HORIZON 2020

PROJECT MANAGEMENT AND QUALITY ASSURANCE PLAN

ROBORDER
740593

Deliverable Information
Deliverable Number: D8.1 **Work Package:** 8
Date of Issue: 31/07/2017
Document Reference: 740593-ROBORDER-Project_Management_Plan
Version Number: 1.0
Nature of Deliverable: Report **Dissemination Level of Deliverable:** Public
Author(s): TEKEVER (Responsible).
Keywords: Project planning and organization, Quality assurance, Consortium description, Management procedures, Risk assessment and mitigation, Communication and dissemination activities, Ethics requirements.
Abstract:
This document complements the project information already provided in the Grant Agreement Description of Action. The Project Management Plan provides a more detailed planning of the project, describes the project's communication and dissemination plans, addresses ethics requirements and explains the management structure, processes to be followed by the consortium during the execution of the project. Moreover, this document presents the procedures and measures to ensure maximum quality of ROBORDER's results and detect or prognosticate quality flaws.

Document History

Date	Version	Remarks
25/06/2017	0.1	Skeleton
28/07/2017	0.2	First Complete Version
31/07/2017	1.0	Issue

Document Authors

Entity	Contributors
TEK-AS	André, OLIVEIRA Filipe, RODRIGUES João, CARVALHO

Executive Summary

The ROBORDER Project Management Plan complements the project information provided in the Grant Agreement Description of Action by describing the planning, schedule, organization of the consortium, management procedures, risk assessment and mitigation, the quality assurance, communication and dissemination activities, and ethics requirements at a level of detail suitable for the project.

This document describes the consortium partners and their roles in the project, explains the project objectives, the decision bodies and decision making processes to be used as well as tools to be used in the daily management and coordination of project activities.

The risk management plan is reviewed and updated in relation to the one presented at proposal stage. The PMP shows there are no ethical concerns as per the result of the consortium's ethics self-assessment.

Detailed planning for the project's execution is given in the form of a Gantt chart, a TRL roadmap and a development roadmap.

Moreover, the PMP establishes the project's communication and exploitation and dissemination plans which define target audiences and messages and identify the preferred communication channels.

Finally, the PMP defines the measures to be taken in case of detected or prognosticated quality flaws, as well as the quality assurance responsibilities.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Meaning
C4I	Command, Control, Communication, Computers and Intelligence
CA	Consortium Agreement
CESS	Centre for European Security Strategies
CISE	Common Information Sharing Environment
CO	Confidential
DoA	Description of Action
DSL	Domain-Specific Language
EAB	External Advisory Board
EC	European Commission
EDA	European Space Agency
ENFSI	European Network of Forensic Science Institutes
ETAB	Ethics Advisory Board
EU	European Union
GA	Grant Agreement
GPS	Global Positioning System
IA	Innovation Action
ICC	International Chamber of Commerce
IEEE	Institute of Electrical and Electronics Engineers
IM	Innovation Manager
INTERPOL	International Criminal Police Organization
IO	Innovation Objective
IP	Intellectual Property
IPR	Intellectual Property Rights
LEA	Law Enforcement Agency
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
PC	Project Coordinator
PMB	Project Management Board
PMP	Project Management Plan
POC	Point of Contact
PSO	Project Security Officer
PU	Public
RES_EU	Restreint EU / EU Restricted
RF	Radio Frequency
SAB	Security Advisory Board
SME	Small and Medium Enterprise
STM	Scientific and Technical Manager
TBD	To Be Determined
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
UxV	Unmanned Vehicle
WP	Work Package
WPL	Work Package Leader

Table 1 – List of acronyms

1 Introduction

The ROBORDER Project Management Plan (PMP) aims to complement the project information provided in the Grant Agreement Description of Action by describing the planning (Gantt chart), organization of the consortium, management procedures, risk assessment and mitigation, quality assurance, communication and dissemination activities, and ethics requirements at a level of detail suitable for the project.

The PMP has been prepared in such way that its content does not contradict the Grant Agreement. If any contradiction exists, the text of the Grant Agreement shall prevail over what is written in this document.

The PMP will be used as a reference document by the consortium and as a daily tool by the coordinator. Whenever doubts arise concerning the way of working of the consortium, planned communication activities, project risks (e.g. how to identify and monitor them) or the project Gantt, partners can refer to this document for explanations.

This document is organized in the following sections:

- **Introduction** – this section.
- **Organisation** – this provides insights into the consortium's composition, the roles of each partner entity as well as contacts for the key personnel involved in the project.
- **Gantt Chart** – this section provides a detailed Gantt chart for the project, a TRL roadmap and project deliverables.
- **Management plan** – the management plan section recalls the project objectives and its scope, describes the decision bodies and decision making processes as well as the daily tools to be used in the management and coordination of the project activities. In addition, this section also establishes a preliminary development roadmap.
- **Risk and Issues management plan** – this section covers the risk management and explains the processes to be used in flagging a risk, classifying it and monitoring it.
- **Communication Plan** – establishes the communication objectives for the project, defines target audiences and main high level messages, describes the procedures to be used and identifies the preferred communication channels. The section concludes with a calendar for communication activities and a description of the metrics to be used in evaluating the effectiveness of communication activities.
- **Exploitation and dissemination Plan** – this section covers the preliminary individual exploitation plans of partners and the ROBORDER value chain.
- **Ethics requirements** – the final section covers ethics issues and presents the ethics self-assessment performed by the consortium.

2 Organisation

The ROBORDER consortium comprises twenty five entities from fourteen different countries in Europe. A small description of each member of the consortium, their expertise and role within the ROBORDER project is presented below:

- **TEKEVER AS** (TEK-AS), a Small and Medium Enterprise (SME) from Portugal, is an Original Equipment Manufacturer (OEM) of autonomous systems and subsystems, as well as developer of creative disruptive technologies for the corporate, SME, aerospace, defence and security markets. TEK-AS is ROBORDER's coordinator, responsible for leading WP5 and participates in WP2, WP3 and WP7 by leading tasks T2.1, T3.5 and T7.6. Last, TEK-AS is involved in the prototype evaluation in WP6 and in the dissemination activities of WP7 supporting the organization of the 1st Workshop led by GNR in cooperation with MJ.

- **Ethniko Kentro Erevnas Kai Technologikis Anaptyxis** (CERTH), a research and technology organisation from Greece that includes the Information Technologies Institute (ITI) from which CERTH participates in this project with two different research groups (MKLab and ConvCao). CERTH leads WP4, participates in WP3 and WP7 by leading tasks T3.1, T3.2 and T7.2. Moreover, CERTH will be involved in the system integration activities of WP5, the prototype demonstration and evaluation in WP6 and the dissemination activities of WP7 supporting the organization of the 2st Workshop led by HMOD.

- **Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V.** (FHR), a research and technology organisation from Germany, it is highly involved in applied research that drives economic development and serves the wider benefit of society. In the project, FHR participates in WP2 leading T2.2 and also contributes in WP5 working on the integration of the passive radar, in WP6 involved in the prototype evaluation and in dissemination activities of WP7.

- **Sisekaitseakadeemia** (EASS), a research and education centre from Estonia, is a state institution that provides professional education for professional education for civil servants belonging in the area of government under the Estonian Ministry of the Interior. In ROBORDER, EASS contributes to WP1 in the development of end-user requirements, to WP6 in end-user validation and testing, as well as to WP7 in dissemination activities.

- **Teknologian tutkimuskeskus VTT Oy** (VTT), a research and technology organisation from Finland, it is the leading research technology company in the Nordic countries and has a national mandate in Finland. In the project, VTT is involved in WP1 and WP4 by leading tasks T1.5 and T4.1 respectively. Also, VTT contributes to WP5 in the system integration activities, to WP6 in the prototype demonstration and in dissemination activities of WP7.

- **EVERIS SPAIN SL** (EVERIS), a private multi-national consulting company from Spain, provides to its clients comprehensive business solutions covering all aspects of the value chain from business strategy to systems implementation. In ROBORDER, EVERIS is the leader of WP7 and contributes to WP5 by leading task T5.2 that deals with the software integration. Moreover, EVERIS will perform the ROBORDER systems' integration and maintenance in the testing environment along with TEK-AS.

- **Police Service of Northern Ireland** (PSNI), a police service and non profit government body from Northern Ireland, it is a Law Enforcement Agency (LEA) with responsibility for policing and security. PSNI is involved in WP1 by contributing to the development of end-user requirements, as well as providing end-user feedback in the development of technical solutions through various WPs. Additionally PSNI contributes to WP6 in the prototype evaluation.

- **Ministério da Administração Interna** (GNR), a public body from Portugal, is a security force that leads task T6.4 regarding the prototype demonstration and evaluation for marine border threats. Moreover, GNR contributes to WP1 in the specification of user requirements and pilot use cases, as well as to WP7 in the dissemination activities organizing the 1st ROBORDER Workshop in collaboration with PJ and with the support of TEK-AS.

- **NATO Science and Technology Organisation** (CMRE), a research centre from Belgium that deals with multiple disciplines including ocean and environmental sciences. In ROBORDER, CMRE is the leader of WP6 and participates in WP7 by leading task T7.3. Additionally, CMRE contributes to WP1 in the definition of end-user requirements and to WP7 in dissemination activities.

- **Orszagos Rendor – Fokapitanysag** (ORFK), a public body from Hungary, is the only police agency in Hungary. In the project, ORFK is the leader some tasks of WP1 and WP6, respectively T1.3, T6.2 and T6.5. Also, ORFK participates in WP1 with contributes for the end-user requirements and in dissemination activities of WP7.

- **Robotnik Automation SLL** (ROBOTNIK), an SME from Spain, is currently a leading company in the European service robotics market. ROBOTNIK participates in WP2 by leading task T2.5. Moreover, ROBOTNIK is involved in the system integration tasks of WP5, in the protype demonstration and evaluation of WP6 and in exploitation activities of WP7.

- **Serviciul de Protectie Si Paza** (SPP), a Law Enforcement Agency from Romania, participates in the project as an active end-user partner. SPP participation comprises contributions for WP1 with the identification of end-user requirements, as well as feedback regarding the test scenarios and field validation for WP6. Ultimately, SPP is involved in dissemination activities in WP7 with the organization of a user day in collaboration with RBP.

- **Elettronica GMBH** (ELTM), a company from Germany, has systems engineering capabilities including the development, production and system integration, thus having a leading role in the group for design and provision of electronic systems for civilian and Public Security applications. In the project, ELTM is the leader of WP2 by leading tasks T2.3 and 2.5. Also, ELTM contributes to WP3 in task T3.5 that aims at the developing of a detection system for malicious and illegal emissions based on the passive microwave payload. Last, ELTM is involved in WP6 and WP7 with, respectively, the prototype demonstration and evaluation and the exploitation activities.

- **Ministry of National Defence, Greece** (HMOD), a public body from Greece, is the responsible entity for applying the Greek Government's National Defence Policy. In ROBORDER, HMOD is the leader of WP1 and is involved in WP7 by coordinating task T7.1 and organising the 2nd ROBORDER Workshop at the end of the project in

collaboration with CERTH. Moreover, HMOD contributes to the end-user validation and testing activities of WP6.

- **Sheffield Hallam University** (CENTRIC), a research and technology organisation from the UK, focuses in providing a platform for researchers, practioners, policy makers and public to develop research in the Security domain. In the project, CENTRIC provides support to tasks T4.4 and T4.6 of WP4. Additionally, CENTRIC contributes to the activities of WP3, WP5, WP6 and WP7.

- **Autorita Portuale Livorno** (APL), a public body from Italy, is responsible for the guidance, planning, coordination, promotion and control of port operations. In ROBORDER, APL is in charge of hosting a pilot installation related to “Early and effective identification of passive boats moving ashore. Moreover, APL contributes to the definition of end-user requirements in WP1 and in the dissemination activities of WP7.

- **OceanScan – Marine Systems & Technology LDA** (OMST), a private company from Portugal, that is devoted to the development, manufacturing and commercialization of small-sized Autonomous Underwater Vehicles. OMST brings for ROBORDER its unmanned platforms for both surface and underwater, contributing actively for task T2.5 in WP2 and other robotic platform-related tasks. Additionally, OSMT is involved in system integration tasks of WP5, the prototype demonstration and evaluation in WP6 and the exploitation activities of WP7.

- **Institut Po Otbrana** (BDI), a research institute from Bulgaria, is the main scientific-research, testing, design and expert-technical structure in the Ministry of Defence of the Republic of Bulgaria. In the project, BDI participates in WP1 by leading task T1.2 and contributing to the remaining tasks of the WP. Also, BDI is responsible for running a pilot scenario in WP6 about the Unauthorized land border crossing and signals” and contributes for dissemination activities of WP7.

- **Copting GMBH** (Copting), an SME from Germany, is a full service provider for UAV operations (consulting, operations, construction, training and research). Copting brings to the project its unmanned vehicle equipment and works in collaboration with other robotic platform partners in WP2 for task T2.5, as well as in other robotic platform-related tasks. Additively, Copting is involved in the system integration tasks of WP5, the prototype demonstration and evaluation in WP6 and the exploitation activities of WP7.

