INDUSTRIAL RESEARCH

JOINT UNDERTAKING

SESAR Solution 115 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report

Deliverable ID:	D3.1.140
Dissemination Level:	PU
Project Acronym:	ERICA
Grant:	874474
Call:	H2020-SESAR-2019-1
Topic:	ENABLE RPAS INSERTION IN CONTROLLED AIRSPACE (RPAS Accommodation)
Consortium Coordinator:	Leonardo
Edition Date:	19 December 2022
Edition:	00.03.00
Template Edition:	00.00.02

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
INECO / ENAIRE	15/09/2022

Reviewers internal to the project

Beneficiary	Date
AIRBUS DS	--
CRIDA / ENAIRE	--
DASSAULT AVIATION	07/10/2022
DSNA	15/09/2022 & 18/10/2022
ENAIRE	--
ENAV	--
EUROCONTROL	--
FREQUENTIS	--
HUNGAROCONTROL	--
IDS AIRNAV	--
INDRA	--
ISDEFE/ ENAIRE	--
LEONARDO	--
LTP SAFRAN	--
NATS	22/09/2022
ORO NAVIGACIJA	20/09/2022
SAAB	--
THALES AVS	06/10/2022 & 26/10/2022

Reviewers external to the project

Beneficiary	Date
PJ19 Safety Team	11/10/2022
SJU	01/12/2022

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

Beneficiary	Date
AIRBUS DS	16/12/2022
CRIDA / ENAIRE	16/12/2022
DASSAULT AVIATION	16/12/2022
DSNA	16/12/2022
ENAIRE	16/12/2022
ENAV	16/12/2022
EUROCONTROL	16/12/2022
FREQUENTIS	16/12/2022
HUNGAROCONTROL	16/12/2022
IDS AIRNAV	16/12/2022
INDRA	16/12/2022
INECO/ ENAIRE	16/12/2022
ISDEFE/ ENAIRE	16/12/2022
LEONARDO	16/12/2022
LTP SAFRAN	16/12/2022
NATS	16/12/2022
ORO NAVIGACIJA	16/12/2022
SAAB	16/12/2022
THALES AVS	16/12/2022

Rejected By – Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	10/03/2022	Draft	INECO / ENAIRE	First draft for partners' review.
00.01.00	01/06/2022	1st interim version	INECO / ENAIRE	First interim version which includes the comments received from partners.
00.01.01	15/09/2022	Draft	INECO / ENAIRE	Final draft for partner's review.
00.02.00	07/10/2022	Final version	INECO / ENAIRE	Final version for submission to SJU. It includes the comments received from partners
00.02.01	27/10/2022	Draft	INECO / ENAIRE	Final draft which includes the comments received from PJ19 Safety Experts, for partner's review.
00.02.02	03/11/2022	Final version	INECO / ENAIRE	Final version for submission to SJU. It includes the comments received from PJ19.
00.03.00	19/12/2022	Final version	INECO / ENAIRE	Final version. The document has been completed considering the comments provided by SJU during the Maturity Gate (01/12/2022)

Copyright Statement © 2022 – PJ13 ERICA- Solution 115 Partners. All rights reserved. Licensed to SESAR3 Joint Undertaking under conditions.

ERICA

ENABLE RPAS INSERTION IN CONTROLLED AIRSPACE

This Safety Assessment Report is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 874474 under European Union's Horizon 2020 research and innovation programme.

Abstract

Initial demand from existing Remotely Piloted Aircraft System (RPAS) is to rapidly access and transit through controlled airspace. They expect this under similar principles as general air traffic (GAT) users, flying and controlled in instrument flight rules (IFR). This solution focussed on a method responding to that need.

SESAR Solution 115, building on actual experience, defines a concept to accommodate this RPAS demand in the current European ATM system.

The concept is based on use of an adapted separation instead of segregation when RPAS are transiting in a controlled airspace class A, B or C using instrument flight rules as general air traffic and use of existing systems. Nevertheless, the peculiarities of no pilot on board the RPAS and a command-and-control link between the remote pilot station and the remotely piloted aircraft require the introduction of new procedures.

Therefore, the purpose of this Safety Assessment Report is to analyse this RPAS accommodation from a safety perspective, considering both an RPAS flying in nominal and non-nominal situations. That is to say, identifying and evaluating the risks that it generates, and finding mitigation measures to minimize or eliminate their impact on aviation. With this AIM, a series of Safety Requirements, both at ATS service level (SRS) and at refined design level (rSRD), are established

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ.13-W2-115 Solution related to the accommodation of RPAS in Airspace Class A to C in IFR operations. The Safety Assessment Report (SAR) represents Part II of the SPR-INTEROP/OSED document and presents the assurance that the Safety Requirements for the V3 phase are complete, correct and realistic, thereby providing all material to adequately inform the PJ.13-W2-115 Solution SPR-INTEROP/OSED[1].

[1] NOTE: As coordinated with SJU, the TS/IRS is an Annex within the SPR-INTEROP/OSED document.

2 Introduction

2.1 Background

RPAS have been used for many years by the military but have been restricted to segregated airspace to protect their operations and other traffic. As a consequence, nowadays, the accommodation of RPAS operations in manned aviation environments requires the establishment of special arrangements due, amongst other things, to concern over safety aspects, particularly related to the risk of mid-air collisions and the loss of the Command & Control (C2) link between the Remotely Piloted Aircraft (RPA) and the Remote Pilot Station (RPS) on the ground.

This was the reason why RPAS experts were called by the European Commission to develop the 'Roadmap for the integration of civil RPAS into the European aviation system', which was officially launched in June 2013. SESAR 2020 Wave 1 projects were the response to this roadmap. SESAR Wave 1 PJ 10.05 PROSA did identify several SESAR RPAS demonstration projects (SESAR Solution 10-05 SPR-INTEROP/OSED for V2 section 2.4), and a SESAR JU summary «Demonstrating RPAS integration in the European aviation system» [9] exists, although not all are related to MALE IFR RPAS accommodation in class A-C airspace in the short to mid-term.

The principal predecessor project for RPAS insertion into controlled airspace is SESAR 2020 Wave 2 PJ.10.05 PROSA. Nonetheless, this project focused more on RPAS integration, not accommodation. In addition, gaps were detected in terms of flight operations and use cases not yet considered.

The aim of Solution PJ13.W2.115 is to provide an improvement to the results of PJ.10.05 PROSA, by covering those gaps and exploring new operating methods. Moreover, among the work developed by PJ.10.05 PROSA, a Safety Assessment Report (SAR) was conducted as Part II of the OSED Task. This document is also considered by PJ13.W2.115 in order to develop the present SAR in a complete and appropriate manner.

A more complete description of the background can be found in the section 2.4 of the SPR-INTEROP/OSED [5].

2.2 General Approach to Safety Assessment

This safety assessment is conducted as per the SESAR Safety Reference Material (SRM) which itself is based on a twofold approach:

- a success approach which is concerned with the safety of the Solution operations in the absence of failure within the end-to-end Solution functional system, encompassing both Normal operation and Abnormal conditions,
- a conventional failure approach which is concerned with the safety of the Solution operations in the event of failures within the end-to-end Solution functional system.

These two approaches are applied to the derivation of safety properties at each of the successive lifecycle stages of the Solution development (Safety Requirements at service level and at design level).

2.3 Scope of the Safety Assessment

This Safety Assessment Report covers the safety related activities in the V3 phase of Solution PJ.13-W2-115. It is based on:

- The Guidance Material developed within SESAR 1 and used during SESAR 1 and Wave 1 (references [3] and [4]).
- The information compiled within the VALR of the precedent Solution of Wave 1 PJ10.05.
- The Safety Assessment Plan developed within this Solution 115, which constitutes Part II of the VALP (reference [5]).

Therefore, the relevant hazards, Safety Criteria and Safety Assurance Activities identified within the SAP will be taken into account and reviewed in order to derive appropriate Safety Requirements to mitigate the risks associated to the concept developed within Solution 115.

Safety lifecycle

The safety lifecycle is one of the important aspects covered in the SESAR Reference Material (SRM) [3]. It details, for each maturity state, the safety assessments that are performed at the Solution level. It is essential that the assessments and the subsequent validation activities are undertaken against a specific operational concept, consistent set of assumptions and simulation scenarios valid for the Solution. This safety lifecycle can be summarised under the following headings:

- V1 safety assessment involves the analysis of the Operational Concept in relation with the AIM models to derive the SAC that will feed the OSED V1.

- V2 is divided in two phases:

  - Phase one safety assessment involves the analysis of the operational services underpinning the AIM models to derive the safety requirements at service level (success and failure) of the OSED V2 to comply with the SAC. The safety requirements at service level from the failure approach are derived as a result of the Functional Hazard Analysis (FHA) equivalent activities.

  - Phase two safety assessment involves the analysis of the architectural representation of the ATM/ANS system design (the SPR level model) in order to derive safety requirements (success and failure) to comply with the safety requirements at service level (success and failure). The safety requirements from the failure approach are derived as a result of the Preliminary System Safety Assessment (PSSA) equivalent activities.

- V3 safety assessment involves the analysis of the Physical Model in order to derive the physical safety requirements (success and failure) to feed the SPR-INTEROP/OSED, complying with the safety requirements (success and failure) at the SPR level model; and the detailed analysis/refinement of the SPR-Level Model related to Human Tasks. The physical safety requirements from the failure approach are derived as a result of the first stage of SSA equivalent activities.

As S115 has no predecessor output on V1 and V2 activities, this assessment is covering all three phases.

Co-funded by the European Union

The safety assessment processes for PJ13-W2-115 supports the Safety Lifecycle with the following activities:

- the identification of applicable hazards,
- the analysis of the operational services underpinning the AIM models to derive the Safety Criteria,
- the derivation of Safety Requirements through Causal analysis (bridging the SPR/INTEROP and AIM levels).

The related safety evidence derived from the Validation results will be documented in the:

- Safety Assessment Report (SAR), Part II of the Final SPR-INTEROP/OSED, this document.
  - Safety specification at ATS service level (Section 4),
  - Safe Design of the Solution functional system (Section 5), and
  - Safety Criteria achievability (Section 6)
- Validation Report (D3.1.030) [8].

2.4 Layout of the Document

This Safety Assessment Report contains the following sections:

Section 1 provides the Executive Summary.

Section 2 is an introduction, in which the purpose of this SAR is described.

Section 3 gives an overview of the Solution PJ.13-W2-115 in terms of the scope of the change introduced by the Solution, the operational environment, the key properties, and the benefits expected for stakeholders. Furthermore, the Safety Criteria (SAC) identified within the SAP are recovered.

Section 4 contains the Safety specification at ATS service level. It deals with the mitigation of risks inherent to aviation in normal, abnormal and failure conditions, and derives a series of related Safety Requirements at ATS Service level (SRS).

Section 5 contains the analysis of the Safe Design of the Solution functional system and includes the derivation of Safety Requirements at refined Design level (rSRD) in normal, abnormal and failure conditions.

Section 6 focuses on the achievability of the Safety Criteria (SAC).

Section 7 lists the used acronyms and terminology, and **Section 8** includes the documents referred to in this SAR.

Moreover, a series of Appendixes complete this Safety Assessment Report:

Appendix A presents the outcomes of the preliminary safety impact assessment and Safety Criteria determination, conducted within the VALP Task.

Appendix B includes the process for deriving Safety Requirements at ATS Service level (SRS) for normal conditions of operation

Appendix C contains the risk analysis of abnormal conditions and the derivation of the related SRS.

Appendix D presents the risk analysis addressing internal functional system failures and the derivation of additional SRS.

Appendix E addresses the design of the Solution functional system for normal conditions of operation, deriving a set of rSRD from the previous identified SRS

Appendix F addresses the design of the Solution functional system for abnormal conditions of operation, deriving a set of rSRD from the previous identified SRS

Appendix G addresses the design of the Solution functional system regarding internal functional system failures, deriving a set of rSRD from the previous identified SRS

Appendix H focuses on the demonstration of Safety Criteria achievability

Appendix I includes a list of assumptions, issues and limitations identified while developing this SAR.

3 Setting the Scene of the safety assessment

The purpose of this section is to provide the main information collected within the SAF&HP Scoping and Change assessment and the Safety Plan development process in order to set the scene for the safety assessment documented in the SAR.

3.1 Operational concept overview and scope of the change

Operational concept overview

The overall project aims to propose a solution to permit initially existing IFR RPASs operating as GAT transit flights, safe operation in nominal, abnormal conditions and emergencies in class A to C controlled airspace. It will also create and test that solution's 115 RPAS accommodation does not have negative impacts on air traffic. This is the reason why the EU founded the PJ13-W2 project, and in particular, solution 115.

That is to say, the project will seek to address the concepts to develop recognised European RPAS operations in non-segregated airspace that will enable civil and STATE RPASs to operate amongst other controlled aircraft within air traffic management systems within Europe. As discussed above, this concept on RPAS accommodation into the ATM network will be implemented in the short-medium term time periods. Accommodation procedures are targeted to respond to initial RPAS user demand, which for the initial know RPAS are state/military RPAS, with the demand described in this operational concept overview.

In summary, focusing on the solution to be developed here, solution 115 aims at proposing a solution to accommodate RPAS transit flights in non- segregated controlled A, B and C airspace focusing on procedural improvements. During the accommodation phase, it will make use of existing ATM and the existing initial RPAS systems. Operations considered in the concept are those currently performed by state RPAS, mainly military, but, prior to this concept, operate segregated and/or as OAT traffic.

Scope of the change

When RPAS fly in civil controlled airspace, they fly in segregated volumes, whether in their mission area or while transiting from the departure aerodrome to the mission area or from the mission area to the destination aerodrome. Today, thanks to the concept of smart segregation, these permanent segregated areas are activated just a few minutes before the RPAS flies in, but this concept is not applicable in all states.

The main problem is the time-consuming preparation work involved. By this work we mean the work done such as in the field of aeronautical information, modification of ATCO HMI to visualize the segregated areas, preparation and distribution of material, specific briefings, the increase of ATCO workload and coordinations when a manned aircraft requires to cross this area, etc.

This solution is focused only on procedural methods, access to controlled airspace for RPAS, and equity for all airspace users including RPAS. The aim is to encourage the early adoption of these accommodation procedures to meet the initial demand for RPAS. This will reduce planning and approval times for operation, improve routine access for IFR GAT RPAS transit flights across airspace class A-C with limited restrictions and achieve an airspace equity to all airspace users. All this is intended to be done with a neutral impact on safety in the target airspace and without a decrease in human performance.

If we refer to the applicable regulatory framework and industry standard, the SPR INTEROP/OSED [1] section 3.2.4. will be used, while if the interest is in the accommodation phase, the current regulatory framework and industry standard are considered as applicable.

Looking at previous projects (e.g., PJ10-05) related to RPAS flight:

- Air traffic controllers reported that, in nominal flight, there were no significant difference in the behaviour of RPAS compared to small general aviation aircraft[2] . It was in non-nominal situations that they did find differences. The principal difference was found when the RPAS loses the command-and-control link (C2 link) between the remotely piloted aircraft (RPA) and the remote pilot station (RPS). This also leads to loss of RP-ATC voice communications which are relayed over this link.
- In addition, the ATCOs wanted to be able to distinguish whether the aircraft they were in charge of was an RPA.

These were many of the comments that were collected in these projects from the comments provided by the controllers to propose an improvement in this new area. The new operating method proposes to use their regular operating / separation methods and encompassing C2 LL procedure similar to the radio communications loss procedure, derived from the ICAO RPAS Panel material to manage RPAS flight.

This solution is not intended to offer changes to the roles and responsibilities of controllers, i.e. given the operational scope of this solution, the number of RPAS in flight controlled by a given ATCO team in a sector at any time will continue to be very limited, and will be managed in the same way as manned flights. In addition, the complexity/density of traffic in the same airspace will also be limited to low or medium. Therefore, it is not necessary to modify the controllers-related tasks, since this is already the method used to manage manned aircraft.

Beyond these controller tasks, the solution must be built using existing ATM systems and the existing ATCO Human Machine Interface (HMI), only considering that an ATCO HMI change is acceptable if it is very light. There are some alternatives that have been proposed that do not modify the ATCO HMI (in principle, no specific training required) such as the controller receiving the information that an aircraft is an RPA by using the flight plan and the information displayed on the ATCO HMI via the strip (paper or electronic) or on the display label.

To conclude this section, it should be noted that remotely piloted aircraft systems (RPASs) offer significant services to civil and military aviation. RPAS routine access to non-segregated airspace would result in major economic benefits and market opportunities, as soon as the safety and operational demonstrations are achieved.

[2] S115 addresses current MALE RPAS, which are large turboprop or piston propelled whose performance is equivalent to manned controlled IFR aircraft of similar size and weight in lower airspace, like:

- HERON/HARFANG: 100 kts – 1.25 tonnes
- REAPER: 260 kts – 4.5 tonnes (main MALE RPAS of interest for accommodation)

3.2 Solution Operational Environment and Key Properties

This section will describe the operational environment for SESAR Solution 115 in a short to medium term timeframe.

First of all, the initial demand foreseen is for current operational state RPAS in an En-route operational environment (ER). These state RPAS, mainly military for the moment, meet acceptable requirements in terms of communication and navigation and surveillance performances and equipment to fly IFR as GAT in the accommodation portion of controlled airspace. Such RPAS are characterised by NATO classification and standards (Class III, STANAG 4671), the main RPAS concerned for the accommodation phase being addressed by this project are MALE and marginally HALE during climb descent through the targeted portion of En-route airspace, as stated above. This means that for S115 where the primary operation is RPAS transit in climb, descent and En-Route manoeuvres, **the only operating environment concerned is the En-route OE, including transit in the TMA flight portion assimilated to En-Route**[3]. In section 3.2.1 of SESAR Solution 115 SPR-INTEROP/OSED for V3 - Part I, a further definition of the characteristics of this environment is provided. These include different cases of operations such as pre-flight, nominal operation, in a C2 link loss contingency or in an emergency situation.

Secondly, low/medium density of traffic is envisaged in a non-segregated and controlled Class A-C airspace. Within this traffic there is a low number of IFR RPAS movements.

Finally, this is intended to reduce planning and approval time and improve routine access to the initial demand for RPAS from the STATE as General Air Traffic (GAT) with limited restrictions.

Referring to the main properties that this operational environment will have, all of them are listed below and can be completed with section 3.2 of the *SESAR Solution PJ.13-W2-115 SPR-INTEROP/OSED for V3 – Part I* [5]:

- ATC knows and clears all traffic in its controlled airspace (identification, position, trajectories).
- All RPAS operations are conducted under IFR rules on the basis of the initial RPAS CNS capabilities (VHF voice communications, Area Navigation with published AIRAC data, GPS/Inertial hybrid positioning, Mode A-C transponder).
- RPS / RPS handover between command centres is neither necessary nor used during GAT transit segment of RPAS.
- No technical / system changes to ATC systems.
- RPAS ICAO compliance limitations.
- Remote Pilot IFR Qualification.

On the other hand, as a reminder, the following functionalities and operational conditions are outside the scope of this Solution 115, which relies on available and existing functionalities:

- Airspace classes D to G.
- Airspaces classified as High complexity airspaces during medium/high traffic periods.
- Mission specific profiles and departure/arrival (non En-route operating environment).

[3] Terminal Airspace OE and associated manoeuvres, approach/departure to aerodromes related to it are not in the solution scope

- Remain Well Clear (RWC) or Collision Avoidance (CA) systems (see also section "3.4.2. Detection and avoidance systems (DAA) in RPAs").

3.3 Stakeholders' expected benefits with potential Safety impact

Several benefits are expected to be achieved with this solution PJ13-W2-115, which intends to foster a quick acceptance of accommodation procedures for the initial RPAS demand. This will enable:

- to reduce the planning and approval time for these RPAS operations, and
- to provide routine access for transit flights in Class A-C airspace with limited restrictions.

With these improvements, the equity of airspace for all airspace users, is being pursued.

From a **safety** perspective, the accommodation of RPAS in IFR environment might induce risks in terms of lack of compatibility between procedures or flying objects behaviours. Moreover, the handling of mixed traffic (regular and RPAS) might increase the complexity of the controller's tasks (traffic monitoring and management, vectoring, etc.). Therefore, the objective is to maintain the current levels of safety, to guarantee the safe operation of all Airspace Users, and the safe manage of air traffic.

3.4 Safety Criteria

The safety validation objectives presented in this Solution 115 must be formulated as safety criteria (SACs) in order to be able to perform measurements. They should all be measurable at precursor level in the Accident Incident Model (AIM), as described in the SESAR Safety Reference Material in Guide D [5]. In the Safety Assessment Plan, this full set of Safety Criteria (SACs) applicable for this solution was defined in section 4.2.3.

These SACs were defined considering the mentioned Guidance D of the Guidance to apply SESAR Safety Reference Material [4] and also the EU Regulation 2017/373 [1] (and any subsequent updates). Considering the information:

- collected in the Safety and Performance Requirements online workshops (encompassing the preliminary hazard identification), and
- provided in sub-sections 4.2.1 and 4.2.2 below (hazards identified),

a set of applicable Safety Criteria (SAC) for this ATS operational Solution has been established in the following Table 1.

SAC ID	Description	Barrier / Precursor
SAC#1 **SAC-13-115-001**	**The number of crew/aircraft induced tactical conflict[4] shall not increase.** These conflicts are induced by an event triggered by the RPAS/RP.	MF 6.1

[4] In this context, a tactical conflict is considered an event which has occurred during the tactical phase of operation.

SAC ID	Description	Barrier / Precursor
SAC#2 **SAC-13-115-002**	**The number of planning conflicts shall not increase due to RPAS operations**. These conflicts are those that remain unresolved by the traffic planning and synchronization barrier (hence presented to the tactical conflict management barrier).	MF 5.1
SAC#3 **SAC-13-115-003**	**The number of VFR (existing manned) / IFR (manned + RPAS) conflicts shall not increase due to RPAS operations.**	MF 9.1
SAC#4 **SAC-13-115-004**	**The number of ATC-induced tactical conflicts shall not increase due to RPAS operations.** These conflicts are generated by ATC actions on the managed traffic.	MF 7.1
SAC#5 **SAC-13-115-005**	**The number of separation imminent infringements shall not increase due to RPAS operations.** Separation imminent infringements appear when all the different conflict management failed (e.g., VFR IFR conflict management, ATC induced conflict management).	MF 5,6, 7 and 9
SAC#6 **SAC-13-115-006**	**The number of imminent collisions shall not increase due to RPAS operations.** Imminent collisions appear when ATC collision prevention has failed.	MF 4
SAC#7 **SAC-13-115-007**	**The number of NEAR MACs shall not increase due to RPAS operations.** Near MAC appears when all the previous barriers failed, including visual and ACAS warning**.**	MF 3a

Table 1: Safety criteria identified in the SAP

Moreover, the following Figure 1 depicts the simplified Mid- Air Collision AIM with the precursors upon which the SACs are set. These SACs have been anchored into this simplified AIM model:

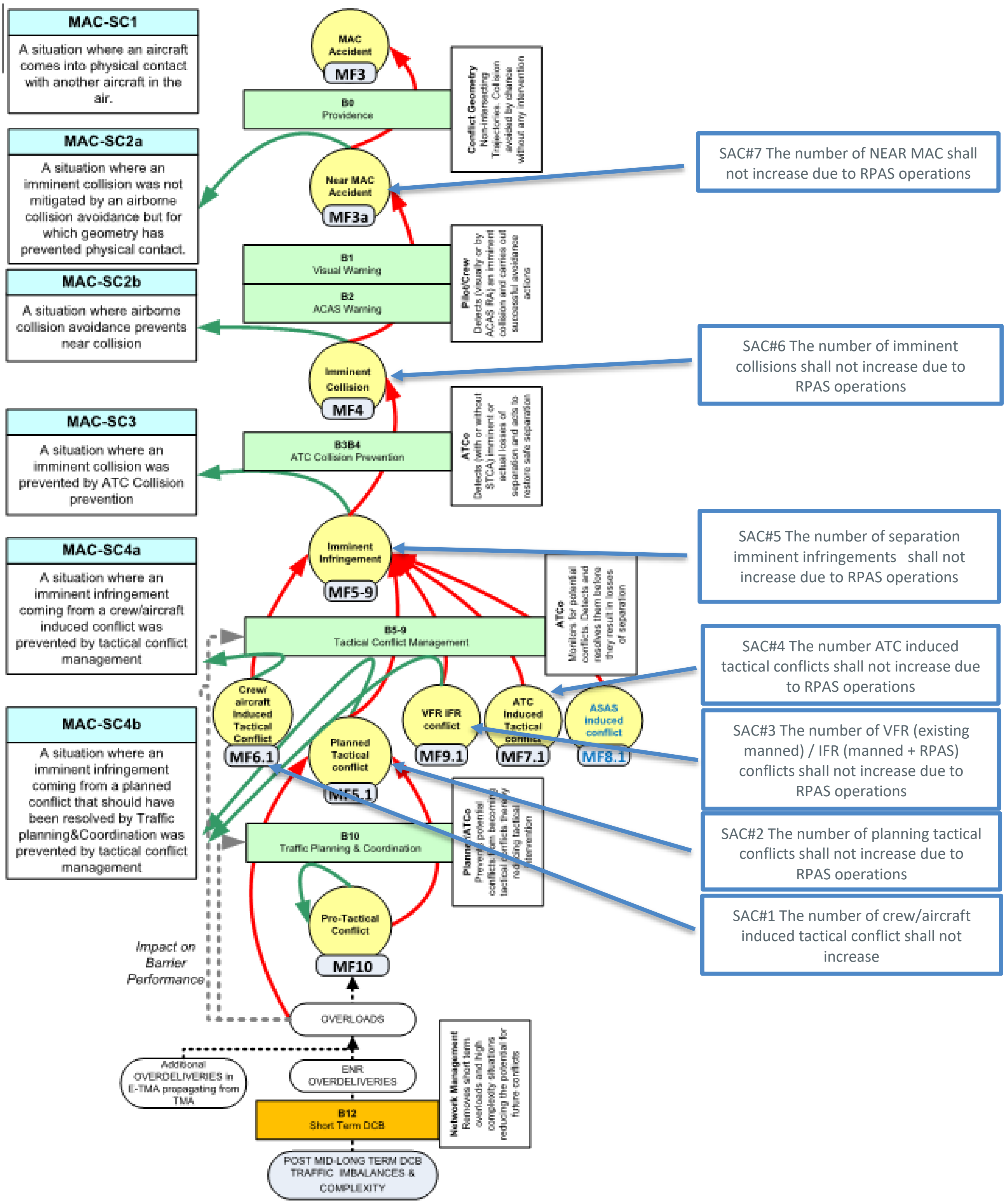

MAC-SC1
A situation where an aircraft comes into physical contact with another aircraft in the air.
MAC-SC2a
A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact.
MAC-SC2b
A situation where airborne collision avoidance prevents near collision
MAC-SC3
A situation where an imminent collision was prevented by ATC Collision prevention
MAC-SC4a
A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management
MAC-SC4b
A situation where an imminent infringement coming from a planned conflict that should have been resolved by Traffic planning&Coordination was prevented by tactical conflict management
Impact on Barrier Performance
MAC Accident
MF3
B0
Providence
Conflict Geometry
Non-intersecting Trajectories. Collision avoided by chance without any intervention
Near MAC Accident
MF3a
B1
Visual Warning
B2
ACAS Warning
Pilot/Crew
Detects (visually or by ACAS RA) an imminent collision and carries out successful avoidance actions
Imminent Collision
MF4
B3B4
ATC Collision Prevention
ATCo
Detects (with or without STCA) imminent or actual losses of separation and acts to restore safe separation
Imminent Infringement
MF5-9
B5-9
Tactical Conflict Management
ATCo
Monitors for potential conflicts. Detects and resolves them before they result in losses of separation
Crew/aircraft Induced Tactical Conflict
MF6.1
Planned Tactical conflict
MF5.1
VFR IFR conflict
MF9.1
ATC Induced Tactical conflict
MF7.1
ASAS induced conflict
MF8.1
B10
Traffic Planning & Coordination
Planner/ATCo
Prevents potential conflicts from becoming tactical conflicts thereby reducing tactical intervention
Pre-Tactical Conflict
MF10
OVERLOADS
Additional OVERDELIVERIES in E-TMA propagating from TMA
ENR OVERDELIVERIES
B12
Short Term DCB
Network Management
Removes short term overloads and high complexity situations reducing the potential for future conflicts
POST MID-LONG TERM DCB TRAFFIC IMBALANCES & COMPLEXITY
SAC#7 The number of NEAR MAC shall not increase due to RPAS operations
SAC#6 The number of imminent collisions shall not increase due to RPAS operations
SAC#5 The number of separation imminent infringements shall not increase due to RPAS operations
SAC#4 The number ATC induced tactical conflicts shall not increase due to RPAS operations
SAC#3 The number of VFR (existing manned) / IFR (manned + RPAS) conflicts shall not increase due to RPAS operations
SAC#2 The number of planning tactical conflicts shall not increase due to RPAS operations
SAC#1 The number of crew/aircraft induced tactical conflict shall not increase

Figure 1: Severity Class Scheme for Mid-air Collision ENR with Solution 115 SAC

Moreover, for each SAC, rationales for nominal and non-nominal situations and safety demonstration strategy are listed in the **Table 2** below.

