SafeShore – Needs of the end-users

Marian Buric

Protection and Guard Service

SafeShore

12th CoU Meeting,

4th December, 2018, Brussels, Belgium

Overview

- Why?
- What are the targets of the SafeShore solution?
- Targets assessment
- The requirements set
- Requirements evaluation
- Wat's next?
- Proposal for a synergy between two key issues intimately connected to Law Enforcement Authorities' missions

Why? Legitimate & illegal use of RPAS & small vessels

- Many legitimate use cases:
  - Mapping
  - Police
  - SAR
  - Movies & Films
  - Hobby
  - Delivery
  - Inspection
  - …

SafeShore

The Problem – Traffic Control

- Over the course of centuries, we created a road traffic network, with a set of rules and a police force to control / enforce these rules
- Now, we have to do the same with low-altitude aerial traffic
- ***But how can we enforce these rules if we do not know where the different agents (drones) are?***

SafeShore

The Problem – Illegal use of drones

- Smuggling: borders, restricted areas, prisons, illegal items (drugs, CBRN goods, weapons, …), tax evasion (cigarettes, …)

- Examples:
  - Drone found crashed in Tijuana while carrying high-risk drugs (Mexico, 20 January 2015).
  - Drone was used to deliver a container with radioactive material on the roof of the Japan's Prime Minster's residence (9 April 2015).
  - The drone attack on President Nicolas Maduro during a speech at a military parade on 4th August 2018.

SafeShore

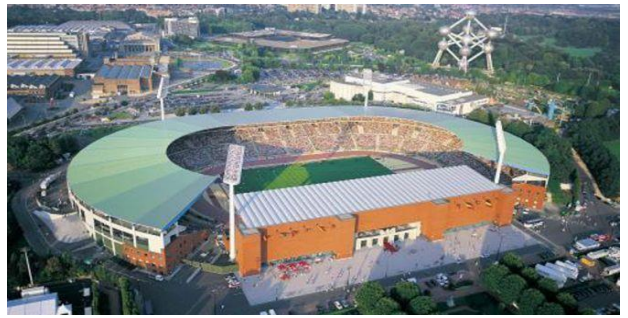
The Problem – Illegal use of drones

- Illegal surveillance:
  - 56 cases of drones illegal surveillance of nuclear power plants since October 2014
  - Violation of privacy of celebrities, neighbours, …

SafeShore

The Problem – Illegal use of drones

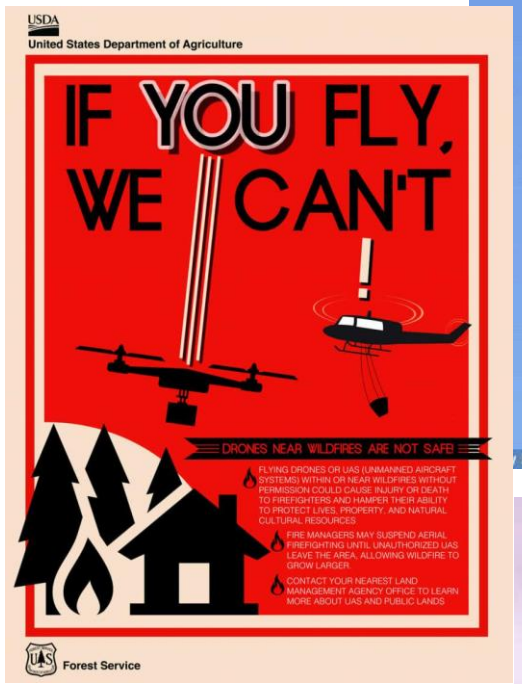
- Terrorism:
  - IS using drones domestically to spy on ‘enemy’ troops / force protection
  - Hamas using drones against Israel
- Activism
  - Drones were used during the 2013 German election campaign.
  - Drone with Palestinian flag apprehended in Brussels before Belgium-Israel football game.
  - A drone quadcopter carrying an Albanian nationalist banner during a UEFA 2016 qualifying match.



SafeShore

The Problem – Illegal use of drones

- Drones interfering with manned aviation:
  - More and more incidents near airports
    - ➔ Huge economical impact
  - Drones interfering with SAR / forest fire operations
    - ➔ Huge societal impact



- Drones falling / injuring people
  - Small drones generally have no redundant fail-safe systems.

