



# European Defence Fund (EDF)

## Call for proposals

EDF-2023-DA

Call for EDF **development actions**  
implemented via actual cost grants

Version 1.1  
22 June 2023



<b>HISTORY OF CHANGES</b>			
<b>Version</b>	<b>Publication Date</b>	<b>Change</b>	<b>Page</b>
1.0	13.04.2023	– Initial version.	
1.1	22.06.2023	<ul style="list-style-type: none"> <li>– Update of table of contents (page numbers only)</li> <li>– Addition of reference to adopted EDF work programme 2024 part 1 and removal of caveat on 2024 budget</li> <li>– Update of the call opening date</li> <li>– Addition of provisions following the Council Implementing Decision (EU) 2022/2506 of 15 December 2022 on measures for the protection of the Union budget against breaches of the principles of the rule of law in Hungary</li> </ul>	<ul style="list-style-type: none"> <li>– 5-6</li> <li>– 7 105</li> <li>– 105</li> <li>– 108</li> </ul>
		–	
		–	



**EUROPEAN COMMISSION**  
Directorate-General for Defence Industry and Space  
DEFIS.A – Defence Industry

## CALL FOR PROPOSALS

### TABLE OF CONTENTS

0. Introduction .....	7
1. Background .....	8
2. Type of action and funding rate — Objectives — Scope and types of activities — Functional requirements — Expected impact — Specific topic conditions .....	9
Type of action and funding rate .....	9
Specific topic conditions .....	12
EDF-2023-DA-MCBRN-FCS: Federating CBRN systems .....	12
Objectives .....	12
Scope and types of activities .....	13
Functional requirements .....	15
Expected impact .....	17
EDF-2023-DA-C4ISR-LCOM: Laser communications .....	17
Objectives .....	17
Scope and types of activities .....	18
Functional requirements .....	21
Expected impact .....	21
EDF-2023-DA-C4ISR-TRPAS: Tactical RPAS .....	22
Objectives .....	22
Scope and types of activities .....	23
Functional requirements .....	25
Expected impact .....	28
EDF-2023-DA-C4ISR-DAA: Detect and avoid .....	29
Objectives .....	29
Scope and types of activities .....	30
Functional requirements .....	34
Expected impact .....	35
EDF-2023-DA-SENS-GRID: Sensor grid .....	36
Objectives .....	36
Scope and types of activities .....	37
Functional requirements .....	40

Expected impact .....	41
EDF-2023-DA-CYBER-CSA: Full-Spectrum Cyber Situational Awareness for enhanced Cyberspace Operations Support.....	41
Objectives.....	41
Scope and types of activities .....	42
Functional requirements .....	45
Expected impact .....	46
EDF-2023-DA-CYBER-DAAI: Deployable Autonomous AI Agent.....	46
Objectives.....	46
Scope and types of activities .....	47
Functional requirements .....	50
Expected impact .....	51
EDF-2023-DA-SPACE-SSA: Initial operational capacity for Space situational awareness C2 and sensors .....	51
Objectives.....	51
Scope and types of activities .....	52
Functional requirements .....	55
Expected impact .....	56
EDF-2023-DA-MATCOMP-MJR-CBDIN: Technologies and processes for maintenance, joining and repair through an innovation test hub .....	56
Objectives.....	56
Scope and types of activities .....	58
Functional requirements .....	63
Expected impact .....	64
EDF-2023-DA-AIR-STFS: Smart technologies for next generation fighter systems.....	65
Objectives.....	65
Scope and types of activities .....	65
Functional requirements .....	68
Expected impact .....	69
EDF-2023-DA-AIR-SPS: Self-protection systems.....	69
Objectives.....	69
Scope and types of activities .....	70
Functional requirements .....	72
Expected impact .....	74
EDF-2023-DA-AIRDEF-CUAS: Counter unmanned aerial systems .....	74
Objectives.....	74
Scope and types of activities .....	75
Functional requirements .....	77
Expected impact .....	79
EDF-2023-DA-GROUND-MBT: Main battle tank platform systems.....	79
Objectives.....	79
Scope and types of activities .....	80
Functional requirements .....	82
Expected impact .....	84
EDF-2023-DA-GROUND-IFS: Long-range indirect fire support capabilities for precision and high efficiency strikes.....	85

Objectives.....	85
Scope and types of activities .....	85
Functional requirements .....	87
Expected impact.....	89
EDF-2023-DA-NAVAL-MMPC: Modular and multirole patrol corvette .....	89
Objectives.....	89
Scope and types of activities .....	90
Functional requirements .....	93
Expected impact.....	94
EDF-2023-DA-UWW-ASW: Unmanned anti-submarine and seabed warfare .....	94
Objectives.....	94
Scope and types of activities .....	95
Functional requirements .....	98
Expected impact.....	99
EDF-2023-DA-UWW-MCMC: Future maritime mine countermeasures capability .....	99
Objectives.....	99
Scope and types of activities .....	100
Functional requirements .....	103
Expected impact.....	103
3. Available budget.....	103
4. Timetable and deadlines .....	105
5. Admissibility and documents .....	105
6. Eligibility.....	106
Eligible participants (eligible countries).....	106
Consortium composition .....	108
Eligible actions and activities.....	108
Geographic location (target countries).....	109
Duration .....	109
Project budget.....	110
Ethics.....	110
Security.....	110
7. Financial and operational capacity and exclusion.....	111
Financial capacity .....	111
Operational capacity .....	112
Exclusion .....	112
8. Evaluation and award procedure .....	113
9. Award criteria.....	114
10. Legal and financial set-up of the Grant Agreements.....	117
Starting date and project duration .....	117
Milestones and deliverables.....	117
Form of grant, funding rate and maximum grant amount.....	117
Budget categories and cost eligibility rules.....	118
Reporting and payment arrangements.....	119
Prefinancing guarantees .....	120

Certificates .....	120
Liability regime for recoveries .....	121
Provisions concerning the project implementation .....	121
Other specificities .....	122
Non-compliance and breach of contract .....	122
11. How to submit an application .....	122
12. Help .....	123
13. Important .....	124
Annex 1 .....	127
Annex 2 .....	129
Annex 3 .....	131

## 0. Introduction

This is a call for proposals for EU **action grants** in the field of collaborative defence research and development under the **European Defence Fund (EDF)**.