Safety criteria	SAC#1 – The number of crew/aircraft induced tactical conflict shall not increase (MF6.1) - these conflicts are induced by an event from the RPAS/RP		SAC#2 – The number of planning tactical conflicts shall not increase due to RPAS operations (MF5.1) – these conflicts are induced by an event during the traffic planning and synchronisation at the tactical level		SAC#3 – The number of VFR (existing manned) /IFR (manned + RPAS) conflicts shall not increase due to RPAS operations (MF9.1)		SAC#4 –The number of ATC induced tactical conflicts shall not increase due to RPAS operations (MF7.1)		SAC#5 – The number of imminent infringements shall not increase due to RPAS operations (MF5-9) – these conflicts are induced by a loss of separation between two aircraft		SAC#6 – The number of imminent collisions shall not increase due to RPAS operations (MF4) – these conflicts are induced if ATC collision prevention has failed.		SAC#7– The number of NEAR MAC shall not increase due to RPAS operations (MF3a). Only visual collision avoidance and ACAS warnings remain.	
Nominal/ non- nominal Rationale	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal
RPAS do behave as manned aircraft. Nevertheless, to encompass RPAS specific procedures, they will clearly be identified as unmanned aircraft on ATCO's HMI.	x		x		x		x		x		x		X	
The new procedures and operating methods for nominal situations will be known by both RP and ATCO	x		x				x		x		x		X	
The controller will have the possibility to contact the remote pilot using a direct ground telephone line.		x		x		x		x		x		x		X
The remote pilot operates the RPAS under the basis of suitable recognized IFR license.	x								x		x			

Safety criteria	SAC#1 – The number of crew/aircraft induced tactical conflict shall not increase (MF6.1) - these conflicts are induced by an event from the RPAS/RP		SAC#2 – The number of planning tactical conflicts shall not increase due to RPAS operations (MF5.1) – these conflicts are induced by an event during the traffic planning and synchronisation at the tactical level		SAC#3 – The number of VFR (existing manned) /IFR (manned + RPAS) conflicts shall not increase due to RPAS operations (MF9.1)		SAC#4 –The number of ATC induced tactical conflicts shall not increase due to RPAS operations (MF7.1)		SAC#5 – The number of imminent infringements shall not increase due to RPAS operations (MF5-9) – these conflicts are induced by a loss of separation between two aircraft		SAC#6 – The number of imminent collisions shall not increase due to RPAS operations (MF4) – these conflicts are induced if ATC collision prevention has failed.		SAC#7– The number of NEAR MAC shall not increase due to RPAS operations (MF3a). Only visual collision avoidance and ACAS warnings remain.	
Nominal/ non- nominal Rationale	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal
The relevant information regarding the programmed contingency procedure(s) will be known by the ATCO before the contingency occurs.		x												
The position of the RPAS will be known by the ATCO due to radar information.	x	x	x		x		x		x		x		x	
The new procedures, operating methods (e.g., new transponder code used for C2 link loss) and RPAS systems for non-nominal situations will be known/implemented by RP and ATCO/RPAS		x		x		x		x		x		x		X
Remote pilot will operate the RPAS under the basis of suitable recognized IDE license and be trained to operate the RPAS in case of contingency.		x								x		x	X	

Safety criteria	SAC#1 – The number of crew/aircraft induced tactical conflict shall not increase (MF6.1) - these conflicts are induced by an event from the RPAS/RP		SAC#2 – The number of planning tactical conflicts shall not increase due to RPAS operations (MF5.1) – these conflicts are induced by an event during the traffic planning and synchronisation at the tactical level		SAC#3 – The number of VFR (existing manned) /IFR (manned + RPAS) conflicts shall not increase due to RPAS operations (MF9.1)		SAC#4 –The number of ATC induced tactical conflicts shall not increase due to RPAS operations (MF7.1)		SAC#5 – The number of imminent infringements shall not increase due to RPAS operations (MF5-9) – these conflicts are induced by a loss of separation between two aircraft		SAC#6 – The number of imminent collisions shall not increase due to RPAS operations (MF4) – these conflicts are induced if ATC collision prevention has failed.		SAC#7– The number of NEAR MAC shall not increase due to RPAS operations (MF3a). Only visual collision avoidance and ACAS warnings remain.	
Nominal/ non- nominal Rationale	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal
The planning system and planner controller tools will use RPAS performances data base (e.g., BADA) that will be available to avoid generating additional tactical conflicts.			x	x	x	x	x	x			x	x	X	X
RPAS may be managed as manned aircraft by ATCO applying same conflict management methods/procedure.							x							
ATCO will have the usual tools (e.g., safety net) to detect possible conflicts.							x		x		x	X	X	
Most leisure VFR (which are the majority of infringers) do not fly above FL100.											X *(see section 3.4.1)*	X *(see section 3.4.1)*		
According to ANSP's experience, only a small proportion of infringer VFR cannot be contacted by radio communication											X *(see section 3.4.1)*	X *(see section 3.4.1)*		

Safety criteria	SAC#1 – The number of crew/aircraft induced tactical conflict shall not increase (MF6.1) - these conflicts are induced by an event from the RPAS/RP		SAC#2 – The number of planning tactical conflicts shall not increase due to RPAS operations (MF5.1) – these conflicts are induced by an event during the traffic planning and synchronisation at the tactical level		SAC#3 – The number of VFR (existing manned) /IFR (manned + RPAS) conflicts shall not increase due to RPAS operations (MF9.1)		SAC#4 –The number of ATC induced tactical conflicts shall not increase due to RPAS operations (MF7.1)		SAC#5 – The number of imminent infringements shall not increase due to RPAS operations (MF5-9) – these conflicts are induced by a loss of separation between two aircraft		SAC#6 – The number of imminent collisions shall not increase due to RPAS operations (MF4) – these conflicts are induced if ATC collision prevention has failed.		SAC#7– The number of NEAR MAC shall not increase due to RPAS operations (MF3a). Only visual collision avoidance and ACAS warnings remain.	
Nominal/ non- nominal Rationale	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal
Only one RPAS may be authorized to fly at the same time under the responsibility of one sector, which may reduce the likelihood of encounters between two or more aircraft, all of them suffering a contingency due to C2LL[5].											X[6]	X[6]	X	X
Some manned aircraft are equipped with ACAS system. They will receive Traffic advisory (In solution 115, RPAS is not equipped)													X *(see section 3.4.2)*	X *(see section 3.4.2)*

[5] This statement has been modified, according to the discussions that have taken place within the different safety workshops. It should be interpreted as follows: "Two RPAs under the responsibility of one sector and suffering a C2LL will not have crossing trajectories (in space or in time) at any time during the contingency. Otherwise, only one RPA will operate at the same time under responsibility of one sector".

[6] This SAC includes imminent collision with an infringer not detected neither by the RPAS nor by the ATCO. These rationales should be considered.

Safety criteria	SAC#1 – The number of crew/aircraft induced tactical conflict shall not increase (MF6.1) - these conflicts are induced by an event from the RPAS/RP		SAC#2 – The number of planning tactical conflicts shall not increase due to RPAS operations (MF5.1) – these conflicts are induced by an event during the traffic planning and synchronisation at the tactical level		SAC#3 – The number of VFR (existing manned) /IFR (manned + RPAS) conflicts shall not increase due to RPAS operations (MF9.1)		SAC#4 –The number of ATC induced tactical conflicts shall not increase due to RPAS operations (MF7.1)		SAC#5 – The number of imminent infringements shall not increase due to RPAS operations (MF5-9) – these conflicts are induced by a loss of separation between two aircraft		SAC#6 – The number of imminent collisions shall not increase due to RPAS operations (MF4) – these conflicts are induced if ATC collision prevention has failed.		SAC#7– The number of NEAR MAC shall not increase due to RPAS operations (MF3a). Only visual collision avoidance and ACAS warnings remain.	
Nominal/ non- nominal Rationale	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal
Likelihood of see and avoid action will be reduced at least by 50%. This is due to the loss of "one pair of eyes". Provided that the meteorological visibility allows visual detection of other aircraft.	x												x	x
If Traffic information is provided to RP, the RP could use the MALE RPAS camera to "visually" acquire proximate aircraft- there should be few proximate aircraft in low-mid density..[7]													x	

[7] The remote pilot may be provided in the RPS by a real time situational awareness of the collaborative traffic environment. This would prevent to use the camera or provide additional and more precise information.

Safety criteria	SAC#1 – The number of crew/aircraft induced tactical conflict shall not increase (MF6.1) - these conflicts are induced by an event from the RPAS/RP		SAC#2 – The number of planning tactical conflicts shall not increase due to RPAS operations (MF5.1) – these conflicts are induced by an event during the traffic planning and synchronisation at the tactical level		SAC#3 – The number of VFR (existing manned) /IFR (manned + RPAS) conflicts shall not increase due to RPAS operations (MF9.1)		SAC#4 –The number of ATC induced tactical conflicts shall not increase due to RPAS operations (MF7.1)		SAC#5 – The number of imminent infringements shall not increase due to RPAS operations (MF5-9) – these conflicts are induced by a loss of separation between two aircraft		SAC#6 – The number of imminent collisions shall not increase due to RPAS operations (MF4) – these conflicts are induced if ATC collision prevention has failed.		SAC#7– The number of NEAR MAC shall not increase due to RPAS operations (MF3a). Only visual collision avoidance and ACAS warnings remain.	
Nominal/ non- nominal Rationale	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal	Nominal	Non-nominal
Safety demonstration strategy	RTS Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace		RTS Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace		RTS Questionnaire, analysis of trends at European level, Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace		RTS (questionnaire to ATCO) Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace		RTS Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace		Questionnaires to ATCO Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace		Questionnaires to ATCO Safety assessment and trials feedback for French Air Force RPAS flights in non-segregated airspace	

Table 2: Safety criteria and rationale per nominal and non-nominal situation

3.4.1 Study of infringement occurrences in Airspace classes A to C.

With the aim of evaluating the risk that recreation VFR flights could pose, while accommodating RPAS flights in controlled airspace classes A to C and above FL100, Solution 115 team has tried to gather EU aviation safety data regarding controlled airspace incursions.

- **EVAIR (EUROCONTROL voluntary ATM incident reporting):**
  No occurrences registered for airspace infringements that involved VFR flights. Nevertheless, EVAIR does not normally get VFR recreation flights through the voluntary reporting stream.

As an example of airspace infringements that involve VFR flights, the following information has been provided by NATS (UK):

- A very small proportion of reported infringements are above FL100 (0.1% in 2019, 0.5% since), all infringing aircraft above FL100 were Mode C equipped.
- Over the period 01/01/2020 – 30/06/2022:
  - 1608 infringements reported.
  - 37 infringements reported above FL100 (including Danger Area infringements and infringements by commercial aircraft under ATC service).
    - 8 infringements of controlled airspace (excluding Danger Areas) by aircraft not under ATC service.
    - One Class C airspace, 6 Class A, one not specified.
    - All infringing aircraft had Mode C
- In 2019 (pre-pandemic traffic patterns):
  - 909 infringements
  - 10 over FL100 (including Danger Area infringements and infringements by commercial aircraft under ATC service),
  - Only 1 by civil GA aircraft
    - Class A airspace
    - Mode C equipped.

According to the data compiled so far, it can be concluded that airspace infringements by VFR flights in controlled airspace classes A to C and above FL100 are rare events.

3.4.2 Detection and avoidance systems (DAA) in RPAs.

ICAO defines DAA as the capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action.

DAA concerns two specific areas:

- Pilot's role in airspace classes where pilots have an explicit separation responsibility role in using see / sense and avoid conflicting traffic. *These airspace classes are not included in the scope of Solution 115.*
- Last resort collision avoidance, which for certain aircraft categories, in the current civil airspace, is supported by the ACAS system.

In solution 115, RPAS are not equipped with Detection and Avoidance Systems.

In current aviation, there is already a comparative case where aircraft fly with no collision avoidance systems on-board. According to "COMMISSION REGULATION (EU) 2016/583 of 15 April 2016 amending Regulation (EU) No 1332/2011 laying down common airspace usage requirements and operating procedures for airborne collision avoidance": *turbine-powered aeroplanes, with a maximum certificated take-off mass (MCTOM) of more than 5700 kg or authorised to carry more than 19 passengers are required to be equipped with a new software version 7.1 of the airborne collision avoidance system (ACAS II) to avoid mid-air collision*. Therefore, small/light aircraft (<5.7 T, < 19 pax.) have no regulatory obligation to be equipped with this system.

The existing situation means that both equipped and non-equipped aircraft can operate simultaneously in the same airspace. Solution 115-compliant RPAS will therefore be an additional non-equipped aircraft type within a pre-existing category.

Nevertheless, to mitigate possible conflicts, it must be taken into account that, in the general scope of IFR flights in Class A-C airspace:

- All pilots, including pilots of RPAS, have a level of traffic awareness through the "party-line radio communications, that is, ability to listen, or at least hear, communications between other aircraft and ATC.

- RPAS are expected to be equipped with a transponder, so that they are electronically visible to ATC and to other ACAS equipped airspace users.

4 Safety specification at ATS service level

The purpose of this section is to derive the Safety Requirements at Service level for the ATS operational Solution.

The Safety Requirements at ATS Service level (SRS) specify the desired safety behavior of the change at its interface with the ATS operational context considering normal and abnormal conditions of the context (success approach) and the failures of the functional system (failure approach). They are placed on the services of the Solution functional system that are changed or affected by the change (through change in behavior or through new interactions introduced).

The assumptions, safety issues and limitations identified during the service specification process are recorded in Appendix I.

4.1 Overview of activities performed

This section addresses the following activities:

- derivation of Safety Requirements at ATS Service level (SRS) in view of mitigating the relevant risks inherent to aviation in normal conditions of operation– section 4.2
- assessment of the adequacy of the ATS operational services provided by the Solution under abnormal conditions of the Operational Environment & derivation of necessary SRSs – section 4.3
- assessment of the adequacy of the ATS operational services provided by the Solution in the case of internal failures and mitigation of the Solution functional system-generated hazards through derivation of SRSs – section 4.4.
- verification of the operational safety specification process (mainly about obtaining Backing evidence from the properties of the processes by which Direct Evidence was gleaned) – section 4.5.

4.2 Mitigation of Risks Inherent to Aviation – Normal conditions

The purpose of this section is to present the Safety Requirements at ATS Service level (SRS) derived for Normal conditions of operation following **Guidance F of Safety Reference Material.**

These Safety Requirements at the ATS Service level (SRS) show the desired safety behaviour of the change at its interface with the operational context considering normal conditions. Most of the SRS have been derived from the relevant Uses Cases described in the OSED, and also using EATMA Models at operational specification level (NOV-5 diagrams) to complete them.

Use case (NOV-5)
IFR RPAS Pre-Flight Operations (Preparation and Filing of RPAS Flight Plan)
IFR RPAS Nominal Operations

Table 3: Use Cases related to normal conditions of operation

As a result, a complete set of SRSs is provided in order to ensure satisfaction of the Safety Criteria in Normal conditions of operation.

4.2.1 Safety Requirements at ATS Service level (SRS) for Normal conditions of operation

In this section, a set of Safety Requirements of ATS Service level (SRS) for normal conditions of operation is presented. The complete analysis is included in Appendix B, while the following tables display a summary of the most relevant information.

First of all, the ATS operational services potentially impacted by the change in the relevant operational environment are compiled and related to the hazards inherent to aviation (identified in Appendix A.1[8]) in order to address and mitigate them.

ID	ATS Operational Service	Hazards inherent to aviation
ATS-01	Flight Plan filling, revision and validation	**-**
ATS-02	Radio and radar contact and monitoring	**-**
ATS-03	Conflict detection and resolution	**Hi#1, Hi#6, Hi#8**
ATS-04	Transfer flight control between ATS Units	-

Table 4: ATS Operational services potentially impacted and Hazards inherent to aviation

On the other hand, Table 5 presents the consolidated list of the SRS for normal conditions of operation that have been derived in Appendix B.

SRS ID	SRS for Normal conditions of operation	Related SAC
SRS 001a	The RP shall initiate contact with the relevant ATS Unit.	SAC#1
SRS 001b	The RP shall provide the ATCO in initial radio contact with each sector with the standard contact information regarding identification including RPAS, next route element(s)/flight level and minimum elements of the pre-programmed C2LL contingency trajectory	SAC#1
SRS 002	The ATS Unit shall acknowledge the RP's first notification and assume the control of RPAS flight.	SAC#2
SRS 003a	The ATS Unit shall monitor the RPAS flight trajectory through cooperative secondary radar surveillance data.	SAC#2
SRS 003b	The ATS Unit shall use surveillance data to monitor the traffic (manned and unmanned), in order to apply separation minima between aircraft. The objective is for ATS Unit to apply identical separation minima with the RPAS.	SAC#2

[8] These hazards inherent to aviation were identified as part of the activities conducted in order to develop the Safety Assessment Plan. They were selected from the list available in the "Guidance to Apply SESAR Safety Reference Material" [4].

SRS ID	SRS for Normal conditions of operation	Related SAC
SRS 004a	The ATS Unit shall detect the possible conflicts with RPAS flight trajectory	SAC#2
SRS 004b	The ATS Unit shall issue clearances and provide instructions to RPAS for resolution of conflicts (Vector/ Heading/ Altitude/ Speed instructions).	SAC#4
SRS 005	Upon obtaining a new clearance/instruction, RPS Operations shall verify compatibility of existing pre-programmed C2LL contingency trajectory, and if necessary, re-program a revised C2LL contingency trajectory.	SAC#1
SRS 006a	If a C2LL contingency trajectory is re-programmed/revised, RPS Operations shall provide information of the revised C2LL trajectory to ATCO, at or after clearance/instruction read-back.	SAC#1
SRS 006b	RPS Operations shall modify RPAS navigation according to the new instructions provided by ATS Unit.	SAC#1
SRS 007	RPS Operations shall continue to monitor the RPA trajectory during nominal flight.	SAC#1
SRS 008	Transferring ATS Unit (civil) shall transfer radio and radar RPAS flight contact to accepting ATS Unit.	SAC#4
SRS 009	Accepting ATS Unit (civil or military) shall assume radio and radar control of RPAS flight and issue ATC clearances and instructions.	SAC#4
SRS 010a	RPS Operations shall contact accepting ATS Unit *(and also provide the ATCO in initial radio contact with C2LL behaviour information → see SRS 001b)*	SAC#1
SRS 010b	RPAS shall enter the new sector through the instructed point and after the RP establishes contact with the relevant accepting ATS Unit	SAC#1

Table 5: List of SRS (functionality & performance) for normal conditions of operation

4.2.2 Additional SRS related to adjacent airspace or neighbouring ATM Systems

No additional SRS related to adjacent airspace or neighbouring ATM Systems have been detected in relation with Solution 115.

4.3 Mitigation of Risks Inherent to Aviation - Abnormal conditions

The purpose of this section is to present the Safety Requirements at ATS Service level (SRS) derived for Abnormal conditions of operation.

The SRS in this section refer to the ability of the Solution to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the Solution functional system, that might be encountered relatively infrequently (i.e. abnormalities of the context in which the Solution 115 functional system is intended to operate.

4.3.1 Identification of Abnormal Conditions

The abnormal conditions that are relevant for the Solution context can be described as follows:

- ABN 1. RPAS technical system failure: C2 Link Loss (C2LL) and associated ATC Voice loss.
- ABN 2. RPAS Emergency Operations: Engine failure emergency.
- ABN 3. Bad weather encounter or sudden deterioration of weather conditions.
- ABN 4. Wake turbulence encounter.

NOTE: Both the list of abnormal operational conditions and the list of system-generated hazards include some system failures.

Nevertheless, the following rules have been applied in order to distinguish them:

- *Non-nominal in-flight situations around contingency/ emergency procedures are considered as abnormal operational conditions.*
- *Failures of the systems required when accommodating IFR RPAS in airspace classes A to C are considered as failure mode or hazards (see section 0)*

4.3.2 Safety Requirements at ATS Service level (SRS) for Abnormal conditions of operation

The following table presents the consolidated list of the SRS for abnormal conditions of operation that have been derived in Appendix C.

SRS ID	Description	Related SAC
SRS 011	ATS Unit shall be informed of the RPAS C2LL through a specifically defined SSR code automatically set by RPA Operations. *NOTE: RPAS is pre-programmed to squawk a specific SSR code as soon as C2LL is detected.*	SAC#1
SRS 012	Follow-up of C2LL Contingency shall be coordinated between ATS Unit and RPS Operations through a backup audio (telephone or direct point-to-point line, if equipped) to exchange useful information, in particular, the remote pilot shall provide details of the C2LL trajectory/behaviour, and the ATCO shall provide information regarding the next ATC sector.	SAC#1 SAC#2
SRS 013	ATS Unit shall monitor traffic and apply an adapted separation strategy as deemed necessary by ATCO to separate the RPA C2LL trajectory from other (manned) aircraft trajectories.	SAC#2
SRS 014	RPAS shall fly the contingency procedure. This contingency procedure shall be pre-programmed in Flight Plan, or re-programmed in-flight as necessary, if a vector/heading/altitude/speed instruction has been given by the ATS Unit.	SAC#1
SRS 015	RPS Operations shall monitor the C2 link state trying to re-establish it (if possible, with the available RPS means).	SAC#1
SRS 016	If the C2L is never re-established, the RPAS shall continue flying its pre-programmed C2 link loss (C2LL) contingency trajectory. This includes:	SAC#1

SRS ID	Description	Related SAC
	- Returning to flight plan after a set time, - Flying until the DIVERSION pre-programmed waypoint, from where it shall continue flying to the pre-programmed C2LL destination airfield, that the operator will have chosen during pre-programming (an alternate aerodrome, or the departure one, or the original final destination).	
SRS 017	If the C2L is re-established, RPS Operations shall detect it and inform ATS.	SAC#1
SRS 018	If the C2L is re-established, RPS Operations shall revert to previous transponder code (SQUAWK). *NOTE: Reversion to the original (previous) transponder code is on ATCO instruction (thus not automated): if C2L is working, the RP can change the squawk as often as required.*	SAC#1
SRS 019	If the C2L is re-established, RPS Operations shall use the frequency communicated at telephone coordination to contact the appropriate ATS Unit.	SAC#1
SRS 020	RPA Operations shall determine the engine status in order to analyse the impact of engine loss.	SAC#1
SRS 021	RPS Operations shall broadcast emergency state through the emergency frequency to all concerned traffic.	SAC#1
SRS 022	RPAS shall follow the Emergency Flight Plan to guarantee the highest level of safety. Use of the "Safest Shortest" principle to make that decision.	SAC#1
SRS 023	RP shall contact/coordinate with the ATS Unit to declare the flight path to terminate the flight in the worst-case scenario, that is, where the emergency destination is not achievable.	SAC#1 SAC#2
SRS 024	RPAS shall monitor Emergency Flight in order to: • control the trajectory and adhere to declared Emergency Flight Plan. • alert ATCO when a deviation is observed that cannot be mitigated by RPS Operations.	SAC#1
SRS 025	ATS Unit shall coordinate termination of the emergency RPA flight with the State/military authority or civil authority in case of Military/State terminal area (Airfield / Ditching area) or in case of entering uncontrolled area all along the flight.	SAC#2
SRS 026	ATS Unit shall clear the path for RPAS trajectory and provide separation of surrounding traffic until RPA enters CTR.	SAC#4
SRS 027	ATS Unit shall maintain the coordination with Airport Ops Support that will host the termination action.	SAC#2
SRS 028	ATS Unit at arrival aerodrome shall clear its airspace and runways from any traffic, including ground vehicles, which may endanger the operation of the arriving emergency RPA.	SAC#4

Co-funded by the European Union

SRS ID	Description	Related SAC
SRS 029	RP shall be able to deal with possible sudden deterioration of weather conditions during the flight. This includes requesting the ATCO a lateral or vertical deviation to avoid the area.	SAC#1
SRS 030	ATS Unit shall be able to manage situations related to sudden deterioration of weather conditions.	SAC#4
SRS 031	RP shall be able to deal with possible wake turbulence encounters during the flight.	SAC#1
SRS 032	ATS Unit shall be able to manage situations related to wake turbulence encounters.	SAC#4

Table 6: List of additional SRS for Abnormal conditions of operation

4.4 Mitigation of System-generated Risks (failure conditions)

The purpose of this section is to present the Safety Requirements at ATS Service level (SRS) associated with the operational hazards (caused by internal failures of the Solution functional system). The SRS provided in this section complete the safety specification of the Solution at operational service level, providing the adequate mitigation against the possible adverse effects that failures internal to the Solution functional system might have upon the provision of the relevant ATS operational services. Two types of SRS are to be included here:

- Additional SRS (functionality & performance) to mitigate against operational hazard effects (protective mitigation)
- SRS addressing integrity/reliability in order to limit the maximum allowable frequency of the Solution' functional system-generated operational hazards.

The SRS here might be associated either with new operational hazards introduced by the Solution or with operational hazards existing in Reference operations, but which are modified by the Solution.

NOTE: Both the list of abnormal operational conditions and the list of system-generated hazards include some system failures. Nevertheless, the following rules have been applied in order to distinguish them:

- *Non-nominal in-flight situations around contingency/ emergency procedures are considered as abnormal operational conditions (see section 4.3).*
- *Failures of the systems required when accommodating IFR RPAS in airspace classes A to C are considered as failure mode or hazards.*

4.4.1 Operational Hazards Identification and Analysis

In this section, the consolidated results from the hazard identification, analysis and HAZID workshop are presented. The detailed working tables, results and HAZID workshop participation are included in Appendix D).

For each identified operational hazard, it is shown:

- the assessed operational effect,

- the mitigations taken into account for assessing the operational effect (protecting against effect propagation) with a reference to existing safety barriers (as per the relevant AIM model), to existing SRS (functionality & performance) or, if applicable, to new derived SRS (functionality & performance).
- the assessed severity of the most probable effect from hazard occurrence as per the relevant AIM-based Severity Classification Scheme(s) (SCS) from Guidance G.3 of the “Guidance to Apply SESAR Safety Reference Material” [4].

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
OH 01a	Incorrect preparation of a possible C2LL contingency. On first radio contact, or after receiving new instructions from ATCO, the RP: • does not communicate the contingency procedure to ATC, or • communicates incorrect contingency procedure information to ATC.	If a C2LL does not occur: • Light increase of workload of ATCO and RP in order to correct the mistake.	No communication: **M1**. ATCO needs to recognize a RPAS (**SRD 003A:** ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)) **M2.** ATCO detects the lack of information related to the C2LL behaviour and requests the RP the missing information (Current mitigation means: ATCOs are trained to request information, if necessary, from the RP flying in their sectors). **Assumption 005** **M3**. The ATCO has a means of recording information related to the contingency procedure. **Assumption 005** **M4.** There will always be an additional/backup pilot in the Remote Pilot Station to cross-check. (**SRD_candidate_001:** A team of pilots shall be always available to manage the RPA, and one will take the RP position whenever necessary (REQ-PJ13.115-SPRINTEROP-0350)). Incorrect communication: **M4.** There will always be an additional/backup pilot in the Remote Pilot Station to cross-check. (**SRD_candidate_001:** A team of pilots shall be always available to manage the RPA, and one will take the RP position whenever necessary (REQ-PJ13.115-SPRINTEROP-0350)). **M5**: RP can recheck programmed behaviour at any time before a C2LL occurs (skill included within RP's training). *Only valid in case the information in the system is wrong. If the RP rechecks it and detects the mistake, they shall contact the ATCO again to provide the correct data (for example, the diversion point is hundreds of NM away: named WPTs – more than one with the same name (different locations) can exist in the NAV database, and thus inadvertently selected in the nav system programming).* **Assumption 006b**	MAC_SC04b
OH 01b	Incorrect preparation of a possible C2LL contingency: RP does not (correctly) reprogram the C2LL contingency procedure in the RPA system.	If a C2LL does not occur: • Light increase of workload of the RP in order to correct the mistake.	**M5**: RP can recheck programmed behaviour at any time before a C2LL occurs (skill included within RP's training). **Assumption 006b** **M13:** RP can ask ATCO to confirm if the actual C2LL trajectory conforms with the information provided to ATCO. **Assumption 006a**	MAC_SC04b
OH 02	Inconsistency between the programmed C2LL contingency procedure and	If the occurring C2LL inconsistency is not detected:	**M1**. ATCO needs to recognize a RPAS (**SRD 003A:** ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070))	MAC_SC04a

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
	the ATCO expectations of the RPAS trajectory.	• Increase of workload of ATCO to manage/separate RPAs at a later stage. • Increase of workload of the RP in order to check and transmit the correct information. • Unknown/unexpected RPA flight trajectory in case of C2LL. Possible loss of separation between the RPA and other aircraft, including possible VFR intruders. • Possible conflict between two RPAS both in a C2LL situation.	**M2.** ATCO detects the lack of information related to the C2LL behaviour and requests the RP the missing information (Current mitigation means). **Assumption 005** **M3**. The ATCO has a means of recording the information related to the contingency procedure. **Assumption 005** **M4.** There will always be an additional/backup pilot in the Remote Pilot Station to cross-check. (**SRD_candidate_001:** A team of pilots shall be always available to manage the RPA, and one will take the RP position whenever necessary (REQ-PJ13.115-SPRINTEROP-0350)) **M5**: RP can recheck programmed behaviour at any time before a C2LL occurs (skill included within RP's training). **Assumption 006b** If a C2LL occurs without the inconsistency being detected, the following additional mitigations are also available: **Assumption A001:** During the accommodation phase, RPAS will operate in medium/low traffic density environments. **Assumption A001:** During the accommodation phase, all traffic is known and cleared into the controlled airspace **Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M6.** ATCO could apply larger separation to RPAS that squawks the designated C2LL code (**SRD 017**: ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS. (REQ-PJ13.115-SPRINTEROP-0150)). **M7.** RPAS FL is limited in such a way that reduces chances to have traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders) (**SRD_candidate_002:** RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040)) *(this makes the severity decrease from SC03 to SC04b)*.	