The Problem – Illegal use of small vessels

- E.g. RHIB's used for human trafficking or drug trafficking

Detection targets – small vessels

- Mostly the fishing and small passenger ships with a lenght between 4m and 10m
- Unmanned Sea Vehicles, small boats for up to 4 persons
- Jets Skies (used on terrorist attack in Tunisia)

Detection targets – Humans at sea

- Humans on boats
- Kite surfers
- Swimmers

The Problem – How to detect drones cost-effectively?

- Military-grade RADAR-based solutions do exist, but:
  - Are immensely expensive (>M€ per unit)
  - Still have a limited range (few km)
  - Are illegal for use in any non-military context (outside a theatre of war), as they do not respect limitations on the emitted power

SafeShore

SafeShore project – challenges and scope

Specific challenge

- The use of **low cost and "green" technologies** is expected to become mandatory for future border control systems in environmentally sensitive areas. Passive systems fit this application, due to **electromagnetic invisibility**, **lower detectability** and **cost** and the **possibility of use practically anywhere**.

Scope

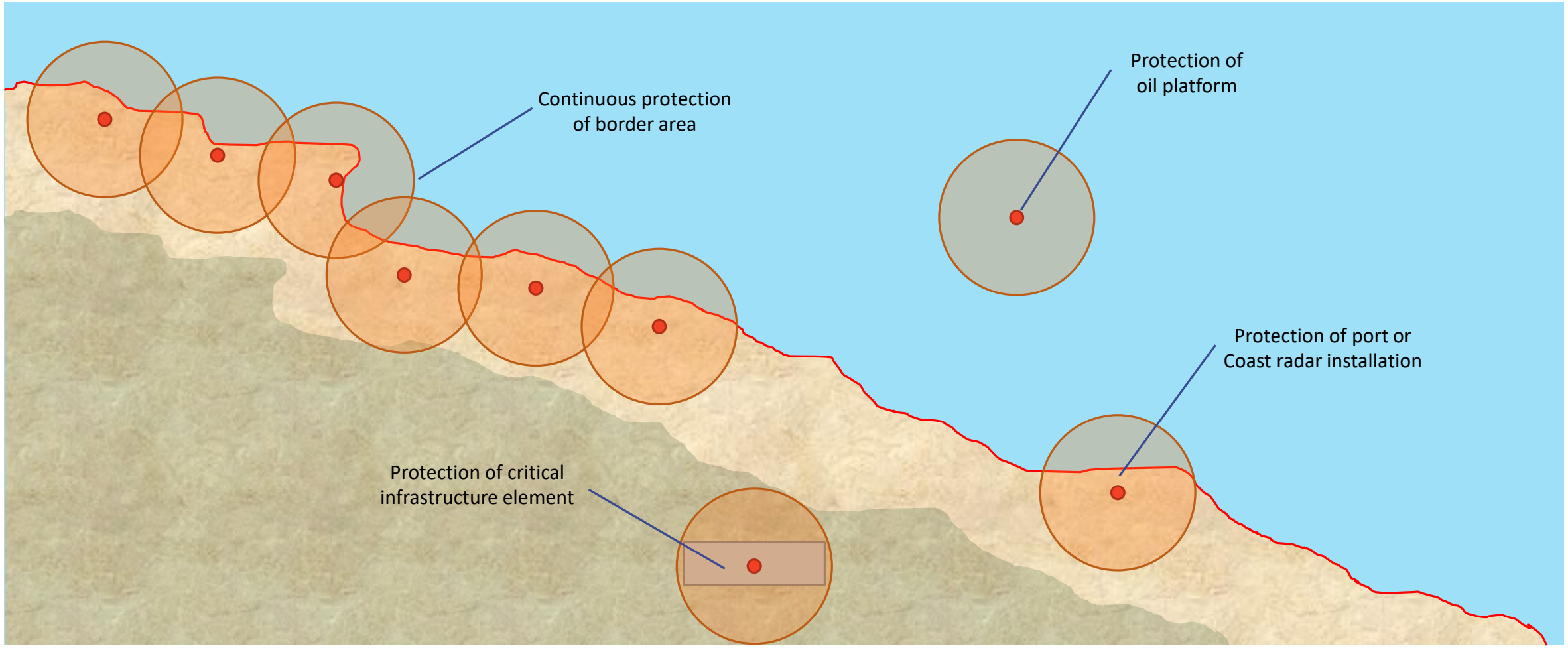
- further development of **devices and sensors for maritime targets and environment** (e.g. fit for mobile platforms) easily deployable on field and with **limited impact on spectrum environment**.
- development of specific, **early identification, tracking and fusion** algorithms
- operation in **network configurations** together with other systems for improved performances

What is the proposed SafeShore solution?