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2018/1046 ([EU Financial Regulation](#))
- the basic act (EDF Regulation [2021/697](#)<sup>1</sup>).

The call is launched in accordance with the Work Programmes 2023 Part II<sup>2</sup> and 2024 Part I<sup>3</sup> and will be managed by the **European Commission, Directorate-General for Defence Industry and Space (DG DEFIS)**.

The call covers the following **topics**:

- **EDF-2023-DA-MCBRN-FCS: Federating CBRN systems**
- **EDF-2023-DA-C4ISR-LCOM: Laser communications**
- **EDF-2023-DA-C4ISR-TRPAS: Tactical RPAS**
- **EDF-2023-DA-C4ISR-DAA: Detect and avoid**
- **EDF-2023-DA-SENS-GRID: Sensor grid**
- **EDF-2023-DA-CYBER-CSA: Full-Spectrum Cyber Situational Awareness for enhanced Cyberspace Operations Support**
- **EDF-2023-DA-CYBER-DAAI: Deployable Autonomous AI Agent**
- **EDF-2023-DA-SPACE-SSA: Initial operational capacity for Space situational awareness C2 and sensors**
- **EDF-2023-DA-MATCOMP-MJR-CBDIN: Technologies and processes for maintenance, joining and repair through an innovation test hub**
- **EDF-2023-DA-AIR-STFS: Smart technologies for next generation fighter systems**
- **EDF-2023-DA-AIR-SPS: Self-protection systems**
- **EDF-2023-DA-AIRDEF-CUAS: Counter unmanned aerial systems**
- **EDF-2023-DA-GROUND-MBT: Main battle tank platform systems**
- **EDF-2023-DA-GROUND-IFS: Long-range indirect fire support capabilities for precision and high efficiency strikes**
- **EDF-2023-DA-NAVAL-MMPC: Modular and multirole patrol corvette**

---

<sup>1</sup> Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092 (OJ L 170, 12.5.2021).

<sup>2</sup> Commission Implementing Decision C(2023) 2296 final of 29.03.2023 on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2023 - Part II.

<sup>3</sup> Commission Implementing Decision C(2023) 4252 final of 21.06.2023 on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2024 - Part I.

- **EDF-2023-DA-UWW-ASW: Unmanned anti-submarine and seabed warfare**
- **EDF-2023-DA-UWW-MCMC: Future maritime mine countermeasures capability**

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

We invite you to read the **call documentation** carefully, and in particular this Call Document, the Model Grant Agreement, the [EU Funding & Tenders Portal Online Manual](#) and the [EU Grants AGA — Annotated Grant Agreement](#).

These documents provide clarifications and answers to questions you may have when preparing your application:

- the [Call Document](#) outlines the:
  - background, type of action and funding rate, objectives, scope and types of activities, functional requirements, expected impact and specific topic conditions (sections 1 and 2)
  - timetable and available budget (sections 3 and 4)
  - admissibility and eligibility conditions, including mandatory documents (sections 5 and 6)
  - criteria for financial and operational capacity and exclusion (section 7)
  - evaluation and award procedure (section 8)
  - award criteria (section 9)
  - legal and financial set-up of the Grant Agreements (section 10)
  - how to submit an application (section 11)
- the [Online Manual](#) outlines the:
  - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
  - recommendations for the preparation of the application
- the [AGA — Annotated Grant Agreement](#) contains:
  - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant (*including cost eligibility, payment schedule, accessory obligations, etc.*).

You are also encouraged to visit the [DG DEFIS webpage](#) to consult the list of projects funded previously.

## 1. Background

The European Defence Fund (EDF) fosters the competitiveness, efficiency and innovation capacity of the European defence technological and industrial base (EDTIB).



It contributes to the EU strategic autonomy and its freedom of action, by supporting collaborative actions and cross-border cooperation between legal entities throughout the Union, in particular SMEs and mid-caps, as well as by strengthening and improving the agility of both defence supply and value chains, widening cross-border cooperation between legal entities and fostering the better exploitation of the industrial potential of innovation, research and technological development, at each stage of the industrial lifecycle of defence products and technologies.

The EDF funds projects which are consistent with the defence capability priorities commonly agreed by EU Member States within the framework of the Common Foreign and Security Policy (CFSP), through:

- collaborative research that could significantly boost the performance of future capabilities, aiming to maximise innovation and introduce new defence products and technologies, including disruptive technologies for defence, and aiming to make the most efficient use of defence research spending in the EU

or

- collaborative development of defence products and technologies, thus contributing to the greater efficiency of defence spending in the EU, achieving greater economies of scale, reducing the risk of unnecessary duplication and thereby fostering the market uptake of European defence products and technologies and reducing the fragmentation of defence products and technologies, ultimately leading to an increase in the standardisation of defence systems and a greater interoperability between Member States' capabilities.

In line with the Work Programmes 2023 part II and 2024 part I, this call covers thematic topics addressing development actions (including one action with financial support to third parties), which will be implemented through actual cost grants.

Subject to successful conclusion of the evaluation of the proposals and the contribution agreements with the entrusted entities concerned:

- the action(s) related to the topic EDF-2023-DA-MATCOMP-MJR-CBDIN will be implemented in indirect management by the European Defence Agency (EDA)
- the action(s) related to the topic EDF-2023-DA-NAVAL-MMPC will be implemented in indirect management by the Organisation Conjointe de Coopération en Matière d'Armement / Organisation for Joint Armament Co-operation (OCCAR).