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
			M8. RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M10.** In the short term, there is no change in the RPAS trajectory. The ATCO will have time to get the correct information from the RP via the alternative communication mean. (**SRD 013:** The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260)) **M11a**: In the medium/long term, the ATCO will be able to detect a deviation in the execution of the C2LL trajectory through active surveillance (SSR code and radar available). Via the alternative communication means, the ATCO will be able to get feedback from the RP about the status of the C2L and/or about the procedure pre-programmed or re-programmed so that they can check if it is the expected one. (**SRD 006:** ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)) **M12:** ATCO are trained to face non-nominal situations involving RPA traffics (**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)) **Issue I001:** In case C2LL occurs just after vectoring instructions there might be no sufficient time for ATCO to fully check the details of the contingency procedure with the RP (currently 2 minutes – To be validated). *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	
OH 03	Malfunction of the C2 link.	Increase of workload of ATCO to manage other	**Assumption A006:** It is considered that RPs are already trained with regard to the basic procedures and way of operating. Therefore, actions such as:	MAC_SC03

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
		traffic around RPA C2LL trajectory Increase of workload of RP to manage the C2LL situation. RPA is no longer controllable by the RP. The RP loses awareness of the RPA's position. Possible conflict with other aircraft. Possible conflict between two RPAS both in a C2LL situation under the responsibility of one sector (if more than one RPAS is considered under control of each sector).	• the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)*, or • the detection of the C2LL (loss of data with the RPA), are considered within RP's current skills. **Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M14.** RPA makes sure that the malfunction is not temporary. RPA only sets code when malfunction is confirmed: decision time implemented (existing RPAS feature / mitigation). **Assumption 006b** **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M15.** Availability of a predictable C2LL trajectory pre-programmed/re-programmed to take into account latest conditions. The trajectory is always available in RPA and is automatically activated if C2LL condition detected. (**SRD 009:** RP shall always pre-program RPA with a C2LL trajectory that shall be automatically triggered and flown when the RPAS goes into a C2LL state (REQ-PJ13.115-SPRINTEROP-0310)) **M6.** ATCO could apply larger separation to RPAS that squawks the designated link loss code (**SRD 017**: ATC shall be able to manage other traffic around RPA specific RPA C2LL trajectory: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150)). **M11b.** The ATCO monitors the traffic continuously and will be able to detect possible deviations or issues related to the RPA. (Current mitigation means). **Assumption 005** **M16a**: Only one RPA will operate at the same time under responsibility of one sector. **M16b:** In very specific and limited situations in which RPAS demand is to operate in pairs, the two RPAs shall not have crossing C2LL trajectories (in space or in time) at any time during the	

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
			contingency – this requires C2LL trajectories strategic-agreement between RPAS operator and ANSP. (**SRD 016:** Only one RPAS shall be authorized to fly at the same time under responsibility of one sector. In those specific cases in which two RPAS are inevitably operating under the responsibility of the same sector (demand of RPAS operating in pairs, collapsed sectors during the period of flight of the RPAS, etc.), the RPAS operator (single operator for the two RPAS) shall guarantee through strategic-agreement with the ANSP that the two RPAs will not have crossing trajectories (in space or in time) at any time during a possible C2LL contingency. Moreover, as the RP will be providing the C2LL behaviour at initial contact, the ATCO can also check that the C2LL behaviour of the two RPAS are not in conflict, which is assumed to generate negligible additional planning workload. (REQ-PJ13.115-SPRINTEROP-0050)) **M12:** ATCO are trained to face non-nominal situations involving RPA traffics (**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)) *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings*	
OH 04	Malfunction of RPA system: the RPA system fails to initiate the pre-programmed/re-programmed contingency procedure once the C2LL occurs or starts/follows the wrong one.	Increase of workload of ATCO and RP to manage the RPA. Increase of coordinations between the ATCO and the RP. Unknown/unexpected RPA flight trajectory. Possible loss of separation between the RPA and other aircraft.	**Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M17.** Ensure that the pre-programmed trajectory equipment performance and integrity standards meet at least the navigation requirements in the targeted class of airspace. (**SRD 004:** RPAS shall be able to navigate during flight in a structured airspace with performances and capabilities associated with the airspace, including the C2LL trajectory: • Positioning aids (GNSS, inertial); • AIRAC cyclic navigation data (ATS routes, waypoints);	MAC_SC04a

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
			- RNAV required in the class A-C airspace environment (RNAV5 En-Route / RNAV1 Terminal); (REQ-PJ13.115-SPRINTEROP-0090)) **M6.** ATCO could apply larger separation to RPAS that squawks the designated C2LL code (**SRD 017**: ATC shall be able to support the specific RPAS contingency procedures: - Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150)). **M8.** RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M11a**: In the medium/long term, the ATCO will be able to detect a deviation in the execution of the C2LL trajectory through active surveillance (SSR code and radar available). Via the alternative communication means, the ATCO will be able to get feedback from the RP about the status of the C2L and/or about the procedure pre-programmed or re-programmed so that they can check if it is the expected one. (**SRD 006:** ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)) *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	
OH 05	The ATS Unit fails to integrate the established procedure for the loss of C2L of an RPAS in the	Increase of workload of ATCO to manage traffic.	**Assumption 005.** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/ operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the managing of	MAC_SC04b

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
	management of the other traffic.	Increase of coordinations between the ATCO and the RP. Increase of separation actions from the ATCO to other pilots of manned aircraft. Possible loss of separation between the RPA and other aircraft.	emergency/contingency-related situations in which manned traffic have particular behaviour is within ATCO's current skills. **Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M18.** RP provides information to the ATCO prior to contingency (**SRD 002:** RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)). **M19:** The trajectory in the RPA is programmed, so it is fixed and predictable (**SRD 002: :** RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)) **M3**. The ATCO has a means of recording the information related to the contingency procedure. **Assumption 005** *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	
OH 06	The RPA fails to reach the programmed landing location.	Landing with risk to ground assets.	**Assumption A005.** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that coordinating the contingency management with the different actors (not only RP, but also State Authority / Civil Authority, and Airport/ Airport Operations) is similar as for manned aviation and within ATCO's current skills. **Assumption A006.** It is considered that RPs are already trained with regard to the basic procedures and way of operating. Therefore, the application of procedures/operating methods for non-nominal situations is within RP's current skills (no additional training because of flying in GAT). The RPA behaves / is controlled in a similar way than manned aircraft, taking into account the limitations of RPAs (for example, limited flying time, which will reduce the options for the landing).	MAC_SC04b

ID	Operational Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*
			M20. The RP takes into account the current situation, and RPAS characteristics including emergency limited endurance when pre/re-programming a C2LL trajectory & landing destination. **Assumption 010**	
OH 07	Loss of Remote Pilot situational awareness	Increase of workload of RP to manage the RPA. Increase of workload of ATCO to support RP. RP incorrectly complies with the instructions received from the ATS Unit. Unknown/unexpected RPA flight trajectory. Possible loss of separation between the RPAS and other aircraft, including possible VFR intruders.	**Assumption A001:** During the accommodation phase, RPAS will operate in medium/low traffic environments. **Assumption A001:** During the accommodation phase, all traffic is known and cleared into the controlled airspace. **M21.** RP has equivalent information in their remote cockpit to manned aircraft (for similar aircraft types and environmental conditions) (Current mitigation means) **Assumption 007** **M7.** RPAS FL limited such as to reduce chances to have traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders) (**SRD_candidate_002:** RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040)) *(this makes the severity decrease from SC03 to SC04b)*. **M8.** RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M11b.** The ATCO monitors the traffic continuously and will be able to detect possible deviations or issues related to the RPA. (Current mitigation means). **Assumption 005** *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	MAC_SC04b

Table 7: Operational Hazards and Analysis

4.4.2 Safety Requirements at ATS Service level (SRS) associated to failure conditions

There are additional SRS (functionality & performance) associated to failure conditions that have been derived during the operational hazard assessment:

SRS ID	Additional Safety Requirements at ATS Service level *(functionality & performance)*	Mitigated Operational Hazard
SRS 033	There will always be an additional/backup pilot in the Remote Pilot Station to cross-check	OH 01a & OH 02
SRS 034	RPAS FL shall be limited such as to reduce chances to have VFR traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders)	OH 02 & OH 07
SRS 035	RPAS speed shall be limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn	OH 02 & OH 04 & OH 08
SRS 036	The pre-programmed trajectory equipment performance and integrity standards shall meet at least the navigation requirements in the targeted class of airspace	OH04

Table 8: Additional SRS (functionality & performance) to mitigate operational hazards

On the other hand, the SRS (integrity and reliability) associated to failure conditions are defined. In order to do so, the method included in the Guidance E of the "Guidance to apply SESAR Safety Reference Material" is followed. A quantitative definition of the SRSs integrity is defined considering the equation:

$$SRS = \frac{MTFoO_{relevant\_severity\_class}}{N \times IM}$$

Where:

- MTFoO (Maximum Tolerable Frequency of Occurrence) is associated to the severity class of the Operational Hazard, according to the maximum tolerable frequency of occurrence for each severity class related to the MAC AIM for En-route and TMA included in the SRM.
- N is the number of hazards for the severity class included in the SRM.
- IM is the Impact Modification Factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard. For the OH within Solution 115, this IM is assumed to be 1.

Co-funded by the European Union

SRS ID	Safety Requirements at ATS Service level *(integrity/reliability)*	Related Operational Hazard	Severity & IM
SRS 037a	The frequency of an event in which the RP does not communicate the contingency procedure to ATC shall be no more than 1e-4 per Flight Hour	OH 01a	MAC_SC04b IM=1
SRS 037b	The frequency of an event in which the RP communicates incorrect contingency procedure information shall be no more than 1e-4 per Flight Hour	OH 01a	MAC_SC04b IM=1
SRS 038	The frequency of an event in which the RP does not (correctly) pre- and re-program the C2LL contingency procedure in the RPA system shall be no more than 1 e-4 per Flight Hour.	OH 01b	MAC_SC04b IM=1
SRS 039	The frequency of an inconsistency between the programmed C2LL contingency procedure and the ATCO expectations of the RPAS trajectory shall be no more than 3,3 e-5 per Flight Hour.	OH 02	MAC_SC04a IM=1
SRS 040	The frequency of a malfunction of the C2 link shall be no more than 4 e-6 per Flight Hour.	OH 03	MAC_SC03 IM=1
SRS 041	The frequency of a RPAS failure to initiate the pre-programmed/re-programmed contingency procedure once the C2LL occurs or starts/follows the wrong one, shall be no more than 3,3 e-5 per Flight Hour.	OH 04	MAC_SC04a IM=1
SRS 042	The frequency of an ATS Unit failure to integrate the established procedure for the loss of C2L of an RPAS in the management of the other traffic shall be no more than 1 e-4 per Flight Hour.	OH 05	MAC_SC04b IM=1
SRS 043	The frequency of an RPA failure to reach the programmed landing location shall be no more than 1 e-4 per Flight Hour.	OH 06	MAC_SC04b IM=1
SRS 044	The frequency of a loss of Remote Pilot situational awareness shall be no more than 1 e-4 per Flight Hour.	OH 07	MAC_SC04b IM=1

Table 9: Safety Requirements at Service level - integrity/reliability

4.5 Process assurance of the Safety Specification at ATS Service level

The different topics covered in this section have been developed by the safety team and reviewed/validated by the multidisciplinary team of experts working in Solution 115, during:

- PJ13-W2-115_SAR_Workshop #01 (19/11/2021): The aim of this meeting was to review the four UCs included in the OSED from a safety perspective, to validate a list of Safety Requirements at Service level (SRS) related to both normal and abnormal conditions of operation (More information available in: https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F27713654).
- PJ13-W2-115_SAR_Workshop #02 (14/01/2022): The aim of this meeting was to work on the failure conditions of operation through a hazard identification session. (More information available in: https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F27998203).
- PJ13-W2-115_SAR_Workshop #03 (07/02/2022): The aim of this meeting was to continue working on the failure conditions of operation through a hazard identification session. (More available in: https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F28491054).

5 Safe Design of the Solution functional system

The purpose of this section is to document the Safety Requirements at Design level (SRD) for the ATS operational Solution 115.

The Safety Requirements at Design level (SRD) are design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SACs (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SACs are met). They are placed on the elements of the Solution functional System that are changed or affected by the change (through change in behaviour or through new interactions introduced).

The set of Safety Requirements at Service level (SRS) identified in section 4 enables the derivation of a correct and complete set of Safety Requirements at Design level (SRD), that for Solution 115 refer to rSRD, that is, Safety Requirements at refined designed level (i.e. the final SESAR design specification), for a SAR in V3.

The derived SRDs are consistent with the set of requirements produced by the Solution team in charge of SPR-INTEROP/OSED Part I (Section 4) and completeness and correctness of the full set of SRDs with regards to the satisfaction of the Safety Criteria will be shown in the next sections of this document.

On the other hand, the assumptions, safety issues and limitations identified during the service specification process is recorded in Appendix I.

5.1 Overview of activities performed

This section addresses the following activities:

- introduction of the design model (initial or refined) of the Solution functional system – section 5.2
- derivation of Safety Requirements (functionality & performance) at Design level (SRD) in normal conditions of operation from the SRS (functionality & performance) of section 4.2 and supported by the analysis of the initial or refined design model above - section 5.3
- derivation of Safety Requirements (functionality & performance) at Design level (SRD) in abnormal conditions of operation from the SRS (functionality & performance) of section 4.3 and supported by the analysis of the operation of the initial or refined design under abnormal conditions of operation - section 5.4
- assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution operational hazards (identified at section 4.4) through derivation from SRS (integrity/ reliability) of Safety Requirements (functionality & performance) and Safety Requirements (integrity/reliability) at Design level (SRD)- section 5.5
- realism of the refined safe design (i.e. achievability and “testability” of the SRD) - section 5.6
- safety process assurance at the initial or refined design level - section5.7

5.2 Design model of the Solution functional system

The Design Model of the Solution functional system represents the architecture combining the elements composing the Solution functional system in terms of procedures, human resources and equipment. Therefore, Safety requirements at design level (SRD) are to be placed on those elements.

This high-level architectural representation of the Solution system design is composed by four NSV-4 diagrams:

- Preparation and Filing of RPAS Flight Plan
- IFR RPAS Nominal Operations
- IFR RPAS Contingency Operations
- IFR RPAS Emergency Operations

They can be found in EATMA.

5.2.1 Description of the Design Model

Due to the reason that the safety assessment refers to EATMA models developed by the Project/Solution, no particular description is provided here.

5.2.2 Task Analysis

Human operators' tasks and working methods have been analysed in the "SESAR Solution 115 SPR-INTEROP/OSED for V3 - Part IV - Human Performance Assessment Report" (see [7])

5.3 Deriving Safety Requirements at Design level for Normal conditions of operation

The purpose of this section is to present the Safety Requirements at Design level (SRD) derived for Normal conditions of operation. The derivation of the SRD for Normal conditions of operation is mainly driven by the SRS (functionality & performance) for Normal conditions of operation from section 4.2.

5.3.1 Safety Requirements at Design level (SRD) – Normal conditions of operation

In this section, a set of Safety Requirements at Design level (SRD) for normal conditions of operation is presented. For each SRD, information about the element of the design model on which the SRD is placed, as well as the associated SRS, is provided

The complete analysis is included in Appendix C, while the following table displays a summary of the most relevant information.

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance)	Derived from SRS (ID)
SRD 001 [External: RP training]	RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	**SRS 001a** **SRS 001b** **SRS 005** **SRS 006a** **SRS 006b** **SRS 010a** **SRS 010b**
SRD 002 [Conf RPS; ER ACC/APP ACC]	RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)	**SRS 001b** **SRS 006a** **SRS 010a**
SRD 003A [Info: Air Surveillance Data] [Info: RPAS identification]	ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)	**SRS 002** **SRS 003a** **SRS 003b** **SRS 004a** **SRS 009**
SRD 003B [Info: RPAS identification]	The RP shall add "REMOTE" to the callsign (REQ-PJ13.115-SPRINTEROP-0340)	
SRD 004 [External: coordination between ATS Units (civil-military)]	ATC shall be able to support the accommodation of non-segregated transit GAT RPAS among all other GAT (REQ-PJ13.115-SPRINTEROP-0010)	**SRS 002** **SRS 009**
SRD 005 [External: ATCO training]	ATCO shall be trained and shall be able to apply standard IFR procedures/operating methods to RPAS for nominal IFR situations thus to reiterate requests to RP for expected information (REQ-PJ13.115-SPRINTEROP-0230).	**SRS 003a** **SRS 003b** **SRS 004a** **SRS 004b**
SRD 006 [Info: Air Surveillance Data]	ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300).	**SRS 003a** **SRS 003b** **SRS 004a**
SRD 007 [External: ATC tools]	ATCO shall be able to use usual surveillance and conflict management methods (REQ-PJ13.115-SPRINTEROP-0280).	**SRS 003b** **SRS 004a** **SRS 004b**
SRD 008 [Conf RPS; RPA]	RP shall be able to modify the RPAS navigation according to the new instructions (REQ-PJ13.115-SPRINTEROP-0320)	**SRS 006b**
SRD 009 [Conf RPS; RPA]	RP shall always pre-program RPA with a C2LL trajectory that shall be automatically triggered and flown when the RPAS goes into a C2LL state (REQ-PJ13.115-SPRINTEROP-0310) *NOTE: The RP shall re-program this C2LL trajectory whenever it is required*	**SRS 005**
SRD 010 [External: LoA between ATS Units]	Procedures regarding the transfer of control of RPAS between ATS units in nominal conditions shall be used per the LoA or operations manual in effect (REQ-PJ13.115-SPRINTEROP-0400).	**SRS 008** **SRS 009**

Table 10. Safety Requirements at design level (functionality & performance) satisfying SRS for Normal conditions of operation

5.3.2 Static analysis of the functional system behaviour – Normal conditions of operation

No static analysis of the functional system behaviour – Normal conditions of operation has been developed in relation with Solution 115

5.3.3 Dynamic Analysis of the functional system behaviour – Normal conditions of operation

No dynamic analysis of the functional system behaviour – Normal conditions of operation has been developed in relation with Solution 115

5.3.4 Effects on Safety Nets – Normal conditions of operation

Usual tools (e.g. MTCD) used by ATCOs to detect and/or manage possible conflicts involving manned aircraft will be verified by the ANSP considering RPAS performances-related data and, if necessary, will be tuned for RPAS operating in the airspace, so that they are valid supporting tools.

This includes tools such as conflict detection tools or controller support tools, as long as they are already used within each particular airspace. In those airspaces in which these tools are not used, the existing related safety case to operate under those conditions needs to be verified, with the addition of RPAS (Assumption 008)

The only SRD related to ground-based and airborne safety nets is the following one, which will be analysed within the failure conditions analysis:

Safety Requirement ID [Source]	Safety Requirement at Design level (SRD)	Related to SRS
SRD 011 [Conf RPS; ER ACC/APP ACC] [OSED]	ATC shall be able to use the usual tools as used for manned aircraft to detect possible conflicts (REQ-PJ13.115-SPRINTEROP-0290) *NOTE:* *If used in the particular airspace, these tools include, for example:* • *Medium-Term Conflict Detection (MTCD) probe;* • *Short-Term Conflict Alert (STCA) safety net)*	**A 008**

Table 11: Additional SRD derived by analysis of interaction with safety nets (normal conditions of operation)

5.4 Deriving Safety Requirements at Design level for Abnormal conditions of operation

The purpose of this section is to present the Safety Requirements at Design level (SRD) for Abnormal conditions of operation.

The Safety requirements at design level – SRD (functionality & performance) are derived from the SRS (functionality & performance) which have been identified when mitigating risks inherent to aviation in abnormal conditions of operations (section 4.3).

Contingency procedures associated to the degraded modes of operation in which the functional system might enter as a result of certain abnormal conditions of operation need to be captured as SRD.

5.4.1 Safety Requirements at Design level (SRD) for Abnormal conditions of operation

Table 12. Safety Requirements at design level (functionality & performance) satisfying SRS for Abnormal conditions shows the consolidated list of Safety Requirements at Design level (functionality & performance) for Abnormal conditions of operations derived from the Service Requirements at Service level (SRS) documented in section 4.3.

For each SRD it indicates the element of the design model on which the SRD is placed, as well as the associated SRS. If necessary, an indication of the correspondence with the requirement from SPR-INTERP/OSED Part I is provided.

The detail of the derivation process is included in Appendix F

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance) for abnormal operation	Derived from SRS (ID)
SRD 002 [Conf RPS; En-route/Approach ATC]	RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)	**SRS 011**
SRD 012 [Conf RPA]	RPA shall be able to automatically provide specific C2 link loss transponder code and to maintain it active during C2 link loss (REQ-PJ13.115-SPRINTEROP-0140)	**SRS 011**
SRD 013 [Conf RPS; En-route/Approach ATC]	The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260). *RP (resp. ATCO) will request ATCO (resp. RP) to confirm by telephone that the message is well understood, and the ATCO will recontact RP if the actual RPAS behaviour contradicts the expected behaviour.*	**SRS 011** **SRS 012**
SRD 014 [Conf RPA]	A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120).	**SRS 012**
SRD 015 [External: ATCO training]	ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250).	**SRS 013** **SRS 030** **SRS 032**

Co-funded by the European Union

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance) for abnormal operation	Derived from SRS (ID)
SRD 016 [External: pre-condition]	Only one RPAS shall be authorized to fly at the same time under responsibility of one sector In those specific cases in which two RPAS are inevitably operating under the responsibility of the same sector (demand of RPAS operating in pairs, collapsed sectors during the period of flight of the RPAS, etc.), the RPAS operator (single operator for the two RPAS) shall guarantee through strategic-agreement with the ANSP that the two RPAs will not have crossing trajectories (in space or in time) at any time during a possible C2LL contingency. Moreover, as the RP will be providing the C2LL behaviour at initial contact, the ATCO can also check that the C2LL behaviour of the two RPAS are not in conflict, which is assumed to generate negligible additional planning workload. (REQ-PJ13.115-SPRINTEROP-0050)	**SRS 013**
SRD 017 [Conf ER ACC/APP ACC]	ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150).	**SRS 013** **SRS 016**
SRD 018 [Conf RPA]	RPAS shall be able to identify its emergency status and to execute the emergency procedure associated with the severe failure situation (REQ-PJ13.115-SPRINTEROP-0160).	**SRS 020** **SRS 022** **SRS 024**
SRD 019 [Conf RPA]	RPAS shall be able to set specific emergency transponder code and to maintain it active during emergency. (REQ-PJ13.115-SPRINTEROP-0180).	**SRS 021**
SRD 020 [Conf RPS; ER ACC/APP ACC]	ATC shall be able to manage RPAS emergency situation (REQ-PJ13.115-SPRINTEROP-0190) *This includes the appropriate coordination with RP or other actors in order to manage the emergency situation*	**SRS 022** **SRS 023**
SRD 021 [Conf RPA]	RPAS shall be able to remain on the RP controlled/selected trajectory, which takes into account emergency performance (REQ-PJ13.115-SPRINTEROP-0170)	**SRS 022** **SRS 023**

Table 12. Safety Requirements at design level (functionality & performance) satisfying SRS for Abnormal conditions

5.4.2 Analysis of the functional system behaviour – Abnormal conditions of operation

From the safety point of view of exercise EXE_115_001, in which a Real Time Simulation in Clermont-Ferrand airport (LFLC) was performed, it is analysed which of the abnormal conditions, described in previous sections, have been covered. This exercise refers to the use cases:

- *Use Case IFR RPAS Contingency Operations (C2LL)*
- *Use Case IFR RPAS Emergency Operations*

The purpose of this section is to list the abnormal conditions that have been analysed in the EXE to evaluate the behaviour of the functional system and the results of this analysis.

For *ABN1 - RPAS technical system failure: C2 Link Loss (C2LL) and ATC Voice (VHF) loss (PLOC: prolonged loss of communication)*, the objective was to validate ATCO use of predefined contingency procedures when managing RPAS within manned traffic. To this regard, two validation objectives are analysed:

- The validation objective OBJ-115-V3-VALP-004 analyses the "management of abnormal C2LL specific RPAS situations" (information exchange procedure & C2LL procedure management). It is considered accomplished from RTS execution.
- The validation objective OBJ-115-V3-VALP-007 is also analysed from RTS evaluation, for safety assessment to be tested. It considers contingency procedures, especially in case of loss of C2 link, defined and validated.

Regarding *ABN2- RPAS Emergency Operations: Engine failure emergency*, the objective was to assess information exchanges during urgency situation. This abnormal condition was only addressed through the S115 group workshops. No specific RTS situation was considered necessary as the management an emergency is deemed equivalent to a manned aircraft emergency. The only related validation objective analysed is OBJ-115-V3-VALP-005, to assess information exchanges and management during emergency situations including transponder and engine failures, and it is considered accomplished.

Therefore, it can be concluded that the previous validation objectives have been covered and adequate safety levels are maintained.

On the other hand, the objective OBJ-115-V3-VALP-003 analyses the "management of abnormal RPAS situations identically to manned aviation", considering Voice Communication loss with no C2 link loss, GNSS/positioning loss, and transponder failure/loss. The aim is to validate:

- ATCO use of predefined contingency procedures for these abnormal situations
- Standard IFR contingency procedures and operating methods identically to manned aviation

Its validation also confirms that identical procedures to manned aviation could be used with RPAS for abnormal situations not specific to RPAS, while maintaining the safety of operations.

The detailed analysis of SESAR Solution Validation Results per Validation objective is contained in VALR section 4 (see reference [8]).

No additional SRD (functionality & performance) are derived from this analysis of the functional system behaviour (abnormal conditions of operations).

5.5 Safety Requirements at Design level addressing Internal Functional System Failures

The purpose of this section is to present the Safety Requirements at Design level (SRD) associated to internal failures of the Solution functional system.

Safety requirements at design level - SRD are derived from the SRS (functionality & performance) and SRS (integrity/reliability) which have been identified when mitigating system generated risks (section 4.4).

The following Safety requirements at design level (SRD) are to be included (derived from a top down causal analysis of the operational hazards identified at section 4.4.1, from a bottom up failure modes and effects analysis encompassing the analysis of common causes and, if applicable, from the SRS (functionality & performance) derived during the operational hazard assessment at section 4.4.1):

- SRD (functionality & performance) derived to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard
- SRD (integrity/reliability) to limit the frequency with which failure of modified/new equipment elements in the Solution functional system could be allowed to occur
- If applicable, SRD (functionality & performance) derived to provide mitigation against operational hazard effects (protective mitigation, from the SRS (functionality & performance) derived during the operational hazard assessment at section 4.4.1).

5.5.1 Design analysis addressing internal functional system failures

The design analysis addressing internal functional system failures has been conducted through:

- A top-down causal analysis through Fault Trees that show for each operational hazard, its causes and the associated mitigations.
- A bottom-up analysis through a Failure Modes and Effects Analysis, for selected parts of the Solution functional system, in order to determine potential common cause failures but also in order to allow a more in-depth causal analysis of certain parts of the functional system design

The aim of this work is to:

- Ensure identification of a complete list of Solution functional system failures that could cause each operational hazard.
- Ensure identification of the required Mitigation means preventing causes to occur or preventing their effect to propagate towards each operational hazard
- Contribute to demonstrate the feasibility and effectiveness of the contingency procedures associated to the degraded modes of operation in which the functional system might enter as a result of certain failure modes
- Determine potential common cause failures and ensure their mitigation through dedicated SRD or design choice.

An overview of the main outcomes of these analyses is included in Appendix G.

5.5.2 Safety Requirements at Design level associated to internal functional system failures

Table 13 contains the consolidated list of Safety Requirements at Design level (functionality & performance) associated to internal system failures. Include the following:

- the SRD (functionality & performance) derived from the SRS (integrity/reliability) from section 4.4.2 to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard, with due consideration for mitigating the common cause failures,
- the SRD (functionality & performance) derived to provide mitigation against operational hazard effects (protective mitigation, from the SRS (functionality & performance) derived

during the operational hazard assessment at section 4.4.1), with due consideration for mitigating the common cause failures.

For each SRD (functionality & performance) the element of the design model on which the SRD is placed is indicated, as well as the originating SRS.

The detail of the derivation process is included in Appendix G.

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common cause failure
SRD 001	RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	SRS 037a & SRS 037b & SRS 038 SRS 041
SRD 002	RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110).	SRS 039
SRD 003A	ATCO shall be able to easily recognise the RPAS traffic. (REQ-PJ13.115-SPRINTEROP-0070).	SRS 039 SRS 042
SRD 003B	The RP shall add "REMOTE" to the callsign (REQ-PJ13.115-SPRINTEROP-0340).	
SRD 006	ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300) *NOTE: This includes that the ATC system shall process and highlight specific C2 link loss transponder code on CWP.*	SRS 042
SRD 009	RP shall always pre-program RPA with a C2LL trajectory that shall be automatically triggered and flown when the RPAS goes into a C2LL state (REQ-PJ13.115-SPRINTEROP-0310). *NOTE: The RP shall re-program this C2LL trajectory whenever it is required*	SRS 039 SRS 041
SRD 012	RPA shall be able to automatically provide specific C2 link loss transponder code and to maintain it active during C2 link loss (REQ-PJ13.115-SPRINTEROP-0140).	SRS 042
SRD 013	The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260).	SRS 039
SRD 015	ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250).	SRS 037a & SRS 037b & SRS 038 SRS 039 SRS 042
SRD 020	RPAS shall be able to identify its emergency status and to execute the emergency procedure associated with the severe failure situation with RP in the loop (REQ-PJ13.115-SPRINTEROP-0160).	SRS 043
SRD 022	A team of pilots shall be always available to manage the RPA, and at all times during flight there will be one pilot designated Pilot in Command in the RP position (REQ-PJ13.115-SPRINTEROP-0350).	SRS 033 SRS 037a & SRS 037b & SRS 038 SRS 039

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common cause failure
SRD 023	RP shall be able to execute the standard IFR contingency procedures and operating methods identically to manned aviation: • Voice Comm loss with No C2 link loss; • GNSS/positioning loss; • Transponder failure/loss. (REQ-PJ13.115-SPRINTEROP-0130).	SRS 037a & SRS 037b & SRS 038 SRS 039
SRD 024	RP shall be trained and shall be able to apply new procedures including specific RPAS preparation procedures and operating methods for RPAS non-nominal situations. RP will, if necessary, re-program diversion preparation in case of changes in nominal flight (i.e. prior to C2LL) (REQ-PJ13.115-SPRINTEROP-0270)	SRS 039
SRD 025	RPAS shall be able to navigate during flight in a structured airspace with performances and capabilities associated with the airspace, including the C2LL trajectory: • Positioning aids (GNSS, inertial); • AIRAC cyclic navigation data (ATS routes, waypoints); • RNAV required in the class A-C airspace environment (RNAV5 En-Route / RNAV1 Terminal). (REQ-PJ13.115-SPRINTEROP-0090) *The aim is to ensure the capability of the system in nominal conditions and while applying C2LL procedures.*	SRS 036 SRS 039 SRS 041
SRD 026	RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040) *NOTE: The span of flight levels considered will usually be above low levels to minimise recreational VFR traffic risk (> FL100), and below high levels to minimise flying within high speed cruising jet aircraft (~ FL200). Nevertheless, these vertical limits could be adapted depending on the specific characteristics of each operational environment*	SRS 034
SRD 027	RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)	SRS 035

Table 13. SRD (functionality & performance) to mitigate the operational hazards

No Safety Requirements at Design level (integrity/reliability) associated to internal system failures derived from the Service Requirements at Service level (integrity/reliability) documented in section 4.4.2 have been identified.

5.6 Realism of the safe design

5.6.1 Achievability of Safety Requirements (SRD) and Assumptions

The Safety Requirements identified in section 5.3 to 5.5 have been determined and validated through safety workshops, and are also based on the results of the validation activities. The involvement of operational and technical experts during these workshops ensures the achievability of the safety requirements (SRD) and assumptions.

Some of these safety requirements have been evaluated during the validation activities, though no formal traceability between the safety requirements and the safety validation objectives has been developed.

5.6.2 Verification of Safety Requirements (SRD)

The safety requirements (SRD) were validated whilst conducting the validation exercise and via involvement of experts during the safety workshops.

5.7 Process assurance for a Safe Design

The different topics covered in this section have been developed by the safety team and reviewed/validated by the multidisciplinary team of experts working in Solution 115, during the meetings indicated in section "4.5. Process assurance of the Safety Specification at ATS Service level", and also in the following workshops:

- PJ13-W2-115_SAR_Workshop #04 (13/06/2022). (More information available in: https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F30407783)
- PJ13-W2-115_SAR_Workshop #05 (17/06/2022). (More information available in: https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F30407812)
- PJ13-W2-115_SAR_Workshop #06 (07/09/2022). (More information available in: https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F31114888)

The aim of these meetings was to work on the safe design of the functional system.

6 Safety Criteria achievability

The purpose of this section is to provide conclusions of the safety assessment for the ATS operational Solution 115.

The Safety Criteria set in section 3.4 are expected to be achieved through the Safety Requirements at ATS Service level (SRS) identified in section 4, which have been derived into safety requirements at design level (SRD)) in section 5. The Safety Criteria should be achieved by implementing these safety requirements.

The validation exercise (RTS) allows to verify the compliance with the defined safety criteria for all safety validation objectives. This confirms the ATS Operational Solution 115 enables the management of an RPAS flight efficiently and safely, both in normal and abnormal conditions, and maintains the level of safety within the airspace. It is observed that the measures designed for the flight of RPAS are efficient and solve the particularities of these aircraft, such as the C2LL behavior.

One important consideration that has emerged is that, at the time of the first radio contact with every ATCO the RPA is transferred to, the RP has to inform the ATCO about the aircraft being a RPAS and has to provide the ATCO with details of the pre-programmed RPAS C2LL trajectory.

There is one validation criterion that could not be covered by any validation means. This is the CRT-PJ13.115-V3-VALP-007-0004 “Safe recovery of RPAS degraded operations in airspace classes A, B, C during accommodation”, as the RTS does not reproduce the completion of a C2LL and reversion to nominal flight.

The extent of this safety assessment is recorded in Appendix H.

6.1 Detection and avoidance (DAA) in RPAS.

In solution 115, RPAS are not equipped with Detection and Avoidance Systems *(see detailed explanation of the current situation in section 3.4.2)*.

Since this limitation is part of the Solution’s description, it has always been considered while developing the present SAR and, therefore, several safety arguments and requirements have been compiled along the text, in order to ensure that the risk of mid-air collisions does not increase (despite the lack of a DAA system). These arguments and requirements are summarized in the following paragraphs.

Regarding nominal conditions of operation, the following measures are applicable:

- Both ATCOs and RPs will be trained to operate in the new scenario and under nominal conditions.
- RPAS is equipped with a transponder. It is electronically visible to ATC and to other ACAS equipped aircraft.
- RPAS operates in an environment where all traffic is known and under ATC services.
- ATCOs will be able to:

  - perform surveillance of RPA with the current secondary surveillance tools and technologies.
  - use usual controller methods.
  - use the usual tools, already in place for manned aircraft, to detect possible conflicts: MTCD and STCA safety net (adapted if needed to RPAS performances), as long as they are already in used in the concerned airspace.
- The ATM layered model (DCB, Planning, Tactical, ATC safety net) requires pilot conformance to ATC instruction, through which ATCO ensures conflict avoidance and separation.
- RP / RPAS allows modification of the RPAS navigation according to the new instructions provided by ATC.

