Project no.: 314680 (Call: FP7-AAT-2012-RTD-1)

ULTRA
Unmanned Aerial Systems in European Airspace

Thematic Priority:	AAT.2012.7-25. Assessment of the potential insertion of unmanned aerial system in the air transport system
Instrument:	Coordination and Support Actions (CSA)

Safety aspects of civil RPAS operations

Due date of deliverable: **31/03/2013** **Actual submission** **30/08/2013**

Start date of project: **01/06/2012** **Project duration:** **18 months**

Leader organisation of this deliverable: NLR **Revision status: Final**

Approval status		
Author	**Verification Authority**	**Project Approval**
NLR	NLR	INDRA
Lennaert Speijker	Henk Hesselink	Daniel Cobo-Vuilleumier
ULTRA WP3.1 Leader	ULTRA WP3 Manager	ULTRA Coordinator (TPC)
29 August 2013	30 August 2013	30 August 2013

Project co-funded by the European Commission within the Seventh Framework Programme (2007-

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Contributing partners	
Company	**Name**
NLR	Lennaert Speijker
A2TEC	Jarno Puff
ONERA	Claude Le Tallec
BRTE	David Esteban Campillo, Vera Gimeno

Distribution list			
Company	**Name**	**Company**	**Name**
European Commission	Pablo Pérez-Illana	NLR	Alex Rutten
INDRA	Daniel Cobo-Vuilleumier	Studio Legale AST	Anna Masutti
NLR	Henk Hesselink	Cranfield Aerospace	Gordon Dickman
NLR	Jan Floris Boer	Cranfield Aerospace	Robert Jones
NLR	Lennaert Speijker	Integra	Gilles Fartek
A2TEC	Jarno Puff	Integra	Christian Scheel Struwe
ONERA	Claude le Tallec	BRTE	David Esteban Campillo
Studio Legale AST	Alfredo Roma	BRTE	Vera Gimeno

Document Change Log				
Revision	**Edition Date**	**Author**	**Modified Sections / Pages**	**Comments**
1.0	30/08/2013	Lennaert Speijker et al.	All	First approved version

Table of Contents

List of Figures

List of Tables

1. INTRODUCTION

1.1. Project Objective

The overall objectives of the ULTRA project are:

- To provide a comprehensive set of recommendations for the incremental insertion of civil Light RPAS (RPA with operating mass up to 150 Kg) in the European airspace in the short-term (i.e. within 5 years from now)
- To provide specific recommendations for selected “Use Cases” to be explored as “quick win” business cases.
- Highlight what needs to be done in order to unlock the full potential of the civil Light RPAS market in the long-term (i.e. 10-15 years from now)

These overall objectives are further divided into the following technical objectives in order to address the European Commission expectations for this project:

- Current RPAS status:

  Analyze current and past work relative to civil RPAS, including existing best practices – regulatory authorities and qualified entities (certification & operations), commercial (manufacturers & RPAS operators) and non-commercial (research, scientific, governmental non-military) –, and propose a starting point for Light RPAS operations in the short term.

- Realistic business model and short term, applications:

  Develop a business model for civil Light RPAS applications. Explore short-term, high value applications, and analyze their sustainability and level of impact on European industry and society.

- Social acceptance and building trust with the regulators:

  Perform an in-depth analysis on how to overcome the barriers and mistrust of (Light) RPAS by the general public. Follow a step-by-step approach to build trust between the (Light) RPAS industry and the regulators.

- Foster innovation in and support SMEs access to market:

  Foster the European innovation in terms of aviation automation and provide a path which facilitates access to market for European SMEs.

- Set of Recommendations:

  Develop recommendations to support a sustainable civil Light RPAS market in the short-term and highlights the steps needed in order to unlock the full potential of the (Light) RPAS market in the long-term.

1.2. Background

The ULTRA project is an 18-month duration "*Coordination and Support Action (CSA)*" funded under the call *FP7-AAT-2012-RTD-1* of the *Transport* (including "Aeronautics") Cooperation Theme of the European Commission (EC) 7th Framework Programme (FP7) to address the activity: *AAT.2012.7-25. Assessment of the potential insertion of unmanned aerial system in the air transport system*, for which the following content, scope and expected impact were established by the EC:

Content and scope: *The study should establish the minimum requirements in terms of standards equipments and regulations to allow the safe insertion of UAS in the civil airspace. It should also anticipate the steps required for the certification and the validation of the insertion. In the light of this, the path to exploitation will be investigated: market trends, adaptation of infrastructures and investments, obstacles to social acceptance. The consortium should gather a representative group of stakeholders including among others manufacturers, regulators, air navigation service providers, and customers*.

Expected impact: *Proposals should demonstrate contributing to analyse and assess the innovation steps needed to allow the insertion of Unmanned Aerial Systems (UAS) for civil application in the air transport system*.

To address these requirements, with the focus on Light RPAS, the ULTRA Consortium defined the project objectives indicated in section **¡Error! No se encuentra el origen de la referencia.**, and organized the work in the following work packages:

- WP1 – *Regulatory and Certification Base*
    - Identification of gaps and new/modified regulations within the existing regulatory framework
    - Proposed set of actions to fill the gaps in the existing regulatory framework
- WP2 – *Adaptation of Infrastructures*
    - State-of-the-art report of civil RPAS solutions and enabling technologies
    - Time-phased alternative solutions for all equipment and infrastructure enablers
- WP3 – *Safety and Social Acceptance*
    - Safety aspects of civil (Light) RPAS operations
    - The social dimension of civil (Light) RPAS operations
    - Impact of (Light) RPAS (on society)
- WP4 – Business Case and Impact on European Industry
    - Most relevant use cases for civil (Light) RPAS in Europe in the 2013-2014 timeframe
    - Civil (Light) RPAS applications in Europe: Deployment plan and economic sustainability of the business case
- WP5 – Conclusions and Recommendations
    - Project Final Report
    - Dissemination activities and material, and project website
- WP6 – Coordination

As indicated in the “project objectives” (section **¡Error! No se encuentra el origen de la referencia.**), one of the main objectives is *to provide specific recommendations for selected “Use Cases” to be explored as “quick win” business cases*. Therefore, the work developed by the different work-packages will feed into the “selected use cases” in order to provide specific recommendations for them from the different key aspects addressed in the project, and support the development of the corresponding business cases. This work logic is depicted in Figure 1.

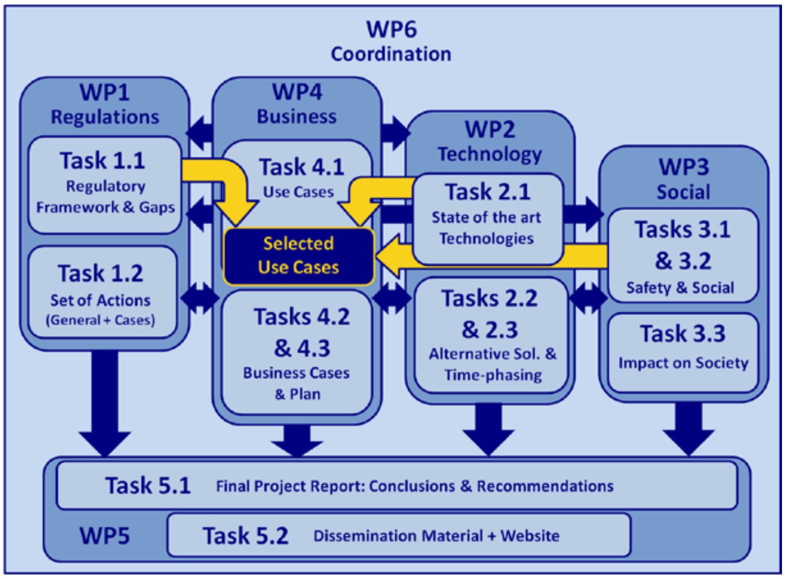

Figure 1 ULTRA work logic

The project started in June 2012 and its duration is 18 months. The ULTRA Consortium gathers a representative group of stakeholders including large and small organizations, as illustrated in Figure 2.

Figure 2 ULTRA consortium

It is worth noting that the ULTRA Consortium has been participating in the **European RPAS Study Group (ERSG)** of the European Commission (see ULTRA D1.1 [58]).

1.3. Purpose of the Document

The main objectives of this study are:

- To identify the main safety aspects,
- To provide suggestions for assessing the safety of RPAS operations,
- To provide suggestions for the (further) development of mitigating measures.

1.4. Document Structure

The document is structured as follows:

1. Introduction, which provides a description of the document purpose and indicates the references and acronyms list used throughout this document;
2. Expected RPAS operations, which details the envisaged generic application(s) (the different expected operations of RPAS in non-segregated airspace) associated with the ULTRA Use Cases;
3. Risks to be regulated, which discusses the development of a risk criteria framework, including risks to be regulated, the suitability of risk metrics, and the setting of an acceptable safety level;
4. Safety assessment methods, which summarizes different Safety Risk Management methods for assessing safety of operations with Unmanned Aircraft Systems in non-segregated airspace;
5. Building a safety case, which explains how the results of a Safety Risk Management process may be used to build a safety case for RPAS operations in non-segregated airspace;
6. Risk mitigating measures, which provides guidelines for the elimination or mitigation of identified hazards related to RPAS operations in non-segregated airspace to an acceptable or tolerable level;
7. Conclusions and recommendations.

1.5. Applicable and Reference Documents

R.1 Grant Agreement (Contract) ref. ACS2-GA-2012-314680-ULTRA (Grant Agreement no. 314680). 7th Framework Programme. Coordination and Support Action. European Commission DG-Research & Innovation. June, 2012.
R.2 ULTRA Annex I of the Grant Agreement (no. 314680) – Description of Work (DoW), 15/05/2012.
R.3 ICAO; Convention on International Civil Aviation.
R.4 ICAO; Unmanned Aircraft Systems (RPAS), Circular 328-AN/190, ISBN 978-92-9231-751-5, 2011.
R.5 ICAO; Manual on Airspace Planning Methodology for the Determination of Separation Minima, Doc 9689 AN/953.
R.6 ICAO; Safety Management Manual (SMM), Doc 9859, AN/474, Second Edition, 2009.
R.7 EUROCONTROL Safety Regulation Commission (SRC); ESARR 3 – Use of safety management systems by ATM service providers, Edition 1.0, 17-07-2000.
R.8 EUROCONTROL Safety Regulation Commission (SRC); ESARR4 – Risk assessment and mitigation in ATM'.
R.9 EASA; Policy for Unmanned Aerial Vehicle (RPAS) certification; EASA Advance Notice of Proposed Amendment (A-NPA) No 16/2005.

R.10 EASA; Airworthiness Certification of Unmanned Aircraft Systems (RPAS), Policy Statement E.Y01301, 2009.
R.11 EASA; Airworthiness aspects of RPAS – Preliminary Regulatory Impact Assessment, MDM.030, TE.RMP.00037-002, Version 1.0, 06-12-2010.
R.12 EUROCONTROL; Safety Case Development Manual, Edition 2.1, October 2006.
R.13 JAA/EUROCONTROL RPAS Task Force; A Concept for European Regulations for civil Unmanned Aerial Vehicles (RPAS), Final Report, 2004.
R.14 SAE; Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, ARP 4761, 1996.
R.15 A.D. Ozuncer, L.J.P. Speijker, J.A.A.M. Stoop, R. Curran; Development of a safety assessment methodology for the risk of collision of a Unmanned Aircraft System with the ground, NLR-TP-2011-325, August 2011 (published by SAE in Journal of Aerospace, Vol.4, No.2, November 2011)
R.16 L.J.P. Speijker, X. Lee, R. van de Leijgraaf; Framework for Unmanned Aircraft System Safety Risk Management, NLR-TP-2011-326, August 2011 (published by SAE in Journal of Aerospace, Vol.4, No.2, November 2011).
R.17 B. Ale, L.J. Bellamy, R.M. Cooke, M. Duyvis, D. Kurowicka, P.H. Lin, O. Morales, A. Roelen, J. Spouge; Causal model for air transport safety - Final Report, 2009.
R.18 European Commission; Hearing on light Unmanned Aircraft Systems (RPAS), TREN F2/LT/GF/gc D(2009), Brussels, 8 October 2009
R.19 European Commission; Conclusions of the first European High Level Conference on Unmanned Aircraft Systems Brussels, 1st July 2010
R.20 European Commission; Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS), SWD(2012) 259 final, Brussels, 04-09-2012
R.21 European RPAS Steering Group; Roadmap for Complementary Measures on RPAS, 18 December 2012
R.22 European Commission; Regulation EC No. 785/2004 covering the liability of the operator for passenger, baggage, cargo and third parties.
R.23 ICAO; ADREP 2000 taxonomy, as implemented in ECCAIRS 428, 17 September 2010
R.24 H. de Jong (DFS), R. Priego Lopez (ISDEFE), Scope of risks and safety criteria, INOUI D5.0b, Version 2.0, 27 March 2009.
R.25 D. Durrett, H. de Jong (DFS), J. Tattersall (Rheinmetall); Functional Hazard Analysis, INOUI D5.2, 29 June 2009.
R.26 M. Lemoine (ONERA), C. Montes(BR&TE), C. Martinez, J. Bueno (ISDEFE), H. de Jong (DFS); Towards safety requirements for the integration of UAS, INOUI D5.3, 15 December 2009.
R.27 J. Bueno, C. Martinez (ISDEFE); Aerodrome safety analysis, INOUI D5.4, 15 December 2009.
R.28 EUROCONTROL; Safety Assessment Methodology (SAM), Edition 2.1
R.29 A. Clough, M. Ainley, S. Hunt; Preliminary Impact Assessment on the safety of communications for UAS, Volume 1 (Study Report) and 2 (Annexes), EASA.2008.OP.08, 8 December 2009, Issue 1.0.
R.30 EUROCONTROL; Unmanned Aircraft Systems - ATM Collision Avoidance Requirements (Phase 1), Edition 1.2, 14 December 2009, CND/CoE/CNS/09-156.
R.31 EUROCAE ED-78A (equivalent to RTCA/DO-264); Guidelines for approval of the provision and use of ATS supported by data communications.
R.32 UK Defence Standard 00-56, Safety management requirements for Defence Systems, 1996.
R.33 European Operational Concept Validation Methodology (E-OCVM), Version 3.0, March 2010.
R.34 M.A. Piers, M.P. Loog, M.K.H. Giesberts, G. Moek, M.J.H. Couwenberg and M.C.J. Smeets; The development of a method for the analysis of societal and individual risk due to aircraft accidents in the vicinity of airports, NLR CR 93372 L.