## **2. Type of action and funding rate — Objectives — Scope and types of activities — Functional requirements — Expected impact — Specific topic conditions**

### Type of action and funding rate

The topics under this call for proposals concern EDF Development Actions (DA).

For Development Actions, the IT system (*e.g. budget table in the Submission System, payment calculator in the Grant Management System*) will for technical reasons display a general funding rate of 100% for all automated calculations.

In order to calculate the rates that are due under the EDF Regulation, you will have to calculate the individual funding rates for your project (via the Detailed budget table available in the Submission System, *see section 5*).

These rates will be based on the:

- baseline funding rates (per type of activity)
- and
- bonuses (per type of activity and depending on type of participants, if any).

Types of activities (art 10(3) EDF Regulation)		Baseline funding rate	PESCO bonus	SME bonus		Mid-cap bonus	Maximum funding rate with bonuses
				non- cross- border	cross border		
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	Cannot be funded	Cannot be funded	Cannot be funded	Cannot be funded	Cannot be funded	Cannot be funded
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	65%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 100%
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	90%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 100%
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	65%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 100%
(e)	<b>System prototyping<sup>4</sup></b> of a defence product, tangible or intangible component or technology	20%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 55%
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	45%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 80%
(g)	<b>Qualification<sup>5</sup></b> of a defence product, tangible or intangible component or technology	70%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 80%

<sup>4</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>5</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

Types of activities (art 10(3) EDF Regulation)		Baseline funding rate	PESCO bonus	SME bonus		Mid-cap bonus	Maximum funding rate with bonuses
				non- cross- border	cross border		
(h)	<b>Certification</b> <sup>6</sup> of a defence product, tangible or intangible component or technology	70%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 80%
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	65%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 100%

In order to obtain the bonuses, the applicants must fulfil the following conditions:

Type of bonus	Condition	Bonus (additional number of percentage points to the baseline funding rate)
<b>PESCO bonus</b>	Project developed in the context of a project of the permanent structured cooperation (PESCO) <sup>7</sup>	+ 10%
<b>SME<sup>8</sup> bonus (non-cross border)</b>	Proportion of eligible costs allocated to SMEs (beneficiaries, affiliated entities and subcontractors involved in the action; not associated partners)  ≥ 10% (for the activity concerned)	+ % of the proportion of eligible costs allocated to non-cross-border SMEs <sup>9</sup> (up to maximum 5%)
<b>SME bonus (cross-border)</b>		+ twice the % of the proportion of eligible costs allocated to cross-border SMEs <sup>10</sup>
<b>Mid-cap bonus</b>	Proportion of eligible costs allocated to mid-caps <sup>11</sup> (beneficiaries, affiliated entities and subcontractors involved in the action; not associated partners)  ≥ 15% (for the activity concerned)	+ 10%

<sup>6</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.


<sup>7</sup> See Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States (OJ L 331, 14.12.2017, p. 57).


<sup>8</sup> 'SMEs' means small and medium-sized enterprises as defined in the Annex to EU Recommendation [2003/361/EC](#).

<sup>9</sup> 'Non-cross-border SMEs' are SMEs established in the Member States or EDF associated countries in which the beneficiaries that are not SMEs are established.

<sup>10</sup> 'Cross-border SMEs' are SMEs established in Member States or EDF associated countries other than those in which the beneficiaries that are not SMEs are established.

<sup>11</sup> 'Middle-capitalisation company (mid-cap)' means an enterprise that is not an SME and that has up to 3 000 employees, where the staff headcount is calculated in accordance with Articles 3 to 6 of the Annex to EU Recommendation [2003/361/EC](#).

 Please note that only entities which are registered in the Participant Portal (i.e. have a PIC) and which have a positive SME/Mid-cap self-assessment result (for the current and 2 previous years) can be counted for the SME/Mid-cap bonuses. Please make sure that all your project participants fulfil these requirements ([Funding & Tenders Portal account](#) > My Organisations > Actions > Modify Organisation > SME tab > Start SME self-assessment (> Mid-cap self-declaration)); for more information, see [IT How To](#)).

 Please also note that for WP 1 — Project management and coordination, you must always use the funding rate for the type of activity (c) Studies.

The funding rates that will cap the maximum amounts that may be requested for each applicant and reporting period will then be fixed in Annex 2e of the Grant Agreement.

### Specific topic conditions

For all topics under this call:

- multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (*see section 6*)
- the following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment (*see section 10*)

For the topic EDF-2023-DA-MATCOMP-MJR-CBDIN, financial support to third parties is allowed, but only within the set threshold (*see section 10*)

## **EDF-2023-DA-MCBRN-FCS: Federating CBRN systems**

### Objectives

#### **General objective**

Recent CBRN<sup>12</sup> events necessitate an increased and comprehensive CBRN-defence effort. The CBRN threat is also continuously evolving and imposes adaptation of existing technologies and development of new solutions in order to improve the armed forces' CBRN defence capabilities.

The general objective of this topic is to create an overarching information system that enables interoperability between the different existing national CBRN defence information management systems, or subsystems, with the aim to improve and to better use and coordinate available CBRN defence resources within the EU Member States and EDF associated countries (Norway) to obtain greater endurance for their armed forces.

#### **Specific objective**

Member States and EDF associated countries (Norway) armed forces need to act in a combined and joint environment and maintain the operational capabilities under CBRN conditions.

However, European CBRN capabilities are currently mainly based on widely different equipment and systems, hence making it challenging to obtain a coherent and efficient EU and EDF associated countries (Norway) CBRN defence. Therefore, this topic aims to create a comprehensive software system that enables interoperability between the Member States and EDF associated countries (Norway) through a

---

<sup>12</sup> Chemical Biological Radiological Nuclear.

system-of-systems approach including modular equipment.