Moreover, with respect to traffic awareness:

- RP will have a level of traffic awareness through the “party-line radio communications”, that is, the ability to listen, or at least hear, communications between other aircraft and ATC.
- Since RPs are in the ground, they could also benefit from additional situational awareness systems that show traffic, for instance.
- RPs may also use the RPA camera to see around the aircraft and also have a better situational awareness from ground (although this has not been considered as an absolute behaviour of RP).
- Most aircraft operating in airspaces classes A to C are equipped with ACAS system (according to “COMMISSION REGULATION (EU) 2016/583 of 15 April 2016 amending Regulation (EU) No 1332/2011 laying down common airspace usage requirements and operating procedures for airborne collision avoidance”). Therefore, they will receive Traffic Advisory alerts regarding the RPAS in their surroundings.

Additionally, regarding risk mitigation:

- Solution 115-compliant RPAS will be an additional non-equipped aircraft type within a pre-existing category, per precedents & regulation.
- Only one RPA will operate at the same time per ATC sector under the sector responsibility, (aside from very specific cases). The addition of one RPAS (or pairs) per sector is not significant in terms of increasing the overall risk, and ATC is providing the same service as for manned aviation.
- RPAS operator will plan the flight within flight levels where a minimum traffic risk is usually present
  - Above low levels to minimise recreational VFR traffic risk (> FL100) – above most likely recreational incursions into controlled airspace.
  - Below high levels to minimise flying within high-speed cruising jet aircraft (below ~FL200/300).

    - Vertical limits could be adapted depending on the specific characteristics of each operational environment.

Finally, in non-nominal conditions of operation the above-mentioned measures will be complemented by the following ones:

- RP will be able to execute the standard IFR contingency procedures and operating methods identically to manned aviation:
    - Voice Comm loss with No C2 link loss;
    - GNSS/positioning loss;
    - Transponder failure/loss.

And, in particular, while suffering a C2LL):

- Both ATCOs and RPs will be trained to operate in the new scenario and under non-nominal conditions.
- The ATCO will always be aware of the RPAS intentions given that the RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness on first radio contact and each time the C2 link loss trajectory is re-programmed. Moreover, the communication between RP and ATCO can be maintained in case of contingency through the alternative communication means.
- RPAS is a slow traffic (speeds <~200 knots) and operates in low density environments, which allows sufficient time for ATCO to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence.
- Even though only one RPA will operate at the same time under the responsibility of one sector, there could be very specific and limited situations in which RPAS demand is to operate in pairs. In such cases, the RPAS Operator (single operator) is expected to guarantee that the two RPAs shall not have crossing C2LL trajectories (in space or in time) at any time during the contingency. This requires C2LL trajectories strategic-planning by the RPAS operator. This should include collapsed sector situations, if applicable during the period of flight of the RPAS.

7 Acronyms and Terminology

The following table presents a list of the different acronyms used along the document.

Acronym	Definition
ABN	Abnormal (conditions of operation)
ACAS	Airborne Collision Avoidance System
ACC	Area Control Centre
AIM	Accident Incident Model
AIRAC	Aeronautical Information Regulation and Control
AMC	Acceptable Means of Compliance
APP	Approach
ARES	Airspace reservation/restrictions
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATS	Air Traffic Services
ATSU	ATS Unit
BADA	Base of aircraft data
CFIT	Controlled Flight Into Terrain
CRT	Criteria
CTR	Control Zone / Controlled Traffic Region[9]
CWP	Controller Working Position
DAA	Detection and Avoidance
EATMA	European Air Traffic Management Architecture
EC	European Commission
ECAC	European Civil Aviation Conference
ENR	En-route
ERICA	Enable RPAS Insertion In Controlled Airspace
EU	European Union
EXE	Exercise

[9] A CTR is a volume of controlled airspace, usually situated below a control area, normally around an airport, which extends from the surface to a specified upper limit, established to protect air traffic operating to and from that airport.

Acronym	Definition
FHA	Functional Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FP/FPL	Flight Plan
GAT	General Air Traffic
GM	Guidance Material
GNSS	Global Navigation Satellite System
HALE (RPAS)	High Altitude Long Endurance RPAS
HAZID	Hazard Identification
HMI	Human Machine Interface
HP	Human Performance
ICAO	International Civil Aviation Association
INTEROP	Interoperability Requirements
IM	Impact Modification Factor
IFR	Instrumental Flight Rules
IRS	Interface Requirements Specification
MAC	Mid-Air Collision
MALE (RPAS)	Medium Altitude Long Endurance RPAS
MIL	Military
MTCD	Medium Term Conflict Detection
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NM	Network Manager
NOV	NAF Operational View
NSV	NAF System View
OAT	Operational Air Traffic
OBJ	Objective
OE	Operational Environment
OH	Operational Hazard
OR	Operational Requirement
OSED	Operational Service and Environment Definition
PLOC	Prolonged Loss Of Communication
PROSA	Provision Of Separation in Air Traffic Management
PSSA	Preliminary System Safety Assessment

Acronym	Definition
REQ	Requirement
RNAV	Area Navigation
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
RP	Remote Pilot
RPS	Remote Pilot Station.
RTS	Real Time Simulation
SAC	Safety Criteria
SAF	Safety
SAM	Safety Assessment Methodology
SAP	Safety Assessment Plan
SAR	Safety Assessment Report
SC	Severity Class
SCS	Severity Classification Scheme(s)
SESAR	Single European Sky ATM Research
SJU	SESAR Joint Undertaking
SPR	Safety and Performance Requirements
SRD	Safety Requirement at Design Level
SRM	Safety Reference Material
SRS	Safety Requirement at Service level
SSA	System Safety Assessment
STANAG	Standardization Agreement
STCA	Short Term Conflict Alert
TMA	Terminal Manoeuvring Area
TS	Technical Specification
TWR/TWC	Control Tower
UC	Use Case
VALR	Validation Report
VALP	Validation Plan
VFR	Visual Flight Rules
VHF	Very High Frequency
WOC	Wing Operation Centre

Table 14: Acronyms

The following table presents a list of the most important terminology used along the document.

Term	Definition
Functional System	A combination of procedures, human resources and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions (Regulation (EU) No 2017/373 [1])
Hazard	Any condition, event, or circumstance which could induce a harmful effect (Regulation (EU) No 2017/373 [1])
Risk	The combination of the overall probability or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect (Regulation (EU) No 2017/373 [1])
Safety Criteria	Criteria that allow the ATS provider to determine the safety acceptability of a change to a functional system, based on the analysis of the risks posed by the introduction of the change (Regulation (EU) No 2017/373 [1])
Safety Requirement at Design Level	Design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SACs (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SACs are met).
Safety Requirement at Service Level	Requirements that specify the desired safety behavior of the change at its interface with the ATS operational context considering normal and abnormal conditions of the context (success approach) and the failures of the functional system (failure approach).
Solution Functional System	Designates the Solution Functional ATM/ANS System as defined in Regulation (EU) No 2017/373 [1] (i.e. encompassing procedures, human resources and equipment).

Table 15: Glossary of terms

8 References

Safety

[1] Regulation (EU) No 2017/373 laying down common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011 and (EU) No 1035/2011 and amending Regulation (EU) No 677/2011 (and associated AMC and GM)

[2] SAM EUROCONTROL Safety Assessment Methodology, Edition 2.0

[3] SESAR Safety Reference Material – Edition 04.01, December 2018

[4] Guidance to Apply SESAR Safety Reference Material – Edition 03.01, December 2018

Reference documents

[5] SESAR Solution PJ.13-W2-115 SPR-INTEROP/OSED for V3 – Part I

[6] SESAR Solution PJ.13-W2-115 Validation Plan (VALP) for V3 – Part II – Safety Assessment Plan

[7] SESAR Solution 115 SPR-INTEROP/OSED for V3 - Part IV - Human Performance Assessment Report

[8] SESAR Solution PJ.13-W2-115 Validation Report (VALR) for V3

[9] Demonstrating RPAS integration in the European aviation system. SESAR.

[10]ICAO Doc 4444

[11]EASA's "ANNUAL SAFETY RECOMMENDATIONS REVIEW 2022

Appendix A Preliminary safety impact assessment

This first appendix identifies the Safety Criteria that have already been realised in VALP to provide a preliminary safety impact assessment. They are all documented in the Safety Assessment Plan (Part II of the VALP), performed in accordance with the relevant SAF-GUI in STELLAR.

A.1 Relevant Hazards Inherent to Aviation

As indicated in previous sections, the aim of PJ.13-W2-115 is the accommodation of IFR RPAS in airspaces Class A to C, with low/medium complexity/density. Therefore, the pre-existing hazards in such operational environment should be considered.

These are relevant hazards inherent to aviation that the Solution services must mitigate in order to guarantee an acceptable safety level and are provided in the following Table 16.

Hazards inherent to aviation [Hi]	ATM-related accident type & AIM model
Hi#1: Situation in which the intended trajectories of two or more aircraft, including RPAS, are in conflict	Mid-Air Collision (MAC) En Route & TMA AIM models
Hi#2: Situation when the RPAS encounters adverse weather which generates conflict with other aircraft because of deviation	Mid-Air Collision (MAC) En Route & TMA AIM models
Hi#3: Controlled Flight Into Terrain	Controlled Flight into Terrain [CFIT v1.0]
Hi#4: RPAS trajectory impacted by wake vortex leading to loss of control	AIM model not available
Hi#5: Incursion of General Air Traffic RPAS into ARES	Mid-Air Collision (MAC) En Route & TMA AIM models
Hi#6: Airspace infringement by a VFR intruder	Mid-Air Collision (MAC) En Route & TMA AIM models
Hi#7: Fire issue, engine failure, fuel shortage	AIM model not available
Hi#8: Traffic excursion from an ARES on collision course with an RPAS flying as a General Air Traffic	Mid-Air Collision (MAC) En Route & TMA AIM models

Table 16. Hazards inherent to aviation relevant for the Solution

A.1.1 Relevant hazards which are not considered as being relevant in the solution

Some of the above identified hazards have finally been discarded, since they are not the most relevant ones regarding the changes introduced by Solution 115. The hazards and the related reasons are included in the following paragraphs.

Hazard Hi#3: Controlled Flight Into Terrain, which is a hazard inherent to aviation but especially for approach / landing environment, has not been considered for the following reasons:

- Scope of the solution focus on RPAS transit at levels (above FL100) where a collision with terrain may be possible but very rare (European data base for statistics))

- By definition, the current and initial RPAS do not carry passengers. Therefore, consequence of a CFIT is only to damage or destroy material, not life.
- The probability that an RPAS crash around 3000m height impacts people and /or wildlife on ground is very low.

Hazard Hi#4: RPAS trajectory impacted by wake vortex leading to loss of control

- RPAS is considered as a light aircraft. Hence, the way it could be separated from bigger aircraft is not different to other light manned aircraft. The separation distance could be up to 6NM if the preceding aircraft is in the heavy category (ICAO Doc 4444) [10].
- Consequence of a loss of RPA's control is only damage to the RPA itself, unless the RPA, due to the loss of control, collides with a manned aircraft or hits a property, people or wildlife on the ground.

Nevertheless, specificities of RPAS, which have usually bigger wingspan than usual manned aircraft (e.g., excluding gliders) may require further investigations. The impact of wake turbulence is considered within the abnormal conditions of operations analysis.

Hazard Hi#5: Incursion of General Air Traffic RPAS into ARES

- It has been identified that in case of command and control link loss, when programming the RPAS before the failure occurs, the trajectory entered by the remote pilot will need to be planned in such a way that the RPAS shall not enter these zones, and ATC would not vector RPAS towards such zones.
- One of the mitigations proposed is the possibility for the remote pilot to have access to a variety of information and tools which provide him with a situational awareness exhaustive enough to avoid the RPAS to be programmed to cross restricted, dangerous or forbidden areas.

Hazard Hi#7: Fire issue, engine failure, fuel shortage, has not been taken into account provided that:

- An RPAS is not different than a manned aircraft with regard to the hazards themselves and,
- For an RPAS, these hazards do not impact passengers on board. In addition, RPAS are constantly pre-programmed all along the flight to crash in a cleared area in order to avoid crash impacts to property/people on ground.

A.2 Functional system-generated hazards (preliminary)

Functional system-generated hazards can refer to:

- either existing hazards in Reference operations but potentially affected by the Solution in terms of causes, circumstances of occurrence, mitigation
- or potential new hazards introduced by the Solution.

In the scope of the Solution 115, a preliminary list of these hazards was identified in the SAP and are compiled in the following Table 17. Moreover, the information has been completed by indicating, for each functional system-generated hazard, the way they are impacted by the change.

Functional system-generated hazards (preliminary)	Impacted (new/modified) & justification
Hr#1: RP does not include the correct contingency procedure in the system	New Contingency procedure needs to be included in the initial Flight Plan and updated each time controllers provide a vector/heading/altitude/speed deviation to the RPAS.
Hr#2: RP does not communicate the contingency procedure to ATC/or communicates the wrong one	New Information about contingency procedures needs to be provided to the ATCO on first radio contact and after re-programming the procedure due to vector/heading/altitude/speed changes instructed by ATCOs.
Hr#3: ATC does not integrate the established procedure for the loss of C2L of an RPAS in the management of the other traffic	New The C2L is a system linked to RPAS (not to manned aircraft). The related contingency procedures are new for ATS Units too.
Hr#4: Malfunction of C2 link (e.g., abnormal delay, total loss)	New The C2L is a system linked to RPAS (not to manned aircraft).
Hr#5: Loss of Remote Pilot situational awareness (including environmental, mode and system awareness, spatial disorientation, and time horizon)	Modified Both manned and unmanned aircraft pilots can lose their situational awareness. Nevertheless, RP are not inside the aircraft, which constitutes an important difference with respect to manned aviation.
Hr#6: Malfunction in Communication link with ATS (Air Traffic Service) or ATM Unit. (Late execution of a manoeuvre)	Modified In the Accommodation phase, ATC Voice (VHF) is lost when the C2Link is lost because RPA Operations relays both the Command/Control information and the Voice information on the same C2 Link to RPS Operations.
Hr#7: Misinterpretation of radio-communication which has or could have endangered the aircraft, other aircraft, or any person (side effect of standard latency in relayed communication link).	Modified RPA are new actors in IFR controlled airspace classes A to C, therefore, RP are not used to operate in this kind of environment and this lack of experience could lead to communication problems.

Table 17. Functional system-generated hazards applicable to the Solution (preliminary list)

Appendix B Derivation of SRS (Functionality & Performance) for Normal conditions of operation

This appendix presents the derivation of the SRS (functionality & performance) in order to mitigate the hazards inherent to aviation under normal conditions of operation, i.e. those conditions that are expected to occur on a day-to-day basis.

With this purpose, the description of the new operating method within Solution 115 is reviewed, in order to specify through a list of SRSs the safety-relevant changes in the delivery of each impacted operational service or the safety behaviour of the Reference functional system at operational level which needs to be preserved for the SAC to be satisfied.

This description of the new operating method is available via:

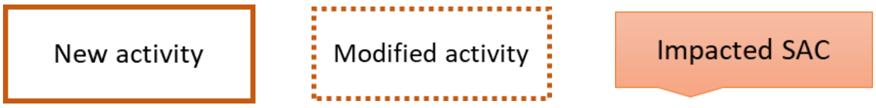
- The description of each Use Case included in the OSED. For normal conditions of operation, the related UC within Solution 115 are:
    - IFR RPAS Pre-Flight Operations.
    - IFR RPAS Nominal Operations.
- The EATMA representation as per the Operational layer (i.e. the NOV-5 diagrams related to the above-mentioned UC, where each one of them is described through a process model made up of activities interacting via information flows).

The consolidated list of SRSs is provided in Section 4.2.1.

B.1 EATMA Process models or alternative description

In this section, a copy of the EATMA process models regarding each one of the two mentioned Use Cases is included.

In them, the new or modified activities are highlighted and mapped against the impacted SACs as follows:



B.1.1 Use Case: IFR RPAS Pre-Flight Operations

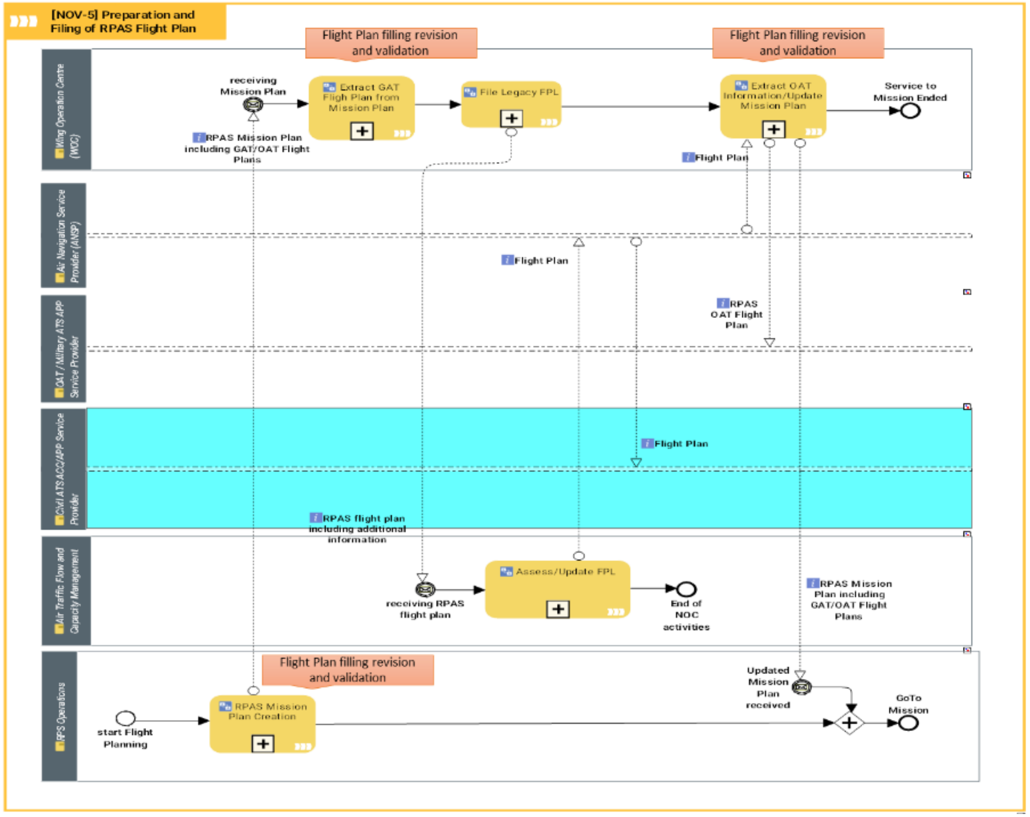

[NOV-5] Preparation and Filing of RPAS Flight Plan
Wing Operation Centre (WOC)
Air Navigation Service Provider (ANSP)
OAT / Military ATS APP Service Provider
Civil ATS ACC/APP Service Provider
Air Traffic Flow and Capacity Management
RPS Operations
Flight Plan filling revision and validation
receiving Mission Plan
Extract GAT Fligh Plan from Mission Plan
File Legacy FPL
Extract OAT Information/Update Mission Plan
Service to Mission Ended
RPAS Mission Plan including GAT/OAT Flight Plans
Flight Plan
Flight Plan
RPAS OAT Flight Plan
Flight Plan
RPAS flight plan including additional information
receiving RPAS flight plan
Assess/Update FPL
End of NOC activities
RPAS Mission Plan including GAT/OAT Flight Plans
Flight Plan filling revision and validation
start Flight Planning
RPAS Mission Plan Creation
Updated Mission Plan received
GoTo Mission

Figure 2 : EATMA [NOV-5] IFR RPAS Pre-Flight Operation[10]

[10] Since this FP RPAS information has already been validated, the related activities are not considered as changes compared to the previous operating method, and no SACs are defined to this regard. Therefore, the operational services are mapped, instead of the SACs.

B.1.2 Use Case: IFR RPAS Nominal Operations

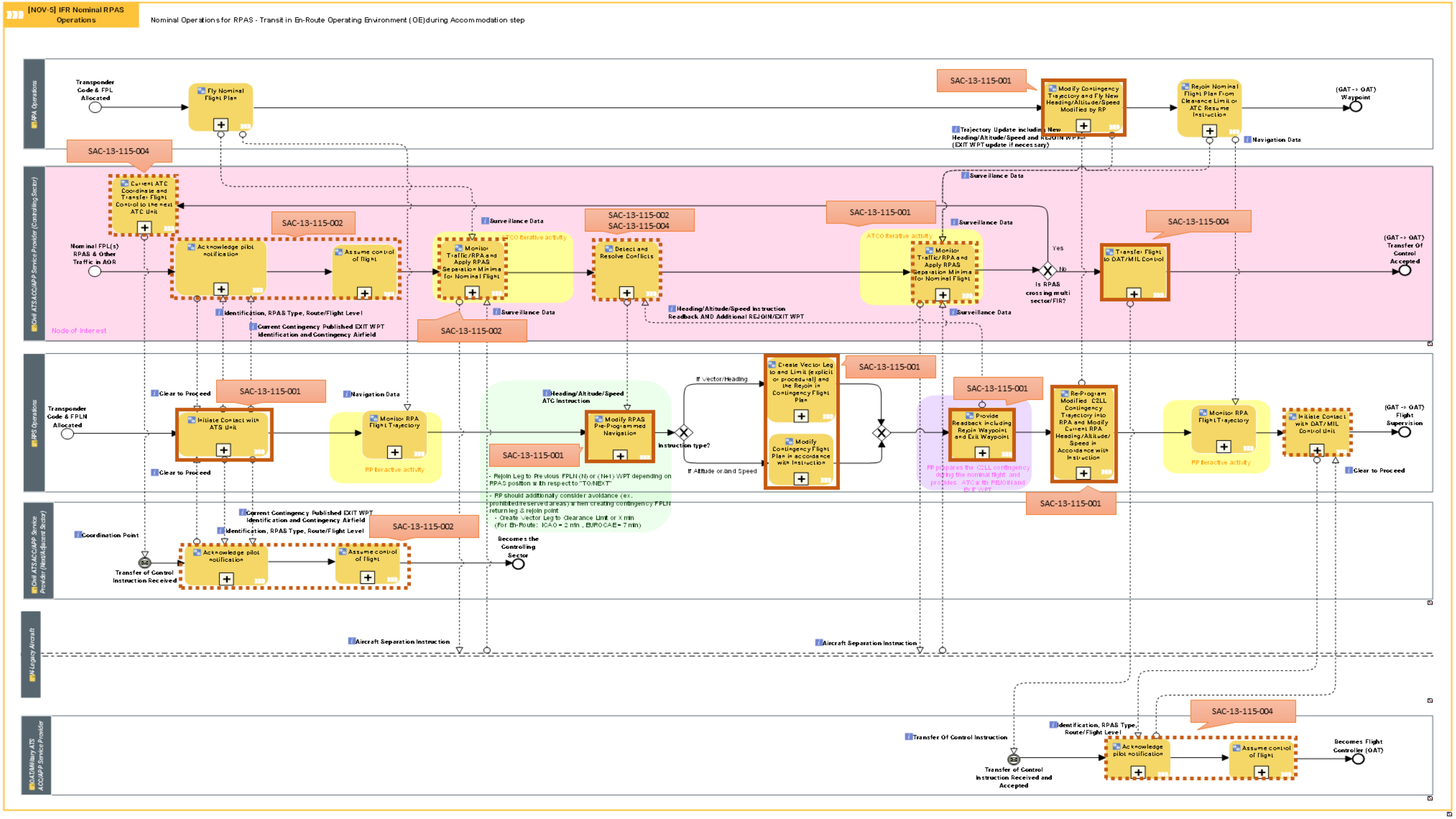

[NOV-5] IFR Nominal RPAS Operations
Nominal Operations for RPAS - Transit in En-Route Operating Environment (OE) during Accommodation step
RPA Operations
Civil ATS ACC/APP Service Provider (Controlling Sector)
RPS Operations
Civil ATS ACC/APP Service Provider (Next/Adjacent Sector)
IFR Legacy Aircraft
OAT/Military ATS ACC/APP Service Provider
Transponder Code & FPL Allocated
Fly Nominal Flight Plan
SAC-13-115-004
SAC-13-115-001
Modify Contingency Trajectory and Fly New Heading/Altitude/Speed Modified by RP
Trajectory Update including New Heading/Altitude/Speed and REJOIN WPT (EXIT WPT update if necessary)
Rejoin Nominal Flight Plan From Clearance Limit or ATC Resume Instruction
Navigation Data
(GAT -> OAT) Waypoint
Current ATC Coordinate and Transfer Flight Control to the next ATC Unit
Nominal FPL(s) RPAS & Other Traffic in AOR
SAC-13-115-002
Acknowledge pilot notification
Assume control of flight
Identification, RPAS Type, Route/Flight Level
Current Contingency Published EXIT WPT Identification and Contingency Airfield
Node of Interest
Surveillance Data
ATCO Iterative activity
Monitor Traffic/RPA and Apply RPAS Separation Minima for Nominal Flight
SAC-13-115-002
SAC-13-115-002
SAC-13-115-004
Detect and Resolve Conflicts
Heading/Altitude/Speed Instruction Readback AND Additional REJOIN/EXIT WPT
SAC-13-115-001
Surveillance Data
ATCO Iterative activity
Monitor Traffic/RPA and Apply RPAS Separation Minima for Nominal Flight
Surveillance Data
Yes
No
Is RPAS crossing multi sector/FIR?
SAC-13-115-004
Transfer Flight to OAT/MIL Control
(GAT -> OAT) Transfer Of Control Accepted
Transponder Code & FPLN Allocated
Clear to Proceed
SAC-13-115-001
Initiate Contact with ATS Unit
Clear to Proceed
Navigation Data
Monitor RPA Flight Trajectory
RP Iteractive activity
Heading/Altitude/Speed ATC Instruction
Modify RPAS Pre-Programmed Navigation
SAC-13-115-001
- Rejoin Leg to Previous FPLN (N) or (N+1) WPT depending on RPAS position with respect to "TO/NEXT"
- RP should additionally consider avoidance (ex. prohibited/reserved areas) when creating contingency FPLN return leg & rejoin point
- Create Vector Leg to Clearance Limit or X min (For En-Route: ICAO = 2 min , EUROCAE = 7 min)
If Vector/Heading
Instruction type?
If Altitude or/and Speed
Create Vector Leg to and Limit (explicit or procedural) and the Rejoin in Contingency Flight Plan
Modify Contingency Flight Plan in accordance with Instruction
SAC-13-115-001
SAC-13-115-001
Provide Readback including Rejoin Waypoint and Exit Waypoint
RP prepares the C2LL contingency during the nominal flight and provides ATC with REJOIN and EXIT WPT
Re-Program Modified C2LL Contingency Trajectory into RPA and Modify Current RPA Heading/Altitude/Speed in Accordance with Instruction
SAC-13-115-001
Monitor RPA Flight Trajectory
RP Iteractive activity
Initiate Contact with OAT/MIL Control Unit
Clear to Proceed
(GAT -> OAT) Flight Supervision
Coordination Point
Current Contingency Published EXIT WPT Identification and Contingency Airfield
Identification, RPAS Type, Route/Flight Level
SAC-13-115-002
Transfer of Control Instruction Received
Acknowledge pilot notification
Assume control of flight
Becomes the Controlling Sector
Aircraft Separation Instruction
Aircraft Separation Instruction
Transfer Of Control Instruction
Identification, RPAS Type, Route/Flight Level
SAC-13-115-004
Transfer of Control Instruction Received and Accepted
Acknowledge pilot notification
Assume control of flight
Becomes Flight Controller (OAT)

Figure 3 : EATMA [NOV-5] IFR RPAS Nominal Operations

B.2 Derivation of SRS for Normal Operations

In order to derive the SRS for Normal Operations, the EATMA representations presented in section B.2 are analysed in such a way that, for each ATS Operational Service within each Use Case:

- It is check whether the identified change(s) is (are) safety relevant (i.e. if the change could impact the efficiency of a safety barrier or the occurrence of a safety precursor).
- A list of SRS is derived in order to describe the safety-relevant changes in the delivery of that operational service by the Solution (the change might impact the WHAT or the HOW of the operational service).

The following Table 18 provides the derivation of SRS in normal conditions of operation driven by EATMA Process Models associated to Solution 115.

ATS Operational Service	EATMA Use Case- Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
Use Case: IFR RPAS Pre-Flight Operations			
Flight Plan filling, revision and validation *Assumption A002: The FP RPAS information has already been validated. This*	RPS Operations: create RPAS Mission Plan including GAT/OAT FPL and additional information linked to the execution of the FPL	*Taking into account that this FP RPAS information has already been validated, this activity is not considered a change compared to the previous operating method, and it does not impact the WHAT or the HOW of the operational service. Therefore, no SRS are derived.*	---
	Wing Operation Centre (WOC): Extract GAT Flight Plan from Mission Plan and file legacy FPL	*Taking into account that this FP RPAS information has already been validated, this activity is not considered a change compared to the previous operating method, and it does not impact the WHAT or the HOW of the operational service. Therefore, no SRS are derived.*	---

ATS Operational Service	EATMA Use Case- Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
means that the standard filling and validation process of FP processing is applicable.	Civil ATS APP/ACC service providers: Process the information within the FP *NOTE: Regarding the RPAS specific data included in the FP, both the automated process and the non-automated processes on ACC that could be in place in ACCs are considered*	*This activity is not considered a change compared to the previous operating method, and it does not impact the WHAT or the HOW of the operational service. Therefore, no SRS are derived.*	---
	Air Traffic Flow and Capacity Management (ATFCM): Assess/Update FPL	*This activity is not considered a change compared to the previous operating method, and it does not impact the WHAT or the HOW of the operational service. Therefore, no SRS are derived.*	---
	Wing Operation Centre (WOC): Extract OAT Information/Update Mission Plan	*Taking into account that this FP RPAS information has already been validated, this activity is not considered a change compared to the previous operating method, and it does not impact the WHAT or the HOW of the operational service. Therefore, no SRS are derived.*	---
		Use Case: IFR RPAS Nominal Operations [11]	
Radio and radar contact and monitoring	RPS Operations: Initiate contact with ATS Unit: offer all the information in the first radio contact, including contingency data.	**SRS 001a:** The RP shall initiate contact with the relevant ATS Unit. **SRS 001b:** The RP shall provide the ATCO in initial radio contact with each sector with the standard contact information regarding identification including RPAS, next route element(s)/flight level and minimum elements of the pre-programmed C2LL contingency trajectory	SAC-13-115-001 (AIM MAC MF 6.1)
	ATS Unit: acknowledge pilot notification and assume control of RPAS flight	**SRS 002:** The ATS Unit shall acknowledge the RP's first notification and assume the control of RPAS flight.	SAC-13-115-002 (AIM MAC MF 5.1)

[11] This Use Case refers to Nominal Operations, especially focusing on how to anticipate a **possible C2LL contingency** situation.