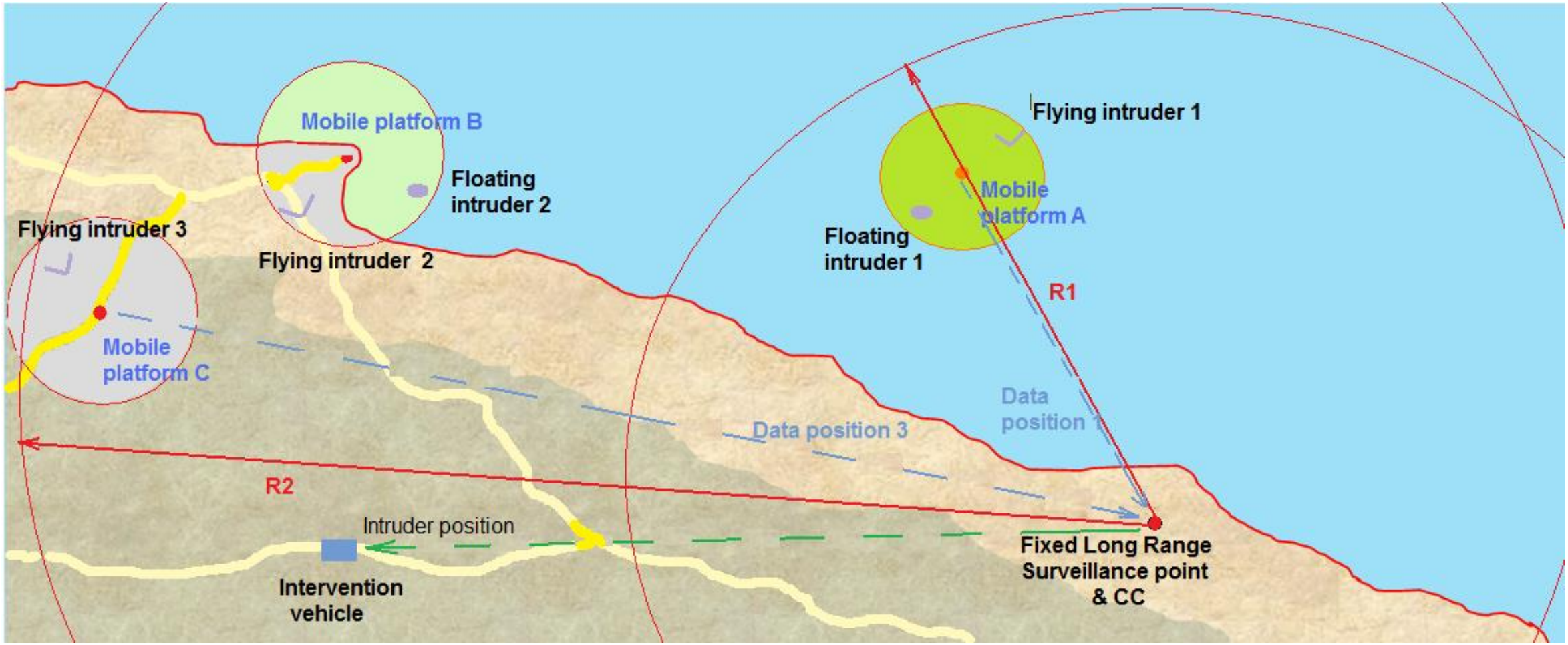
- **Mission**
  - Detection of **low altitude RPAS and their remote control equipment** involved in unauthorized surveillance and offensive actions (delivery of explosive charges or small projectile attacks), launched from boats, ships or land, in border area harbours, in coast radar locations, at river border crossings and on-board oil platforms and large ships.
  - Detection of **small vessels coming to shore**
  - Detection of **humans emerging from the sea**

- **The SafeShore system need to be used as:**
  - **stationary detection point**
    - in harbour areas, at river border crossing, to detect remote delivery of explosives or chemical weapons, and border trafficking of drugs
    - for coast radars, to detect remote delivery of explosive charges
  - **stationary chain-of-detectors** along high-risk border areas, to provide long term protection in areas with persistent problems
  - **mobile deployable system** in areas where intelligence predicts higher volume of illegal or threatening activities.