### Scope and types of activities

#### **Scope**

The proposals must address the design and the prototyping of a European CBRN system of systems cross-border solution.

The proposals should focus on integration of CBRN defence technologies into a comprehensive software system. However, the proposals may also provide analysis of the relevance and feasibility of novel CBRN technologies, mapping of CBRN defence capacities across the EU and EDF associated countries, as well as options for ensuring access and availability of CBRN technologies.

The proposals may also consider others aspects such as education, training and logistics and may specify a solution that can task and manage CBRN operations both in the military and civilian realm.

#### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (see *Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>13</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (optional)

<sup>13</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

Types of activities (art 10(3) EDF Regulation)		Eligible?
(g)	<b>Qualification<sup>14</sup></b> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification<sup>15</sup></b> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - provide an inventory of the systems available (or in development) in the Member States and EDF associated countries (Norway) armed forces;
  - provide a comprehensive approach analysis with solutions and functionalities that covers Detection, Identification and Monitoring (DIM), CBRN Knowledge Management (KM), Physical Protection (PP), and Hazard Management (HM) for all addressed CBRN-threats;
  - provide a proof of concept based on one, several or all of these functions (DIM, KM, PP, HM);
  - address the requirements for a standardised IoT<sup>16</sup> framework, enabling more equipment integration. The proposed framework should be presented and described in OV-1 format<sup>17</sup>.
- Design:
  - identify an overall architecture, based on open, publicly available and international standards widely used, such as ISO 10303<sup>18</sup> and related specifications from ISO TC 184/SC 4<sup>19</sup>;
  - provide for a modular approach that facilitates the possible subsequent evolutions of the different systems composing the CBRN defence.
- System prototyping:
  - the prototype must be validated through a technical demonstration on at least TRL 6<sup>20</sup>.

<sup>14</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>15</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

<sup>16</sup> Internet of things.

<sup>17</sup> High Level Operational Concept Graphic.

<sup>18</sup> ISO standard for the computer-interpretable representation and exchange of product manufacturing information.

<sup>19</sup> International standards organisation responsible for industrial data. ISO/TC 184/SC 4 develops and maintains ISO standards that describe and manage industrial product data throughout the life of the product.

In addition, the proposals must substantiate<sup>21</sup> coherence and interoperability with existing CBRN-related initiatives (such as, but not limited to, PESCO CBRN-SaaS, EDA CatB CBRN-SaaS, Horizon Europe framework programme, NATO initiatives) regarding sensor networking, data exchange and data fusion, as well as substantiate synergies and complementarity with the activities described in the call topics EDIDP-CBRN-DEWS-2020 on *capabilities for CBRN risk assessment, detection, early warning and surveillance* and EDF-2021-MCBRN-R-CBRNDIM on *Detection, identification and monitoring (DIM) of CBRN threats*.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement
 and
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The demonstrated federated CBRN system of systems should meet the following functional requirements:

- General:
  - include functional chains from detection, identification and monitoring (DIM), data communication and management, including sensing data, hazard prediction, decision support, visualisation and other CBRN functions;
  - federate multiple actors and systems and exploit legacy capabilities;
  - include modular kits that are easy to deploy in different operational situations, strategic, operational and tactical levels, in and out the territory of the Member States and EDF associated countries (Norway) in a multi-domain environment;
  - able to integrate innovative technologies such as new sensors, robotics, AI<sup>22</sup>, virtual reality;

---

<sup>20</sup> Technology Readiness Level 6 (System/subsystem model or prototype demonstration in a relevant environment.

<sup>21</sup> To the extent of information available on open sources.

<sup>22</sup> Artificial Intelligence.

- able to fuse all generated data into an intuitive common operational picture and present it in a single front end;
- able to ensure overall data exchange in situations with constrained communications.
- be built upon existing harmonised civilian and military standards widely used in this domain (e.g. NATO ATP-45/AEP-45<sup>23</sup>, JC3IEDM<sup>24</sup>) where applicable;
- be modular and scalable in order to be able to integrate future solutions.
- Usability:
  - ensure exchange of data and information between CBRN information systems, covering joint military branches, multi-domain (Land, Air, Sea) and civil-military cooperation (CIMIC) to support collaboration and cooperation between Member States and EDF associated countries (Norway). In addition, possible solutions for data exchange regarding classified and protected data may be included;
  - ensure fusion of all available data and information sources to achieve an easy-to-understand common operational picture that enables deliberate and ad-hoc decision making, and should be connectable to existing crisis management software applications;
  - include the availability of sensor data, as well as the complete configuration management aspects and logistics status including maintenance status of these systems;
  - include solutions to predict and simulate hazard development in time and space in case of a CBRN defence event, and that should be applicable also in urban and indoors settings. The simulation solutions should be applicable for planning-, exercise- and real instances;
  - implement mathematical modelling methods like reverse dispersion modelling to enable localisation of CBRN-sources;
  - allow communication between the different constituent parts, including a common standardised API for application integrations.
- Interoperability/Data sources:
  - include integration of weather data (live and forecast);
  - include interface and data transfer solutions to integrate information from civilian data sources (e.g. radiation early warning sensor networks);
  - include alternative data sources (e.g. social media reports of smell/symptoms, uncommon symptom results from hospitals, emergency call centre reports, etc.) also using novel approaches (e.g. AI) for data analysis and evaluation.

---

<sup>23</sup> NATO ATP- AEP-45 Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents (reference manual).

<sup>24</sup> Joint Consultation, Command and Control Information Exchange Data Model.



### Expected impact

The outcome should contribute to:

- improved CBRN defence capabilities of Member States and EDF associated countries (Norway) armed forces, with an enhanced level of situational awareness, as well as a reduced risk of false alarms and misinterpretation in order to enable a quicker and more efficient response;
- a standardisation of CBRN defence systems information and data exchange at European level;
- the integration of contemporary and emerging CBRN defence technologies;
- an enhanced operational readiness and effectiveness..

