



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

OPERATIONAL SERVICES AND ENVIRONMENT DEFINITIONS (OSED) FOR REMOTELY PILOTED AIRCRAFT SYSTEMS (RPAS) AUTOMATION AND EMERGENCY RECOVERY (A&ER) FUNCTIONS

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-253

March 2019

OPERATIONAL SERVICES AND ENVIRONMENT DEFINITIONS (OSED) FOR REMOTELY PILOTED AIRCRAFT SYSTEMS (RPAS) AUTOMATION AND EMERGENCY RECOVERY (A&ER) FUNCTIONS

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-253

March 2019

FOREWORD

1. This document was prepared by EUROCAE Working Group 105 “Unmanned Aircraft Systems (UAS)” in the framework of the Enhanced RPAS Automation Focus Team and was approved by the Council of EUROCAE on 14 March 2019.
2. EUROCAE is an international non-profit making organisation in Europe. Membership is open to manufacturers and users of equipment for aeronautics, trade associations, national civil aviation administrations, and, under certain conditions, non-European organisations. Its work programme is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.
3. The findings of EUROCAE are resolved after discussion amongst Members of EUROCAE and in collaboration with RTCA Inc., Washington D.C., and/or the Society of Automotive Engineers (SAE), Warrendale PA, U.S.A., through their appropriate committees.
4. EUROCAE performance specifications and other documents are recommendations only. EUROCAE is not an official body of the European Governments. Its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.
5. Copies of this document may be obtained from:

EUROCAE
9-23, rue Paul Lafargue
93200 Saint Denis
France

Telephone: 33 1 49 46 19 65
Email: eurocae@eurocae.net
Website: www.eurocae.net

TABLE OF CONTENTS

FOREWORD	I
TABLE OF CONTENTS	II
LIST OF FIGURES	III
LIST OF TABLES	IV
CHAPTER 1 INTRODUCTION	1
1.1 SCOPE	1
1.2 PROJECT ASSUMPTIONS AND EXCLUSIONS	3
1.2.1 GENERAL ASSUMPTIONS	3
1.2.2 EXCLUSIONS	4
1.3 DOCUMENT OVERVIEW	5
CHAPTER 2 CONCEPT SUMMARY	6
2.1 CONCEPT DESCRIPTION	6
2.2 HIGH LEVEL ARCHITECTURE	7
2.3 FUNCTIONAL DESCRIPTION OF AUTOMATION AND EMERGENCY RECOVERY FUNCTION	9
2.3.1 AUTHORITY CONCEPT	10
2.3.2 AUTOMATION CONCEPT	10
2.3.3 ESCALATION LEVEL CONCEPT	11
2.3.4 FLIGHT TERMINATION CONCEPT	13
2.3.5 PREDICTABILITY CONCEPT	14
2.3.6 FAULT MANAGEMENT CONCEPT	15
CHAPTER 3 OPERATIONAL SERVICES AND CAPABILITIES	17
3.1 MANNED AVIATION CAPABILITIES TO BE CONSIDERED FOR A&ER	17
3.2 A&ER CAPABILITIES WITH ALL COMMUNICATIONS LINKS FUNCTIONING	18
3.2.1 JUSTIFICATION OF CHANGES	18
3.2.2 CAPABILITY CHANGES	19
3.2.3 OPERATIONAL CHANGES	22
3.2.4 INTERFACE CHANGES	23
3.3 LINK LOSS SITUATIONS	23
3.4 A&ER (LOC) CAPABILITIES AND CAPABILITY DESCRIPTIONS	24
3.4.1 JUSTIFICATION OF CHANGES	24
3.4.2 CAPABILITY CHANGES	25
3.4.3 USAGE OF CAPABILITY FOR LINK LOSS	25
3.4.4 OPERATIONAL CHANGES	26
3.4.5 INTERFACE CHANGES	27
3.4.6 PERSONNEL CHANGES	27
CHAPTER 4 OPERATIONAL ENVIRONMENT	28
4.1 IDENTIFICATION OF THE ENVIRONMENT CONSTRAINTS	28
4.2 PERSONNEL REQUIREMENTS	28
4.3 SUPPORT REQUIREMENTS	28
CHAPTER 5 SCENARIOS DESCRIPTION	29
5.1 A&ER01 - NOMINAL FLIGHT	30
5.2 A&ER02 - FLIGHT PLAN DEVIATIONS EN-ROUTE	32
5.3 A&ER03 - SYSTEM FAILURE DURING TAKE-OFF AND EN-ROUTE	34
5.4 A&ER04 - FLIGHT PLAN MANAGEMENT EN-ROUTE (CA)	36
5.5 A&ER05 - PLAN TO LAND AT NEAREST/NEXT SUITABLE AIRPORT	38

	5.6	A&ER06 – PRIORITISATION OF CONFLICTING PROPOSALS	40
	5.7	LL01: COMMUNICATION FAILURE PROCEDURES IN RULES OF THE AIR.....	42
	5.8	LL02: ATC VOICE COMMUNICATION FAILURE.....	44
	5.9	LL03: ATC VOICE COMMUNICATION RECOVERY	46
	5.10	LL04: C2 UP-LINK FAILURE.....	48
	5.11	LL05: C2 UP-LINK RECOVERY	50
	5.12	LL06: C2 UP- AND DOWN-LINK FAILURE.....	52
	5.13	LL07: C2 UP- AND DOWN-LINK FAILURE WITHOUT ATC COMMUNICATION	54
	5.14	LL08: AUTOMATIC LANDING IN C2 LINK LOSS MODE	56
	5.15	LL09: SYSTEM FAILURE DETECTED IN C2 LINK LOSS MODE	58
	5.16	LL10: FLIGHT DEVIATION REQUESTED IN C2 LINK LOSS MODE	60
CHAPTER 6		SUMMARY	62
	6.1	OPERATIONAL ASSUMPTIONS	62
	6.2	OPERATIONAL REQUIREMENTS	64
CHAPTER 7		APPENDIX.....	66
	7.1	ACRONYMS.....	66
	7.2	GLOSSARY OF TERMS	68
	7.3	RPAS OPERATIONAL PHASES AND TYPE OF ACTIONS.....	72
	7.4	A&ER CAPABILITY RELEVANT ASSUMPTIONS AND OPERATIONAL REQUIREMENTS	73
	7.5	REFERENCED / APPLICABLE DOCUMENTS	74
		WG-105 / FT ERA / AUTOMATION AND EMERGENCY RECOVERY SUB-GROUP MEMBERSHIP ..	76
		IMPROVEMENT SUGGESTION FORM	77

LIST OF FIGURES

FIGURE 1.1: RPAS SYSTEMS AND INTERACTIONS WITH OTHER AIRSPACE USERS	2
FIGURE 2.1: A&ER OPERATION	7
FIGURE 2.2: GENERIC RPAS ARCHITECTURE	8
FIGURE 2.3: FAULT MANAGEMENT CHAIN FOR ERA	16
FIGURE 3.1: LINKS BETWEEN ATC, RPA AND RPS	23
FIGURE 5.1: A&ER01 NOMINAL FLIGHT.....	30
FIGURE 5.2: A&ER02 FLIGHT PLAN DEVIATIONS EN-ROUTE	32
FIGURE 5.3: A&ER03 SYSTEM FAILURE DURING TAKE-OFF AND EN-ROUTE	34
FIGURE 5.4: A&ER04 FLIGHT PLAN MANAGEMENT EN-ROUTE (CA).....	36
FIGURE 5.5: A&ER05 PLAN TO LAND AT THE NEXT SUITABLE AIRPORT	38
FIGURE 5.6: A&ER06 PRIORITISATION OF CONFLICTING PROPOSALS	40
FIGURE 5.7: LL01 COMMUNICATION FAILURE PROCEDURES IN RULES OF THE AIR.....	42
FIGURE 5.8: LL02 ATC VOICE COMMUNICATION FAILURE	44
FIGURE 5.9: LL03 ATC VOICE COMMUNICATION RECOVERY	46
FIGURE 5.10: LL04 C2 UP-LINK FAILURE.....	48
FIGURE 5.11: LL05 C2 UP-LINK RECOVERY.....	50
FIGURE 5.12: LL06 C2 UP- AND DOWN-LINK FAILURE.....	52
FIGURE 5.13: LL07 C2 UP- AND DOWN-LINK FAILURE WITHOUT ATC	54
FIGURE 5.14: LL08 AUTOMATIC LANDING IN C2 LINK LOSS MODE	56
FIGURE 5.15: LL09 SYSTEM FAILURE DETECTED IN C2 LINK LOSS MODE	58
FIGURE 5.16: LL10 FLIGHT DEVIATION REQUESTED IN C2 LINK LOSS MODE	60