How will the SafeShore system be set up?



How will the SafeShore system be set up?



Compatibility Requirements

- In line with EUROSUR framework
- Compatible with the SCOMAR command and control system
- Compatible with Maritime Cross Point command and control system
- Differentiating between legal and illegal flights (detection results)
- Secure data recording and data stored for an appropriate period
- In accord with:
  - European Human Rights Convention
  - Charter Fundamental Rights in European Union
  - European Data Protection Directive
- Compatible with future RPAS (automatic) identification and registration systems
- Ethics, health and safety procedures conforming to the local / national guidelines / legislation
- Comply with IEC 61508 'Functional safety of electrical, electronic and programmable electronic (E/E/PE) safety-related systems'

SafeShore

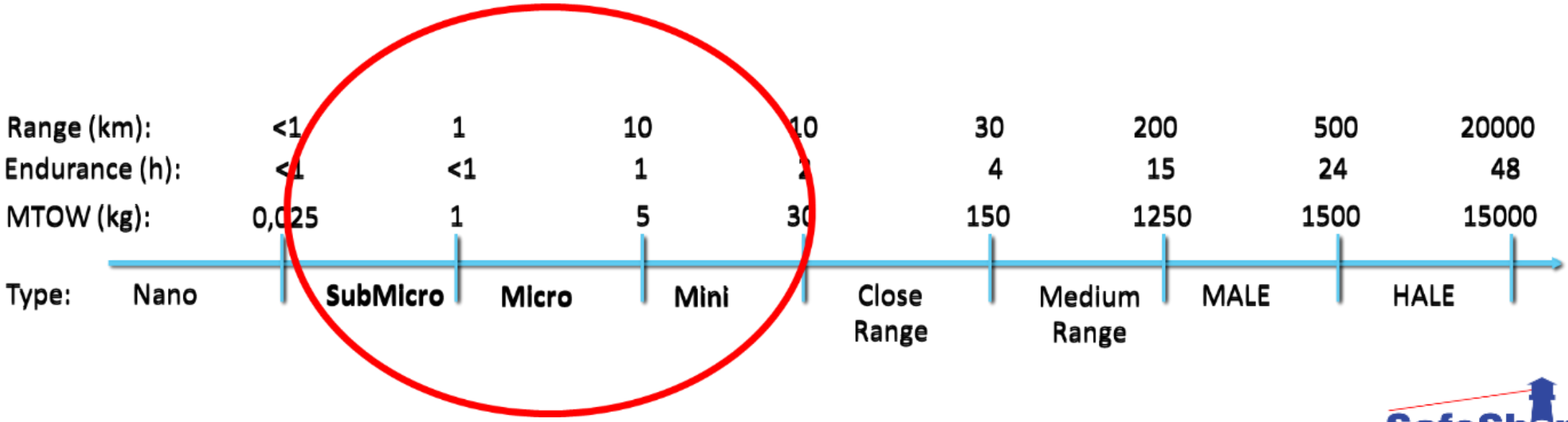
Operational and Functional requirements

1. ***The research activity on an effective Counter Remotely Aircraft System is strongly impelled by the operational requirements of the LEAs and naturally follow both the course of the latest terrorist events and technological development.***

2. ***From an end-user point of view, the implemented sensing and sensor processing modality (which includes all levels of data fusion) is irrelevant: it is the end result of the resulting system as a whole which counts!***

Detection targets - RPAS

- Any RPA and its operator according to ICAO classification – VLL up to 400ft, non-segregated space, VLOS / BVLOS, RLOS / BRLOS
- Minimum 3 RPAS simultaneously, autonomously, asynchronously, in real time
- The aim of the SafeShore – only RPASs which are designed to be used by civilians in recreational and commercial applications (generally RPASs are used for civil or military goals)