ATS Operational Service	EATMA Use Case- Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
	ATS Unit: monitor and command RPA trajectory & traffic in flight. Apply RPAS separation minima for nominal flight.	**SRS 003a:** The ATS Unit shall monitor the RPAS flight trajectory through cooperative secondary radar surveillance data. **SRS 003b:** The ATS Unit shall use surveillance data to monitor the traffic (manned and unmanned), in order to apply separation minima between aircraft. *The objective is for ATS Unit to apply identical separation minima with the RPAS.*	SAC-13-115-002 (AIM MAC MF 5.1)
Conflict detection and resolution	ATS Unit: detect a conflict with RPA flight trajectory and provide instruction to RP for resolution (Vector/ Heading/ Altitude/ Speed instructions).	**SRS 004a:** The ATS Unit shall detect the possible conflicts with RPAS flight trajectory **SRS 004b:** The ATS Unit shall issue clearances and provide instructions to RPAS for resolution of conflicts (Vector/ Heading/ Altitude/ Speed instructions).	SAC-13-115-002 (AIM MAC MF 5.1) SAC-13-115-004 (AIM MAC MF 7.1)
	RPS Operations: anticipate/prepare a possible C2LL contingency which could occur during flight according to the instruction.	**SRS 005:** Upon obtaining a new clearance/instruction, RPS Operations shall verify compatibility of existing pre-programmed C2LL contingency trajectory, and if necessary, re-program a revised C2LL contingency trajectory.	SAC-13-115-001 (AIM MAC MF 6.1)
	RPS Operations: provide read-back and information on the RPA behaviour in case of C2LL to the ATS Unit, and modify current trajectory in accordance with the instruction given by ATS Unit.	**SRS 006a:** If a C2LL contingency trajectory is re-programmed/revised, RPS Operations shall provide information of the revised C2LL trajectory to ATCO, at or after clearance/instruction read-back. **SRS 006b:** RPS Operations shall modify RPAS navigation according to the new instructions provided by ATS Unit.	SAC-13-115-001 (AIM MAC MF 6.1)
	RPS Operations: monitor RPA Flight trajectory	**SRS 007:** RPS Operations shall continue to monitor the RPA trajectory during nominal flight.	SAC-13-115-001 (AIM MAC MF 6.1)
Transfer flight control between ATS Units	Transferring ATS Unit (civil): transfer radio and radar RPAS flight contact to accepting ATS Unit	**SRS 008:** Transferring ATS Unit (civil) shall transfer radio and radar RPAS flight contact to accepting ATS Unit.	SAC-13-115-004 (AIM MAC MF 7.1)

ATS Operational Service	EATMA Use Case- Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
NOTE: The accepting ATS Unit could be a Civil one or the OAT/MIL Control	Accepting ATS Unit (civil or military): assume radio and radar control of RPAS flight and issue ATC clearances and instructions	**SRS 009:** Accepting ATS Unit (civil or military) shall assume radio and radar control of RPAS flight and issue ATC clearances and instructions.	SAC-13-115-004 (AIM MAC MF 7.1)
	RPS Operations: contact accepting ATS Unit and pass the coordination point.	**SRS 010a:** RPS Operations shall contact accepting ATS Unit *(and also provide the ATCO in initial radio contact with C2LL behaviour information → see SRS 001b)* **SRS 010b:** RPAS shall enter the new sector through the coordinated point and after the RP establishes contact with the relevant accepting ATS Unit	SAC-13-115-001 (AIM MAC MF 6.1)

Table 18: Derivation of SRS for Normal Operations driven by Use Cases and related EATMA Process models

Appendix C Risk analysis of Abnormal conditions and derivation of SRS (functionality & performance)

This appendix presents the derivation of the SRS (functionality & performance) in order to mitigate the hazards inherent to aviation under abnormal conditions of operation, i.e. those conditions under which the functional system has to operate in a reversionary mode due to, for example, conditions of the operation environment that the functional system may exceptionally encounter or equipment failures external to the ATM system concerned.

For each abnormal condition of operation identified and listed in section 4.3.1, the immediate operational effect and the possible mitigations of the safety consequences are assessed, in order to establish a list of SRS. Theses SRSs could be related to the ones already identified SRS in section 4.2 or they could be new ones derived from this analysis of abnormal conditions.

The risk analysis for abnormal conditions of operation is conducted from three perspectives:

- can Solution 115 functional system continue to operate effectively (i.e. reduce risk inherent to aviation)?
- if Solution 115 functional system cannot continue to operate fully effectively (i.e. its risk reduction performance is diminished somewhat) – is the overall risk still within the tolerable limits and can the System recover sufficiently quickly when the abnormality is removed (or at least mitigated)?
- to what degree could such abnormal conditions, while they persist (i.e. degraded mode of operation), cause the Solution functional system to behave in a way that could actually induce a risk that would otherwise not have arisen?

The following Table 19 provides the derivation of SRS in abnormal conditions of operation associated to Solution 115[12].

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / SRS
ABN1	RPAS technical system failure: C2 Link Loss (C2LL) and ATC Voice (VHF) loss (PLOC: prolonged loss of communication)	ATC unable to manage RPA flight trajectory. Impossibility for RP to control the RPA. C2 link performance has deteriorated as a result of a C2 link disruption that has a duration longer than the decision time of the loss of the C2 link.	When a RPAS technical system failure (C2 Link Loss (C2LL) and ATC Voice (VHF) loss) the following activities are expected: **SRS 011:** ATS Unit shall be informed of the RPAS C2LL through a specifically defined SSR code automatically set by RPA Operations.

[12] *NOTE: abnormal conditions are analysed one by one: the simultaneously appearance/occurrence of two abnormal conditions is not considered in this analysis.*

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / SRS
	Assumption A003: In the Accommodation phase, ATC Voice (VHF) is lost when the C2Link is lost because RPA Operations relays both the Command/Control information and the Voice information on the same C2 Link to RPS Operations	Impossibility to maintain radio contact between the remote pilot and the relevant ATS Unit. Increase of the workload of the ATCOs and RP to manage the RPA. The RPAS flies autonomously during the C2LL, so: • Possible loss of separation between the RPA and other aircraft. • Possible collision between two RPA, both having a C2LL. Start pre-programmed contingency procedure associated to the C2LL. ATS Unit transfer of Control during contingency: increase of coordinations between ATS Units in order to transfer the control of RPAS during contingency. *This is due to the fact that this transference should take into account all the other operational effects identified (lack of control of the RPAS, possible conflicts with other traffics in the vicinity, etc.), and should be conducted according to the procedures stablished in the LoA or operation manual in effect in case of contingency.*	*NOTE: RPAS is pre-programmed to squawk a specific SSR code as soon as C2LL is detected* **SRS 012:** Follow-up of C2LL Contingency shall be coordinated between ATS Unit and RPS Operations through a backup audio (telephone or direct point-to-point line, if equipped) to exchange useful information, in particular, the remote pilot shall provide details of the C2LL trajectory/behaviour, and the ATCO shall provide information regarding the next ATC sector. **SRS 013:** ATS Unit shall monitor traffic and apply an adapted separation strategy as deemed necessary by ATCO to separate the RPA C2LL trajectory from other (manned) aircraft trajectories. **SRS 014:** RPAS shall fly the contingency procedure. This contingency procedure shall be pre-programmed in Flight Plan, or re-programmed in-flight as necessary, if a vector/heading/altitude/speed instruction has been given by the ATS Unit. **SRS 015:** RPS Operations shall monitor the C2 link state trying to re-establish it (if possible, with the available RPS means) **SRS 016:** If the C2L is never re-established, the RPAS shall continue flying its pre-programmed C2 link loss (C2LL) contingency trajectory. This includes: - Returning to flight plan after a set time, - Flying until the DIVERSION pre-programmed waypoint, from where it shall continue flying to the pre-programmed C2LL destination airfield, that the operator will have chosen during pre-programming (an alternate aerodrome, or the departure one, or the original final destination). **SRS 017:** If the C2L is re-established**,** RPS Operations shall detect it and inform ATS.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / SRS
			SRS 018: If the C2L is re-established, RPS Operations shall revert to previous transponder code (SQUAWK). *NOTE: Reversion to the original (previous) transponder code is on ATCO instruction (thus not automated): if C2L is working, the RP can change the squawk as often as required.* **SRS 019:** If the C2L is re-established, RPS Operations shall use the frequency communicated at telephone coordination to contact the appropriate ATS Unit
ABN2	RPAS Emergency Operations: Engine failure emergency. *NOTE: Only loss of engine propulsion is considered since most of the other emergency events will provide more margins for the RPAS to complete its emergency flight. Underlying logic remains exactly the same*	Aircraft severe limitation to continue the flight requiring landing as soon as possible. RPS Operations keep control of command but without energy for other actions and during a certain time. Increase of the workload of the ATCOs and RP to manage the RPAS. Possible loss of separation between the RPAS and other aircraft (deconfliction). Traffic has to be cleared from the RPAS trajectory. Start procedure related to engine failure emergency: *NOTE: In this section we consider the state of an RPAS during its flight as GAT which is submitted to an engine failure issue. At least for now, we will not introduce the moment of the engine relight if it can occur.*	When a RPASEmergency Operations (e.g., Engine failure emergency) occurs: **SRS 020:** RPA Operations shall determine the engine status in order to analyse the impact of engine loss **SRS 021:** RPS Operations shall broadcast emergency state through the emergency frequency to all concerned traffic. **SRS 022:** RPAS shall follow the Emergency Flight Plan to guarantee the highest level of safety. Use of the "Safest Shortest" principle to make that decision. **SRS 023:** RP shall contact/coordinate with the ATS Unit to declare the flight path to terminate the flight in the worst-case scenario, that is, where the emergency destination is not achievable. **SRS 024:** RPAS shall monitor Emergency Flight in order to: • control the trajectory and adhere to declared Emergency Flight Plan. • alert ATCO when a deviation is observed that cannot be mitigated by RPS Operations. **SRS 025:** ATS Unit shall coordinate termination of the emergency RPA flight with the State/ military authority or civil authority in case of

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / SRS
			Military/State terminal area(Airfield / Ditching area) or in case of entering uncontrolled area all along the flight. **SRS 026:** ATS Unit shall clear the path for RPAS trajectory and provide the separation of surrounding traffic until RPA enters CTR **SRS 027:** ATS Unit shall maintain the coordination with Airport Ops Support that will host the termination action. **SRS 028:** ATS Unit at arrival aerodrome shall clear its airspace and runways from any traffic, including ground vehicles, which may endanger the operation of the arriving emergency RPA. The RP alert ATCO when a deviation is observed that cannot be mitigated by crew *(existing mitigation means).* ATCO has to clear the path for RPAS trajectory when an emergency occurs *(existing mitigation means)* Aerodrome ATS Units prepare the airspace and runways under their control for the emergency arrival of the RPAS *(existing mitigation means).* Use of the squawk code to identify RPAS emergency implemented in all ATC centres accommodating RPAS *(existing mitigation means).*
ABN3	Bad weather encounter or sudden deterioration of weather conditions (weather conditions not according to forecasted ones). ***Assumption A004:*** *The FP is filed or modified short before the flight and considering the latest weather forecast. Therefore, the RPAS will not operate under severe weather conditions since the trajectory included in the FP*	RPA will possibly need to avoid the area with lateral or vertical deviation. RP asks the ATCO before deviation. No change compared to the current situation with manned aircraft. Increase of the workload of the ATCOs and RP to manage the RPAS. Loss of situation awareness (the RP is located on ground and, therefore, it is more difficult for them to assess the situation). If the RPAS enters the zone, there could be a loss of control or loss of performances, leading to trajectory deviation. Possible loss of separation	**SRS 029:** RP shall be able to deal with possible sudden deterioration of weather conditions during the flight. This includes requesting the ATCO a lateral or vertical deviation to avoid the area. *This SRS will minimize to an acceptable level the risk of weather encounter with additional C2LL due to electromagnetic disturbances of bad weather.* **SRS 030:** ATS Unit shall be able to manage situations related to sudden deterioration of weather conditions. **There is no need to conduct a further safety analysis regarding failure conditions.**

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / SRS
	will avoid forecasted events like thunderstorms, icing, or electromagnetic disturbances.	between the RPA and other aircraft due to deviation.	
ABN 4	Wake turbulence encounter. ***Assumption 001:*** *During the accommodation phase, and regarding wake-turbulence separation, RPAS are considered as L category aircraft (including en-route separation).* ***Assumption 006 B):*** *It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations (no additional training because of flying in GAT) is within RP's current skills.* ***Assumption 007:*** *RP have traffic awareness in their RPS through radio communications on shared frequency and they are able to identify certain threatens like the wake risk and request additional instructions to ATCO, if necessary.* *Moreover, the RP is operating in IFR operational environment, so their situational awareness should be linked to the controls they need in this environment.*	RPA will possibly need to avoid the area with lateral or vertical deviation. RP asks the ATCO before deviation. No change compared to the current situation with manned aircraft. If situation is not well managed: possible loss of separation between the RPA and other aircraft due to necessary deviation. Increase of the workload of the ATCOs and RP to manage the RPA.	**SRS 031:** RP shall be prepared for possible wake turbulence encounters during the flight. **SRS 032:** ATS Unit shall be able to manage situations related to wake turbulence encounters. **There is no need to conduct a further safety analysis regarding failure conditions.** (See also rationale attached to Hazard Hi#4, section A.1.1.)

Table 19: Risk analysis for Abnormal conditions of operation

Appendix D Risk analysis addressing internal functional system failures and derivation of SRS

This appendix presents the risk analysis done at the level of the ATS service specification, including operational hazards identification and analysis in view of deriving additional SRS.

D.1 HAZID workshop

A HAZID online workshop was held within Solution 115 the 14th of January and the 7 of February 2022.

The following assumptions were made in order to identify new functional system failures related to the change (see Appendix I for full list).

- From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groupings of sectors concerned. (A002)

  Therefore:

  - The training and knowledge of the operational environment of the ATS Unit, grant the properly monitoring of the RPAS trajectory through surveillance and FP data, in order to:
    - apply RPAS separation minima with another aircraft.
    - detect a conflict with RPAS flight trajectory.
  - The provision of ATS Unit's instructions to RPAS for resolution of conflicts (Vector/ Heading/ Altitude/ Speed instructions) is not conducted in a different way than for manned aircraft.

  Are within ATCO's current skills.

- It is considered that RPs are already trained with regard to the basic procedures and way of operating. (A006)

  Therefore, actions such as:

  - initiating contact with the relevant ATS Unit (including first radio contact both when reaching the first GAT sector and when transferred to the next/adjacent ATS Unit)

  Are within RP's current skills.

On the other hand, the table below presents the results of this HAZID workshop, and includes:

- The different operational failure modes identified at ATS service level.
- The causes of these operational failure mode.

- The assessed immediate operational effect.
- The mitigations taken into account for defining the operational effect (protecting against effect propagation) with a reference to existing safety barriers (as per the relevant AIM model), to mitigation already identified through SRS (functionality & performance) or to new mitigations from which new SRS will be derived (functionality & performance).
- The operational hazard which consolidates the operational failure mode (multiple operational failure modes displaying similar operational effects are regrouped under the same operational hazard), together with the assessed severity of the most probable effect of the operational hazard occurrence as per the relevant AIM-based Severity Classification Scheme(s) (SCS) from Guidance G.3 of Safety Reference Material.

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
RPS Operations does not anticipate/prepare a possible C2LL contingency: • On first radio contact, the RP does not provide the established **information related to the C2LL contingency** to the ATS Unit, or provides the wrong one (Includes Hr#2)	RP does not apply procedure for first radio contact. RP is not available.	If a C2LL does not occur: • Light increase of workload of ATCO and RP in order to correct the mistake.	No communication: **M1**. ATCO needs to recognize a RPAS (**SRD 003A:** ATCO shall be able to easily recognise the RPAS traffic (CWP) / HMI (REQ-PJ13.115-SPRINTEROP-0070)) **M2.** ATCO detects the lack of information related to the C2LL behaviour and requests the RP the missing information (Current mitigation means: ATCOs are trained to request information, if necessary, to the pilots flying in their sectors). **Assumption 005** **M3**. The ATCO has a means of recording the information related to the contingency procedure. **Assumption 005** **M4.** There will always be an additional/backup pilot in the Remote Pilot Station to cross-check. (**SRD_candidate_001:** A team of pilots shall be always available to manage the RPA, and one will take the RP position whenever necessary (REQ-PJ13.115-SPRINTEROP-0350)) Incorrect communication: **M4.** There will always be an additional/backup pilot in the Remote Pilot Station to cross-check. (**SRD_candidate_001:** A team of pilots shall be always available to manage the RPA, and one will take the RP position whenever necessary (REQ-PJ13.115-SPRINTEROP-0350)) **M5**: RP can recheck programmed behaviour at any time before a C2LL occurs (skill included within RP's training). *Only valid in case the information in the system is wrong. If the RP rechecks it and detects the mistake, they shall contact the ATCO again to provide the correct data (for example, the diversion point is hundreds of NM away: named WPTs – more than one with the same name (different locations) can exist in the NAV database, and thus inadvertently selected in the nav system programming).* **Assumption 006b**	**OH 01a:** Incorrect preparation of a possible C2LL contingency: on first radio contact, the RP does not communicate the contingency procedure to ATC or communicates incorrect contingency procedure information. Severity: MAC_SC04b
		If a C2LL occurs without the inconsistency being detected: • Increase of workload of ATCO to	If a C2LL occurs without the failure being detected, the following additional mitigations are also available: **Assumption A001:** During the accommodation phase, RPAS will operate in medium/low traffic density environments. **Assumption A001:** During the accommodation phase, all traffic is known and cleared into the controlled airspace.	**OH 02:** Inconsistency between the programmed C2LL contingency procedure and the ATCO expectations of the RPAS trajectory. Severity: MAC_SC04a

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
		manage/separate ATCO at a later stage. • Increase of workload of the RP in order to check and transmit the correct information. • Unknown/unexpected RPA flight trajectory in case of C2LL. Possible loss of separation between the RPA and other aircraft.	**Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M6.** ATCO could apply larger separation to RPAS that squawks the designated C2LL code (**SRD 017**: ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150)). **M7.** RPAS FL limited such as to reduce chances to have traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders) (**SRD_candidate_002:** RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040)) *(this makes the severity decrease from SC03 to SC04b)*. **M8.** RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M10.** In the short term, there is no change in the RPAS trajectory. The ATCO will have time to get the correct information from the RP via the alternative communication mean. (**SRD 013:** The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260))	

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
			M11a: In the medium/long term, the ATCO will be able to detect a deviation in the execution of the C2LL trajectory through active surveillance (SSR code and radar available). Via the alternative communication means, the ATCO will be able to get feedback from the RP about the status of the C2L and/or about the procedure pre-programmed or re-programmed so that they can check if it is the expected one. (**SRD 006:** ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)) **M12:** ATCO are trained to face non-nominal situations involving RPA traffics (**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)) **Issue I001:** In case C2LL occurs just after vectoring instructions there might be not sufficient time for ATCO to fully check the details of the contingency procedure with the RP (currently 2 minutes – To be validated). *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	
RPS Operations does not anticipate/prepare a possible C2LL contingency when receiving new instructions from the ATS Unit during the flight or when flying the filled FP. This includes: - Not re-programming or incorrectly re-programming the C2LL contingency procedure into RPA with the	RP does not correctly manage the instructions received by ATCO. RP's loss of situational awareness. Lapse due to workload, demanding operational environment, etc. RP is not available.	<u>If a C2LL does not occur:</u> - Light increase of workload of the ATCO and the RP in order to correct the mistake.	**M2.** ATCO detects the lack of information related to the C2LL behaviour and requests the RP the missing information (Current mitigation means: ATCOs are trained to request information, if necessary, to the pilots flying in their sectors). **Assumption 005** **M5**: RP can recheck programmed behaviour at any time before a C2LL occurs (skill included within RP's training). **Assumption 006b** **M13:** RP can request ATCO to confirm that the C2LL trajectory is conforming to information provided to ATCO. **Assumption 006b**	**OH 01a:** Incorrect preparation of a possible C2LL contingency: <u>when receiving new instructions from ATCO</u>, RP does not communicate the contingency procedure to ATC or communicates incorrect contingency procedure information. Severity: MAC_SC04b **OH 01b:** Incorrect preparation of a possible C2LL contingency: RP does

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
contingency waypoints. (Hr#1). • Not providing the re-programmed C2LL contingency procedure to the ATS Unit, or communicating the wrong one. (Hr#2).				not (correctly) re-program the C2LL contingency procedure in the RPA system. Severity: MAC_SC04b
		If a C2LL occurs without the inconsistency being detected: • Increase of workload of ATCO to manage/separate RPA at a later stage. • Increase of workload of the RP in order to check and transmit the correct information. • Unknown/unexpected RPA flight trajectory in case of C2LL. Possible loss of separation between the RPA and other aircraft. • Possible conflict between two RPAS both in a C2LL situation.	If a C2LL occurs without the failure being detected, the following additional mitigations are also available: **Assumption A001:** During the accommodation phase, RPAS will operate in medium/low traffic density environments. **Assumption A001:** During the accommodation phase, all traffic is known and cleared into the controlled airspace. **Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation**M6.** ATCO could apply larger separation to RPAS that squawks the designated C2LL code (**SRD 017**: ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150)). **M7.** RPAS FL limited such as to reduce chances to have traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders) (**SRD_candidate_002:** RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040)) *(this makes the severity decrease from SC03 to SC04b)*. **M8.** RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is	**OH 02:** Inconsistency between the programmed C2LL contingency procedure and the ATCO expectations of the RPAS trajectory. Severity: MAC_SC04a

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
			below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M10.** In the short term, there is no change in the RPAS trajectory. The ATCO will have time to get the correct information from the RP via the alternative communication mean. (**SRD 013:** The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260)). **M11a**: In the medium/long term, the ATCO will be able to detect a deviation in the execution of the C2LL trajectory through active surveillance (SSR code and radar available). Via the alternative communication means, the ATCO will be able to get feedback from the RP about the status of the C2L and/or about the procedure pre-programmed or re-programmed so that they can check if it is the expected one. (**SRD 006:** ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)) **M12:** ATCO are trained to face non-nominal situations involving RPA traffics (**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)) **Issue I001:** In case C2LL occurs just after vectoring instructions there might be not sufficient time for ATCO to fully check the details of the contingency procedure with the RP (currently 2 minutes – To be validated). *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	
Malfunction of C2 link (e.g., abnormal delay, total loss) (Hr#4)	Technical failure	Increase of workload of ATCO and RP to manage the C2LL situation.	**Assumption A006:** It is considered that RPs are already trained with regard to the basic procedures and way of operating. Therefore, actions such as: • the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)*, or	**OH 03.** Malfunction of the C2 link. Severity: MAC_SC03

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
		RPA is no longer controllable by the RP: RP does not comply with the instructions received from the ATS Unit (this includes not modifying RPAS pre-programmed navigation/non-programmed navigation mode (direct autopilot) and trajectory according to these instructions). RP loss the situation awareness with the RPA. Integration of the established procedure for the loss of C2L of a RPA in the management of traffic by ATS Unit. Possible conflict with other aircraft. Possible conflict between two RPAS both in a C2LL situation.	• the detection of the C2LL (loss of data with the RPA), are considered within RP's current skills. **Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M14.** RPA makes sure that the malfunction is not temporary. RPA only sets code when malfunction is confirmed: decision time implemented (existing RPAS feature / mitigation). **Assumption 006b** **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M15.** Availability of a predictable C2LL trajectory pre-programmed/re-programmed to take into account latest conditions. The trajectory is always available in RPA and is automatically activated if C2LL condition detected. (**SRD 009:** RP shall always pre-program RPA with a C2LL trajectory that shall be automatically triggered and flown when the RPAS goes into a C2LL state (REQ-PJ13.115-SPRINTEROP-0310)) **M6.** ATCO could apply larger separation to RPAS that squawks the designated C2LL code (**SRD 017**: ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150)). **M11b.** The ATCO monitors the traffic continuously and will be able to detect possible deviations or issues related to the RPA. (Current mitigation means). **Assumption 005** **M16a**: Only one RPA will operate at the same time under responsibility of one sector. **M16b:** In very specific and limited situations in which RPAS demand is to operate in pairs, the two RPAs shall not have crossing C2LL trajectories (in space or in time) at any time	

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
			during the contingency – this requires C2LL trajectories strategic-agreement between RPAS operator and ANSP. (**SRD 016:** Only one RPAS shall be authorized to fly at the same time under responsibility of one sector. In those specific cases in which two RPAS are inevitably operating under the responsibility of the same sector (demand of RPAS operating in pairs, collapsed sectors during the period of flight of the RPAS, etc.), the RPAS operator (single operator for the two RPAS) shall guarantee through strategic-agreement with the ANSP that the two RPAs will not have crossing trajectories (in space or in time) at any time during a possible C2LL contingency. Moreover, as the RP will be providing the C2LL behaviour at initial contact, the ATCO can also check that the C2LL behaviour of the two RPAS are not in conflict, which is assumed to generate negligible additional planning workload. (REQ-PJ13.115-SPRINTEROP-0050) **M12:** ATCO are trained to face non-nominal situations involving RPA traffics (**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)) *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	
RPAS malfunction: the system does not initiate the pre-programmed/re-programmed contingency procedure once the C2LL occurs or starts/follows the wrong one.	Technical failure. Wrong pre-programmed/re-programmed contingency procedure introduced in the RPA system	Increase of workload of ATCO and RP to manage the RPA. Increase of coordinations between the ATCO and the RP. Unknown/unexpected RPA flight trajectory. Possible loss of separation between the RPA and other aircraft.	**Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence, and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M17.** Ensure that the pre-programmed trajectory equipment performance and integrity standards meet at least the navigation requirements in the targeted class of airspace. (**SRD_candidate_004:** RPAS shall be able to navigate during flight in a structured airspace with performances and capabilities associated with the airspace, including the C2LL trajectory:	**OH 04:** Malfunction of RPA system: the RPA system fails to initiate the pre-programmed/re-programmed contingency procedure once the C2LL occurs or starts/follows the wrong one. Severity: MAC_SC04a

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
			• Positioning aids (GNSS, inertial); • AIRAC cyclic navigation data (ATS routes, waypoints); • RNAV required in the class A-C airspace environment (RNAV5 En-Route / RNAV1 Terminal); (REQ-PJ13.115-SPRINTEROP-0090)) **M6.** ATCO could apply larger separation to RPAS that squawks the designated C2LL code (**SRD 0017**: ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150)). **M8.** RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M9.** Availability of alternative communications means. (**SRD 014:** A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)). **M11a**: In the medium/long term, the ATCO will be able to detect a deviation in the execution of the C2LL trajectory through active surveillance (SSR code and radar available). Via the alternative communication means, the ATCO will be able to get feedback from the RP about the status of the C2L and/or about the procedure pre-programmed or re-programmed so that they can check if it is the expected one. (**SRD 006:** ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)) *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
ATS Unit does not integrate the established procedure for the loss of C2L of an RPAS in the management of the other traffic (Hr#3)	ATCO lacks training/experience (RPAs are new actors in IFR controlled airspace classes A to C). Lapse due to workload, demanding operational environment, etc. ATCO does not have the information about the RPA's behaviour during contingency.	Increase of workload of ATCO to manage traffic. Increase of coordinations between the ATCO and the RP. Increase of separation actions from the ATCO to other pilots of manned aircraft. Possible loss of separation between the RPA and other aircraft.	**Assumption 005.** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/ operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the managing of emergency/contingency-related situations in which manned traffic have particular behaviour is within ATCO's current skills **Assumption A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation **M18.** RP provides information to the ATCO prior to contingency (**SRD 002:** RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)) **M19:** The trajectory in the RPA is programmed, so it is fixed and predictable (**SRD 002:** RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)) **M3**. The ATCO has a means to record the information about the contingency procedure. **Assumption 005** *NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.*	**OH 05:** The ATS Unit fails to integrate the established procedure for the loss of C2L of an RPAS in the management of the other traffic. Severity: MAC_SC04b
The RPAS emergency does not allow it to reach the programmed landing location.	The RPA was not initially programmed to land in an appropriate site. The RP did not programme or control the RPA.	Landing with risk to ground assets.	**Assumption A005.** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that coordinating the contingency management with the different actors (not only RP, but also State Authority / Civil Authority, and Airport/ Airport Operations) is similar as for manned aviation and within ATCO's current skills.	**OH 06:** The RPA fails to reach the programmed landing location Severity: MAC_SC04b

EUROPEAN PARTNERSHIP
Co-funded by the European Union

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
	The RPA performance during the emergency does not allow it to fly as planned.		**Assumption A006.** It is considered that RPs are already trained with regard to the basic procedures and way of operating. Therefore, the application of procedures/operating methods for non-nominal situations is within RP's current skills (no additional training because of flying in GAT). The RPA behaves / is controlled in a similar way than manned aircraft, taking into account the limitations of RPAs (for example, limited flying time, which will reduce the options for the landing). **M20.** The RP takes into account the current situation, and RPAS characteristics including emergency limited endurance when pre/re-programming a C2LL trajectory & landing destination. **Assumption 010**	
Loss of Remote Pilot situational awareness (including environmental, mode and system awareness, spatial disorientation, and time horizon) (Hr#5)	RP operates from a Remote Pilot Station instead of being inside the aircraft.	Increase of workload of RP to manage the RPA. Increase of workload of ATCO to manage traffic. RP incorrectly complies with the instructions received from the ATS Unit. Unknown/unexpected RPA flight trajectory. Possible loss of separation between the RPAS and other aircraft.	**Assumption A001:** During the accommodation phase, RPAS will operate in medium/low traffic environments. **Assumption A001:** During the accommodation phase, all traffic is known and cleared into the controlled airspace. **M21.** RP has equivalent information in their remote cockpit to manned aircraft (for similar aircraft types and environmental conditions) (Current mitigation means) **Assumption 007** **M7.** RPAS FL limited such as to reduce chances to have traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders) (**SRD_candidate_002:** RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040)) *(this makes the severity decrease from SC03 to SC04b)*. **M8.** RPAS speed is limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kn. (**SRD_candidate_003:** RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410)). **M11b.** The ATCO monitors the traffic continuously and will be able to detect possible deviations or issues related to the RPA. (Current mitigation means). **Assumption 005**	**OH 07.** Loss of Remote Pilot situational awareness. Severity: MAC_SC04b

Use Case / Operational failure mode	Example of causes& preventive mitigations	Operational effect	Mitigations protecting against propagation of effects	Operational hazard & Severity
			NOTE. The operational effects considered in the severity allocation do not rely on the remaining barriers which are STCA, ACAS and visual warnings.	

Table 20. Full HAZID working table

The following operational failure modes were discarded:

- RP does not comply with the instructions received from the ATS Unit (this includes not modifying RPAS pre-programmed navigation/non-programmed navigation mode (direct autopilot) and trajectory according to these instructions) → the causes and effects are the same as for manned aviation, unless this failure is related to a malfunction of the systems within the RPA (these situations have been captured in other hazards)
- Misinterpretation of radio-communication which has or could have endangered the aircraft, other aircraft, or any person (side effect of standard latency in relayed communication link) (Hr#7) → The causes and effects are the same as for manned aviation, since the expected latency time under 2 seconds does not play a significant role in the management of short-term conflicts. Previous trials have been performed in this operational environment and latency has been reported as a non-significant aspect: ATCOs and RPs can cope with the additional communication delay due to RPAS architecture.

D.2 HAZID participation list

Two HAZID workshops were conducted the 14th of January and the 7th of February 2022. The detailed list of attendees can be found in the meeting registers in Stellar:

- https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F27998203
- https://stellar.sesarju.eu/?link=true&domainName=saas&redirectUrl=%2Fjsp%2Fproject%2Fproject.jsp%3FobjId%3Dxrn%3Adatabase%3Aondb%2Frecord%2F28491054

Appendix E Designing the Solution functional system for normal conditions

E.1 Deriving SRD from the SRS

The Table 21 below shows how the Safety Requirements at ATS Service level (SRS) for normal conditions of operation derived in section 4.2 map onto the related elements of the Design Model (functional system components or interactions/data flows) and derive Safety Requirements at Design level (SRD) (functionality & performance) for normal conditions of operation. . It includes the following information:

- the SRS (functionality & performance) to mitigate risk in normal condition, as presented in section 4.2.
- the derived SRD driven by the mapping of the SRS onto the related elements of the Design Model, accompanied by relevant Assumptions as appropriate.
- the Design Model elements (functional system components or interactions/data flows or external elements impacted by the Change) relevant for the derived SRD and/or assumptions.