- **Ethniko Kai Kapodistriako Panepistimio Athinon** (UoA), a research institute from Greece, participates in the project through the Pervasive Computing Research Group part of the Communication Networks Laboratory of Department of Informatics and Telecommunications. In ROBORDER, UoA is the leader of T4.2 and T4.5 in WP4 and contributes to other WP4 and WP5 tasks. Ultimately, UoA is involved in activities related to prototype demonstration and evaluation in WP6 and to dissemination activities in WP7.

- **Centre Suisse d’Electronique et de Microtechnique SA – Recherche et Developpement** (CSEM), a research and technology organization from Switzerland, is specialized in microtechnology, nanotechnology, microelectronics, systems engineering and communications technologies. It offers its customers and industry partners tailor made innovative solutions based on its technological expertise from applied research. In collaboration with CNIT, CSEM is involved in task T2.6 of WP2,

in system integration activities of WP5, the prototype demonstration and evaluation in WP6 and in activities of WP7.

- **Consorzio Nazionale Interuniversitario per le Telecomunicazioni** (CNIT), a research centre from Italy, promotes and coordinates research in telecomunications on topics such as telecomunications networks, telematics, intelligent transport systems, and others. The role of CNIT in ROBORDER is to participate in WP2 and WP3 by leading tasks T2.6, T3.1 and T3.2. Moreover, CNIT is involved in the prototype demonstration and evaluation activities of WP6 and in the dissemination activities of WP7.

- **Ministério da Justiça** (MJ), a Law Enforcement Agency from Portugal, is the responsible entity for Policia Judiciária which consists in an higher police body. In the project, MJ is responsible for running and evaluating a pilot scenario related to "Detection of marine pollution incidents". Also, MJ contributes in the specification of end-user requirements and pilot use cases in WP1 and in dissemination activities in WP7.

- **Capritech Limited** (CPT), an SME from the UK, is specialized in cyber security and privacy engineering. In ROBORDER, CPT is involved in WP3 by leading tasks T3.4 and participating in T3.5. In addition, CPT is involved in the system integration activities of WP5, the prototype demonstration and evaluation in WP6 and in the dissemination activities of WP7.

- **Inspectoratul General Al Politiei de Frontiera** (RBP), a public body from Romania, is the single authority responsible for border control at all Romanian borders with centralized organization at national, regional and local level. In the project, RBP is an active contributor for the identification of end-user requirements in WP1, as well as test scenarios and field validation in WP6 and dissemination activities in WP7. In particular, RBP along with SPP are responsible for the design and evaluation of a pilot scenario regarding "Detection of terrorist attack coming through cross border".

Partner	Competences	Role in the project
TEK-AS	- Project Management - UAV systems - Communication systems - System integration	- Financial, administrative, technical and ethical management - Illegal communications detection - System integration
CERTH	- Visual recognition of objects/activities - Multimodal sensor fusion - Semantic interoperability and representation - Integration and reasoning - Visual analytics - Decision support systems - Intelligent control	- Low level sensor data fusion - CISE-compliant representation model - Visual analytics and decision support algorithms - Communication and dissemination
FHR	- Electromagnetic sensors in the field of radar and radiometry - Innovative signal processing methods - Innovative technology from microwave to the lower terahertz region	- Optimized passive radar on-board UAVs and UGVs
EASS	- Internal security and safety - Virtual reality, augmented reality - Massive data visualization and analysis	- Ethical and legal requirements - User requirements for border surveillance - Security requirements - Design of pilot test cases

Partner	Competences	Role in the project
VTT	- Human-machine interaction - Virtual / augmented reality - Communications and antennas - Networks and cyber-security - Renewable energies	- Design and concept of operations for the use cases - Novel human-robot interface with immersive 3D virtual reality environment and/or augmented reality interface
EVERIS	- Business consulting - Corporate strategy - Process engineering	- Dissemination and exploitation - Market analysis definition - Business models definition
PSNI	- Public order and crowd management - Counter terrorism investigation - Emergency planning and disaster management - Human Rights focused policing	- User requirements for border surveillance - Security requirements - Ethical and legal requirements - Design of pilot test cases
GNR	- International peace-keeping - Maintenance of public order - Support and rescue - Combat fiscal infringements	- User requirements for border surveillance - Security requirements - Ethical and legal requirements - Design of pilot test cases - Demonstration of pollution and other illegal events in border use case
CMRE	- Acoustic signal processing - Physical and dynamic oceanography - Maritime autonomous vehicles - Interoperability architecture and standards - Systems validation and testing	- End-user evaluation plans and methodology based on requirements and use-case scenarios - Standardization and collaboration with other projects
ORFK	- Law-enforcement - Public policing - Criminal investigation - Traffic policing - Border control	- User requirements for border surveillance - Security requirements - Ethical and legal requirements - Design of pilot test cases - Demonstration of ROBORDER in the land border use-case
ROBOTNIK	- Robotics - Unmanned ground vehicles - Artificial Intelligence	- Re-configuration of agents, carriers and charging solutions for diverse weather and conditions
SPP	- Protection of national and foreign dignitaries - Counter terrorism - Border control	- User requirements for border surveillance - Security requirements - Ethical and legal requirements - Design of pilot test cases
ELETTRONICA	- Sensor systems and payloads for surveillance, interception and signal analysis - Scenario modelling and simulation - Data fusion	- Passive RF signal sensor - Optimization sensors for a variety of situations and conditions
HMOD	- Naval and aero-naval operations - Maritime surveillance, intervention and reaction - Maritime Search and rescue	- Border surveillance user requirements - Security, ethical and legal requirements - Design of pilot test cases - Demonstration of pollution and other illegal events
CENTRIC	- Counter terrorism knowledge - Resilience and security risk assessment - Big data and intelligence management - National security	- Detection and identification of border-related threats - Command and control unit functionalities

Partner	Competences	Role in the project
APL	- Port operations - Port safety and security - Digitalisation and convergence of harbour information in virtual platforms	- User requirements and pilot use cases - Demonstration and evaluation
MST	- Autonomous underwater vehicles - Acoustic navigation - Acoustic communication	- Adaptive sensing, robotics and communication technologies to operational and environmental needs
BDI	- Military techniques - Logistics equipment - C4I systems - Cyber security - Telecommunications	- User requirements and pilot use cases - Demonstration and evaluation
Copting	- Unmanned aerial vehicles - Anti-jamming and EMV systems	- Adaptive sensing, robotics and communication technologies to operational and environmental needs
UoA	- Pervasive computing - Semanics-based navigation - Telecommunications - Data networks - Multimedia applications	- DSL-based missions specification - Risk models
CSEM	- Microtechnology - Nanotechnology - Microelectronics - Systems engineering - Communications Technologies	- Adaptive sensing, robotics and communication technologies to operational and environmental needs
CNIT	- Multimedia communications - Radar and surveillance systems - Photonic Networks	- Photonics-based radars - Detection of pollution incidents - Identification of illegal activities
MJ	- Criminal prevention and investigation - Cyber crime and terrorism - State security offences and terrorism - Narcotraffic - Money counterfeiting - Corruption	- User requirements for border surveillance - Security requirements - Ethical and legal requirements - Design of pilot test cases
CPT	- Cybersecurity and privacy engineering - Software development - Business consulting - IT research	- Detection and clarification framework for recognising cyber and cyber-physical attacks
RBP	- Border surveillance - Information management - Risk analysis - Decision support	- User requirements for border surveillance - Security requirements - Ethical and legal requirements - Design of pilot test cases

Table 2 – Partners expertise and roles in the project

The key personnel involved in this project is listed below:

Partner	Personnel	Role in the project	E-mail
TEK-AS	André Oliveira	Project coordinator; Dissemination and exploitation manager; PMC chairman; Legal, contractual and financial point of contact; WP leader	andre.oliveira@tekever.com
	Filipe Rodrigues	Coordination team	filipe.rodrigues@tekever.com
	João Carvalho	Coordination team	joao.carvalho@tekever.com
	Pedro Petiz	Technical team coordinator	pedro.petiz@tekever.com
CERTH	Stefanos Vrochidis	PMB Member	stefanos@iti.gr
	Elias Kosmatopoulos	PMB Member	kosmatop@iti.gr
	Christos Ravanis		cravanis@iti.gr
	Iakovos Michailidis		michaild@iti.gr
	Panos Michailidis		panosmih@iti.gr
	Kiki Alexandridou		kikialexan@iti.gr
	Villy Kokkinou		villyko@iti.gr
	Christos Korkas		chriskorkas@iti.gr
	Thanasis Kapoutsis		athakapo@iti.gr
	Anna Satsiou		satsiou@iti.gr
	Kostas Ioannidis		kioannid@iti.gr
	Yiannis Kompatsiaris		ikom@iti.gr
	Alexia Briassouli		abria@iti.gr
	Kostas Avgerinakis		koafgeri@iti.gr
	Maria Papadopoulou		marpap@iti.gr
	Stauros Taxos		staxos@iti.gr
FHR	Diego Cristallini	PMB Member	diego.cristallini@fhr.fraunhofer.de
	Heiner Kuschel		heiner.kuschel@fhr.fraunhofer.de
	Thomas Bertuch		thomas.bertuch@fhr.fraunhofer.de
	Frank Weinmann		frank.weinmann@fhr.fraunhofer.de
	Stefano Turso		stefano.turso@fhr.fraunhofer.de
	Monika Flor		monika.flor@fhr.fraunhofer.de
	Bettina Von Hagens		bettina.von.hagens@zv.fraunhofer.de

Partner	Personnel	Role in the project	E-mail
FHR	Vesna Meyer zu Schweicheln		vesna.meyer.zu.schweicheln@zv.fraunhofer.de
EASS	Marek Link	PMB Member	Marek.Link@sisekaitse.ee
	Katrin Pihl		katrin.pihl@sisekaitse.ee
	Liisa Soosuu		liisa.soosuu@sisekaitse.ee
VTT	Kaj Helin	PMB Member	Kaj.Helin@vtt.fi
	Jari Laarni		Jari.Laarni@vtt.fi
	Jari Kiviaho		jari.kiviaho@vtt.fi
	Sirkku Hoikkala		sirkku.hoikkala@vtt.fi
EVERIS	Emmanuel Jamin	PMB Member	emmanuel.jean.jacques.jamin@everis.com
	Miguel Gomez		miguel.angel.gomez@everis.com
	Arnau Roca Palà		arnau.roca.pala@everis.com
	David Lopez López		david.lopez.lopez@everis.com
PSNI	Jonathan Middleton	PMB Member	Jonathan.Middleton@psni.pnn.police.uk
	Una Williamson		Una.Williamson@psni.pnn.police.uk
GNR	Jorge Roma		roma.jfre@gnr.pt
	Nuno Rosário	PMB Member	rosario.nms@gnr.pt
	Paulo Silvério		dperi@gnr.pt
CMRE	Alberto Tremori	PMB Member	Alberto.Tremori@cmre.nato.int
	Pilar Caamano Sobrino		Pilar.Caamano@cmre.nato.int
	Arnau Carrera Vinas		Arnau.Carrera@cmre.nato.int
	Alessandra Barbieri		Alessandra.Barbieri@cmre.nato.int
ORFK	Szekely Zoltan	PMB Member	Szekely.Zoltan@uni-nke.hu
ROBOTNIK	Rafael López	PMB Member	rlopez@robotnik.es
	Raúl Sebastiá		rsebastia@robotnik.es
	Miquel Cantero		mcantero@robotnik.es
SPP	Radan Mircea	PMB Member	radan.mircea@spp.ro
	Roman Razvan		roman.razvan@spp.ro
	Costache Adrian		costache.adrian@spp.ro
	Buric Marian		buric.marian@spp.ro
ELTM	Massimo Sciotti	PMB Member	m.sciotti@elettronica.de
	Francesco Belfiori		f.belfiori@elettronica.de
	Mariano Pamies		m.pamies@elettronica.de
	Sascha Gräbenitz		s.graebenitz@elettronica.de
HMOD	Vasilios Bousis	PMB Member	vmpousis@dideap.mil.gr