### **EDF-2023-DA-C4ISR-LCOM: Laser communications**

#### Objectives

##### **General objective**

Information superiority is a critical capability to be developed and improved with the aim to address future challenges to be faced by European defence forces, and more specifically to support reactive and efficient decision-making processes. To this purpose, an effective and robust EU military Intelligence, Surveillance, Target, Acquisition and Reconnaissance (ISTAR) capability for missions and operations is an essential element of the overall EU effort to facilitate international conflict prevention and crisis management. Moreover, an ISTAR capability could support border and maritime surveillance tasks as well. Acquiring this capability necessitates the drastic improvement of Intelligence, surveillance, and reconnaissance (ISR) and CIS<sup>25</sup> operational capabilities, notably with regard to persistence, acquisition of high-quality and high volume of data, automatic airborne processing and dissemination of information to relevant stakeholders.

Against this background, the unmanned aerial systems (UAS), and in particular the Medium Altitude Long Endurance Remotely Piloted Aircraft System (MALE RPAS), are key for ISTAR missions. An unmanned platform is also able to establish a central/relay node, collecting tactical communications of friend forces in the nearby and relaying to C5ISR<sup>26</sup> centre.

The ISTAR mission of the UAS include EO<sup>27</sup>/IR<sup>28</sup>, radar and signal intelligence sensors, as well as generation of geo-intelligence data. To accomplish these tasks, one of the most critical elements of the UAS aircraft architectural configuration lays in its telecommunications subsystem. In addition, communications play a more important role in the operation of unmanned aircraft than they do in manned ones, since all the decision-making occurs on the ground. The subsystem functionalities must thus provide both command and control instructions (C2 datalink) and relay collected ISR data (ISR data link) by the use of Radio line-of-sight (RLOS) and /or beyond radio line-of-sight (BRLOS).

However, all communications with the ground control station are usually performed via satellite links, which have bandwidth limitations. Therefore, enhanced

---

<sup>25</sup> Communications and information system.

<sup>26</sup> Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance.

<sup>27</sup> Electro-optical.

<sup>28</sup> Infrared.

telecommunication links are required, providing higher wideband characteristics, as well as efficient means of electronic and cyber defence properties against detection, acquisition, jamming and cyber-attacks. Otherwise, loss of the aircraft own control, compromise of the information collected and in the worst-case total control of the aircraft by the adversary may occur. Moreover, the overwhelming demand for data communications with ever increasing data rate, has drastically reduced the availability of RF<sup>29</sup> transmission bandwidth, converting it to a valuable resource. Although hundreds of deployed satellites practically provide global Ku band coverage, the overall congestion of the Ku band causes problems in particular with regard to unmanned aircraft operations. In parallel, timely transmission of voluminous ISR sensor data is often not possible within the available RF channels capacity limitations.

Optical links have already proven their suitability for satellite to mobile platforms applications, by providing orders of magnitude faster transmission, while using much less power than traditional RF links to aircrafts, ships, and even other satellites. The future utilisation of optical data links for Beyond Line of Sight (BLOS) operations of UAS can simultaneously combine all capabilities of high data rate, unlimited bandwidth, low probability of detection (LPD) and low probability of intercept (LPI) communications and integration to network centric architectures. For high bandwidth transmission and to gain an additional communication link, a laser communication between UAS and satellite terminals could be installed. This idea of airborne optical wideband communication via satellite, immune to eavesdropping and jamming, constitutes the general objective of this topic.

### ***Specific objective***

The specific objective of this topic is the development of an Airborne Laser Communication System (ALCoS), able to establish a very high data rate bi-directional communication link to satellite, providing BLOS communication capability with LPD and LPI characteristics.

### ***Scope and types of activities***

#### ***Scope***

The proposals must address activities to design a prototype for airborne laser communication system (ALCoS) to be used on various types of aircraft, manned or unmanned (e.g. envisioned European MALE RPAS).

In detail, the proposals must address:

- an overview about a suitable configuration for airborne laser communication including all parts of the communication chain (RPAS terminal, satellite terminal, satellite orbit position, inter-satellite communication, downlink);
- identification, analysis and mitigation of critical technical risks especially those relating to integration and certification;
- definition of a set of requirements, considering the whole product cycle;
- life cycle cost analysis and management;
- developing of a prototype to demonstrate the possible airborne integration.

#### ***Types of activities***

The following table lists the types of activities which are eligible for this topic, and

---

<sup>29</sup> Radiofrequency.

whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>30</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>31</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>32</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - identify which configurations to be used in the design. As outcome, a set of requirements must be assessed and jointly agreed by supporting Member States and EDF associated countries (Norway);
  - provide influences and limitation of weather and atmospheric conditions on laser communications and possible countermeasures;

<sup>30</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>31</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>32</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- execute risk management for the development of airborne laser communications, including all parts of the communication line, especially for integration, certification and qualification issues;
- provide drawings, reports, analyses, certification plan and data in view of the future certification of the system by the authorities concerned.
- Design:
  - provide a set of requirements, to be assessed and jointly agreed by the supporting Member States and EDF associated countries (Norway);
  - design a flight test campaign to ensure airspace integration and the future certification;
  - design a system prototype in view of a serial system complying with the qualification standards usually applied in this domain (e.g. RTCA/EUROCAE<sup>33</sup> DO-254<sup>34</sup>, DO-178<sup>35</sup> and DO-160<sup>36</sup>)
- System prototyping:
  - a system prototype must be produced to enable concrete testing in live environment.
- Testing:
  - the performances of the system prototype according to the functional requirements, as well as certification and qualification potential issues as identified in the certification plan, must be evaluated through a consistent test campaign, including through a flight test campaign if possible.