LIST OF TABLES

TABLE 3.1: MANNED AVIATION CAPABILITIES TO BE COVERED BY AN A&ER FUNCTION	17
TABLE 3.2: MANNED / UNMANNED CAPABILITIES.....	19
TABLE 3.3: TRANSPONDER CODES	26
TABLE 5.1:SCENARIOS DESCRIPTION.....	29
TABLE 7.1: ACRONYMS	66
TABLE 7.2: GLOSSARY OF TERMS	68
TABLE 7.3 RELEVANT ASSUMPTIONS	73
TABLE 7.4: RELEVANT OPERATIONAL REQUIREMENTS	74

CHAPTER 1

INTRODUCTION

This document provides the Operational Services and Environment Definition (OSSED) for automation and emergency recovery (A&ER) aspects of integration of RPAS into non-segregated airspace and airfields.

This OSSED provides a basis for assessing and establishing operational, safety, performance, and interoperability requirements for the A&ER capabilities for Remotely Piloted Aircraft Systems (RPAS) flying in non-segregated airspace. This document seeks to characterize those differentiated attributes of RPAS and to define their relationship to air traffic services, other airspace participants, and operating environments of the defined airspace.

This OSSED captures high level requirements that have been derived and/or validated as being necessary for the candidate's capabilities. It is intended to be used as a supporting document for implementation of ED78 process in the definition of Safety and Performance Requirements (SPR) and Interoperability requirements (INTEROP). It is considered as a baseline to support the development of Minimum Operational Performance Specification (MOPS) and Minimum Aviation System Performance Standards (MASPS). The OSSED is based on the information provided in the ERA Concept of Operations (CONOPS).

1.1

SCOPE

Remotely Piloted Aircraft Systems (RPAS) operations are currently performed in segregated airspace or under strict conditions of operation. Their safe integration into the airspace (Controlled and non-controlled airspace (class A to G); i.a.w. Instrument Flight Rules (IFR) / Visual Flight Rules (VFR), under Instrument Meteorological Conditions (IMC) / Visual Meteorological Conditions (VMC)) will improve their benefits for operations and enable their expected use by civilian operators. However, many substantial barriers, including technical issues, certification and regulation changes, and legal and social concerns, must be overcome before widespread use of RPAS in civil aviation is possible.

RPAS is a subcategory of Unmanned Aircraft Systems (UAS) that has a Remote Pilot (RP) controlling and monitoring the aircraft from a remote position. The term system refers to the complex nature of RPAS, where a Remotely Piloted Aircraft (RPA) is piloted from a Remote Pilot Station (RPS) utilizing a command and control (C2) link. Together with other components such as launch and recovery equipment, if utilized, the RPA, RPS and C2 link comprise an RPAS.

RPAS and their interactions are depicted at a high level in [FIGURE 1.1](#), including those possible interactions with the environment and other Airspace users (civil manned aircraft, military aircraft...).

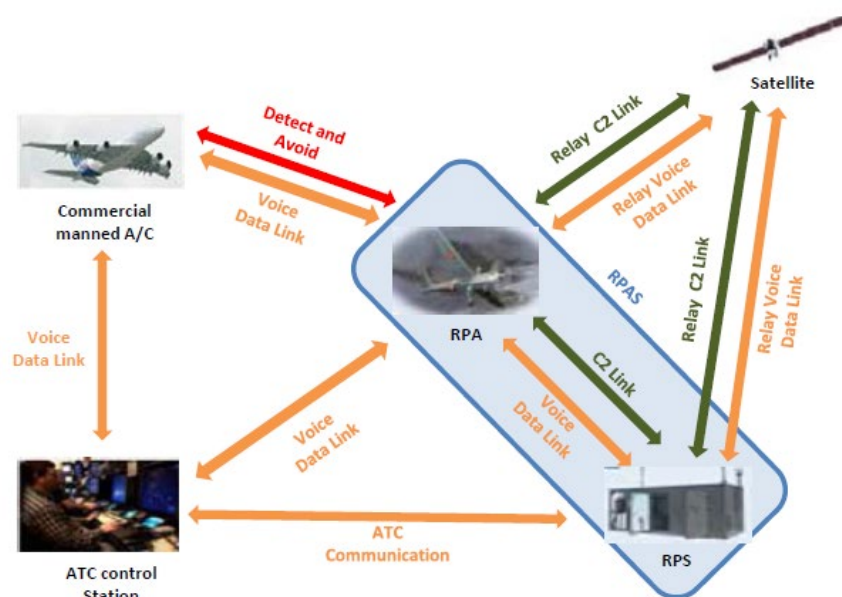


FIGURE.1.1: RPAS SYSTEMS AND INTERACTIONS WITH OTHER AIRSPACE USERS

NOTE: The C2 link includes the direct communications links as well as the relay links.

If RPAS are to be integrated, either for civil or military applications, they will have to comply with the same rules and procedures as the other airspace users, without degradation of the level of safety, or disruption of current operations or modifying air traffic control (ATC) procedures. Therefore, it is considered that RPAS behaviour in operations must be equivalent to manned aviation, including interaction with ATC.

RPAS must adhere to the rules of the airspace and must comply with the communication, navigation and surveillance (CNS) requirements in Air Traffic Management (ATM) context applicable to the class of airspace within which they intend to operate. This includes providing corrective actions and flight information in real time, maintaining position between two points of the trajectory, and verifying that the aircraft is where it should be. RPAS must also meet supplementary certification requirements to fly under specific conditions (e.g. flight into known icing conditions), if their typical mission profile will involve such conditions.

Challenges in airspace integration are related to the fact that the RP is physically separated from the RPA, resulting in a reduced situational awareness, limitations in operating and monitoring the RPA's systems (i.e. in case of C2 link interruption or loss, but possibly also by design), and delays introduced by the C2 link. These factors contribute to the RP's workload and limit the ability to effectively react to situations.

Automation is the way to safely relieve the aircrew of some routine duties thereby reducing fatigue (e.g. by autopilots, auto thrust, auto brake, navigation system). Acceptable Means of Compliance (AMC) 25.1302 – Appendix 2 states that "automation is the autonomous execution of tasks by aeroplane systems started by a high level control action of the flight crew". The intended RPAS automation capability is also expected to be used as a backup strategy to safely cope with the lack of a human in the control loop especially during contingencies, e.g. loss of C2 link, and emergencies. Generally, limits and risks associated with increased levels of automation must carefully be assessed. Especially, Human Factors must be considered. International Civil Aviation Organization (ICAO) Circular 249-AN149 "Human Factors in CNS ATM Systems" provides guidance in this area.

The basic workload tasks of the minimum flight crew considered in the Certification Specification (CS) 25.1523 as adapted for RPAS, are the following:

- Flight path control.
- Collision avoidance.
- Navigation.
- Communications.
- Operation and monitoring of RPAS components.
- Command decisions.

In the RPAS automation context, these pilot-related functions will be allocated to either a RPS or a RPA or to both. Neither of these functional allocation strategies is part of the assumption basis of the current regulations and standards, yet their use must provide a level of safety equivalent to that of manned aircraft operations. Throughout this document the only flight crew member identified is the RP. There is nothing in this documentation to prevent the creation of other flight crew roles, providing the definition and operation of the RPAS complies with the rules of the air.

The European RPAS Roadmap published by the European RPAS Steering Group (ERSG) states:

"...The R&D effort to close the identified operational and technology gaps will include the need to develop operational procedures, technical systems models or prototypes leading to proposed standards in parallel, but clearly linked to the development of regulations and standards for the safe and efficient integration of RPAS..."