Partner	Personnel	Role in the project	E-mail
HMOD	Sotirios Glykofrydis		sglikofridis@dideap.mil.gr
	Panagiotis Tzortzis		ptzortzis@dideap.mil.gr
	Alexiadis Petros		head@dideap.mil.gr
CENTRIC	Babak Akhgar	PMB Member	b.akhgar@shu.ac.uk
	Tony Day		t.day@shu.ac.uk
	Helen Gibson		h.gibson@shu.ac.uk
	Dave Szwejkowski		d.szwejkowski@shu.ac.uk
APL	Antonella Querci	PMB Member	querci@porto.livorno.it
	Francesco Papucci		f.papucci@portauthority.li.it
	Francescalberto De Bari		f.debari@porto.livorno.it
OMST	Alexandre Sousa		alex@oceanscan-mst.com
	Luis Madureira	PMB Member	lmad@oceanscan-mst.com
BDI	Todor Tagarev		t.tagarev@di.mod.bg
	Nikolai Stoianov	PMB Member	n.stoianov@di.mod.bg
	Maya Bozhilova		m.bozhilova@di.mod.bg
	Borislav Genov		b.genov@di.mod.bg
	Hristo Hristov		h.hristov@di.mod.bg
	Grigor Velev		g.velev@di.mod.bg
Copting	Christian Kaiser	PMB Member	ckaiser@copting.de
UoA	Stathes Hadjiefthymiades	PMB Member	shadj@di.uoa.gr
	Vassilis Papataxiarhis		vpap@di.uoa.gr
	Sarantis Paskalis		paskalis@di.uoa.gr
	Spyros Bolis		sbolis@noc.uoa.gr
CSEM	Emmanuel Onillon		Emmanuel.Onillon@csem.ch
	Steve Lecomte	PMB Member	Steve.LECOMTE@csem.ch
	Stefano Maglie		stefano.maglie@csem.ch
CNIT	Antonella Bogoni		antonella.bogoni@cnit.it
	Salvatore Maresca		salva.maresca@gmail.com
	Elisa Razzoli	PMB Member	elisa.razzoli@cnit.it
	Maria Grazia Carrai		mgcarrai@gmail.com
	Paolo Ghelfi		paolo.ghelfi@cnit.it
	Antonio Malacarne		antonio.malacarne@cnit.it
	Nuno Matos		nuno.matos@pj.pt
	Berta Santos	PMB Member	berta.santos@pj.pt

Partner	Personnel	Role in the project	E-mail
MJ	Teresa Porcio		teresa.porcio@pj.pt
	Manuela Cabral		manuela.cabral@pj.pt
CPT	Irene Karapistoli	PMB Member	irene.karapistoli@capritech.co.uk
	George Loukas		george.loukas@capritech.co.uk
	Grant Millar		grant.millar@capritech.co.uk
RBP	Bogdan-Mihail Ivănescu		bogdan.ivanescu@mai.gov.ro
	Petre-Horia Cincan		horia.cincan@mai.gov.ro
	Dacia-Marieta Ardeleanu		dacia.ardeleanu@mai.gov.ro
	Ionel Fieraru		ionel.fieraru@mai.gov.ro
	Richeard-Sebarstian Mitu		richeard.mitu@igpf.ro
	Gabriela Gheorghe		gabriela.gheorghe@igpf.ro
	Florin Ilie		florin.ilie@igpf.ro
	Ion Deaconu		piu_gibp@mai.gov.ro
	Cristian Popa		cristian.popa@igpf.ro
	Mihai-Cristian Bacinschi		mihai.bacinschi@mai.gov.ro
	Costel Giuroiu	PMB Member	costel.giuroiu@igpf.ro

Table 3 – ROBORDER's key personnel

The project is divided into nine (9) work packages (WP), each one leaded by a different member of the consortium. This information is present below:

- WP1 – User requirements and pilot use cases (HMOD)
- WP2 – Sensing, robotics and communication technologies (ELTM)
- WP3 – Detection and identification of border-related threats (CNIT)
- WP4 – Command and control unit functionalities (CERTH)
- WP5 – Integration of ROBORDER platform for the remote assessment of border threats (TEK-AS)
- WP6 – Demonstrations and evaluation (CMRE)
- WP7 – Dissemination and exploitation (EVERIS)
- WP8 – Project management (TEK-AS)
- WP9 – Ethics requirements (TEK-AS)

As described later on in subsection 4.3, the main decision body of the project is the Project Management Board (PMB). The members of the PMB are identified in Table 3 and repeated below for convenience:

- PMB Chairman – André Oliveira (TEK-AS)
- PMB Member – Elias Kosmatopoulos (CERTH)
- PMB Member – Stefanos Vrochidis (CERTH)
- PMB Member – Diego Cristallini (Fraunhofer FHR)
- PMB Member – Bettina Von Hagens (Fraunhofer ZV)
- PMB Member – Marek Link (EASS)
- PMB Member – Kaj Helin (VTT)
- PMB Member – Emmanuel Jacques Jamin (EVERIS)
- PMB Member – Jonathan Middleton (PSNI)
- PMB Member – Nuno Rosário (GNR)
- PMB Member – Alberto Tremori (CMRE)
- PMB Member – Szekely Zoltan (ORFK)
- PMB Member – Rafael López (ROBOTNIK)
- PMB Member – Radan Mircea (SPP)
- PMB Member – Massimo Sciotti (ELTM)
- PMB Member – Vasilios Bousis (HMOD)
- PMB Member – Babak Akhgar (CENTRIC)
- PMB Member – Antonella Querci (APL)
- PMB Member – Luís Madureira (MST)
- PMB Member – Nikolai Stoianov (BDI)
- PMB Member – Christian Kaiser (Copting)
- PMB Member – Stathes Hadjiefthymiades (UoA)
- PMB Member – Steve Lecomte (CSEM)
- PMB Member – Elisa Razzoli (CNIT)

- PMB Member – Berta Santos (MJ)
- PMB Member – Irene Karapistoli (CPT)
- PMB Member – Costel Giuroiu (RBP)

3 Project Gantt

A detailed Gantt chart for the ROBORDER project is provided in the next page. The following should be noted when considering the Gantt:

- Each task will comprise two periods: a period to carry out the technical activities described in the Description of Action (DoA) of the contract and a period to compile results, prepare and submit, if applicable, any deliverable.
- Five milestones are scheduled. These correspond to critical points of the project as well as to periodic reviews.
- Submission of deliverables is scheduled to take place two (2) weeks before each milestone
- Periodic technical and financial reports drafts compiling information about each period are prepared and submitted two (2) weeks before each milestone
- Periodic reviews are proposed to take place as soon as possible after each milestone.
- Submission of the final periodic technical and financial reports takes place up to four (4) weeks after the periodic review occurs.
- Submission of the final deliverables is done up to the official conclusion date of the project (30th April 2020).

The Project close out meeting is proposed to take place two (2) weeks after the official close of the project. The consortium explicitly acknowledges the fact that any costs incurred after 30th April 2020 (including but not limited to travel costs to participate in the review or changes to deliverables depending upon the assessment reservations) are not eligible and will be at the own expense of the partners.

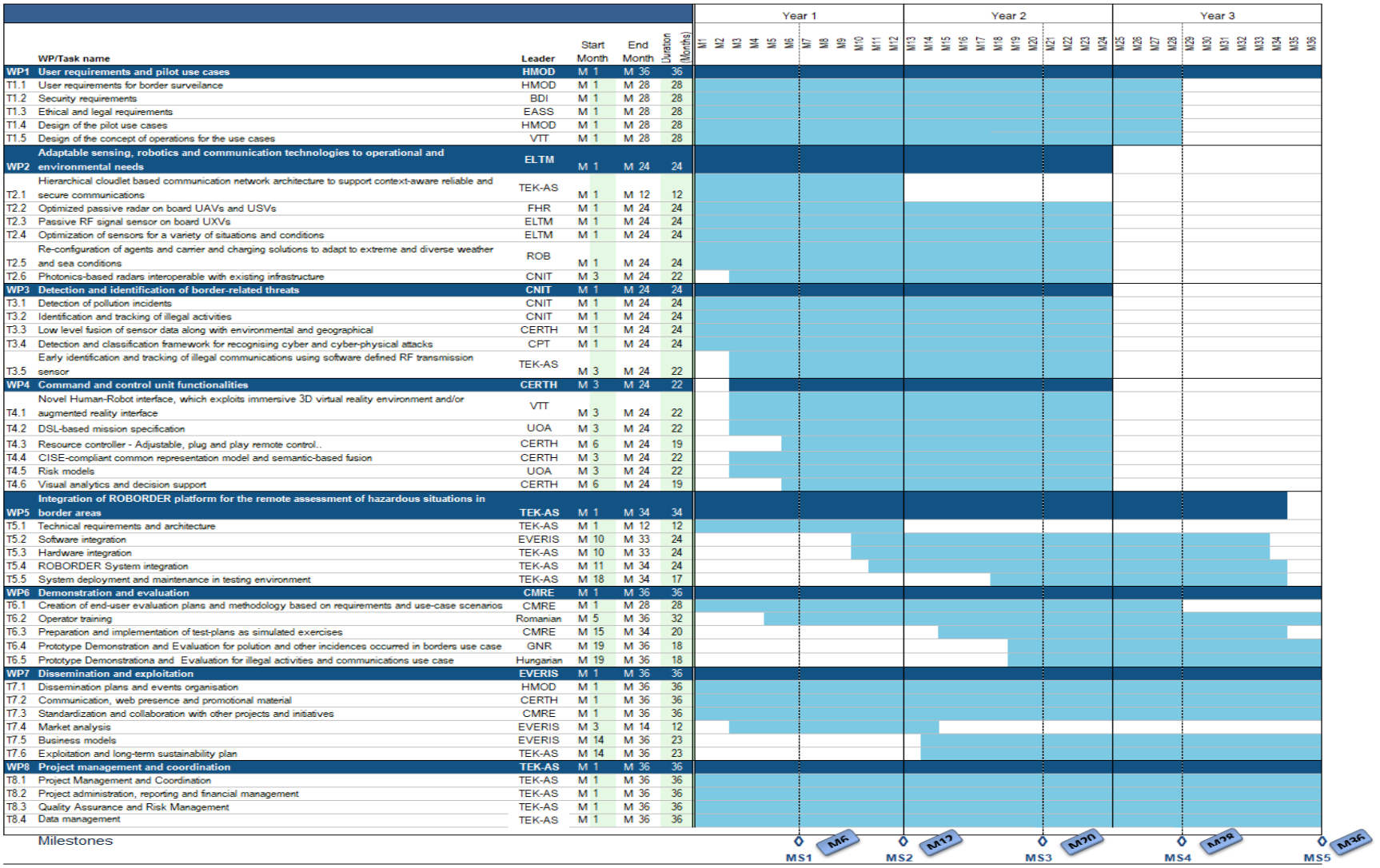

Figure 1 – ROBORDER Gantt Chart

Table 4 presents the list of deliverables due in the project and is provided here as reference to support the analysis of the Gantt charts presented in the previous page. Each leader is expected to distribute, to the rest consortium members, the content he is responsible for, until the last day of the month present in Table 4.

No.	Deliverable name	WP	Leader	Type	Diss. level[1]	Due date (months)	Due date (mm/yyyy)
D7.1	Dissemination Plan	7	HMOD	R	PU	3	07/2017
D7.2	ROBORDER Website and communication material	7	CERTH	R	PU	3	07/2017
D8.1	Project management and quality assurance plan	8	TEK-AS	R	PU	3	07/2017
D9.1	POPD – Requirements No. 10	9	TEK-AS	ETHICS	CO	3	07/2017
D9.2	NEC – Requirements No. 21	9	TEK-AS	ETHICS	CO	3	07/2017
D5.1	Technological Roadmap	5	TEK-AS	R	RES_EU	6	10/2017
D6.1	Evaluation Methodology using benchmarking	6	CMRE	R	RES_EU	6	10/2017
D8.2	Self-assessment and data management plan V1	8	TEK-AS	R	PU	6	10/2017
D9.3	OEI – Requirements No. 14	9	TEK-AS	ETHICS	CO	6	10/2017
D2.1	Communication architecture report	2	TEK-AS	R	RES_EU	12	04/2018
D2.2	Performance assessment of ROBORDER configurations	2	ELTM	R	RES_EU	12	04/2018
D5.2	Technical requirements and operational architecture.	5	TEK-AS	R	RES_EU	12	04/2018
D9.4	H – Requirements No. 5	9	TEK-AS	ETHICS	CO	12	04/2018
D9.5	POPD – Requirements No. 6	9	TEK-AS	ETHICS	CO	12	04/2018
D9.6	DU – Requirements No. 15	9	TEK-AS	ETHICS	CO	12	04/2018
D9.7	GEN – Requirements No. 19	9	TEK-AS	ETHICS	CO	12	04/2018
D7.3	Market Analysis	7	EVERIS	R	PU	14	06/2018
D6.2	Action plan for PUC	6	CMRE	R	PU	15	07/2018
D5.3	First integrated ROBORDER system	5	TEK-AS	R	RES_EU	17	09/2018
D1.1	Draft of Concept of Operation, Use Cases and Requirements	1	HMOD	R	RES_EU	18	10/2018
D6.3	First M&S based Test Bed Demonstration	6	CMRE	R	RES_EU	18	10/2018
D6.6	First Evaluation report	6	CMRE	R	RES_EU	18	10/2018
D7.4	Mid-Project Dissemination Reports	7	HMOD	R	PU	18	10/2018
D8.3	Mid-term review and progress report	8	TEK-AS	R	PU	18	10/2018
D2.3	Final Sensors Implementations	2	ELTM	R	RES_EU	24	04/2019
D2.4	Adaptability solutions for robotic platforms	2	ROBOTNIK	R	RES_EU	24	04/2019

[1] After approval from the Security Advisory Board, a public version of some confidential deliverables will be realised and published to the ROBORDER website (e.g. the technology-oriented ones).

