 factor between G/G ATN/IPS routers: it is measuring the interdependency between two G/G ATN/IPS router devices of the same model providing redundancy.
- β3 factor between A/G ATN/IPS routers: it is measuring the interdependency between two A/G ATN/IPS routers devices of the same model providing redundancy.
- β4 factor between Airborne ATN/IPS End systems: it is measuring the interdependency between two Airborne ATN/IPS End systems devices of the same model providing redundancy.
- β5 factor between Airborne Mobility (AGMI): it is measuring the interdependency between two Airborne Mobility (AGMI) devices of the same model providing redundancy.
- β6 factor between Airborne ATN/IPS routers: it is measuring the interdependency between two Airborne ATN/IPS routers devices of the same model providing redundancy.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

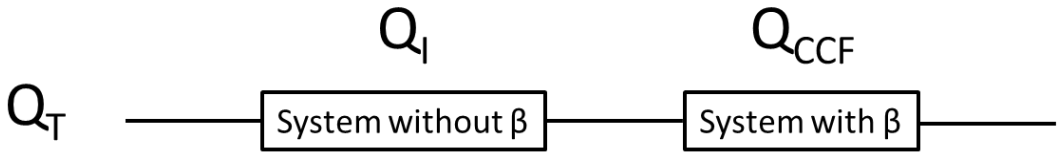
- β7 factor between Ground ATN/OSI End systems: it is measuring the interdependency between two Ground ATN/OSI End systems devices of the same model providing redundancy.
- β8 factor between G/G ATN/OSI routers: it is measuring the interdependency between two G/G ATN/OSI routers devices of the same model providing redundancy.
- β9 factor between OSI/IPS gateways: it is measuring the interdependency between two OSI/IPS gateways devices of the same model providing redundancy.
- β10 factor between A/G ATN/OSI routers: it is measuring the interdependency between two A/G ATN/OSI routers devices of the same model providing redundancy.
- β11 factor between Airborne ATN/OSI End systems: it is measuring the interdependency between two Airborne ATN/OSI End systems devices of the same model providing redundancy.
- β12 factor between Airborne ATN/OSI routers: it is measuring the interdependency between two Airborne ATN/OSI routers devices of the same model providing redundancy.
- β13 factor between VDLm2 and LDACS: it is measuring the interdependency between these two VDLm2 and LDACS A/G datalink subnetworks.

The β factor method is an approximation method used for the quantitative evaluation of CCFs. In this method, the likelihood of the CCF is evaluated in relation to the random failure rate for the component. A β factor is estimated such that β% of the failure rate is attributed to the CCF and (1- β)% to the random failure rate of the component. Ideally, this factor is obtained through historical data by determining the percentage of all the component failures in which multiple similar components failed.

This means that a β factor = 0 means that both systems are completely independent with no common point of failure and β factor = 1 means a total interdependency between both systems provoking that, when one of both systems fails, the other one also fails at the same time.

Component failures are then split into independent failures, affecting just the component, and common cause failures, affecting all components sharing the common failure mode. The beta factor is the ratio of common cause failures to total failures for the component.

By stipulating a common cause, the events are no longer independent, and the approach is no longer valid. The common cause must be treated as a separate, single point of failure. The Rare approximation (only accurate for small probability values) for this would be: $P(A \cap B) = P(A) \cdot P(B) + P(CCF)$. This is represented in the following figure:



The calculation of the unavailability due to CCF would be:

$Q_{CCF} = \beta * Q$

and the unavailability considering both systems completely independent would be:

Co-funded by the European Union

$Q_I = ((1- \beta) * Q) * ((1- \beta) * Q)$

Finally, the total unavailability would be: $Q_T = Q_I + Q_{CCF} - Q(I \cap CCF) = Q_I + Q_{CCF}$

6.2.3.3.1.1 Duplicated FCI datalink solution elements as per FCI datalink design (β1 to β12 factor).

Critical devices used in a FCI datalink solution design are electronic equipment with no moving or wearing parts which are critical for the functionality.

Normal implementation approach is to install two devices in a couple of the same manufacturer to perform a specific function. In this way, a certain degree of redundancy is achieved in order that, if one of the devices is down, the other one of the same couple goes on working ensuring that the service is up.

Nevertheless, the software running on both devices is identical. That means that, if a bug exists in one of the network devices, it is highly likely that the same bug already exists in the redundant one.

Considering all above points mentioned, Common Cause Failure (CCF) for FCI datalink solution elements can be estimated as extremely low even when reliable information about CCF for critical elements is not available.

To compensate low reliability of the data, an initial conservative value of $\beta1 = \beta2 = \beta3 = \beta4 = \beta5 = \beta6 = \beta7 = \beta8 = \beta9 = \beta10 = \beta11 = \beta12 = 10\%$ will be used by default in reliability calculations for FCI datalink elements during RAM analysis.

6.2.3.3.2 CCF that could impact independency of the four A/G datalink subnetworks (β13 factor).

FCI datalink solution relies on four independent Air/Ground datalink subnetworks. In the case of VDLm2 and LDAC technology, it is highly probable that both A/G access networks will share transmission media infrastructures such as the VGS station, as well as elements with a certain dependency (equipment from the same manufacturer, common lines, similar maintenance procedures or carried out by the same company, etc.). Therefore even if they are from operated by different operators, a common failure factor is considered, the β13 factor, which considers possible common failures in these infrastructures.

An initial value of $\beta13 = 0\%$ will be considered by default in reliability calculations for FCI datalink elements during RAM analysis.

6.2.4 AIR TRAFFIC (FLIGHT HOURS) CONSIDERED DURING RAM ANALYSIS.

Safety objectives described in EUROCAE ED228A are identified in terms of probability of identified hazard happening during one flight hour.

Reliability studies performed in FCI RAM must consider the number of flight hours managed by FCI systems. It is therefore required to estimate a value of this parameter to perform the RAM calculations.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

In general, safety studies are developed considering pessimistic scenarios to assure that the outcomes of these safety analysis are always applicable to all the scenarios.

In addition,, it is assumed that datalink capabilities are delivered over FL285 in accordance with the EC Mandates. So, it has been estimated that, on average, half of the flight time is over FL285 and the other half is under that flight level.

6.2.4.1.1 Air traffic (Flight Hours) considered for FCI ground and A/G access network systems.

Taking into consideration these factors, it has been considered that the number of flight hours a year managed by the FCI ground and A/G access network system providing datalink services to a small to medium ANSP over FL285 are 50.000 FH/year, which corresponds to 50.000 FH x 2 = 100.000 FH/year in total. This value means an average of 275 flights a day.

Considering that the total number of flights managed by NM in all Europe is around 25.000 flights a day, the value of 275 flights a day is in a right order of magnitude.

6.2.4.2 Air traffic (Flight Hours) considered for FCI Airborne systems.

Taking into consideration these factors, it has been considered that the number of flight hours a day when the FCI airborne systems are using datalink services is 10 hours that represents a value of 3.650 FH a year.

6.2.5 FUNCTIONAL ARCHITECTURE.

For assessing Operational Hazards in the context of FCI system, it is considered that the composition and architecture of the FCI system is illustrated as follows:

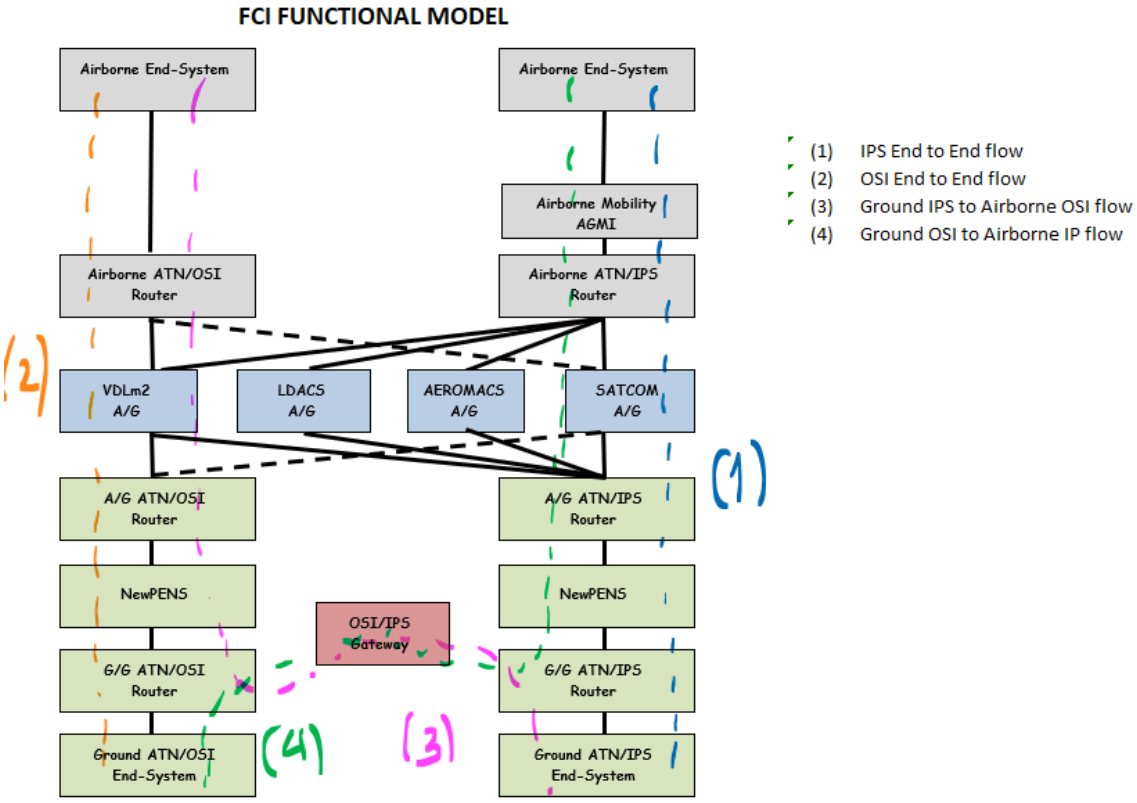


Figure 2: Main FCI information flows

Three different traffic flows have been considered to perform the RAM analysis:

- Ground IPS – Airborne IPS flow.
- Ground OSI – Airborne IPS flow.
- Ground IPS – Airborne OSI flow.

6.2.6 OUTCOMES OF THE RAM ANALYSIS.

6.2.6.1 Initial values considered to perform FCI RAM analysis.

Some initial values to perform the FCI RAM analysis have been described in the previous sections and are summarized as follows:

MTTR airborne systems (h):	24	
MTTR A/G access network (h):	4	
MTTR NewPENS (h):	4	
β1 factor between Ground ATN/IPS End systems:		0,10
β2 factor between G/G ATN/IPS routers:		0,10
β3 factor between A/G ATN/IPS routers:		0,10
β4 factor between Airborne ATN/IPS End systems:		0,10
β5 factor between Airborne Mobility (AGMI):		0,10
β6 factor between Airborne ATN/IPS routers:		0,10
β7 factor between Ground ATN/OSI End systems:		0,10
β8 factor between G/G ATN/OSI routers:		0,10
β9 factor between OSI/IPS gateways:		0,10
β10 factor between A/G ATN/OSI routers:		0,10
β11 factor between Airborne ATN/OSI End systems:		0,10
β12 factor between Airborne ATN/OSI routers:		0,10
β13 factor between VDLm2 and LDACS:		0,00
MTBF Ground ATN/IPS End-System (h):		5,00E+05
MTBF G/G ATN/IPS router (h):		5,87E+05
MTBF A/G ATN/IPS router (h):		5,66E+05
MTBF Airborne ATN/IPS End-System (h):		5,00E+05
MTBF Airborne Mobility (AGMI) (h):		5,00E+05
MTBF Airborne ATN/IPS router (h):		5,66E+05
MTBF Ground ATN/OSI End-System (h):		5,00E+05
MTBF G/G ATN/OSI router (h):		5,87E+05
MTBF A/G ATN/OSI router (h):		5,66E+05
MTBF OSI/IPS gateway (h):		5,87E+05
MTBF Airborne ATN/OSI End-System (h):		5,00E+05
MTBF Airborne ATN/OSI router (h):		5,66E+05
VDLm2 A/G availability:		99,990%
LDACS A/G availability:		0,000%
SATCOM A/G availability:		0,000%
AeroMACS A/G availability:		0,000%
NewPENS availability:		99,9900%
Number of flight hours managed by Ground systems a year (FH):		5,00E+04
Number of flight hours managed by Air systems a year (FH):		3,65E+03
Number of flight hours managed by A/G access network a year (FH		5,00E+04
Number of flight hours a day:		10,00

6.2.6.2 Fault Tree for OH-DC-1 – Detected loss of CPDLC capability [single aircraft].

The fault tree corresponding to this hazard has been analysed and compiled in this section.

Three different traffic flows have been considered for this hazard:

- OH-DC-1a: Ground IPS – Airborne IPS flow.
- OH-DC-1b: Ground OSI – Airborne IPS flow.
- OH-DC-1c: Ground IPS – Airborne OSI flow.

In the proposed fault tree, it is considered that the OH-CPDLC-1a, OH-CPDLC-1b and OH-CPDLC-1c hazards may happen due to one of the following basic causes:

Co-funded by the European Union

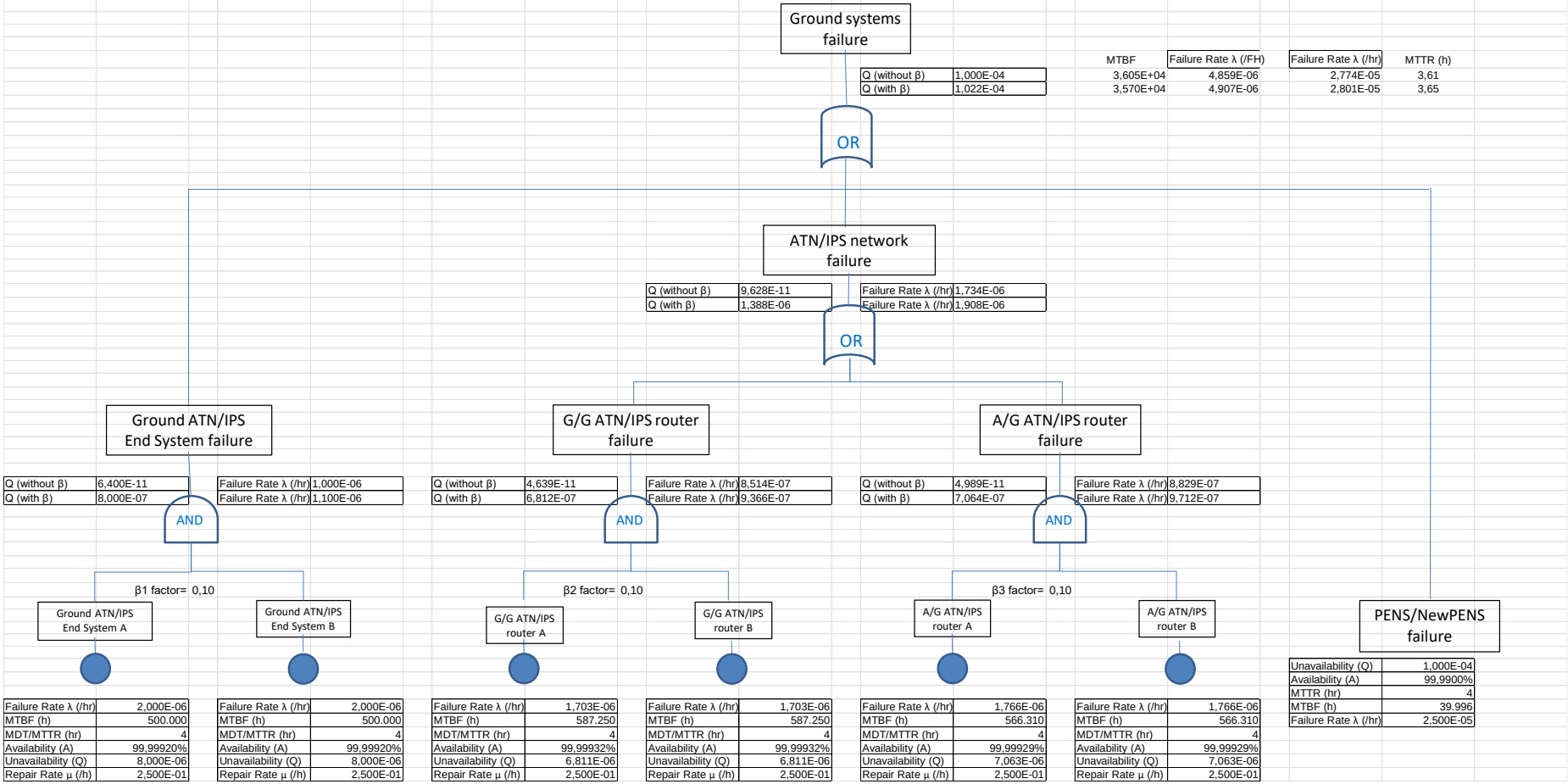
- A detected or undetected loss of the Aircraft ATC applications, which should encompass all failure cases on the Aircraft ATC system (Airborne ATN/IPS or ATN/OSI End System and Airborne Mobility AGMI) for which it can be determined that datalink services should not be used anymore and that the flight crew must revert to voice communications.
- A detected or undetected loss of the Aircraft ATN/IPS or ATN/OSI communications, which should encompass all failure cases on Aircraft ATN/IPS or ATN/OSI routing system that lead to an ATN/IPS or ATN/OSI communication failure for which it can be determined that datalink services should not be used anymore and that the flight crew has to revert to voice communications.
- A combined loss of different A/G access networks (VDLm2, LDACS, SATCOM, AeroMACS), which should encompass cases of simultaneous failures on any of these A/G radio systems, leading to an ATN/IPS or ATN/OSI communication failure, for which it can be determined that datalink services should not be used anymore and that the flight crew has to revert to voice communications.
- A detected or undetected loss of the Ground systems involved in the datalink communication (Ground ATN/OSI or ATN/IPS End System, G/G ATN/IPS or ATN/OSI router, A/G ATN/IPS or ATN/OSI router and NewPENS) for which it can be determined that datalink services should not be used anymore and that the flight crew has to revert to voice communications.