The scope of the A&ER function is limited to those phases where operational responsibility is with the RP.

Additional operations done before "Handover to Remote Pilot" or after "Handover to Ground Crew" such as maintenance procedures, mission planning, etc. are considered beyond the scope of this OSED. Aspects beyond the scope of the A&ER function (but their existence in the RPAS is expected) are:

- Avoidance Manoeuvres which are defined by other subsystems, e.g. Detect & Avoid (DAA) for intruder avoidance and, as far as required by the mission profile, weather and terrain avoidance (however, A&ER needs to prioritise between conflicting information from those subsystems).
- Standard flight guidance and control functions like flying standard turns, following the planned route, acquiring and holding target values for altitude, heading, etc., as detailed in Aeronautical Radio, Incorporated (ARINC) 702A standard;
- Sensing, identifying and isolating subsystem failures;
- Detection of events e.g fire, bird strike, hard landing, lightning strike, severe turbulence, unusual vibration, hail and icing;

Further, the following aspects are considered beyond the scope of the A&ER function and not expected in an RPAS:

- Voice recognition and synthetic voice communication;
- Task that cannot be automated with current state-of-the-art technology;

1.2 PROJECT ASSUMPTIONS AND EXCLUSIONS

1.2.1 GENERAL ASSUMPTIONS:

- **Assumption #01 (AS#01):** All RPAS operations are conducted under IFR.
- **AS#02:** RPAS operate as General Air Traffic (GAT).
- **AS#03:** This OSED applies to RPAS which are type certified to operate in the intended environment.
- **AS#04:** RPAS can operate from a variety of surfaces.
- **AS#05:** RPAS use instrument approach and departure procedures applicable to the airfield and for the available navigation equipment aboard the RPA.

- **AS#06:** RPAS use straight-in approaches, and does not operate in the traffic pattern.
- **AS#07:** The RP complies with ATC instructions within the RPAS's capabilities in an equivalent manner as the pilot of a manned aircraft.
- **AS#08:** Each RP has the appropriate qualifications, training and license to operate the RPAS in the UAS certified category of operations and in the intended environment.
- **AS#09:** The RP always has control or override authority over the RPAS unless circumstances prevent him from using this authority in a timely manner;
- **AS#10:** The RP is responsible for ensuring that the RPAS will meet RPA performance and equipment requirements for the intended operating environment and comply with relevant procedures.
- **AS#11:** All RPAS equipment and functions are covered by the type design approval and are suitable for flight in the environment in which the RPAS operates.
- **AS#12:** Critical systems on board the RPA monitor their health status and provide that status to the A&ER function and, via the C2 downlink, to the RPS for display to the RP.
- **AS#13:** The RPA, RPS, C2 link and other flight or safety critical elements will attain necessary certifications and / or approval for flight operations.
- **AS#14:** To the maximum extent practicable RPAS and their operation will conform to existing manned regulations and procedures. If peculiarities of an RPAS prevent this, an equivalent level of safety must be reached by alternative regulations and procedures.
- **AS#15:** The A&ER function monitors RPA status and situation during the entire RPAS operation. It has the authority to issue commands if necessary, but can be overruled by the RP when the C2 link is available and the initiated action can be undone.
- **AS#16:** For RPAS operation a flight plan (FP) must be prepared which includes Alternate or / and Emergency / contingency sites, including forced landing / ditching sites, where required. The additional information will be made available to ATC or, where ATC is not in a position to handle it, kept at hand by the RP to be communicated to ATC on request.
- **AS#17:** All data links are secure against any unauthorized access.
- **AS#18:** New or revised operational rules are in place, along with associated standards, procedures and policies that enable the ground, terminal, and en-route operations described in this OSED.
- **AS#19:** Both the RPA and RPS are equipped with a flight data recorder.
- **AS#20:** The RPA is uninhabited meaning there is no person on board.

1.2.2

EXCLUSIONS

- Legal aspects related to the performance of emergency recovery actions, selection of forced landing sites / ditching areas as well as related to the execution of a forced landing because they shall be the decision of the individual States.
- The specifics of securing the data links.
- Design and development of functions and techniques for active or passive protection against any hostile attacks or actions (security threats) are out of the scope. This project will consider security in the functional architecture of the three functions as far as applicable.
- Fuel jettison / dumping is not considered due to its complexity.

1.3 DOCUMENT OVERVIEW

This document aims to describe the characteristics, behaviour and conditions of operation of a RPAS equipped with an A&ER function, flying in non-segregated airspace.

The intended audience is the future users and personnel whose work will be affected by the introduction of A&ER. This includes RPAS operators, RPs, RPAS system developers, Air Navigation Service Providers (ANSPs) air traffic controllers, EUROCONTROL, Civil Aviation Authorities (CAA), Regulatory Agencies, Aircraft Operators, flight crew of manned aviation, Aircraft Manufacturers, Avionics Manufacturers, Military Authorities and Military Aircraft Operators.

The document is organized as follows:

- Chapter 1 – Introduction;
- Chapter 2 – Concept Summary;
- Chapter 3 – Operational services and Capabilities;
- Chapter 4 – Operational Environment;
- Chapter 5 – Scenarios descriptions;
- Chapter 6 – Summary.

Annexes:

- Annex 7.1: Acronyms
- Annex 7.2: Glossary and Terms
- Annex 7.3: RPAS Operational Phases and Type of Actions;
- Annex 7.4: A&ER Capability Relevant Assumptions and operational Requirements
- Annex 7.5: Referenced / Applicable Documents
- WG-105 / FT ERA / Automation and Emergency Recovery Sub-Group Membership;
- Improvement Suggestion Form

This document leverages information from the on-going ERA project, in particular from the ERA CONOPS, as well as additional expertise brought in during the review process within EUROCAE Working Group-105 (WG-105).

CHAPTER 2

CONCEPT SUMMARY

2.1

CONCEPT DESCRIPTION

The A&ER function's main purpose is to take over decision making when the RP is unable to effectively perform that task, e.g. during link loss or when latencies introduced by the data link would prevent a timely reaction. Further, the A&ER function assists the RP in decision making with C2 link available by carrying out certain tasks to reduce workload and to provide better situational awareness. Possibly, it also supports the RP in the communication with ATC during C2 link loss.

According to ERA CONOPS, the operational scope of the three ERA System of Interests (SOIs) with respect to the operational phases of a generic RPAS can be defined as follows:

- Automatic Take-Off and Landing (ATOL) is operationally active during Take-off / Rejected Take-off / Initial climb / Initial and Intermediate Approach (including holding procedures) / Final Approach / Landing and ground roll up to RPA full stop/ Go Around / Missed Approach;
- AutoTaxi is operationally active during surface operations;
- A&ER is operationally active during all phases: Take-off / Rejected Take-off / Initial climb / En-route flight / Initial and Intermediate Approach (including holding procedures) / Final Approach / Landing and ground roll up to RPA full stop (or safe taxi speed achieved) / Go Around / Missed Approach and Surface Operations.

The complexity increases when defining which tasks fall within A&ER's perimeter and which fall within ATOL / AutoTaxi's perimeter. This can best be achieved by noting that:

- In all phases of flight, the authority to issue high-level commands will fall entirely in the perimeter of A&ER, unless A&ER is overruled by the RP, who has the final authority whilst he/she has the means to effectively make use of it;
- ATOL and AutoTaxi as sublevel functions will control all operations of their associated flight phase, whether they are nominal or non-nominal;
- Basic Flight Management System (FMS) functions are used to control operations in the en-route phase of flight;
- The health monitoring of the SOIs will fall within the scope of the SOI.

The A&ER function monitors RPA system states in all phases of flight. When the C2 link is available, the A&ER function reports any non-normal system states – unless they are already made available by the affected systems themselves – to the RP, possibly together with proposals for rectification. In situations that cannot be handled by the RP, e.g. in case of C2 link loss or in time-critical situations, the A&ER function initiates an RPA reaction without waiting for the RP's approval. As an example, if the ATOL system detects an abnormal ATOL system status that leads to an increased risk when landing, it would send a request to initiate a go-around to the A&ER function. The A&ER function then assesses whether the status of all other RPA systems permits to safely execute a go-around and missed approach procedure and – if positively assessed – sends the go-around command to ATOL.

