Test Methods for Counter-UAS Systems

Alexander Borghgraef
Royal Military Academy
alexander.borghgraef@mil.be

Geert De Cubber
Royal Military Academy
geert.de.cubber@mil.be

This project has received funding from the European Union's
Internal Security Fund under Grant Agreement 101034655

Problem Statement

- 2022: >500 commercial C-UAS systems
- Different systems <> different use case scenarios
- Performance claims often unsupported by evidence
- Different test methodologies make comparison impossible
- **No Silver Bullet**
- Each operational environment will require different cUAS Detection Tracking and Identification capabilities
- **NEUTRALISATION not covered by Project COURAGEOUS**

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Problem Solution

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate D: Law Enforcement and Security
Unit D.2 : Counter-Terrorism

European Programme for counter UAS systems testing

COURAGEOUS

This project has received funding from the European Union's
Internal Security Fund under Grant Agreement 101034655

COURAGEOUS

Who?

End users

HELLENIC POLICE

Police

ROMÂNIA SERVICIUL DE PROTECȚIE ȘI PAZĂ

POLICE LËTZEBUERG

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

INTERPOL

Estonian Police and Border Guard Board

Research & Technology Org.

RMA Royal Military Academy Brussels

TNO

Military University of Technology WAT

Universidad de Sevilla

KEMEA

Standardisation Org.

asro ORGANISMUL NAȚIONAL DE STANDARDIZARE

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

ISF POLICE

Timetable of Activities

	Responsible	Month	April M01	May M02	June M03	July M04	August M05	September M06	October M07	November M08	December M09	January M10	February M11	March M12	April M13	May M14	June M15	July M16	August M17	September M18	October M19	November M20	December M21	January M22	February M23	March M24	April M25	May M26	June M27	July M28	August M29	September M30	October M31	November M32	December M33	January M34	February M35	March M36	April M37	May M38	June M39	July M40	August M41	September M42
WP1	**RMA**	**Management and Coordination of the Action**																																										
A1.1	RMA	Management of the consortium, financial administration & reporting	D1.1																				D1.2																					
A1.2	RMA	Technical Coordination, risk assessment & risk management																																										
A1.3	KEMEA	LEA community engagement programme management																																										
A1.4	RMA	Safety, Security, Ethical & Legal compliance monitoring																																										
WP2	**KEMEA**	**Standard scenario development**																																										
A2.1	INT	Report on previous incidents & identifications of gaps			*D2.1*				D2.1																																			
A2.2	WAT	Review of current C-UAS framework (methods & technologies)			*D2.2*				*D2.2*					D2.2																														
A2.3	KEMEA	Definition of Standard Scenarios			*D2.3*				*D2.3*					*D2.3*					D2.3-1									D2.3-2																
A2.4	KEMEA	Risk analysis and definitions of metrics							*D2.4*					*D2.4*					*D2.4*				D2.4-1				D2.4-2																
WP3	**SPP**	**Performance requirements**																																										
A3.1	SPP	Operational needs on the basis of the standard scenarios												*D3.1*					*D3.1*				D3.1-1				D3.1-2																
A3.2	WAT	Functional and performance requirements and metrics												*D3.2*					*D3.2*				D3.2-1				*D3.2*								D3.2-2								
A3.3	SPP	Develop an evaluation framework												*D3.3*					*D3.3*				D3.3-1				*D3.3*								D3.3-2								
WP4	**TNO**	**Test methodology development**																																										
A4.1	USE	Generation of test environment												*D4.1*					*D4.1*				D4.1-1				*D4.1*			D4.1-2													
A4.2	TNO	Functional test development												*D4.2*					*D4.2*				D4.2-1				*D4.2*								D4.2-2								
A4.3	USE	Integral test development																	*D4.3*				*D4.3*				D4.3-1											D4.3-2					
A4.4	TNO	Validation method																					*D4.4*				D4.4-1											D4.4-2					
WP5	**USE**	**Performance testing**																																										
A5.1	USE	Test planning and logistics																					D5.1-1																				D5.1-2		
A5.2	KEMEA	Test execution																																										
A5.3	TNO	Test evaluation																																										
A5.4	RMA	Evaluation of results and methodology																																	D5.2								D5.3	
WP6	**INT**	**Dissemination, Exploitation and Standardisation**																																										
A6.1	INT	Communication, Dissemination & Exploitation Action Plan Development												*D6.1*					D6.1																										
A6.2	INT	Implementation																					D6.2																				D6.3	
A6.3	SPP	Standardisation Actions																																										D6.5