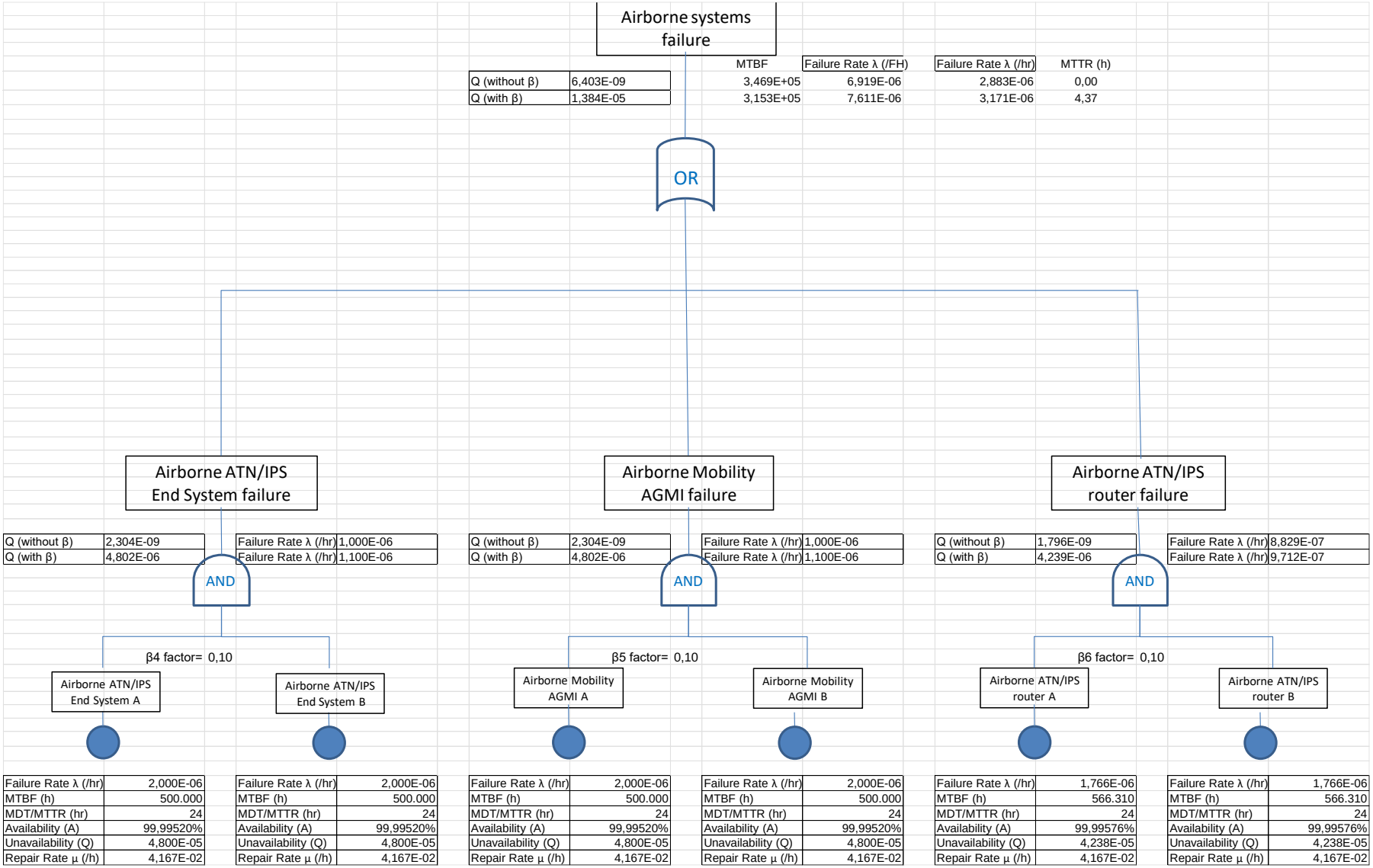
In addition to the previous basic failure causes, it is considered that for OH-CPDLC-1b and OH-CPDLC-1c hazards also apply the following basic cause:

- A detected or undetected loss of the OSI/IPS gateway for which it can be determined that datalink services should not be used anymore and that the flight crew must revert to voice communications.

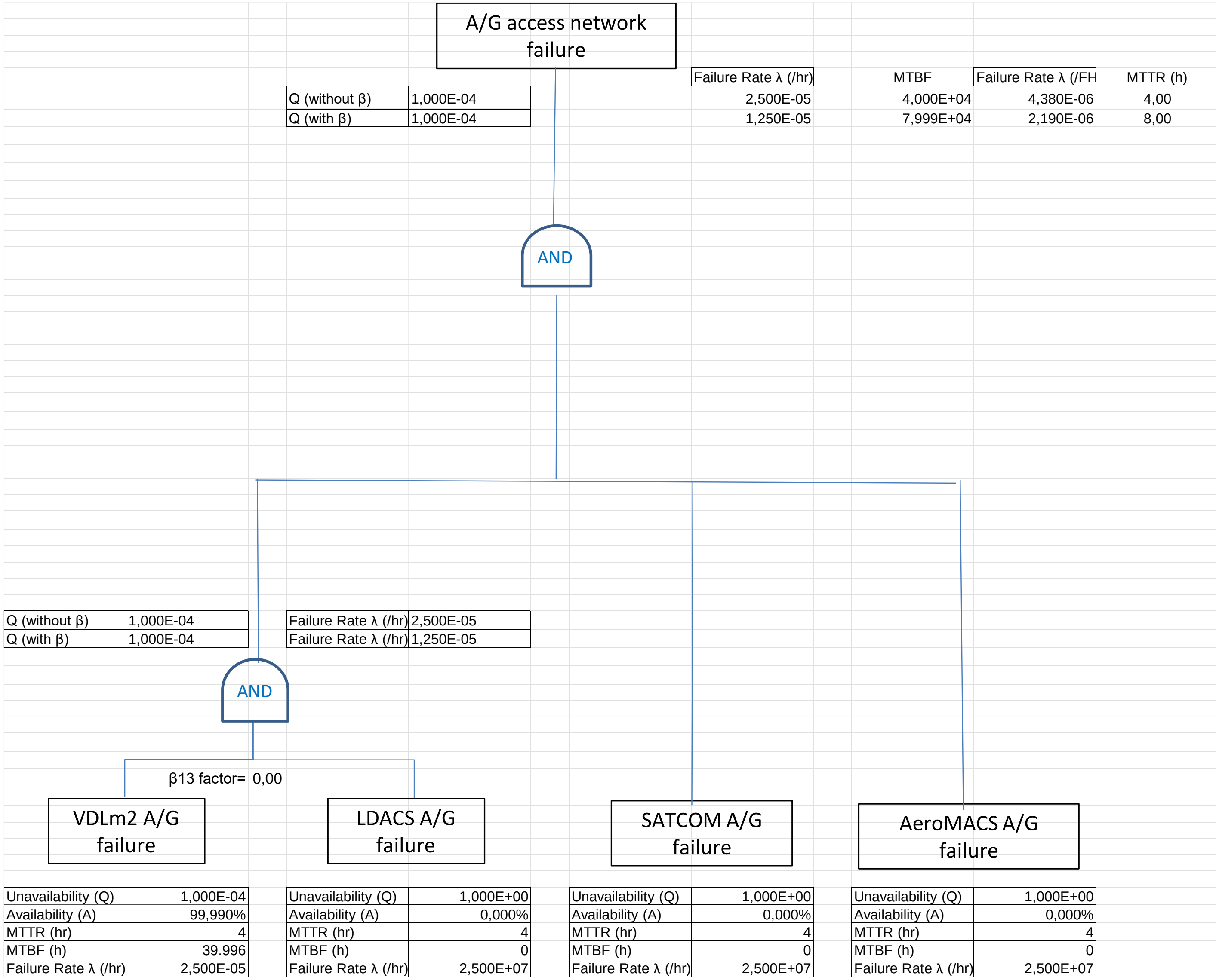
The outcomes obtained after performing the RAM analysis on these OH-DC-1a, OH-DC-1b and OH-DC-1c hazards are as follows:

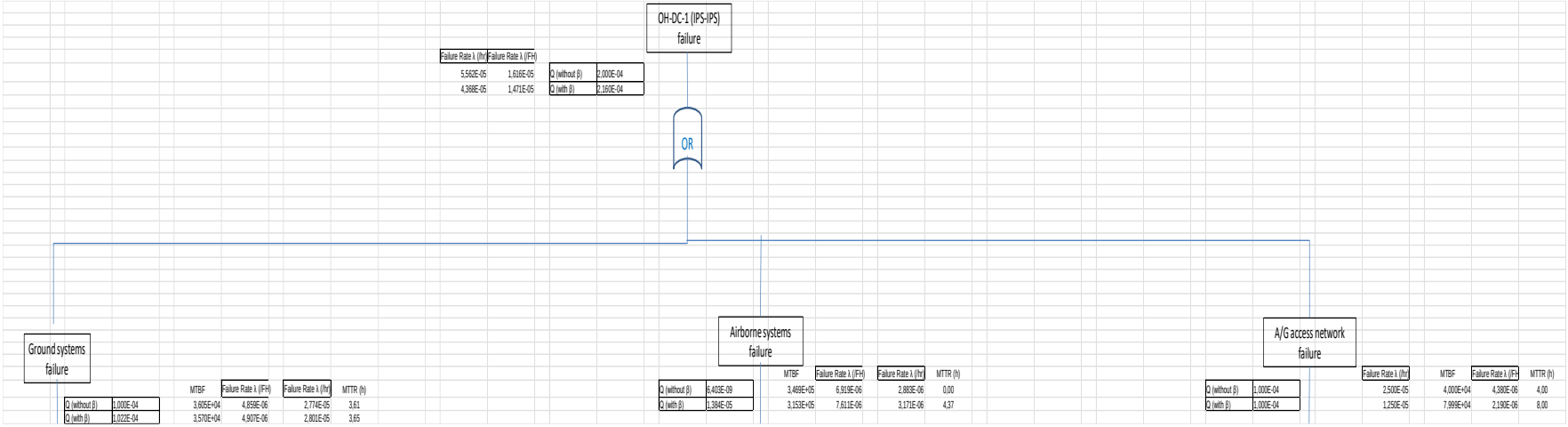
OH-DC-1a – Detected loss of CPDLC capability [single aircraft] (IPS-IPS flow):



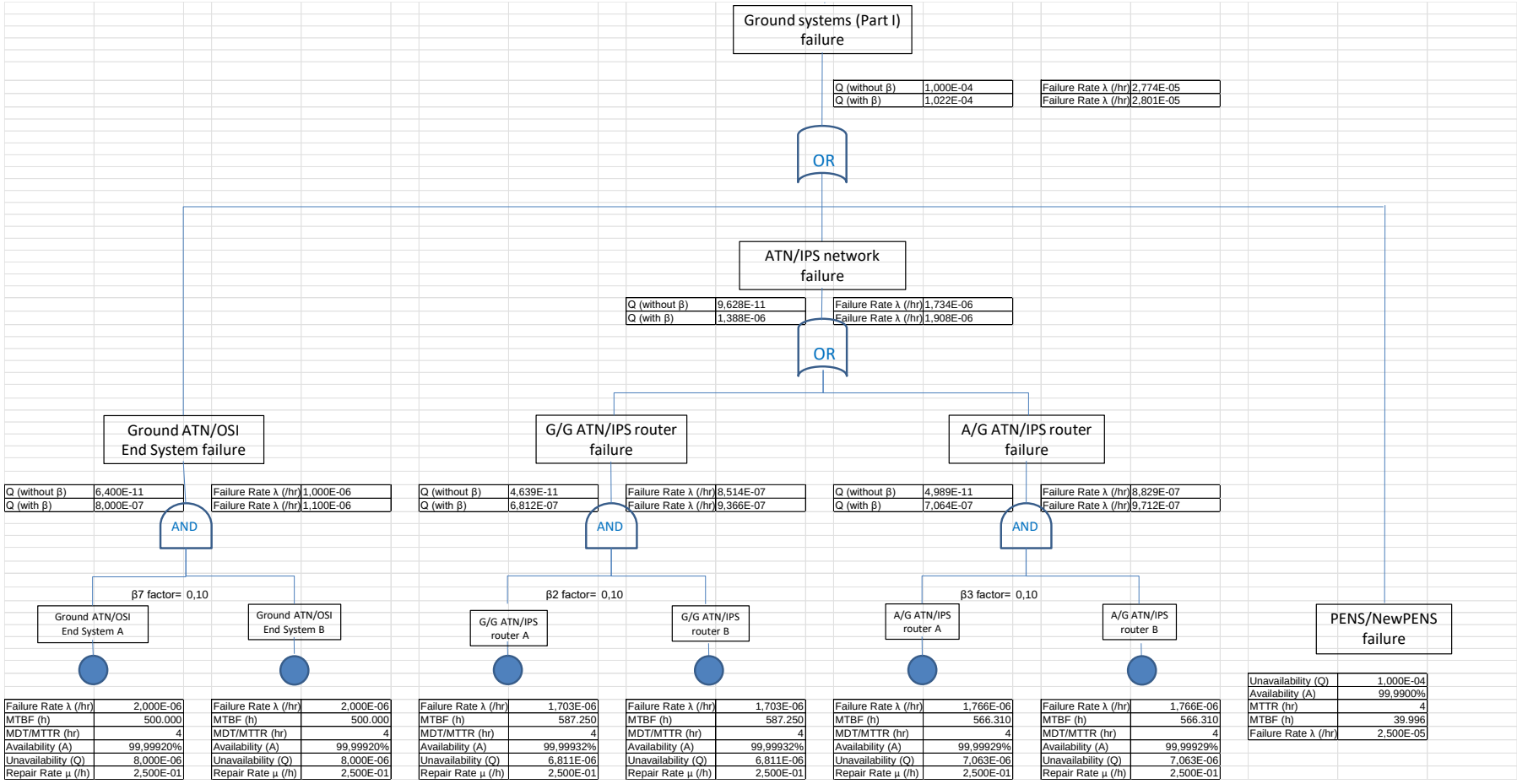


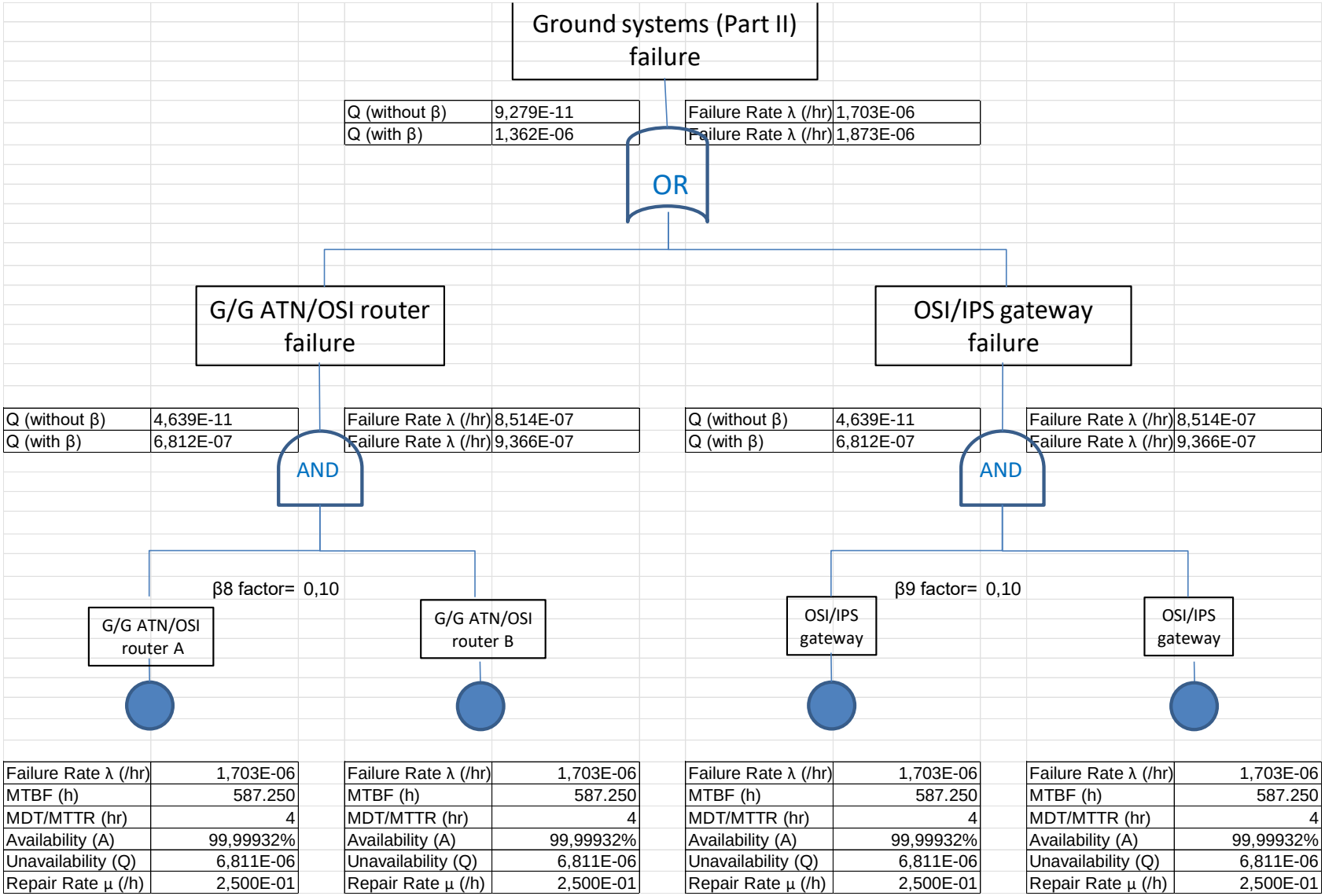
EUROPEAN PARTNERSHIP
Co-funded by the European Union