The OSED focusses on the A&ER capability taking into account its interfaces with the ATOL and the AutoTaxi SOIs.

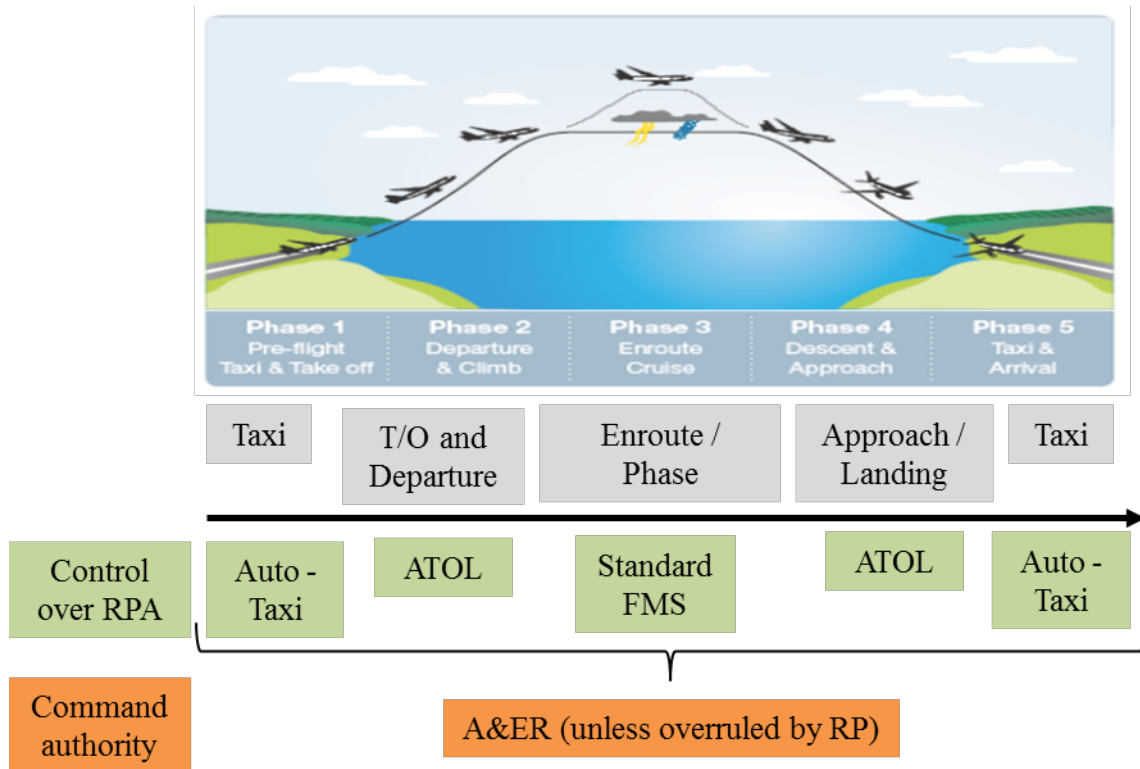


FIGURE 2.1: A&ER OPERATION

AS#21: RPAS requires certification according to appropriate standards published by the applicable certification agency.

Operational Requirement #01 (OR#01): The A&ER function shall support the RP in performing the actions required for a given situation in order to avoid errors, omissions and wrong order of operating steps.

OR#02: The A&ER function shall be designed to comply with applicable RPAS airworthiness standards.

AS#22: It is assumed that RPAS are equipped with a DAA system that provides a collision avoidance capability. The DAA system also provides traffic information to the RP to provide situational awareness and to support him to keep the RPA well clear of traffic.

NOTE: *Terrain Avoidance and Weather Avoidance systems, including ice protection, are not always mandated for RPAS integration into non-segregated airspace. In analogy to manned aviation, flight under IFR may be safely feasible and permissible without such systems. However, the absence of such systems can be expected to considerably restrict the range of missions which can be flown. If, to avoid such limitations or required for certification, those systems are installed, it is expected that they are handled in a similar way than a Traffic Avoidance system.*

AS#23: The DAA system is assumed to forward required avoidance manoeuvres to the A&ER function for prioritisation against other systems.

NOTE: *Traffic avoidance manoeuvres will always have priority and override any other inputs from other systems, except in some severe failure cases where the priority would be to keep the RPA in a limited flight envelope where it is impossible to manoeuvre.*

2.2

HIGH LEVEL ARCHITECTURE

The proposed A&ER function is seen as part of the overall Air Vehicle Management System (AVMS) functions of the RPA. In other words, the A&ER SOI groups together

all AVMS functions which are related to the recognition of system failure states, and to the respective system reaction.

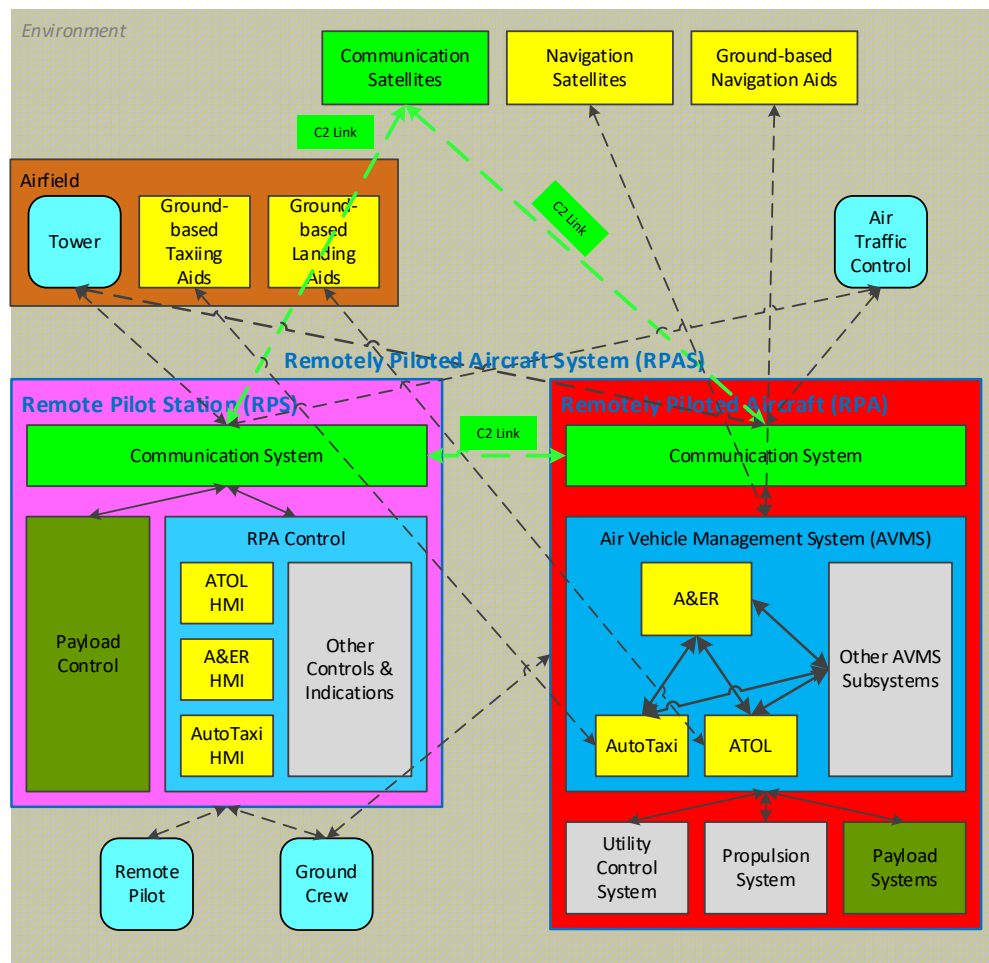


FIGURE 2.2: GENERIC RPAS ARCHITECTURE

FIGURE 2.2 shows a generic RPAS architecture consisting of following elements:

- The RPAS consisting of the RPA and the RPS.
- The RPAS Operational Environment comprising:
 - The Airfield infrastructure consisting of the control tower and the installed standard or RPAS-specific approach / landing / taxiing aids e.g.: Instrument Landing System (ILS), Ground Based Augmentation system (GBAS).
 - The ATC unit responsible for the envisioned flight phases in controlled airspace.
 - The communication satellites used to relay telemetry and C2 uplink in case direct Line-Of-Sight communication between RPS and RPA are not available.
 - The navigation satellites i.e. Global Navigation Satellite System (GNSS) providing positioning and navigation services to the RPA.
 - Ground-based navigation aids providing the required backup navigation means.
 - ATC surveillance systems providing RPA surveillance data to ATC e.g. Automatic Dependent Surveillance-Broadcast (ADS-B), Automatic Dependent Surveillance-Contract (ADS-C), Aircraft Communications Addressing and Reporting System (ACARS) and the operator (e.g. ACARS, GADSS).
- The system operators represented by the RP and the RPAS Ground Crew.