R.35 A.J. Pikaar, C.J.M. de Jong, J. Weijts; An enhanced method for the calculation of third party risk around large airports – with application to Schiphol, NLR-CR-2000-147.
R.36 M.A. Piers, B.J.M. Ale; Policy options for dealing with societal risk around Schiphol, NLR-CR-2000-084.
R.37 A.D. Balk, Analysis of U.S. General Aviation Accident Rates, National Aerospace Laboratory, NLR-TR-2011-236.
R.38 A. Oztekin, R. Wever; Development of a regulatory safety baseline for UAS Sense and Avoid, FAA and National Aerospace Laboratory, NLR-TP-2012-439.
R.39 J. Verstraeten, M. Stuip, T. van Birgelen; Assessment of Detect and Avoid solutions for use of Unmanned Aircraft Systems in Non-segregated Airspace, National Aerospace Laboratory, NLR-TP-2012-494.
R.40 J.G. Verstraeten, R. Wever, L.J.P. Speijker; Risk analysis of command and control in commercial air transport: Baseline for data-link related hazards for Unmanned Aircraft Systems, National Aerospace Laboratory, NLR-CR-2011-439
R.41 M. Masson, Y. Morier; Methodology to assess future risks, EASp EME 1.1 Deliverable, 11-12-2012
R.42 B.E. Smith, R. den Hertog, M. Kavoliunas, A. Marosvari, C. Bieder, J.P. Magny, A. Roelen; Phase 1 Report (Rev. 3) on Task EME1.1, Methodology to Assess Future Risks From the Emerging Issues Section of the European Aviation Safety Plan, 30 January 2012.
R.43 M.H.C. Everdij; H.A.P. Blom (editors); Safety Methods Database, Version 1.0, 4 March 2013, NLR
R.44 Future Aviation Safety Team (FAST); The FAST approach to discovering aviation futures and associated hazards, 03-12-2008.
R.45 D. Esteban, J. Puff, H. Hesselink, C. le Tallec, A. Ubeda; Most relevant user cases for civil UAS in the European Airspace in the 2013 – 2014 timeframe, ULTRA D4.1, 4 February 2013.
R.46 R.E. Weibel, R. John Hansman; Safety considerations for operation of unmanned aerial vehicles in the National Airspace System, Report No. ICAT-2005-1, March 2005.
R.47 Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, with supporting Annex 1 “A Regulatory Approach for the integration of civil RPAS into the European Aviation System”, Annex 2 “A Strategic R&D Plan for the integration of civil RPAS into the European Aviation System”, and Annex 3 “A study on the societal impact of the integration of civil RPAS into the European Aviation System”, June 2013
R.48 EC Regulation No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (amended by Commission Regulation (EC) No 690/2009 and No 1108/2009).
R.49 DEVA1206042A. *Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent* (Decree dated 11 April 2012 concerning the design of civil aircraft which fly without anyone on board, their conditions of use, and the skills required of their users)
R.50 List of French RPAS approved operators: http://www.developpement-durable.gouv.fr/ Demarches-pour-effectuer-des.html (retrieved 07/05/2013).
R.51 N.A. Sabatini, FAA Associate Administrator for Aviation Safety; Statement before the House Committee on Transportation and Infrastructure, Subcommittee on Aviation on UAS Activities, 29 March 2006.
R.52 NATO; UAV Systems Airworthiness Requirements (USAR), STANAG 4671, 2007.
R.53 EASA CS-25; Certification Specifications for Large Aeroplanes.
R.54 FAA/EUROCONTROL Action Plan 15 “Safety”; ATM Safety Techniques and Toolbox, Version 1.0.
R.55 GAIN; Guide to Methods & Tools for Airline Flight Safety Analysis, Second Edition, June 2003.
R.56 FAA; Sense and Avoid (SAA) for UAS Second Caucus Workshop Report, January 18, 2013

R.57 CAA UK; Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases: For Aerodrome Operators and Air Traffic Service Providers, CAP 760, 2010.

R.58 ULTRA Deliverable D1.1 – Identification of gaps and new/modified regulations within the existing regulatory framework. ULTRA Consortium. V2.0. 16/01/2013.

1.6 Glossary

AC	Advisory Circular
ADS-B	Automatic Dependent Surveillance Broadcast
AGL	Above Ground Level
ADREP	Accident/Incident Data Reporting
AIP	Aeronautical Information Publication
ALARP	As Low As Reasonably Practicable
AMC	Acceptable Means of Compliance
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ARP	Aerospace Recommended Practice
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATO	Air Traffic Organization
ATSI	Air Transport Safety Institute
AOC	Air Operator Certificate
B-RLOS	Beyond Radio Line Of Sight
B-VLOS	Beyond Visual Line Of Sight
CAA	Civil Aviation Authorities
CATS	Causal model for Air Transport Safety
CBP	Customs and Border Protection
CCE	Catastrophic Collision Event
CS	Certification Specification
DGAC	Direction Générale de l'Aviation Civile
EASA	European Aviation Safety Agency
EC	European Commission
ECCAIRS	European Coordination Centre for Accident/Incident Reporting System
E-OCVM	European Operational Concept Validation Methodology
ESARR	EUROCONTROL Safety Regulatory Requirement
ESD	Event Sequence Diagram
EU	European Union
EUROCAE	Europe Organization Civil Aviation Equipment
EUROCONTROL	European Organization for the Safety of Air Navigation
E-VLOS	Extended Visual Line Of Sight
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FH	Flight Hour
FHA	Functional Hazard Assessment

FL	Flight Level
FMEA	Failure Mode and Effects Analysis
FOV	Field of View
FT	Fault Tree
GA	General Aviation
GPS	Global Positioning System
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HEMS	Helicopter Medical Emergency Service
HMI	Human Machine Interface
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
JAR	Joint Aviation Requirements
JARUS	Joint Authorities for Rulemaking on RPAS
MAC	Mid Air Collision
MFD	Multi Function Display
MSL	Mean Sea Level
MTOM	Maximum Take Off Mass
MTOW	Maximum Take Off Weight
NAA	National Aviation Authority
NATO	North Atlantic Treaty Organization
NAS	National Aviation System
NextGen	Next Generation Air Transportation System
NOTAM	NOTice to AirMen
PSSA	Preliminary System Safety Assessment
R&D	Research and Development
RLOS	Radio Line Of Sight
RPAS	Remotely Piloted Aircraft System
RPS	Remote Pilot Station
RR	Risk Ratio
RTCA	Radio Technical Commission for Aeronautics
RVSM	Reduced Vertical Separation Minima
SAA	Sense And Avoid
SAC	Scheduled Air Carrier
SAE	Society of Automotive Engineers
SAM	Safety Assessment Methodology
SAR	Search And Rescue
SARP	Standards and Recommended Practices
SES	Single European Sky
SESAR	Single European Sky ATM Research
SMS	Safety Management System
SRM	Safety Risk Management
SSA	System Safety Assessment
STANAG	Standardization Agreement
SWIM	System Wide Information Management

TLS	Target Level of Safety
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
ULTRA	Unmanned Aerial Systems in European Airspace
UMTS	Universal Mobile Telecommunications System
UK	United Kingdom
VOL	Value Of Life
VLL	Very Low Level
VLOS	Visual Line Of Sight
VMC	Visual Meteorological Conditions
VFR	Visual Flight Rules
VWP	Value Willing to Pay

1.7. Definitions

In June 2013, the European RPAS Steering Group has produced definitions in its roadmap [47] that are of interest for the scope of this study, because they are related to the defined ULTRA use cases [45]. Very Low Level (VLL) operations (alias non-standard VFR or IFR operations) below the typical IFR and VFR altitudes for manned aviation, i.e. not to exceed 500 feet above ground level that comprise:

- Visual Line of Sight (VLOS) in a range depending on the aircraft visibility, but typically not greater than 500 meters from the remote pilot, in which the remote pilot maintains direct unaided visual contact with the remotely piloted aircraft;
- Extended Visual Line of Sight (E-VLOS) where the pilot is supported by one or more observers and in which the crew maintains direct unaided visual contact with the remotely piloted aircraft[1];
- Beyond VLOS (B-VLOS) where the operations are still below 500 ft., but beyond visual line of sight, hence requiring additional technological support.

2. EXPECTED RPAS OPERATIONS

2.1. Introduction

The purpose of this section is to describe the envisaged generic application(s) (the different expected operations of RPAS in non-segregated airspace) in support of the construction of a safety assessment and safety case. User cases have been developed for the expected operations as part of work package 4 of the ULTRA project on the basis of the following characteristics [45]:

- RPAS mode of operation
- Duration of the RPAS operation
- Physical characteristics of the RPAS
- RPAS flight performance
- Other airspace users
- Weather restrictions
- Command and control characteristics
- Detect and avoid capabilities
- Communication, navigation and surveillance
- Airspace classifications
- Flight rules
- Populated areas
- Pilot/operator qualifications
- ATM requirements
- Fail safe
- Flight termination

The ECCAIRS 4 list of aviation operations are based on ICAO´s ADREP2000 taxonomy [23]. They have been organised at different hierarchical levels. An operation type can be defined at each desired level.

- Operation Code “3000000” identifies ‘Aerial Work’: *An aircraft operation in which an aircraft is used for specialized services such as agriculture, construction, photography, surveying, observation and patrol, search and rescue, aerial advertisement, etc. Annex 6 Part1, Chapter 1.H9.*
- Operation Code “3010000” identifies the sub-level “Commercial”: *An aerial work flight carried out for remuneration or reward.*
- Operation Code “3020000” identifies the sub-level “Non-Commercial”: *An aerial work operation not for remuneration or reward.*

From each *Commercial Operations (3010000)* category/level, one specific business case example is extrapolated, which will reflect the same common aspects of the entire given category/level. We have associated to this category/level the most common (or most relevant) flight operation modes: Visual Line Of Sight (VLOS), Extended Visual Line Of Sight (EVLOS), Beyond Line Of Sight (BLOS), and integration into ‘non-segregated’ airspace. The variable “populated area” will have an impact on the determination of the level of reliability and safety required for the RPAS in order to operate over a specific area. The VLOS business case descripted could be performed today, where UAS operations are allowed, with the given legislation and freely available frequency spectrums. The E-VLOS business case is more difficult, while the BLOS business case is the most critical and complex and can not be performed today with the given legislation and freely available frequency spectrums. The *Non Commercial Operations (3020000)* category may be considered social acceptance related and may be easier related to commercial operations to get permissions to be performed today with the given legislation and available frequency spectrums.

2.2. Use case 1: Aerial photography

VLOS Flight Mode (short-term solution):
3011100 Photography: hydroelectric power plant inspection; biomass combustion plant inspection; photovoltaic power plant inspection; building insulation inspection; gas imaging and leaks detection for petrochemical, pharmaceutical and industrial plants; concrete structure assessment and inspection (dam, bridge, chimney, cooling tower, nuclear plant, …); flare tip inspection; wind farm inspection; real estate; filming and media; post-disaster damage assessment and insurance estimation.

Introduction: The commercial operation “filming & media”, better know commonly as “aerial photography”will reflect the common operational aspects of category “3011100 Photography” for the short-term solution VLOS Flight Mode. As mentioned In several EU countries UAS regulations/drafts, VLOS is defined as an “operational volume” of 500 m in radius and 400 feet in altitude. Therefore, the most suitable platform is based on rotary wings with vertical take-off and landing, hover and slow motion capabilities. Rotary wing platforms can be used in every operational scenario: urban, sub-urban and extra urban environments. Today, the most used platforms are based on multirotors due to its easy piloting capabilities (totally electronically stabilized), autopilot features (waypoint flying, come home, autoland, altitude hold, position hold, …) and cost effective construction methods (no complex moveable rotor mechanics). A Maximum Takeoff Weight (MTOW) of up to 20-25 kg will be the most interesting one, in case no airworthiness certification will be required for this weight class, because this results in less expensive RPAS solutions available on the market

Scenario Description: The operational scenarios of Multirotors and helicopters are based on the real time, electronic stabilization assisted, flight mode in the Class G airspace. The pilot will always have unaided line of sight contact to the platform and will operate under Visual Meterological Conditions (VMC). The pilot is responsible for obstacle avoidance on his flight path, such as trees, buldings, objects and people, following the Visual Flight Rules (VFR). However, it will be very difficult for the pilot to estimate the attitude and physical position of the aircraft related to the objects, due the lack of a correct perception of depth on longer distances.

Radius of Action: The maximum distance that the RPAS can travel away from its pilot station without losing unaided line of sight contact, allowing for all safety and operating factors. The effective radius of action of the aircraft depends on its size, shape,colors and metereological conditions, and may vary from few dozens of meters up to over standard VLOS limitations of 500 m. Radius of action limitations should be descripted in the aircraft flight manual.

Endurance: Flight duration is given by the battery or fuel capacity. For filming and media operations, electric driven, fiber carbon structure based systems are preferable because of low weight, low vibration and low noise generation as compared to fuel based systems. System size ranges from 800 mm to 1100 mm in shaft to shaft diameter for multirotors, and 1000 mm to 2000 mm in rotor diameter for helicopters. Average flight time is between 5 to 20 minutes per battery pack, depending on meteorological conditions and payload capacity installed. Talking to pilots, they claim to usually need a short break after about 10 to 20 minutes flight, because, depending on the level of automation of the system, VLOS flights may be quite stressfull. Flight performance is very different for multirotors and helicopters. Multirotors have an average maximum forward speed of 50 km/h, helicopters can fly at over 150 km/h. This results in using multirotors mainly for hover and stare operations, helicopters more for high dynamic movie pictures, e.g. following a running vehicle or skirider. Regarding payload capacity, multirotors with a MTOW of up to 10-12 kg may handle payloads of 3 to 5 kg, helicopters with a MTOW of up to 20-25 kg payloads of up to 10 kg, using electric driven systems.