In addition, the proposals must substantiate synergies and complementarity with ongoing multilateral European programmes and activities in the field of laser communications (e.g. EDRS<sup>37</sup>).

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the

---

<sup>33</sup> Radio Technical Commission for Aeronautics/European Organisation for Civil Aviation Equipment.

<sup>34</sup> RTCA/EUROCAE DO-254 ED-80 Design Assurance Guidance for Airborne Electronic Hardware.

<sup>35</sup> RTCA/EUROCAE DO-178C Software Considerations in Airborne Systems and Equipment Certification.

<sup>36</sup> RTCA/EUROCAE DO-160 Environmental Conditions and Test Procedures for Airborne Equipment.

<sup>37</sup> European Data Relay System (European Space Agency project).

technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed product and technologies should meet the following functional requirements:

- obtain higher reception power and signal-to-noise ratio at the receiver side, as compared to RF, enabling faster bi-directional communications with lower bit-error-rates and high data rate in the order of Gbps;
- achieve reliable airborne laser telecommunications within 2 seconds for establishing the link with the satellite;
- use same interfaces as for RF communications;
- include beam-steering for precision pointing and tracking of the satellite (LEO<sup>38</sup>, MEO<sup>39</sup> and GEO<sup>40</sup>), compensate vibrations or resist to vibrations;
- provide power consumption and heat dissipation that can be supported by the aircraft;
- perform signal transmission which does not risk inflicting any danger, while being resistant to blinding and dazzling;
- establish a laser communication link under influence of challenging atmospheric (e.g. magnetic anomalies) and light weather conditions (e.g. partly cloudy conditions);
- be designed to be integrated into various aircraft (e.g. fixed-wing medium/high-altitude unmanned aerial vehicles, fixed-wing governmental multi-role aircraft), with enhanced SWaP-C<sup>41</sup>.

### Expected impact

The outcome is expected to contribute to:

- the enhancement of information superiority during EU missions and operations;
- the effectiveness and unity of command during ISTAR operations;
- the enhancement of the EU freedom of action in the field of ISTAR, but also joint electronic warfare, hence reinforcing the strategic autonomy of the EU;
- the increase of survivability of UAS, notably MALE RPAS, due to the drastic increase of the aircraft C2 link immunity;
- the acquisition of an increased innovative potential for the European defence industry in the technological field of airborne laser communications.

---

<sup>38</sup> Low Earth Orbit.

<sup>39</sup> Medium-Earth Orbit.

<sup>40</sup> Geostationary Orbit.

<sup>41</sup> Size, Weight, Power and Cost.

**EDF-2023-DA-C4ISR-TRPAS: Tactical RPAS**Objectives**General objective**

Due to rapidly and continuously evolving geopolitical conditions, EU Member States and EDF associated countries (Norway) are facing the challenge to carry out operational tasks and military missions, including with relation to Common Security and Defence Policy (CSDP). This requires a credible tactical picture built in an efficient and timely manner, hence contributing to situational awareness, while helping to manage the battlefield and the forces engaged. For that purpose, a set of Information, Surveillance and Reconnaissance (ISR) capabilities, notably including tactical Unmanned Aircraft Systems (UAS), is necessary.

As highlighted in commonly agreed capability development priorities, there is a permanent need to detect, identify and track ships, aircraft, vehicles, personnel and other equipment through a continuous air-space wide area, using interoperable unmanned surveillance systems. Such systems should operate with guaranteed data integrity in all weather conditions and all types of environment, including in contested and denied environments. To support this need, tactical remote piloted aircraft systems (T-RPAS) equipped with modern sensors for ISR missions can provide reliable, cost-effective, easily deployable and recoverable means for the effective collection and timely delivery of information for the production of intelligence, situational awareness and decision-making.

**Specific objective**

The specific objective of this topic is to develop a multi-purpose/multi-role T-RPAS, for the potential use by units of mainly up to divisional size. It will collect tactical level intelligence (real-time target cinematics, terrain, enemy location and movements) with high-performance multi-sensor equipment, through ISR (ground, maritime and air) and targeting missions, in addition to other related tasks (target acquisition, identification, tracking).

T-RPAS pose the problem of operational versatility. Indeed, fitting these platforms with best-in-class performance characteristics could lead to an increase in size and weight, with the risk of losing their tactical specificity. Therefore, the new generation of T-RPAS should meet the need for an efficient payload while being equipped with low SWaP (Size, Weight and Power) vehicle management systems. The aircraft should also have increased endurance and range, in order to maximise its operational availability in a given Area of Interest (AoI).

Most of EU Member States and EDF associated countries (Norway) need to grant a Type Certificate to their RPAS through their military aviation or civil airworthiness authority. Up to now, most systems have been certified according to in-house rules elaborated from existing standards and specificities related to RPAS. Consequently, one challenge is to unify the approach of the supporting Member States and EDF associated countries (Norway) for T-RPAS certification by applying standards widely used in this domain (e.g. NATO STANAG<sup>42</sup> 4671<sup>43</sup>) as well as processes for fixed-wings RPAS of more than 150kg. In that respect, compliance with such standards, also applicable to T-RPAS already under development, must be carefully taken into account from the early design of the proposed new capabilities.

---

<sup>42</sup> North Atlantic Treaty Organisation STANdardization Agreement.

<sup>43</sup> NATO STANAG 4671 Ed.3 Unmanned aircraft systems airworthiness requirements (USAR) - AEP-4671 Edition B.

The proposals should target at least TRL<sup>44</sup> 8 (actual system completed and "flight qualified" through test and demonstration) to be validated through extensive flight testing and verification of the level of compliance with applicable airworthiness requirements.