The consolidated list of derived SRDs is to be included in section 5.3.1, while the associated assumptions are included in the Assumptions log table from Appendix I.1

The Safety Requirement identified in Table 21 are consistent with the ones defined in Section 4 of SPR-INTEROP/OSED Part I.

SRS for Normal Operation (ID & content)	Safety Requirement at Design level[13] (SRD) or Assumption	Maps onto
SRS 001a: The RP shall initiate contact with the relevant ATS Unit.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training
SRS 001b: The RP shall provide the ATCO in initial radio contact with each sector with the standard contact information regarding identification including RPAS, next route element(s)/flight level and minimum elements of the pre-programmed C2LL contingency trajectory	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training
	SRD 002: RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)	Model element (service interaction): RPS→ ER ACC/ APP ACC
SRS 002: The ATS Unit shall acknowledge the RP's first notification and assume the control of RPAS flight.	**A005**: From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groupings of sectors concerned. Therefore, the current training of the ATCOs prepares them to manage radio communications in order to assume the control of the different flights and provide them with instructions.	Model element (function): ER ACC/ APP ACC

[13] iSRD for the initial design or rSRD for the refined design

SRS for Normal Operation (ID & content)	Safety Requirement at Design level[13] (SRD) or Assumption	Maps onto
	SRD 003A: ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)	Model element (info): RPAS identification Model element (info): Air Surveillance data
	SRD 003B: The RP shall add "REMOTE" to the callsign (REQ-PJ13.115-SPRINTEROP-0340)	Model element (info): RPAS identification
	SRD 004: ATC shall be able to support the accommodation of non-segregated transit GAT RPAS among all other GAT (REQ-PJ13.115-SPRINTEROP-0010)	External element: coordination between ATS Units (civil-military)
SRS 003a: The ATS Unit shall monitor the RPAS flight trajectory through cooperative secondary radar surveillance data.	**SRD 003A:** ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)	Model element (info): Air Surveillance data
	SRD 005: ATCO shall be trained and shall be able to apply standard IFR procedures/operating methods to RPAS for nominal IFR situations thus to reiterate requests to RP for expected information (REQ-PJ13.115-SPRINTEROP-0230).	External element: training
	SRD 006: ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)	Model element (info): Air Surveillance data
SRS 003b: The ATS Unit shall use surveillance data to monitor the traffic (manned and unmanned), in order to apply separation minima between aircraft. *The objective is for ATS Unit to apply identical separation minima with the RPAS.*	**SRD 003A:** ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)	Model element (info): Air Surveillance data
	SRD 005: ATCO shall be trained and shall be able to apply standard IFR procedures/operating methods to RPAS for nominal IFR situations thus to reiterate requests to RP for expected information (REQ-PJ13.115-SPRINTEROP-0230).	External element: training
	SRD 006: ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300)	Model element (info): Air Surveillance data
	SRD 007: ATCO shall be able to use usual surveillance and conflict management methods (REQ-PJ13.115-SPRINTEROP-0280).	External element: ATC operating methods
SRS 004a: The ATS Unit shall detect the possible conflicts with RPAS flight trajectory	**SRD 003A:** ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)	Model element (info): Air Surveillance data
	SRD 005: ATCO shall be trained and shall be able to apply standard IFR procedures/operating methods to RPAS for nominal IFR situations thus to reiterate requests to RP for expected information (REQ-PJ13.115-SPRINTEROP-0230).	External element: training
	SRD 006: ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300).	Model element (info): Air Surveillance data

SRS for Normal Operation (ID & content)	Safety Requirement at Design level[13] (SRD) or Assumption	Maps onto
	SRD 007: ATCO shall be able to use usual surveillance and conflict management methods (REQ-PJ13.115-SPRINTEROP-0280).	External element: ATC operating methods
SRS 004b: The ATS Unit shall issue clearances and provide instructions to RPAS for resolution of conflicts (Vector/ Heading/ Altitude/ Speed instructions).	**SRD 005:** ATCO shall be trained and shall be able to apply standard IFR procedures/operating methods to RPAS for nominal IFR situations thus to reiterate requests to RP for expected information (REQ-PJ13.115-SPRINTEROP-0230).	External element: training
	SRD 007: ATCO shall be able to use usual surveillance and conflict management methods (REQ-PJ13.115-SPRINTEROP-0280).	External element: ATC operating methods
SRS 006b: RPS Operations shall modify RPAS navigation according to the new instructions provided by ATS Unit	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training
	SRD 008: RP shall be able to modify the RPAS pre-programmed navigation according to the new instructions (REQ-PJ13.115-SPRINTEROP-0320).	Model element (service interaction): RPS → RPA
SRS 005: Upon obtaining a new clearance/instruction, RPS Operations shall verify compatibility of existing pre-programmed C2LL contingency trajectory, and if necessary, re-program a revised C2LL contingency trajectory.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training
	SRD 009: RP shall always pre-program RPA with a C2LL trajectory that shall be automatically triggered and flown when the RPAS goes into a C2LL state (REQ-PJ13.115-SPRINTEROP-0310). *NOTE: The RP shall re-program this C2LL trajectory whenever it is required*	Model element (service interaction): RPS → RPA
SRS 006a: If a C2LL contingency trajectory is re-programmed/revised, RPS Operations shall provide information of the revised C2LL trajectory to ATCO, at or after clearance/instruction read-back.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training
	SRD 002: RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness. (REQ-PJ13.115-SPRINTEROP-0110).	Model element (service interaction): RPS→ ER ACC/ APP ACC
SRS 007: RPS Operations shall continue to monitor the RPA trajectory during nominal flight.	**A006**: It is considered that RPs are already trained with regard to the basic procedures and way of operating. Therefore, actions such as the monitoring of the flight trajectory are within RP's current skills.	External element: training
SRS 008: Transferring ATS Unit (civil) shall transfer radio and radar	**SRD 010:** Procedures regarding the transfer of control of RPAS between ATS units in nominal conditions shall be	External element: LoA between ATS Units

SRS for Normal Operation (ID & content)	Safety Requirement at Design level[13] (SRD) or Assumption	Maps onto
RPAS flight contact to accepting ATS Unit	used per the LoA or operations manual in effect (REQ-PJ13.115-SPRINTEROP-0400).	
SRS 009: Accepting ATS Unit (civil or military) shall assume radio and radar control of RPAS flight and issue ATC clearances and instructions	**A005**: From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groupings of sectors concerned. Therefore, the current training of the ATCOs prepares them to manage radio communications in order to assume the control of the different flights and provide them with instructions.	Model element (function): ER ACC/ APP ACC
	SRD 003A: ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)	Model element (info): Air Surveillance data
	SRD 003B: The RP shall add "REMOTE" to the callsign (REQ-PJ13.115-SPRINTEROP-0340)	Model element (info): RPAS identification
	SRD 004: ATC shall be able to support the accommodation of non-segregated transit GAT RPAS among all other GAT (REQ-PJ13.115-SPRINTEROP-0010)	External element: coordination between ATS Units (civil-military)
	SRD 010: Procedures regarding the transfer of control of RPAS between ATS units in nominal conditions shall be used per the LoA or operations manual in effect (REQ-PJ13.115-SPRINTEROP-0400).	External element: LoA between ATS Units
SRS 010a: RPS Operations shall contact accepting ATS Unit *(and also provide the ATCO in initial radio contact with C2LL behaviour information →→ see SRS 001b)*	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training
	SRD 002: RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110).	Model element (service interaction): RPS→ ER ACC/ APP ACC
SRS 010b: RPAS shall enter the new sector through the instructed point and after the RP establishes contact with the relevant accepting ATS Unit.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations (REQ-PJ13.115-SPRINTEROP-0240).	External element: training

Table 21: SRD derived by mapping SRS for normal conditions of operation to Design Model Elements

E.2 Static analysis of the solution functional system behaviour

No static analysis has been carried out

E.3 Dynamic analysis of the Solution functional system behaviour

No static analysis has been carried out

Appendix F Designing the Solution Functional system for Abnormal conditions of operation

F.1 Deriving SRD from SRS

The Table 22 below shows how the Safety Requirements at ATS Service level (SRS) for abnormal conditions of operation derived in section 4.3 map onto the related elements of the Design Model (functional system components or interactions/data flows) and derive Safety Requirements at Design level (SRD) (functionality & performance) for abnormal conditions of operation. Include the following information:

- the SRS (functionality & performance) to mitigate the consequences of the abnormal condition, as presented in section 4.3,
- the derived SRD driven by the mapping of the SRS onto the related elements of the Design Model, together with the used assumptions as appropriate,
- the Design Model elements (functional system components or interactions/data flows or external elements impacted by the Change) relevant for the derived SRD and/or assumptions.

The consolidated list of derived SRDs is to be included in section 5.4.1, while the associated assumptions are included in the Assumptions log table from Appendix I.1.

The Safety Requirement identified in Table 22 are consistent with the ones defined in Section 4 of SPR-INTEROP/OSED Part I.

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
ABN1	**SRS 011:** ATS Unit shall be informed of the RPAS C2LL through a specifically designed SSR code automatically set by RPA Operations *NOTE: RPAS is pre-programmed to squawk a specific SSR code as soon as C2LL is detected*	**SRD 012:** RPA shall be able to automatically provide specific C2 link loss transponder code and to maintain it active during C2 link loss (REQ-PJ13.115-SPRINTEROP-0140)	Model element (function): En-route/Approach ATC
		SRD 013: The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260). *RP (resp. ATCO) will request ATCO (resp. RP) to confirm by telephone that the message is well understood, and the ATCO will recontact RP if the behaviour is not conforming to the understood behaviour.*	Model element (service interaction): RPS ←→ En-route/Approach ATC
		SRD 002: RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110)	Model element (service interaction): RPS → En-route/Approach ATC
ABN1	**SRS 012:** Follow-up of C2LL Contingency shall be coordinated between ATS Unit and RPS Operations through a backup audio (telephone or direct point-to-point line, if equipped) to exchange useful	**A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL	External element: pre-condition

Co-funded by the European Union

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
	information, in particular, the remote pilot shall provide details of the C2LL trajectory/behaviour, and the ATCO shall provide information regarding the next ATC sector.	contingency is equivalent to the increase of workload due to a PLOC in manned aviation	
		SRD 014: A direct telephone line shall be available between ATC and RP/RPS as backup solution in C2 link loss situation (REQ-PJ13.115-SPRINTEROP-0120)	External element: alternative communications means
		SRD 0013: The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260)	Model element (service interaction): RPS ←→ ER ACC/APP ACC
ABN1	**SRS 013:** ATS Unit shall monitor traffic and apply an adapted separation strategy as deemed necessary by ATCO to separate the RPA C2LL trajectory from other (manned) aircraft trajectories.	**A011:** Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation	External element: pre-condition
		SRD 015: ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)	External element: training
		SRD 016: Only one RPAS shall be authorized to fly at the same time under responsibility of one sector In those specific cases in which two RPAS are inevitably operating under the responsibility of the same sector (demand of RPAS operating in pairs, collapsed sectors during the period of flight of the RPAS, etc.), the RPAS operator (single operator for the two RPAS) shall guarantee through strategic-agreement with the ANSP that the two RPAs will not have crossing trajectories (in space or in time) at any time during a possible C2LL contingency. Moreover, as the RP will be providing the C2LL behaviour at initial contact, the ATCO can also check that the C2LL behaviour of the two RPAS are not in conflict, which is assumed to generate negligible additional planning workload. (REQ-PJ13.115-SPRINTEROP-0050)	External element: pre-condition
		SRD 017: ATC shall be able to support the specific RPAS contingency procedures:	Model element (function): ER ACC/APP ACC

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
		• Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150).	
ABN1	**SRS 014:** RPAS shall fly the contingency procedure. This contingency procedure shall be pre-programmed in Flight Plan, or re-programmed in-flight as necessary, if a vector/heading/altitude/speed instruction has been given by the ATS Unit.	**A 009:** Aside from internal system malfunctions, RPA systems follow the pre-programmed/ re-programmed procedures introduced by RPS Operations.	Model element (function): RPA
ABN1	**SRS 015:** RPS Operations shall monitor the C2 link state trying to re-establish it (if possible, with the available RPS means).	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.	External element: training
ABN1	**SRS 016:** If the C2L is never re-established, the RPAS shall continue flying its pre-programmed C2 link loss (C2LL) contingency trajectory. This includes: - Returning to flight plan after a set time, - Flying until the DIVERSION pre-programmed waypoint, from where it shall continue flying to the pre-programmed C2LL destination airfield, that the operator will have chosen during pre-programming (an alternate aerodrome, or the departure one, or the original final destination).	**A 009:** Aside from internal system malfunctions, RPA systems follow the pre-programmed/ re-programmed procedures introduced by RPS Operations	Model element (function): RPA
		SRD 017: ATC shall be able to support the specific RPAS contingency procedures: • Recognize C2LL information provided in the procedure to know possible C2LL trajectory of RPAS (REQ-PJ13.115-SPRINTEROP-0150).	Model element (function): ER ACC/APP ACC
ABN1	**SRS 017:** If the C2L is re-established**,** RPS Operations shall detect it and inform ATS	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.	External element: training
ABN1	**SRS 018:** If the C2L is re-established, RPS Operations shall revert to previous transponder code (SQUAWK). *NOTE: Reversion to the original (previous) transponder code is*	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.	External element: training

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
	on ATCO instruction (thus not automated: if C2L is working, the RP can change the squawk as often as required).		
ABN1	**SRS 019:** If the C2L is re-established, RPS Operations shall use the frequency communicated at telephone coordination to contact the appropriate ATS Unit.	**A 006 A):** It is considered that RPs are already trained with regard to the IFR procedures and way of operating. Therefore, actions such as initiating contact with the relevant ATS Unit (including first radio contact both when reaching the first GAT sector and when transferred to the next/adjacent ATS Unit) are within RP's current skills.	External element: training
ABN2	**SRS 020:** RPA Operations shall determine the engine status in order to analyse the impact of engine loss	**SRD 018:** RPAS shall be able to identify its emergency status and to execute the emergency procedure associated with the severe failure situation. (REQ-PJ13.115-SPRINTEROP-0160)	Model element (function): RPA
ABN2	**SRS 021:** RPS Operations shall broadcast emergency state through the emergency frequency to all concerned traffic.	**SRD 019:** RPAS shall be able to set specific emergency transponder code and to maintain it active during emergency. (REQ-PJ13.115-SPRINTEROP-0180)	Model element (function): RPA
ABN2	**SRS 022:** RPAS shall follow the Emergency Flight Plan to guarantee the highest level of safety. Use of the "Safest Shortest" principle to make that decision.	**SRD 018:** RPAS shall be able to identify its emergency status and to execute the emergency procedure associated with the severe failure situation. (REQ-PJ13.115-SPRINTEROP-0160)	Model element (function): RPA
		SRD 020: ATC shall be able to manage RPAS emergency situation (REQ-PJ13.115-SPRINTEROP-0190) *This includes the appropriate coordination with RP or other actors in order to manage the emergency situation*	Model element (service interaction): RPS ←→ ER ACC/APP ACC
		SRD 021: RPAS shall be able to remain on the RP controlled/selected trajectory, which takes into account emergency performance (REQ-PJ13.115-SPRINTEROP-0170)	Model element (function): RPA
ABN2	**SRS 023:** RP shall contact/coordinate with the ATS Unit to declare the flight path to terminate the flight in the worst-case scenario, that is, where the emergency destination is not achievable.	**SRD 020:** ATC shall be able to manage RPAS emergency situation (REQ-PJ13.115-SPRINTEROP-0190) *This includes the appropriate coordination with RP or other actors in order to manage the emergency situation*	Model element (service interaction): RPS ←→ ER ACC/APP ACC
		SRD 021: RPAS shall be able to remain on the RP controlled/selected trajectory, which takes into account emergency performance (REQ-PJ13.115-SPRINTEROP-0170)	Model element (function): RPA
ABN2	**SRS 024:** RPAS shall monitor Emergency Flight in order to:	**A006:** It is considered that RPs are already trained with regard to the basic procedures and way of operating. Therefore, actions such as alerting the relevant ATCO when a deviation that	External element: training

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
	• control the trajectory and adhere to declared Emergency Flight Plan. • alert ATCO when a deviation is observed that cannot be mitigated by RPS Operations.	cannot be mitigated by crew is observed are within RP's current skills	
		SRD 018: RPAS shall be able to identify its emergency status and to execute the emergency procedure associated with the severe failure situation. (REQ-PJ13.115-SPRINTEROP-0160)	Model element (function): RPA
ABN2	**SRS 025:** ATS Unit shall coordinate termination of the emergency RPA flight with the State/ military authority or civil authority in case of Military/State terminal area(Airfield / Ditching area) or in case of entering uncontrolled area all along the flight.	**A 005:** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/ operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the following action are within ATCO's current skills: • Clearing of the path for RPAS trajectory (ACC/APP Controller).	Model element (function): ER ACC/APP ACC
		A 005: From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/ operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the following actions are within ATCO's current skills: • Preparing airspace and runways for the emergency arrival of the RPAS (TWR Controller).	Model element (function): TWR
		A 010: Regarding emergencies related to RPAS flights (for example, engine failure): • The RP will be still under limited control of the RPA and will have voice communications. • The RPAS will fly a FPLN / trajectory deemed suitable by the Remote Pilot (within capabilities of the emergency state). It will be flown by the RP to an EMERGENGY DIVERSION waypoint and then to a termination area (airfield or emergency landing site). The information will be provided by the RP to ATC. • From an ATCO perspective, the management of this emergency flight has no additional RPAS particularities: the same contingency specificities apply.	Model element (function): ER ACC/APP ACC ←→ TWR ER ACC/APP ACC ←→ OAT/Military ER ACC/APP ACC
ABN2	**SRS 026:** ATS Unit shall clear the path for RPAS trajectory and provide the separation of	**A 005:** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/	Model element (function): ER ACC/APP ACC

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
	surrounding traffic until RPA enters CTR.	operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the following actions are within ATCO's current skills: • Clearing of the path for RPAS trajectory (ACC/APP Controller).	
		A 010: Regarding emergencies related to RPAS flights (for example, engine failure): • The RP will be still under limited control of the RPA and will have voice communications. • The RPAS will fly a FPLN / trajectory deemed suitable by the Remote Pilot (within capabilities of the emergency state). It will be flown by the RP to an EMERGENGY DIVERSION waypoint and then to a termination area (airfield or emergency landing site). The information will be provided by the RP to ATC. • From an ATCO perspective, the management of this emergency flight has no additional RPAS particularities: the same contingency specificities apply.	Model element (function): ER ACC/APP ACC ←→ TWR ER ACC/APP ACC ←→ OAT/Military ER ACC/APP ACC
ABN2	**SRS 027:** ATS Unit shall maintain the coordination with Airport Ops Support that will host the termination action	**A 005:** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/ operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the following action are within ATCO's current skills: • Preparing airspace and runways for the emergency arrival of the RPAS (TWR Controller).	Model element (function): TWR
		A 010: Regarding emergencies related to RPAS flights (for example, engine failure): • The RP will be still under limited control of the RPA and will have voice communications. • The RPAS will fly a FPLN / trajectory deemed suitable by the Remote Pilot (within capabilities of the emergency state). It will be flown by the RP to an EMERGENGY DIVERSION waypoint and then to a termination area (airfield or emergency landing site). The information will be provided by the RP to ATC. • From an ATCO perspective, the management of this emergency flight has	Model element (function): ER ACC/APP ACC ←→ TWR ER ACC/APP ACC ←→ OAT/Military ER ACC/APP ACC

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
		no additional RPAS particularities: the same contingency specificities apply.	
ABN2	**SRS 028:** ATS Unit at arrival aerodrome shall clear its airspace and runways from any traffic, including ground vehicles, which may endanger the operation of the arriving emergency RPA.	**A 005:** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/ operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the following action are within ATCO's current skills: • Preparing airspace and runways for the emergency arrival of the RPAS (TWR Controller).	Model element (function): TWR
ABN3	**SRS 029:** RP shall be able to deal with possible sudden deterioration of weather conditions during the flight. This includes requesting the ATCO a lateral or vertical deviation to avoid the area.	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.	External element: training
		A 004: The FP is developed short before the flight and considering the latest weather forecast. Therefore, the RPAS will not operate under severe weather conditions since the trajectory included in the FP will avoid forecasted events like thunderstorms, icing, or electromagnetic disturbances.	Model element (function): RPS
ABN3	**SRS 030:** ATS Unit shall be able to manage situations related to sudden deterioration of weather conditions.	**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations. (REQ-PJ13.115-SPRINTEROP-0250).	External element: training
ABN4	**SRS 031:** RP shall be prepared for possible wake turbulence encounters during the flight.	**A 001:** During the accommodation phase, and regarding wake-turbulence separation, RPAS are considered as L category aircraft (including en-route separation).	Model element (function): RPAS weight category
		A 006 B): It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.	External element: training
		A 007: RP have traffic awareness in their RPS through radio communications on shared frequency and they are able to identify certain threatens like the wake risk and request additional instructions to ATCO, if necessary.	Model element (function): RPAS tool

Co-funded by the European Union

Ref	SRS for Abnormal Operation	Derived Safety Requirements at design level and Assumptions	Map on to
ABN4	**SRS 032:** ATS Unit shall be able to manage situations related to wake turbulence encounters.	**A 001:** During the accommodation phase, RPAS will operate in environments with medium/low density of traffic. *Therefore, the likelihood of wake encounters is extremely low.*	External element: environment
		A 001: During the accommodation phase, and regarding wake-turbulence separation, RPAS are considered as L category aircraft (including en-route separation).	Model element (function): RPAS weight category
		SRD 015: ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations. (REQ-PJ13.115-SPRINTEROP-0250).	External element: training

Table 22: SRD derived by mapping SRS for Abnormal conditions of operation onto Design Model elements

F.2 Analysis of the Solution functional system behaviour for abnormal conditions of operation

No static analysis has been carried out

Co-funded by the European Union

Appendix G Designing the Solution functional system addressing internal functional system failures

This appendix presents the detailed risk evaluation and mitigation of the operational hazards identified at section 4.4, performed at the level of the design of the Solution functional system.

G.1 Deriving SRD from the SRS (integrity/reliability)

The purpose is to derive from the SRS (integrity/reliability) that have been derived in section 4.4.2:

- SRD (functionality & performance) in order to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard.
- SRD (integrity/ reliability) to limit the frequency with which failure of modified/new equipment elements in the Solution Functional system could be allowed to occur.

The above should be derived with due consideration of the common cause failures (in case such failures are revealed by the common causes analysis).

G.1.1 Top-down causal analysis

In this section, for each operational hazard, it is performed a top-down identification of Solution functional system failures and combinations thereof that could cause the operational hazard. To achieve that, a Fault Tree showing for each operational hazard its causes and the associated mitigations is used. The latter represent preventive mitigations for the operational hazard, but they might either prevent a basic cause to occur or they protect against the propagation of the basic cause effect up to the operational hazard occurrence.

Although the SRD (functionality & performance) already derived in sections 4.2 and 4.3 play a mitigation role, additional SRD (functionality & performance) are derived in order to ensure the satisfaction of the SRS (integrity/reliability) associated to the operational hazard.

SRD (integrity/reliability) associated to internal system failures are derived from the SRS (integrity/reliability) documented in section 4.4.2, driven by the causal analysis of each operational hazard, accounting for the existing or new proposed preventive mitigations and with due consideration of any potential common cause failure.

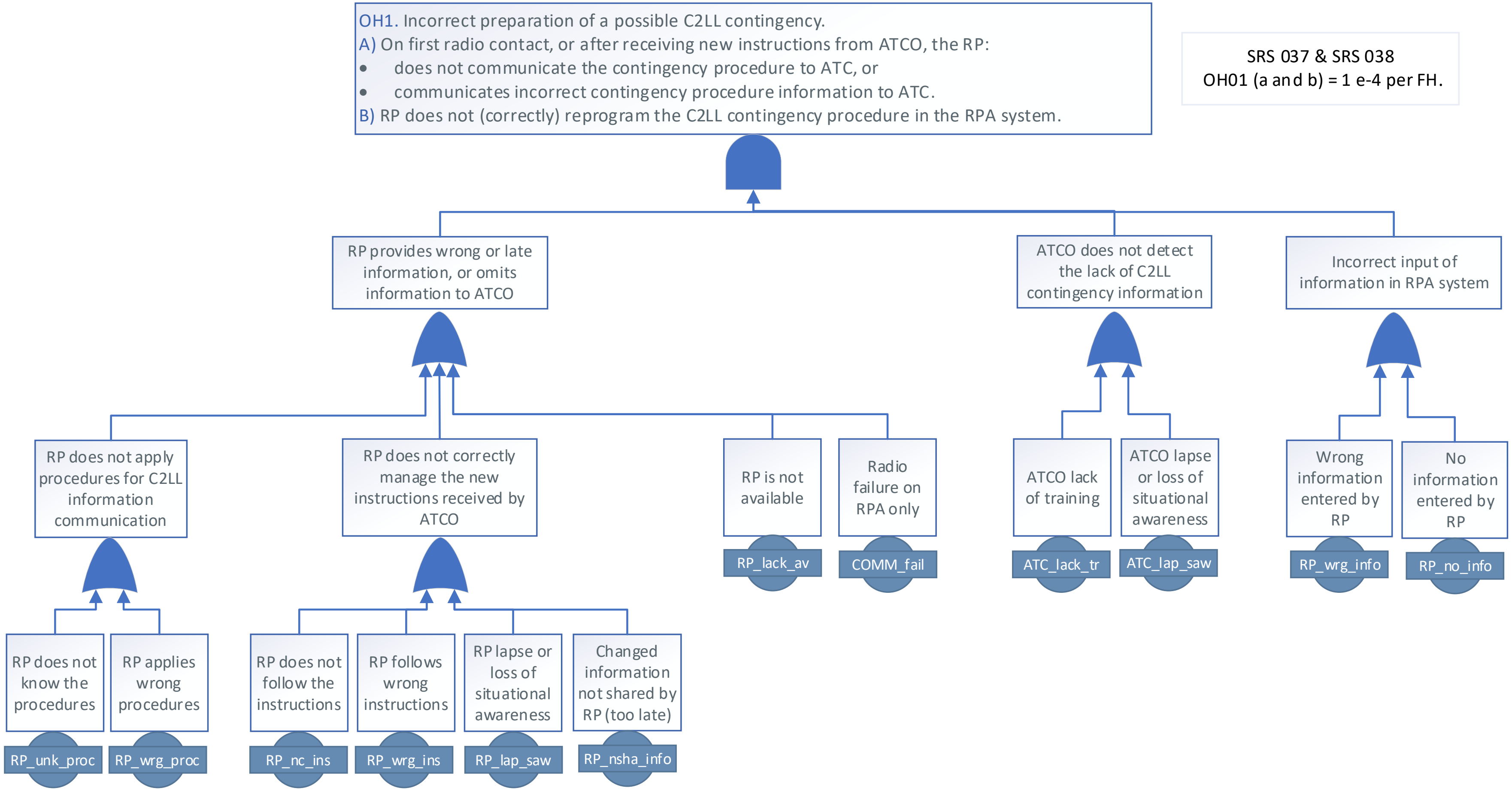

OH1. Incorrect preparation of a possible C2LL contingency.
A) On first radio contact, or after receiving new instructions from ATCO, the RP:
• does not communicate the contingency procedure to ATC, or
• communicates incorrect contingency procedure information to ATC.
B) RP does not (correctly) reprogram the C2LL contingency procedure in the RPA system.
SRS 037 & SRS 038
OH01 (a and b) = 1 e-4 per FH.
RP provides wrong or late information, or omits information to ATCO
ATCO does not detect the lack of C2LL contingency information
Incorrect input of information in RPA system
RP does not apply procedures for C2LL information communication
RP does not correctly manage the new instructions received by ATCO
RP is not available
RP_lack_av
Radio failure on RPA only
COMM_fail
ATCO lack of training
ATC_lack_tr
ATCO lapse or loss of situational awareness
ATC_lap_saw
Wrong information entered by RP
RP_wrg_info
No information entered by RP
RP_no_info
RP does not know the procedures
RP_unk_proc
RP applies wrong procedures
RP_wrg_proc
RP does not follow the instructions
RP_nc_ins
RP follows wrong instructions
RP_wrg_ins
RP lapse or loss of situational awareness
RP_lap_saw
Changed information not shared by RP (too late)
RP_nsha_info

Figure 4. Fault Tree associated to OH1

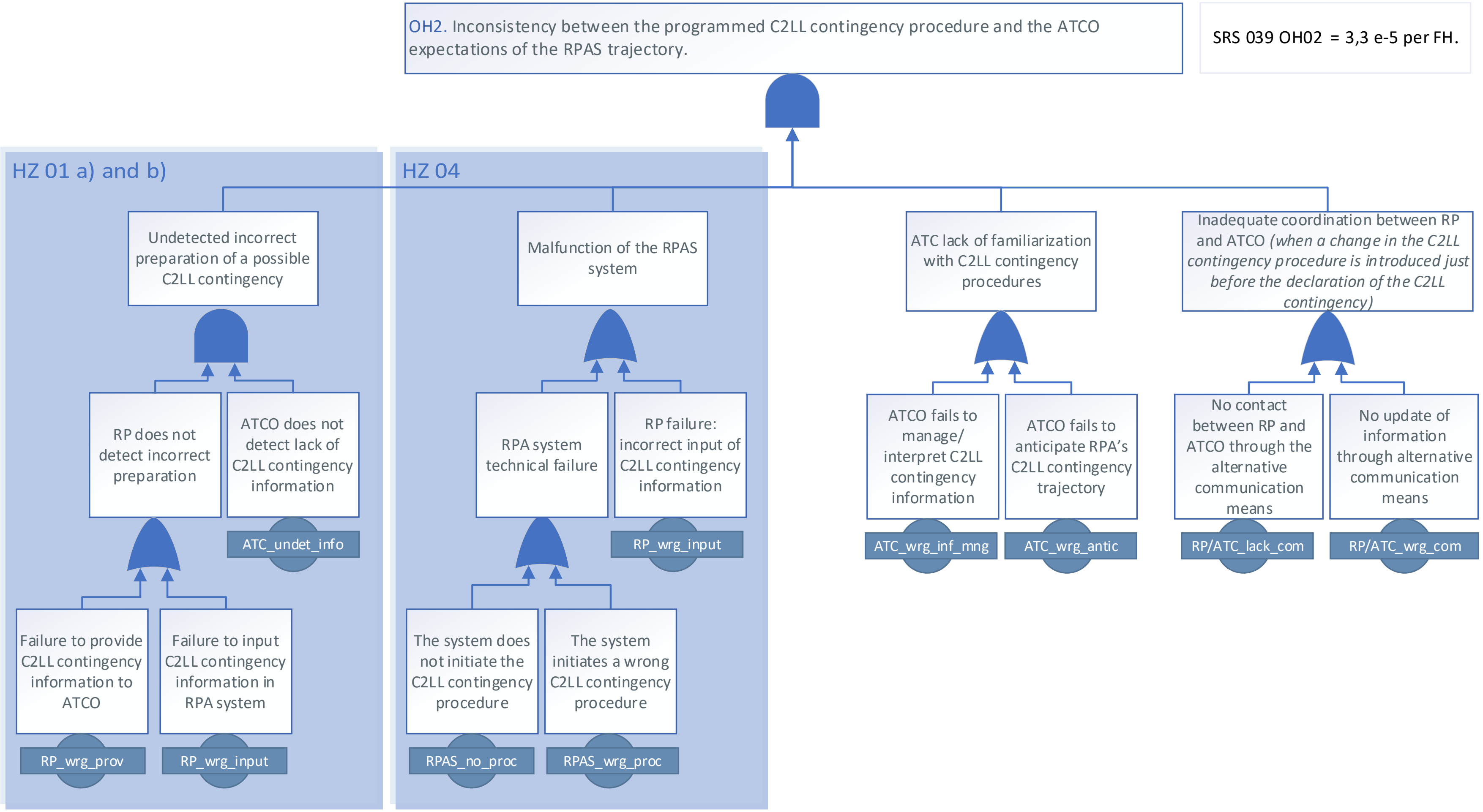
Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
RP_unk_proc [RP]	The RP does not know the C2LL procedures.	RP is not familiarized with the C2LL procedures for information communication and, therefore, he/she does not provide the appropriate information to the ATCO.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations. (REQ-PJ13.115-SPRINTEROP-0240).
RP_wrg_proc [RP]	The RP applies wrong C2LL procedures.	RP applies incorrectly the C2LL procedures for information communication and, therefore, he/she does not provide the appropriate information to the ATCO.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations. (REQ-PJ13.115-SPRINTEROP-0240)
RP_nc_ins [RP]	RP does not follow ATC instructions	RP does not correctly manage the instructions received by the ATCO, by not following these instructions correctly. Therefore, he/she does not provide the appropriate C2LL information to the ATCO.	**A 006 A):** It is considered that RPs are already trained with regard to the IFR procedures and way of operating. Therefore, actions such as assessing ATCOs instructions and providing read back of them are within RPs current skills.
RP_wrg_ins [RP]	RP follows wrong ATC instructions	RP does not correctly manage the instructions received by the ATCO, by following wrong instructions (misinterpreting them or following the ones provided to another aircraft). Therefore, he/she does not provide the appropriate C2LL information to the ATCO	**A 006 A):** It is considered that RPs are already trained with regard to the IFR procedures and way of operating. Therefore, actions such as assessing ATCOs instructions and providing read back of them are within RPs current skills.
RP_lap_saw [RP]	RP lapse or loss of situational awareness	RP suffers a lapse or a loss of their situational awareness and, therefore, does not correctly manage the instructions received, and does not provide the appropriate C2LL information to the ATCO	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations. (REQ-PJ13.115-SPRINTEROP-0240)
RP_nsha_info [RP]	Changed information not shared by RP (too late)	RP does not correctly manage the instructions received by the ATCO, by sharing the changed information related to the C2LL too late with the ATCO.	**A 006 B):** It is considered that RPs are trained and aware of the C2LL contingency procedures and they have already conducted diversion preparation in case of change.
RP_lack_av [RP]	RP is not available	The RP managing the RPA is not available and, therefore, he/she does not provide the appropriate C2LL information to the ATCO.	**SRD 022:** A team of pilots shall be always available to manage the RPA, and at all times during flight there will be one pilot designated Pilot in Command in the RP position (REQ-PJ13.115-SPRINTEROP-0350).