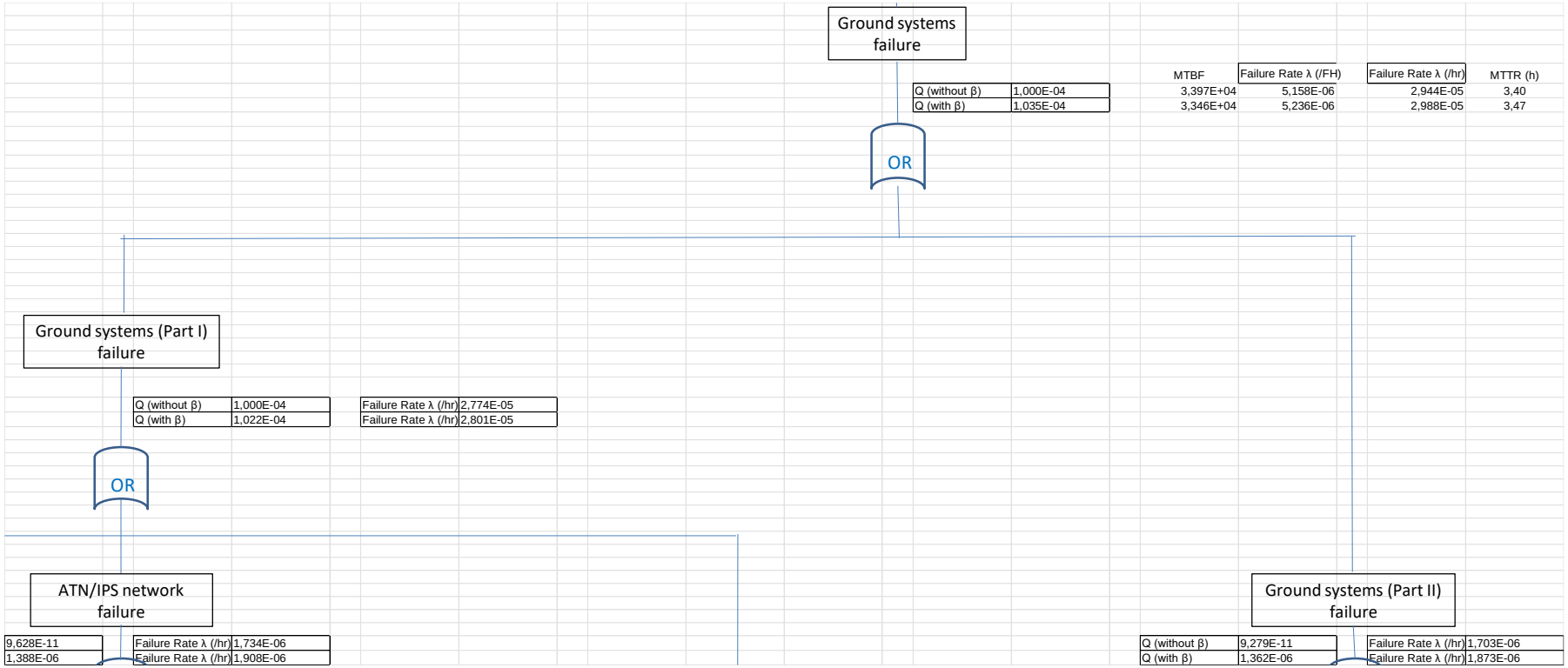


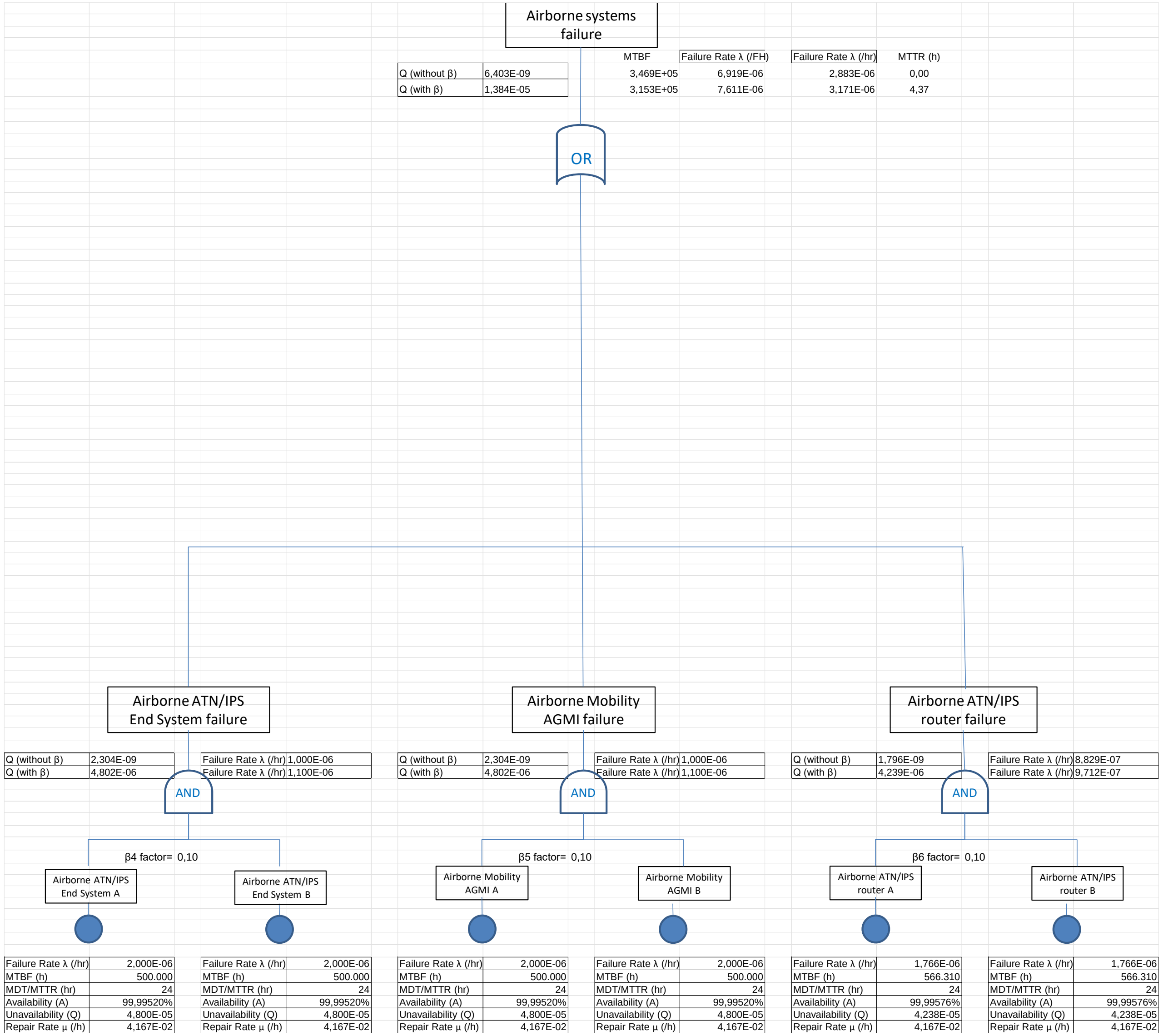

OH-DC-1 (IPS-IPS) failure
Failure Rate λ (/hr)
Failure Rate λ (/FH)
5,562E-05
1,616E-05
4,388E-05
1,471E-05
Q (without β)
2,000E-04
Q (with β)
2,160E-04
OR
Ground systems failure
Q (without β)
1,000E-04
Q (with β)
1,022E-04
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
3,605E+04
4,859E-06
2,774E-05
3,61
3,570E+04
4,907E-06
2,801E-05
3,65
Airborne systems failure
Q (without β)
6,403E-09
Q (with β)
1,384E-05
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
3,469E+05
6,919E-06
2,863E-06
0,00
3,153E+05
7,611E-06
3,171E-06
4,37
A/G access network failure
Q (without β)
1,000E-04
Q (with β)
1,000E-04
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH)
MTTR (h)
2,500E-05
4,000E+04
4,288E-06
4,00
1,250E-05
7,999E+04
2,190E-06
8,00

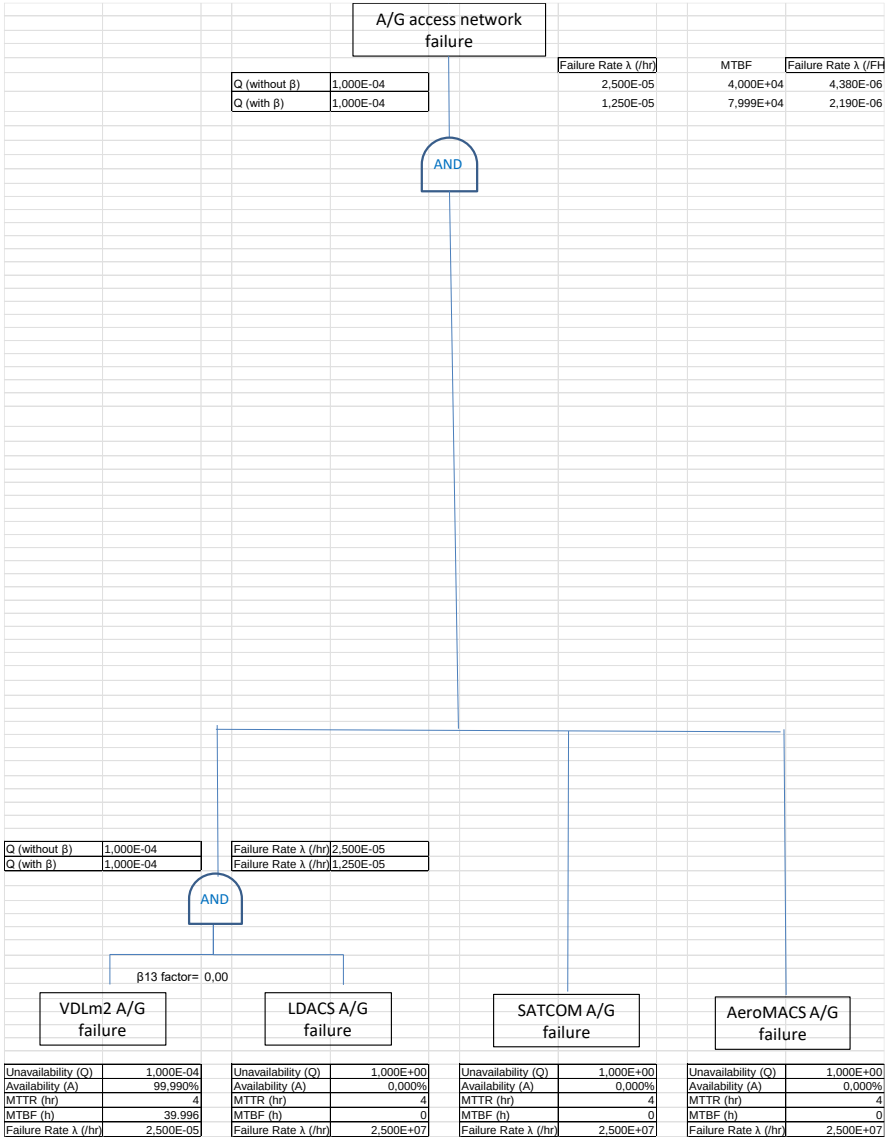
OH-DC-1b – Detected loss of CPDLC capability [single aircraft] (OSI-IPS flow):

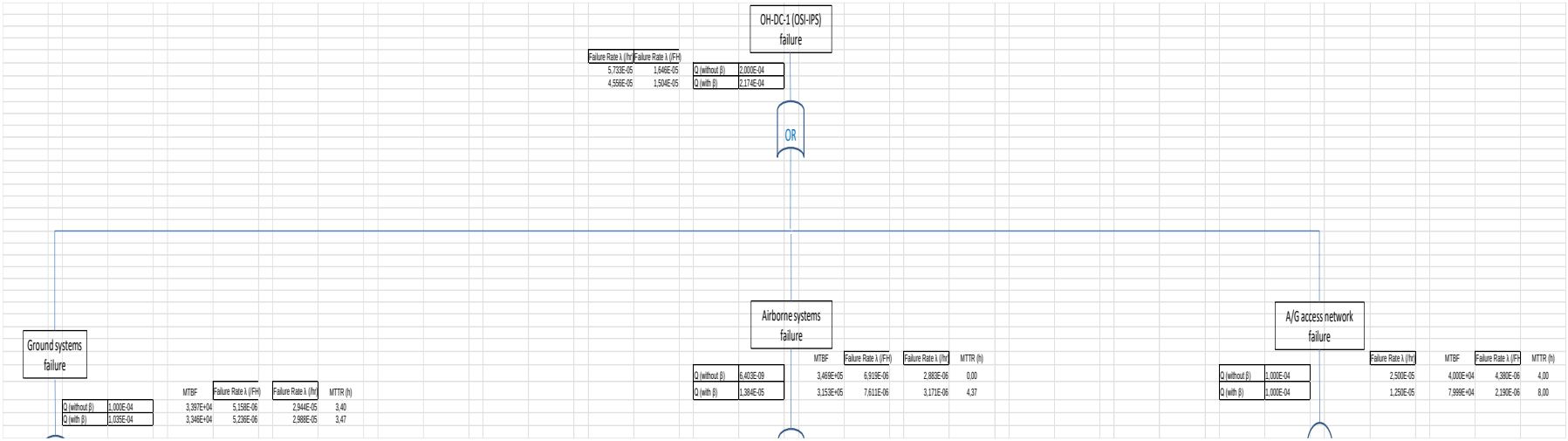



Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06
OR
G/G ATN/OSI router failure
OSI/IPS gateway failure
Q (without β) 4,639E-11
Q (with β) 6,812E-07
Failure Rate λ (/hr) 8,514E-07
Failure Rate λ (/hr) 9,366E-07
AND
β8 factor= 0,10
β9 factor= 0,10
G/G ATN/OSI router A
G/G ATN/OSI router B
OSI/IPS gateway
OSI/IPS gateway
Failure Rate λ (/hr) 1,703E-06
MTBF (h) 587.250
MDT/MTTR (hr) 4
Availability (A) 99,99932%
Unavailability (Q) 6,811E-06
Repair Rate μ (/h) 2,500E-01

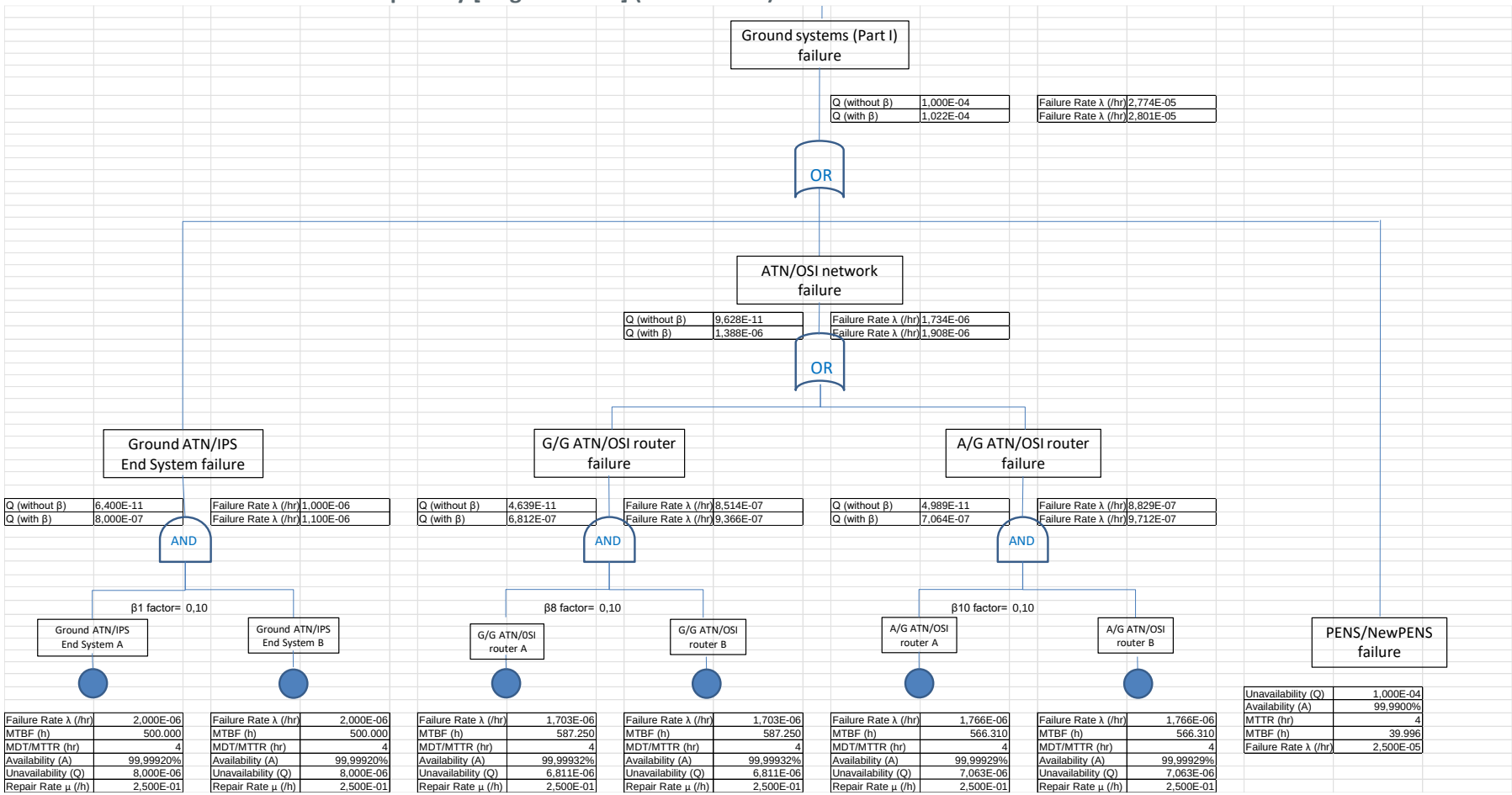

Ground systems failure
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
Q (without β) 1,000E-04 3,397E+04 5,158E-06 2,944E-05 3,40
Q (with β) 1,035E-04 3,346E+04 5,236E-06 2,988E-05 3,47
OR
Ground systems (Part I) failure
Q (without β) 1,000E-04
Q (with β) 1,022E-04
Failure Rate λ (/hr) 2,774E-05
Failure Rate λ (/hr) 2,801E-05
OR
ATN/IPS network failure
9,628E-11
1,388E-06
Failure Rate λ (/hr) 1,734E-06
Failure Rate λ (/hr) 1,908E-06
Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06