No.	Deliverable name	WP	Leader	Type	Diss. level[1]	Due date (months)	Due date (mm/yyyy)
D3.1	Event and activity detection and recognition	3	CERTH	R	RES_EU	24	04/2019
D3.2	Intrusion and illegal communications detection	3	CPT	R	RES_EU	24	04/2019
D4.1	UxVs tele-operation framework and interface	4	CERTH	R	RES_EU	24	04/2019
D4.2	Visual analytics and decision support tools based on risk models and reasoning methods	4	CERTH	R	RES_EU	24	04/2019
D7.6	Business Model	7	EVERIS	R	PU	24	04/2019
D8.4	Self-assessment and data management plan V2	8	TEK-AS	R	PU	24	04/2019
D5.4	Second integrated ROBORDER system.	5	TEK-AS	DEM	RES_EU	26	06/2019
D6.4	Second M&S based Test Bed Demonstration	6	CMRE	R	RES_EU	26	06/2019
D1.2	Final Concept of Operation, Use Cases and Requirements	1	HMOD	R	RES_EU	28	08/2019
D6.7	Second Evaluation report	6	CMRE	R	RES_EU	28	08/2019
D5.5	Final integrated ROBORDER system.	5	TEK-AS	R	RES_EU	34	02/2020
D6.5	Final M&S based Test Bed Demonstration	6	CMRE	R	RES_EU	34	02/2020
D6.8	Final Evaluation reports	6	CMRE	R	RES_EU	36	04/2020
D6.9	Operator Training Manual	6	ORFK	R	RES_EU	36	04/2020
D7.5	Final Dissemination Reports	7	HMOD	R	PU	36	04/2020
D7.7	Report on Standards and Collaborations	7	CMRE	R	PU	36	04/2020
D7.8	Exploitation plan and sustainability model	7	EVERIS	R	PU	36	04/2020
D8.5	Public final activity report	8	TEK-AS	R	PU	36	04/2020

Table 4 – ROBORDER list of deliverables

4 Management Plan

4.1 Objectives of the project

The main objective of ROBORDER is to develop a fully-functional autonomous border surveillance system with unmanned mobile robots including aerial, water surface, underwater and ground vehicles (UAV, USV, UUV and UGV), capable of functioning both as standalone and in swarms, and incorporate multimodal sensors as part of an interoperable network. The system will be equipped with technologies that can operate in a wide range of operational and environmental settings. To provide a complete and detailed situational awareness picture that supports highly efficient operations, the network of sensors will include

a. Passive radars that can extend the capabilities of the existing border surveillance radars;
b. Passive RF-signal sensing devices to intercept emission sources that are present in area, enrich the overall situational awareness picture with this information, allowing for further characterizing the nature and behaviour of entities in the picture, and detecting unauthorized signal sources and;
c. Other mobile sensors like thermal cameras (infra-red), optical cameras and more.

To succeed in the implementation of an operational solution, a number of supplementary technologies will also be applied, enabling the establishment of robust communication links between the command and control unit and the heterogeneous robots.

To this end, ROBORDER addresses a number of multidisciplinary Innovation Objectives (IOs) (Table 5), each one concerning a specific challenge defined by the border authorities' current and foreseen needs.

No.	Objective
IO1	**Adaptable sensing, robotics and communication technologies for different operational and environmental needs:** The protection of long stretches of borders with heterogeneous terrain is extremely challenging, particularly when it includes areas unapproachable by humans or is marked by adverse weather conditions. Human patrols are subjected to strenuous and often dangerous work. This has led to the recent rise in the use of UxVs as they present distinct functional advantages over manual patrolling (e.g., manned vehicles).
IO2	**Detection and identification of border-related threats:** Once sensor data is gathered by IO1 platforms, border authorities face the challenge of processing this amount of data as effectively and quickly as possible, detecting, classifying and identifying border-related threats and critical situations in order to inform border control investigations.
IO3	**Tele-operation of autonomous agents through 3D user interface and decision support** Currently, the overwhelming amount of information available to border authorities can distract rather than assist a surveillance mission. The time and resources required to analyse detected information can quickly render that information useless due to the passage of time or events. Therefore, information that could have been vital for predicting or intercepting a critical or illegal border-related situation is lost without having been assessed properly.
IO4	**ROBORDER platform development and integration** This objective will deal with the integration of all subsystems which make part of the ROBORDER platform. The system architecture will follow an open architectural framework documented in the NATO Architecture Framework v3.0 (NAF) views that will facilitate the system design.

Table 5 – List of ROBORDER innovation objectives

4.2 Decision bodies and governance

ROBORDER project's governance follows the structure depicted in Figure 2.

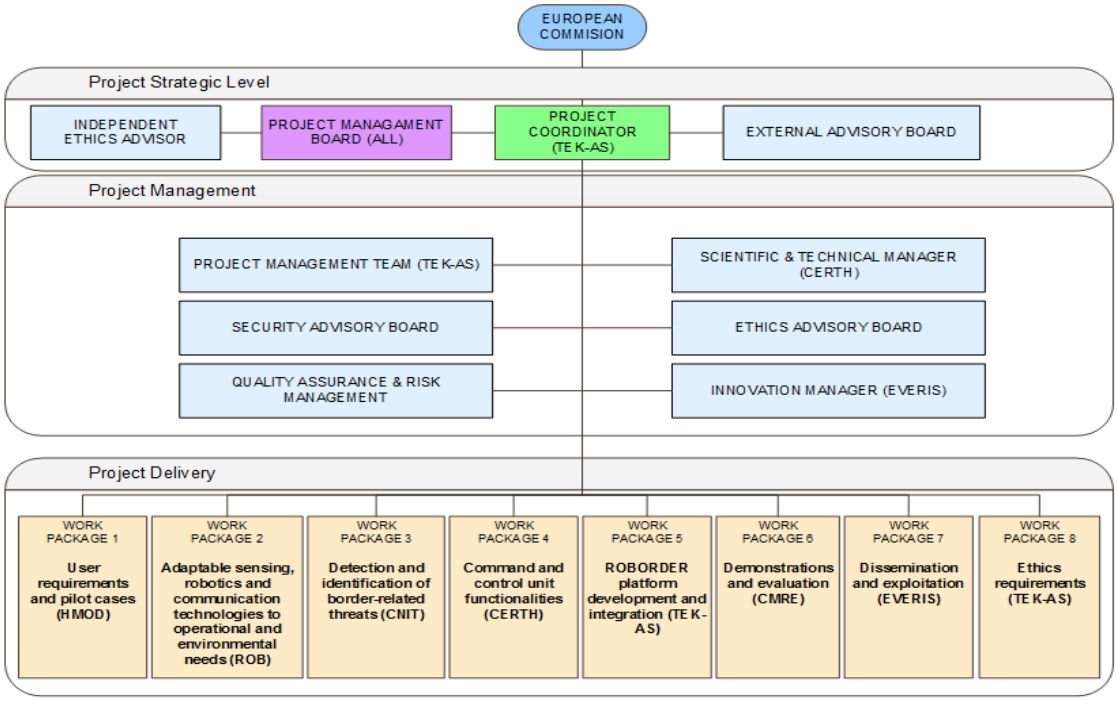

Figure 2 – ROBORDER's management structure and organisational bodies

There is only one decision body in ROBORDER: the Project Management Board (PMB). This body acts as the supervisory body for the execution of the Project and ultimate decision-making body of the Consortium. The PMB is free to act on its own initiative to formulate proposals and take decisions in accordance with the procedures set out in the project's Consortium Agreement. In particular, the following decisions fall under the responsibility of the Project Management Committee:

Content, finances and intellectual property rights

a. Proposals for changes to Annex 1 and 2 of the Grant Agreement to be agreed by European Commission;
b. Changes to the Consortium Plan;
c. Modifications to the list background intellectual property rights included in the project;
d. Additions to the list of third parties for simplified transfer of rights;
e. Additions to identified affiliated entities;

Evolution of the Consortium

f. Entry of a new Party to the Consortium and approval of the settlement on the conditions of the accession of such a new Party;
g. Withdrawal of a Party from the Consortium and the approval of the settlement on the conditions of the withdrawal;
h. Declaration of a Party to be a Defaulting Party;
i. Remedies to be performed by a Defaulting Party;
j. Termination of a Defaulting Party's participation in the Consortium and measures relating thereto;
k. Proposal to the Funding Authority for a change of the Coordinator;
l. Proposal to the Funding Authority for suspension of all or part of the Project;
m. Proposal to the Funding Authority for termination of the Project and the Consortium Agreement;

Appointments

n. Agree on the Dissemination and Exploitation Manager, upon a proposal by the Coordinator;

In addition, the Project Management Board has the following roles:

- To keep the technical programme on schedule;
- To merge and produce the Bi-annual (every 6 months) Progress Reports providing a qualitative summary of the work performed;
- To evaluate the evolution of the project (e.g. through the progress reports produced);
- To revise the project strategy (e.g. milestones);
- To discuss and approve solutions and deliverables (previously approved by WP leaders);
- To define the technical content presentations to the European Commission (EC);
- To propose mechanisms for corrective actions, if needed;
- To determine solutions for arising conflicts. In case of insoluble conflicts regarding some directions of the project, an independent expert in the field will be asked to arbitrate;
- To propose changes in budget allocation, partnership (termination and/or entering contractor) and new coordinator;
- To validate exploitation and dissemination documents and actions;

In the case of abolished tasks as a result of a decision of the Project Management Committee, the tasks of the Parties concerned will be rearranged. Such rearrangement shall take into consideration the legitimate commitments taken prior to the decisions, which cannot be cancelled.

The PMB is chaired by the Project Coordinator (PC) and has a representative from each partner as well as a representative for each of the following bodies: the Scientific and Technical Manager (STM), Security Advisory Board (SAB), Innovation Manager (IM) and Ethics Advisory Board (ETAB). The key persons in this body are listed in Section 2. The PMB meets (either physically or remotely) at least once every 6 months and reviews all major issues of the project as established in the meeting's agenda which is delivered 14 days before.

The SAB will be composed of the following members of the Consortium's project team, who are experienced in the protection of classified material and matters of National Security:

- ORFK: Police Major Zoltán Székely (ROBORDER's Project Security Officer);
- TEK: André Oliveira (also ROBORDER PC and TEK's security officer);
- CMRE: Prof. Jean-Guy Fontaine;
- PSNI: Detective Inspector Stephen Brown.

The SAB is responsible for leading and advising on all security matters relating to the ROBORDER project. The main responsibility of the SAB will be to analyse every deliverable and output of the project to determine if its dissemination level/classification must be modified form the initially planned. Where matters relating to security arise within the life of the project the SAB will liaise with representatives from the end user groups. Security matters will also be a standing agenda item at PMB meetings. Furthermore, the SAB will be responsible for handling the classified documents produced under the project and will be responsible for their submission to the EC as well as their storage and safekeeping (which if necessary will take place at TEK facilities).

Mr Zoltán Székely, from ORFK, has been appointed as Project Security Officer (PSO) for ROBORDER. He will be responsible for leading and advising the project participants and the PMB on all security matters relating to the ROBORDER project. He will be supported by the SAB. Currently working as university assistant lecturer, Mr. Székely is also qualified as a lawyer, having undertaken the Bar Exam. He has 14 of years policing experience, both operationally (2 years as patrol, 9 years as commanding officer for patrols at the airport, 1 year as lawyer) and in the provision of training with the Police College, Faculty of Border Management (2 years). Primarily attached to the Airport Police Directorate Budapest, Hungarian National Police, he has been seconded to the National University of Public Sciences, Faculty of Law Enforcement, where he is an assistant lecturer since May 2013. His expertise includes law, law enforcement, IT, management, and international relations, ISO 9001, speaking English (C1), German (B2), Roumanian (B1) and Hungarian (mother tongue).

The ETAB which will be composed of the following experts:

- SPP: Mr. Ionita Valentin;
- BDI: Prof. Yantsislav Yanakiev;
- ORFK: Mr. Zoltán Székely.

The ETAB will be responsible for evaluating the projects outputs in relation with the Ethics requirements laid out in WP9 and in general with the EC's ethics standards.

The operational bodies represented in Figure 2 are concerned with the daily activities and execution of the project. For a complete description of their roles please refer to the Description of Action Part B (Annex 1) of the Grant Agreement.

Governance follows the schematic of Figure 3. The core document for governance is the Grant Agreement which includes the DoA Annexes covering the activities to be performed by the project. The Consortium Agreement (CA) establishes the rules, guidelines and best practices for relations between partners of the consortium. Whenever inconsistencies or conflict arises between the terms of these documents, the terms of the Grant Agreement shall prevail. In case of conflicts between the attachments and the core text of the Consortium Agreement, the latter shall prevail.

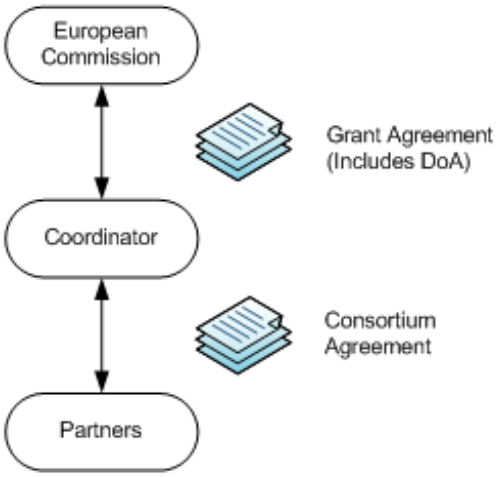

Figure 3 – Governance of ROBORDER

4.3 Decision making process – collaborative management model

Decisions concerning any of the aspects that fall under the responsibility of the PMB will follow the procedure described below.