New Milestones	1 Project plan ready	2 Draft scenario review 1	3 Draft scenario review 2	4 Draft requirements review - Preliminary inputs for Romanian trial ready	5 Final scenario review - Results from Romanian trial incorporated	6 Draft test review - System ready for Greek test	7 Greek Test analysed	8 System ready for Belgian test	9 Belgian test analysed - Requirements completed	10 Test methodology complete - System ready for Spanish test	11 Project end
	M01	M03	M06	M12	M17	M21	M25	M29	M32	M35	M42

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Standard scenario development

- Report on previous incidents & identifications of gaps

- Review of current C-UAS framework (methods & technologies)

- Definition of Standard Scenarios

- Risk analysis and definitions of metrics

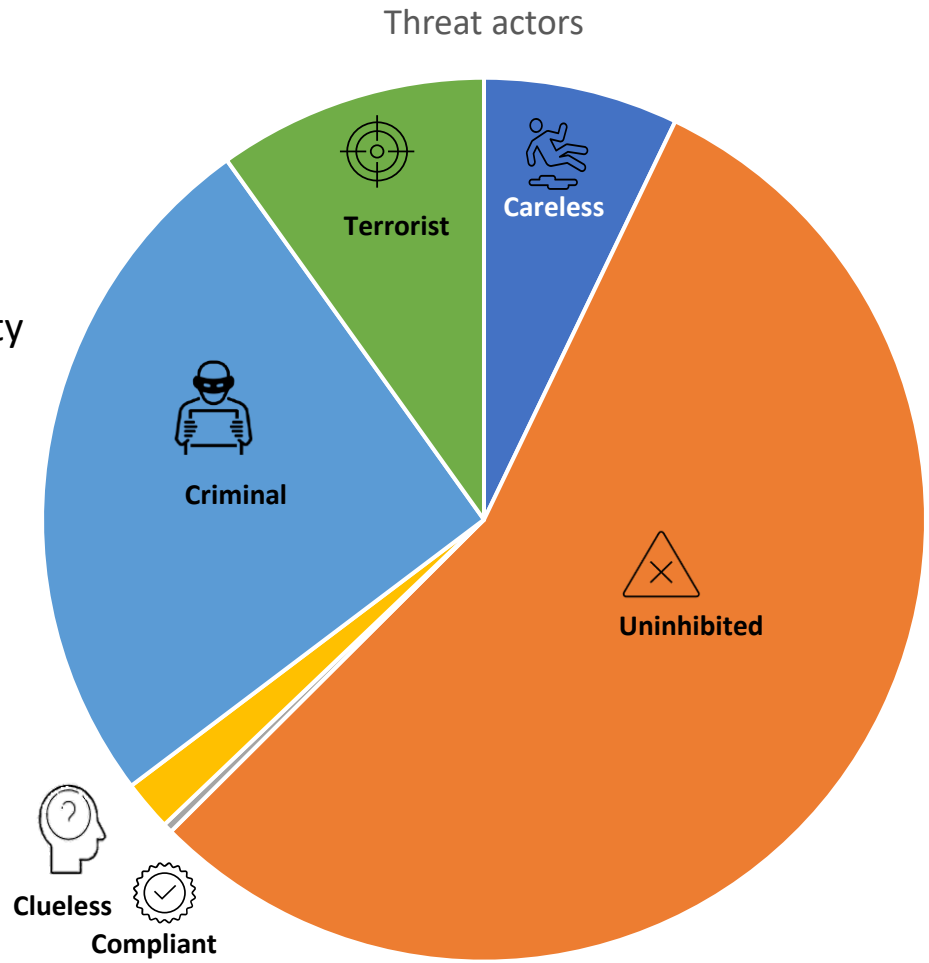
This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Standard scenario development

Task 2.1: Report on previous incidents & identification of gaps

- Extended literature review and research on previous drone related security threatening events covering EU MS and identification of gaps.
- Project Courageous has gathered eight hundred and twenty-three drone incidents from across the globe and has analyzed each of them to identify trends and any gaps that should be filled to ensure a coherent and cohesive approach to the drone threat across member states
- The analysis of previous drone incidents and identification of gaps has been created in order to understand the evolving incident landscape, involving drones and to identify gaps in current responses to such threats.