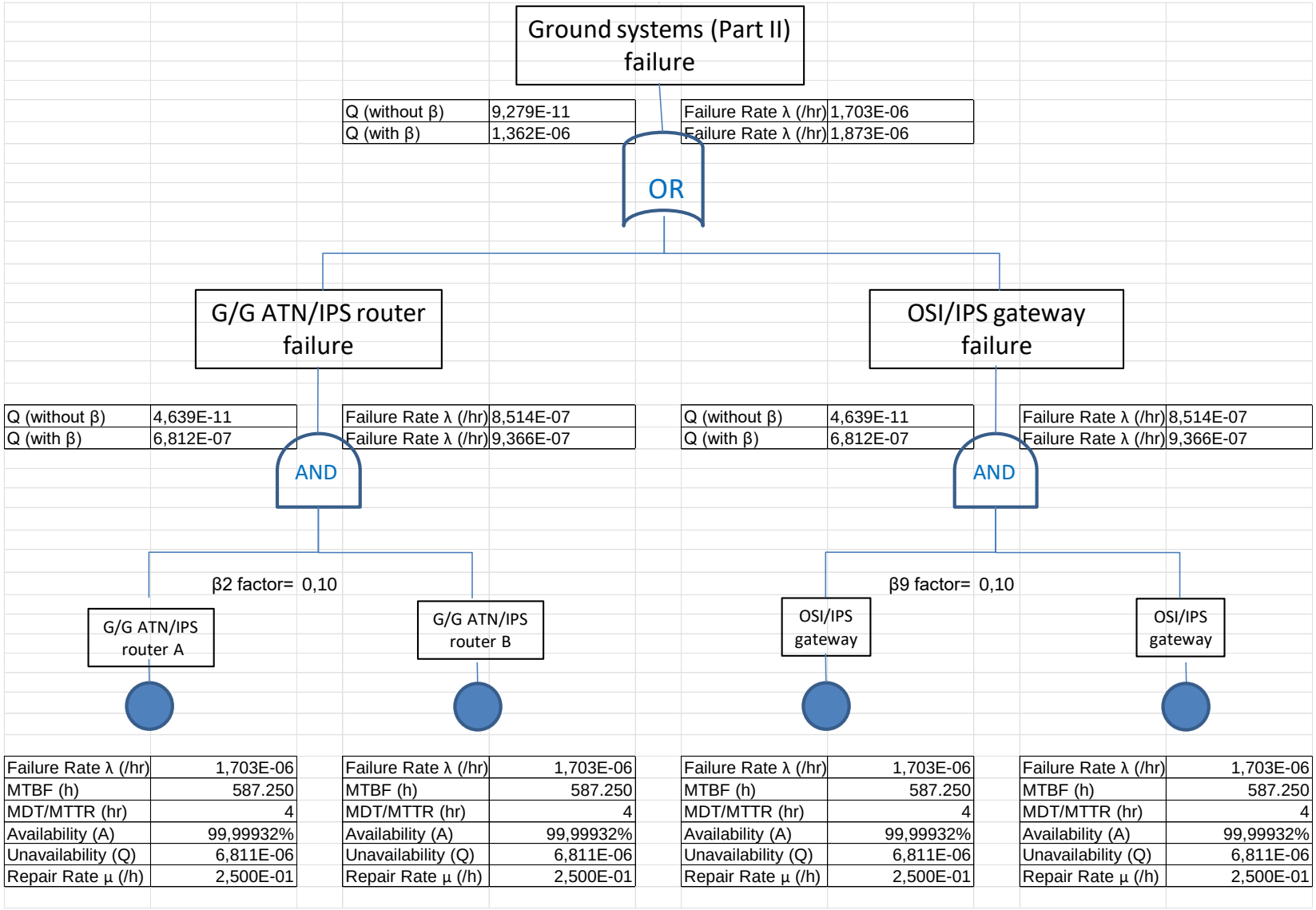


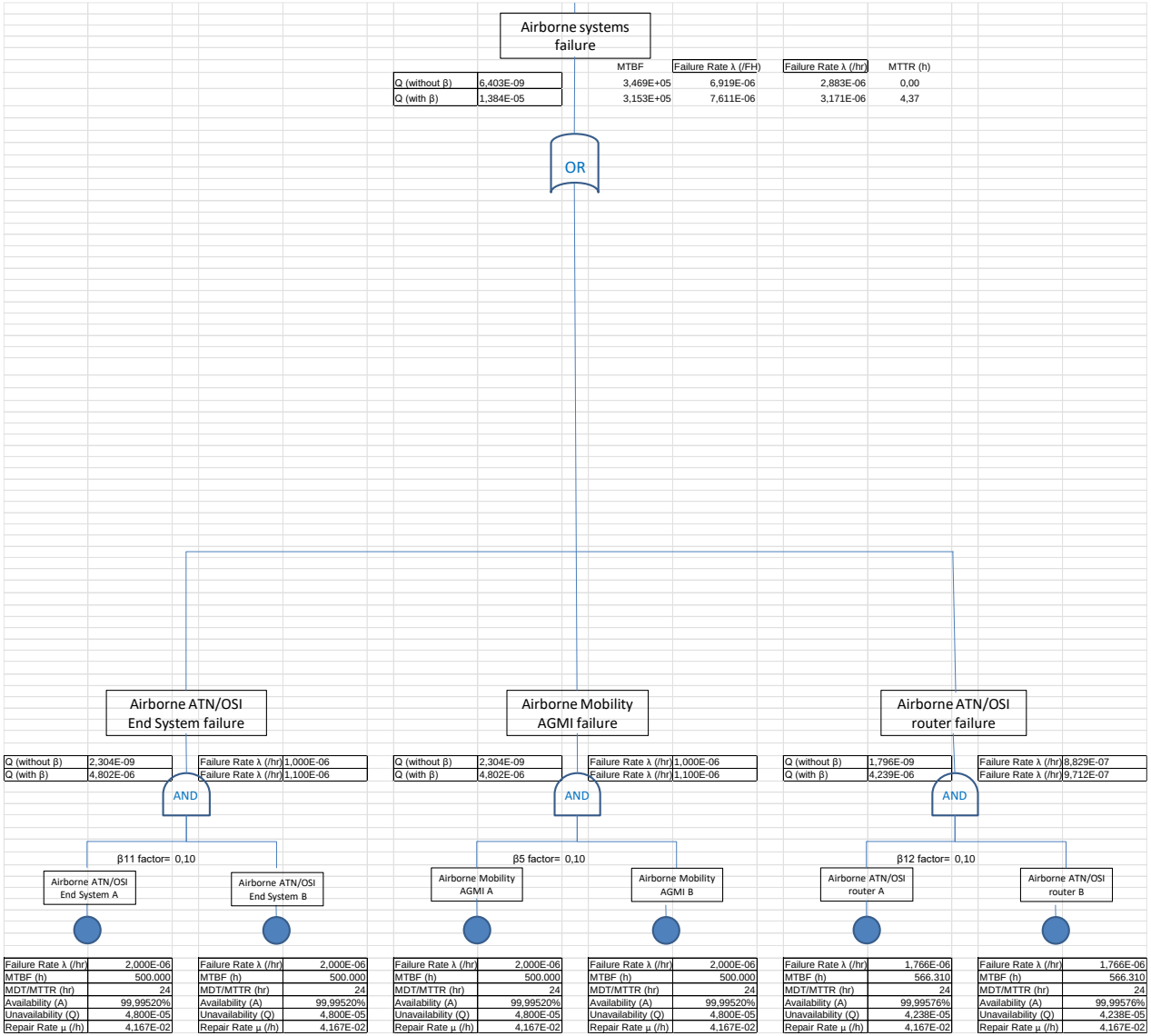

A/G access network failure
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
Q (without β) 1,000E-04
Q (with β) 1,000E-04
2,500E-05
4,000E+04
4,380E-06
1,250E-05
7,999E+04
2,190E-06
AND
Q (without β) 1,000E-04
Q (with β) 1,000E-04
Failure Rate λ (/hr) 2,500E-05
Failure Rate λ (/hr) 1,250E-05
AND
β13 factor= 0,00
VDLm2 A/G failure
LDACS A/G failure
SATCOM A/G failure
AeroMACS A/G failure
Unavailability (Q) 1,000E-04
Availability (A) 99,990%
MTTR (hr) 4
MTBF (h) 39.996
Failure Rate λ (/hr) 2,500E-05
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07

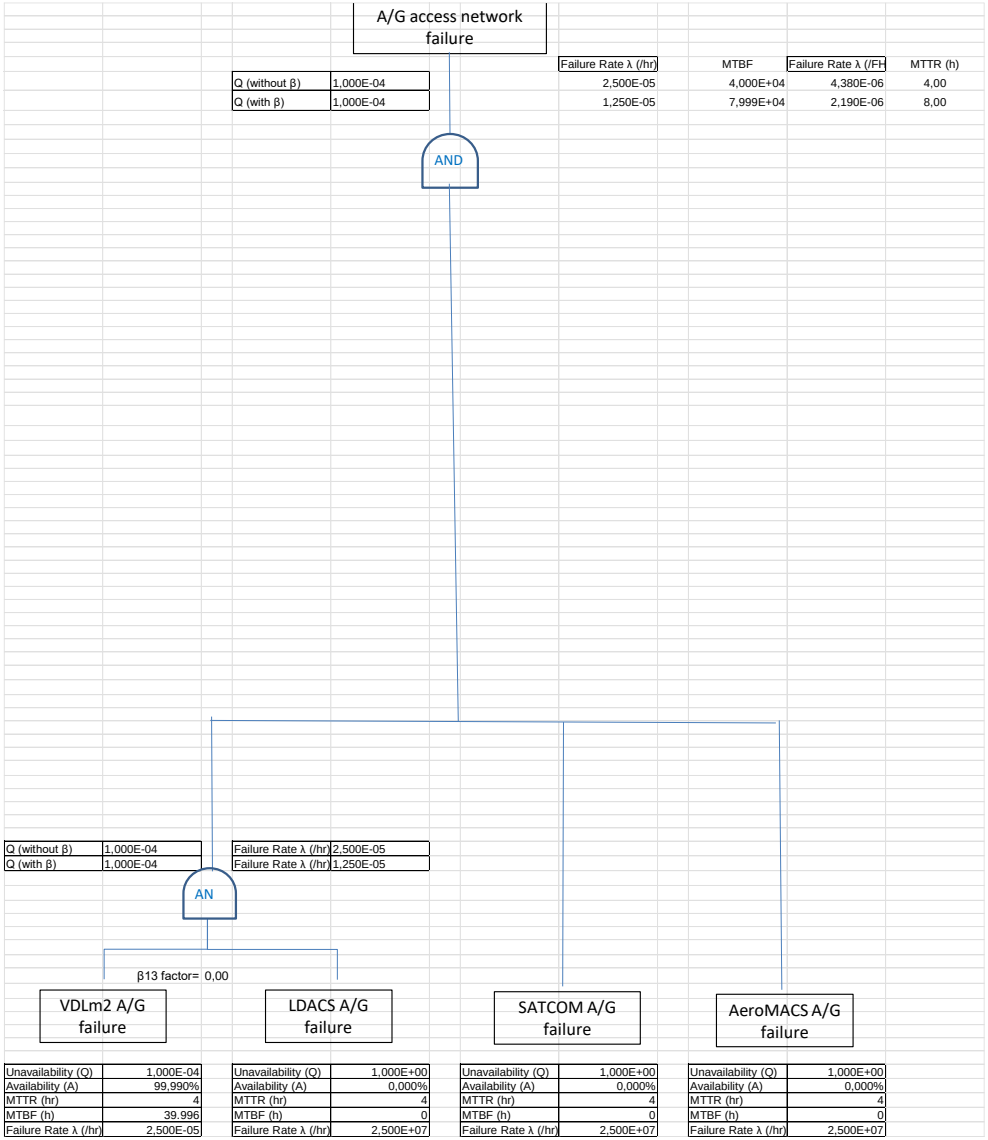

OH-DC-1 (OSI-IPS) failure
Failure Rate λ (/hr
Failure Rate λ (/FH)
5.733E-05
1.646E-05
4.556E-05
1.504E-05
Q (without β)
2.000E-04
Q (with β)
2.174E-04
OR
Ground systems failure
Airborne systems failure
A/G access network failure
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr
MTTR (h)
Q (without β)
1.000E-04
Q (with β)
1.035E-04
3.397E+04
5.158E-06
2.944E-05
3.40
3.346E+04
5.236E-06
2.988E-05
3.47
6.403E-09
3.469E+05
6.919E-06
2.883E-06
0.00
1.384E-05
3.153E+05
7.611E-06
3.171E-06
4.37
2.500E-05
4.000E+04
4.380E-06
4.00
1.250E-05
7.999E+04
2.190E-06
8.00

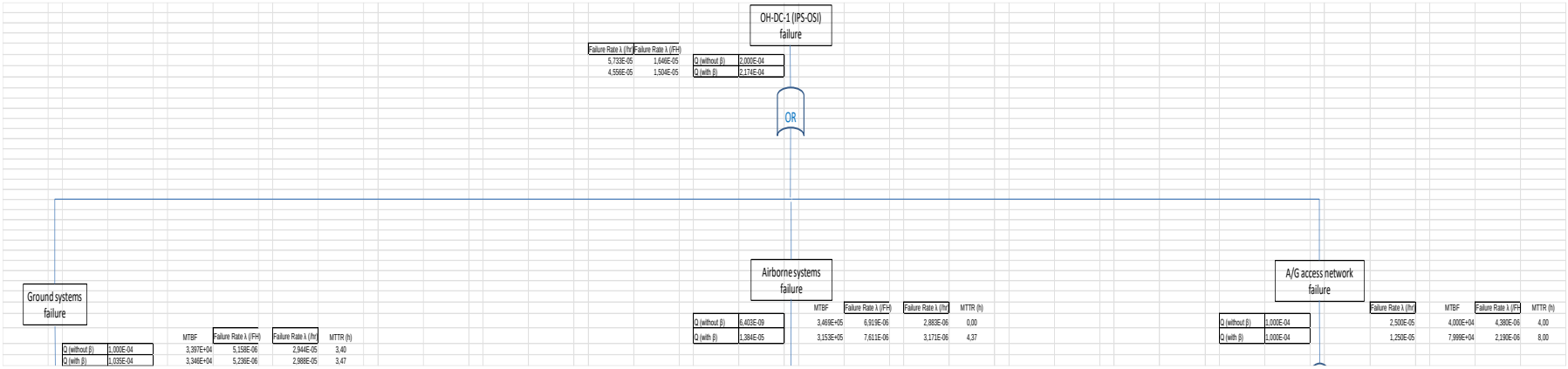
OH-DC-1c – Detected loss of CPDLC capability [single aircraft] (IPS-OSI flow):




Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06
OR
G/G ATN/IPS router failure
OSI/IPS gateway failure
Q (without β) 4,639E-11
Q (with β) 6,812E-07
Failure Rate λ (/hr) 8,514E-07
Failure Rate λ (/hr) 9,366E-07
AND
AND
β2 factor= 0,10
β9 factor= 0,10
G/G ATN/IPS router A
G/G ATN/IPS router B
OSI/IPS gateway
OSI/IPS gateway
Failure Rate λ (/hr) 1,703E-06
MTBF (h) 587.250
MDT/MTTR (hr) 4
Availability (A) 99,99932%
Unavailability (Q) 6,811E-06
Repair Rate μ (/h) 2,500E-01


Airborne systems failure
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
Q (without β) 6,403E-09 3,469E+05 6,919E-06 2,883E-06 0,00
Q (with β) 1,384E-05 3,153E+05 7,611E-06 3,171E-06 4,37
OR
Airborne ATN/OSI End System failure
Airborne Mobility AGMI failure
Airborne ATN/OSI router failure
Q (without β) 2,304E-09
Q (with β) 4,802E-06
Failure Rate λ (/hr) 1,000E-06
Failure Rate λ (/hr) 1,100E-06
Q (without β) 1,796E-09
Q (with β) 4,239E-06
Failure Rate λ (/hr) 8,829E-07
Failure Rate λ (/hr) 9,712E-07
AND
β11 factor= 0,10
β5 factor= 0,10
β12 factor= 0,10
Airborne ATN/OSI End System A
Airborne ATN/OSI End System B
Airborne Mobility AGMI A
Airborne Mobility AGMI B
Airborne ATN/OSI router A
Airborne ATN/OSI router B
Failure Rate λ (/hr) 2,000E-06
MTBF (h) 500.000
MDT/MTTR (hr) 24
Availability (A) 99,99520%
Unavailability (Q) 4,800E-05
Repair Rate μ (/h) 4,167E-02
Failure Rate λ (/hr) 1,766E-06
MTBF (h) 566.310
MDT/MTTR (hr) 24
Availability (A) 99,99576%
Unavailability (Q) 4,238E-05
Repair Rate μ (/h) 4,167E-02


A/G access network failure
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
MTTR (h)
Q (without β) 1,000E-04
Q (with β) 1,000E-04
2,500E-05
4,000E+04
4,380E-06
4,00
1,250E-05
7,999E+04
2,190E-06
8,00
AND
Q (without β) 1,000E-04
Q (with β) 1,000E-04
Failure Rate λ (/hr) 2,500E-05
Failure Rate λ (/hr) 1,250E-05
AN
β13 factor= 0,00
VDLm2 A/G failure
LDACS A/G failure
SATCOM A/G failure
AeroMACS A/G failure
Unavailability (Q) 1,000E-04
Availability (A) 99,990%
MTTR (hr) 4
MTBF (h) 39.996
Failure Rate λ (/hr) 2,500E-05
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07


OH-DC-1 (IPS-OSI) failure
Failure Rate λ (/hr)
Failure Rate λ (/FH)
5,733E-05
1,646E-05
4,556E-05
1,504E-05
Q (without β)
2.000E-04
Q (with β)
2.174E-04
OR
Ground systems failure
Airborne systems failure
A/G access network failure
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
Q (without β)
1.000E-04
Q (with β)
1.035E-04
3,397E+04
5,158E-06
2,944E-05
3,40
3,346E+04
5,236E-06
2,988E-05
3,47
6.403E-09
1.384E-05
3,469E+05
6,919E-06
2,883E-06
0,00
3,153E+05
7,611E-06
3,171E-06
4,37
1.000E-04
1.000E-04
2,500E-05
4,000E+04
4,380E-06
4,00
1,250E-05
7,999E+04
2,190E-06
8,00

6.2.6.3 Fault Tree for OH-DC-2 – Detected loss of CPDLC capability [multiple aircraft].

The fault tree corresponding to this hazard has been analysed and compiled in this section.

Three different traffic flows have been considered for this hazard:

- OH-DC-2a: Ground IPS – Airborne IPS flow.
- OH-DC-2b: Ground OSI – Airborne IPS flow.
- OH-DC-2c: Ground IPS – Airborne OSI flow.

In the proposed fault tree, it is considered that the OH-CPDLC-2a, OH-CPDLC-2b and OH-CPDLC-2c hazards may happen to one of the following basic causes:

- A combined loss of different A/G access networks (VDLm2, LDACS, SATCOM, AeroMACS), which should encompass cases of simultaneous failures on any of these A/G radio systems, leading to an ATN/IPS or ATN/OSI communication failure, for which it can be determined that datalink services should not be used anymore and that the flight crew must revert to voice communications.
- A detected or undetected loss of the Ground systems involved in the datalink communication (Ground ATN/OSI or ATN/IPS End System, G/G ATN/IPS or ATN/OSI router, A/G ATN/IPS or ATN/OSI router and NewPENS) for which it can be determined that datalink services should not be used anymore and that the flight crew must revert to voice communications.