The first step is to determine if an item requiring a decision by the PMB can be addressed at the next PMB meeting. If the item is too urgent or if there is no meeting planned that will allow speedy decision, a decision can be taken without a meeting (offline process). In this case, the PMB chairperson (the coordinator) circulates to all members a written document which is then voted on and signed by the defined majority of members (see below).

If the members agree the item can be discussed and decided at the next meeting, it must first be identified as an item requiring decision on the meeting's agenda. Any member may add an item to the original agenda by written notification to all of the other members no later than 7 (seven) calendar days preceding the meeting. If the item is not included in the agenda there is the possibility to add it to the original agenda during a meeting. In order to accomplish this, the PMB members present or represented must unanimously agree to add the new item to the original agenda. If they do not, the decision on that item is postponed.

The decision making follows the points presented in the next bullets:

- Decisions can be taken at meetings or without meetings (special conditions and written notifications);
- PMB members are informed of items to pass decision on prior to discussion;
- All issues (both technical/operational and strategic) are discussed among the members receiving inputs from task leaders;
- Decisions are based on voting;
- All members of the PMB have equal votes (except STM, SAB, IM and ETAB. Coordinator vote is tie breaker);

- Decisions can only be voted if there is quorum which is defined as 19/29 (65.5%) of attendees;
- Decisions are carried at a majority of 13 votes of the PMB present or represented by proxy;
- Any decisions so taken are subject to the additional provision that any Member whose work or the time for performance of it are thereby affected or whose costs or liabilities are thereby changed has voted in favour of the decision;
- Vetos are possible as long as party can show its legitimate interests would be jeopardized (no veto possible when being voted defaulting party).

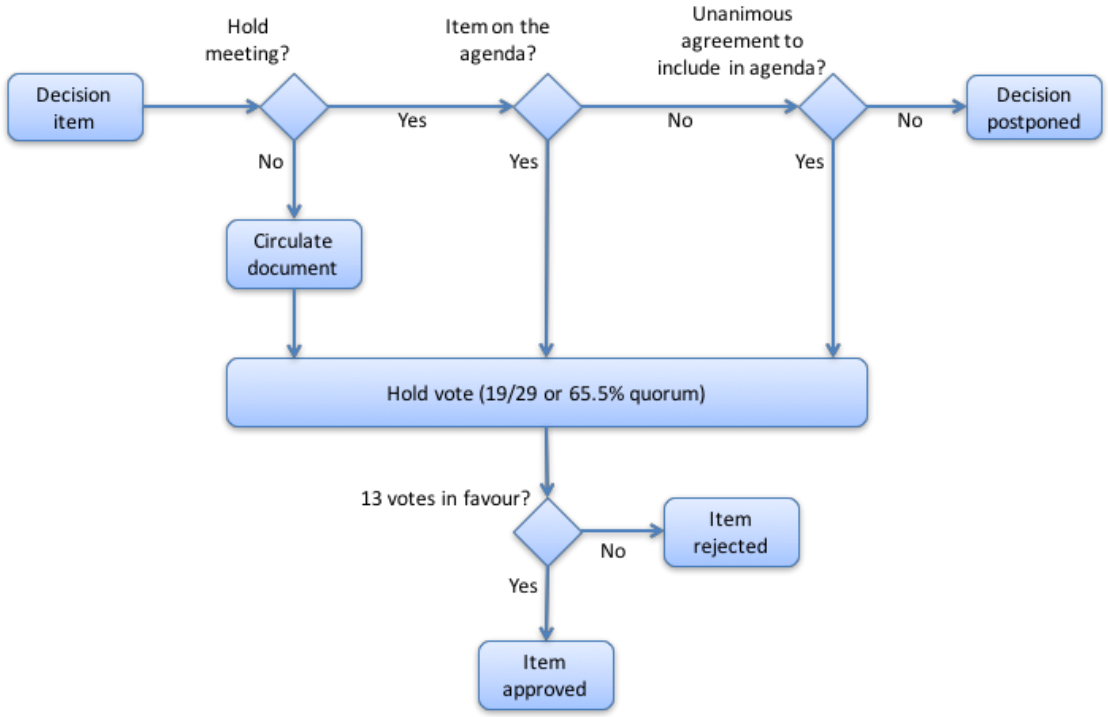

Figure 4 – ROBORDER's decision making process

A member who can show that its own work, time for performance, costs, liabilities, intellectual property rights or other legitimate interests would be severely affected by a decision of the PMB may exercise a veto with respect to the corresponding decision or relevant part of the decision. When the decision is foreseen on the original agenda, a member may veto such a decision during the meeting only. When a decision has been taken on a new item added to the agenda before or during the meeting, a member may veto such decision during the meeting or within 15 (fifteen) calendar days after the draft minutes of the meeting are sent. A party may not veto decisions relating to its identification as a Defaulting Party. A Defaulting party may not veto decisions relating to its participation and termination in the Consortium or their consequences.

Decisions concerning daily activities (e.g. at Work Package level) are to be taken by the Work Package Leader (WPL) after consulting and discussing with the WP participants. If the WPL judges the matter to be sufficiently important he/she may raise the issue with the PMB and ask it to pass decision on the issue. In this case, the process of Figure 4 will be applied by the PMB.

4.4 Quality assurance measures

Quality Assurance procedures will be applied to all activities and will be the joint responsibility of all partners until complete discharge of their obligations under the EC contract. The main goals of the Quality Assurance procedures are:

- Establishing documentation, reporting and communication procedures;
- Producing high quality deliverables on time;
- Identifying technical and commercial risks, or deviations at an early stage;
- Realising any necessary remedial actions as soon as possible.

In the case of deliverables, the first level of quality will be exercised by the responsible Task Leader who will establish a deliverable development plan identifying the deliverable coordinator, contributors, the development procedure and the evaluation process. The task leader and PC will identify two partners (the revisers), not involved in the preparation of the deliverable, to peer review the deliverable once the preliminary version is finished. The two revisers will provide in the shortest period of time, comments and proposed corrections to the document authors, in order to ensure high quality of the final document. The final version will be submitted to the PC that will perform a final revision before the submission to the EC.

The identification of risks for the achievement of the research and innovation objectives will be ensured through self-assessment. Project self-assessment is an important task throughout the project, which includes monitoring and reporting on the achievements of the project, as well as the risks foreseen for the upcoming work. The self-assessment of risks will be kept in a risk register that will be updated every six months (until month 24). The risk register is present in Section 5 of this document.

The STM will monitor quality of work and deliverables and report to the PMB on quality progress and resolution of issues.

4.5 Daily tools

Daily management of the consortium and coordination of the work to be carried out will be made using the following tools.

4.5.1 Communications

Communications between partners will be made through:

- **E-mails** – will be the default means of communication between partners. When the subject is relevant to a specific WP (e.g. WPX, where X is the number of the WP), roborder_wpX@tekever.com mailing list should be used. For matters involving the PMB, the roborder_PMB@tekever.com mailing list has been created. The roborder_coordination@tekever.com mailing list should be kept in carbon copy of all e-mails related to the project. All e-mails should identify the project in the subject field (e.g. [ROBORDER]: …)
- **Telephone** – preferred for one-to-one communication for quick discussions, status checking and decisions. The outcome of the telephone call should be distributed to the call participants in writing (e.g. using e-mail), if relevant.
- **Conference calls** – preferred for communication between several parties for quick discussions, status checking and decisions. The use of an online meeting tool such

as Webex or Gotomeeting is preferred. Minutes of the conference call should be distributed in writing afterwards (through e-mail).

- **Printed letter** – preferred for official correspondence. To be used when distributing administrative and/or contractual documents. Official correspondence should always be sent by registered mail and preference should be given to the use of express courier services.

Communications between the consortium and the European Commission will be the sole responsibility of the coordinator and will use the same instruments:

- **E-mails** – will be the default means of communication between the consortium and European Commission. The roborder_coordination@tekever.com mailing list should be kept in carbon copy of all e-mails exchanged. All e-mails should identify the project in the subject field (e.g. [ROBORDER]: …)

- **Telephone** – preferred for one-to-one communication for quick discussions, status checking and decisions. The outcome of the telephone call should be distributed to the European Commission in writing (e.g. using e-mail), if relevant.

- **Printed letter** – preferred for official correspondence. To be used when the consortium submits administrative and/or contractual documents to the European Commission. Official correspondence should always be sent by registered mail and preference should be given to the use of express courier services.

4.5.2 Repository

A repository will be setup for use by the consortium. The coordinator will provide a repository of its own. The repository should have version control and will be accessible through an installable client, via online browser and through a client requiring no installation.

The following folder structure will be implemented in the ROBORDER repository:

ROBORDER Template Structure

- **WPs** – working documents, images, schematics, news clips, videos, references, etc. for the work packages of the project
  - WP1
  - …
  - WP9

- **Meetings** – presentations and minutes for each meeting

- **Contractual Docs** – copy of the GA and of the CA. Any amendments will also be posted here

- **Deliverables** – official deliverables as submitted to the European Commission in the participant portal

- **Public** – documents to be made public to the outside world. Link to the project website public section will be established

- **All** – any documents to be made available to the costumer and all partners

- **Templates** – templates for presentations and deliverables

Other folders may be added throughout the project, given that the purpose of such folder is well defined and deemed relevant. Details on how to use and access the repository will be made available through a separate internal consortium document.

4.5.3 Disputes

The parties shall endeavour to settle their disputes amicably. All disputes arising out of or in connection with the CA, which cannot be solved amicably, shall be subject to the following escalation procedure:

- Level 0: conflict is brought to the attention of the PC by the involved parties. PC mediates parties' discussion in trying to find a solution or compromise. If no solution can be agreed, PC escalates to Level 1;
- Level 1: issue is discussed by the PMB and the involved parties. Solutions and compromises are proposed by Parties and PMB. If conflicting Parties cannot agree in a pre-defined timeframe or fail to find a compromise, the issue is escalated to Level 2;

- For the avoidance of doubt, the General Assembly shall be informed of any dispute or conflict if the issue is considered to have a strategic impact on the Project;

- Level 2b: Assuming there is no strategic impact on the project, the conflict is finally settled under the Rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said Rules. The place of arbitration shall be Brussels if not otherwise agreed by the conflicting Parties. The language to be used in the arbitral proceedings shall be English unless otherwise agreed upon. The award of the arbitration will be final and binding upon the Parties. However, should any of the Parties involved provide reasonable justification that certain provisions of its national law mandatorily prevent it from submitting the relevant dispute to arbitration, the concerned Parties will submit the dispute to the jurisdiction of the competent Court in Brussels.

Nothing in the CA shall limit the Parties' right to seek injunctive relief in any applicable competent court.

4.5.4 Meeting calendar

A preliminary schedule of meetings has been defined in Table 6. This will be updated at each meeting as a minimum. Whenever a new meeting is scheduled, the meeting calendar will be updated and distributed to the partners by e-mail.

Meeting description	Location	Participants	Associated Event	Date	Duration (Days)
Kick-off Meeting	Portugal	All	Project Start	M2	2
Progress Meeting 1	Hungary	All	MS1	M6	2
Progress Meeting 2	TBD	All	MS2	M13	2
Mid-term project review	Belgium	All	MS3	M18	2
Progress Meeting 3	TBD	All	MS3	M25	2
Progress Meeting 4	TBD	All	MS4	M30	3
Final Meeting	Belgium	All	MS5	M36	2
Technical Meetings	TBD	TBD	Specific technical issues	TBD	TBD
Testing and Integration Meetings	TBD	TBD	Component and integration meetings	TBD	TBD

Dissemination events	TBD	TBD	Presentations at conferences, relevant events, etc.	TBD	TBD

Table 6 – Official meeting calendar

5 Risks and issues management plan

By nature, innovation projects should be effectively organised in order to handle change since their future is less predictable than other activities. To this end, the objective of risk management is to provide the process and techniques for the evaluation and control of potential project risks, focusing on their precautionary diagnosis and handling. The PC and STM will be in charge of informing the PMB about specific critical situations and possible measures to be taken. There are inherent risks related to situations external to the project (e.g., due to market changes) and risks related to internal consortium problems. In the proposed methodology, the risk management process involves two activities: a) Risk Analysis: identification of a risk and assessment of its importance and evaluation of whether the risk level is acceptable for the project. b) Risk Management: planning of required activities to handle the risk, redistribution of resources, evaluation of the results and ensuring that the new status is stable enough. While it is probably unrealistic to believe that measures can be implemented to accomplish a single strategy, the consortium will strive to propose measures that attempt to achieve some form of control or avoidance. The following scale will be used as a guideline to assess risk impact:

- Highest severity (3) = project prevented from delivering expected results;
- High severity (2) = project delivers expected results but at increased cost or effort;
- Lowest severity (1) = project delivers expected results but at increased timespan.