Leader: INT



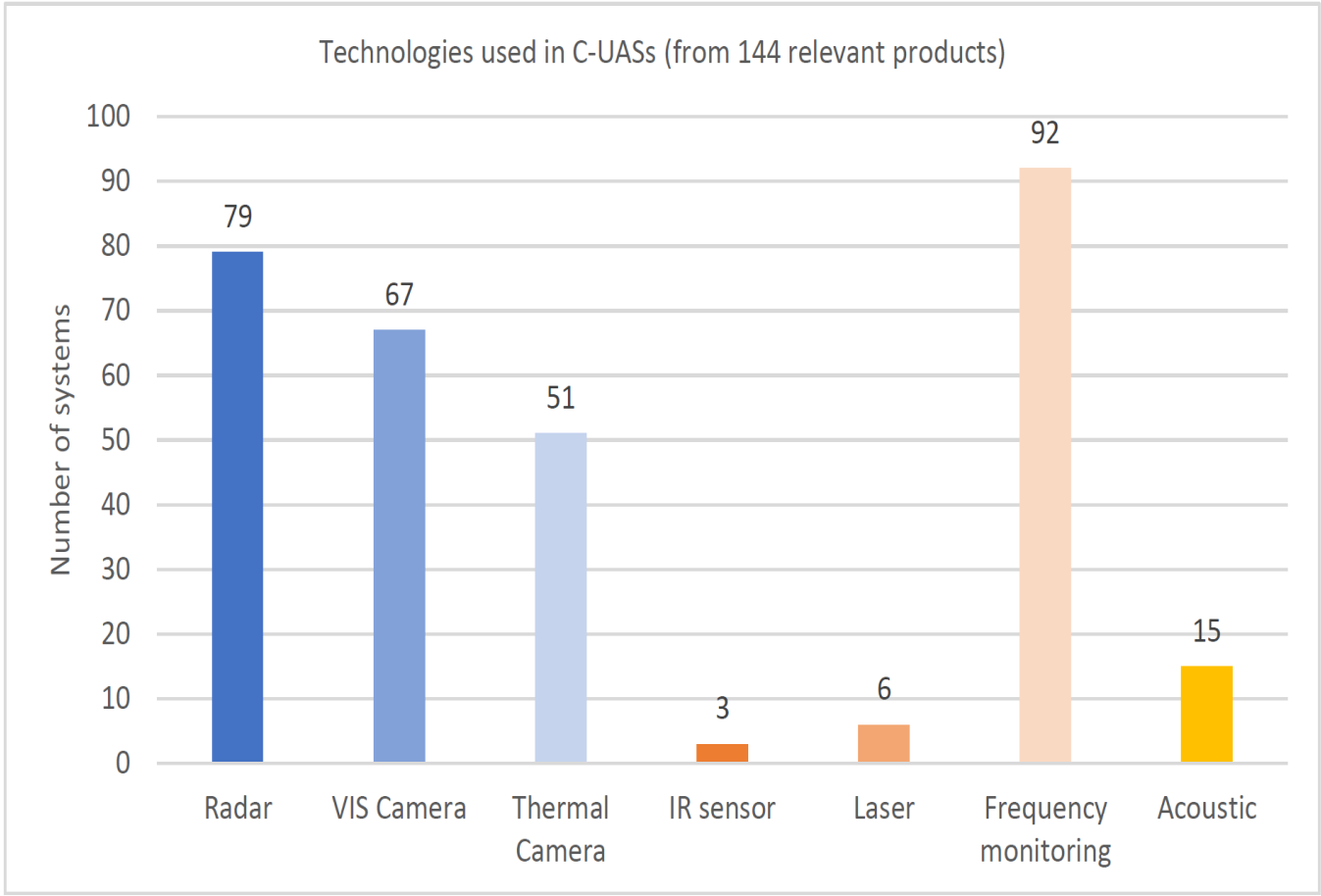
This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Standard scenario development

Task 2.2: Review of current C-UAS framework (methods & technologies)

- **Objectives:**
  - Review the currently available counter-drone technologies (260 anti-drone systems were initially collected and analyzed)
  - Established prevention and response methodologies
  - Enumerate the advantages and disadvantages all technologies and their combinations, in ord to develop comparative metrics for C-UAS solutions, for the next steps of the project

Leader: WAT



This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Standard scenario development

Task 2.3: Definition of Standard Scenarios

- **Objectives:**
  - Combine the report on previous incidents & identifications gaps and the review of current C-UAS framework
  - Ten (10) standard scenarios were developed, into the following three (3) main categories:
    - ❖ Sensitive Sites/Critical National Infrastructure
    - ❖ Public Spaces Protection/Events
    - ❖ Border Protection (Land – Maritime

Leader: KEMEA


Prison


Airport


Concert


Government building


Land border


Maritime border


International summit


Political rally


Stadium


Nuclear plant

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Standard scenario development

Task 2.4: Risk analysis and definitions of metrics

- **Objectives**:
  - Describes the level of risk of the standardized scenarios that were developed
  - Create a risk analysis matrix that merged the ten scenarios
  - Determine the Key Risk Indicators (KRIs) that covered all identified scenarios and use cases