Other airspace users: Below 400 feet, usually no other airspace users are present, but other RPAS, military, state flights and emergency helicopter flights could show up sometimes. Powered motorglider, glider and micro light aircraft or powered aircraft practising engine failure exercises could also show up.

Safety Enhancements: An on-board pilot camera with an on-screen display showing critical flight information data, such as roll, pitch, heading, distance from pilot position and battery/fuel status can increase situational awareness of the pilot. Depending on the type of command and control interface, the pilot can wear a monocle display or use a small monitor mounted on the control station. The most used and familiar control device for VLOS are model handheld radio controllers with an operational temperature range of 0-50° degrees Celcius. Radio Controller model based systems are not made for minus degree operations or rain and snow operation. For this kind of operations, like First Responders, an industrial grade RPS system would be required. Flight timers function with alarm are one of the most important safety features of handheld controllers. Based on the battery capacity, the pilot set the flight timer, calculating 25% of spare. In case of an unexpected voltage drop on the battery pack, an automatic voltage threshold monitoring system on-board the aircraft should initiate a ‘fail safe mode’, enabling to come back to the take-off area in an automatic way, or land immediately. In case of total battery failure or power outage, a ballistic parachute flight termination system should be deployed, if present on board. Link-loss fail safe features should be in place. In case of radio link loss or disturbance this should e.g. allow a safe landing at either a specific nearby located destination or the departure location,. Radius of action limitations should be configured in the autopilot to assure performance limitations are kept up and running. Multirotor and helicopters can be well used in urban environments, but particular attention must be given to the population on the ground. In case of urban operations, the ground area below the flight path should be segregated if:

- no proper flight termination system is present
- flying altitude is not sufficient to deploy the parachute safely
- people on ground are not direct related to the film set or RPAS flight crew

If operation over populated areas is requested, a qualified flight termination system (e.g. ballistic parachute) should be mandatory to ensure safety on ground.

An external observer may be used to increase situational awareness on 360° around the flight crew to help the pilot to look around in order to identify potential incoming hazards, as the latter is in charge to safely fly the aircraft. The external observer should wear an aeronautical radio for ground to air communication between the RPAS flight crew and other airspace users and a link between the observer and the pilot should also be added as part of the RPAS, independently from aeronautical communications to other airspace users.

Note: In case of urban operations, GPS assisted fail safe functions, can show reduced function and reliability issues. Flight crew should check the aircraft behavior to determine correct functioning of GPS related fail safe modes, activating manually the fail safe mode to see if home position and related safety configured parameters are working as expected.

2.3. Use Case 2: Wind farm inspection

EVLOS Flight Mode: **3011100 Photography**: concrete structure assessment and inspection (bridge); **wind farm inspection**; shark spotting and beach safety

Other commercial operations associated to the EVLOS Flight Mode.

- 3010400 Aerial survey: fish & wildlife survey; mining exploration & mapping; civil & environmental engineering; terrain mapping; pollution detection; forestry management
- 3010500 Agricultural: precision agriculture; spraying

Introduction: The commercial operation “wind farm inspection” will reflect the common operational aspects for the mid-term solution EVLOS Flight Mode. EVLOS is not well defined yet, but is simply an extension of range of VLOS. The EVLOS related business has its potential in the extra urban environments, where no or very small population and buildings per square km are present. Wind farm inspections will e.g. have big advantages from the EVLOS flight mode because a flight crew can stay on a fixed ground position and hop from one windmill tower to the next without losing precious time in moving the RPAS ground station. The operational area is about few square km at the time. To perform this kind of operation, more sofisticated gasoline driven industrial grade helicopter platforms are required. Electric driven systems do not have enough endurance to perform this kind of structural inspections.

Scenario Description: EVLOS operational scenarios, e.g. for wind farm inspection, are based on the real time, electronic stabilization assisted, flight mode in the G-Class airspace. The pilot will guide the aircraft using a cockpit style RPS through a video monitor and under Visual Meterological Conditions (VMC). The pilot is responsible for obstacle avoidance on his flight path, such trees, buildings, objects and ppopulation, following the Visual Flight Rules (VFR). The most used and familiar RPS for EVLOS are portable desktop based military cases, installed in vans or trucks, featuring flight control devices, keyboard and a monitor with on screen display showing critical flight information data, such as roll, pitch, heading, distance from pilot position and battery/fuel status. The operational temperature range is usually - 20 until 50°C.

Radius of Action: The maximum distance that the RPAS can travel away from its pilot station without losing direct line of radio sight contact, allowing for all safety and operating factors. Radius of action distance is directly dependent on the operational area of interest. RPAS operators and research institutesin different countries showed a useful distance of few km in radius, an altitude of 400 feet AGL could be acceptable enough to perform broad range of operations. Fixed wing and helicopters are the most suitabled platforms, depending on the requested flight performances on a specific operation. Fixed Wing platforms are focused on large area aerial surveys, where speed and high automation is requested, helicopters instead are focused on large structural inspections, such as bridges and wind turbine farms, where slow and hover capabilities are the focal capabilities

Endurance: The endurance at the radius of action is an important parameter that defines the coverage of the aircraft for a given mission. This parameter is defined based on the mission duration that operators can achieve keeping the aircraft airborne without landing. Safety is directly related to a proper and carefully calculated endurance time. Flight duration is given by the fuel capacity. Average flight time is between 30-90 min per fuel tank, depending on meterological conditions and payload capacity installed.. Flight performance are based on the size and power of the system. Average industrial helicopters dimensions range from 2.0 m up to 3.4 m with MTOM of 15 kg to 150 kg.

Other airspace users: Usually, below 400 feet, no other airspace users are present, but other RPAS, military, state flights and emergency helicopter flights could show up sometimes. Powered motorglider, glider and micro light aircraft or powered aircraft practising engine failure exercises could also show up. Inside wind farms this will not the case as the wind towers form structural obstacles, so the environment can be defined clear and safe from other airspace users. An external observer may be used ().

Safety Enhancements: EVLOS flight operations should be conducted from an environmentally closed command and control place to avoid external distractions. The pilot has to constantly observe real-time pilot cameras feedback for obstacle avoidance and Multi Function Displays (MFD) to determine flight attitude, position, aircraft parameters. A wide Field Of View (FOV) pilot camera up to 120-150° will provide some degree of aircraft collison avoidance also, if the camera monitors are big enough to enable the awareness of other airspace users on the front site. Different experiments conducted indicates, typically, a 23-32" would be the minimum size to accomplish this. On the MFD various safety features can be displayed, e.g. ADS-B In, FLARM (Traffic and Collision Warning for General Aviation fuel levels, temperatures and others. Having a transponder installed in the aircraft can help to increase other airspace users awareness and to identify the RPAS location. An aeronautical radio should be present on the RPS side for listening and position communication. A backup power supply capable of restoring power in sufficient time to avoid loss of aircraft control during power outages should be available. On the aircraft side, navigation lights and strobes should be made mandatory, as well an easy to identify color scheme. Link-loss fail safe features should be in place to allow a safe return to home of the aircraft in case of radio link loss or disturbance. Radius of action limitations should be configured in the autopilot to assure performance limitations are kept up and running. For EVLOS operations, alternate emergency landing places should be programmed in case of engine failure. This is part of the mission planning, same as manned aircraft crews are used to do. A qualified flight termination systems should be part of the standard avionic equipment for EVLOS operations. It has to be deployed in case of critical aircraft malfunction that will not enable a safe continuation of the flight or a return to home.

2.4. Use Case 3: Fire fighting and SAR assistance

Non Commercial Operations (3020000) are subdivided in different levels. We have associated to these levels, the different flight operation modes VLOS, EVLOS as follows:

- 3020700 Fire fighting: post-disaster damage assessment; emergency operation center support
- 3021200 Search and rescue: post-disaster damage assessment; emergency operation center support

Introduction: RPAS would be a valuable tool for Search And Rescue (SAR) and fire-fighting crews, given to them a birds view perspective, which will permit activities not possible from the ground. Large unmanned platforms will be used for wide flooded, burnt or damaged area surveying, forest fire plume detection, damaged ship detection, large burnt area mapping, etc,But,large systems are complex machines and need to fly safely in the national airspace, socomplex and costly detect and avoid systems need to be installed and qualified prior to take to the sky. This is one of the reasons why the industry will focus on small affordable systems using VLOS and EVLOS operation modes. Like in the VLOS and EVLOS application, helicopter are the most used RPAS platforms. However, for area mapping, small fixed wing aircraft would be a perfect partner to rotary wing systems.

In the SAR environment, small portable RPAS platforms can help coordination-crews to identify possible locations for emergency tents, portable toilets, and field kitchen deployment, as well as locate possible hazards near the emergency centres. Another application could be first aid and communication devices precise deployment to people isolated in flooded areas, mainly on the roofs. TV news and written articles in magazines evidence that today, small systems are widely used for post disaster assessment and documentation. One valuable application could be the prevention of “crime activities in disaster areas, flying routine patterns during day and night using daylight and thermal sensors. Another interesting application could be establishing wi-fi and mobile phone communication bubbles. This is particularly suited for low speed flying devices, such as airships and balloons.

In the Firefighting environment, small systems are used for hot spot detection, damage assessment and burnt building structure stability estimation/prediction after fire has been extinguished. During active fire, the turbulences could become so strong and not predictable that it will not be safe to fly close to it. Smaller burnt areas can be mapped with small systems, avoiding high expenses using manned large systems.

Scenario Description: Operational scenarios for disaster assessment (fire, flooding, earthquake, etc) are mainly based on the same condition as descripted in Section 2.2 “Aerial Photography”, as the platforms are quite the same or similar. Particularly care must be given to the crew location to avoid injuries to the flight crew from debris on the ground and possible falling down from damaged structures. A precise “Operation Manual” has to be written for specific dangerous and hazardous situations. The main difference from Section 2.2 is the case that for emergency operations not only VMC are allowed, but on all meteorological conditions and at night, if lives can be saved.

Radius of action
See section 2.3 for VLOS operation and 2.3 for EVLOS operations. Radius of action limitations should bypassed only in case there is no danger for other persons and for absolute emergency situations where it could save lifes.

Endurance: see section 2.3 for VLOS operation and 2.3 for EVLOS operations.

Other airspace users: SAR, Helicopter Emergency Medical Service (HEMS), Law Enforcement, military and news gathering helicopters could be also present in this low height airspace. A correct flight coordination issued by the Emergency Coordination Centre between manned and unmanned systems has to be put in place. This is more a “how to do” and “Operation Protocol” issue instead of a technological issue.

Safety Enhancements: As described above, some manned helicopters could be present in the operational area. One or more External Observer should be mandatory to enhance situational awareness on 360° of the flight crew and the operating platform. Surveying in the EVLOS mode needs to be approved by a NOTAM to avoid low altitude collisions between manned and unmanned systems. However, today Mode-S and ADS-B transponders are becoming incredibly small, lightweight and affordable and can be even installed in small unmanned systems to help to increase situational awareness to other airspace users. In summary, all safety enhancements described in section 2.2 and 2.3 are applicable to this section also.

2.5. Use Case 4: Pipeline monitoring

BLOS Flight Mode (long-term solution): 3010300 Aerial patrol: pipeline control; power line control; railway control; vegetation patrol; river water quality monitoring; border patrol.

Other commercial operations associated to the BLOS Flight Mode.

- 3010100 Advertising: banner towing

Introduction: The commercial operation “pipeline control/power line control” case will reflect the common operational aspects present in other business cases related to the long-term solution BLOS Flight Mode. BLOS is the most complicated flight operation mode as it implies civil aviation stakeholders acceptance, general public acceptance, liability issues and technology reliability questions. BLOS could mean beyond line of sight, but still in radio line of sight, but also beyond radio line of sight. The two different operational modes may be distinguished in terms of communication technology and behavior. Beyond visual line of sight, but still in radio line of sight, allows a real time piloting and communication between the ground control station and the aircraft without delays, beyond radio line of sight requests a satellite data link that induces delays in the command & control and video feedback data link. BLOS is the preferred operational mode for “patrol and long range survey” missions. Infrastructure monitoring/patrol, e.g. pipeline and power line control, are performer in low altitudes up to 500ft AGL in VFR to gather infrastructural details and defectsLow altitude patrol, where only VFR is applicable, it will encounter a lot of issues if not performed in extreme remote locations, such e.g. artic, deserts, etc. The main issues are the aircraft reliability and airspace separation in VFR airspaces, as this kind of systems are typically heavier and bigger in size compared to VLOS/EVLOS platforms, in order to carry enough fuel and payload capacity to fulfil BLOS missions in a cost effective way compared to manned missions. Some sort of BLOS missions could also be performed with light fixed wing systems that carry a consumer camera of a few hundreds grams. Test campaigns have shown the ability to fly autonomously over pipeline routes in stretches of the order of 20 to 40 km.

Scenario Description: BLOS operational scenarios, e.g. for pipeline/powerline inspection, are based on a predefined waypoint mission in the G-Class airspace. The pilot will take-off in VLOS flight under Visual Meterological Conditions (VMC) and in direct radio line of sight. Once in flight, the pilot will switch from manual to automatic mission mode to enable waypoint approach operation, and enable beyond radio line of sight communication too. As soon the aircraft is out of direct radio line of sight, satellite or GSM/GPRS/UMTS (where available) communication links will become the primary data link. The most used and familiar RPS for BLOS optimized systems are rack based command and control seats, installed in vans or trucks, featuring flight control devices, keyboard and monitors with on screen display showing critical flight information data, such roll, pitch, heading, distance from pilot position and battery/fuel status, video recorder, mission planner, etc. Smaller systems uses portable desktop based military cases, with same functionality as the bigger systems, but concentrated and resized to be fitted in the military case. The RPAS needs to be able to operate in extreme climatic conditions, e.g in the northest part of the EU with total darkness in winter time, temperatures that drop to -40°C, snow and ice on RPS and aircraft; and up to +45°C in the southest part of the EU. For special patrol operations, such as to discover people engaged in “bunkering” activities, night flight operations would become a request.