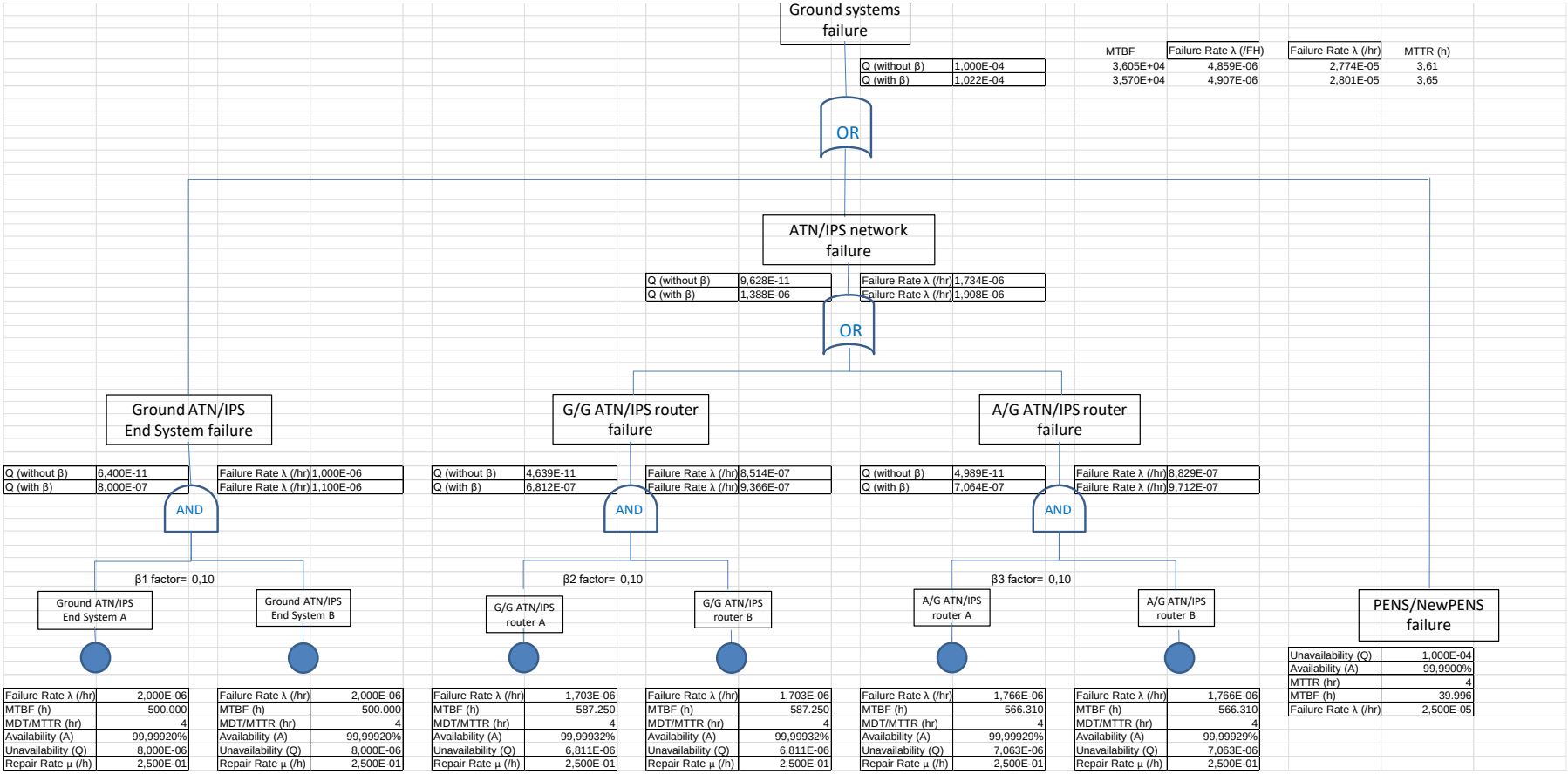
In addition to the previous basic failure causes, it is considered that for OH-CPDLC-2b and OH-CPDLC-2c hazards also apply the following basic cause:

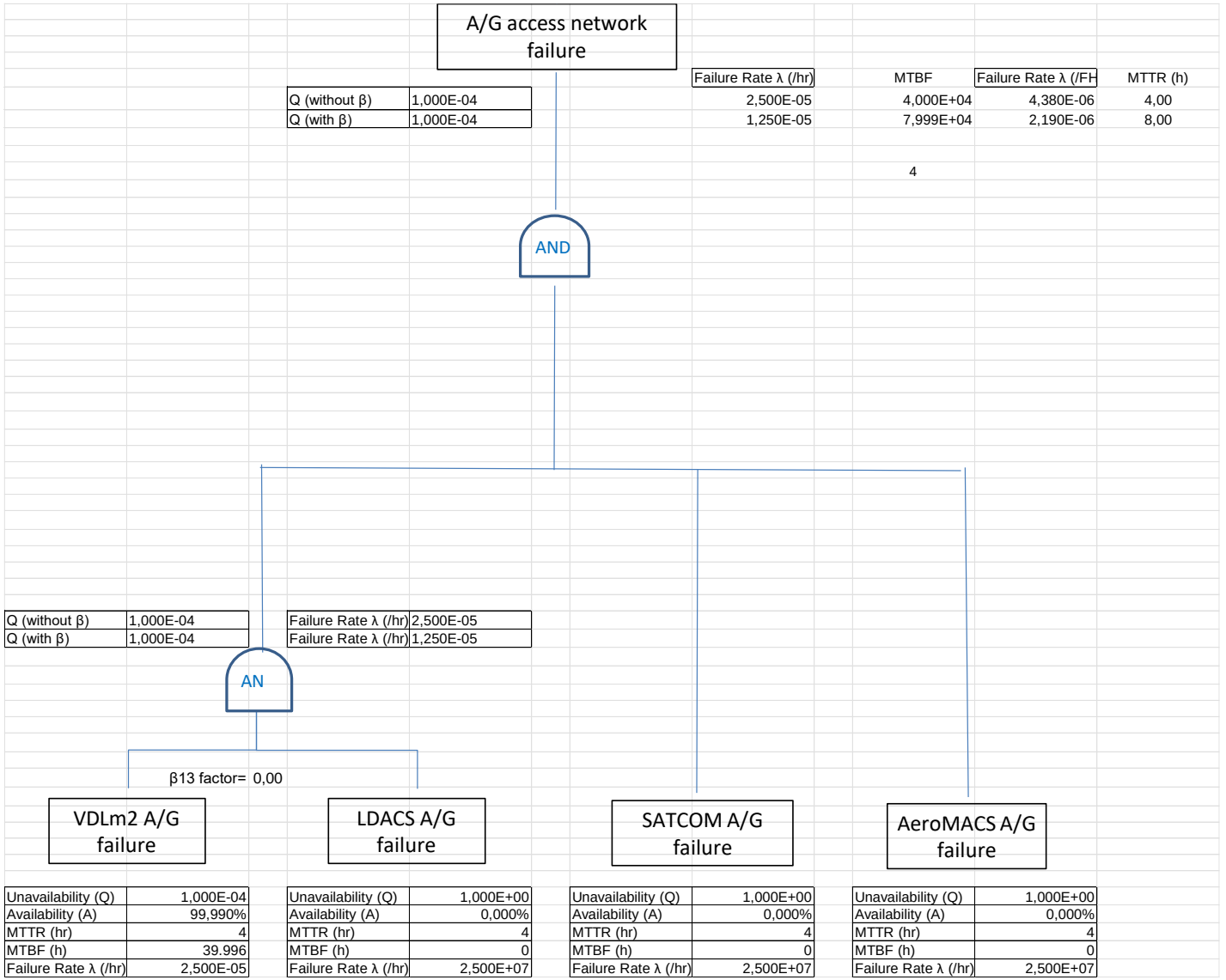
- A detected or undetected loss of the OSI/IPS gateway for which it can be determined that datalink services should not be used anymore and that the flight crew must revert to voice communications.

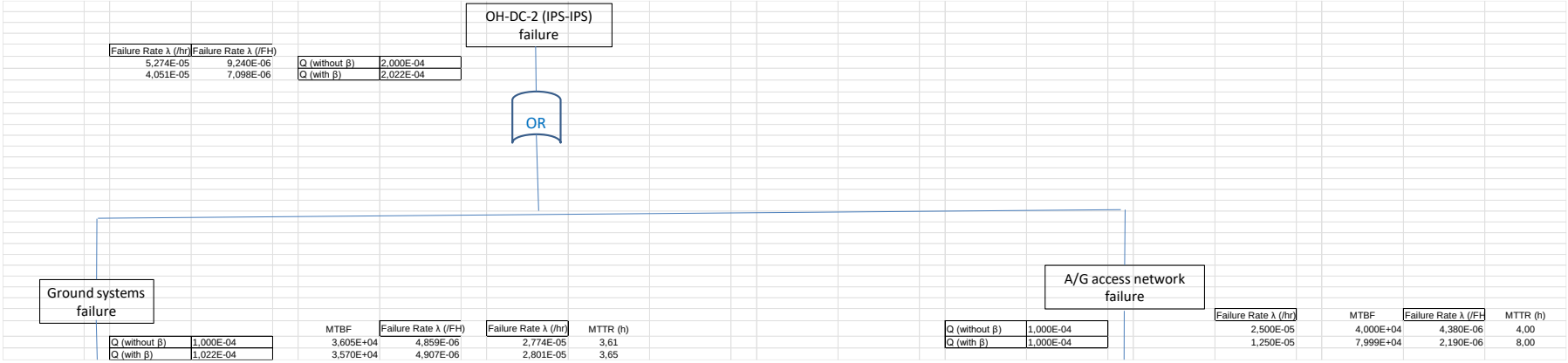
It must be highlighted that failures of any Aircraft FCI system are not considered in these hazards since they are not impacting multiple aircrafts at the same time.

The outcomes obtained after performing the RAM analysis on these OH-DC-2a, OH-DC-2b and OH-DC-2c hazards are as follows:

OH-DC-2a – Detected loss of CPDLC capability [multiple aircraft] (IPS-IPS flow):

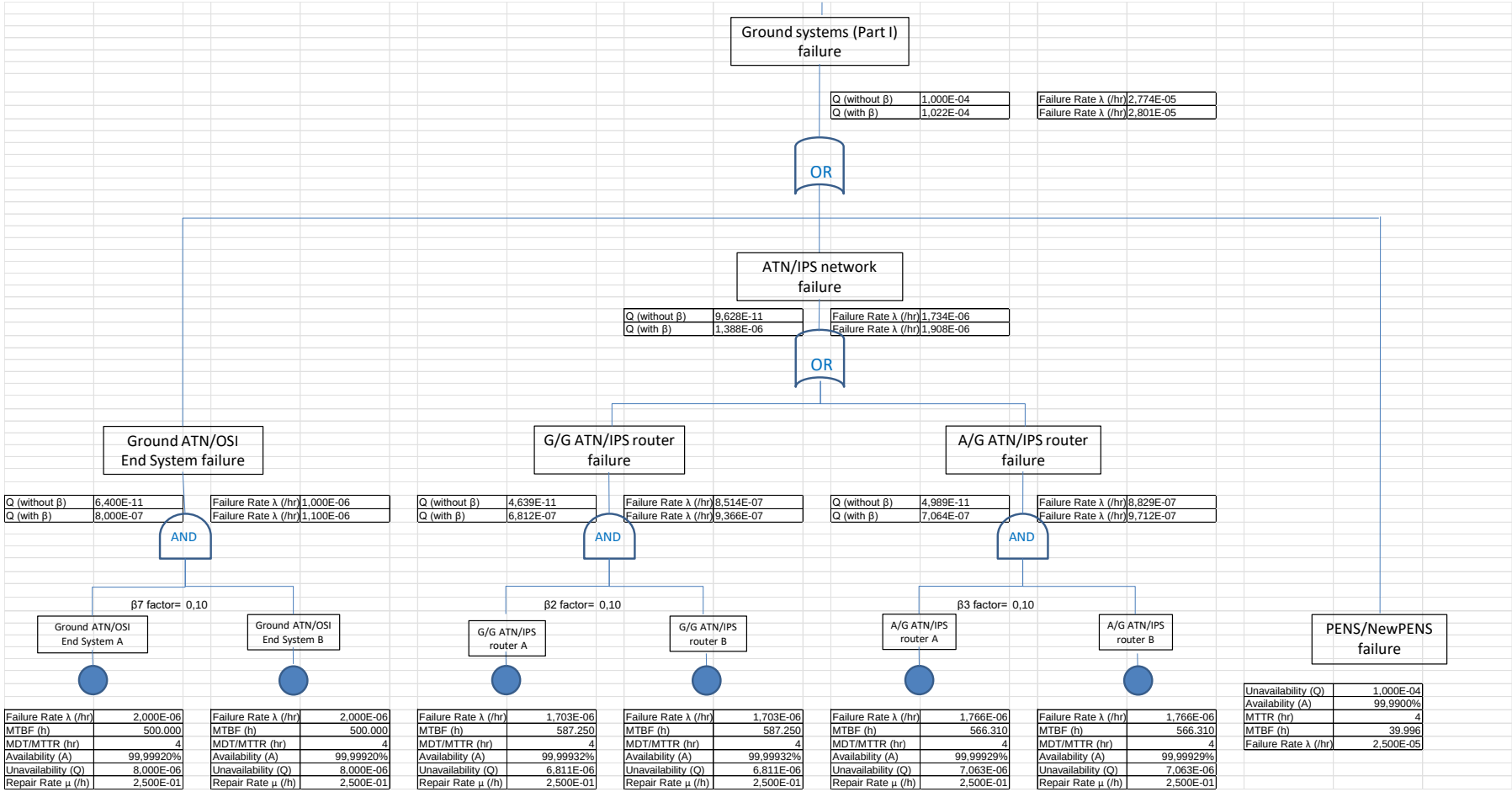


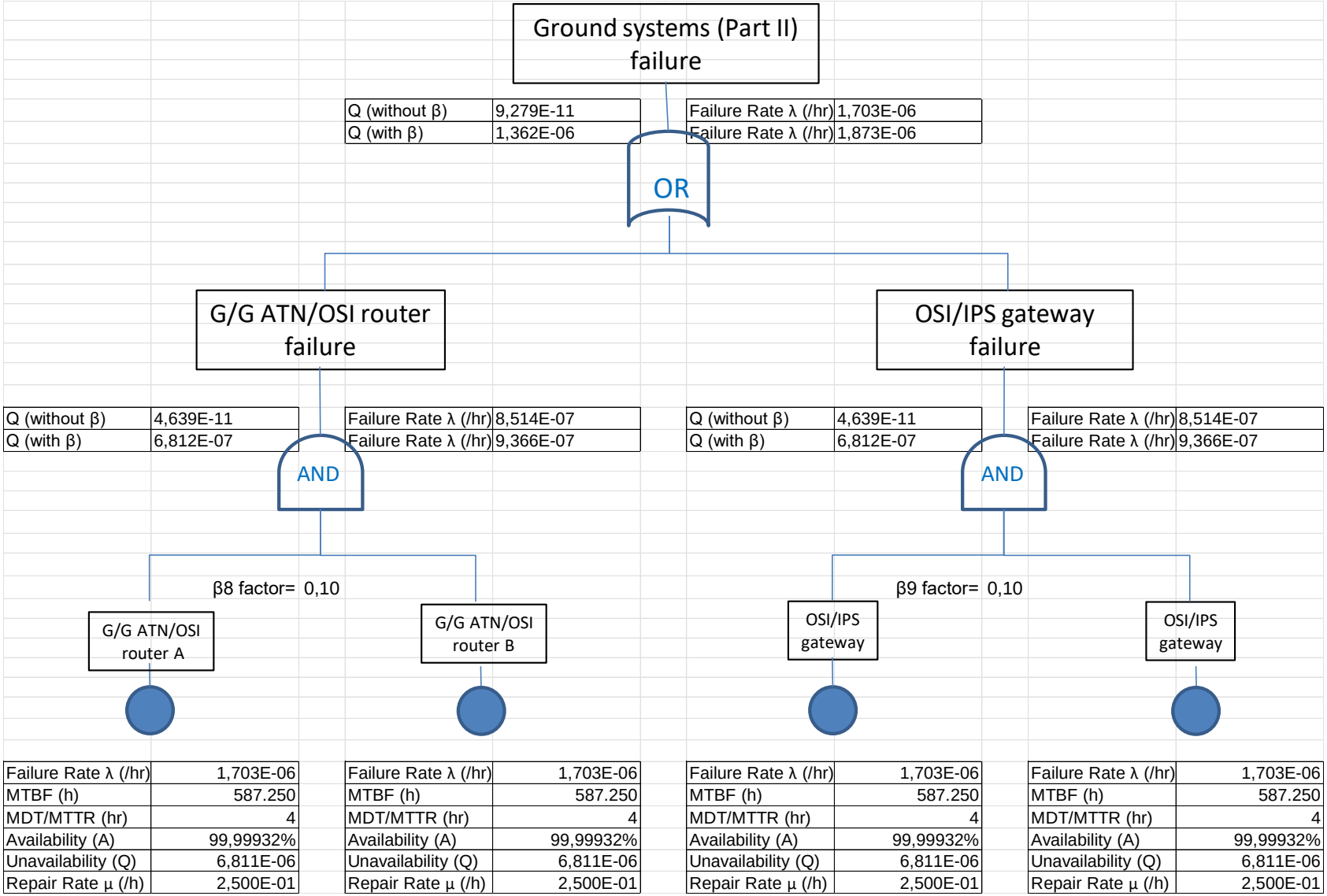

A/G access network failure
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
MTTR (h)
Q (without β) 1,000E-04
Q (with β) 1,000E-04
2,500E-05
4,000E+04
4,380E-06
4,00
1,250E-05
7,999E+04
2,190E-06
8,00
4
AND
Q (without β) 1,000E-04
Q (with β) 1,000E-04
Failure Rate λ (/hr) 2,500E-05
Failure Rate λ (/hr) 1,250E-05
AN
β13 factor= 0,00
VDLm2 A/G failure
LDACS A/G failure
SATCOM A/G failure
AeroMACS A/G failure
Unavailability (Q) 1,000E-04
Availability (A) 99,990%
MTTR (hr) 4
MTBF (h) 39.996
Failure Rate λ (/hr) 2,500E-05
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07