The RPA contains an Air Vehicle Management System (AVMS) which is controlling the RPA in all operational phases, acting on RP commands and monitored by the RP located in the RPS whenever possible. The AVMS controls the thrust setting by sending the appropriate commands to the Propulsion System. It also sends

commands (like the change of the nose wheel direction, the application of the brake, etc.) to the Utility Control System. A dedicated interface allows exchanging data and commands with the Payload System(s).

The AVMS contains the ATOL system, the AutoTaxi system and the A&ER function, including the link loss functionality. The A&ER function is directly interfaced to the ATOL and AutoTaxi systems, and is connected via the AVMS interface to the Communication System, Utility Control System, Propulsion System, and Payload Systems.

The RPA interfaces with the RP located at the RPS via the Communication System – for situations where a direct Line-Of-Sight communication between RPS and RPA is not possible, communication satellites might be used as relay.

It is assumed that the standard RP-ATC communication is performed via the on-board communication system (ATC radios), with the RPA acting as a relay. A direct communication line between RP and ATC might also be considered, either as nominal or as backup communication.

The RPS hosts the Human-Machine Interface (HMI) consisting of the relevant displays, command and control interfaces and communication means. Specific indications and controls for A&ER, ATOL and AutoTaxi are incorporated in the HMI, as well as a Mission Control Station for the management of the mission, as far as applicable.

AS#24: It is assumed that the RPA is equipped with primary and backup navigation means as required for the intended operation, i.e. flight under IFR, and airspace. A typical setup may be an Inertial Navigation System (INS) coupled with a GNSS receiver for primary means of navigation and terrestrial radio navigation e.g. Very High Frequency Omnidirectional Range (VOR) / Distance Measuring Equipment (DME) for backup.

AS#25: The AVMS is assumed to be capable to safely continue the flight by using the backup navigation source when the primary navigation source is no longer available or has insufficient accuracy and integrity.

AS#26: The RPA is assumed to be operating under IFR. Typically, it will be a fixed wing type aircraft, though this does not exclude other aircraft classes.

AS#27: The assumption is that RPAS contain an AVMS which is controlling the RPA in all operational phases, acting on High Level Commands received from the RP located at the RPS.

AS#28: It is assumed that the A&ER function is interfaced – either directly or via the AVMS interface – with the ATOL and AutoTaxi functions, the Communication System, Utility Control System, Propulsion System and Payload Systems, including their respective health monitors.

OR#03: The A&ER function shall be compatible with the ATOL and Auto-Taxi capabilities.

AS#29: The RPA interfaces with the RP located at the RPS via the C2 uplink. It is assumed that Beyond Radio Line Of Sight (BRLOS) communication is possible. Link performance e.g. latency, availability is assumed to be in agreement with minima for the airspace the RPA is operating in.

2.3

FUNCTIONAL DESCRIPTION OF AUTOMATION AND EMERGENCY RECOVERY FUNCTION

This paragraph describes the characteristics, behaviour and conditions of operation of an RPAS equipped with an A&ER function

In manned aviation it is the task of the pilot to perform certain actions at certain points in time during the flight or when certain events occur. The actions are usually defined in corresponding checklists, but also in a quick reaction handbook or an operator's manual. Further, they are based on memory items, cockpit flows and basic airmanship. The operation of RPAS will be determined by the purpose of the flight, the flight rules, and areas of operation and the functional levels of the C2 uplinks. Because there is no pilot inside the RPA, the management and controlling of RPA

systems/equipment must necessarily be performed either remotely by the pilot or via automation.

The inherent delays introduced by the C2 uplink might jeopardize the prompt execution of time critical actions, e.g. the reaction to sudden failures or external events like conflicting air traffic requiring an immediate avoidance manoeuvre. Therefore for an RPAS it is necessary to perform time-critical actions automatically. Equally, the A&ER function has to assume authority over the RPA whenever the C2 link becomes unavailable. As a beneficial side effect the automation layer can relieve, if properly used, the RP from the performance of routine tasks and support him in high workload situations, e.g. during an emergency.

The automatic reactions of the A&ER function are expected to be based on basic concepts as detailed below.

2.3.1

Authority Concept

The A&ER function has the role of monitoring the status of all the systems and also the external situation. It recognises a need to react to external and internal requests from A&ER, ATOL and AutoTaxi, as well as from other system as Traffic Avoidance, Terrain Avoidance or Weather Avoidance. It then proceeds to assess the situation, prioritise and come to a decision in terms of the best way forward. This request-command-execute cycle is the architecture that is followed for all of the interactions between A&ER, ATOL and AutoTaxi. This means, that even if ATOL and AutoTaxi have commands that need to be carried out, they can only request it, as A&ER has a more comprehensive situation awareness of the state of the RPA. As a result, the decision-making architecture is concentrated in the A&ER function.

Whilst the C2 link is available, the RP has the final authority over all decisions. Therefore, the highest-ranking reaction according to the A&ER function's prioritisation is presented in the RPS, to be accepted, declined or modified by the RP. Depending on the HMI concept implemented, further options may also be shown for selection by the RP. The RPA will execute the proposed reaction only on the RP's command.

Time-critical situations where limited situational awareness of the RP or latencies introduced by the C2 uplink would make a timely and correct RP response unlikely, e.g. a propulsion issue during take-off requiring a take-off abort, are exempt from this rule. Further, reactions which can easily be undone by the RP, e.g. switching of lights, may be automatically commanded by the A&ER function while informing the RP. In any case, a detailed safety assessment of the RPAS will be required to ensure such automatic reactions do not introduce undue hazards.

OR#04: Any automatic reactions of the A&ER function shall be in accordance with applicable regulations and procedures, unless overruled by a RP decision to deviate from those rules.

OR#05: The A&ER function shall react to alerts and critical failures by commanding pre-defined reactions if the RP cannot be expected to initiate a crucial action in a timely manner – e.g. in case of link loss or in time-critical situations – or if the automatic reaction easily can be undone by the RP.

OR#06: Automatic reactions of the A&ER function shall not create or aggravate risks to the RPA, other air traffic or persons and property on ground.

OR#07: The RPA shall accept commands only from one RPS at any given time. This RPS needs to be clearly identified and handovers must be unambiguous.

OR#08: The A&ER function shall support RPS handovers, e.g. by assisting in configuring the receiving RPS.

2.3.2

Automation Concept

The selection of the level of automation depends on the nature of the automation task but also on constraints imposed by regulatory bodies on which level of automation is acceptable. As a consequence, the following levels of automation are applied by the A&ER function.

- (1) If data link is available and an immediate reaction is not necessary then the A&ER function may propose an action but the RP has the final decision, with the following options for the system:

- wait for RP's command
- execute the proposed action if the RP does not react

The behaviour of the A&ER function will be as follows:

- When the link is available, high level alerts will be provided together with a proposed way of action prepared by the A&ER function for which authorisation from the RP is requested. Those high level alerts can have different priority levels (i.e. advisory, caution, warning).
- Depending on the condition the A&ER function will:
 - (1) wait for RP's command e.g. low fuel to request an appropriate re-planning, or
 - (2) execute the proposed action if the RP does not react within a defined period of time e.g. engine on fire shut down requested.
- (2) If an immediate, time-critical reaction is necessary to prevent unsafe conditions then the system has to react automatically.