Radius of Action: The maximum distance the RPAS can travel away from its ground control station along a given course with mission payoad, carry out its intended mission, and return without refueling, allowing for all safety and operating factors needs to be defined. Radius of action distance is directly dependent on the operational area of interest. From custom interviews (Terna, Italy), it was determined that the typical radius of action should be at least 100 km at a single flight mission.

Endurance: The endurance at the radius of action is an important parameter that defines the coverage of the RPAS at the specified loiter speed, typical operating altitude and sensor properties. Endurance is mainly dependent on the RPAS aerodynamic design, and fuel amount carried. Safety is directly related to a proper and carefully calculated endurance time. Average flight time is between 2-7 hours per fuel tank, depending on meterological conditions and payload capacity installed.

Other airspace users: Depending on the mission altitude, defined as the altitude where the specified payload provides the best performance results, we will encounter other airspace users. For missions lower than 400 feet, no other airspace users are present, but military, state flights and emergency helicopter flights could show up sometimes. Powered motorglider and micro light aircraft could also show up. Above 500 feet, GA airspace users could be encountered. NOTAM allong the complete mission route should be mandatory.

Safety Enhancements: BLOS flight operations should be conducted from an environmentaly closed command and control place to avoid external distractions. The pilot has to constantly observe real-time pilot cameras feedback for obstacle avoidance and Multi Function Displays (MFD) to determine flight attitude, position, and aircraft parameters. A wide field of view (FOV) pilot camera up to 120-150° will allow some degree of aircraft separation also (on direct radio line of sight), if the camera monitor is big enough to allow the awareness of other airspace users on the front site. Typically, a 23-32" would be the minimum size to accomplish this. On the MFD various safety features can be displayed, e.g. ADS-B In, Flarm, fuel levels, temperatures and others. Having a transponder installed in the aircraft can help to increase other airspace users awareness and to identify the RPAS location. An aeronautical radio should be present on the RPS side for listening and position communication. A backup power supply capable of restoring power in time to avoid loss of aircraft control during power outages should be available.
On the aircraft, navigation lights and strobes should be made mandatory, as well as easy to identify color scheme. Link-loss fail safe features should be in place to allow a safe return to home of the aircraft in case of radio link loss or disturbance. Radius of action limitations should be configured in the autopilot to assure performance limitations are kept up and running. For BLOS operations, alternate emergency landing locations should be programmed in case of engine failure. This is part of the mission planning, same as manned aircraft crews are used to do. A qualified flight termination systems and ELT (Emergency Locator Transmitter) should be part of the standard avionic equipment for BLOS operations, which has to be deployed in case of critical aircraft malfunction that will not allow a safe continuous of flight or return to home.

2.6. Summary of envisaged application(s)

The list for potential commercial applications is long, however, the VLOS and EVLOS missions would be the most promising business drivers in the next years. Technology to assure safety and related social acceptance, and civil aviation authorities requirements on system and flight crew "qualification" are already affordable. Aerial photography, which encapsulates industrial inspections also, would become the most used business driver, followed by short range aerial surveys and precise agriculture applications. A EU wide harmonization in the RPAS rules will help to increase the potential business.

On the safety aspects, safety measures should be taken so that undesired consequences are kept to a minimum during a hazardous event. Risk of personal injury or material damage due to hardware, software, procedural or environmental hazards must be at acceptable levels. RPAS emergency modes and flight termination systems improve the operational safety and its social acceptance. A sort of airworthiness "qualification" and pilot licensing for small systems would be welcome to ensure a minimum of system and procedures safety level and reliability.

Note that in France, the National CAA, DGAC, has authorized the use of small RPAS in four scenarios based on a simplified safety analysis approach made by a group of experts. These scenarios, operation modes and concerned RPAS have been defined in a law (arrêté) published in June 2012 [49]. A list of approved RPAS operators has also been defined [50].

3. RISKS TO BE REGULATED

3.1. Introduction

It will not be possible to introduce new expected RPAS operations, if it cannot be shown that the associated risks and hazards can be adequately regulated and controlled. ICAO states “The principal objective of the aviation regulatory framework is to achieve and maintain the highest possible and uniform level of safety” [3, 6]. In the case of RPAS, this means ensuring the safety of any other airspace user as well as the safety of persons and property on the ground [4]. Before developing a specific plan for RPAS Safety Risk Management (SRM), it is first necessary to understand RPAS safety policies and guidance provided by the regulators. In Europe, EASA provides guidance for RPAS airworthiness certification [9, 10] and a preliminary regulatory impact assessment [11], which recommends initiation of a rulemaking task intended to reduce the safety/environmental/economic risks identified in relation to RPAS. Additionally, it is noted that for introducing and/or planning changes to the ATM system, in Europe also an ATM safety risk analysis is recommended (ESARR 4 [8]) and ATM safety monitoring (ESARR 3 [7]). So far, RPAS are mostly used in segregated airspace under specific requirements. Therefore, when looking at newly proposed RPAS operations, it is expected that risks or hazards may be identified for which estimation of hazard severity or likelihood of occurrence may turn out to be difficult prior to implementation of the operation(s). The European Commission’s view on the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)” [21] states that EC Regulation No. 785/2004 [22] which covers the liability of the operator for passenger, baggage, cargo and third parties, will require some adaptations to better address the real risks related to the commercial and corporate exploitation of RPAS. This includes the limitation to third parties damage, introduction of further categories to accommodate different classes of RPAS below 500 kg, and adaptation of risk levels to the flight characteristics of the very light RPAS [21]. Main technology developments required in the safety area to support air traffic insertion include e.g. development of a methodology for the justification and validation of RPAS safety objectives.

What are the ‘risks’ to be considered and regulated? According to EASA, risks to be regulated are ‘collision with people/property on the ground’ and ‘collision with other aircraft in flight’ [11]. This is in line with EUROCONTROL, which suggests accounting for 1) risks to other airspace users 2) third party risk 3) potential new risks specifically related to unmanned aircraft. The EC states “since there are no people on board the RPA, the safety objective is targeted at the protection of third parties on the ground and in the air” [21]. The EC furthermore states that ‘RPAS must not have a negative impact to overall aviation safety objectives, must not require changes to ATM procedures and must not have an impact on the air traffic control capacity of the Air Navigation Service Providers. The future RPAS “safety objectives”, to be defined at European level, need however to be reasonable and adapted to RPAS specificities and developed with a ‘dual use’ concept, as much as possible, (i.e. civil or military)’. In the United States, FAA aims to ensure that RPAS ‘do no harm’ to other operators in the NAS and, to the maximum extent possible, the public on the ground’ [51]. FAA supports introduction of RPAS in Non-segregated Airspace ‘provided that the risks of flying the unmanned aircraft in the civil airspace can be appropriately mitigated’ [51]. There is consistency between the approaches taken in Europe and United States of America. Clearly, the concern is that RPAS operations might not only interfere with commercial and general aviation aircraft operations, but will possibly also pose a safety problem for other aircraft and people and objects on the ground. All hazards that may lead to these risks occurring will need to be identified and properly mitigated.

3.2. RPAS risk criteria framework

SRM is required to maintain or even improve the current level of safety. Risk criteria based policies for control of major risks have therefore been in use for many years. Many of these policies are based on some sort of quantification of the risk level that could be allowed. This concept of a level of risk has a number of implications. Because safety risk of future operations cannot be measured directly, an alternative approach for evaluating safety is necessary to be able to demonstrate that a certain target will be met. Two widely spread risk criteria framework approaches are in use to control and regulate risks:

- Target Level of Safety (TLS) approach;
- As-Low-As-Reasonably-Practicable (ALARP) approach.

The TLS approach is based on the specification of an acceptable value of risk which can be used as a yardstick against which the risks associated with a system or procedures can be evaluated. The ALARP approach is based on a decision structure, which contains a tolerable region bounded by maximally negligible and minimally unacceptable levels of risk. Within the tolerable region the risk must be proven to be ALARP in order to be acceptable. A commonly used risk criteria framework for aviation safety risk includes a) a single risk metric defined in terms of the probability per unit of exposure, and b) a risk requirement for this risk metric, which is based on the TLS approach. The associated basic methodology for determining whether the system is acceptably safe uses an evaluation of the system risk against a TLS, which is often expressed in terms of a maximum number of fatal accidents per flying hour. Within the aviation sector, the ALARP approach is mostly used in qualitative safety assessments of changes in the ATM domain. It has not yet been used for controlling and regulating UAS related risks.

A commonly accepted risk criteria framework for RPAS does not yet exist, although proposals have been made and are being discussed within different working groups. A RPAS risk criteria framework contains:

1. Definitions of risks to be regulated;
2. Definitions of appropriate metrics;
3. Risk criteria for judging the acceptability of the risks.

3.3. Risk metrics for RPAS

It is commonly accepted that risk is not a single quantity, has many different aspects, and may be quantified in many different ways. Different classes of metrics are distinguished:

- Risk metrics based on ‘probability of an adverse event (or occurrence of undesirable events) per unit of exposure’, without considering the possible consequences.
- *Economic risk metric*. The sum of expected economic losses due to fatalities and loss of equipment, where the sum is taken per time period of exposure. For loss due to one fatality two types of values are usually used: Value Of Life (VOL) and/or Value Willing to Pay (VWP).
- *Individual risk metric*. The risk experienced by a single individual in a given time period, at a given location. It reflects severity of the hazard and amount of time the individual is in proximity to the risk. It takes no account of numbers of people affected by an event.
- *Societal risk metric*. The risk experienced by a group of people exposed to the hazard, often expressed as a relationship between frequency of, and the number of people affected by, an event.

What types of metrics have commonly been used to regulate and control aviation safety risk? Aircraft system failure probabilities in terms of ‘probability per flight hour’ are used as part of the airworthiness certification process to e.g. show that any failure condition which would prevent continued safe flight and landing is extremely improbable. For aerospace system health management, commonly used metrics are Probability of Loss of Control and Probability of Loss of Vehicle. Two metrics for the collision risk between aircraft are e.g. 1) collision probability per movement (e.g. approach, take off), and 2) collision probability per year (or expected average time interval between two risk events). The collision risk of an aircraft with the ground is usually assessed for movements in the airport environment (i.e. take-off or landing). Metrics used to manage third party risk to persons on the ground are usually based on individual risk metrics. Such metrics are presently used in the Netherlands [34, 35] and in the United Kingdom to control new housing development and purchasing of existing houses. E.g. in the UK, individual risks of loss of life higher than 10^{-4} per annum are intolerable for the public and those below 10^{-6} per annum are regarded as broadly acceptable. In addition to criteria based on individual risk, it is also possible to define criteria in terms of societal risk [36]. Societal risk is the risk of widespread or large scale detriment from the realization of a defined risk, the implication being that the consequence would be on such a scale as to provoke a socio/political response. The basic principle for societal risk metrics is to reflect the society's point of view in a single metric curve. In this perspective, risks having low probability and high consequence are taken into account. Societal risk is generally expressed by f-N or F-N curves. When the frequency of events which causes at least N fatalities is plotted against the number N on loglog scales, the result is called F-N curves. If the frequency scale is replaced by annual probability, then the resultant curve is called f-N curves.

Societal aspects of risk acceptability include e.g. the following:

- Voluntary versus involuntary: Voluntary risks are more tended to be taken than involuntary risks.
- Controllability versus uncontrollability: Once the risk is under personal control (e.g. travelling as a passenger), it is more acceptable than when the risk is posed or controlled by other parties.
- Familiarity versus unfamiliarity: When people are familiar with risk involved in an activity they are more willing to accept it.
- Short versus long-term consequences: Many people continue smoking, being aware of the fact that they will not be affected immediately and the long-term consequences are difficult to assess.
- Presence of existing alternatives: If there are no alternatives, many risks are tolerated by people.
- Type and nature of consequences: Risks due to events causing more damage and fatalities are more difficult to accept.
- Derived benefits of society and the individual play significant role in risk acceptance.
- Presentation in the media: Verbal and visual presentation of an adverse event in mass media has some influence on risk acceptability.
- Personal involvement: If the societies' vulnerable groups (e.g. children, elderly or disabled) are exposed to risk or if a specific person is presented rather than some statistics, the risk acceptance will be affected. For people having their personnel property in risk there may be different acceptable risk levels than having others' property.
- Information availability: Informed societies can have better preparedness for natural hazards, while societies having frequent natural disasters have fresh memories about the consequences.
- Level of automation: people may be less accepting the risks related to use of automated systems.

Which types of risk metrics are suitable for addressing and regulating the risks related to RPAS operations? At least these risk metrics have to address a) risk of collision with other aircraft, b) risk of collision risk with the ground (and/or the associated risk to persons/property on the ground). Commonly accepted RPAS risk metrics do not yet exist, although proposals have been made and are being discussed in various working groups. Insight in the different possibilities for addressing the relevant risks is provided in the following.

3.4. RPAS risk criteria

As mentioned in the above, a commonly accepted risk criteria framework for RPAS does not yet exist. JAA/EUROCONTROL RPAS Task Force [13], NATO 52], and EASA [9, 10, 11] provide more insight. The *Joint JAA/EUROCONTROL RPAS Task Force* was the first international effort by aviation authorities to establish an acceptable risk criteria framework for RPAS operations in Europe. This Task Force defined 5 levels of hazard severity [13]:

- *Severity I* ("Catastrophic"): RPAS is unable to continue controlled flight and reach any predefined landing site (uncontrolled flight followed by an uncontrolled crash, with potentially fatalities or severe damage on ground.
- *Severity II*: Failure conditions leading to the controlled loss of the RPAS over an unpopulated emergency site, using Emergency Recovery procedures where required.
- *Severity III*: Failure conditions leading to significant reduction in safety margins (e.g. total communication loss with autonomous flight, landing on predefined emergency site that is unpopulated and fulfills certain requirements).
- *Severity IV*: Failure conditions leading to slight reduction in safety margins (e.g. loss of redundancy).
- *Severity V*: Failure conditions leading to no Safety Effect.