### Scope and types of activities

#### **Scope**

The proposals must address:

- airworthiness type certification and relevant supporting actions for certifying T-RPAS under development that can carry, release and control small Unmanned Aircraft (UA) and/or weapons;
- development of technology blocks to improve the T-RPAS capabilities, notably a vehicle management system (VMS) and parts of mission management system (MMS), allowing T-RPAS effective operations, including in GNSS<sup>45</sup> denied or contested environments, mission autonomy, and weapons engagement.

The unmanned nature of RPAS impacts the VMS and MMS architectures, the level of mission autonomy, as well as the envisioned weapons engagement capability, and requires demonstration and certification of a quantified level of safety, redundancy and accuracy, in line with the functional requirements.

The proposals must substantiate synergies and complementarity with activities described in the call topic EDIDP-ISR-TRPAS-2019 targeting the *development of a low-observable tactical RPAS with the capability to provide near real time information and with modern self-protection*.

#### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)

<sup>44</sup> Technology Readiness Level.

<sup>45</sup> Global Navigation Satellite System.

Types of activities (art 10(3) EDF Regulation)		Eligible?
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>46</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>47</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	<b>Certification</b> <sup>48</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

Each capability of the T-RPAS should be tested and demonstrated separately.

A flight demonstration is required for the weapon release/engagement capability. The effort should focus on safety with respect to applicable standards in military aviation combined with RPAS specificities. This work will be followed closely by the supporting Member States and EDF associated countries (Norway) military airworthiness authorities in order to define a common weapon integration preliminary standard for T-RPAS.

Supporting Member States and EDF associated countries (Norway) military airworthiness authorities will closely follow airworthiness type certification and relevant supporting actions of T-RPAS under development that can carry, release and control small UA and/or weapons.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement

<sup>46</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>47</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>48</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.



and

- based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed product and technologies should meet the following functional requirements:

- 1) The system to develop should possess the following main top-level capabilities:
  - technologies and standards that allow an open architecture, autonomy, modularity, and interoperability according to standards widely used in such fields (e.g. NATO STANAG 4586<sup>49</sup>);
  - re-configurable sensor payloads flexibly selectable according to the mission;
  - operation in contested and denied airspace environment;
  - short take-off and landing (STOL)<sup>50</sup> capabilities<sup>51</sup>;
  - long-range, robust, covert and ad-hoc radio communication systems;
  - near real-time data processing for target detection, recognition, classification, identification and tracking;
  - support of collaborative ISR missions while minimising operator workload;
  - cyber-secure and versatile ground station supporting multiple user profiles;
  - incorporated sensor suite able to detect and localise enemy threats;
  - execution of tactical air reconnaissance missions, which obtain combat information about enemy and population activities and resources through sensing payloads;
  - execution of surveillance missions, which focus on systematic observation of airspace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, imagery or other means to collect information;
  - equipment with low SWaP (Size, Weight and Power) vehicle management systems;
  - release of small UA or weapons<sup>52</sup>, with the capability to control them through the available communication links and the ability to hand over control of small UA to other parties;
  - supporting training and exercises for pilots and payload operators, using an

<sup>49</sup> NATO STANAG 4586 Ed.4 standard interfaces of UA control system (UCS) for NATO UA interoperability - AEP-84 Edition A.

<sup>50</sup> Ability of the aircraft to clear a 50-foot (15-metre) obstacle within a distance of 1500 feet (450 metres) when taking-off or landing.

<sup>76</sup> Proposals may also consider vertical take-off and landing (VTOL).

<sup>52</sup> In line with the weapon integration preliminary standard for T-RPAS to be addressed within the current call for proposals.

embedded simulation system within the Ground Control Station (GCS).

2) Several key aspects of the functions and/or equipment to be installed on T-RPAS should be addressed, notably:

- versatility: functions/equipment/architectures to be implemented on several T-RPAS;
- compliance with standards widely used in this domain, such as NATO STANAG 4586 and NATO STANAG 4671. A European Military Advisory Circular (AC) should be proposed to provide details for acceptable means on showing compliance of a UA VMS to applicable standards and references (e.g. STANAG 4671 / USAR.U1330 (Flight control performance), taking also into account RTCA<sup>53</sup>/EUROCAE<sup>54</sup> DO-178C<sup>55</sup> and DO-254<sup>56</sup>, as well as SAE<sup>57</sup> ARP94910<sup>58</sup>);
- special conditions covering aspects beyond the applicable standards (e.g. STANAG 4671), as well as the relevant Acceptable Means of Compliance (AMCs), which are expected to be related to small UAs or weapons delivery from the T-RPAS;
- interoperability in terms of ISR product exchange in near real-time;
- cost effectiveness.

3) In particular, the VMS should:

- be capable to effectively manage a T-RPAS in GNSS denied or contested environment;
- enable hand over of control to other remote operators, or other manned assets;
- provide systems and functions that are used to sense and effectively derive vehicle position, airspeed, wind frame angles, inertial velocity, attitudes, rates, and accelerations, heading and altitude;
- provide guidance, navigation and control systems and functions that generate flight path commands and follow these commands by controlling aircraft force and moment producers. The flight path commands should be derived using various sources i.e. way points, curve paths, 4D trajectories or time coordinated paths with other UAS;
- provide control functions for altitude, airspeed, heading, attitude, body and stability axis angular rates, lateral, normal and longitudinal accelerations, aerodynamic or geometric configuration and structural modes, and follow the commands transmitted by a remote operator;
- include flexible data communication interfacing properties.

In any case, the prototyped VMS must be installed and tested in at least one RPAS satisfying relevant standards, such as STANAG 4671.

---

<sup>53</sup> Radio Technical Commission for Aeronautics, United States non-profit organisation.

<sup>54</sup> European Organisation for Civil Aviation Equipment.

<sup>55</sup> RTCA/EUROCAE DO-178C Software Considerations in Airborne Systems and Equipment Certification.

<sup>56</sup> RTCA/EUROCAE DO-254 Design Assurance Guidance for Airborne Electronic Hardware.