Scenario	Total Risk
Scenario 1 - Target: Prison	264,3
Scenario 2 - Target: Airport	253,4
Scenario 3 - Target: Nuclear Plant	227,3
Scenario 4 - Target: Government Building	252,9
Scenario 5 - Target: Stadium	238,7
Scenario 6 - Target: Outdoor Concert	253,5
Scenario 7 - Target: Outdoor Political Rally	253,4
Scenario 8 - Target: International Summit	217,3
Scenario 9 - Target: Land Border	235
Scenario 10 - Target: Maritime Border	244,1

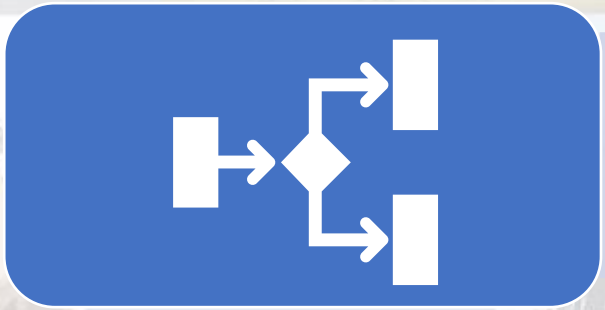
Leader: KEMEA

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Performance requirements

- Operational needs based on the standard scenarios

- Functional and performance requirements and metrics



- Develop an evaluation framework

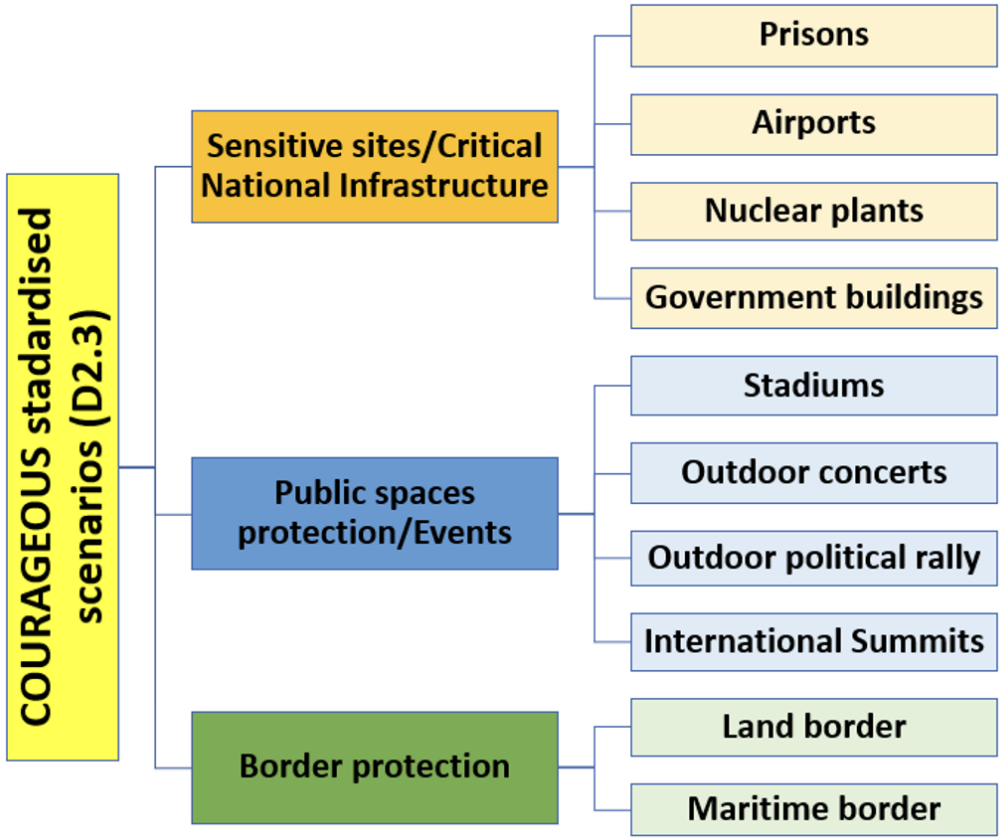
This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Performance requirements

A3.1 - Develop operational needs on the basis of the standard scenarios

Req. N°	
Req. Name	
Description	
Importance	

Field	Meaning of the field	Format
Req. Nº	*Unique code identifying each requirement for future references.*	*GR followed by two numbers - Ex. GR05, for a general requirement* *SR followed by two numbers - Ex. SR05, for a specific requirement*
Req. Name	*Concise description of the requirement.*	*Free text.*
Description	*More detailed description of the requirement, with special emphasis on the motivation behind the requirement.*	*Free text*
Importance	*Assessment by project stakeholders of the importance of each requirement for the project.*	*Value from a list:* • *Shall* • *Should* • *May*



This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

WP3 - Define the performance requirements of C-UAS systems

A3.2 - Develop C-UAS system functional and performance requirements and metrics

Based on a defined set of standard scenarios and related operational needs, then developed into detailed functional and performance requirements that UAS detection, tracking and identification systems must meet, **a set of metrics has been developed with which to measure them**. Both requirements and metrics should be as technology independent as possible, and must be clearly defined and measurable for **two reasons**:

a) will be used as a basis for developing a testing methodology; and

(b) may be provided to C-UAS manufacturers who may be prepared to have their systems tested under the COURAGEOUS programme.