No explicit maximum allowable frequencies at which the events at the distinct hazard levels may occur are provided. However, it is stated that the quantitative safety objective for the RPAS 'Severity conditions' should be set, per RPAS category, based upon a rationale similar to AMC 25.1309 [10, 53]. The hazard definitions proposed by the Task Force only apply to people and property on the ground; no such levels are provided for the risk to people in the air.

NATO STANAG 4671 [52] addresses risk criteria for the risks to people on the ground, because a RPAS carries no passenger or crew. Therefore, the consequences of an event in terms of casualties cannot be considered with respect to occupants. NATO uses a probability level reference system with 5 classes: *Extremely Improbable, Extremely Remote, Remote, Probable* and *Frequent* (based on occurrence levels per flight hour). Compliance should take into account the following severity definitions:

- *Catastrophic*: Failure conditions that result in a worst credible outcome of at least uncontrolled flight (including flight outside pre-planned or contingency flight profiles/ areas) and/or uncontrolled crash, which can potentially result in a fatality. Or 'Failure conditions which could potentially result in fatality to RPAS crew or ground staff'.
- *Hazardous*: Failure conditions that either by themselves or in conjunction with increased crew workload, result in a worst credible outcome of a controlled-trajectory termination or forced landing potentially leading to loss of RPAS where it can be reasonably expected that a fatality will not occur. Or "Failure conditions which could potentially result in serious injury to RPAS crew or ground staff".
- *Major*: Failure conditions that either by themselves or in conjunction with increased crew workload, result in a worst credible outcome of an emergency landing of the RPAS on a predefined site where it can be reasonably expected that a serious injury will not occur. Or "Failure conditions which could potentially result in injury to RPAS crew or ground staff".
- *Minor*: Failure conditions that do not significantly reduce RPAS System safety and involve RPAS crew actions that are well within their capabilities. These conditions may include a slight reduction in safety margins or functional capabilities, and a slight increase in RPAS crew workload.
- *No safety effect*: Failure conditions that have no effect on safety.

EASA considers two possible approaches to certify the airworthiness of RPAS [10]:

- *Conventional* approach, based on a defined airworthiness code to the design of aircraft. This approach is common in civil manned aviation, and it is a common philosophy of this approach that it avoids any presumption of the purposes for which the aircraft will be used in service.
- *Safety Target* approach, based on setting an overall safety objective for the aircraft within the context of a defined mission and operating environment.

EASA initially concludes that the existing civil regulatory system has delivered continually improving safety levels whilst being flexible enough to cope with the relentless evolution and development in aircraft design, and that any proposal to depart from the established system in favor of a Safety Target approach will be hard to justify today. Hence the conventional approach for airworthiness certification is used. With regard to RPAS risks to people on the surface, initially the severity levels and safety objectives used by EASA have been equal to those established by the JAA/EUROCONTROL RPAS Task Force [13]. With no persons onboard the aircraft, the airworthiness objective is primarily targeted at the protection of people and property on the ground. The RPAS safety risk assessment shall show that the RPAS complies with safety objectives e.g. the probability level associated with the risk of an uncontrolled crash is less than an agreed figure and the severity of various potential failure conditions is compatible with their agreed probability of occurrence. EASA does not define these severities and probability levels because the work is still ongoing to reclassify the severity of failure conditions for RPAS. As an interim position, EASA refers to the quantitative values applicable to requirement 1309 contained in the applicable airworthiness code used as the reference in defining the type-certification basis of the individual RPAS, with as minimum the minimum values contained in CS 23.1309 for Class 1 aeroplanes [10, 11, 53]. EASA addresses the intrinsic safety of the RPAS, i.e. the certification of its airworthiness; it does not address the protection of other airspace users because this is dependent on ATC/ATM separation procedures and defined “detect and avoid” criteria, commensurate to the airspace class and type of operations (i.e. within or beyond visual line of sight). With the recent extension of EASA’s remit to also cover ATM/ANS, EASA is now dealing with the protection of (other) airspace users as well [48]. Furthermore, it should be noted that EASA is currently engaged in developing a safety Regulatory Roadmap for civil RPA above 150 kg and EASA's work plan for 2013 includes specific rulemaking tasks related to RPAS. Therefore, further guidelines from EASA regarding the establishment of RPAS risk criteria (including those with respect to other airspace users, i.e. in relation to the risks of collision between a RPAS and a (manned aircraft)) are expected in the near future.

The views on acceptability of risks are clearly not yet consistent. According to one line of reasoning, most RPAS are equivalent to CS-23 aircraft because of their weight and number of people that could be at risk, and shall meet risk criteria applicable to CS-23 aircraft. According to another line of reasoning, RPAS are too complex for comparison with CS-23 aircraft, are equivalent with CS-25 aircraft, and shall therefore meet the risk criteria applicable to CS-25 aircraft. Additionally, many express the wish to account for society’s point of view in a more explicit way by introducing and using societal risk metrics for RPAS operations in order to more adequately assess the risks to property or people on the ground. For this purpose, so called F-N curves may turn out to be useful. Societal aspects that influence the risk acceptability of society regarding newly proposed RPAS operation(s) may need to be investigated further.

4. SAFETY ASSESSMENT METHODS

4.1. Introduction

This section deals with RPAS safety risk management methodologies. Safety Risk Management (SRM) is ‘a formal process within a Safety Management System (SMS), and is composed of describing the system, identifying hazards, assessing the risk, analyzing the risk, and controlling the risk’ [16]. Risk Management is defined by ICAO as ‘the identification, analysis and elimination (and/or mitigation to an acceptable or tolerable level) of those hazards, as well as the subsequent risks, that threaten the viability of an organization’ [6]. The objective is to ensure that risks associated with hazards to flight operations are systematically and formally identified, assessed, and managed within acceptable safety levels. Typically, SRM consists of five steps:

1. Describe the system to be introduced or changed;
2. Identify the associated hazards and causal factors;
3. Analyze risks (characterise risk in terms of hazard severity and likelihood of occurrence);
4. Assess (acceptability of) risks (and provide results for decision making);
5. Treat/control the risks (i.e. mitigate, monitor and track).

The purpose of such SRM methodology is to assist in the identification and classification of RPAS hazards, the assessment of their risks, and the definition of corresponding mitigation strategies. As such, the methodology can be used to produce safety evidence to present to safety regulators to justify that the introduction of a newly proposed RPAS operation is sufficiently safe. This section therefore provides and overview of safety methods that can be used to deal with the following issues and questions:

- What shall the core elements be, and the associated sequential steps of safety risk management?
- How shall potential applicants show that the risk of RPAS operations with a newly certified RPAS will be acceptable and adequately controlled?
- What would be an acceptable means to perform RPAS safety risk management, to evaluate risk mitigation measures, and to evaluate a list of assumptions and parameters?
- What sequences of events and what root hazards might lead to the identified risks?
- What main mitigation measures can and should be implemented to ensure that the risk of RPAS Non-segregated Airspace operations will be maintained to be acceptably low?

It has been motivated that the main safety risks that need to be addressed to ensure that newly proposed RPAS operations can be introduced in the airspace without degrading safety are *Risks to other airspace users* and *Third party risk*. This sub-section will provide guidelines for the development of risk analysis methodologies for assessing both types of risks. It should be noted that the methods (and supporting tools) should be developed in the context of the following two research questions:

- How shall potential applicants show that the risk of RPAS operations with newly certified RPAS will be acceptable and adequately controlled?
- What would be an acceptable means to perform a RPAS safety risk analysis, to identify risk mitigation measures, and to establish a list of assumptions and parameters?

4.2. Overview of safety assessment methods

The products of a RPAS SRM process may, besides safety argumentation in support of the introduction of new proposed RPAS operations, include safety evidence such as e.g. RPAS safety data, risk models, results from hazard brainstorm sessions, risk assessment simulation results and safety assurance reports. These products would document and support decision-making on the proposed changes that impact safety and implement safety enhancements for RPAS operation. An RPAS safety risk assessment may have to deal with the entire RPAS lifecycle, including a) specification b) manufacturing c) implementation d) transition to operational service e) operational service and f) decommissioning. A primary consideration for determining the scope and level of detail is what information is required to know enough about the change, the associated hazards, and each hazard's associated risk to choose which controls to implement and whether to accept the risk of the change. A description of the system and/ or proposed change should be complete (at appropriate detail level) and correct (accurate, without ambiguity or error).

There is an enormous variety of risk assessment conceptual frameworks, methodologies, and methodologies catalogues. Three catalogues of safety methods that exist are:

- Safety assessment methods database [43]. This document gives an overview of about 800 techniques, methods, databases, and/or models that can be used during a Safety Assessment. Besides a summary of the aim, description, domain (e.g. nuclear, chemical, air traffic management, aviation, aircraft development, computer processes), application (i.e. applicable to hardware, software, human, procedures, or to organisation) of the method, it describes for which safety assessment stage (i.e. scope the assessment, learning the nominal operation, identify hazards, combine hazards into risk framework, evaluate risk, identify potential mitigating measure to reduce risk, safety monitoring and verification, and/or learning from safety feedback) a particular safety method could be used.
- ATM safety techniques and toolbox [54].This document comprises 27 techniques that can be used to evaluate and improve safety in ATM. It outlines a simplified eight-stage safety assessment approach and then provides details about the safety assessment techniques. It explains where the technique comes from, its maturity and life cycle stage applicability, the process and data requirements, and practical and theoretical advantages and disadvantages. The overall approach biased towards concept design and development, but most of the techniques can also be applied to existing systems.
- Guide to methods and tools for airline flight safety analysis [55]. This document provides summaries of 57 methods and tools that can be used to analyse flight safety data including event reports and digital flight data. These methods and tools are organized into three areas: flight safety event reporting and analysis systems, flight data monitoring analysis tools, and specific purpose analytical tools.

In response to a request from EASA, Future Aviation Safety Team (FAST) conducted a review of safety risk analysis methods, in order to devise a methodology to assess (as well as anticipating and mitigating) future risks [41]. Criteria to rate about 30 identified applicable methods, according to its ability to provide insight into the future hazard/risk identification objectives, have been developed and applied. The resulting FAST/EME1.1 method, which describes a proposed process of carrying out a future risk assessment, is initially targeted at commercial entities and governmental organizations. Nevertheless, application to newly proposed changes in the aviation system is also foreseen within the EC Project ASCOS (Aviation Safety and Certification of new Operations and Systems), which is coordinated by NLR. The FAST method is built on three critical elements: a credible depiction of the future, a description of scenarios that will result in a number of hazards by looking forward in time, and a set of tools to execute the risk analysis that will produce credible results (while using e.g. credible data, addressing human factors influences).

The FAST Method is aimed at identifying future hazards that have not yet appeared because the changes within the aviation system that may produce these hazards have not yet taken place. The method process flow consists of 12 steps; 1) Be responsible for implementation of global aviation system changes; recognize your need for systematic prediction of hazards associated with changes and to design those hazards out of the system or avoid or mitigate the hazard; 2) Clearly define scope of expert team study; 3) Assemble an expert team; 4), 5) and 6) Communicate with FAST and Customer to understand the complete task; to understand pertinent Areas of Change (AoC); to determine key interactions; 7) Refine the visions of the future; 8) Compile the hazards; 9) Determine the watch items; 10) Compile recommendations; 11) Inform FAST regarding results; 12) Inform customers regarding results. The FAST method introduces safety assessment of an appropriately scoped future system in its future context, using a scenario-based approach and an enriched safety assessment methodology (see Figure 1) [41, 42, 44].

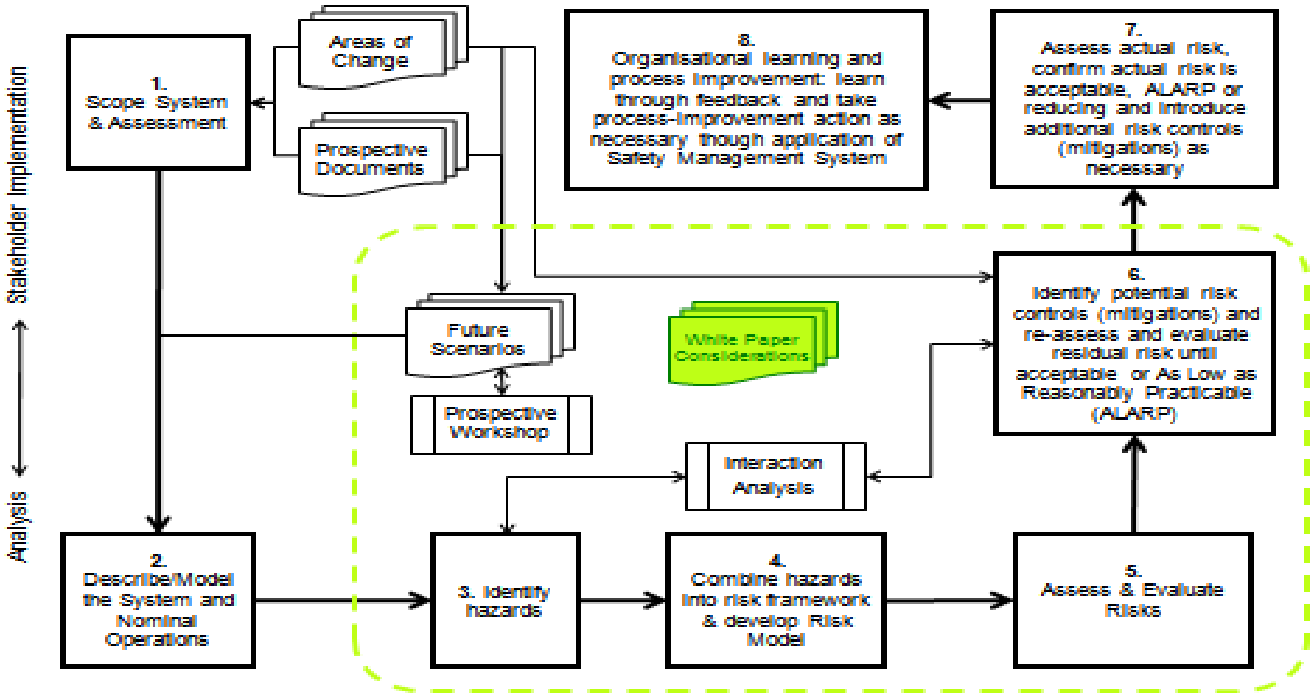

Figure 3 Future Aviation Safety Team (FAST) methodology

Various European RPAS safety risk analysis activities have already been performed. Noteworthy are e.g.:

- EUROCAE Working Group 73/93 RPAS Safety work;
- RPAS ATM Preliminary Safety Case;
- RPAS ATM Collision Avoidance Requirements [30];
- RPAS safety issues for civil operations (EC Project USICO);
- Innovative Operational RPAS Integration (EC Project INOUI) [24, 25, 26, 27];
- Preliminary Impact Assessment on the Safety of Communications for RPAS (project for EASA) [29];
- Safety of UAS operations in non-segregated airspace (performed by NLR for FAA and CAA NL));
- FAA Principles for Sense and Avoid (SAA) systems safety [56];
- JARUS systems safety assessment.