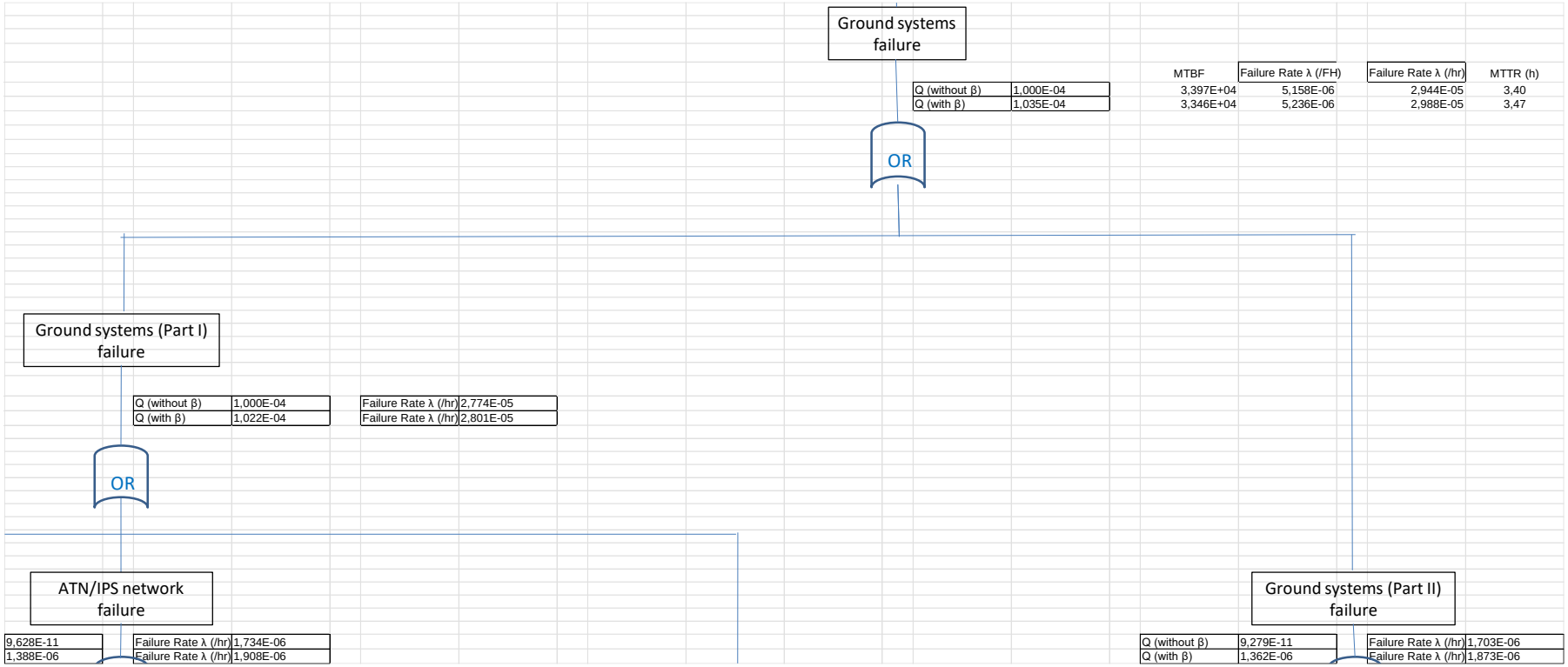


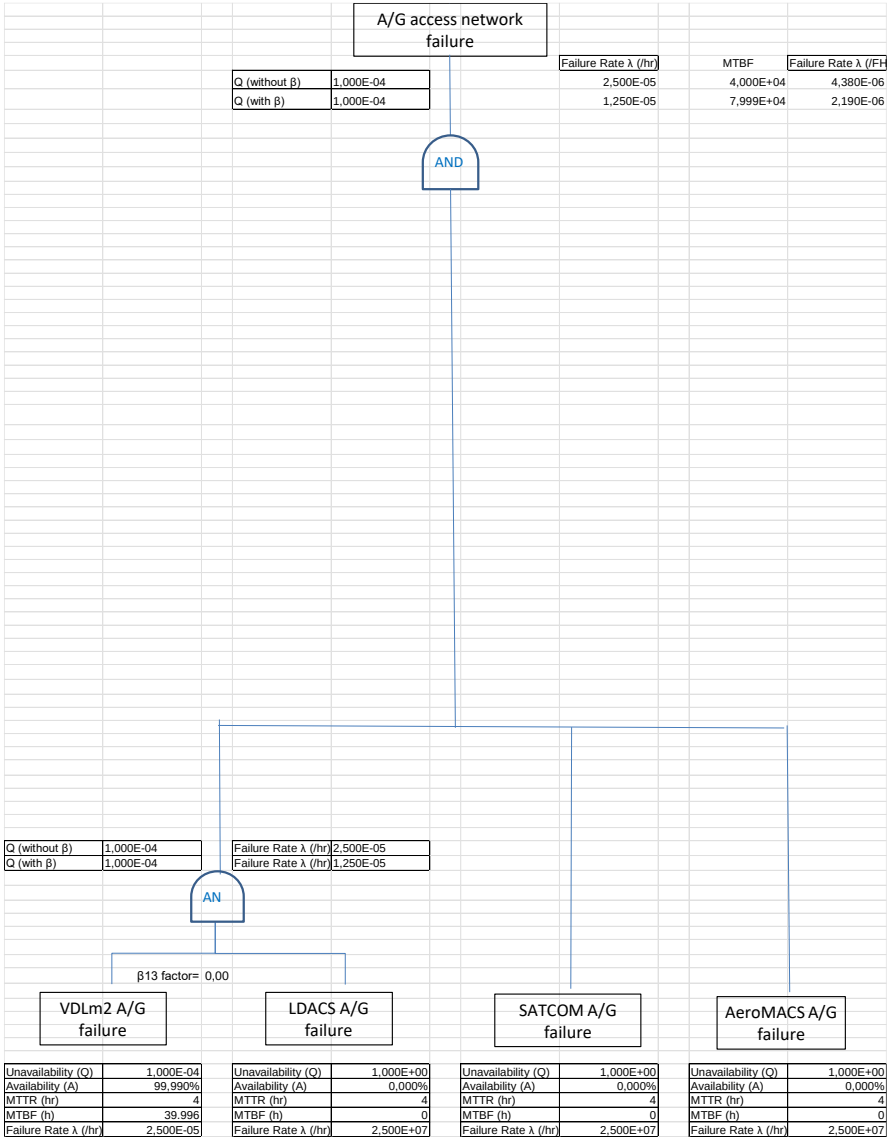
EUROPEAN PARTNERSHIP
Co-funded by the European Union

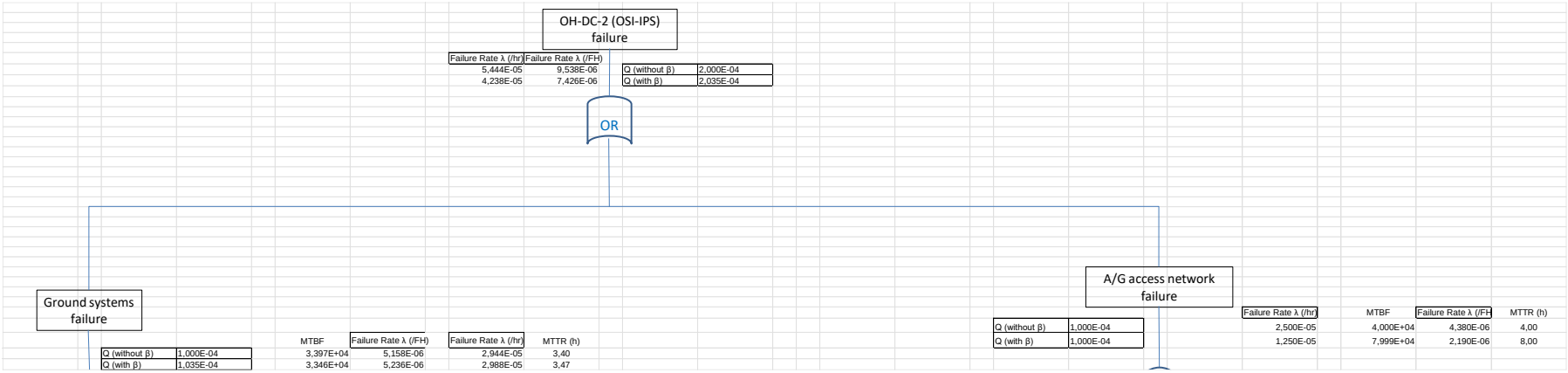
OH-DC-2b – Detected loss of CPDLC capability [multiple aircraft] (OSI-IPS flow):



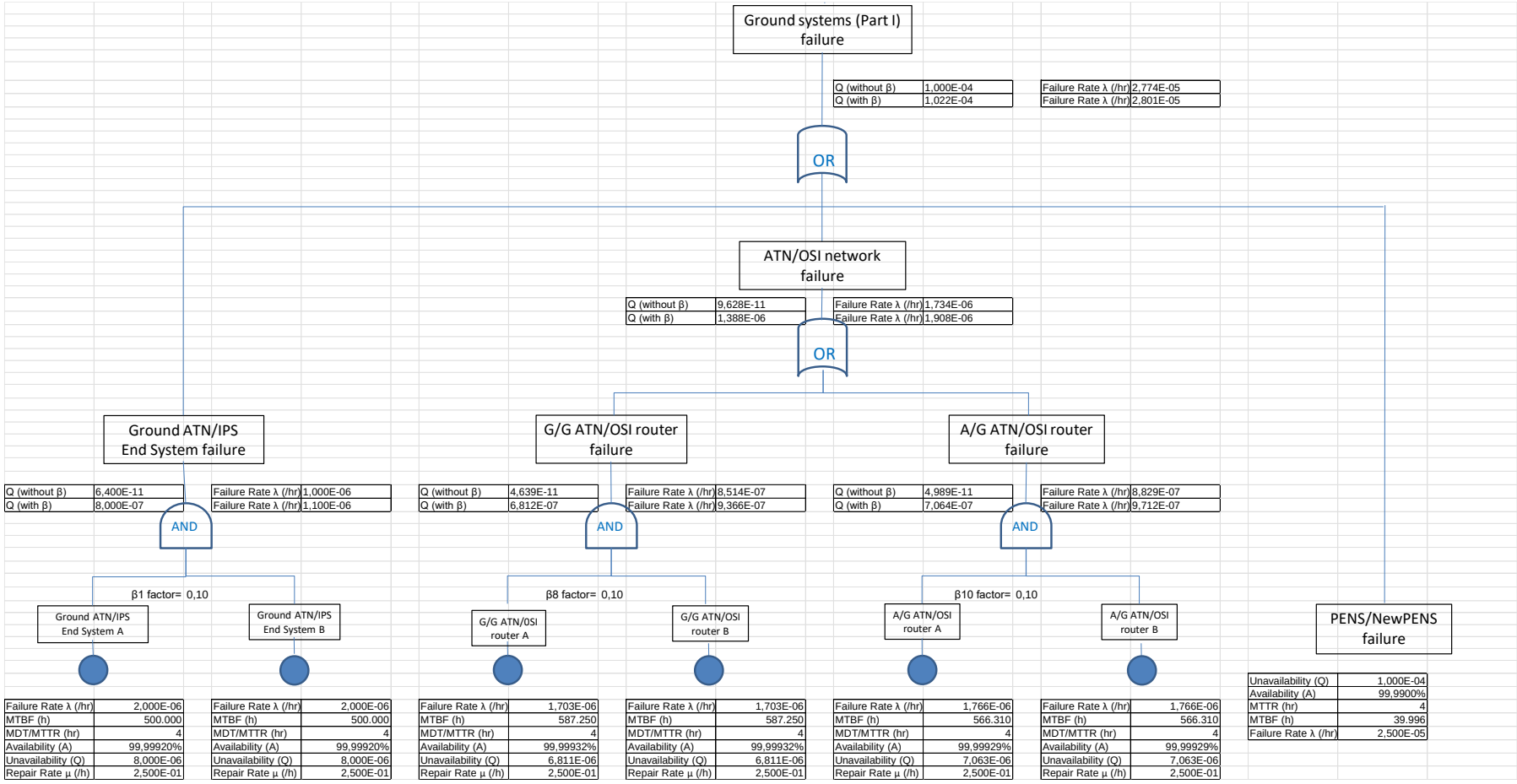

Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06
OR
G/G ATN/OSI router failure
OSI/IPS gateway failure
Q (without β) 4,639E-11
Q (with β) 6,812E-07
Failure Rate λ (/hr) 8,514E-07
Failure Rate λ (/hr) 9,366E-07
AND
β8 factor= 0,10
β9 factor= 0,10
G/G ATN/OSI router A
G/G ATN/OSI router B
OSI/IPS gateway
OSI/IPS gateway
Failure Rate λ (/hr) 1,703E-06
MTBF (h) 587.250
MDT/MTTR (hr) 4
Availability (A) 99,99932%
Unavailability (Q) 6,811E-06
Repair Rate μ (/h) 2,500E-01

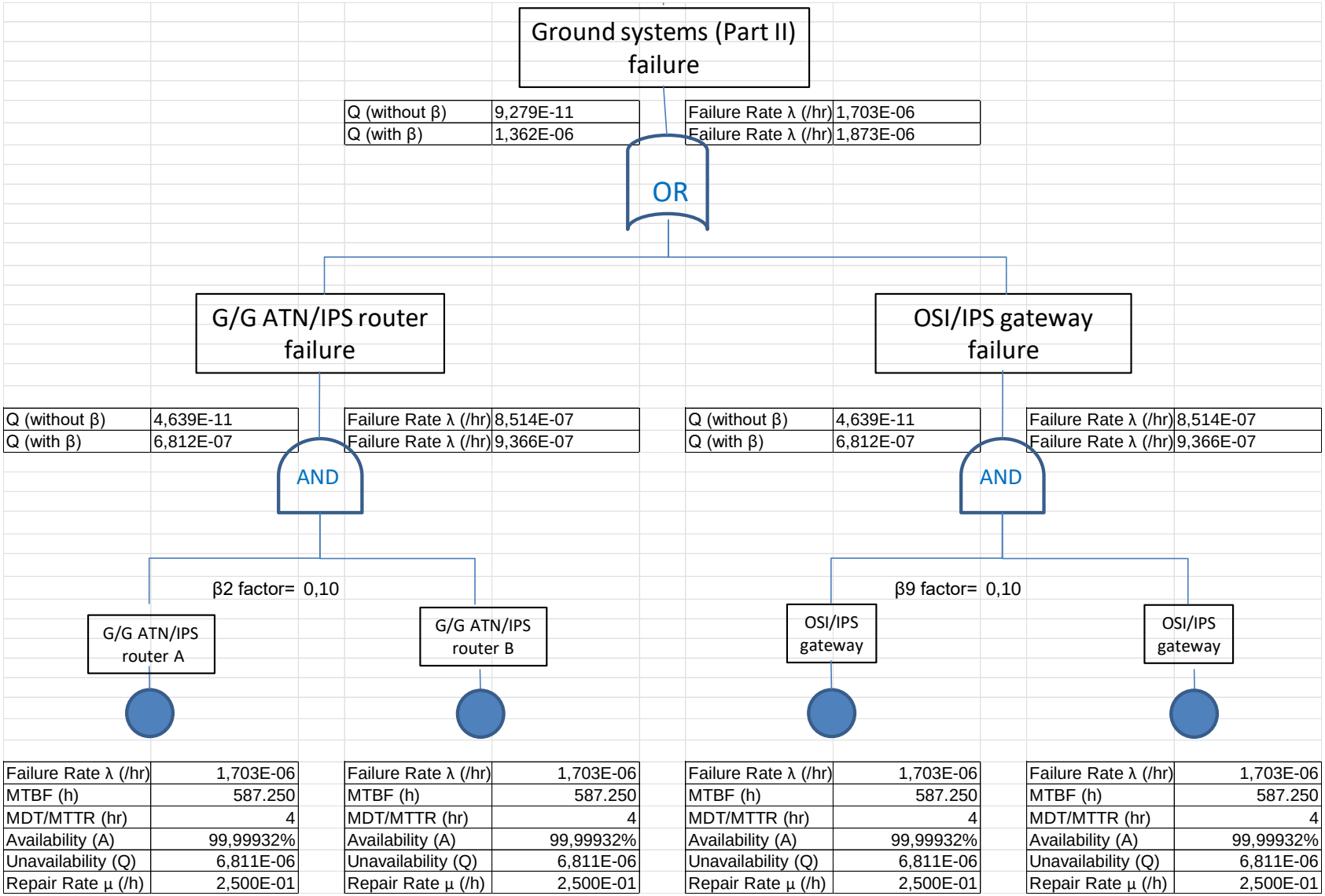

Ground systems failure
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
Q (without β) 1,000E-04 3,397E+04 5,158E-06 2,944E-05 3,40
Q (with β) 1,035E-04 3,346E+04 5,236E-06 2,988E-05 3,47
OR
Ground systems (Part I) failure
Q (without β) 1,000E-04
Q (with β) 1,022E-04
Failure Rate λ (/hr) 2,774E-05
Failure Rate λ (/hr) 2,801E-05
OR
ATN/IPS network failure
9,628E-11
1,388E-06
Failure Rate λ (/hr) 1,734E-06
Failure Rate λ (/hr) 1,908E-06
Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06

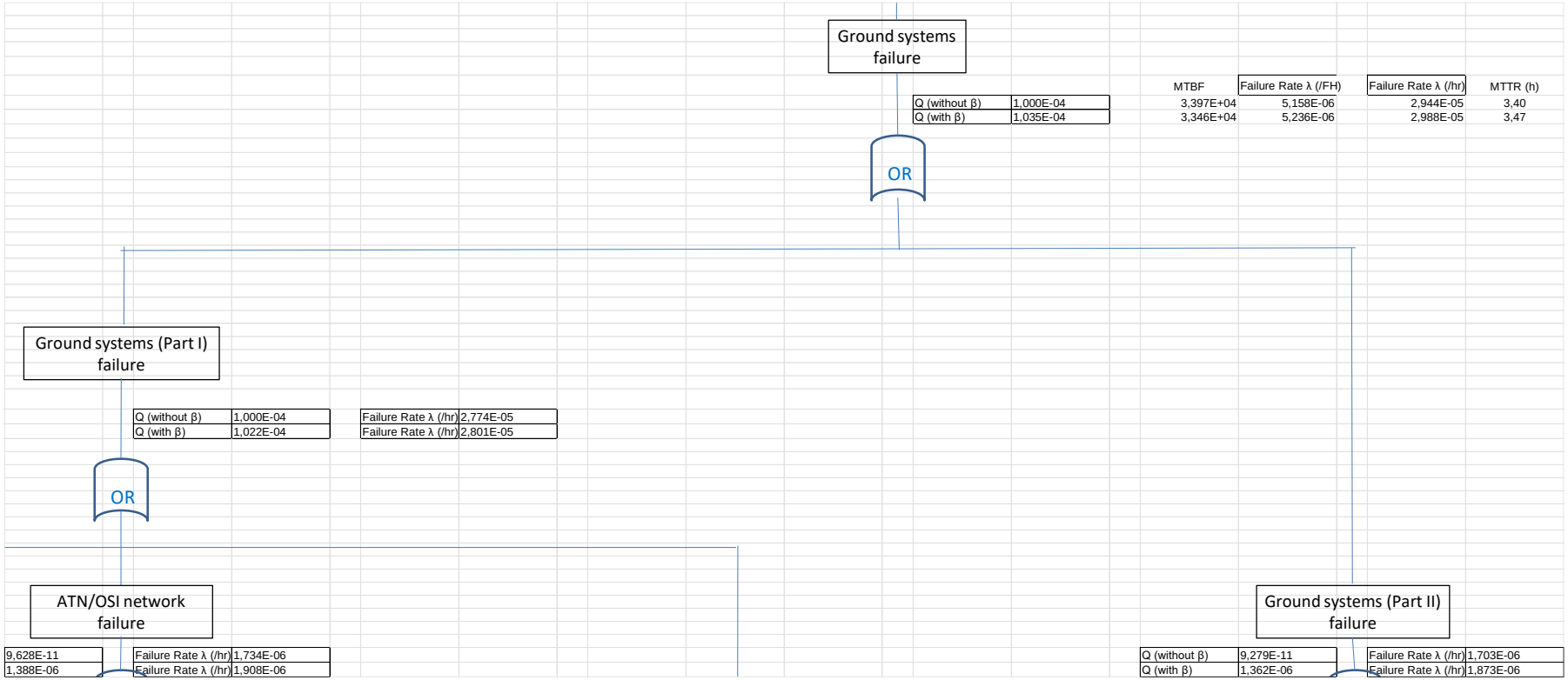

A/G access network failure
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
Q (without β) 1,000E-04
Q (with β) 1,000E-04
2,500E-05
1,250E-05
4,000E+04
7,999E+04
4,380E-06
2,190E-06
AND
Q (without β) 1,000E-04
Q (with β) 1,000E-04
Failure Rate λ (/hr) 2,500E-05
Failure Rate λ (/hr) 1,250E-05
AN
β13 factor= 0,00
VDLm2 A/G failure
LDACS A/G failure
SATCOM A/G failure
AeroMACS A/G failure
Unavailability (Q) 1,000E-04
Availability (A) 99,990%
MTTR (hr) 4
MTBF (h) 39.996
Failure Rate λ (/hr) 2,500E-05
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07