Such conditions may be e.g. envelope protection, reconfiguration due to faulty sensors, pumps, etc.)

The behaviour of the A&ER function will be as follows:

- When the link is available perform the required action and cancel it when requested by the RP e.g. mid-air collision avoidance manoeuvre.
- (3) If the C2 uplink is NOT available then the RP is disconnected and cannot act onto the on-board system. Under such conditions, the system will, instead of proposing an action to the RP:
 - execute the action automatically;

The behaviour of the A&ER function will be as follows:

- In case of a confirmed C2 downlink loss (link failed for pre-defined time, all attempts to automatically reestablish the C2 downlink have failed) , high level alerts will be generated and stored for later transmission to the RP. In order to ensure predictability, the resolving action is identified through application of a rule based, pre-defined course of action accepted by the RP at flight planning stage. This includes prioritization of conflicting tasks as well as communication of status and intent to the outside world.
- The identified action will be performed automatically and stored for later transmission to the RP, i.e. after the C2 downlink has become available again.

OR#09: The response to loss of the C2 Link shall be part of the A&ER function.

OR#10: The A&ER function shall be capable of monitoring the status of all data links and to notify the RP if a link Loss is detected. Alternatively, the data links may be monitored by communication system, as long as this has the required integrity.

2.3.3

Escalation Level Concept

As a general rule, the Escalation Levels shall ensure goals as listed below, in order of decreasing precedence:

- Safety of life must be the highest priority; therefore hazards to people, both in the air and on the ground as well as to critical infrastructure must be minimised and safety requirements must be kept within acceptable limits.
- Damage to or destruction of the RPA should be avoided unless it causes undue burden on the Air Traffic System.
- The impact on the air traffic system must be kept to a minimum. Ideally, RPA should not create additional workload to ATC and other airspace users, as compared to a manned aircraft flying a similar mission.
- RPA shall operate as efficiently as possible. To achieve this, as many mission objectives as possible shall be fulfilled while consuming as little resources as

possible. Resources include fuel, time and effort for preparing the RPA for a successive mission.

The Escalation Levels mostly are introduced to determine the strategic behaviour and goals of the RPA in case of C2 link loss. With the C2 link available, actions may still be governed by the concept of Escalation Levels, but are freely decided by the RP. Basically, the Escalation Levels are derived from the decision making process commonly employed in manned aviation, which have been analysed and adapted to RPAS.

Escalation Level “Nominal”

This Escalation Level is used as long as RPA status and situation permit to safely fulfil the mission. As long as higher goals, i.e. safe and efficient integration into the air traffic system are ensured, mission efficiency is the main goal. As the RPA is flying, typically on the pre-planned nominal route as filed in the (ATC) flight plan, under control of the RP, who is acting according to ATC instructions, predictability is at least equal to that of a manned aircraft.

The RPA will continue towards its pre-planned destination on the nominal route. Small deviations are possible, but the RPA will re-join the nominal route after completing the deviation.

As C2 link loss is considered a contingency, the escalation level “Nominal” is only available as long as the C2 link is available.

Escalation Level “Contingency”

If the original destination, using the nominal route, cannot be reached anymore, at least parts of the mission cannot be fulfilled anymore. The main goal now is to minimise adverse effects on the air traffic system, as long as higher goals like safety of life and avoiding damage to equipment remain assured. Predictability being a key aspect of integration into the air traffic system, the contingency behaviour of the RPA must be pre-planned in detail, or alternatively agreed between RP and ATC.

The RPA will change to a pre-planned contingency route leading to a contingency landing site. Again, small deviations are permissible without further increase of the Escalation Level as long as the RPA can return to the contingency route.

The risk associated to a contingency landing shall not be higher than that of a nominal landing, therefore any contingency landing site would be equipped in a similar way as the nominal destination, e.g. in terms of landing aids. The same applies for a landing under C2 link loss and consequently for C2 link loss landing sites. Therefore, the Escalation Level “Contingency” will be set if C2 link loss occurs, unless a higher escalation level is mandated by additional occurrences.

According to guidance received from ICAO RPAS Panel, the cases where the RPA will deviate from the nominal route due to C2 link loss will be limited to very few situations, e.g. C2 link loss while the RPA still is in the terminal area of the departure airport.

Escalation Level “Emergency (Emergency Landing)”

If the RPA is unable to reach the original destination or any contingency landing site, or the RPA status and situation mandates that the RPA must land at the nearest suitable airport, the Escalation Level is increased to “Emergency (Emergency Landing)”. The main goal now is to save the RPA, as long as this creates no undue hazard to persons or property on the ground. In analogy to manned aviation, a reduced level of predictability is acceptable in an emergency, but still the RPA is supposed to act according to generally known and accepted rules and to communicate its status and intention as far as possible.

The RPA will change to a at least partly pre-planned emergency route leading to an emergency landing site. As emergency landings are expected to be rather rare events, the associated components of the safety budget may be different as for normal operations as long as the overall safety level is maintained. After a deviation, the RPA will continue flying to the emergency landing site as long as it is still able to reach it.

Escalation Level “Emergency (Flight Termination)”

If no pre-planned landing site of any kind can be reached anymore, the Escalation Level increases to “Emergency (Flight Termination)”. It is assumed that the RPA cannot be saved anymore, therefore the only remaining goal is to minimise risk to persons and property on ground and in air. Predictability should be maintained as far as possible, but safety of life must take precedence.

The RPA will fly to a suitable location and enter a flight termination manoeuvre there. Selection of such a location and flight termination manoeuvres are described in more detail in the flight termination section of this document.

The A&ER function is not permitted to undo a decision for emergency landing or flight termination made by the RP even if there is a C2 link loss.

OR#11: Under C2 link loss, the A&ER function shall command necessary deviations from the nominal trajectory, including – if necessary – emergency landings and flight termination.

2.3.4

Flight Termination Concept

In manned aviation, the pilot will attempt an off-airport landing in case an emergency landing is required and no suitable airfield can be reached. The location for that off-airport landing will typically be visually identified and selected in a way to maximise survivability for persons on board the aircraft, taking into account factors like geography and obstacles.

In principle, off-airport landings are an option for RPAS as well. However, due to the limited situational awareness of the RP, selection of an appropriate location and ad-hoc planning of the trajectory will almost invariably be more difficult than for the pilot of a manned aircraft. In case of C2 link loss, off-airport landings are generally assumed to be very challenging as an autonomous system would be required to identify a suitable location. Therefore, off-airport landings are presently not considered an option for RPAS.

Instead, flight termination is in the C2 link loss case the only viable option. Since the RPA is uninhabited, the main concern would be not to endanger persons or property on the ground or other air traffic. This is mainly achieved by appropriate selection of the location where the flight termination manoeuvre will be performed. The following options are available for this:

- As long as the C2 data link is available and suitable sensors provide adequate information, the RP may manually select a location and command the flight termination there. Predictability would be assured by the RP communicating his decision to ATC. The A&ER function may support the RP by proposing a suitable location based on a list of pre-planned termination areas.
- Under C2 link loss, the A&ER function may select a suitable flight termination area from a list of pre-planned, designated termination areas, as far as they are available and within reach. The selection of the flight termination area would be based on the geographic position of the RPA according to pre-defined rules, thus assuring predictability as far as still possible. Also, the RPA would communicate its intention to ATC with all available and permissible means. Assuming that identification of prospective flight termination areas during flight planning has properly considered avoiding risk to third parties, this approach would minimise hazards.
- Especially in sparsely populated areas, where flight termination generally would carry no undue risk to persons or property on the ground, avoidance areas may be defined during flight planning. In case flight termination is required, the RPA would perform a flight termination manoeuvre anywhere except in one of those avoidance areas. Avoidance areas would have to be defined around population centres, critical infrastructure and other vulnerable areas or objects. Predictability would be very limited for this option, as the exact location where flight termination is performed is not pre-defined.
- In a staged approach, flight termination would preferably be performed in a flight termination area. Only in case this cannot be achieved, the RPA would revert to

the avoidance area concept as a last resort in order to avoid damage to third parties.