EUROCAE Working Group 73/93 RPAS Safety work

EUROCAE deals with standardization of aviation equipment and systems. Working Group 73 on RPAS performs safety work with the EUROCAE ED-78A methodology, Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications [31], so as to establish interoperability requirements, safety and performance requirements, and operational services & environment definition for aviation systems. Account is taken of ESARR 4 (Risk assessment and mitigation in ATM), together with the future legal/regulatory requirements and associated implications of the Single European Sky (SES) Regulations and Implementing Rules. The EUROCAE ED-78A methodology is equivalent to RTCA DO 264 as the guidance was developed by a joint group: EUROCAE WG53/RTCA SC189. The method provides means to establish the operational, safety, performance, and interoperability requirements.

RPAS ATM Preliminary Safety Cases

EUROCONTROL has constructed Preliminary Safety Cases for the introduction of Unmanned Aircraft Systems in Non-segregated Airspace, based on detailed Functional Hazard Assessments (FHA) and Preliminary System Safety Assessments (PSSA) for two previously defined baseline scenarios for the use of RPAS. The work has been carried out in compliancy with EUROCONTROL Safety Regulatory Requirements and Safety Assessment Methodology (SAM) [12, 28]. The overall objective is to identify a set of ATM safety requirements which, if implemented, will ensure that the introduction of RPAS in non-segregated airspace will be acceptably safe. This study produces:

- Safety Arguments for the safe introduction of RPAS in the ATM environment;
- Safety Assessment Plan, with Safety Criteria and planning/scheduling of Safety Activities;
- ATM Safety Assessment Reports for two predefined baseline operational scenarios;
- Preliminary Safety Cases for the two predefined baseline operational scenarios.

RPAS ATM Collision Avoidance Requirements

EUROCONTROL has assessed various aspects of potential RPAS equipage with a “detect, sense and avoid” functionality [30]. This RPAS ATM collision avoidance requirement study exploits methods and tools developed in a series of EUROCONTROL studies, which have investigated safety benefits resulting from equipage of manned aircraft with Airborne Collision Avoidance Systems (ACAS). The basic method and tools consist of three elements (the so-called Encounter model and Logic risk ratio, Risk ratio, and Contingency tree and Full System risk ratio). A measure of the safety of ACAS, known as the full-system risk ratio, can be evaluated. The risk ratio represents an upper bound on the safety benefit that can be delivered; the full-system risk ratio represents safety benefits likely to be realised in practice when other factors are considered. The risk ratio and contingency tree approach has so far mainly being used by safety consultants performing contract research for Eurocontrol. In Europe, no acceptable safety level has been determined or used.

RPAS safety issues for civil operations (USICO)

The European Commission project USICO (RPAS Safety Issues for Civil Operations) contains various activities that deal with airworthiness certification of RPAS technologies (including Sense and Avoid systems) and operational procedures. However, only one task "System safety and risk areas" deals with the safety assessment of RPAS operations in non-segregated airspace. This task is furthermore also restricted to the identification of Safety Objectives and the risk areas that are particular to RPAS. It contains the following four activities: 1) RPAS leading particulars, 2) Safety objectives, 3) Generic Functional Hazard Analysis, and 4) Impact on certification regulations. The Safety Objectives do not cover segregation of aircraft and collision avoidance requirements.

For the definition of Safety Objectives related to the risks associated to system failure conditions, the following methodology has been defined and applied:

1. Define an Overall Safety Objective, based upon an adequate definition of a RPAS worst severe risk to be prevented and minimised, considering previous study results and draft regulations.
2. Detail and interpret the Overall Safety Objectives, so that it can be translated in concrete quantitative terms for RPAS Safety Assessment, consistent with manned aircraft requirements.
3. Define lower severity categories applicable to RPAS and criteria for the acceptability of risks associated to corresponding failure conditions.
4. Define additional specific system safety criteria, considering results from other tasks.

The risk areas that are particular to RPAS operations have been identified through a generic Functional Hazard Analysis (FHA). Guidelines and methods for performing this FHA have been taken from the SAE ARP 4761 [14], which support safety assessment for certification of civil aircraft, in order to show compliance with paragraph 1309 of JAR CS 25 [53] and FAR CS 25. SAE ARP 4761 provides a top-down approach for identifying the functional failure conditions and assessing their effects (where it should be noted that steps 6 and 7 are outside USICO scope):

1. Identification of all functions associated with the level under study;
2. Identification and description of failure conditions associated with these functions, considering single and multiple failures in normal and degraded environments;
3. Determination of the effects of the failure condition;
4. Classification of failure condition effects on the aircraft (e.g. catastrophic, hazardous, major, minor, and no safety effect corresponding to respectively severity I, II, III, IV, and V);
5. Assignment of requirements to failure conditions to be considered at the lower level;
6. Identification of the supporting material required to justify the failure effect classification;
7. Identification of method used to verify compliance with the failure condition requirements.

Innovative Operational RPAS Integration (INOUI)

The European Commission project INOUI (Innovative Operational RPAS Integration) contained a Work Package 5 "Safety Analysis of civil RPAS operation", which included the following tasks:

- Setting appropriate scope of risks for integration of RPAS in non-segregated airspace;
- Propose Safety Criteria for the integration of RPAS in non-segregated airspace in Europe;
- Perform Functional Hazard Analysis (FHA)
- Derive Safety Requirements
- Perform Aerodrome Safety Analysis

The following occurrence categories generate the scope of risks: collisions between aircraft, collisions between aircraft and vehicles; and wake vortex encounters. The safety criteria developed by INOUI associate maximally allowable ATC related accident probabilities to the following ATC sub-products: Tower Control (Landing, Line-up, Start-up and pushback, Take off; and Taxiing), Approach Control (Departure, Initial and intermediate approach; and Final approach), and Area Control (Control Area inbound, Control Area outbound; and Control Area transit). The safety assessment of RPAS integration in non-segregated airspace [24, 25] has been performed largely with the Safety Assessment procedure of the Deutsche Flügsicherung (DFS) (see [26, 27]), which contains three phases: Functional Hazard Analysis (Phase 1), Determination of Safety Requirements (Phase 2), and Safety Analysis (Phase 3). The safety assessment process selected for addressing safety issues at aerodromes in INOUI emerged from the FAA/EUROCONTROL Action Plan 15, and contains the following 7 steps [9]: Scope of the Assessment, Describe the nominal and non-nominal operation, Identify Hazards, Combine Hazards, Evaluate Hazards, Identify potential mitigation measures, and Feedback to Operation, Assessment, and

Design. These steps are related with the EUROCONTROL SAM [28]. The SAM FHA is similar to Step 3, Step 4, and Step 5. The SAM PSSA is similar to Step 6. Step 1 and Step 2 are not explicitly included in the EUROCONTROL SAM; but are in this process used as input for the FHA Process. Step 7 (Feedback to Operation, ...) is a recurrent step which is recommended every time it is needed to inform concept developers about an important safety issue. This step usually takes place at the end of the FHA and at the end of the PSSA.

Preliminary Impact Assessment on the Safety of Communications for RPAS
A hazard identification and risk assessment was performed to identify and record functional hazards arising from each of 20 defined communication architectures, containing all elements that might be used by a remote pilot when communicating with the RPAS and with ATC. The risk analysis was based on the EUROCONTROL Safety Assessment Methodology [28]. When considering different communication architectures, the following events were considered to be hazardous:

- Loss of voice communications between RPAS pilot and ATC
- Interruptions to voice communications between RPAS pilot and ATC
- Intelligibility and latency of voice communications between RPAS pilot and ATC
- Loss of command and control link between RPAS and RPS
- Interruption of command and control link between RPAS and ATC
- Loss of surveillance information feed to ATC
- Interruption of surveillance information feed to ATC
- Loss of surveillance information to other airspace users
- Interruption of surveillance information to other airspace users.

Safety of RPAS operations in non-segregated airspace
Under a co-operation agreement between the US FAA and CAA-NL, NLR-ATSI was contracted to conduct research into the development of standards for certification, airworthiness, and operations of RPAS operating in non-segregated airspace. This multi-year (2007 - 2012) UAS safety project focused on the development and application of a RPAS safety risk management methodology. A framework for RPAS Safety Risk Management was established [16]. This framework covers among others, the risks to be regulated, suitable risk metrics, recommendations for defining an acceptable level of safety, and potential mitigation measures. Safety studies have been performed [38, 39, 40] in order to assess and evaluate RPAS traffic separation and collision avoidance capabilities and data-link reliability. Issues addressed are:

- What are the hazards that may result a RPAS to collide with the ground?
- Which requirements should be imposed on detect and avoid systems and operations for RPAS?
- What are the most promising technological and operational solutions for RPAS detect and avoid?
- What reliability requirements and contingency procedures should apply to the use of data-links?

The proposed SRM process assumes that the main risks to mitigate in order to safely introduce in non-segregated airspace without degrading safety are risks to other airspace users and third party risk (to people objects on the ground). The proposed SRM process for third party risk is based on a method that combines an accident probability model with an accident location model and an accident consequence model, and provides insight into the chance that a RPAS accident occurs at different particular locations. The RPAS hazards underlying the accident probability model are provided in Table 1. The causal chains of events that may lead to a collision with the ground are modelled by Event Sequence Diagrams (ESDs).

Table 1 RPAS hazards that might resulting in collision with the ground

ESD number	Name of the Event Sequence Diagrams
5	Operation of RPAS by remote pilot inappropriate
6	RPAS takes off with contaminated wing
7	Weight and balance outside limits (takeoff)
8	RPAS encounters performance decreasing windshear
11	Fire on board RPAS
12	Remote pilot spatially disorientated
13	Flight control system failure
14	Remote pilot(s) incapacitation
15	Anti-ice system not operating
16	Flight instrument failure
17	RPAS encounters adverse weather
18	Single engine failure
19	Unstable approach
21	Weight and balance outside limits (approach/landing)
37	Wake vortex encounter
40	RPAS positional information system failure
41	RPAS data link failure
42	Unnatural conditions in RPAS Ground Control Station
43	RPAS mid-air collision
44	A part of the RPAS falls down

The method has been applied to derive Safety Objectives for hazardous events related to commercial operations, performed with a RPAS that is to a large extent equivalent with manned aircraft in category CS-25. For other UAS types, it will be necessary to investigate if the ESDs developed in that study still apply or whether further adaptations are required. It also remains to be investigated if the fact that a RPAS does not carry passengers could allow for less stringent Safety Objectives than for manned aviation [15].

NLR has also analysed historical accident rates of US General Aviation (GA), to obtain insight in the risks associated with different flight phases and different flight rules. This could provide a baseline level of safety for RPAS categories equivalent to GA aircraft. This is achieved by performing a database analysis of accident flights operated under Federal Aviation Regulations (FAR) Part 91, while focusing on aircraft with a maximum certified gross weight of less than 19000 lb. The results may be used by regulators as baseline levels of safety for UAS categories that are equivalent with manned aircraft in category Certification Specifications (CS) 23. If it is shown that proposed operations with such UAS categories do not exceed this safety level, one might argue that such UAS operations may be introduced, without degrading safety levels. Three scenarios are considered for which a baseline safety level is derived [37]:

- Mid-air collisions;
- Accidents at or near the aerodrome;
- Accidents outside the aerodrome.

FAA Principles for Sense and Avoid (SAA) system safety

In the USA, the second FAA Sponsored “Sense and Avoid” Workshop has achieved a significant work about SAA principles and requirements. The report that was published in January 2013 [56] also contains conclusions and recommendations regarding TLS and Derived SAA Risk Ratio Requirements.