Targets assessed as threatening vectors

Threats	Appropriate RPAS type / classification
Violation of privacy	Quadcopter ≤ 2 kg
Intelligence (ISTAR – information, surveillance, target acquirement and reconnaissance)	Quadcopter ≤ 2 kg; Glider
Weapons and ammunition transport	Quadcopter ≤ 20 kg
Terrorist attacks using weapons, bombs, grenades, radioactive materials, etc.	Quadcopter ≤ 20 kg
Intentional collide with other authorized aircraft vehicles	All quadcopter types; Jet turbine
Using drones as projectiles (kamikaze drones)	Jet turbine
Unintentional collide with other authorized aircraft vehicles	All quadcopter types; Glider Jet turbine
People injuring	All quadcopter types; Jet turbine
Propaganda (looking for headlines)	Quadcopter ≤ 2 kg
Critical infrastructure, properties and goods damage	All quadcopter types; Jet turbine
Transport of the illegal objects (smugglers)	Quadcopter ≤ 20 kg; Glider
Stopping or slowing commercial RPASs' industry development	N/A

Targets assessed as threatening vectors

1. Low cost of the recreational and commercial RPASs
   - So far there are not one C-RPAS with one hundred successful rate
   - For terrorist forces it is worth spending money on even dozens of RPAS if only one gets the target
2. Weakness of the export control
   - Dual use goods
3. Gaps into existing regulatory framework
   - Control, registration, trading and use of recreational and commercial RPASs
   - Carefully rethink legal challenges on using C-RPAS tools
     - ✓Privacy violation
     - ✓How can legally label and treat as hostile or at least malicious
     - ✓There are legal references which convict destruction or taking away someone else proprietary
     - ✓Jamming or interfering with authorized radio communication
     - ✓Damaging an authorized computer program

SafeShore

Targets assessed as threatening vectors

1. Lack of the effective C-RPAS technology
   - There is not a common standard for an effective C-RPAS technology
2. Deployment challenges
3. Misunderstanding by the different decision level of the real threat dimension
4. Technological rapidly development
5. Most of the recreational and commercial RPASs are already getting ISTAR capabilities
6. Recreational and commercial RPASs could be easily modified to get military features and capabilities
7. Environments where malicious RPASs can be used

Targets risk level assessment

Sometimes the safety risk level of the effects of the counter measures could be higher than the potential risks of the offending RPAS!

1. ***Type of target***
2. ***Direction of arrival***
3. ***Range***
4. ***Velocity***
5. ***Estimated time of arrival***
6. ***Number of the target that have been detected and are tracking in the same time***
7. ***Number of sensors that have confirmed the target***
8. ***Altitude***
9. ***Interrogation results of other data bases***
10. ***Target's size***

SafeShore

RPASs assessed as threatening vectors

Mitigating the threats of illegal use of the RPASs envisages:

1. Legal
2. Technological aspects
3. An effective counter RPAS

Five “kill chain” model:

Detection

Classification

Prioritization

Tracking

Neutralization

Forensic

For what SafeShore was designed for

General requirements

1. Detection distance & intervention time (heavily interlinked and depend on scenarios)
2. Detection speed
3. Detection accuracy ($Accuracy = 1 - \%_{FalsePositive} - \%_{FalseNegative}$)
   - Machine validation
   - Human validation
4. Position accuracy and spread
5. Accuracy of velocity magnitude and direction
6. Environmental resistance
7. Operating temperature range
8. Wind resistance
9. Wave height
10. Environmental issues
11. Exploitation requirements

Functional requirements

1. Interoperability
   - Output data format
   - Interoperable with the command and control systems
2. Communication
   - Secured links
   - Broadband Mobile Network for Public Safety applications
   - Flexibility to switch communication technology from one country to another
   - Flexibility to switch communication technology from one applicability to another
   - Web application to push-alarms from SafeShore system
3. Deployment
4. Automatic assessment and displaying of the criticality of alerts on SafeShore interface (based on parameters asked by end-users)
5. Concept of operation

Functional requirements

Concept of operation:

1. Detection of the threat / threats
2. Threat / threats assessment
3. The alarm sending
4. Push-notifications on the web application
5. Field team response

Requirements summarization

User requirements categories:

1. Command & Control - 28
2. Document
3. Generic - 30
4. Prototype -25
5. Sensing – 41

Requirements evaluation

Target Performance levels

Validation scenarios:

1. Maritime Border Protection (primary scenarios)
2. Maritime Public Order
3. Security

Validation scenarios:

1. Static VIP protection for major events
2. Human traffic
3. Drugs traffic
4. Fishing vessel monitoring
5. Monitoring of kite-surfers
6. Critical infrastructure protection
7. Protection against terrorist attacks coming from off-shore
8. Search and rescue operation
9. Monitoring of hostile RPAS during land border infiltration
10. Smuggling vessels

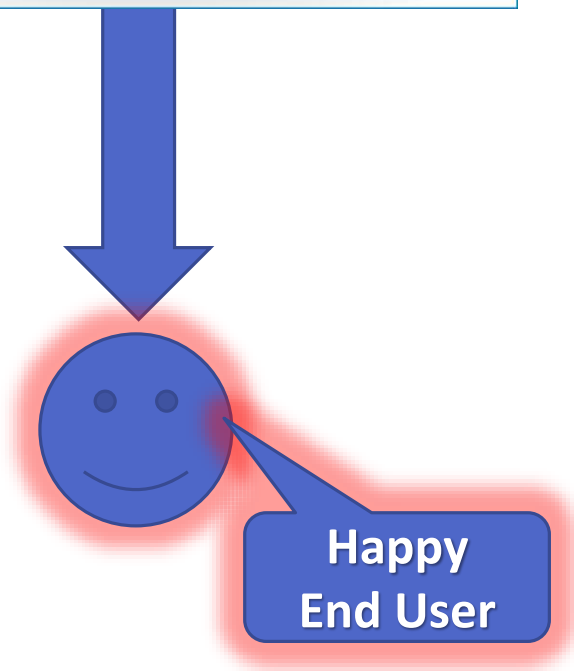
Traceability matrix for each validation scenarios

Identified Key Performance Indicators

Capability score for qualitative assessment of the target performance levels

Way ahead…

- Further integration:
  - Use a complete mix of sensors (e.g. passive radar that is using “electro smog”, B-field detection)
- A large and strong C-RPAS community (LEAs, regulation, research and industry)
- Fill the gaps on legislation
- C-RPAS technology standardization
- Integration into the foreseen mobile broadband network for Public Safety applications (4G/LTE technology) – synergy between this project and other EC major project
- Appropriate for deployment over metropolitan area / adaptability to Other Use Cases
- Solution for a complete C-RPAS solution (neutralization and forensic phases need to be added) / to be used in combination with various C-RPASs measures
- Push from TRL 6 system to a TRL 9 product
  - ➔ Commercial partners within SafeShore