Flight termination may be performed in a number of different ways. Preserving the structural integrity of the RPA may not necessarily be an aim, especially where this is in conflict with the aim to reliably restrict damage effects to the location chosen for flight termination. The following kinds of flight termination manoeuvres are conceivable:

- Controlled flight into terrain, including into bodies of water, is believed to be a flight termination manoeuvre available to all RPA. Therefore, all reference to flight termination in this document will typically be made with this flight termination manoeuvre in mind.
- A manoeuvre resembling an off-airport emergency landing may be performed at suitable flight termination sites, including bodies of water. This may minimise damage to the RPA while also preventing a breakup, thus limiting the crash footprint.
- Specific flight attitudes and manoeuvres, e.g. deep stall, spin or helicoidal descent, and RPA configurations may be employed to minimise the kinetic energy at impact and/or to maintain controllability and structural integrity of the RPA in a steep final descent.
- Technical means, e.g. airframe parachutes, may be employed to minimise the kinetic energy at impact or to enhance survivability of the RPA.

AS#30: Suitability of a location for flight termination is defined in a data base available aboard the RPA.

OR#12: Under C2 link loss, and if the RPA is incapable of flying to an emergency landing site and safely landing there, the A&ER function shall command flight termination at a suitable location.

2.3.5

Predictability Concept

Within the context of this document, predictability is understood as the absence of any behaviour unexpected by other actors in the airspace system, predominantly by ATC, but to a lesser extent also by surrounding air traffic.

Generally, predictability in the air traffic system is ensured by air traffic following ATC instructions, by pilots communicating situation and intention when unable to follow ATC instructions, and by pilots following commonly known and accepted rules, especially in case communication with ATC and surrounding air traffic is lost.

In manned aviation, predictability is ensured by an on-board pilot capable of ensuring the expected behaviour of the aircraft even in absence of ATC instructions. In an RPAS, the RP is unable to interact with the RPA if the C2 link is lost. Therefore, automatic functions need to ensure predictability in that case.

There are multiple layers aiming at ensuring predictability of RPAS operating within the air traffic system, taking account of the fact that the RP is not on board the RPA:

- As long as the C2 link is available, the RP is expected to control the RPA in a predictable manner, in the same way the pilot of a manned aircraft would do.
- With the C2 link lost, a number of measures are in place to maintain predictability of the RPA's behaviour:
 - The RPA follows pre-planned routes that are communicated to and agreed on with ATC as far as feasible, otherwise acts according to pre-defined and commonly accepted rules.
 - Specific transponder codes are used to make ATC aware of the link loss situation (7400)¹ and of emergency situations requiring deviation from the pre-planned route (7700). Temporary deviations from the pre-planned

¹ A specific transponder code for indicating link loss is presently being discussed between ICAO RPAS Panel and other stakeholders, with 7400 being the most likely candidate. However, there is no agreement yet.

and cleared trajectory, e.g. due to traffic or weather avoidance, would also be indicated with a specific transponder code (7700).

- The RPA uses every available and accepted means to communicate situation and intention to ATC and potentially to other airspace users. Those means may be intent reporting through ADS-B, non-voice ATC data links or blind voice transmissions.
- Even with the C2 uplink lost, the remote pilot can still contribute to predictability of the RPA behaviour by communicating to ATC the most probable intention of the RPA. This prediction may be based on knowledge of pre-planned behaviour of the RPA, on direct observation of RPA behaviour through a still available C2 downlink, on ATC forwarding their observations or other data sources available to the RP.

Under C2 link loss the predictability of the RPA's behaviour must be high enough for ATC and other airspace users to ensure safe operation. This requires tailoring of rules and procedures followed by manned aircraft and clear definitions of rules for automatic reactions.

Predictability of the RPA's behaviour during C2 link loss is limited by the incomplete knowledge of the RPA's status and situation. Differences between reality and assumptions made by RP and ATC will translate into behaviour deviating from expectations. This is not too different from what must be expected from a manned aircraft encountering communications loss. However, it is commonly assumed that the technically more complex – as compared to a voice communication system – data link and the lack of human insight on board the RPA make predictability more critical in an RPAS. Therefore, care must be taken to design procedures to be employed in case of link loss to be as robust as possible against uncertainties in properties used to define the RPA's behaviour.

Another limitation arises from the fact that predictability and efficiency are competing goals, at least to some extent. Procedures may be perfectly predictable but unacceptable from an operational point of view as they consume an undue amount of resources like airspace, RPA operation time, or ATC workload.

During C2 link loss, there are three main objectives driving the predictability concept: safety, no significant increase of ATC workload and minimize disturbance of other air traffic. The aim of high predictability is a consequence of the last two objectives. Therefore, as long as a safe flight can be ensured, the RPA should follow its clearly defined behaviour. However, when internal failures or external events imply that it is not safe to follow the pre-planned route, the RPA needs to deviate. The RPA should then communicate its intention with all available means. Nevertheless, it is inevitable that ATC workload will increase in these situations.

OR#13: Under C2 link loss, the RPA shall follow pre-planned routes as long as safely possible.

OR#14: The A&ER function shall be capable of managing the communication system of the RPAS.

OR#15: RPA behaviour due to a link loss must be as close as possible to the behaviour of a manned aircraft under a similar situation to ensure that the behaviour is transparent for ATC and other airspace users.

2.3.6

Fault Management Concept

The A&ER function is responsible for reacting to failures, warnings and abnormal situations. In highly automated manned aircraft, pilots are made aware of warnings through the Centralised Failure Detection and warnings System. They proceed to react in the most suitable way possible.

Due to the lack of a pilot in the cockpit of an RPA, there is a need for an automated reaction to a non-nominal status report, especially in the case of C2 link loss. This is where a distinction needs to be drawn between existing standards and the scope which falls within the A&ER parameter. ARINC 726-1 is a standard from 1981 that outlines a set of warnings which are flight and ATA chapter based. The ARINC 726 Flight Warning Computer System (FWCS) enables the crew to:

- Be aware of any failure or abnormal situation and its severity regarding aircraft and system control;
- Identify the failed system without ambiguity;
- Decide the appropriate corrective action without any risk of error.

Warnings generated by the FWCS are assigned a warning level for prioritisation between warnings. ARINC 726 defines the following warning levels:

- Level 3: Emergency
- Level 2: Abnormal
- Level 1: Advisory
- Level 0: Information

The following chain of events is foreseeable in order to mitigate and tackle a warning:

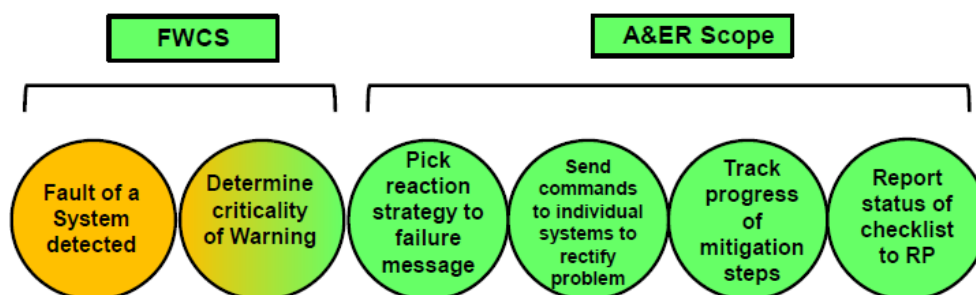


FIGURE 2.3: FAULT MANAGEMENT CHAIN FOR ERA

A portion of the determination of the criticality of a warning is within the A&ER scope, as there are warnings that will be generated by A&ER that have not been prioritized in terms of warning levels by the FWCS. Consequently, these warnings need to be assigned a level according to the levels defined in the FWCS standard. Automated response, including generation of proposals for actions and evaluation of RP responses to those proposals, and progress tracking of the steps taken, as seen in the figure above, are within the scope of A&ER. The progress will then be sent to the RP and the final state of this chain could trigger the start of this chain once again (in case of a failure to solve) or stop the chain if the problem has been solved.