In order for the metrics to objectively evaluate individual systems and have added value in the project, it is necessary to develop them in such a way that they are as **universal and transparent** as possible. Can be used for different C-UAS and for equal measurement conditions - test environment.

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

WP3 - Define the performance requirements of C-UAS systems

A3.2 - Develop C-UAS system functional and performance requirements and metrics

Four thematic groups have been distinguished in the metrics:

1. test facility specification (UAS),
2. environmental conditions,
3. specification and equipment of the test site,
4. parameters subject to testing for detection, tracking and identification,

Within each of the metrics, ranges have been defined for which weighting points will be assigned, resulting in a numerical value that will determine the quality of the proposed solution.

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

WP3 - Define the performance requirements of C-UAS systems

A3.3 - Develop an evaluation framework

Will provide a structured tool to systematically document, review, compare and evaluate test results.

The result is intended to create a common baseline understanding amongst Member State authorities concerning the effectiveness of different C-UAS solutions, which in turn shall support decision-making at national level regarding the development, procurement and/or operational deployment of different systems.

SCENARIOS

MEASURABLE RESULTS

FLEXIBILITY

ITERATIVE PROCESS

STAKEHOLDERS

VERIFIABLE ACTIVITIES

TECHNOLOGY DIVERSITY

TESTS FOUNDATION

TEAMWORK

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Test methodology development