This is compared with a likelihood of occurrence (estimated according to past experience, similar past situations and intuition) to determine the risk's criticality. The risks are then put into domains of acceptability and non-acceptability in the following manner:

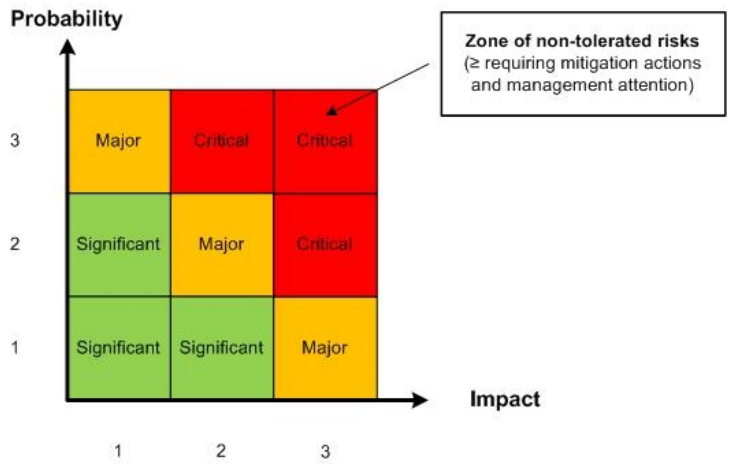

Figure 5 – Risk criticality

Measures to deal with the risks will focus on implementing actions that achieve one of the following:

- Avoidance – avoid the risk altogether by eliminating it or withdrawing from the actions that originate the risk in the first place;
- Control – keeping the risk in check by mitigating its impact or reducing the likelihood of occurrence and monitoring its progress closely;

- Acceptance – accept the consequences of the risk and manage the aftermath as best as possible;

- Sharing – sharing the impact of the risk with another party external to the consortium.

The following table summarises the critical risks for the project in its entirety and their mitigation measures while potential risks for innovation and user-oriented activities have been identified and described together with the respective contingency plans in section 1.3.6 of annex 1 part B of the GA.

Description of risk	WP(s)	Proposed risk-mitigation measures
Violation of data privacy	WP1 WP5 WP6	ROBORDER will conform to all necessary procedures to safeguard privacy requirements (Task 1.3). Participation will be voluntary, with a clear document on how private information will be used during the project and private data will be anonymised according to the ethical protocols (details in section 5.1).
Failure of scientific integration	WP5	The consortium includes partners with excellent capabilities in cross-discipline collaboration. Clear inter-play between WPs and tasks and appropriate monitoring practices have been designed in order to promote integration from the very beginning of the project. If some research modules cannot be integrated, dedicated small demonstrators will be provided.
The planned approach is not successful because of new technical developments that render it obsolete.	WP5	The "plug-n-play" nature of the ROBORDER platform enables the easy and straightforward interfacing and integration of new technologies that may be available during the project lifetime.
Difficulties recruiting sufficient numbers of users for PUCs by the consortium	WP6	We will proceed with the recruitment of users at the institutions of the members of the user group.
Time for development of the prototype and its validation is underestimated	WP6	Change prioritisation of developed tasks. Project checkpoints will monitor and detect problems early and take corrective action. Successive project approach with 3 evaluation cycles allows for smooth re-scoping to mitigate against delayed delivery of platform.
Partner drops out of the project	WP8	We will target a direct replacement with a partner of similar expertise. The good reputation of all partners of the consortium and their complementary expertise will facilitate this task.
As a direct impact of the EU referendum result (Brexit), the eligibility of UK entities to receive EU research funding beyond 2018 are currently unknown. Should the UK's access to funding be revoked during the projects funded period, this may pose an immediate impact on UK entities ability to fulfil their commitments to the project.	WP8	1) The UK Government announced on Saturday (13 August) that it will underwrite funding for approved Horizon 2020 projects applied for before the UK leaves the European Union. The guarantee applies to funding applied for before Brexit, and the Government will underwrite the payment of such awards, even when specific projects continue beyond the UK's departure from the EU. Details of the announcement can be found here: http://www.hefce.ac.uk/news/newsarchive/2016/Name,109430,en.html 2) Sheffield Hallam University's Vice Chancellor has also committed to funding the fulfilment of CENTRIC's obligations using its own resources, should there be any shortfall in funding due to ineligibility after Brexit. A formal letter containing confirmation of this commitment is attached in Annex B of parts 4-6.

Description of risk	WP(s)	Proposed risk-mitigation measures
Ill implemented interoperability interfaces may limit the impact of ROBORDER	WP5	Clear definition of interfaces and provision of APIs to existing systems will be fundamental in preventing this risk. (addressed in T5.1)
Lack of resources to carry out demos will limit the impact and acceptance of ROBORDER	WP6	A plan for demonstrations has been setup and will be detailed in WP N. The responsible partners and end-users have planned resources to make them possible according to their best expertise. Both technical partners and practitioners have made provisions for making assets available (existing and new ones such as UGV, UUV, USV and UAVs). If for some reason, some practitioners cannot commit means to tests and demos, the MB will propose a shift of effort and budget to another end-user to carry out the demo. The demos will happen in the second half of the project, allowing sufficient time to plan and commit assets.
Lack of testing all combinations of modules (possibly at the same time) may pass the impression of an incomplete technical validation	WP6	Indeed it will be impossible to test all combinations merely because some functionalities are not made to work together. By giving priority to user driven workflows and testing different user cases and scenarios prepared by end-users, the consortium is confident the practitioner and scientific communities will be satisfied.

Table 7 – Preliminary identification of critical risks

Beyond the risks explicitly identified in Table 7 above, specific risks associated with each IO and respective IAs have been identified. These risks and their respective contingency plans are detailed in Section 1.3.6 of annex 1 part B of the GA.

6 Dissemination and exploitation plan

ROBORDER's consortium will deploy an integrated framework to ensure high quality, coherent and collaborative dissemination of results as well as focused and market-oriented valorisation strategy. To this end, and in testimony of its importance, Task 7.1 and Task 7.6 includes the careful planning and execution of the dissemination and exploitation plan for the project results, focusing on defining the strategies for future exploitation activities.

The consortium's dissemination strategy for ROBORDER's results will ensure transparent information access while respecting all confidentiality and Intellectual Property Rights (IPR) issues. The dissemination strategy will include:

a. Scientific publications of the main project outcomes;

b. Provision of a consortium website with access to working papers, tutorials, project updates and contact persons;

c. Strategic use of the European unitary patent where applicable;

d. Active collaboration with national administrations, industry associations, research groups, Non-Governmental Organisations (NGOs) and Small-and-Medium Sized Enterprises (SMEs).

Furthermore, the consortium is committed to a coherent valorisation strategy based on technology development and commercialisation activities. These include:

e. Licensing Programs based on reasonable and fair industry practices;

f. Start-up engagement;

g. Collaborative research with public research institutions and private industry;

h. Implementation assistance;

i. Strategic participation in Intellectual Property (IP) aggregation and IP exchange platforms;

j. Close cooperation with education institutions.

The complete dissemination plan will be prepared, with contribution from all project partners, and in close connection with the exploitation plan development, so as to ensure that exploitation and dissemination planning are in sync and jointly support the impact goals of the project. The dissemination actions undertaken and their impact will be assessed in regular time intervals and, based on this assessment; updates of the dissemination plan will be carried out.

6.1 Target communities

Establishing contact with the relevant communities will allow the consortium to gain sensitivity to the challenges and impact that this technology could have. It is important to mention that part of those communities is not specifically related with defence/security or Law Enforcement Agencies (LEAs) – including for instance aeronautics, robotics and other fields of application for radar and UxV technologies – and, by incorporating them in ROBORDER's dissemination and exploitation process, the achievements in this project will

reach beyond that specific scope. Table 2.5 lists the most relevant communities identified at this proposal stage.

Communities	Activities
Coast Guards, Police, Navies and other potential end-users	The objectives of the project will be shared to the end-users community to be able to disseminate the main goals and to incorporate their inputs.
LEAs in general	End-user partners in the consortium will use all the communication channels with stakeholders, in order to disseminate the results of this project. Dissemination activities in the perspective of sharing information and knowledge within law enforcement community will include: • On the external level, with international partners, mainly at the bilateral co-operation level with counterpart LEAs and services; • On the internal level, within units of the consortium partners and with other national entities, as well as with LEAs.
Institutional and Regulatory Bodies	The consortium will activate its contact network and use communication and dissemination events to reach these entities and increase awareness of the project and its goals, improving their openness to the topic and access to knowledge. This interface will be used to prepare in as much advance as possible all required steps to improve and adapt the legal framework to the project results, as well as to take into account regulatory constraints in the project development. This aspect is also important to maximise the impact, especially in opening the door for future market implementation of the developed system, particularly regarding UAVs
R&D community in Europe	The consortium has extensive contacts across the research and development community in Europe. They will leverage these relationships in order to raise awareness of the new concepts and approaches taken within the project to encourage future application in research and development activities.

Table 8 – ROBORDER target communities

6.2 Key dissemination events and activities

The activities to be undertaken during the project will include participation in events and activities of great relevance, such as those mentioned in the two following tables.

WP	Event
WP1	**Conferences**: Applied Human Factors and Ergonomics **Journals**: Human Factors, Ergonomics, Applied Ergonomics, Military Psychology
WP2	**Conferences**: IEEE International Radar Conference, International Conference on Intelligent Robots and Systems, IEEE International Symposium on Technologies for Homeland Security, IEEE Transactions on Communications **Journals**: IEEE Transactions on Aerospace and Electronic Systems, IET Radar Sonar and Navigation, IEEE Transactions on Geoscience and Remote Sensing, IEEE Transactions on Signal Processing
WP3	**Conferences**: Microwave Symposium, IEEE International Topical Meeting on Microwave Photonics, International Conference on Image Processing (ICIP), British Machine Vision Conference (BMVC) **Journals**: IET Radar, Sonar & Navigation, International Journal of Microwave and Wireless Technologies, Image Communication, Computer Vision and Image Understanding

WP	Event
WP4	**Conferences**: ACM Multimedia, Hadoop Summit, EuroVR, Science and Systems Conference, International Conference on Robotics and Automation **Journals**: IEEE Transactions on Multimedia, IEEE Transactions on Information Forensics and Security, Multimedia Tools and Applications, IEEE Transactions on Robotics, Journal of Field Robotics

Table 9 – List of events of great relevance

Dissemination impact indicators applicable to ROBORDER include:

a. Visits/views of website and social media measured with tools such as "Google Analytics" (target: 20% increase per year);

b. Downloads of publicly available online material, especially scientific publications, released software and datasets (target: 300 downloads);

c. Social media engagement and outreach measured by the number of followers/connections and interactions (target: active on at least two platforms);

d. Scholarly impact of scientific publications measured by journals' impact factor, conferences' acceptance rate, number of citations, views in academic social networks (target: at least 15 scientific publications including at least 2 open access publications);

e. Participation/attendance in workshops where ROBORDER presentations or demonstrations are given (target: 3 workshops: 1 scientific workshop collocated with a well reputed conference with at least 20 participants (research, industrial) and 2 workshops (road show events) focusing on ROBORDER demonstration to border authorities (at least 10 LEAs and border authorities)).