OR#16: The A&ER function shall permanently monitor the RPA status and situation.

CHAPTER 3

OPERATIONAL SERVICES AND CAPABILITIES

The desired A&ER function will be an enabler for the integration of RPA into non-segregated airspace. The functional performance will be compliant with the existing aviation regulatory framework and it will provide levels of safety which are comparable or exceed those of manned aircraft.

3.1

MANNED AVIATION CAPABILITIES TO BE CONSIDERED FOR A&ER

For the A&ER function, the manned aviation capabilities which are within the scope of A&ER are of prime importance to this document. The reason for this lies in the fact that this document aims at harmonising the RPAS operations with manned aviation operations maintaining commonality as much as possible. These are described in this chapter. Naturally, there will be a delta between the two environments (manned and unmanned) and so a new set of capabilities, specific to the unmanned system, will be generated, which will be described in chapter 3.2. These could be simple modifications of manned capabilities, or completely new capabilities.

The capabilities for manned aviation which are seen to be in the scope of the A&ER function were identified as the following set. They are described for clarity. These will then be migrated to the unmanned aviation environment and any delta capabilities identified.

TABLE 3.1: MANNED AVIATION CAPABILITIES TO BE COVERED BY AN A&ER FUNCTION

Capability	Capability Description
The capability for the pilot to select routes on the FMS, and fly them, or utilise semi-automatic modes, to achieve a goal which can be a request from ATC or the pilots choice of where to fly.	The pilot must be able to execute the decision that he/she has made regarding where to fly. This can be carried out by a utilisation of semi-automatic modes (Altitude Hold and Acquire, Climb, Heading, etc.) or by coupling the modes to the FMS to achieve full 3-axis automatic behaviour.
The capability to utilise semi-automatic modes, or hand fly the aircraft back to the cleared flight plan route after a vectoring request.	During the course of a flight, the pilot will most likely have to pilot the aircraft to a location which is off the cleared flight plan. This can happen after a collision avoidance manoeuvre, vectoring, or for many other reasons. After this is complete, the pilot must be able to return the aircraft to the cleared flight plan.
The capability for the pilot to operate and manage the aircraft systems throughout the flight under Nominal Operations	During the normal course of a flight, the pilot is responsible for operating the on-board equipment. This can include operation of aircraft lights, extension of landing gear and changing of radio frequencies. Some of these actions assist in the operation of the aircraft, and some are mandatory.
The capability for the pilot to respond to abnormal events and alter the flight path of the aircraft, i.e. to enter the relight envelope after an engine failure, traffic avoidance, abnormal aircraft attitude recovery etc.	The pilot will have to respond to events which are not planned and can be considered abnormal, by altering the flightpath of the aircraft. This can be done by hand flying or utilisation of semi-automatic modes. The reasons for this can include collision avoidance, weather avoidance, engine failure, etc.

Capability	Capability Description
The capability to respond to failures of aircraft systems both in failure management, and strategic goal alteration (i.e. carrying out a forced landing/ditching)	When aircraft systems fail, the pilot must be able to assess the failure and decide a course of action. This course of action might only be operation of the affected system, operation of other systems or altering the strategic goal of the mission. The latter could refer to making an early diversion or emergency landing. It is foreseeable that a combination both is possible.
The capability to prioritise incoming requests from various aircraft systems	Various aircraft systems will prompt the pilot for actions, and it is possible that conflicting requests will require the pilot to assess, prioritise and execute the action of choice. An example would be a terrain avoidance request conflicting with a collision avoidance request.
The capability for the pilot to communicate with ATC and other aircraft	The pilot must be able to communicate with ATC to receive instructions for vectoring, clearances, communication actions and status reporting.
The capability for the pilot to be aware of the situational status of the aircraft	For the pilot to operate the aircraft effectively, he/she must be aware of the status of the aircraft, including position, vector and aircraft systems health together with other air traffic, weather, terrain, changes to airfield availability, or navigational services provided to the aircraft.
The capability for the pilot to carry out checklist duties	During flight phase changes, the aircraft must be configured accordingly. Checklist of this configuration change is mandatory under normal operations. Under abnormal operations, i.e. a system failure like an engine abnormality, the pilot will carry out checklisting of the procedures applicable to the abnormal event.

3.2

A&ER CAPABILITIES WITH ALL COMMUNICATIONS LINKS FUNCTIONING

The A&ER function's main purpose is to assist the RP in the decision making process e.g. in cases of immediate action required where the RP cannot provide this due to data link delay, and to assist the RP to carry out certain tasks to reduce workload (checklists etc.). The overall operation of the A&ER capability shall be deterministic and comply with pre-defined rules, whose safety will be demonstrated through a safety assessment. When the C2 link is operational, the RP shall govern the operation of the RPA. The A&ER capability will provide assistance by making an action proposal to the RP to resolve the condition at hand, in case no RP intervention occurs the proposed action will, under certain situations, be executed after a delay, or in situations that are considered "time critical" (i.e. rejected take-off), immediately. In addition, the automation of recurring tasks will be considered to reduce RP work load.

3.2.1

Justification of changes

In manned aviation it is the task of the pilot to perform certain sequences of actions at certain points in time during the flight or when certain events occur. The sequences of actions are usually defined in corresponding checklists.

- Because there is no pilot sitting in an RPA, the management and switching of RPA systems and equipment must necessarily be performed remotely by the RP sitting at the RPS, and sending commands to the RPA via the C2 link.
- Nevertheless, the inherent delays introduced by the C2 link chain (in the order of seconds/minutes) might jeopardize the prompt execution of time critical actions, e.g. the reaction to sudden failures or external events like conflicting air traffic requiring an immediate avoidance manoeuvre, or a take-off abort.

Therefore in an RPA it is necessary to perform these actions automatically.

As a beneficial side effect the automation layer relieves the pilot from the performance of routine tasks and supports him in high workload situations, e.g. during an emergency.

3.2.2 Capability changes

The adaptation of the capabilities to RPAS must ensure that the RPA behaviour stays predictable to ATC and the RP at all times. In addition it has to be ensured that even under first failure conditions a Continued Safe Flight and Landing is still guaranteed.

Looking at the set of manned aviation capabilities, these will have to be altered for unmanned aviation. In addition, entirely new capabilities will have to be introduced. Both of these sets will be described below.

The capabilities have been split into three sections; Maintained Capabilities (where the capability is essentially the same in unmanned aviation as it is in manned aviation, aside from some minor wording changes), Altered Capabilities (where the capability is altered from manned aviation to unmanned aviation due to the change of system or environment) and Delta Capabilities (where the capability is completely new and only present in unmanned aviation).

The philosophy followed for these capabilities was the following:

- Capabilities that generate a proposal
- Capabilities that figure out what to do with that proposal
- Capabilities that are needed in support of the first two categories in unmanned aviation

This philosophy was followed as far as possible, but it should be remembered that capabilities are typically very high level and generalised.

3.2.2.1 Maintained Capabilities

The following capabilities were seen as equivalent for manned and unmanned aviation, aside from minor wording differences as outlined in the table:

TABLE 3.2: MANNED / UNMANNED CAPABILITIES

Manned Capabilities	Unmanned Capabilities
The capability to utilise semi-automatic modes, or hand fly the aircraft back to the cleared flight plan route after a vectoring request.	The capability to return the RPA to its predetermined route
The capability for the pilot to operate and manage the aircraft systems throughout the flight under Nominal Operations	The capability to manage the RPA systems under nominal conditions based on aircraft state
The capability for the pilot to respond to abnormal events and alter the flight path of the aircraft, i.e. to enter the relight envelope after an engine failure, traffic avoidance, abnormal aircraft attitude recovery etc.	The capability to change the RPA's flight path based on assessment of abnormal events. NOTE: <i>Recovery from abnormal attitudes is expected to be a FGS / FCS capability and is therefore out of scope for the A&ER function.</i>