FAA conclusions and recommendations about TLS and derived SAA Risk Ratio Requirement include:

1. TLS is the key metric for substantiating the safety level of RPAS in the NAS ATM system, but TLS does not easily lend itself to describe the levels of mitigation that an UAS SAA system needs to achieve. The TLS should be broken down into RPAS SAA system mitigating components and should express those components in the form of a risk ratio.
2. The safety metric for RPAS SAA Target Level of Safety should be expressed in terms of Catastrophic Collision Event per flight hour (CCE/FH), where one (1) MAC, regardless of fatalities or damage to either aircraft, is defined to comprise two (2) Catastrophic Collision Events, and the quantitative values and methodologies described in ICAO Doc 9689-AN/953 [5] should be retained as the safety substantiation for RPAS SAA.
3. There should be at least two RPAS TLS, a more stringent TLS for airspace predominately occupied by Scheduled Air Carriers (SAC) aircraft, using a Separation Service Provider, and a less stringent TLS for airspace predominately occupied by General Aviation (GA) aircraft using see and avoid.
    a. A more stringent RPAS SAA TLS is set at $2x10^{-9}$ CCE per FH ($1x10^{-9}$ MAC/FH) for RPAS operating where transponders are required by regulation:
        i. Class A, B, or C airspace;
        ii. All airspace at and above 10,000 ft. MSL, excluding the airspace at and below 2,500 ft. AGL;
        iii. All airspace above the ceiling and within the lateral boundaries of a Class B or C airspace area designated for an airport upward to 10,000 ft. MSL;
        iv. All airspace within 30 nautical miles of an airport listed in Appendix D, section 1 of 14 CFR §91, from the surface upward to 10,000 ft. MSL (Mode C veil).
    b. A less stringent RPAS SAA TLS is set at $2x10^{-7}$ CCE per FH ($1x10^{-7}$ MAC/FH) for RPAS operating in all other airspace where the more stringent UAS SAA TLS is not required.
4. For RPAS integration into the NAS, an RPAS should be required to have some form of SAA (SS and/or CA) mitigation regardless of the operational airspace aircraft density.
5. The Risk Ratio objective for an aircraft operating under a Separation Provision Service should be derived from the TLS based on encounter data, modeling and simulation or structured analysis as applied within the Conflict Mitigation Model. Additional research is needed to solidify risk ratio values for each airspace and operating type based on standards and historical data.
6. The Risk Ratio objective for an aircraft operating under Self-Separation should be derived from the TLS based on encounter data, modeling and simulation or structured analysis as applied within the Conflict Mitigation Model. Additional research is needed to solidify risk ratio values for each airspace and operating type based on standards and historical data.

JARUS system safety assessment

JARUS (http://www.jarus-rpas.org) is a group of experts from the National Aviation Authorities (NAAs) and EASA. Its purpose is to recommend a single set of technical, safety and operational requirements for the certification and safe integration of UAS into airspace and at aerodromes. The primary output of JARUS will be recommended certification specifications and operational provisions, which can be used during the approval process of UAS. JARUS takes into account emerging ICAO standards, recommended practices and guidance material. Regarding safety, it is noteworthy that the JARUS Systems Safety working group produces a systems safety assessment (AMC 1309) for all categories of unmanned aircraft and related systems (including definition of top level UAS airworthiness, system safety objectives and guidance material (AMC UAS.1309) and UAS recommendations and conclusions on UAS failure classifications in terms of severity definition and probability requirements). JARUS also deals with the development of a classification scheme for UAS and Safety Management System considerations. The JARUS Detect and Avoid working group will establish safety objectives for the risk of collisions in the total aviation system.

4.3. Summary on safety methods

A variety of methods are being used (and/or are still under further development) to assess the safety of RPAS operations. The methods used include the EUROCAE ED-78A (which is consistent with the RTCA/DO-264), the EUROCONTROL Safety Assessment Methodology, and similar methods to derive Safety Objectives and Safety Requirements. Most of these safety risk assessment methodologies for RPAS operations include (or recognize a need for) the following core elements: Hazard Identification, Setting of Safety Objectives, and Determination of Safety Requirements. Usually this is recommended through a Functional Hazard Analysis and a Preliminary System Safety Assessment. Providing feedback to the operational developers (or manufacturers) on intermediate safety results from these activities is recognized as being very valuable as a recurrent step, if important safety issues are identified. These methods seem to be consistent with the approach required by the ICAO Safety Management Manual. However, at present only the EUROCAE ED-78A methodology and the RTCA/DO-264 seem to be recognized by both EASA and the FAA as an acceptable method for safety studies.

New safety methods – potentially applicable to assess the safety of RPAS operations – are under (further) development and application. In response to a request from EASA, Future Aviation Safety Team (FAST) conducted a review of safety risk analysis methods, in order to devise a methodology to assess (as well as anticipating and mitigating) future risks. The resulting FAST/EME1.1 methodology describes a proposed process of carrying out such a future risk assessment. NLR has further developed and applied the Causal model for Air Transport Safety (CATS), which was originally developed for the Dutch Civil Aviation Authorities for understanding the causal factors underlying the hazards and risks (and their relation to possible consequences) related to commercial air transport operations, to derive a baseline for RPAS command and control related hazards [17]. Application of the FAST/EME1.1 [41] and CATS method [17] to newly proposed changes in the aviation system is also currently foreseen within EC Project ASCOS (Aviation Safety and Certification of new Operations and Systems), which is coordinated by NLR.

Concerning the scope of the risk assessments, it is observed that - so far - no European study deals with the safety of RPAS operations from a total aviation system point of view. USICO focuses on the definition of safety objectives related to RPAS airworthiness, and excludes the segregation of aircraft and collision avoidance requirements. INOUI and the EUROCONTROL ATM integration safety studies focus on the ATM related safety risks (i.e. collisions between aircraft, collisions between aircraft and vehicles, and wake vortex encounters) and exclude airworthiness related safety issues. An initial EASA study on RPAS safety focuses purely on the safety of RPAS communications. NLR safety studies dealt with the risk of collision with the ground, RPAS detect and avoid systems, and loss of the data link for command and control (often assuming commercial operations with a fixed wing RPAS). It remains open to put all pieces of the safety puzzle together and obtain an overall view of the safety level of expected RPAS operations.

5. RISK MITIGATION MEASURES

The aim of this section is to provide suggestions for the further development of risk mitigating measures. As defined in Section 3, risks to be regulated are ‘collision with people and/or property on the ground’ and ‘collision with other aircraft in flight’. The motivation for this comes from the following policy statements:

- ICAO states “The principal objective of the aviation regulatory framework is to achieve and maintain the highest possible and uniform level of safety. In the case of RPAS, this means ensuring the safety of any other airspace user as well as the safety of persons and property on the ground.”
- EASA states that “With no persons onboard the aircraft, the airworthiness objective is primarily targeted at the protection of people and property on the ground. A civil UAS must not increase the risk to people or property on the ground compared with manned aircraft of equivalent category.

For the purpose and scope of ULTRA, this section therefore considers risk mitigating measures for both risks. It should however be noted that the ULTRA uses cases may include operations above unpopulated areas where damage to people and property will be minimal. For these cases, the consequences of collision with the ground are minimal, and mitigating measures for this risk may be considered out of scope knowing that the risk to damage properties can be covered by insurance

5.1. Risk of collision with other aircraft in flight

The risk of collision with other aircraft in flight is a risk that often has similar characteristics for different uses cases and scenarios. As an example, the risk of collision with other aircraft for the scenario of aerial photography may be comparable with the use case defined for wind energy or pipeline monitoring. In that case, the mitigating measures for such risks in all cases can be considered to be similar. However, low level flight may be safer to the flight as compared to the case where insertion into an air traffic environment is foreseen. In low level flight, specifically near infrastructure, no other aircraft will be present.

Furthermore, the risk mitigation measures for collision with other aircraft are closely related and linked to Sense and Avoid (SAA) issues. RPAS operators are quite unique in the fact that they do not have the capability to “see and avoid” as manned pilots in the aircraft would do unless the RPA is used VLOS or EVLOS. BVLOS operations, the RPAS remotely located pilot and observers are unable to look out the aircraft to check for traffic during flight and take appropriate action to mitigate the risk of collision. This brings added complexity to the RPAS SAA issue.

Much work has already been undertaken in this respect to mitigate risk originating from collision with other aircraft in flight. Both European and USA initiatives and approaches show consistency when attempting to overcome such risk. In fact, the main topics for discussion around the sense and avoid (SAA) mitigating measures are self-separation, collision avoidance, and avoiding weather and ground obstacles.

Self-separation and collision avoidance

Self-separation can be defined as the conditions required maintaining a well clear distance from other aircraft and avoiding the potential for a collision or threat to collide, whereas collision avoidance is the action of the last moment manoeuvring to avoid collision / penetration of a defined collision area.

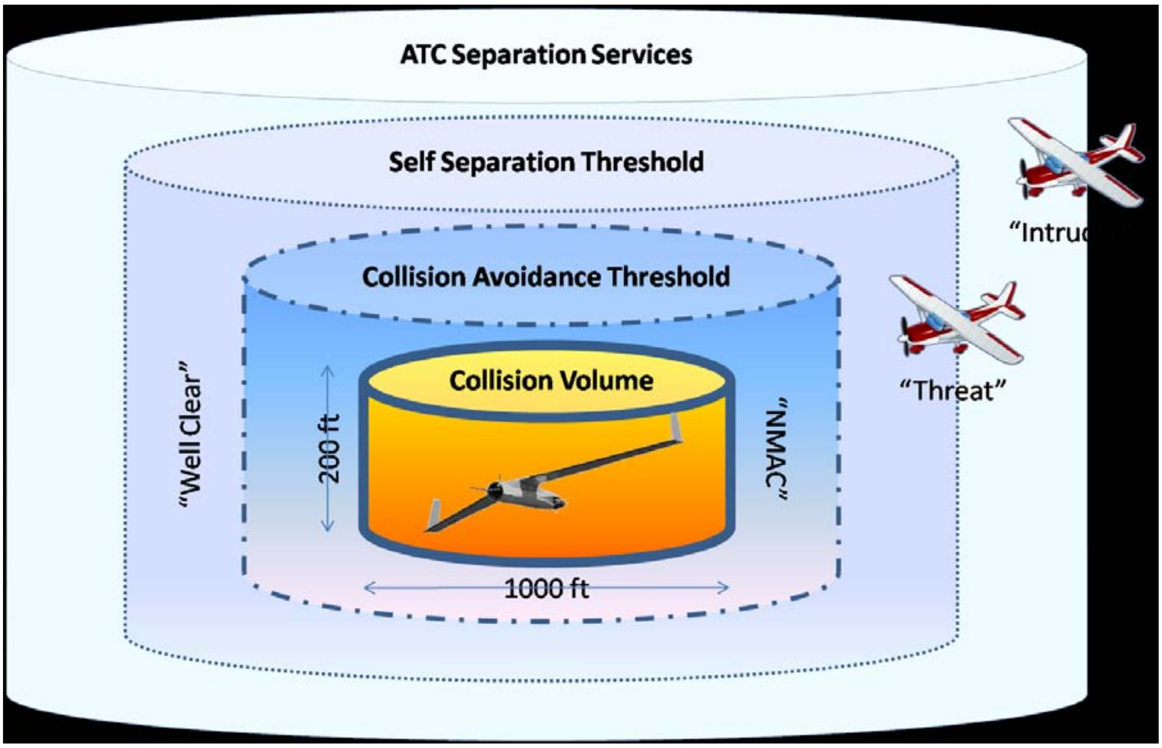

Figure 4 Self separation and collision avoidance thresholds

SAA provides the intended functions of self-separation and collision avoidance as a means of compliance with the regulatory requirements to “see and avoid” compatible with expected behavior of aircraft operating in the airspace system. In the USA, the second FAA Sponsored “Sense and Avoid” Workshop has achieved a significant result on SAA principles and requirements [56].

To highlight some of the work in SAA risk mitigating measures arising from the above workshop, five SAA topics have been identified for further work:

1. UAS Self-Separation and Air Traffic Separation Services;
2. Well Clear as an Airborne Separation Standard;
3. TLS and Derived SAA Risk Ratio Requirements;
4. Certification Considerations for SAA Systems and Equipment;
5. SAA Algorithm Standardization.

The MIT International Center for Air Transportation has defined contributory hazards, and influencing factors in the operational environment, that may cause a ‘mid-air collision’ [46]. Contributory hazards are:

- Loss of communication,
- Degradation of situation awareness,
- Altitude deviation,
- Operational error.

Influencing factors in the operational environment are traffic density and mission profile.
The following mitigation measures to reduce the risk of a potential mid-air collision are proposed:

- Reduce the exposure of risk to other aircraft: Mid-air collision risk is proportional to traffic density in the area of operation. Measures vary in the degree of separation of RPAS traffic from other aircraft. A strategy that is often used is to completely separate RPAS operations from other aircraft. This is currently utilized by limiting some military or research operations to restricted airspace. A more limited form is segregating RPAS operations to a designated flight level and restricting other operations in the area. A final possibility for separating RPAS operations is to conduct them below the height of buildings or structures in the area. For small RPAS, this is a viable strategy to reduce the risk of collision with manned aircraft. Operational strategies can reduce the ambient risk of operations, while still integrating RPAS operations in the airspace. To reduce ambient risk, RPAS could be precluded from operating within airways boundaries, and be required to perform the majority of their mission between major flight levels.
- Reduce the frequency of Initiating Failures: Initiating failures are defined as system or component failures that result in the loss of separation between aircraft. Aircraft separation is assured either through procedural or active separation of traffic. Specific implementations of this category of mitigation might be operational or right of way rules or positive separation through air traffic control.
- Facilitate recovery from failures: Mitigation measures that facilitate recovery from failures prevent collisions if a loss of separation occurs. It requires awareness of other traffic and control authority for collision prevention. As a collision is the result of the interaction of two or more aircraft, mitigation can be applied to facilitate avoidance by either aircraft. Collision avoidance can be achieved through active surveillance and maneuvering to avoid other traffic by capabilities onboard the vehicle or through and external operator. The RPAS must be made visible to other air traffic visually, through air traffic control, or by broadcast.
- Reduce the severity of RPAS mid-air impact: Similar to reducing the energy of ground impact, the risk RPAS pose with respect to mid-air collisions could also be mitigated by reducing the severity of the impact. Additionally, the frangibility, or ease of fracture, of the vehicle influences impact loads. Limiting the RPAS characteristics that influence impact loads to certain thresholds could prevent the loss of another aircraft if a collision occurs.

Although the concept of aircraft self-separation has been widely recognized in ICAO and FAA planning documentation, and even approved in limited cases, the concept has never been fully codified in rules or regulation. The requirement that aircraft see and avoid other aircraft to remain well clear and act in accordance with right of way rules and other applicable rules of the air implies aircraft self-separation. Aviation regulators should adopt the concept and define airborne self-separation for unmanned aircraft.