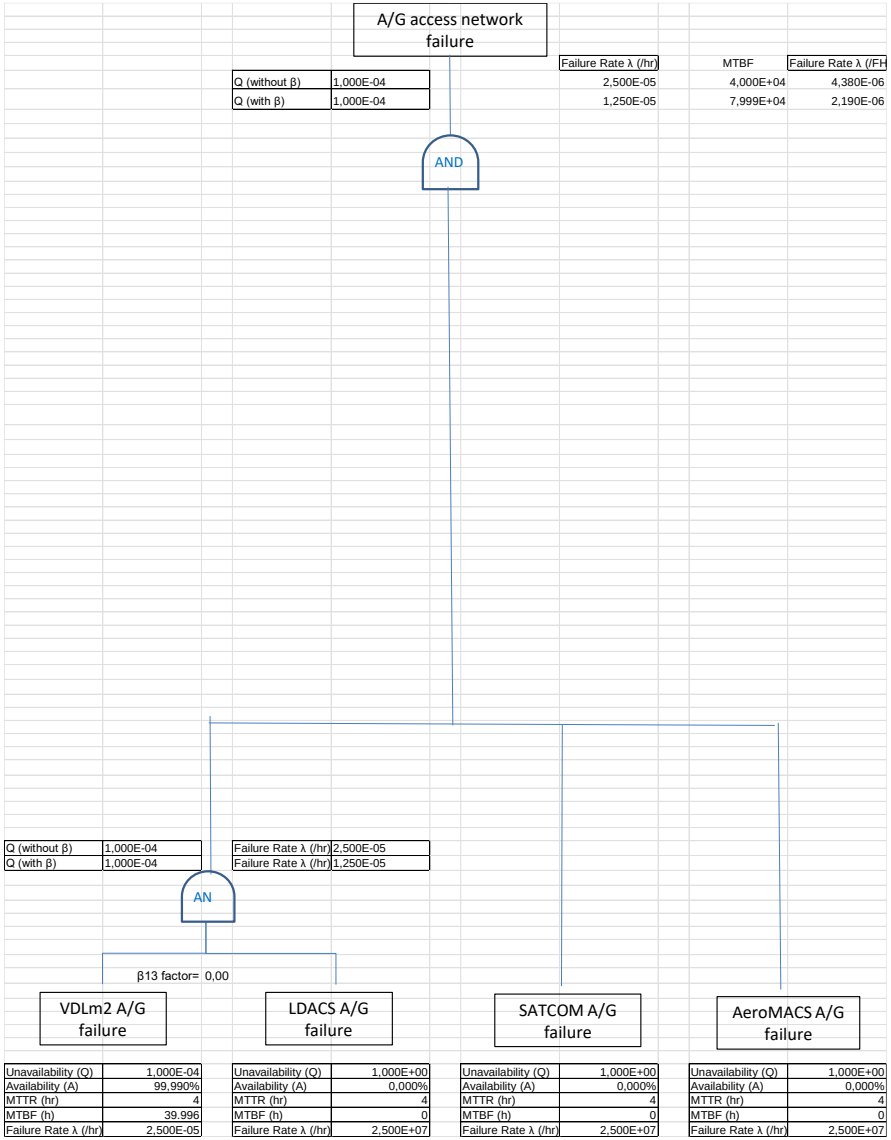

OH-DC-2 (OSI-IPS) failure
Failure Rate λ (/hr)
Failure Rate λ (/FH)
5,444E-05
9,538E-06
4,238E-05
7,426E-06
Q (without β)
2,000E-04
Q (with β)
2,035E-04
OR
Ground systems failure
Q (without β)
1,000E-04
Q (with β)
1,035E-04
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
3,397E+04
5,158E-06
2,944E-05
3,40
3,346E+04
5,236E-06
2,988E-05
3,47
A/G access network failure
Q (without β)
1,000E-04
Q (with β)
1,000E-04
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
MTTR (h)
2,500E-05
4,000E+04
4,380E-06
4,00
1,250E-05
7,999E+04
2,190E-06
8,00

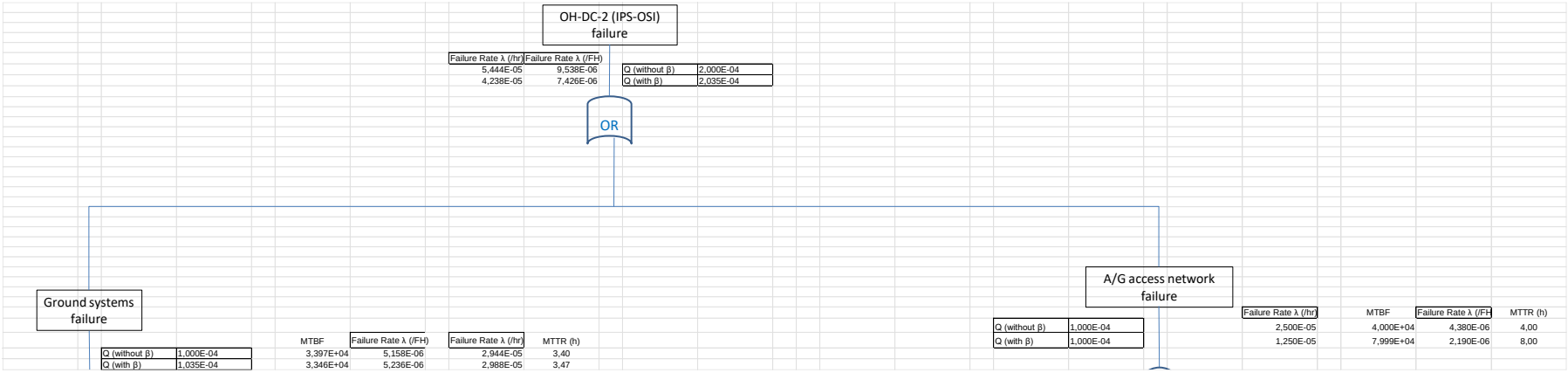
OH-DC-2c – Detected loss of CPDLC capability [multiple aircraft] (IPS-OSI flow):




Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06
OR
G/G ATN/IPS router failure
OSI/IPS gateway failure
Q (without β) 4,639E-11
Q (with β) 6,812E-07
Failure Rate λ (/hr) 8,514E-07
Failure Rate λ (/hr) 9,366E-07
AND
β2 factor= 0,10
β9 factor= 0,10
G/G ATN/IPS router A
G/G ATN/IPS router B
OSI/IPS gateway
OSI/IPS gateway
Failure Rate λ (/hr) 1,703E-06
MTBF (h) 587.250
MDT/MTTR (hr) 4
Availability (A) 99,99932%
Unavailability (Q) 6,811E-06
Repair Rate μ (/h) 2,500E-01


Ground systems failure
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
Q (without β) 1,000E-04 3,397E+04 5,158E-06 2,944E-05 3,40
Q (with β) 1,035E-04 3,346E+04 5,236E-06 2,988E-05 3,47
OR
Ground systems (Part I) failure
Q (without β) 1,000E-04
Q (with β) 1,022E-04
Failure Rate λ (/hr) 2,774E-05
Failure Rate λ (/hr) 2,801E-05
OR
ATN/OSI network failure
9,628E-11
1,388E-06
Failure Rate λ (/hr) 1,734E-06
Failure Rate λ (/hr) 1,908E-06
Ground systems (Part II) failure
Q (without β) 9,279E-11
Q (with β) 1,362E-06
Failure Rate λ (/hr) 1,703E-06
Failure Rate λ (/hr) 1,873E-06


A/G access network failure
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
Q (without β) 1,000E-04
Q (with β) 1,000E-04
2,500E-05
1,250E-05
4,000E+04
7,999E+04
4,380E-06
2,190E-06
AND
Q (without β) 1,000E-04
Q (with β) 1,000E-04
Failure Rate λ (/hr) 2,500E-05
Failure Rate λ (/hr) 1,250E-05
AN
β13 factor= 0,00
VDLm2 A/G failure
LDACS A/G failure
SATCOM A/G failure
AeroMACS A/G failure
Unavailability (Q) 1,000E-04
Availability (A) 99,990%
MTTR (hr) 4
MTBF (h) 39.996
Failure Rate λ (/hr) 2,500E-05
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07
Unavailability (Q) 1,000E+00
Availability (A) 0,000%
MTTR (hr) 4
MTBF (h) 0
Failure Rate λ (/hr) 2,500E+07


OH-DC-2 (IPS-OSI) failure
Failure Rate λ (/hr)
Failure Rate λ (/FH)
5,444E-05
9,538E-06
4,238E-05
7,426E-06
Q (without β)
2,000E-04
Q (with β)
2,035E-04
OR
Ground systems failure
Q (without β)
1,000E-04
Q (with β)
1,035E-04
MTBF
Failure Rate λ (/FH)
Failure Rate λ (/hr)
MTTR (h)
3,397E+04
5,158E-06
2,944E-05
3,40
3,346E+04
5,236E-06
2,988E-05
3,47
A/G access network failure
Q (without β)
1,000E-04
Q (with β)
1,000E-04
Failure Rate λ (/hr)
MTBF
Failure Rate λ (/FH
MTTR (h)
2,500E-05
4,000E+04
4,380E-06
4,00
1,250E-05
7,999E+04
2,190E-06
8,00

6.2.6.4 Fault Tree for OH-DC-7 – Unexpected interruption of a data link transaction [single aircraft].

The fault tree corresponding to this hazard has been analysed and compiled in this section.

Three different traffic flows have been considered for this hazard:

- OH-DC-7a: Ground IPS – Airborne IPS flow.
- OH-DC-7b: Ground OSI – Airborne IPS flow.
- OH-DC-7c: Ground IPS – Airborne OSI flow.

When further reviewing OH-DC-7 compared to OH-DC-1, it is considered that OH-DC-7 materializes when OH-DC-1 materializes or when, even if multiple access networks are available and one subnetwork fails, the failover to another subnetwork takes too much time and creates an interruption of a datalink transaction because of some time-outs, even if the second subnetwork datalink capability is available. But this scenario can only happen if there is a software failure (such as a routing failure) which would need to be subject to a SWAL analysis and therefore is out of scope of the study. This means that OH-DC-7 will provide same results than OH-DC-1.

6.2.6.5 Fault Tree for OH-DC-8 – Unexpected interruption of a data link transaction [multiple aircraft].

The fault tree corresponding to this hazard has been analysed and compiled in this section.

Three different traffic flows have been considered for this hazard:

- OH-DC-8a: Ground IPS – Airborne IPS flow.
- OH-DC-8b: Ground OSI – Airborne IPS flow.
- OH-DC-8c: Ground IPS – Airborne OSI flow.

When further reviewing OH-DC-8 compared to OH-DC-2, it is considered that OH-DC-8 materializes when OH-DC-2 materializes or when, even if multiple access networks are available and one subnetwork fails, the failover to another subnetwork takes too much time and creates an interruption of a datalink transaction because of some time-outs, even if the second subnetwork datalink capability is available. But this scenario can only happen if there is a software failure (such as a routing failure) which would need to be subject to a SWAL analysis and therefore is out of scope of the study. This means that OH-DC-8 will provide same results than OH-DC-8.

6.2.6.6 Summary of initial FCI RAM analysis outcomes.

A summary of the RAM analysis outcomes obtained for all the hazards considered for the FCI systems is summarized as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

The figure above confirms that all FCI system safety objectives are met with the initial assumptions identified in section 6..2.6.1.

6.2.7 ASSESSMENT ON RAM ANALYSIS (SENSITIVITY ANALYSIS).

The initial RAM analysis outcomes summarized in the section above shows that all safety objectives identified in the FHA analysis are met successfully by the FCI solution.

In this chapter, the influence of the following parameters will be analysed in the FCI RAM analysis outcomes:

- NewPENS/national network availability (SLA).
- FCI Airborne systems redundancy considering interdependency β factors.
- FCI Ground systems redundancy considering interdependency β factors.
- FCI A/G access networks availability and potential interdependency β factors.
- FCI G/G ASOI-IPS gateway availability and potential interdependency β factors.
- OSI/Gateway sensitivity analysis.

6.2.7.1 Influence of NewPENS availability.

Currently, NewPENS Service Provider is offering a set of services that are structured and documented in the NewPENS Service Catalogue.

Nowadays, NewPENS is providing IP transport network services using the concept of a single core, which is to say, the NewPENS Service Provider is using the infrastructure of a single Telco to offer the NewPENS communications services.

Regarding NewPENS access infrastructure redundancy, three main approaches are normally contracted by the NewPENS users:

Access infrastructure redundancy	Network Core	Indicative Availability Level
Scenario 1: One site, single connection	Single	99,5 %
Scenario 2: One site, dual connection	Single	99,99%
Scenario 3: Two sites, dual connection per site	Single	99,995 %

Most ANSPs implemented NewPENS scenarios 2 and 3.

NewPENS project is working on the deployment of a future dual core solution with a potential availability of 99,999%. It is however not clear when this approach would be available.

The results of these simulations are shown as follows:

Scenario 1: One site, single connection. NewPENS availability: 99,5%.

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		2,30E-04	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		2,31E-04	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		2,31E-04	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		2,23E-04	FAIL
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		2,23E-04	FAIL
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		2,23E-04	FAIL
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		2,30E-04	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		2,31E-04	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		2,31E-04	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		2,23E-04	FAIL
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		2,23E-04	FAIL
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		2,23E-04	FAIL

FCI safety objectives of both OH-DC 2 (Loss of data link capability [multiple aircraft]) and OH-DC 8 (Unexpected interruption of data link transactions [multiple aircraft]) hazards are not met.

Scenario 2: One site, dual connection. NewPENS availability: 99,99%.

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

All FCI safety objectives are met.

Scenario 3: Two sites, dual connection per site. NewPENS availability: 99,995%.

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,08E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,11E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,11E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		3,16E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		3,48E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		3,48E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,08E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,11E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,11E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		3,16E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		3,48E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		3,48E-06	PASS

All FCI safety objectives are met having much more margin than scenario 2.

A summary of these simulations' outcomes are shown as follows:

Simulation	Effect
Scenario 1: One site, single connection. NewPENS Availability: 99,5%.	OH-DC 2 and OH-DC 8 safety objectives are not met
Scenario 2: One site, dual connection. NewPENS Availability: 99,99%.	All FCI safety objectives are met. OH-DC 2 and OH-DC 8 RAM outcome is 7,43E-06 < 8,00E-06.
Scenario 3: Two sites, dual connection per site. NewPENS Availability: 99,995%.	All FCI safety objectives are met. OH-DC 2 and OH-DC 8 RAM outcome is 3,48E-06 < 8,00E-06.

Looking at the simulations above, it can be concluded that the minimum NewPENS availability to assure that ATS-B2 datalink services can be deployed operational meeting all the safety objectives is 99,99% (One site, dual connection), that corresponds to have a dual connection to NewPENS in at least one site.

It is also highlighted the huge influence of the NewPENS availability in the final RAM analysis outcomes. This leads to the conclusion to recommend the implementation of two sites, dual connection per site, to have a NewPENS availability of 99,995%.

6.2.7.2 Influence of FCI Airborne systems redundancy considering interdependency β factors.

Interdependency β factors affecting to airborne FCI equipment are:

- β4 factor between Airborne ATN/IPS End systems: it is measuring the interdependency between two devices of the same model providing redundancy.
- β5 factor between Airborne Mobility (AGMI): it is measuring the interdependency between two devices of the same model providing redundancy.
- β6 factor between Airborne ATN/IPS routers: it is measuring the interdependency between two devices of the same model providing redundancy.
- β11 factor between Airborne ATN/OSI End systems: it is measuring the interdependency between two devices of the same model providing redundancy.
- β12 factor between Airborne ATN/OSI routers: it is measuring the interdependency between two devices of the same model providing redundancy.
-

An initial value of β4 = β5 = β6 = β11 = β12 = 10% has been used by default in reliability calculations for FCI datalink elements during RAM analysis.

This section is going to analyse the influence of airborne β factors to identify if redundant airborne equipment is required to meet the FCI safety objectives.

For this purpose, two scenarios are going to be considered:

Access infrastructure redundancy	Beta factor value
Scenario 1: FCI Airborne redundant equipment	β4 = β5 = β6 = β11 = β12 = 0,1 (interdependency 10%)
Scenario 2: FCI Airborne single equipment	β4 = β5 = β6 = β11 = β12 = 1 (interdependency 100%)

The results of these simulations are shown as follows:

Scenario 1: FCI Airborne redundant equipment. β4 = β5 = β6 = β11 = β12 = 0,1 (interdependency 10%)

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

All FCI safety objectives are met.

Scenario 2: FCI Airborne single equipment. β4 = β5 = β6 = β11 = β12 = 1 (interdependency 100%)

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		2,09E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		2,13E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		2,13E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		2,09E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		2,13E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		2,13E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

All FCI safety objectives are met.

A summary of these simulations' outcomes are shown as follows:

Simulation	Effect
Scenario 1: FCI Airborne redundant equipment. $\beta 4 = \beta 5 = \beta 6 = \beta 11 = \beta 12 = 0,1$ (interdependency 10%)	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,50E-05 < 8,00E-04. OH-DC-2c and OH-DC-8c RAM outcome is 7,43E-06 < 8,00E-06.
Scenario 2: FCI Airborne single equipment. $\beta 4 = \beta 5 = \beta 6 = \beta 11 = \beta 12 = 1$ (interdependency 100%)	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 2,13E-05 < 8,00E-04. OH-DC-2c and OH-DC-8c RAM outcome is 7,10E-06 < 8,00E-06.

Looking at the simulations above, it can be concluded:

- OH-DC-2 and OH-DC-8 RAM outcomes remain the same in both scenarios since airborne equipment reliability is not affecting these two hazards.
- There is very low influence of FCI airborne system redundancy in the final RAM analysis outcomes when airborne redundant equipment is used, moving from 2,13E-05 FH to 1,50E-05 FH for OH-DC-

1c and OH-DC-7c hazards and from 7,10E-06 FH to 7,43E-06 FH for OH-DC 2c and OH-DC 8c hazards. In both cases, FCI safety objectives are met.

This leads to the conclusion that FCI airborne system redundancy is not required to meet the FCI safety objectives.

6.2.7.3 Influence of FCI Ground systems redundancy considering interdependency β factors.

Interdependency β factors affecting to ground FCI equipment are:

- β1 factor between Ground ATN/IPS End systems: it is measuring the interdependency between two devices of the same model providing redundancy.
- β2 factor between G/G ATN/IPS routers: it is measuring the interdependency between two devices of the same model providing redundancy.
- β3 factor between A/G ATN/IPS routers: it is measuring the interdependency between two devices of the same model providing redundancy.
- β7 factor between Ground ATN/OSI End systems: it is measuring the interdependency between two devices of the same model providing redundancy.
- β8 factor between G/G ATN/OSI routers: it is measuring the interdependency between two devices of the same model providing redundancy.
- β9 factor between OSI/IPS gateways: it is measuring the interdependency between two devices of the same model providing redundancy.
- β10 factor between A/G ATN/OSI routers: it is measuring the interdependency between two devices of the same model providing redundancy.

An initial value of β1 = β2 = β3 = β7 = β8 = β9 = β10 = 10% has been used by default in reliability calculations for FCI datalink elements during RAM analysis.

This section is going to analyse the influence of FCI ground β factors to identify if redundant ground equipment is required to meet the FCI safety objectives.

For this purpose, two scenarios are going to be considered:

Access infrastructure redundancy	Beta factor value
Scenario 1: FCI Ground redundant equipment	β1 = β2 = β3 = β7 = β8 = β9 = β10 = 0,1 (interdependency 10%)
Scenario 2: FCI Ground single equipment	β1 = β2 = β3 = β7 = β8 = β9 = β10 = 1 (interdependency 100%)

The results of these simulations are shown as follows:

Scenario 1: FCI Ground redundant equipment. β1 = β2 = β3 = β7 = β8 = β9 = β10 = 0,1 (interdependency 10%)

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

All FCI safety objectives are met.