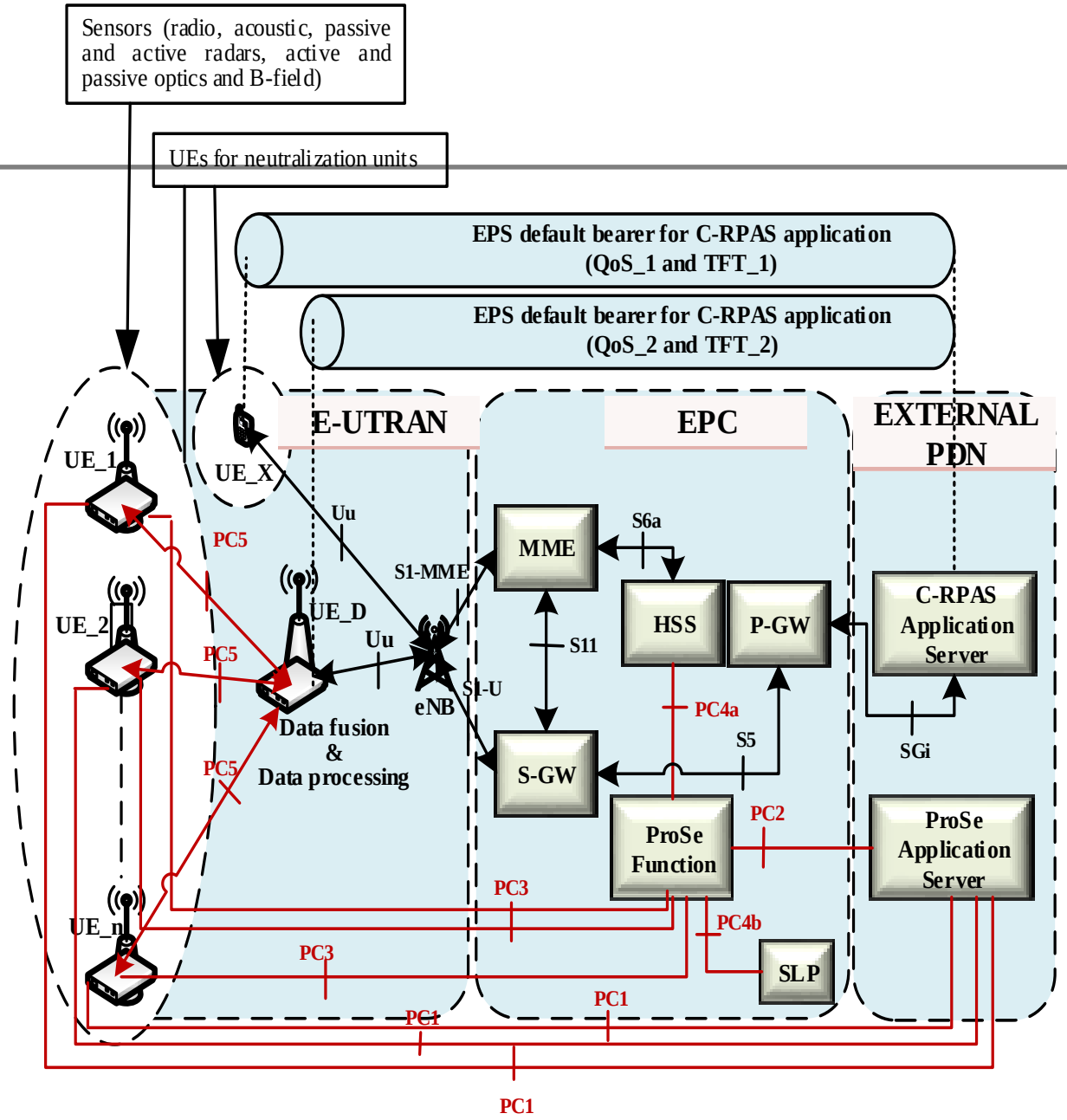


SafeShore

Corespondence between C-RPAS requirements and the Mobile Broadband Communications for Public Safety

1. Data and video information flow between sensors and Data fusion and Data processing unit.
2. Preponderant traffic from sensors towards Data fusion and Data processing unit.
3. A high level of availability and resilience.
4. Multimedia group communications.
5. Proximity-based services (devices are sensing each other).
6. A high reliability network including isolated network operation (fall backhaul connections).
7. C-RPAS is a mission-critical system and accordingly the information flow from sensors towards Data fusion and Data processing and further toward Command and Control Room and then towards neutralization units must be prioritized and traffic guaranteed.
8. Robust, certified and proved security solutions for authentication, confidentiality and data integrity.
9. Extended range of operation.
10. Dynamically changing of terminals configurations and parameters.
11. The mobile network should be a transparent carrier service.

SafeShore


Sensors (radio, acoustic, passive and active radars, active and passive optics and B-field)
UEs for neutralization units
EPS default bearer for C-RPAS application (QoS_1 and TFT_1)
EPS default bearer for C-RPAS application (QoS_2 and TFT_2)
E-UTRAN
EPC
EXTERNAL PDN
UE_1
UE_X
UE_2
UE_D
UE_n
Uu
PC5
S1-MME
MME
S6a
HSS
P-GW
C-RPAS Application Server
S11
S1-U
eNB
Data fusion & Data processing
PC4a
S5
SGi
S-GW
ProSe Function
PC2
ProSe Application Server
PC3
PC4b
SLP
PC1

QUESTIONS?

SafeShore

12th CoU Meeting,

4th December, 2018, Brussels, Belgium