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
COMM_fail [Conf RPAS]	Radio failure on RPA only	There is a failure in the RPA communication systems and, therefore, he/she provides incomplete, late or no C2LL information to the ATCO.	**SRD 023:** RP shall be able to execute the standard IFR contingency procedures and operating methods identically to manned aviation: • Voice Comm loss with No C2 link loss; • GNSS/positioning loss; • Transponder failure/loss (REQ-PJ13.115-SPRINTEROP-0130)
ATC_lack_tr [ATCO]	ATCO lack of training	ATCO lack of training on C2LL contingency procedures prevent them from detecting the lack of information regarding a possible C2LL contingency.	**SRD 015:** ATCO shall be trained and shall be able to apply new procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)
ATC_lap_saw [ATCO]	ATCO lapse or loss of situational awareness	ATCO suffers a lapse or a loss of their situational awareness and, therefore, does not detect the lack of information regarding a possible C2LL contingency.	**A 005:** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore, the current training of the ATCOs in IFR procedures/ operating methods prepares them to manage radio communications in order to assume the control of the different flights and provide them with instructions.
RP_wrg_info [RP]	Wrong information entered by the RP in the RPA systems.	RP enters wrong information regarding a possible C2LL contingency in the RPA systems.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations. (REQ-PJ13.115-SPRINTEROP-0240)
RP_no_info [RP]	No information entered by the RP in the RPA systems.	RP enters no information regarding a possible C2LL contingency in the RPA systems.	**SRD 001:** RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations. (REQ-PJ13.115-SPRINTEROP-0240)

Table 23. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH1

EUROPEAN PARTNERSHIP

Co-funded by the European Union



OH2. Inconsistency between the programmed C2LL contingency procedure and the ATCO expectations of the RPAS trajectory.
SRS 039 OH02 = 3,3 e-5 per FH.
HZ 01 a) and b)
HZ 04
Undetected incorrect preparation of a possible C2LL contingency
Malfunction of the RPAS system
ATC lack of familiarization with C2LL contingency procedures
Inadequate coordination between RP and ATCO (when a change in the C2LL contingency procedure is introduced just before the declaration of the C2LL contingency)
RP does not detect incorrect preparation
ATCO does not detect lack of C2LL contingency information
ATC_undet_info
RPA system technical failure
RP failure: incorrect input of C2LL contingency information
RP_wrg_input
ATCO fails to manage/ interpret C2LL contingency information
ATC_wrg_inf_mng
ATCO fails to anticipate RPA's C2LL contingency trajectory
ATC_wrg_antic
No contact between RP and ATCO through the alternative communication means
RP/ATC_lack_com
No update of information through alternative communication means
RP/ATC_wrg_com
Failure to provide C2LL contingency information to ATCO
RP_wrg_prov
Failure to input C2LL contingency information in RPA system
RP_wrg_input
The system does not initiate the C2LL contingency procedure
RPAS_no_proc
The system initiates a wrong C2LL contingency procedure
RPAS_wrg_proc

Figure 5. Fault Tree associated to OH2

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
ATC_wrg_inf_mng [ATCO]	ATCO fails to manage/interpret C2LL contingency information	ATCO's lack of familiarization with C2LL contingency procedures consisting of a failure to manage/interpret C2LL contingency information.	**SRD 015:** ATCO shall be trained and shall be able to apply new procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)
ATC_wrg_antic [ATCO]	ATCO fails to anticipate RPA's C2LL contingency trajectory	ATCO's lack of familiarization with C2LL contingency procedures consisting of a failure to anticipate RPA's C2LL contingency trajectory.	**SRD 002:** RP shall provide C2 link loss pre-programmed contingency information for ATCO pre-awareness (REQ-PJ13.115-SPRINTEROP-0110).
			SRD 003A: ATCO shall be able to easily recognise the RPAS traffic. (REQ-PJ13.115-SPRINTEROP-0070)
RP/ATC_lack_com [ATCO ←→ RP]]	No contact between RP and ATCO through the alternative communication means	Inadequate coordination between RP and ATCO *(when a change in the C2LL contingency procedure is introduced just before the declaration of the C2LL contingency)* consisting of no contact between RP and ATCO through the alternative communication means.	**SRD 013:** The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260)
RP/ATC_wrg_com [ATCO ←→ RP]	No update of information through alternative communication means	Inadequate coordination between RP and ATCO *(when a change in the C2LL contingency procedure is introduced just before the declaration of the C2LL contingency)* consisting of no update of information through alternative communication means.	**SRD 024:** RP shall be trained and shall be able to apply new procedures including specific RPAS preparation procedures and operating methods for RPAS non-nominal situations. RP will, if necessary, re-program diversion preparation in case of changes in nominal flight (i.e. prior to C2LL) (REQ-PJ13.115-SPRINTEROP-0270)

Table 24. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH2

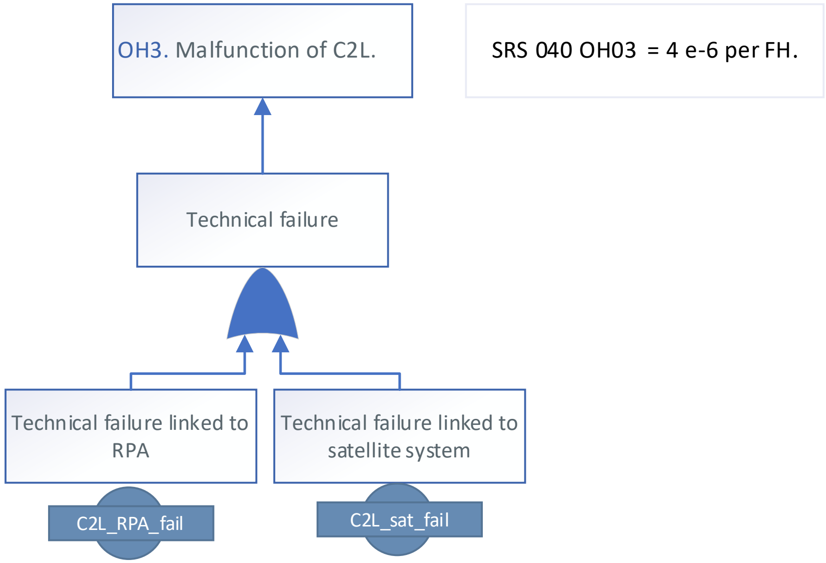

OH3. Malfunction of C2L.
SRS 040 OH03 = 4 e-6 per FH.
Technical failure
Technical failure linked to RPA
Technical failure linked to satellite system
C2L_RPA_fail
C2L_sat_fail

Figure 6. Fault Tree associated to OH3

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
C2L_RPA_fail [RPAS]	Technical failure link to RPA	Malfunction of the C2L due to a technical failure in the RPA.	**A 001:** During the accommodation phase, the C2L used by existing/MIL RPAS meets the existing robustness specifications.
C2L_sat_fail [External]	Technical failure link to satellite system	Malfunction of the C2L due to a technical failure in the satellite system.	**A 001:** During the accommodation phase, the C2L used by existing/MIL RPAS meets the existing robustness specifications.

Table 25. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH3

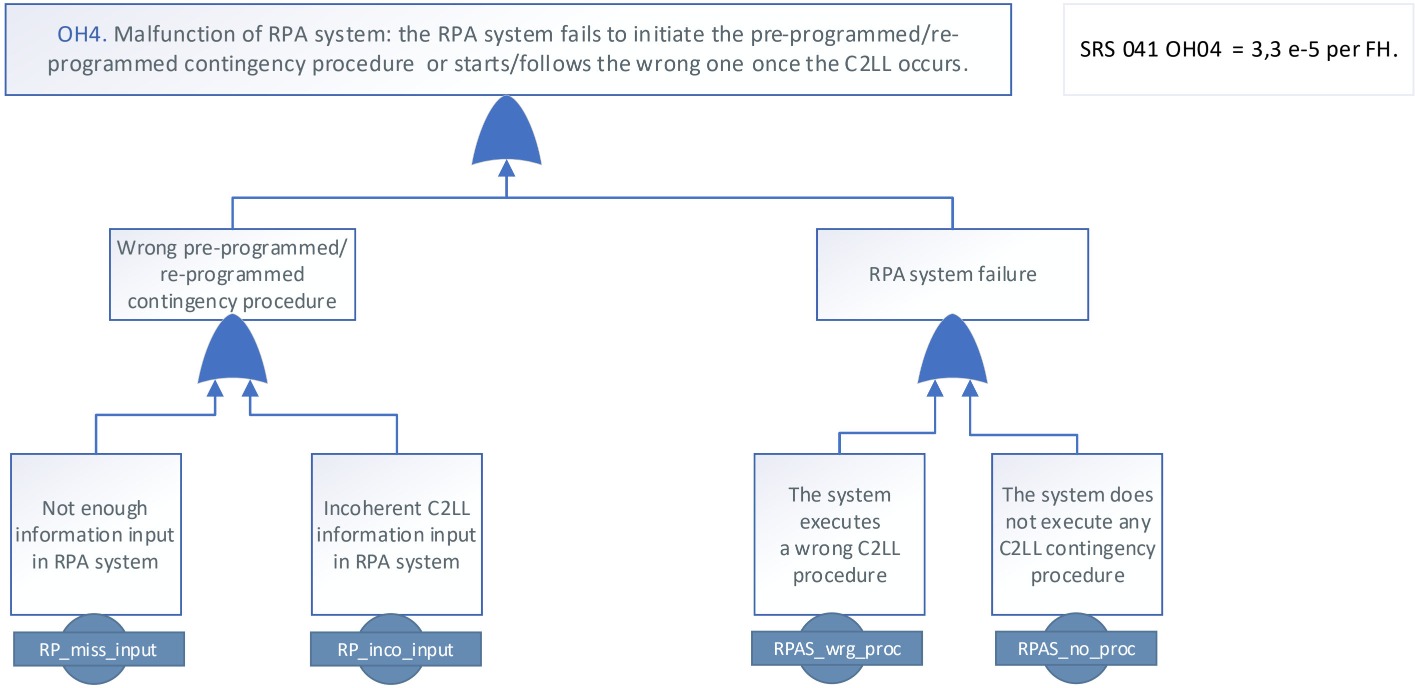

OH4. Malfunction of RPA system: the RPA system fails to initiate the pre-programmed/re-programmed contingency procedure or starts/follows the wrong one once the C2LL occurs.
SRS 041 OH04 = 3,3 e-5 per FH.
Wrong pre-programmed/ re-programmed contingency procedure
RPA system failure
Not enough information input in RPA system
RP_miss_input
Incoherent C2LL information input in RPA system
RP_inco_input
The system executes a wrong C2LL procedure
RPAS_wrg_proc
The system does not execute any C2LL contingency procedure
RPAS_no_proc

Figure 7. Fault Tree associated to OH4

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
RP_miss_input [RP]	Not enough information input in RPA system	The RP does not input enough C2LL information in the RPA system and, therefore, the pre-programmed/ re-programmed C2LL contingency procedure is wrong/incomplete.	**A 009:** Aside from internal system malfunctions, RPA systems follow the pre-programmed/ re-programmed procedures introduced by RPS Operations
			SRD 009: RP shall always pre-program RPA with a C2LL trajectory that shall be automatically triggered and flown when the RPAS goes into a C2LL state. (REQ-PJ13.115-SPRINTEROP-0310) *NOTE: The RP shall re-program this C2LL trajectory whenever it is required*

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
			SRD 001: RP shall be trained, and shall be able to apply new operating methods including the communication to ATCO of the two additional elements related to C2LL contingency procedure, and specific RPAS preparation procedures for RPAS nominal situations. (REQ-PJ13.115-SPRINTEROP-0240)
RP_inco_input [RP]	Incoherent C2LL information input in RPA system	Incoherent input of C2LL information in the RPA system leads to a wrong pre-programmed/ re-programmed C2LL contingency procedure.	**A 009:** The current capabilities of the RPA navigation system prevent the RP from introducing incoherent information.
RPAS_wrg_proc [RPAS]	The system executes a wrong C2LL procedure	A failure occurs in the RPA system that consists of the execution of a wrong C2LL contingency procedure.	**SRD 025:** RPAS shall be able to navigate during flight in a structured airspace with performances and capabilities associated with the airspace, including the C2LL trajectory: • Positioning aids (GNSS, inertial); • AIRAC cyclic navigation data (ATS routes, waypoints); • RNAV required in the class A-C airspace environment (RNAV5 En-Route / RNAV1 Terminal). (REQ-PJ13.115-SPRINTEROP-0090) *The aim is to ensure the capability of the system in nominal conditions and while applying C2LL procedures.*
RPAS_no_proc [RPAS]	The system does not execute any C2LL contingency procedure	A failure occurs in the RPA system that consists of not executing the C2LL contingency procedure.	**A 009:** The RPA system is always programmed with a C2LL trajectory that shall be automatically triggered and flown when the RPA goes into a C2LL state.

Table 26. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH4

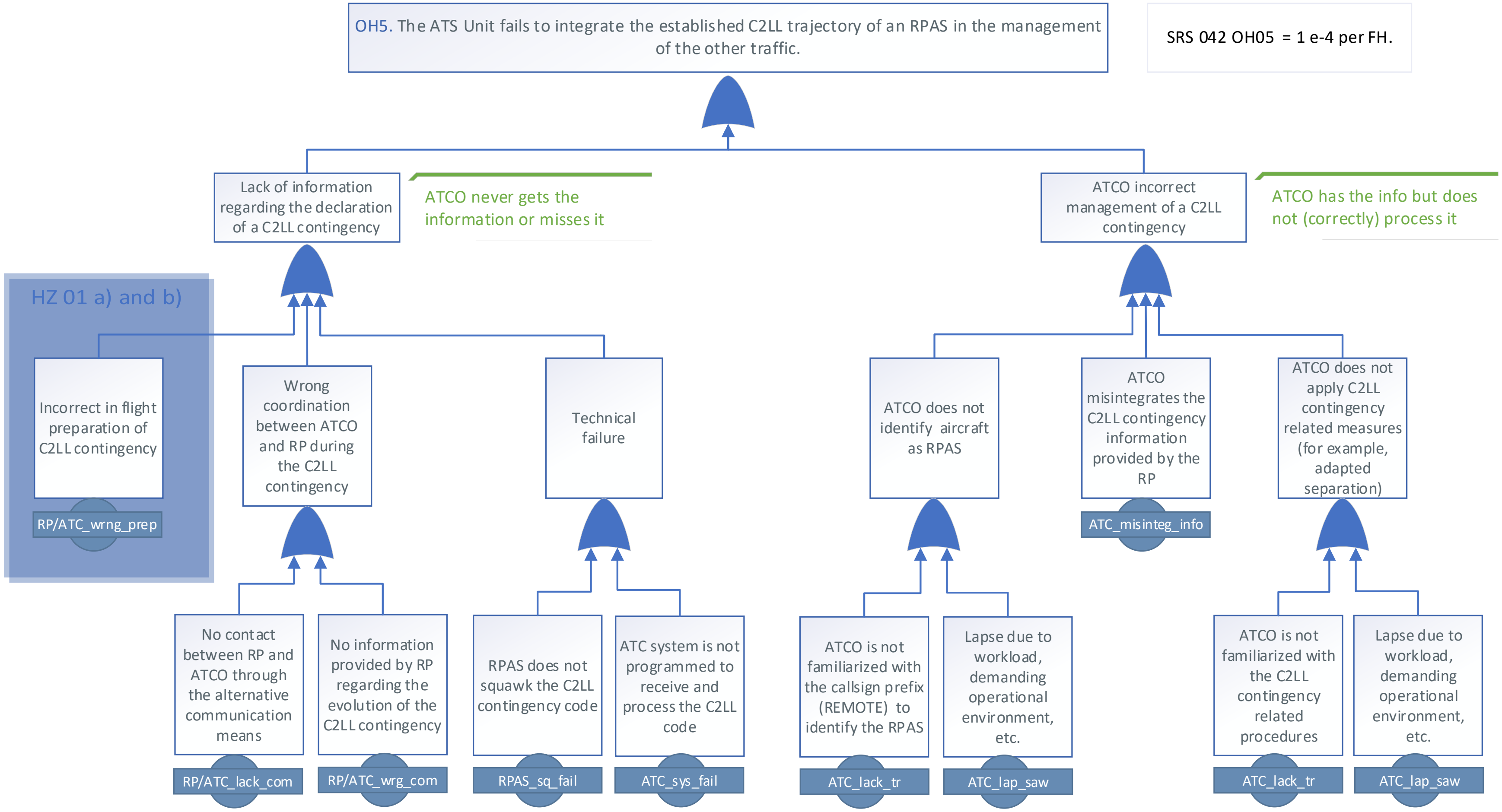

OH5. The ATS Unit fails to integrate the established C2LL trajectory of an RPAS in the management of the other traffic.
SRS 042 OH05 = 1 e-4 per FH.
Lack of information regarding the declaration of a C2LL contingency
ATCO never gets the information or misses it
ATCO incorrect management of a C2LL contingency
ATCO has the info but does not (correctly) process it
HZ 01 a) and b)
Incorrect in flight preparation of C2LL contingency
RP/ATC_wrng_prep
Wrong coordination between ATCO and RP during the C2LL contingency
Technical failure
ATCO does not identify aircraft as RPAS
ATCO misintegrates the C2LL contingency information provided by the RP
ATC_misinteg_info
ATCO does not apply C2LL contingency related measures (for example, adapted separation)
No contact between RP and ATCO through the alternative communication means
RP/ATC_lack_com
No information provided by RP regarding the evolution of the C2LL contingency
RP/ATC_wrg_com
RPAS does not squawk the C2LL contingency code
RPAS_sq_fail
ATC system is not programmed to receive and process the C2LL code
ATC_sys_fail
ATCO is not familiarized with the callsign prefix (REMOTE) to identify the RPAS
ATC_lack_tr
Lapse due to workload, demanding operational environment, etc.
ATC_lap_saw
ATCO is not familiarized with the C2LL contingency related procedures
ATC_lack_tr
Lapse due to workload, demanding operational environment, etc.
ATC_lap_saw

Figure 8. Fault Tree associated to OH5

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
RP/ATC_lack_com [ATCO ←→ RP]]	No contact between RP and ATCO through the alternative communication means	Inadequate coordination between RP and ATCO *(when the C2LL contingency is initially declared)* consisting of no contact between RP and ATCO through the alternative communication means.	**SRD 24:** RP shall be trained and shall be able to apply new procedures including specific RPAS preparation procedures and operating methods for RPAS non-nominal situations. RP will, if necessary, re-program diversion preparation in case of changes in nominal flight (i.e. prior to C2LL) (REQ-PJ13.115-SPRINTEROP-0270)
			SRD 013: The first one of ATCO/RP who observes the C2 link loss shall be able to contact the other using the backup telephone line (REQ-PJ13.115-SPRINTEROP-0260)
			SRD 015: ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)
RP/ATC_wrg_com [ATCO ←→ RP]	No information provided by RP regarding the evolution of the C2LL contingency	Inadequate coordination between RP and ATCO *(when the C2LL contingency is initially declared)* consisting of no update of information through alternative communication means.	**SRD 024:** RP shall be trained and shall be able to apply new procedures including specific RPAS preparation procedures and operating methods for RPAS non-nominal situations. RP will, if necessary, re-program diversion preparation in case of changes in nominal flight (i.e. prior to C2LL) (REQ-PJ13.115-SPRINTEROP-0270)
RPAS_squawk_fail [RPAS]	RPAS does not squawk the C2LL contingency code	The RPAS does not squawk the C2LL contingency code and, therefore, the ATCO does not have information about the declaration of a C2LL contingency.	**SRD 012:** RPA shall be able to automatically provide specific C2 link loss transponder code and to maintain it active during C2 link loss (REQ-PJ13.115-SPRINTEROP-0140)
ATC_sys_fail [Conf ATSU]	ATC system is not programmed to receive and process the C2LL code	Technical failure consisting on the ATC system not being programmed to receive and process the C2LL code. Therefore, the ATCO cannot correctly manage the C2LL contingency.	**SRD 006:** ATCO shall be able to perform surveillance of RPA with the current secondary surveillance tools and technologies which are compatible with airborne Mode A/C transponders (i.e. primarily secondary surveillance radar (SSR)) (REQ-PJ13.115-SPRINTEROP-0300) *NOTE: This includes that the ATC system shall process and highlight specific C2 link loss transponder code on CWP*
ATC_lack_tr [ATCO]	ATCO is not familiarized with the callsign prefix (REMOTE) to identify the RPAS.	The ATCO is not familiarized with the callsign prefix (REMOTE) to identify the RPAS, which prevents him/her from identifying the aircraft as an RPAS. Therefore, the ATCO cannot correctly manage the C2LL contingency.	**A005:** From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groupings of sectors concerned. Therefore, the current training of the ATCOs prepares them to manage radio communications in order to assume the control of the different flights and provide them with instructions.
			SRD 003A: ATCO shall be able to easily recognise the RPAS traffic (REQ-PJ13.115-SPRINTEROP-0070)

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
			SRD 003B: The RP shall add "REMOTE" to the callsign (REQ-PJ13.115-SPRINTEROP-0340)
ATC_lap_saw [ATCO]	Lapse due to workload, demanding operational environment, etc.	ATCO suffers a lapse or a loss of their situational awareness, which prevents him/her from applying C2LL contingency related measures.	**A 001:** During the accommodation phase RPAS will operate in environments with medium/low density of traffic.
			A 011: Regarding C2LL contingency situations it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload, • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation.
ATC_misinteg_info [ATCO]	ATCO misintegrates the C2LL contingency information provided by the RP	ATCO does not properly integrate the C2LL contingency information provided by the RP in the management of the situation.	**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)
ATC_lack_tr [ATCO]	ATCO is not familiarized with the C2LL contingency related procedures	The ATCO is not familiarized with C2LL contingency related procedures, which prevents him/her from applying C2LL contingency related measures.	**SRD 015:** ATCO shall be trained and shall be able to apply adapted procedures/ operating methods for RPAS non-nominal situations (REQ-PJ13.115-SPRINTEROP-0250)
ATC_lap_saw [ATCO]	Lapse due to workload, demanding operational environment, etc.	ATCO suffers a lapse or a loss of their situational awareness, which prevents him/her from applying C2LL contingency related measures.	**A 001:** During the accommodation phase RPAS will operate in environments with medium/low density of traffic.
			A 011: Regarding C2LL contingency situations it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload, • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation.

Table 27. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH5

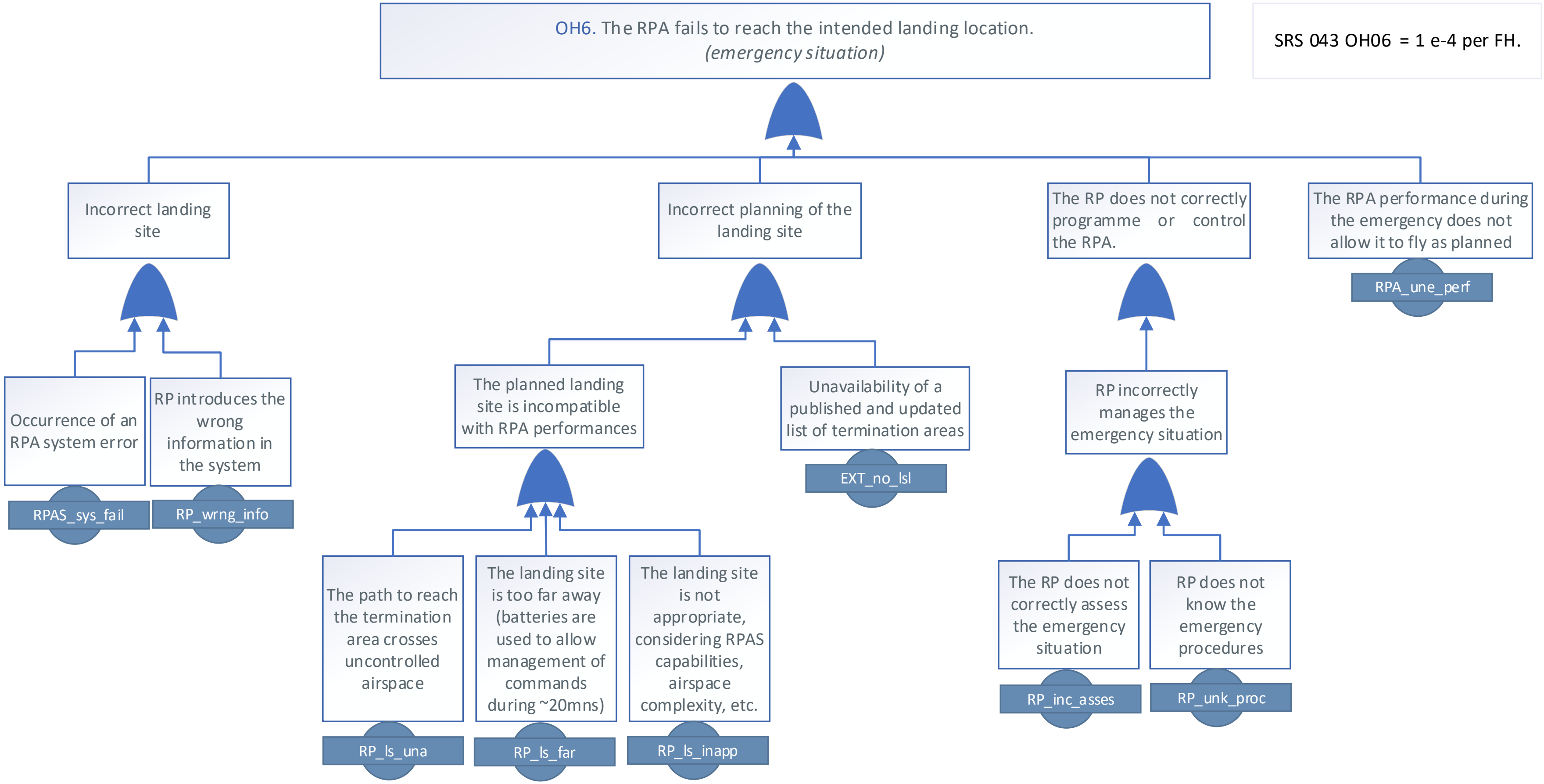

OH6. The RPA fails to reach the intended landing location.
(emergency situation)
SRS 043 OH06 = 1 e-4 per FH.
Incorrect landing site
Incorrect planning of the landing site
The RP does not correctly programme or control the RPA.
The RPA performance during the emergency does not allow it to fly as planned
RPA_une_perf
Occurrence of an RPA system error
RPAS_sys_fail
RP introduces the wrong information in the system
RP_wrng_info
The planned landing site is incompatible with RPA performances
Unavailability of a published and updated list of termination areas
EXT_no_lsl
RP incorrectly manages the emergency situation
The path to reach the termination area crosses uncontrolled airspace
RP_ls_una
The landing site is too far away (batteries are used to allow management of commands during ~20mns)
RP_ls_far
The landing site is not appropriate, considering RPAS capabilities, airspace complexity, etc.
RP_ls_inapp
The RP does not correctly assess the emergency situation
RP_inc_asses
RP does not know the emergency procedures
RP_unk_proc

Figure 9. Fault Tree associated to OH6

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
RPAS_sys_fail [Conf RPAS]	Occurrence of an RPA system error	The intended landing site is incorrect due to an error occurred in the RPA system.	**SRD 020:** RPAS shall be able to identify its emergency status and to execute the emergency procedure associated with the severe failure situation with RP in the loop (REQ-PJ13.115-SPRINTEROP-0160)
RP_wrng_info [RP]	RP introduces the wrong information in the system	The intended landing site is incorrect due to the introduction of the wrong information in the system by the RP.	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.
RP_inc_path [RP]	The path to reach the termination area crosses uncontrolled airspace	The programmed landing site is incompatible with RPAS performances, since the path to reach the termination area crosses uncontrolled airspace.	**A 010:** Regarding emergencies related to RPAS flights (for example, engine failure), it is considered that the planning of emergencies takes into account the capabilities of the RPA, the conditions of the landing site, etc. This is done in an equivalent way to manned aircraft planning.
RP_ls_far [RP]	The landing site is too far away (batteries are used to allow management of commands during ~20mns)	The programmed landing site is incompatible with RPAS performances, since it is too far away considering the batteries duration	**A 010:** Regarding emergencies related to RPAS flights (for example, engine failure), it is considered that the planning of emergencies takes into account the capabilities of the RPA, the conditions of the landing site, etc. This is done in an equivalent way to manned aircraft planning.
RP_ls_inapp [RP]	The landing site is not appropriate (considering RPAS capabilities, airspace complexity, etc.)	The programmed landing site is incompatible with RPAS performances, since it is not appropriate considering RPAS capabilities, airspace complexity, etc.).	**A 010:** Regarding emergencies related to RPAS flights (for example, engine failure), it is considered that the planning of emergencies takes into account the capabilities of the RPA, the conditions of the landing site, etc. This is done in an equivalent way to manned aircraft planning.
EXT_no_lsl [EXT]	Unavailability of a published and updated list of termination areas	The landing site is incorrectly programmed, since an updated list of termination areas is not available.	**A 010:** Regarding emergencies related to RPAS flights (for example, engine failure), it is considered that the planning of emergencies takes into account the capabilities of the RPA, the conditions of the landing site, etc. This is done in an equivalent way to manned aircraft planning.
RP_inc_assess [RP]	The RP does not correctly assess the emergency situation	The RP does not correctly assess the emergency situation which leads to his/her incorrect management of the emergency situation. Therefore, the RP does not programme or control the RPA.	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
RP_unk_proc [RP]	RP does not know the emergency procedures	The RP does not know the emergency procedures which leads to his/her incorrect management of the emergency situation. Therefore, the RP does not programme or control the RPA.	**A 006 B):** It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)* is within RP's current skills.
RPAS_une_per [RPAS]	The RPA performance during the emergency does not allow it to fly as planned	The RPA performance during the emergency does not allow it to fly as planned due to multiple simultaneous failures, to the necessity to modify emergency trajectory during its execution (due to weather hazard, ATC request, etc.), or other reasons.	**A 010:** Regarding emergencies related to RPAS flights (for example, engine failure), it is considered that the planning of emergencies takes into account performance degradation. This is done in an equivalent way to manned aircraft planning.