Scenario 2: FCI Ground single equipment. β1 = β2 = β3 = β7 = β8 = β9 = β10= 1 (interdependency 100%)

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,51E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,57E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,57E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,53E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		8,13E-06	FAIL
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		8,13E-06	FAIL
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,51E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,57E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,57E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,53E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		8,13E-06	FAIL
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		8,13E-06	FAIL

FCI safety objectives OH-DC2b, OH-DC2c, OH-DC8b and OH-DC8c are not met.

A summary of these simulations' outcomes are shown as follows:

Simulation	Effect
Scenario 1: FCI Ground redundant equipment. β1 = β2 = β3 = β7 = β8 = β9 = β10 = 0,1 (interdependency 10%)	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,50E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,43E-06 < 8,00E-06.
Scenario 2: FCI Ground single equipment. ββ1 = β2 = β3 = β7 = β8 = β9 = β10 = 1 (interdependency 100%)	All FCI safety objectives are not met. OH-DC-1c and OH-DC-7c RAM outcome is 1,57E-05 < 8,00E-04. **OH-DC-2b, OH-DC-2c, OH-DC-8b and OH-DC-8c RAM outcomes are 8,13E-06 > 8,00E-06, not meeting safety objectives.**

Looking at the simulations above, it can be concluded:

- OH-DC-2b, OH-DC-2c, OH-DC-8b and OH-DC-8c RAM outcomes do not meet the corresponding safety objectives.

- There is a medium influence of FCI ground system redundancy in the final FCI RAM analysis outcomes when ground redundant equipment is used, moving from 8,13E-06 FH to 7,43E-06 FH for OH-DC-2b, OH-DC-2c, OH-DC-8b and OH-DC-8c hazards.

This leads to the conclusion that FCI ground system redundancy is required to meet the FCI safety objectives, while this redundancy has a medium influence in final FCI RAM analysis outcomes.

6.2.7.4 Influence of using several FCI A/G access networks (multilink) and potential interdependency β factors.

This section is going to analyse the influence of using several FCI A/G access networks (multilink) Also considering the existence of interdependency between two FCI A/G access networks (β13 factor).

Interdependency β factors affecting to FCI A/G networks is:

- β13 factor between VDLm2 and LDACS: it is measuring the interdependency between these two A/G datalink subnetworks.

An initial value of β13 = 10% has been used by default in reliability calculations for FCI datalink elements during RAM analysis.

For this analysis, it is going to be considered a VDLm2 availability of 99,99% independently of the traffic load and Provider Aborts issue.

For this purpose, two scenarios are going to be considered:

Access infrastructure redundancy	Beta factor value
Scenario 1: Only VDLm2 is used.	β13 = 0
Scenario 2: multilink VDLm2 and LDACS are used with no interdependency.	β13 = 0
Scenario 3: multilink VDLm2 and LDACS is used with interdependency.	β13 = 0,1
Scenario 4: multilink VDLm2, LDACS, SATCOM and AeroMACS is used with interdependency.	β13 = 0,1
Scenario 5: only VDLm2 with 99,9 % availability. This scenario considers the situation in which VDLm2 traffic load and Providers Abort issue reduce the real VDLm2 availability to 99,9 %.	β13 = 0
Scenario 6: multilink VDLm2 with 99,9 % and LDACS with 99,99 % are used with no interdependency. This scenario considers the situation in which VDLm2 traffic load and Providers Abort issue reduce the real VDLm2 availability to 99,9 %.	β13 = 0

A datalink Mandate is in force today (EC 310/2015) that requires an availability of 99,99% of VDLm2 A/G access network over FL285. As an initial approach, the same value has been considered for all the potential A/G access networks (LDACS, SATCOM and AeroMACS).

The results of these simulations are shown as follows:

Scenario 1: Scenario 1: Only VDLm2 is used.

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

All FCI safety objectives are met.

Scenario 2: multilink VDLm2 and LDACS are used with no interdependency (β13 = 0).

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,50E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,10E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,43E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,43E-06	PASS

All FCI safety objectives are met.

Scenario 3: multilink VDLm2 and LDACS is used with interdependency (β13 = 0,1).

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,49E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,32E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,64E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,64E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,49E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,32E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,64E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,64E-06	PASS

All FCI safety objectives are met.

Scenario 4: multilink VDLm2, LDACS, SATCOM and AeroMACS is used with interdependency (β13 = 0,1).

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,37E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,40E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,40E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		6,05E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		6,38E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		6,38E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,37E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,40E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,40E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		6,05E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		6,38E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		6,38E-06	PASS

All FCI safety objectives are met.

Scenario 5: only VDLm2 with 99,9 % availability.

This scenario considers the situation in which VDLm2 traffic load and Providers Abort issue reduce the real VDLm2 availability to 99,9 %. This scenario could be considered possible in an environment where the air Traffic density will be at much higher level than today (factor 10 increase) as expected with ATN B2 or ATN B3 phase combined with high growth AOC traffic increase.

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		4,51E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		4,54E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		4,54E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		3,75E-05	FAIL
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		3,78E-05	FAIL
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		3,78E-05	FAIL
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		4,51E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		4,54E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		4,54E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		3,75E-05	FAIL
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		3,78E-05	FAIL
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		3,78E-05	FAIL

FCI safety objectives OH-DC2a, OH-DC2b, OH-DC2c, OH-DC8a, OH-DC8b and OH-DC8c are not met.

Scenario 6: multilink VDLm2 with 99,9 % and LDACS with 99,99 % are used with no interdependency.

This scenario considers the situation in which VDLm2 traffic load and Providers Abort issue reduce the real VDLm2 availability to 99,9 % and LDACS is used with a 99,99 % availability. This scenario could be considered possible in an environment where the air Traffic density will be at much higher level than today (factor 10 increase) as expected with ATN B2 or ATN B3 phase combined with high growth AOC traffic increase.

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,44E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		6,84E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,09E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,09E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,44E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,47E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		6,84E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,09E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,09E-06	PASS

A summary of these simulations' outcomes are shown as follows:

Simulation	Effect
Scenario 1: Only VDLm2 is used.	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,50E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,43E-06 < 8,00E-06.
Scenario 2: multilink VDLm2 and LDACS are used with no interdependency ($\beta 13 = 0$)	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,50E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,43E-06 < 8,00E-06.
Scenario 3: multilink VDLm2 and LDACS is used with interdependency ($\beta 13 = 0,1$).	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,53E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,64E-06 < 8,00E-06.

Scenario 4: multilink VDLm2, LDACS, SATCOM and AeroMACS is used with interdependency (β13 = 0,1).	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,40E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 6,38E-06 < 8,00E-06.
Scenario 5: only VDLm2 with 99,9 % availability.	FCI safety objectives OH-DC2a, OH-DC2b, OH-DC2c, OH-DC8a, OH-DC8b and OH-DC8c are not met. **OH-DC-1a and OH-DC-7a RAM outcomes are 3,75E-05 > 8,00E-06, not meeting safety objectives.** **OH-DC-2b, OH-DC-2c, OH-DC-8b and OH-DC-8c RAM outcomes are 3,78E-05 > 8,00E-06, not meeting safety objectives.**
Scenario 6: multilink VDLm2 with 99,9 % and LDACS with 99,99 % are used with no interdependency	All FCI safety objectives are met. OH-DC-1c and OH-DC-7c RAM outcome is 1,47E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,09E-06 < 8,00E-06.

Looking at the simulations above, it can be concluded:

- Considering VDLm2 availability of 99,99%, the influence of having two multilink FCI A/G access networks is low since, just with only one A/G access network (i.e., VDLm2), an availability of 99,99% is obtained. This availability is comparable with the NewPENS one. The use of two A/G access networks is going to improve only the total A/G access network availability, the unavailability of the NewPENS network (Q) becoming the main factor that determines the final unavailability of the whole FCI system. This is the reason why there is no significant enhancement in the total FCI availability by using two instead of one A/G access networks.
- Considering potential real VDLm2 availability of only 99,9% due to VDLm2 traffic load and Providers Abort issue, the influence of having two multilink FCI A/G access networks is high since with only VDLm2 A/G access network the datalink safety objectives are not met. In this case, it is required the use of a second A/G access network such as LDACS, SATCOM or AeroMACS. This scenario could be considered possible in an environment where the air Traffic density will be at much higher level than today (factor 10 increase) as expected with ATN B2 or ATN B3 phase combined with high growth AOC traffic increase.

This leads to the conclusion that FCI multilink A/G access networks has not significant influence to meet the FCI safety objectives in case that VDLm2 availability is 99,99% but FCI multilink (at least a second A/G access network) would be required in case of considering potential real VDLm2 availability of only 99,9% due to VDLm2 traffic load and Providers Abort issue.

6.2.7.4.1 Influence of OSI/IPS Gateway sensitivity analysis.

Interdependency β factor affecting to OSI/IPS Gateway is:

- β9 factor between OSI/IPS gateways: it is measuring the interdependency between two devices of the same model providing redundancy.

An initial value of β9 = 10% has been used by default in reliability calculations for FCI datalink elements during RAM analysis.

This section is going to analyse the influence of β9 factor to identify if redundant OSI/IPS Gateway is required to meet the FCI safety objectives.

To perform this analysis, it has been considered that the rest of FCI ground systems are redundant (β1 = β2 = β3 = β7 = β8 = β10 = 0,1).

For this purpose, two scenarios are going to be considered:

Access infrastructure redundancy	Beta factor value
Scenario 1: OSI/IPS Gateway redundant equipment	β9 = 0,1 (interdependency 10%)
Scenario 2: OSI/IPS Gateway single equipment	β9 = 1 (interdependency 100%)

The results of these simulations are shown as follows:

Scenario 1: OSI/IPS Gateway redundant equipment. β9 = 0,1 (interdependency 10%)

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,49E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,32E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,64E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,64E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,49E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,53E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,32E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,64E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,64E-06	PASS

All FCI safety objectives are met.

Scenario 2: OSI/IPS Gateway single equipment. β9 = 1 (interdependency 100%)

The outcomes of the FCI RAM analysis are collected as follows:

Hazard ID	Hazard/ Failure mode	Severity	Safety Objective including apportionment (/FH)		FCI RAM outcome (/FH)	Safety Objective (Pass/Fail)
OH-DC-1a	Loss of data link capability [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,49E-05	PASS
OH-DC-1b	Loss of data link capability [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,54E-05	PASS
OH-DC-1c	Loss of data link capability [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,54E-05	PASS
OH-DC-2a	Loss of data link capability [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,32E-06	PASS
OH-DC-2b	Loss of data link capability [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,78E-06	PASS
OH-DC-2c	Loss of data link capability [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,78E-06	PASS
OH-DC-7a	Unexpected interruption of a data link transaction [single aircraft] (IPS-IPS flow)	4	8,00E-04		1,49E-05	PASS
OH-DC-7b	Unexpected interruption of a data link transaction [single aircraft] (OSI-IPS flow)	4	8,00E-04		1,54E-05	PASS
OH-DC-7c	Unexpected interruption of a data link transaction [single aircraft] (IPS-OSI flow)	4	8,00E-04		1,54E-05	PASS
OH-DC-8a	Unexpected interruption of data link transactions [multiple aircraft] (IPS-IPS flow)	3	8,00E-06		7,32E-06	PASS
OH-DC-8b	Unexpected interruption of data link transactions [multiple aircraft] (OSI-IPS flow)	3	8,00E-06		7,78E-06	PASS
OH-DC-8c	Unexpected interruption of data link transactions [multiple aircraft] (IPS-OSI flow)	3	8,00E-06		7,78E-06	PASS

All FCI safety objectives are met.

A summary of these simulations' outcomes are shown as follows:

Simulation	Effect
Scenario 1: OSI/IPS Gateway redundant equipment	All FCI safety objectives are met. OH-DC-1b and OH-DC-7b RAM outcome is 1,53E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,64E-06 < 8,00E-06.
Scenario 2: OSI/IPS Gateway single equipment	All FCI safety objectives are not met. OH-DC-1b and OH-DC-7b RAM outcome is 1,54E-05 < 8,00E-04. OH-DC-2b and OH-DC-8b RAM outcome is 7,78E-06 < 8,00E-06.

Looking at the simulations above, it can be concluded:

- Even in all cases the safety objectives are met because redundancy of the rest of FCI ground systems was considered (see 'Influence of FCI Ground systems redundancy considering interdependency β factors' in section 6.2.7.3), the OH-DC-2b and OH-DC-8b RAM outcomes were improved significantly from 7,78E-06 to 7,64E-06.

This leads to the conclusion that OSI/IPS Gateway redundancy is clearly recommended aligned with the outcomes of 'Influence of FCI Ground systems redundancy considering interdependency β factors' analysis performed in section 6.2.7.3 of this document.

6.2.8 RAM ANALYSIS ON ATS-B3.

A separated RAM analysis can be performed taking into consideration the safety and performance requirements standard for Baseline 3 ATS data communications. It would first require to revisit the potential hazards identified in an ATS-B3 environment.

7 CONCLUSIONS AND SUMMARY

A RAM analysis has been performed on the FCI with a number of hypotheses detailed above. The main conclusions are repeated below and explained in detail in the preceding sections.

- **the minimum NewPENS availability to assure that ATS-B2 datalink services can be deployed operationally and meeting all the safety objectives is 99,99% (One site, dual connection), that corresponds to have a dual connection to NewPENS in at least one site.**
- **There is a huge influence of the NewPENS availability in the final RAM analysis outcomes. This leads to the conclusion to recommend the implementation of two sites, dual connection per site, to have a NewPENS availability of 99,995%.**
- **FCI airborne system redundancy is not required to meet the FCI safety objectives.**
- **FCI ground system redundancy is required to meet the FCI safety objectives, while this redundancy has a medium influence in final FCI RAM analysis outcomes (low sensitivity).**
- **FCI multilink A/G access networks have no significant influence to meet the FCI safety objectives in case that VDLm2 availability is 99,99% but FCI multilink (at least a second A/G access network) would be required in case of considering potential real VDLm2 availability of only 99,9% due to VDLm2 traffic load and Providers Abort issue.**
- **OSI/IPS Gateway redundancy is clearly recommended.**
- **The Availability analysis documented in this report does not cover Continuity, whose analysis is however necessary, in order to build a comprehensive picture of Safety Performance Requirements fulfilment**
- **The Availability modelling used for the analysis assumes random unintentional failures. In case of cyber attacks (e.g. radio jamming) the margin between the required performance and the predicted performance resulting from this analysis gives a first level understanding of the robustness of the system. From this perspective, those configurations that have a higher margin should be preferred.**

8 Acronyms and Terminology

Acronym	Definition
ALARP	As Low As Reasonable Practicable
ALARP	As Low As Reasonable Practicable
AMC	Acceptable Means of Compliance
ATIS	The Alliance for Telecommunications Industry Solutions
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service
BBN	Bayesian Belief Network
BOF	Beginning of File
CCA	Cause Consequence Analysis
CCFA	Common Cause Failure Analysis
CLI	Command Line Interface
CMF	Common Mode failure
COTS	Commercial Off The Shelf
CRC	Cyclical Redundancy Check
DB	Database
E1	E-carrier system
E2E	End-to-End
ECC	Error-Correcting Code
EJB	Enterprise Java Beans
E&M	Ear and Mouth (E&M) interface
ETH	Ethernet
FAT	Factory Acceptance Test

FHA	Functional Hazard Analysis
FHRP	First Hop Redundancy Protocol
FMEA	Failure mode and effects analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FRR	Fast Re-Route
FRU	Field Replaceable Unit
FTA	Fault Tree Analysis
FTP	File Transfer Protocol
GE	Giga bit Ethernet
GUI	Graphical User Interface
HAZOP	Hazard and Operability study
HLD	High Level Document
IEC	International Electrotechnical Commission
ITU-T	ITU Telecommunication Standardization Sector
LLD	Low Level Design
LSP	Label Service Distribution Point
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Restore Services
OSPF	Open Shortest Path First
OSS	Operations Support Systems
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PSSA	Preliminary System Safety Assessment
RBD	Reliability Block Diagram
SAM	Safety Assessment Methodology (Eurocontrol)

SAP	Service Access Points
SAR	Service Aggregation Router
SAT	Site Acceptance Test
SDI	Serial Digital Interface
SDP	Service Distribution Points
SIL	Safety Integrity Level
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SO	Safety Object
SOAP	Simple Object Access Protocol
SR	Safety Requirement
SROS	Service Router Operating System
SSA	System Safety Assessment
SWAL	Software Assurance Level
TAT	Total Acceptance Test
TCP	Transport Communication Protocol
TDM	Time Division Multiplexing
VoIP	Voice Over IP
VCS	Voice Communication System
WAN	Wide Area Network
XML	eXtended Markup Language
SDP	Service Distribution Points
SIL	Safety Integrity Level
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SO	Safety Object
SOAP	Simple Object Access Protocol

SR	Safety Requirement
SROS	Service Router Operating System
SSA	System Safety Assessment
SWAL	Software Assurance Level
TAT	Total Acceptance Test
TCP	Transport Communication Protocol
TDM	Time Division Multiplexing
VoIP	Voice Over IP
VCS	Voice Communication System
WAN	Wide Area Network
XML	eXtended Markup Language
TDM	Time Division Multiplexing
VoIP	Voice Over IP
VCS	Voice Communication System
WAN	Wide Area Network
XML	eXtended Markup Language

Table 4: Acronyms

9 References

[1] SESAR2020 Wave 2 - PJ.14-W2-77 'TRL6 TVALP – Part 2 – Safety Assessment Plan, Ed 01.00.01, 27 Jan. 2022

[2] SESAR2020 Wave 1 - PJ.14.02.04 'Transversal and Complementary Studies', 22 Nov. 2019

[3] AIRBUS 'Safety considerations and their impact on the ATN/IPS standardisation', ICAO Communication Panel – WG-I Meeting 21, May 2016

[4] EUROCAE ED-228A, 'SAFETY AND PERFORMANCE REQUIREMENTS STANDARD FOR BASELINE 2 ATS DATA COMMUNICATIONS - (BASELINE 2 SPR STANDARD), March 2016, Appendix B (also referenced as RTCA DO-350A).

[5] EUROCAE ED78A, 'Guidelines for approval of the provision and use of Air Traffic Services supported by data communications', December 2000

[6] SESAR2020 Wave 2- PJ19, Private Email communication, 9. Nov. 2021

[7] SESAR 1 – Project 15.02.05 – D03 'IRIS Precursor Security, Safety and Performance Analysis'

[8] EUROCONTROL Safety Assessment Methodology, available under Safety assessment methodology (e-SAM) | EUROCONTROL https://www.eurocontrol.int/tool/safety-assessment-methodology (accessed on 10 Oct. 2022).

[9] SESAR 1 – Project 15.02.04 'Future Data Link System Definition' – 'WA1.2: Deliverable D04 - Quality of Service (QoS) and Classes of Service (CoS)', March 2015

[10] EUROCAE ED153, 'GUIDELINES FOR ANS SOFTWARE SAFETY ASSURANCE', Aug. 2009

[11] SESAR2020 Wave 2 - PJ.14-W2-77 'TRL6 TVALR, Ed 01.00.02, 23 Nov. 2022

-END OF DOCUMENT-