Partner	Main dissemination activities	Target audience
TEK-AS	i) Participation in national and international fairs of robotics and security systems; ii) Activation of TEK-AS's contact network within the relevant target communities to raise awareness and support for the ROBORDER system; iii) Contribution to dissemination material content and events; and iv) training	Governmental security institutions, robotics partners and clients, regulatory and standardization bodies
EVERIS	Participation in conferences such as the Border Security Annual Conference organised by SMI (https://www.smi-online.co.uk/defence/europe/border-security), publication of results in Europe Defence Matters, the publication of the European Defence Agency	Science and technology groups, sector companies, policy makers
ELETTRONICA	i) presentation of the results at the yearly MILIPOL Exhibition; (ii) presentation of the results at the Eurosatory Defence & Security international Exhibition, (iii) presentation of the results at the GPEC Exhibition (Internationale Fachmesse und Konferenz für Polizei- und Spezialausrüstung)	Military and law enforcement institutions, environment monitoring and research institutions, wider public.
MST	In the context of its commercial activities, MST participates regularly in the most relevant international fairs, exhibitions and conferences related with marine technology. Information about the ROBORDER project, its demonstrations and outcomes will be disseminated in these events, mainly those that target the military or border control related markets. The company will prepare posters, brochures and multimedia content that will specifically focus the project. Moreover, the company foresees publications in top-tier conferences and journals, presentations	

Partner	Main dissemination activities	Target audience
	in invited sessions, organisation of topic-specific workshops, and communication of project outcomes to the media.	
CPT	(i) Publications at top-quality international journals and conferences in both; the broad area of secure communications and the specialised field of active detection of cyber-assisted attacks, (ii) Preparation of promotional and marketing material for external audiences, (iii) Periodic release of the project outcomes under a special section of the company's website blog and (Iv) Publication of the technologies produced via a profile in Enterprise Europe Network.	Professionals, other companies,, researchers, Science and Technology Group
ROBOTNIK, COPTING	ROBOTNIK and COPTING as SMEs will disseminate results and outcomes from ROBORDER to conferences, exhibits, fairs and will also integrate them in projects and proof of concepts.	Professionals, other companies,, researchers, Science and Technology Group
CERTH, FHR, VTT, CMRE, CSEM	i) Publications in scientific journals and conferences, ii) Participation in workshops, iii) Contribution to dissemination material content	Scientific and technological community
CENTRIC	i) Publications in scientific journals and conferences, ii) Participation and organisation of workshops and conferences, iii) Contribution to dissemination material content, iv) incorporation of findings and practice in taught undergraduate and postgraduate courses; v) via CENTRIC at security and policing events, publications and activities	
UOA	The dissemination of the project results will be assured on an international level as UOA's main target is the publication of its research results in major relevant conferences and peer-reviewed journals. In addition they foresee tutorials within the context of large events, press releases, book chapters as well as publications on the web: p-comp research group web page, presence in social media networks, etc.	Science and Technology Groups (mainly in academia), relative end-users (through the RAWFIE H2020 FIRE+ project)
CNIT	i) Publications in scientific journals and conferences, ii) Participation in the pan-European Workshop, iii) Contribution to dissemination material content, iv) training	Scientific and technological community
GNR	GNR intends to disseminate the experience and outcomes acquired during the project in international forums where the GNR is integrated or which we participate and also internal awareness-raising to the issues related to this project.	International and Portuguese Partners, GNR RPAS pilots, GNR surveillance staff
ORFK	The Scientific Council of the Hungarian National Police intends to host scientific and press events to present the project to the public, ii) participation on an international security conference (ESR, BPC, NISPAcee or equivalent) to present results of the project, inviting Central and East Europe Border Guard and Police authorities, foreign representatives, the Frontex, the Borderpol, the Cepol and the Europol, EU-LISA., iii) In the later stage, on the European Day for Border Guards, in Warsaw, Poland, we plan to participate on the exhibition with a demonstrator of the system.	Military S&T groups, CMRE panels and research task groups, subject matter experts
RBP & SPP	i) ENPPF and APPS professional networks dissemination, ii) Military Technical Academy from Romania and its professional network dissemination, iii) Participation on international workshops and conferences	Security professional community from Romania, CE and worldwide.

Partner	Main dissemination activities	Target audience
HMOD	HMOD, as a public body with non-profit character, will disseminate the expertise and the knowledge among its interested directorates. In order to fulfill its objectives HMOD is going to organize internal seminars for briefing the key personnel so as to anticipate future infrastructure exploitation. Moreover, the results of the project can be projected through its existing web sites and the existing international HMOD networks to other EU parties. Furthermore, HMOD can provide its infrastructures and resources for the dissemination of project's achievements and installed capabilities. Main dissemination activities: i. Exercises in the framework of NATO; ii. Presentations in NATO, EDA seminars and workshops; iii. Presentations to relevant projects in which HMOD participates, iv. Presentations in Community of Users (CoU) and Working Groups (WG) where HMOD has steady participation	National stakeholders from NATO, Europe, Middle East
BDI	BDI will exploit its links to many EDA and CMRE activities and international projects to disseminate ROBORDER and will organise a number of special sessions/tracks focused on ROBORDER data and findings under the Military Technology and System (MT&S) conference, organised and hosted by BDI, and the defence, antiterrorism and security exhibition HEMUS organised under the auspices of the Defence Ministry of Bulgaria.	EDA captech member and experts, Military S&T groups, CMRE panels and research task groups, subject matter experts in Bulgarian Armed Forces.
APL	Publications in industrial sector journals and conferences, 2) Participation in the pan-European Workshop, 3) Contribution to dissemination material content, 4) training of port personnel, 5) contribution to best practices and standards (leveraging the membership in the European Sea Port Organization)	End-users, National and EU LEAs, port authorities
PSNI	Engagement with LEAs and other end-users through national and European organisations; Participation in the pan-European Workshop; Contribution to dissemination material content	End-users, National and EU LEAs, Security Agencies, Policy Makers, Police School, key partners and stakeholders in national security
MJ	As a LEA, MJ will disseminate the project results to other national, European and international LEAs, such as INTERPOL, Europol and ENFSI – European Network of Forensic Science Institutes among others. It will also disseminate it to the public in general through its Institutional Website.	

Table 10 – Specific dissemination per partner

6.3 Exploitation of project results and tools

Supporting the valorisation strategy outlined above, project ROBORDER will produce a number of exploitable results, including the complete system and separate sub-systems. The following table summarizes some of their main characteristics and measures to maximise their market potential.

		Compact-size low-cost passive radar	Microwave passive sensor	Low-cost RF monitoring device	SIMROM	Extreme condition adapted agents	Carrier solution for small robots and sensors	Detection and classification modules	Novel Human-UAV interface	Plug-n-play autonomous navigation framework	Mission Description Language	DDDAS toolkit	Semantic integration and reasoning module	ROBORDER Platform
Type of exploitable result	Product	X	X	X	X	X	X	X	X		X	X		X
	Service									X	X	X	X	X
	Other													
Target Market	Direct End Users	X	X	X	X	X	X		X	X	X			X
	Software Developers / Integrators		X		X	X	X	X		X	X	X		X
	Consultants/ Intermediate users				X					X				
	Research/ Academia	X		X	X	X	X	X	X	X	X	X	X	X
Sales Strategy	Free										X	X	X	
	Academic version								X					
	Standalone version			X										X
	Licensed version				X					X				
	Add-on to existing product/service	X		X	X	X	X	X		X				
	Other		X							X				
Additional Services	Consulting services	X								X	X	X		X
	Extension services										X			
	Training services	X		X	X						X			X
	Support services	X		X		X	X	X	X	X	X	X		X
	Other													
Time To Market	In Months after project completion	6	6	6	3	3	6	6	6	6	3	3	3	3
Targeted Markets	National markets	X	X	X	X	X	X	X	X	X	X	X	X	X
	EU	X	X	X	X	X	X	X	X	X	X	X	X	X
	US					X	X				X	X	X	X
	Other					X	X				X	X	X	X

Table 11 – Exploitable outcomes

7 Ethics and Societal Impact

7.1 Ethics issues

7.1.1 Humans

Interviews to define user requirements are foreseen in ROBORDER. All interviewees will informed of the content, duration, and procedures of the interviews and will be required to provide their explicit consent to participate by signing an informed consent form. The interviewees considered in ROBORDER consist of staff of border control practitioners (e.g. border police, criminal police, navy, customs authorities) involved directly in the project (beneficiaries of the project). If considered relevant by the border control beneficiaries, the consortium may interview staff from other practitioners not involved directly in the project (not beneficiaries). No other persons will be interviewed. The interviewees will consist of researchers from the beneficiaries directly involved in the project activities.

WP4.1 and WP6 foresee the development of advanced human-robot interfaces. Volunteers from the practitioners involved in the project (beneficiaries) will take part in the development work. No personal data (as defined in Directive 95/46/EC) will be collected during the activities of WP4.1 and WP6 and the design and development of the interfaces. The work performed will have a human factors component focused only on human-computer interaction. Activities will include display design (e.g. how to present information, what information to present, how to organize the information presented on a screen), definition of input flows and mechanisms (mouse, joystick, keyboard, voice, etc.) and study of output and feedback flows (e.g. visual, audio, tactile). The role of the volunteers is to work with the research teams to help design the interfaces. Iterative design and empirical measurements (testing the interfaces with users from practitioner beneficiaries) will comprise the bulk of the techniques used. The interface users will be researchers working directly on the project and volunteers from the beneficiaries of the project.

ROBORDER does not intend in any way to collect personal data as defined in Article 2 of Directive 95/46/EC nor to perform identification of persons through any data collected during the project. Furthermore, ROBORDER will not collect any biometric data.

Video will be collected but only for the purposes of detection of persons, not their identification (i.e. detection of the presence of humans in an image or video). This information will be used in so much as to validate the algorithms employed for the detection and is intended to be used by competent authorities (border control practitioners) for the purposes of Search and Rescue and prevention of criminal or illicit activities after project conclusion.

ROBORDER will NOT collect data or monitor any vulnerable groups such as children or adults unable to give informed consent (testing will be done first and foremost with members of the consortium and participants from the beneficiaries).

The majority of the researchers involved in ROBORDER are experienced in H2020 Security collaborative research. Nevertheless, if any new research participants need to be involved, the ROBORDER consortium will identify and recruit research participants from the staff of practitioners and public bodies with security roles involved in the project (e.g. police officer, border control staff).

An Informed Consent form for the interviews has been prepared and is included in the Description of Action (part B - Annex E) of the Grant Agreement. If applicable, the Informed

Consent forms will be provided to the EC services. If considered relevant by the border control beneficiaries, the consortium may interview staff from other practitioners not involved directly in the project (not beneficiaries) to derive requirements. In this case, the interviewees will be informed of the content, duration, and procedures of the interviews and will be required to provide their explicit consent to participate using the template mentioned above.

ROBORDER will NOT collect data or monitor any vulnerable groups such as children or adults unable to give informed consent (testing will be done only with members of the consortium and participants from the beneficiaries).

7.1.2 Protection of personal data

As mentioned in the previous sections, no personal data (in the sense defined in Article 2 of Directive 95/46/EC) is expected to be collected. ROBORDER will not collect any biometric data.

Video and still imagery will be collected but only for the purposes of detection of persons, not their identification (i.e. detection of the presence of humans in an image or video). This information will be used in so much as to validate the algorithms employed for the detection and is intended to be used by competent authorities (border control practitioners) for the purposes of Search and Rescue and prevention of criminal or illicit activities after project conclusion. ROBORDER will not perform identification of persons through any data collected during the project.

In some countries, national legislation allows public safety authorities to store data from people crossing borders (although we do not intend to use this type of information). If, personal data is accidentally collected (e.g. identifiable face of an individual in a video) the consortium will activate and enforce the incidental findings policy defined in the next section. If the practitioners consider the use of data from people crossing borders essential to the project success (at this time this is considered unlikely), the consortium will apply pseudonymization to ensure the protection of the data. All data collected by the rest of the consortium or out of the scope of the abovementioned authorization (for public safety authorities), will be anonymised before sharing with Consortium to build the platform tools. All such data will continue to be stored at practitioner premises following the current procedures (which have been validated already by competent national authorities) and only the pseudonymized data will be shared with technical partners for the execution of the work. In this sense, ROBORDER partners will have no access to the real identity of individuals and the probability of identification will be minimal. The only exceptions are the end-users and only if they are authorized by law.

The collection and or processing of personal data is NOT foreseen at any stage of the ROBORDER project. However, as mentioned above, if the end-users and practitioners consider it relevant the consortium has already established a procedure to deal with this (i.e. pseudonymization and storage at the border control authorities). If this need were to arise, the consortium confirms that all applicable European and national legislation will be complied with.

If the need were to arise for use of personal data in ROBORDER research (i.e. if deemed relevant by the practitioners), such data would be publicly available.

ROBORDER will name a Data Protection Officer who will confirm all data collection and processing is carried out according to applicable EU and national legislation. The Data Protection Officer for ROBORDER will be Mr. Zoltán Székely.

If applicable, copies of confirmation by the competent institutional data protection officer and/or authorization or notification by the National Data Protection Authority will be submitted in deliverable D9.5 – POPD Requirements No6.

If personal data other than that publicly available is used in ROBORDER, the relevant authorizations for use of secondary personal data will be provided to the EC services through deliverable D9.1 – POPD Requirements No10.

7.1.3 Third countries

All work with the Swiss partner will apply the same guidelines and follow the same best practices and rulings as with other partners from other countries.

No personal data will be exchanged with Switzerland. The only data to be exchanged with the Swiss partner is of technical origin and not personal.

Furthermore, the ROBORDER consortium confirms that the ethical standards and guidelines of Horizon2020, as well as national ethical standards and guidelines, will be applied and followed in all countries involved in the project.

The consortium does not foresee any exports (i.e. procedure of allowing Community goods to leave the customs territory of the Community). Hence, no authorizations will be required.

If during the project, the situation changes and the consortium verifies the need to export project technology or equipment, the General Export Authorization No EU001 (which applies to all items listed in Annex I of EU Regulation 428/2009) will be employed. This authorization enables the export of dual use items to non-EU countries such as Switzerland. We do not expect to make use of this as testing will not take place in Switzerland and no actual exports (as defined in EEC Regulation 2913/92) will take place.

7.1.4 Environmental protection and safety

It is important to ensure that the border demonstrations and trials foreseen in ROBORDER do not put participants at risk. The consortium does not foresee any risk to participants. Participants in the tests will be chosen from volunteers from the staff of the beneficiaries (in particular end-users). None of the demonstrations foresees dangerous activities. Additionally, personnel from the end-users (practitioners) are trained professionals (the vast majority border guard, navy and police personnel) so the demonstrations and tests will constitute another exercise in line with the ones they already execute for training purposes. The risk of harming humans (researchers, technicians, etc.) participating in experiment with UxVs, or the citizens around the experimental area is very small, as the testing and demonstration areas will be cordoned off to the general public and secured by end-users and practitioners staff.