5.2. Risk of collision with the ground

Mitigating the risk of collision with the ground is often ensured by setting certain airworthiness objectives and demonstrating – as part of the airworthiness certification process – that these objectives are met. The EASA policy, which currently applies to RPAS larger than 150 kg – states that airworthiness standards should be set to be no less demanding than those currently applied to comparable manned aircraft nor should they penalise RPAS by requiring compliance with higher standards simply because technology permits. JARUS is defining top level RPAS airworthiness, system safety objectives and guidance material (AMC RPAS.1309) and RPAS recommendations and conclusions on RAS failure classifications in terms of severity definition and probability requirements (expected to apply to RPAS smaller than 150 kg only).

Table 1 shows that the risk of collision with the ground for commercial operations with larger RPAS may be mitigated through reducing the likelihood and/or consequences of occurrence of *twenty* RPAS hazards. For smaller RPAS, within scope of JARUS and possible useful for the quick win ULTRA use cases, the situation may be different. Safety requirements for some (or most of these) hazards may be less stringent, especially in case the flight is above unpopulated area with only potentially minimal damage to properties. In this context, it is noted that damage to equipment, including the RPA, or to third party property may not even have to be considered a safety risk, but only an economic risk which can be mitigated through insurance. Such approach could even imply that the risk of collision with the ground does not have to be considered as safety risk within RPAS risk assessments, in case of flights above unpopulated areas.

In case, the safety risk of collision with the ground has to be considered, it is important to note that – in addition to the hazards already mentioned – two primary causes attributed to a significant portion of current RPAS accidents are electromechanical failure and human error. The likelihood of exposure to harm is influenced primarily by the population characteristics in the area of operation. Based on the work conducted by MIT International Center for Air Transportation, the proposed mitigating measures for different hazards that may lead to the risk of collision with the ground are [46]:

- Reduce the exposure to risk of the public on the ground: One mitigation measure is to limit the operations of the RPAS to reduce exposure of the public on the ground to risk.
    - Approach 1: Limit the operation of RPAS to sparsely populated areas or away from major population centers. This is currently utilized for experimental test flights of military aircraft. This measure protects the public from harm, but also restricts RPAS from operations where they may be most useful.
    - Approach 2: Ensure local control over the exposure of risk to persons on the ground, utilizing a highly precise navigation system that limits the operation of the aircraft to designated areas of low risk. For example, the RPAS's flight path could be limited to operation over waterways, undeveloped land, or above buildings with sufficient sheltering to protect the building occupants from harm.
- Ensure RPAS System Reliability: Mitigation strategies in this area ensure greater system reliability. Improving training and facilitating operation can also reduce the amount of human errors that result in system failures. The increased utilization of software in RPAS systems will require several measures to ensure that the software contributes to system reliability.
- Facilitate Safe Recovery from Failures: By recovering from failures, operation of the system can continue with safety margins reduced, or a sufficient level of control can still be exercised to further mitigate the effects of the failure. Recovery methods can influence the effects of impact by diverting from populated areas if a failure occurs, or initiating additional mitigation systems that reduce the effects of RPAS ground impact.
- Reduce the effects of RPAS ground impact: Ballistic recovery systems could be used to slow the descent of the vehicle, if an uncontrollable failure occurs and flight termination systems offer the possibility of detonating parts of the vehicle while still in the air to reduce the size, energy and therefore potential for harm of debris.

Several factors must be considered regarding active mitigation measures. They require a control ability to detect and activate in the event of a potential vehicle loss, and could initiate an accident by unintended activation. They may not be appropriate for larger RPAS that cannot be slowed to sufficient speed, or would cause more damage with dispersed debris. Measures such as flight termination system effectively destroy the aircraft, which results in a complete financial and functional loss of the system.

6. BUILDING THE SAFETY CASE

A Safety Case is a structured argument that presents evidence intended to demonstrate that a system is as safe as reasonably practicable. A safety case aims to show that specific *safety claims* are met and that risks are kept as low as necessary to meet *safety targets*. Various definitions of “Safety Case” exist:

- The CAA UK [57] uses the term 'Safety Case' in respect of a set of one or more documents that include claims, arguments and evidence that a system is safe. A Safety Case provides all the documentation and references necessary to demonstrate, both to the operator themselves and to the CAA, that a new system or a change to an existing system is tolerably safe and will meet specified Safety Objectives.
- A definition by UK Defence Standard 00-56 Issue 4 [32] states "A Safety Case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment".
- According to EUROCONTROL, a Safety Case is – broadly – “the documented assurance (ie argument and supporting evidence) of the achievement and maintenance of safety. It is primarily the means by which those who are accountable for service provision or projects assure themselves that those services or projects are delivering (or will deliver), and will continue to deliver, an acceptable level of safety”. Such Safety Case “should also provide an adequate means of obtaining regulatory approval for the service or project concerned” and is “a means of structuring and documenting a summary of the results of a Safety Assessment, and other activities (eg simulations, surveys etc.), in a way that a reader can readily follow the logical reasoning as to why a change (or on-going service) can be considered safe.
- The European Operational Concept Validation Methodology (E-OCVM) [33] uses the term “Safety Case in R&D” to refer to “a means of grouping validation results about safety, such that it supports all stakeholders and decision makers as they consider investment and implementation options. The development of such a Safety Case aims to provide them with timely information as evidence concerning the potential of a concept to meet defined safety goals”.

A Safety Case is based on an evidence-based approach, which can be contrasted with a prescriptive approach to safety commonly enforced by safety standards, which require safety to be justified using a prescribed process. Such standards typically do not explicitly require evidence of safety and instead rest on the assumption that by following the prescribed process will ensure safety. For the proposed ULTRA use cases, a prescriptive process most likely does not exist. Building a Safety Case and using a non-prescriptive (i.e. evidence-based) approach to justify safety, may be the only option to obtain the approval.

A Safety Case for an ULTRA use case should identify all relevant (generic) safety requirements that must be satisfied in order to ensure the safe introduction of the envisaged use case, as well as the actual evidence that the safety requirements are met for the specific use case. The approach to set-up the generic safety case and derive the (generic) safety requirements usually follows standard steps:

- Identification of all relevant (regulatory) safety requirements;
- Functional Hazard Assessment (FHA);
- Preliminary System Safety Assessment (PSSA);
- System Safety Assessment (SSA).

A combination of the above mentioned steps could form the basis of a safety case, which is to be complemented by safety evidence showing that risks may be considered *acceptably safe* by authorities.

What may be considered acceptably safe is usually derived from or stated in (safety) regulation. In this context, it is noteworthy that the recently published roadmap for the integration of civil RPAS into the European Aviation System distinguishes several actions within its Annex I “A Regulatory Approach for the integration of civil RPAS into the European Aviation System” that will have to be completed [47]:

- *Civil/military safety objectives for airworthiness (for RPAS of any mass)* (2014-2017), aiming to mitigate the risk to persons on the ground, so as to enable the manufacturing industry to develop platforms potentially purchased by either civil or military customers. EASA to publish an Acceptable Means of Compliance (AMC) for the airworthiness safety objectives for RPAS (‘1309’).
- *Target Level of Safety objectives for ‘Detect and Avoid’ (D&A) and ‘Command and Control’ in the total aviation system (2013)*, aiming to support the introduction of restricted RPAS en-route operations (B-VLOS/RLOS/IFR) in controlled airspace classes A, B, C.
- *Extend the scope of EC Regulation 216/2008 […] and related rules to RPAS comprising RPA of any mass*, on the understanding that below a certain threshold to be determined (e.g. 20-25 Kg or other criteria) there would be no formal airworthiness processes, but only safety assessment of the system, under responsibility of the RPAS operator.

It is stated in Annex II (the ‘Strategic R&D Plan’) of the roadmap for the integration of civil RPAS into the European Aviation System [47] as high level operational requirement that ‘RPAS integration shall not compromise existing aviation safety levels, nor increase risk: the way RPAS operations are conducted shall be equivalent to manned aircraft, as much as possible’. To meet this operational requirement, it will be necessary to develop a methodology for the justification and validation of RPAS safety objectives of the integration in the current ATM environment (short term validation methodology) and the future ATM environment (based on SESAR, integrated in SES and SWIM) (long term validation methodology). Note that this Annex II also mentions the possibility of ‘different safety cases for small RPAS flying in an airspace with limited air traffic giving provisions for less demanding solutions’. Annex II considers it ‘essential to provide data on achievability of safety requirements in light of innovative nature of RPAS operations’. It would be a risk that the available technologies will not be able to meet the safety requirements that will need to be met in order to be acceptably safe for authorities, with the current technological state of the art.

Annex III “A study on the societal impact of the integration of civil RPAS into the European Aviation System” [47] complicates the situation even further, because it seems to motivate that the derivation of acceptable risks/safety may (have to) depend on public acceptance of RPAS applications. For example, this Annex III indicates that there are substantial differences in what risk is measured and what risk is perceived. It is stated that ‘risk perception, and not the objective measure of risk, will be the driver behind the acceptance of RPAS operations in civilian airspace. It is expected that the public will place higher demands on the safety of RPAS operations than that of manned aircraft operations. Distinctions must be made between those RPAS applications where the principal risk exposure is voluntary from those of involuntary risk exposure’. If and how exactly such principles are to be take into account in the establishment of safety requirements and safety objectives (as planned by Annex I) is currently not clear.

During the past years different attempts to build a safety case for RPAS operations have been conducted. None of the attempts has dealt with safety of RPAS operations from a total aviation system point of view. Therefore, it still remains open to put all pieces of the safety puzzle together and obtain an overall view of the safety level of anticipated civil RPAS operations and obtain the required approval from the authorities. As suggested in Annex I of the Roadmap [47], it may be much easier to obtain such approval for the ULTRA use cases if – for RPAS that are below a certain threshold mass – there is no formal airworthiness process needed, but only system safety assessment under the responsibility of the RPAS operator.

7. CONCLUSIONS AND RECOMMENDATIONS

Although RPAS have already been used in segregated airspace where separation from other traffic is assured, many users would like to deploy RPAS in airspace, where other traffic may fly. ULTRA has described expected RPAS operations for a number of ‘quick win’ use cases, which are most likely to be introduced in case required approval by regulatory authorities can be obtained. This study has contributed to the process of obtaining such regulatory approval by providing guidance to produce a ‘Safety Case’. A Safety Case is based on an evidence-based approach, which can be contrasted with a prescriptive approach to safety commonly enforced by safety standards, which require safety to be justified using a prescribed process. Such standards typically do not explicitly require evidence of safety and instead rest on the assumption that by following the prescribed process will ensure safety. For the proposed ULTRA use cases, a prescriptive process most likely does not exist. Building a Safety Case and using a non-prescriptive (evidence-based) approach to justify safety, may be the quickest option to obtain an approval.

This study has identified the main safety aspects, provided suggestions for assessing the safety of RPAS operations, and provided suggestions for the (further) development of mitigating measures. It was concluded that a commonly agreed risk criteria framework for RPAS operations does not yet exist. Such framework, which has to be defined by regulators, is crucial for judging the acceptability of risk. This study provides some guidelines for the establishment of such framework, but the actual implementation should preferably be done jointly by a group that includes EASA, FAA and/or JARUS. It has been motivated that main safety risks to be addressed to ensure that RPAS use cases can be introduced without degrading safety are *risks to other airspace users* and *risks to people/property on the ground*. It will be necessary to show that these risks do not increase compared to the current situation with manned aircraft only.

A variety of methods are being used (and/or are still under further development) to assess the safety of RPAS operations. The methods used include the EUROCAE ED-78A (which is consistent with the RTCA/DO-264), the EUROCONTROL Safety Assessment Methodology, and similar methods to derive Safety Objectives and Safety Requirements. Most of these safety risk assessment methodologies for RPAS operations include (or recognize a need for) the following core elements: Hazard Identification, Setting of Safety Objectives, and Determination of Safety Requirements. Usually this is recommended through a FHA and PSSA. New safety methods – potentially applicable to assess the safety of RPAS operations – are also under (further) development and application. The FAST/EME1.1 methodology, which has been developed with support of EASA, describes a proposed risk assessment process that may be useful for assessing the safety risks of expected RPAS operations in a future environment. NLR has further developed and applied the CATS, which was originally developed for the Dutch Civil Aviation Authorities for understanding the causal factors underlying the hazards and risks (and their relation to possible consequences) related to commercial air transport operations, to derive a baseline for RPAS command and control related hazards. Application of the FAST/EME1.1 and CATS method to newly proposed changes in the aviation system is also currently foreseen within EC Project ASCOS (Aviation Safety and Certification of new Operations and Systems), which is coordinated by NLR.

Concerning the scope of the risk assessments, it is observed that - so far - no European study has dealt with the safety of RPAS operations from a total aviation system point of view. USICO focuses on the definition of safety objectives related to RPAS airworthiness, and excludes the segregation of aircraft and collision avoidance requirements. INOUI and the EUROCONTROL ATM integration safety studies focus on the ATM related safety risks (i.e. collisions between aircraft, collisions between aircraft and vehicles, and wake vortex encounters) and exclude airworthiness related safety issues. An initial EASA study on RPAS safety focuses purely on the safety of RPAS communications. NLR safety studies dealt with the risk of collision with the ground, RPAS detect and avoid systems, and loss of the data link for command and control (often assuming commercial operations with a fixed wing RPAS). It remains open to put all pieces of the safety puzzle together and obtain an overall view of the safety level of expected RPAS operations.

Beside the complex and long ongoing process to set up ways to routinely operate UAS in the airspace over population, preliminary RPAS operations can be authorized for scenarios that do not create any hazard to other airspace users and populations (e.g. VLOS over identified zones). These operations will enable the RPAS community to gain experience, and sense of realism, whereas regulators will gain confidence providing RPAS designers do a good job in proposing adequately safe RPAS and operators make a reasonably safe use of their system depending on their skills, system capabilities and implemented functions. It is possible, and maybe even likely, that the important feature of unmanned aircraft of not having its pilot at risk will be used for ever to perform restricted operations with system having a safety level adequately adjusted to their use.

Legal notice *:*

The ULTRA project is co-funded under the European Community's Seventh Framework Programme (FP7/2007-2013) under the grant agreement n° 314680 (Aeronautics Research). The views expressed in this report are the sole responsibility of the authors and do not necessarily reflect the views of the European Commission.
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the information.

END OF DOCUMENT