- Generation of test environment

- Functional test development

- Integral test development

- Validation method

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

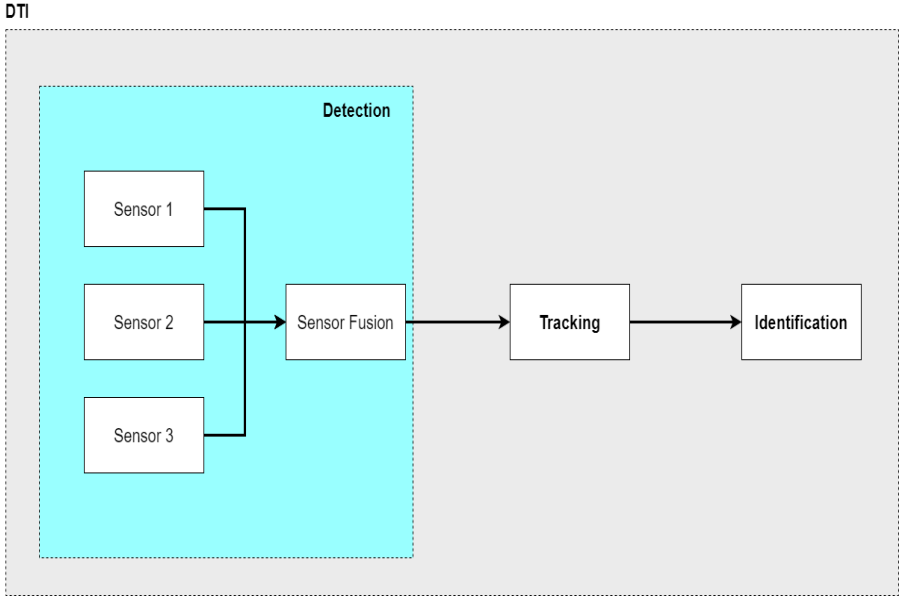
WP4 - Test methodology development

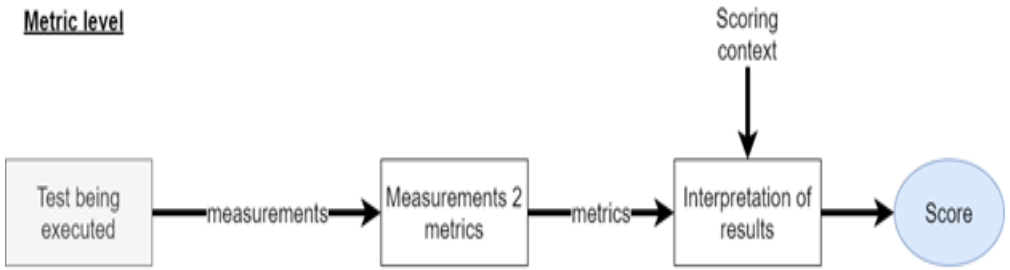
- Main WP4 Objectives:
  - A methodology for testing of Detection Tracking and Identification (DTI) systems and sub systems under realistic conditions and scenarios
    - A methodology that helps the end-users evaluate a DTI system: does the system meet operational needs/requirements from the end-user perspective?
    - It is **NOT** about the ranking or comparison of DTI systems
  - Key aspects
    - Standard, relevant, user-defined test scenarios
    - Black-box validation approach
    - Future-proof methodology
    - Technology agnostic
    - Field validation & iterative design improvement

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

WP4 - Test methodology development

- COURAGEOUS test methodology concept (1/2):
  - Start with user-defined test scenarios
    - Standardized test scenarios lead to quantifiable data (detection, tracks, classifications)
    - Context is important (objects and area to monitor (and how), metrics/KPIs, deployment of systems)
  - Derive metrics from the DTI output (from test scenarios)
    - Examples of metrics: detection range, track continuity, false alarm rate, object classification
  - Generate ‘score’ per DTI functionality from the results
    - @component, @system (integrated) level.
    - Score is context dependent (e.g. scenario aspects)

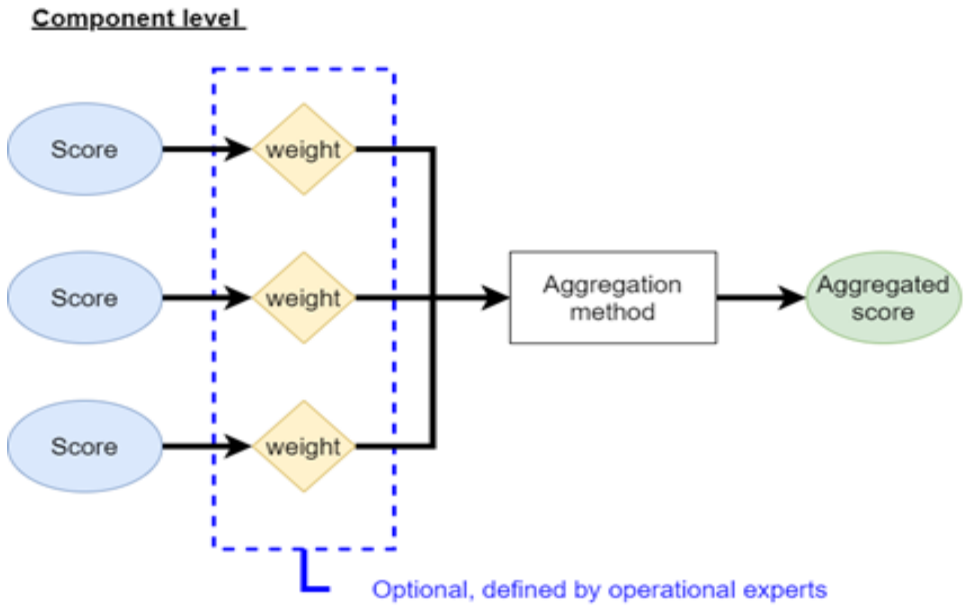




This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

WP4 - Test methodology development

- COURAGEOUS test methodology concept (2/2):
  - Optionally weigh the scores
    - Based on expert/end-user input (e.g., prioritization of certain metrics above others)
  - Translate the (weighted) ‘scores’ into a total ‘score’ per DTI
- Enables
  - Evaluation of DTIs based on test results given the test scenarios (including context)



This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Performance testing

- Test planning and logistics

- Test execution

- Test evaluation

- Evaluation of results and methodology

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Performance testing - Planning

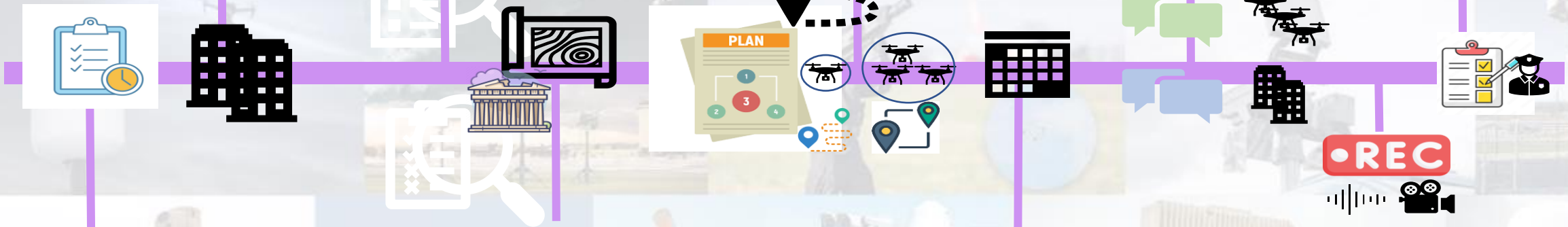
Arrange DTI companies
What to expect

Expectations of stakeholders:
- What is acceptable?
- Expected outcomes
- Prologue (check-in, briefing all involved)

Flight plan(s)
- 1 route or multiple
- Flight height
- 1 or multiple drones
- Ground truth & recording of ground truth
- ....