All partners in the project are committed to comply with applicable national and European guidelines and legislation concerning health and safety at work, namely:

- Directive 89/391/EEC on measures to improve safety and health at work
- National legislation, where applicable and relevant will also be considered and applied, for example: Portuguese Law Lei nº 7/2009, de 12 de Fevereiro - Código do Trabalho - Art.º 281º a 284º which establishes the principles in terms of safety and health at work in Portugal.

7.1.5 Dual use

The ROBORDER project will address solely civilian needs which are much less demanding in terms of performance than military applications.

While it may be argued that the technologies developed and used in ROBORDER have the possibility for dual use (i.e. use in both civilian and military applications), it should be noted that all technologies considered have been designed for the civilian market (namely public safety) or used successfully and further improved in civilian applications even if their original designs result from defence activities. The following paragraphs provide some more details on these aspects. A significant body of the work done in the area of Unmanned systems and passive radar has so far been motivated and funded by military applications, so the results of this project have the potential to be used back in the defence sector. Nevertheless, the technologies behind ROBORDER are not lethal or harmful technologies nor will they be developed and improved for military applications.

Despite counting with the participation of military organizations in the consortium, these have a long tradition of civilian work. For example, the HMOD has been joining effort with LEAs and contributing significantly to maritime border security and fighting criminal activities at sea in Greece as well as in other countries. An important aspect to bear in mind is that consortia should commit to not applying directly the knowledge developed with civilian funds in military applications and that adequate measures are put in place to ensure that no dissemination of sensitive aspects of the research work which may have higher degree of applicability to the military field takes place. As mentioned in the EC's explanatory note on exclusive focus on civil applications, "Research activities aimed at the development or improvement of dual use technologies or goods can be financed through H2020, provided that the research is fully motivated by, and limited to civil applications". This is precisely the case with ROBORDER which focuses on a strictly civilian application (land and marine border surveillance).

The consortium declares that it will not apply directly the research results of ROBORDER in military applications or in the military domain.

1. We will not use, follow, consider any military standard while implementing our system
2. We have no intention and we will not make any effort to solve two special issues which are essentially important for military use: *jamming resistance* and *low observance*
3. We will not design our system to be jam resistant other than resistance against natural and common unintentional artificial sources of interference (e.g. sunlight, normal background RF emission, etc.)
4. We will not deal in any way with the observability of our system. The active markers of the landing platform, the radio communication will be easily detectable with many commercially available devices.
5. We will use only commercially available technologies (e.g. GPS receiver, optical emitter and detector, RF modem, etc.) while implementing our system
6. We declare that the jamming and observance issues can't be solved with additional modification of the system. Only the complete redesign of the landing add-on might solve the problems.
7. The reason why this platform is proposed is because the commercial UAVs have significantly shorter flight endurance than military ones (some military UAVs can fly for up to 40 hours), so the solution is not needed in the military domain.
8. There are more complex platforms already available in the military domain having better ergonomy from the viewpoint of military use, see Patent 1. from listed patents.

Although some of the technologies and equipment used in ROBORDER may be classified as dual-use items as defined in Article 2(1) of EU Regulation 428/2009 (i.e. goods, software and technology normally used for civilian purposes but which may have military applications) and listed in Annex I of said regulation, the consortium does not foresee any exports (i.e.

procedure of allowing Community goods to leave the customs territory of the Community). Hence, no authorizations will be required.

If during the project, the situation changes and the consortium verifies the need to export project technology or equipment, the General Export Authorization No EU001 (which applies to all items listed in Annex I of EU Regulation 428/2009) will be employed. This will be reported in deliverable D9.2 – NEC Requirements No21. This authorization enables the export of dual use items to non-EU countries such as Switzerland. We do not expect to make use of this as testing will not take place in Switzerland and no actual exports (as defined in EEC Regulation 2913/92) are expected.

7.1.6 Misuse

By definition, current research may be exploited by criminal organisations and individual criminals when planning to perpetrate acts of serious crime or terrorism. The research and applied knowledge acquired in this project has the potential to be exploited by terrorists or criminal elements due to the fact that the research and development area focuses on the identification of illegal activities and communications and will also research current operational capabilities and gaps through the user requirements tasks.

One of the key objectives of the Consortium will be to safeguard the material gathered by the partners throughout the research process and protect the outputs generated. The research conducted within ROBORDER and the tools developed within the project to achieve the project aims could be subject to dual use threat. It is of the utmost importance that a robust system is in place to ensure the work of the project is not exploited for subversive means. The Consortium has put in place a tried and tested management and security advisory system to protect the outputs of the project from being used in this manner. The security procedures detailed in Section 6 will be activated for the purpose of preventing dual use by terrorists and criminals.

As mentioned above, ROBORDER will take a lot of care in implementing security procedures to ensure the adequate protection of sensitive information which may have the potential to be misused by criminals or terrorists. In this sense, all technical deliverables have been classified as RESTREINT UE. As such, access to the information and data included in these documents will be provided on a need to know basis. None of the ROBORDER technical results will be available publicly. The only information made public will be that related to the business model and potential market for ROBORDER solutions as well as general information about the solutions developed with no indication of performance or technical details of their implementation.

The classification of ROBORDER results, the application of security best practices (e.g. need to know) and the involvement of experienced security researchers as indicated in the Description of Action (part B – Section 5.1.6) of the Grant Agreement are considered sufficient measures to prevent the misuse of research findings.

7.1.7 Other issues

An internal Ethics Advisory board has been created and involves experts from some ROBORDER beneficiaries. The people involved in the board have the relevant expertise to monitor the ethical concerns of the project. The members and role of this board are described in the Description of Action (part B – Section 5.1.7) of the Grant Agreement.

In addition, an independent ethics advisor (external to the consortium) has been nominated. This external ethical advisor will complement the work of the internal ethics advisory board by independently analysing ROBORDER deliverables and will work to ensure the project

complies with European ethical guidelines and rulings. This independent external advisor will be subcontracted by the coordinator and will be responsible also for preparing a mid-term ethics assessment report. Mr Reinhard Hutter from the Centre for European Security Strategies (CESS) will be the external ethical advisor of ROBORDER.

UAV flight approvals are highly dependent on the country where the operation takes place, the type (size and weight) of the UAV and the airspace used (segregated or unsegregated). All ROBORDER partners involved in the operation of UAVs in the ROBORDER test already have approvals to fly in their own countries. In most cases, UAVs operated by public security forces are considered state aircraft and thus operate under a different set of rules than civil aviation.

ROBORDER will strive to carry out its tests under segregated airspace in which case approvals might not even be necessary (e.g. military airspace). Nevertheless, ROBORDER partners undertake to inform EC services of any authorization procedure followed and its results during the course of the project. This constitutes deliverable D9.3 – OEI Requirements No14.

The ROBORDER independent external advisor (Mr Reinhard Hutter from the Centre for European Security Strategies) will prepare a mid-term ethics assessment report to be submitted to EC services with the periodic reports of the project. This constitutes deliverable D9.7 –GEN Requirements No19.

7.1.8 Incidental findings policy

In case the ROBORDER system or the border control personnel detects anything illegal or unintentionally captures personal data through its sensors (e.g. cameras) that may lead of the identification of individuals, three different types of actions may apply depending on the conditions:

a. If an illegal activity is detected
    I. And it has been carried out by a person working for the project with the sole purpose of testing the system (and without previous knowledge of the border personnel on site) the local practitioner authority (e.g. National Police or Navy) will issue said person with a Letter of Commission stating that he or she has performed the action resembling an illegal act for the sole purpose of testing the system. As long as the act committed is exactly as outlined in the commission document, no actions other than the normal border control has to be carried and the illegal act is ignored,
    II. And it has been performed by someone not involved in the project or not directly authorized by the project during the testing activities, the person will be handed over to the border police units present who will carry out standard operational procedures determined by regulations on the given case, and all relevant data has to be secured and handed over to the police as evidence, including those who were collected with the perpetrators consent.

b. Any data collected from video, imagery or other sensors that incidentally may be considered relevant for the identification of individuals not involved in the project will be immediately isolated and erased from all storage devices (cameras, computers, servers and all other physical supports). It will be the responsibility of the partners using the sensor to flag such concerns to the Data Protection Officer who will decide accordingly if the data constitutes an incidental finding and if it should be erased. The Data Protection Officer will confirm erasure and issue to the Management Board a form describing the incident, date of occurrence and action taken.

In all cases, the Data Protection Officer has to be informed, and will act accordingly.

Any other incidental findings, not happening at the border and/or in presence of police officers, for example video collected on known terrorist suspects, devices connecting from areas under insurgent control, videos collected on persons known (wanted) as kidnapped or lost, will be handed over to the relevant national authorities through the Data Protection Officer.

7.2 Societal Impact

Question 1: Does the proposed research address documented societal security need(s)?

By developing and introducing a range of technologies to improve border surveillance, ROBORDER addresses key security needs, particularly those of the environment (with the use of passive detection systems and unmanned systems that require less fuel to deploy and by promptly detecting pollution incidences), health (border surveillance is crucial when dealing with illegal immigration and the human life risks it implies) as well as those of property (by preventing or adequately responding to illegal trafficking).

Question 2: Does the research output meet these needs? Will this be demonstrated? Will the level of societal acceptance be assessed?

The output meets these needs by improving capability of existing maritime surveillance systems and by introducing green technologies. The research will be demonstrated in life-like yet controlled conditions using the actual systems used every day by authorities. Societal acceptance will not be assessed.

Question 8: If implemented, could the research have a negative impact on the rights and values enshrined in the Treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection?

The implementation of the ROBORDER solution will not have a negative impact on the rights and values enshrined within the European Treaties.

Question 9: If implemented, could the research impact disproportionately upon specific groups or unduly discriminate against them?

The implementation of the ROBORDER solution will not impact disproportionately upon any individual or specific group, or unduly discriminate against anyone or any group.

Question 10: Will specific measures be taken to ensure that the research outcomes comply with the European Charter of Fundamental Rights and to mitigate against any of the negative impacts described above?

The ROBORDER consortium is cognisant of the necessity of complying with the European Charter of Fundamental Rights, and will ensure that all activities which are undertaken during the course of the project are in keeping with the requirements of the charter. In formulating the project, the consortium has included specific tasks and deliverables within WP1 User requirements and pilot use cases, namely T1.3 Ethical and Legal requirements, to consider the Ethical, legal, societal and cultural aspects of the proposed solutions and ensure they are designed to ensure compliance. Although no negative impacts have been identified as resulting from the ROBORDER project, the inclusion of this in WP1will ensure that should an issue which may potentially conflict with the European Charter of Fundamental Rights, the consortium will be in a position to introduce effective measures which can address such an occurrence.

8 Security

Detailed information on the design, characteristics, operation and requirements of, and prototypes for, key functional devices for use in border security, such as sensors and radars, should be classified RESTREINT UE/EU RESTRICTED. Also, systems information (such as the functional or technical architecture, operating systems, platforms, software and algorithms) should be classified RESTREINT UE/EU RESTRICTED.

In this scope, deliverables 1.1, 1.2, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 should be classified at a RESTREINT UE/EU RESTRICTED level.

8.1 Other Project Specific Security Measures

Any members of the ROBORDER project consortium requiring access to classified information will have to demonstrate the appropriate level of personal security clearance as well as need to know.

A partner will not handle classified information unless it is required as part of the Project and they will not handle the information unless they have the relevant Personal Security Clearance.

Where required to comply with security conditions the partner, who does not have personal security clearance shall, until such security conditions be achieved:

- Conduct all research/work using "Dummy/Unclassified" (i.e. simulated, not real) data;

- Attend relevant meetings during which time "Public" matters are discussed following which they shall absent themselves from and will not participate in the meeting when "Classified" matters are discussed.

In addition, the following policy will be adopted concerning the production of classified deliverables:

- Deliverable contributors generate content for the deliverable as normal for any other deliverable. No specific measures for protection of content are foreseen at this point.

- The owner / editor of the deliverable generates a draft deliverable based on the content compiled from all contributors. The next steps are determined by the classification level of the deliverable:
    - No classification
        - All non-classified deliverables as public so no additional security measures are expected. The owner / editor will share the draft deliverable with the Security Advisory Board and the Project Security Officer who will determine if the document contains any sensitive information preventing its publication or warranting a change in the classification level (from unclassified to RESTREINT UE)
    - Classified as RESTREINT UE
        - Owner / editor will encrypt the document using an encryption tool accredited by the EU and sends it to the STM, SAB and the PSO for validation.
        - The SAB and the PSO decrypt the document and validate it from the security perspective. All SAB members provide their assessment to the PSO who issues an assessment to the Coordinator.

- The STM decrypts the document and validates the document from the technical and scientific perspective (this may result in revision of the document with the owner / editor).
- The STM encrypts the deliverable using an encryption tool accredited by the EU and sends it to the Coordinator for final revision and submission.
- The Coordinator decrypts the document and performs the final quality check and final editing.
- The Coordinator encrypts the deliverables and submits it to the EU.