Table 28. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH6

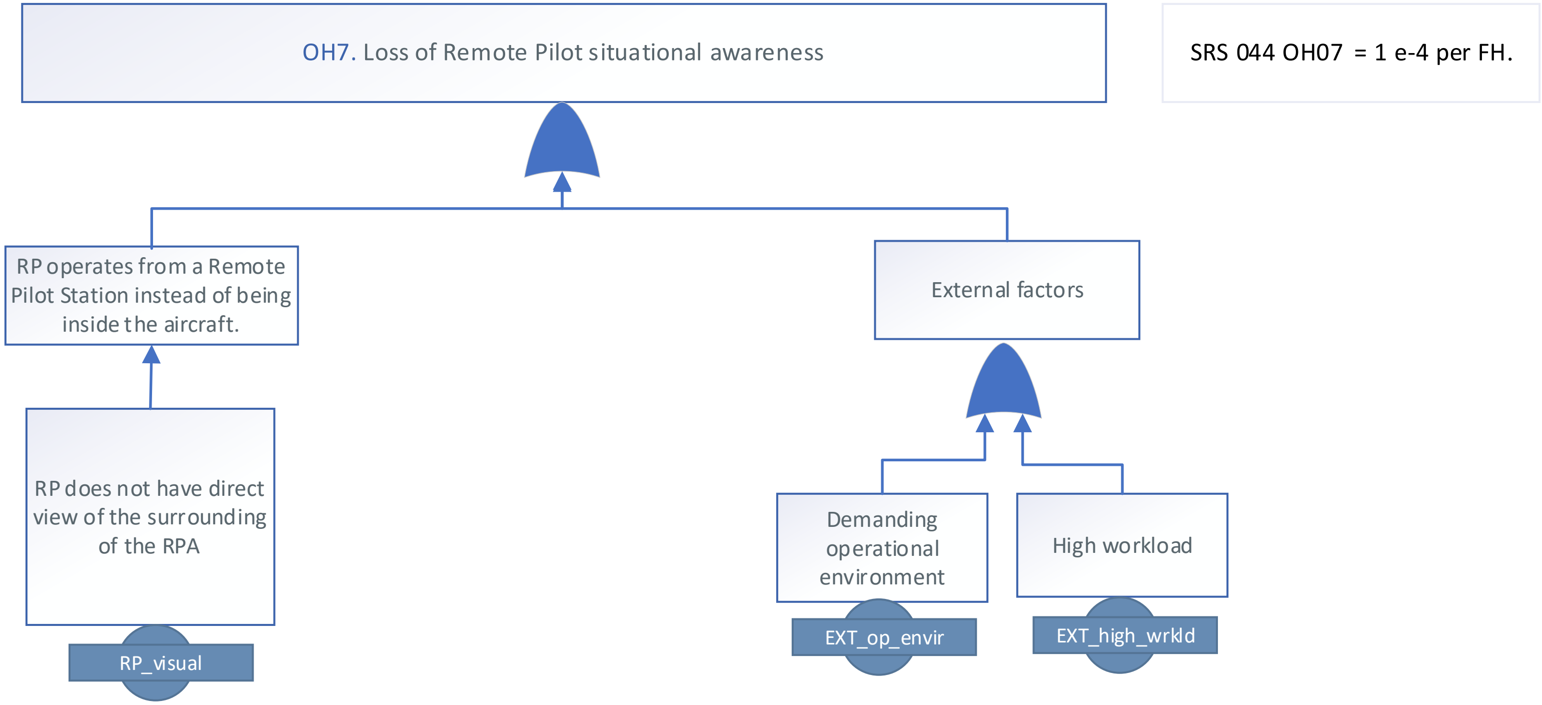

OH7. Loss of Remote Pilot situational awareness
SRS 044 OH07 = 1 e-4 per FH.
RP operates from a Remote Pilot Station instead of being inside the aircraft.
External factors
RP does not have direct view of the surrounding of the RPA
RP_visual
Demanding operational environment
EXT_op_envir
High workload
EXT_high_wrkld

Figure 10. Fault Tree associated to OH7

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
RP_visual [RP]	RP does not have direct view of the surrounding of the RPA.	RP does not have direct view of the surrounding of the RPA, since it operates from a Remote Pilot Station instead of being inside the aircraft.	**A 007:** RP have traffic awareness in their RPS through radio communications on shared frequency and they are able to identify certain threatens like the wake risk and request additional instructions to ATCO, if necessary. Since RPs are in the ground, they could also benefit from additional situational awareness systems that show traffic, for instance. Moreover, the RP is operating in IFR operational environment, so their situational awareness should be linked to the controls they need in this environment.

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
EXT_op_envir [EXT]	Demanding operational environment	There is a demanding operational environment due to external factors.	**A 001:** During the accommodation phase RPAS will operate in environments with medium/low density of traffic.
EXT_high_wrkld [EXT]	High workload	There are high workload conditions due to external factors.	**A 001:** During the accommodation phase RPAS will operate in environments with medium/low density of traffic.

Table 29. Fault tree causes and associated mitigations (SRD, preventing operational hazard occurrence) of OH6

G.1.2 Bottom-up failure modes and effects analysis

A bottom-up analysis of the failure modes of the Solution functional system elements / element-to-element interfaces and of their effects is provided, for selected parts of the Solution functional system. This is used in order to determine potential common cause failures but also in order to allow a more in depth causal analysis of certain parts of the functional system design, in view of complementing the Fault Tree findings. The technique used is FMEA (Failure mode and effects analysis), and its results are provided in Table 30.

Functional system element	Failure mode	Effects	Mitigation/Safety Requirement	Operational hazard
ATCO	Incorrect preparation of C2LL contingency	Lack of (correct) C2LL contingency information.	RP/ATCO coordination through normal communication channels.	OH 01. Incorrect preparation of C2LL contingency.
	Incorrect management of C2LL contingency	Possible conflict between RPAS executing C2LL contingency procedure and other aircraft in the vicinity.	ATCO surveillance of traffic. ATCO/RP coordination through alternative communication means	OH 05. The ATS Unit fails to integrate the established procedure for the loss of C2LL of an RPAS in the management of the other traffic
RP	Incorrect preparation of C2LL contingency	Lack of (correct) C2LL contingency information.	RP/ATCO coordination through normal communication channels.	OH 01. Incorrect preparation of C2LL contingency.
	Incorrect management of C2LL contingency	Possible conflict between RPAS executing C2LL contingency procedure and other aircraft in the vicinity.	RP monitoring of RPA. ATCO surveillance of traffic. ATCO/RP coordination through alternative communication means	OH 02. Inconsistency between the programmed C2LL contingency procedure and the ATCO expectations of the RPAS trajectory
	Incorrect management of an emergency	Landing with risk to ground assets.	RP training.	OH 06. The RPA fails to reach the programmed landing location.
	Loss of situational awareness (RP not inside RPA, but in RPS)	Increase of workload of RP to manage the RPA. Increase of workload of ATCO to manage traffic. RP incorrectly complies with the instructions received from the ATS Unit. Unknown/unexpected RPA flight trajectory.	RP training ATCO surveillance of traffic. ATCO/RP coordination through alternative communication means	OH 07. Loss of Remote Pilot situational awareness.
C2L system	Technical failure of C2L	The C2LL contingency procedure needs to be applied by the RPA systems. Meanwhile, the ATCO has to integrate this procedure in the management of traffic and coordinate with the RP whatever necessary through the alternative communication means.	Availability of re-programmed or re-programmed C2LL contingency procedure. ATCO surveillance of traffic. ATCO/RP coordination through alternative communication means	OH 03. Malfunction of C2L

Functional system element	Failure mode	Effects	Mitigation/Safety Requirement	Operational hazard
	Malfunction of RPA system	No initiation of C2LL contingency procedure or execution of the wrong one.	RP monitoring of RPA. ATCO surveillance of traffic. ATCO/RP coordination through alternative communication means	OH 04. Malfunction of RPA system: the RPA system fails to initiate the pre-programmed/ re-programmed contingency procedure or starts/follows the wrong one once the C2LL contingency is declared.

Table 30. Failure Modes and Effects Analysis table

G.2 Deriving SRD from the SRS (functionality & performance) for protective mitigation

The purpose of this section is to derive SRD (functionality & performance) from the SRS (functionality & performance) that have been derived in section 4.4.2 to provide mitigation against operational hazard effects (protective mitigation), with due consideration of the potential common cause failures that might affect the operational hazard causes and its protective mitigation.

Therefore, Table 31 shows how the Safety Requirements at ATS Service level (SRS) functionality & performance derived in section 4.4.2 for protective mitigation map onto the related elements of the Design Model (functional system components or interactions/data flows) and derive additional Safety Requirements at Design level (SRD) (functionality & performance) for internal failure conditions of operation. It includes the following information:

- the SRS (functionality & performance) derived in section 4.4.2 to provide mitigation against operational hazard effects (protective mitigation),
- the derived SRD driven by the mapping of the SRS onto the related elements of the Design Model, together with any necessary assumptions,
- the Design Model elements (functional system components or interactions/data flows or external elements impacted by the Change) relevant for the derived SRD and/or assumptions.

SRS (functionality & performance) for protective mitigation (ID & content)	Safety Requirement at Design level[14] (SRD) or Assumption	Maps onto
SRS 033: There will always be an additional/backup pilot in the Remote Pilot Station to cross-check.	**SRD 022:** A team of pilots shall be always available to manage the RPA, and at all times during flight there will be one pilot designated Pilot in Command in the RP position (REQ-PJ13.115-SPRINTEROP-0350).	[RPS]

[14] iSRD for the initial design or rSRD for the refined design

SRS (functionality & performance) for protective mitigation (ID & content)	Safety Requirement at Design level[14] (SRD) or Assumption	Maps onto
SRS 034: RPAS FL shall be limited such as to reduce chances to have VFR traffic below. The solution operating environment for transit flights is above FL100 (thus an extremely low probability of the majority of leisure VFR intruders)	**SRD 026:** RPS Operations shall be able to plan flight within flight levels where a minimum traffic risk is usually present (REQ-PJ13.115-SPRINTEROP-0040) *NOTE: The span of flight levels considered will usually be above low levels to minimise recreational VFR traffic risk (> FL100), and below high levels to minimise flying within high speed cruising jet aircraft (~ FL200). Nevertheless, these vertical limits could be adapted depending on the specific characteristics of each operational environment*	[Conf RPA]
SRS 035: During C2LL state, RPAS speed shall be limited such as to produce a temporal separation of the RPA sufficiently high to allow ATCOs to update the RPA clearance or reorganize and clear the traffic around them, if needed. In the solution operating environment, the RPA speed is below 200kts	**SRD 027**: RPAS shall fly low speeds (below 200 knots) in order to allow ATCO sufficient time to update the RPA clearance or re-organize the traffic around RPAS after C2LL occurrence (REQ-PJ13.115-SPRINTEROP-0410).	[Conf RPA]
SRS 036: The pre-programmed trajectory equipment performance and integrity standards shall meet at least the navigation requirements in the targeted class of airspace	**SRD 025:** RPAS shall be able to navigate during flight in a structured airspace with performances and capabilities associated with the airspace, including the C2LL trajectory: • Positioning aids (GNSS, inertial); • AIRAC cyclic navigation data (ATS routes, waypoints); • RNAV required in the class A-C airspace environment (RNAV5 En-Route / RNAV1 Terminal); (REQ-PJ13.115-SPRINTEROP-0090)) *The aim is to ensure the capability of the system in nominal conditions and while applying C2LL procedures.*	[Conf RPA]

Table 31: SRD derived by mapping SRS (functionality & performance) for protective mitigation on to Design Model Elements

Appendix H Demonstration of Safety Criteria achievability

This section shows the extent to which the achievability of the Safety Criteria has been demonstrated through the satisfaction of the success criteria of the safety validation objectives defined in relation to the Solution RTS.

The demonstration holds to the extent where this exercise addresses all the SRS (functionality & performance), and more specifically, all the derived SRD (functionality & performance) (the SAC achievability accounting for internal functional system failures, i.e. considering the integrity/reliability safety requirements can be demonstrated only by predictive safety assessment – see sections 4.4 and 5.5).

The safety-related outcomes of the RTS brings therefore an essential contribution to the demonstration of the Safety Criteria achievability by the Solution design.

The safety-relevant results of the validation are summarized in the following table, in which the extent to which the relevant SRDs have been covered is indicated.

Exercise ID, Name, Goals	Exercise Safety Validation Objective & related SAC(s)	Success criterion	Coverage (SRS and/or SRD)	Validation results
EXE-115-001 Real Time Simulation in Clermont-Ferrand airport (LFLC). RPAS flight will be accommodated with cooperative and/or known traffic within LFLC TMA (class D). Nevertheless, to match the simulations with the scope of the project, all traffics will be separated except VFR with VFR. They will be provided with traffic information. Objectives are: • To assess impact of adapted separation between one RPAS and manned aircraft. • To assess impact of dedicated RPAS C2 link loss procedure within a mid-density, mid-complexity TMA environment for transiting RPAS.	**OBJ-115-V3-VALP-002** Operational acceptability of RPAS non-segregated transit as GAT among all other GAT [SAC#2 & SAC#4]	**CRT-PJ13.115-V3-VALP-002-0001** Nominal procedures & working methods acceptable for controllers and compatible with controller's procedures and working methods. Identical support tools to manned aviation used. Clear evidence of feasibility for any certified IFR RPA to fly in any controlled airspace of classes A, B, C with a limited added complexity of ATCO procedures (under limitations of number of RPA in a given sector).	**SRD 001**: fully covered **SRD 002:** fully covered **SRD 003A & B:** fully covered **SRD 004:** fully covered **SRD 005:** fully covered **SRD 006:** fully covered **SRD 007:** fully covered **SRD 008:** fully covered **SRD 010:** fully covered	ATCO is able to perform as they used to do for manned aircraft. ATCOs find a need to communicate that the aircraft is an RPAS at first radio contact. ATCOs succeeded in managing RPAS in the traffic safely and efficiently.
	OBJ-115-V3-VALP-003 Validation is on the confirmation that identical procedures to manned aviation could be used with	**CRT-PJ13.115-V3-VALP-003-0002** Safety of operations maintained.	**SRD 023**: fully covered	ATCOs confirmed that non-RPAS specific contingency management must be identical to the way those are managed for other manned aircraft operations.
		CRT-PJ13.115-V3-VALP-003-0004 Clear evidence of feasibility for any certified IFR RPA to fly in any	**SRD 026**: fully covered	

Exercise ID, Name, Goals	Exercise Safety Validation Objective & related SAC(s)	Success criterion	Coverage (SRS and/or SRD)	Validation results
	RPAS for abnormal situations not specific to RPAS [SAC#1, SAC#2 & SAC#4]	controlled airspace of classes A, B, C with reuse of existing procedures (under limitations of number of RPA in a given sector).		
	OBJ-115-V3-VALP-004 Validation is on the C2LL Contingency procedure information exchange procedure & C2LL procedure management • C2LL information, procedure & working methods acceptable for controllers [SAC#1, SAC#2 & SAC#4] • Support tools are still usable by controllers	**CRT-PJ13.115-V3-VALP-004-0001** Safe contingency procedures and (tools-direct phone line) to be applied by RPS, ATC, defined and validated, including key waypoints characterising contingency trajectories.	**SRD 001**: fully covered **SRD 002**: fully covered **SRD 006**: fully covered **SRD 007**: fully covered **SRD 009**: fully covered **SRD 011**: fully covered **SRD 012**: fully covered **SRD 013**: fully covered **SRD 014**: fully covered **SRD 015**: fully covered **SRD 016**: fully covered **SRD 017**: fully covered **SRD 025**: fully covered **SRD 026**: fully covered	No safety issues were measured or raised by ATCOs feedbacks while RPA was on its C2LL trajectory.
		CRT-PJ13.115-V3-VALP-004-0002 Safety of operations maintained during rerouting after exit point until OAT transfer of control.	**SRD 006**: fully covered **SRD 015**: fully covered **SRD 016**: fully covered **SRD 026**: fully covered	ATCOs simulated the transfer of the RPAS flight in C2LL state to other sector by providing the level and destination. No safety issue has been raised.
		CRT-PJ13.115-V3-VALP-004-0003 Contingency procedures, especially in case of loss of C2 link, defined and validated.	**SRD 001**: fully covered **SRD 002**: fully covered **SRD 014**: fully covered **SRD 015**: fully covered **SRD 017**: fully covered **SRD 024**: fully covered **SRD 025**: fully covered	ATCOs confirmed that they need to know the RPAS trajectory when C2 Link Loss occurs. Therefore, procedure shared at the first radio contact is useful and necessary as a first indication.
	OBJ-115-V3-VALP-005 ATC accommodation of RPAS detailed analysis. Management of urgency RPAS situations [SAC#1, SAC#2 & SAC#4]	**CRT-PJ13.115-V3-VALP-005-0001** Minimum negative impacts on legacy operations compared to the current emergency ones, reducing to the minimum possible the local procedures at	**SRD 018**: fully covered **SRD 019**: fully covered **SRD 020**: fully covered **SRD 021**: fully covered	RPAS transponder and engine failures have been assessed as having the same impact to manned aviation and ATCOs as if they were affecting manned aircraft.

Exercise ID, Name, Goals	Exercise Safety Validation Objective & related SAC(s)	Success criterion	Coverage (SRS and/or SRD)	Validation results
		Network Operation, ATC and Airport level		Part of the flight between the failure and the ditching area or the alternate aerodrome would be flown as if the aircraft were manned. A deviation from the programmed C2LL trajectory will be managed as an emergency, traffic will be cleared out of the area. In case of electric power failure, RPA is equipped with battery(ies) allowing a minimum flight capability (from several tens of minutes to hours) for reaching an aerodrome or ditching area.
		CRT-PJ13.115-V3-VALP-005-0002 Emergency procedure evaluated through expert judgement.	**SRD 018**: fully covered **SRD 019**: fully covered **SRD 020**: fully covered **SRD 021**: fully covered	
	OBJ-115-V3-VALP-006 ATC accommodation of RPAS detailed analysis. Human Performance	**CRT-PJ13.115-V3-VALP-006-0001** RTS + Observations + ATCO feedback	**SRD 001**: fully covered **SRD 003A & B**: fully covered **SRD 005**: fully covered **SRD 006**: fully covered **SRD 015**: fully covered **SRD 024**: fully covered	Roles and responsibilities for controllers remained the same. ATCOs were informed of the C2LL state. This issue was raised by ATCOs. The phraseology used for C2LL procedure sharing was deemed appropriate and short enough. ATCO requested higher level of knowledge of RPAS behaviour in particular in C2LL state.
	OBJ-115-V3-VALP-007 Safety objectives are based on the following items: • NMAC	**CRT-PJ13.115-V3-VALP-007-0001** Safe contingency procedures and (tools-direct phone line) to be applied by RPS, ATC, defined and validated, including key	**SRD 001**: fully covered **SRD 002**: fully covered **SRD 003A & B**: fully covered **SRD 004**: fully covered	ATCOs considered important that the RPAS trajectory behaviour pre-programmed on C2LL is provided by the remote pilot at the first radio contact and the possibility to

Exercise ID, Name, Goals	Exercise Safety Validation Objective & related SAC(s)	Success criterion	Coverage (SRS and/or SRD)	Validation results
	- Loss of separation - Number of instructions are counted - Duration (time to execute) [SAC#1, SAC#2, SAC#3 & SAC#4]	waypoints characterising contingency trajectories	**SRD 005**: fully covered **SRD 008**: fully covered **SRD 009**: fully covered **SRD 012**: fully covered **SRD 015**: fully covered **SRD 016**: fully covered **SRD 018**: fully covered **SRD 025**: fully covered **SRD 029**: fully covered	exchange with the remote pilot by the back-up phone line during the contingency.
		CRT-PJ13.115-V3-VALP-007-0002 Safety of operations maintained during rerouting after exit point until OAT transfer of control.	**SRD 006**: fully covered **SRD 015**: fully covered **SRD 016**: fully covered **SRD 026**: fully covered	No conflict has raised during the transfer of control action.
		CRT-PJ13.115-V3-VALP-007-0003 Safe procedures and trajectories of RPAs with respect to the other Airspace Users in the current sector, defined and validated	**SRD 001**: fully covered **SRD 005**: fully covered **SRD 008**: fully covered **SRD 006**: fully covered **SRD 007**: fully covered **SRD 011**: fully covered **SRD 016**: fully covered **SRD 026**: fully covered	RPAS has been considered as any other aircraft flying with IFR. RPAS maneuvers complied, and safety was kept at a high level.
		CRT-PJ13.115-V3-VALP-007-0004 Safe recovery of RPAS degraded operations in airspace classes A, B, C during accommodation	**N/A**	(The RTS did not perform the end of a C2LL and reversion to nominal flight)
		CRT-PJ13.115-V3-VALP-007-0005 Contingency procedures, especially in case of loss of C2 link, defined and validated	**SRD 016**: fully covered	Appropriate controlling methods regarding the flight area were used, maintaining safety even when RPAS entered in C2LL state.
	OBJ-115-V3-VALP-008 ATC accommodation of RPAS detailed analysis. Airspace User acceptability	**CRT-PJ13.115-V3-VALP-008-0003** Clear evidence of non-interference, seen from the legacy AUs, with any certified IFR RPA flying in any controlled	**SRD 026**: fully covered	No general privilege was given to the aircraft or to the RPAS. RPAS flight did not interfere with manned aircraft usual flight.

Exercise ID, Name, Goals	Exercise Safety Validation Objective & related SAC(s)	Success criterion	Coverage (SRS and/or SRD)	Validation results
		airspace of classes A, B, C with no procedural changes		
	OBJ-115-V3-VALP-009 ATC accommodation of RPAS detailed analysis	**CRT-PJ13.115-V3-VALP-009-0001** Standardization / harmonisation needed on the specific RPAS accommodation procedures.	**SRD 001**: fully covered **SRD 003A & B**: fully covered **SRD 012**: fully covered	ATCO requires a specific call sign prefix to recognise that the aircraft managed is a RPAS. The existing RPAS require specific C2LL diversion trajectories due to RPAS features or operator strategies.

Table 32: Solution Safety Validation results

Appendix I Assumptions, Safety Issues & Limitations

I.1 Assumptions log

Assumptions are statements that are taken for granted or that are considered true. They are usually related to matters outside the scope of the change, but which are essential to the completeness and/or correctness of the safety assessment results.

In this section, all the assumptions:

- Related to aspects regarding the RPAS accommodation phase that are relevant for the conduction of this SAR
- Necessarily raised in deriving the Safety Requirements considered

are listed in Table 33. Moreover, a rationale or evidence on which the validity of these assumptions is based is provided.

Ref	Assumption	Validation
A001	Accommodation allows for early RPA flights on a temporary and transitional basis and in limited numbers before the required technology, standards, and regulations are in place. During the accommodation phase: • RPAS will fly outside segregated airspace, that is, in IFR controlled airspace classes A to C. • RPAS will operate in environments with medium/low density of traffic. • All traffic is known and cleared into the controlled airspace. • For wake-turbulence separation, RPAS are considered as L category aircraft (including en-route separation). • The C2L used by existing/MIL RPAS meets the existing robustness specifications.	Scope of Solution 115
A002	The Flight Plan RPAS information has already been validated. This means that the standard filling and validation process of FP processing is applicable.	Scope of Solution 115
A003	In the Accommodation phase, ATC Voice (VHF) is lost when the C2Link is lost because RPA Operations relays both the Command/Control information and the Voice information on the same C2 Link to RPS Operations.	Scope of Solution 115
A004	The FP is filed or modified short before the flight and considering the latest weather forecast. Therefore, the RPAS will not operate under severe weather conditions since the trajectory included in the FP will avoid forecasted events like thunderstorms, icing, or electromagnetic disturbances.	Current experience of RPAS operation in segregated airspace.
A005	From an ATC environment point of view, the flight of the RPAS is considered to be an ordinary flight in the sectors or groups of sectors concerned. Therefore: • The current training of the ATCOs in IFR procedures/ operating methods prepares them to manage radio communications in order to assume the control of the different flights and provide them with instructions. Moreover, if the ATCO does not receive the expected information from an aircraft, they will ask the pilot or Remote Pilot to provide it.	Current experience of ATCOs in IFR controlled airspace classes A to C.

Ref	Assumption	Validation
	- The current training of the ATCOs in IFR procedures/operating methods prepares them to manage technical failures related to the ATSU, like radio failures, CWP failures, etc. - The training and knowledge of the operational environment of the ATS Unit, grant the proper monitoring of the RPAS trajectory through surveillance and FP data, in order to: ○ Apply separation minima in order to separate RPAS from other aircraft. ○ detect a conflict with RPAS flight trajectory. - The provision of ATS Unit's instructions to RPAS for resolution of conflicts (Vector/ Heading/ Altitude/ Speed instructions) is not conducted in a different way than for manned aircraft. - The current training of the ATCOs (TWR, APP, ACC Units) in IFR procedures/operating methods prepares them to face aircraft emergencies like engine failures. In such a situation, it is considered that the following actions are within ATCO's current skills: ○ Clearing of the path for RPAS trajectory (ACC/APP Controller). ○ Preparing airspace and runways for the emergency arrival of the RPAS (TWR Controller).	
A006	**A.** It is considered that RPs are already trained with regard to the IFR procedures and way of operating. Therefore, actions such as: - Initiating contact with the relevant ATS Unit (including first radio contact both when reaching the first GAT sector and when transferred to the next/adjacent ATS Unit). - Assessing ATCOs instructions and providing read back of them. - Alerting the relevant ATCO when a deviation that cannot be mitigated by crew is observed. Are within RP's current skills.	Current experience of RPAS operation in segregated airspace.
	B. It is considered that RPs are already trained with regard to the basic procedures of RPA management. Therefore, the following actions are within RP's current skills: - Application of procedures/operating methods for non-nominal situations *(no additional training because of flying in GAT)*. - Monitoring of flight trajectory. - Detection of the C2LL (loss of data with RPA). Moreover, RPs are trained and aware of the C2LL contingency procedures and they have already conducted diversion preparation in case of change, including the rechecking programmed behaviour at any time before a C2LL occurs	RP current training
A007	RP have traffic awareness in their RPS through radio communications on shared frequency and they are able to identify certain threats like the wake turbulence risk and request additional instructions to ATCO, if necessary. Since RPs are in the ground, they could also benefit from additional situational awareness systems that show traffic, for instance. Moreover, the RP is operating in IFR operational environment, so their situational awareness should be linked to the controls they need in this environment.	Current experience of ATCOs in IFR controlled airspace classes A to C.

Ref	Assumption	Validation
	RPs may also use the RPA camera to see around the aircraft and also have a better situational awareness from ground, but this has not been considered as an absolute behaviour of RP.	
A008	Usual tools (e.g. MTCD) used by ATCOs to detect and/or manage possible conflicts involving manned aircraft will be verified by the ANSP considering RPAS performances-related data and, if necessary, will be tuned for RPAS operating in the airspace, so that they are valid supporting tools. This includes tools such as conflict detection tools or controller support tools, as long as they are already used within each particular airspace. In those airspaces in which these tools are not used, the existing related safety case to operate under those conditions needs to be verified, with the addition of RPAS.	Scope of Solution 115
A009	Regarding the RPA systems related to C2L: • Aside from internal system malfunctions, RPA systems follow the pre-programmed/ re-programmed procedures introduced by RPS Operations. • The current capabilities of the RPA navigation system prevent the RP from introducing incoherent information. • The RPA system is always programmed with a C2LL trajectory that shall be automatically triggered and flown when the RPA goes into a C2LL state.	Current experience of RPAS operation in segregated airspace.
A010	Regarding emergencies related to RPAS flights (for example, engine failure): • The RP will be still under limited control of the RPA and will have voice communications. • The RPAS will fly a FPLN / trajectory deemed suitable by the Remote Pilot (within capabilities of the emergency state). It will be flown by the RP to an EMERGENGY DIVERSION waypoint and then to a termination area (airfield or emergency landing site). The information will be provided by the RP to ATC. • From an ATCO perspective, the management of this emergency flight has no additional RPAS particularities: the same contingency specificities apply. • It is considered that the planning of emergencies takes into account: ○ the capabilities of the RPA, the conditions of the landing site, etc. ○ performance degradation. This is done in an equivalent way to manned aircraft planning	Experience from RTS execution.
A011	Regarding C2LL contingency situations, it has been checked that: • The C2LL awareness procedure (during nominal flight at initial contact) does not generate additional workload, • C2LL is not a frequent occurrence and the increase of workload due to a C2LL contingency is equivalent to the increase of workload due to a PLOC in manned aviation	RTS conducted under the scope of Solution 115

Table 33: Assumptions log

Co-funded by the European Union

I.2 Safety Issues log

The following Table 34 contains the Safety Issues that were necessarily raised during the safety assessment, together with the necessary actions allowing to resolve them within the current scope of the SESAR Solution or the proposed strategy for a resolution beyond SESAR scope.

Ref	Safety issue	Resolution
I001	In case C2LL occurs just after vectoring instructions there might be no sufficient time for ATCO to fully check the details of the contingency procedure with the RP (currently 2 minutes – To be validated).	Validated within the RTS in Solution 115
I002	The conclusions stated in this SAR need to be confirmed through the collection of real data.	To be checked in next industrialisation/deployment phases (live trials)

Table 34: Safety Issues log

I.3 Operational Limitations log

No Operational Limitations were raised during the development of the safety assessment.

-END OF DOCUMENT-