Interface agreements:
- Drones
- DTIS

Evaluation:
- End-users
- Prologue, debrief, check-out
- Analysis of results, recommendations



Division of responsibilities and tasks between partners

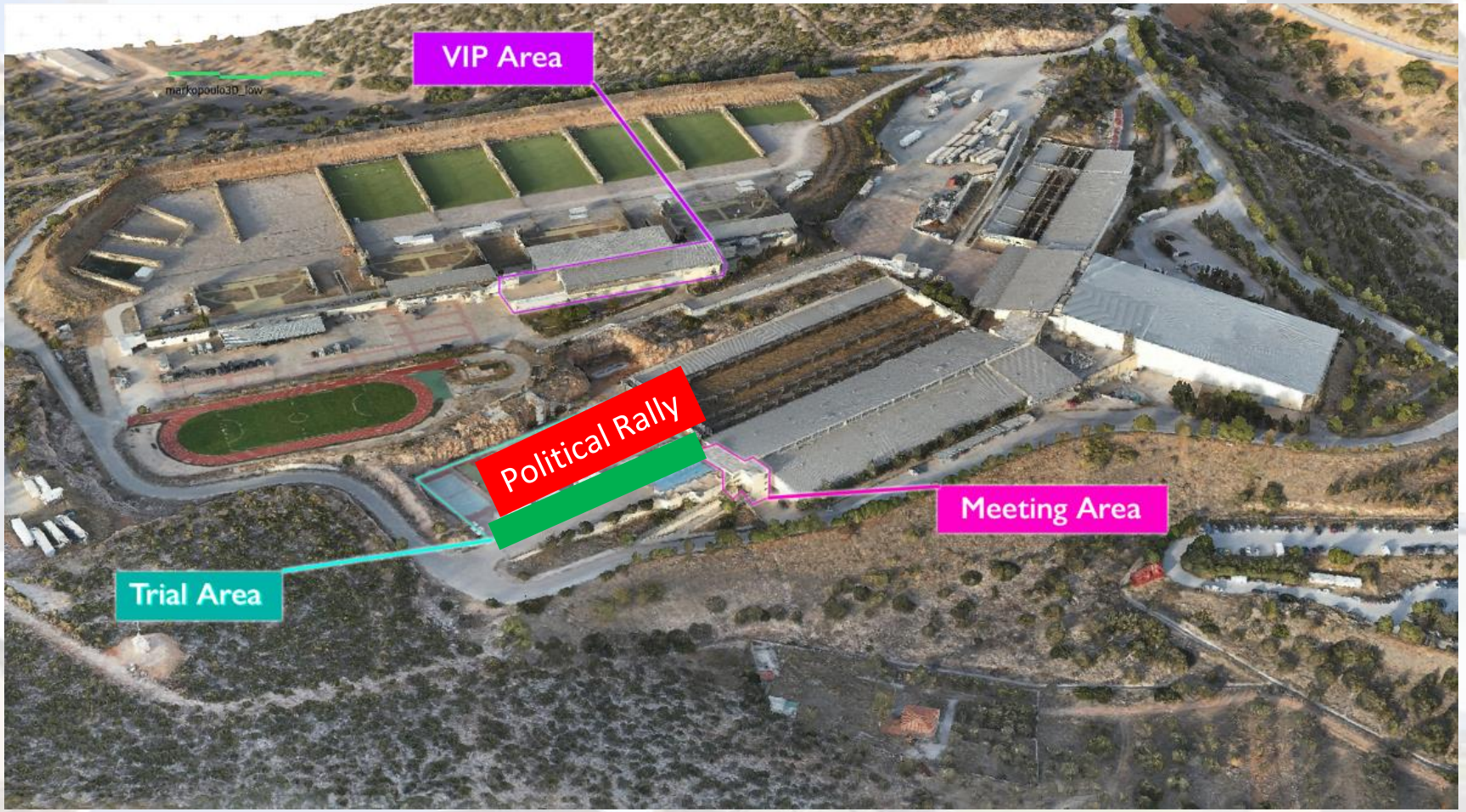
Clear idea of what the trial site looks like:
- Locations of DTI(s)
- Area of Interest (urban, open field, etc?)

Trial schedule:
- Opening
- Setting up
- Testing: who when
- Closing
- ...

What to record / measure

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Performance testing – Trial 1



This project has received funding from the European Union's
Internal Security Fund under Grant Agreement 101034655

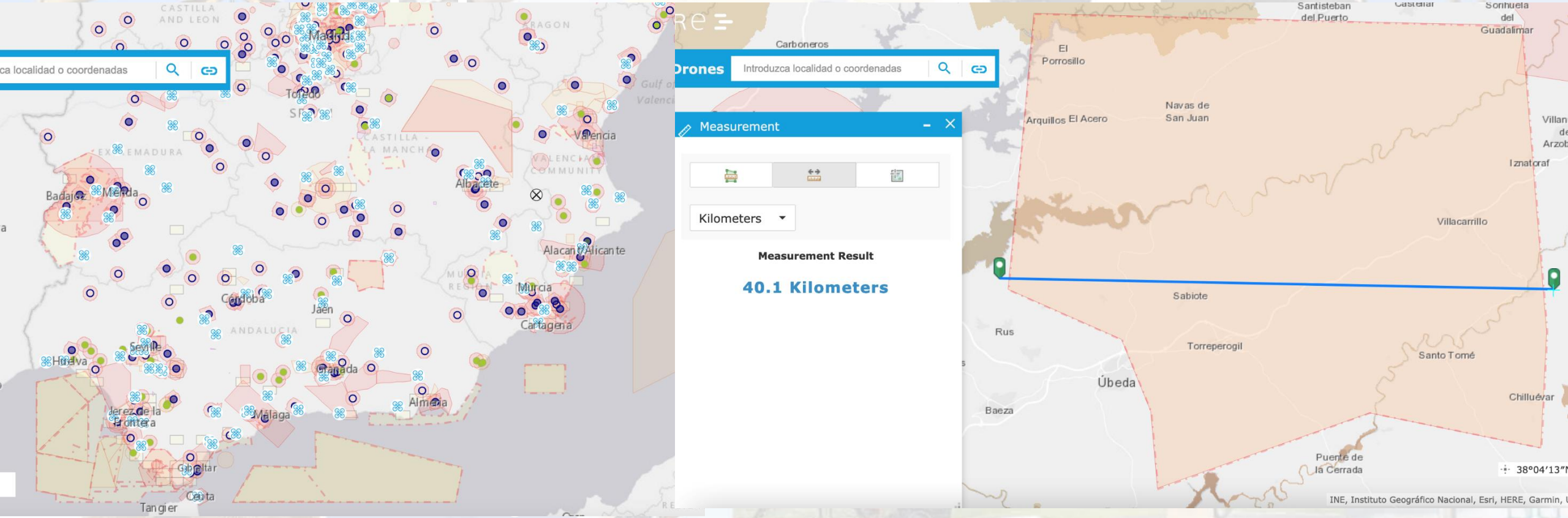
Performance testing – Trial 2

- Nieuwpoort, Belgium: Maritime shooting range – 2-6 October 2023

This project has received funding from the European Union's
Internal Security Fund under Grant Agreement 101034655

Performance testing – Trial 3

- ATLAS Flight Test Center: Segregated airspace (1000 Km^2) – Spring 2024



This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Project Impact Maximization

- Dissemination

- Standardization

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Dissemination

Five levels of dissemination:

- Intra-consortium: deliverables, reports: quantitative
- EU LEAs: CIRCABC platform: qualitative
- INTERPOL global network of LEAs
- Industry: Industrial partners officially registered as standardization partners: insight in pre-normative drafts
- Global Public

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Standardisation

Converge to a pre-standard ➔ CENELEC Workshop Agreement

How?

- Use data from deliverables produced in COURAGEOUS
- Discuss this approach with industry and amend work in COURAGEOUS based on industry inputs
- Validate the methodology with industry, e.g. during trials
- ➔ Should evolve to pre-standard CWA by June 2024

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

Conclusions

- We globally need a better common understanding of the performance & capabilities of counter-UAS technologies
- For this purpose, COURAGEOUS in working in the EU on a standardised counter-UAS testing methodology
- Results will be shared with the end-user community

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655

COURAGEOUS

Thank you for your attention

- Alexander Borghgraef
- Royal Military Academy
- alexander.borghgraef@mil.be

- Geert De Cubber
- Royal Military Academy
- geert.de.cubber@mil.be

This project has received funding from the European Union's Internal Security Fund under Grant Agreement 101034655