<sup>57</sup> SAE International, previously Society of Automotive Engineers.

<sup>58</sup> SAE ARP94910 Aerospace - Vehicle Management Systems - Flight Control Design, Installation and Test of, Military Unmanned Aircraft, Specification Guide For ARP94910.

4) The mission autonomy and safety technology blocks contributing to the MMS, should:

- provide solutions for optimum 2D or 3D almost real-time flight path generation considering a combination of constraints such as:
  - threat avoidance and survival of T-RPAS;
  - specific information collection, i.e. electronic or signal intelligence;
  - EO<sup>59</sup>/IR<sup>60</sup> sensors capabilities;
  - emergency landing;
  - remote operator defined:
    - area coverage for ISR within specific time boundaries;
    - spots of high interest;
    - avoidance areas, i.e. crowded areas or hot zones;
    - landing areas in case of power loss;
- enable remote operators, in their workspace, to define the combination of constraints and to intervene at any time through automatic mode by altering those constraints or switching to manual or semi-automatic mode<sup>61</sup>;
- be capable to engage weapons with specific safety chain and relevant functionalities of the Ground Control Station;
- include scalable level of autonomy to alleviate the workload of the operators and allow more automatic and high-level control of the T-RPAS while preserving safety (i.e. loss of control) and minimising certification needs;
- allow for multiple and reconfigurable sensing payloads depending on the missions, such as airborne Synthetic Aperture Radar (SAR), maritime surveillance radar, EO/IR imaging sensors, COMINT<sup>62</sup> / ELINT<sup>63</sup> equipment;
- provide on-board processing, to improve mission efficiency and target correlation, avoiding significant loss of information due to datalinks limitations. Data considered could be EO and IR full definition motion video, radar, COMINT, ELINT, etc.;
- provide automatic orientation of the different payloads based on on-board information fusion (e.g. based on available information fusion, the EO/IR payload automatically takes pictures and even identifies targets);
- allow for automatic path alteration for the accomplishment of a high value task, i.e. target identification within a window of opportunity, threat avoidance or emergency landing.

5) The T-RPAS under development and those T-RPAS used for testing and

---

<sup>59</sup> Electro-optical.

<sup>60</sup> Infrared.

<sup>61</sup> Semi-automatic modes are manual modes augmented partially by automatic means that minimise the remote operator's workload in lateral or longitudinal guidance.

<sup>62</sup> Communication intelligence.

<sup>63</sup> Electronic intelligence.

demonstrating the technology blocks must:

- have a maximum take-off weight between 450 and 1250kg;
- have a minimum endurance of 8 hours;
- be able to release at least four small UA with Maximum Take-Off Weight (MTOW) between 10 and 50kg, or weapons. The weapons and the releasable UA must be certified for safe separation and engagement. The releasable UA must also be qualified for safe teaming with the mothership tactical RPAS (including datalinks, latency for critical aspects, C2<sup>64</sup>, guidance and position in GNSS-denied or contested environment, etc.);
- be certified in accordance with applicable requirements and AMCs as per applicable standards, such as NATO STANAG 4671 taking also into account RTCA/EUROCAE DO-178C and DO-254, as well as SAE ARP94910, with additional special conditions related to releasable UA or weapons engagement and delivery from the T-RPAS.

In case the T-RPAS uses a not yet certified engine, certification actions must be proposed accordingly.

Where relevant, type certificate or equivalent from EASA<sup>65</sup> should be considered in order to cover the envisioned non-military functions and systems of the T-RPAS.

A Military Type Certificate must be issued by a competent European Military Airworthiness Authority containing at least: (a) System Identification, (b) System configuration details, (c) Requested operating frequencies, (d) Statement of compliance with applicable standards, such as STANAG 4671 (including if applicable additional conditions, exemptions, and deviations), (e) List of approved publications – Operating and maintenance, (f) Issuing Agency, (g) Date of Issue.

### Expected impact

The outcome is expected to contribute to:

- improving the usage of the civilian airspace for a European tactical RPAS without compromising flight safety;
- decreasing the risk of unmanned ISR missions through the drastic increase of the T-RPAS survivability thanks to the adoption of self-protection measures regarding robustness to GNSS jamming and datalinks contests at the borders of Europe;
- raising a unified airworthiness certification methodology and baseline for Tactical RPAS by all supporting Member States and EDF associated countries (Norway), based on applicable standards, such as NATO STANAG 4671. This will ease the mutual acceptance of Type Certificates for T-RPAS delivered by the supporting Member States and EDF associated countries (Norway);
- opening the way for certification according to applicable standards such as STANAG 4671 by EU Member States and EDF associated countries (Norway) Military Airworthiness Authorities for tactical RPASs with small releasable drones or weapon engagement capability;
- maximising the capability of the tactical RPAS system to operate efficiently in

---

<sup>64</sup> Command and Control

<sup>65</sup> European Union Aviation Safety Agency

wider operational domains by developing a state-of-the-art Vehicle Management System;

- strengthening the European RPAS industrial base at the front edge of the international RPAS competition, enabling a real EU strategic autonomy in this domain, especially on critical functions.

## **EDF-2023-DA-C4ISR-DAA: Detect and avoid**

### Objectives

#### **General objective**

Nowadays, unmanned aerial systems (UAS) (or remotely piloted aerial systems - RPAS) are used to support an extended spectrum of military missions. Their involvement in the future, notably with the next generation air combat systems, is expected to increase. However, these UAS may be limited to operate in segregated airspace or within visual line of sight, especially when the need arises for their safe simultaneous operation together with other manned and/or unmanned assets.

To overcome these limitations, all manned and unmanned air assets need to be integrated safely and effectively in non-segregated airspace, notably in the context of the Single European Sky.

Detect and Avoid (DAA) systems are technologies that allow UAS to integrate safely into airspace including civil airspace, avoiding collisions with other aircraft. These systems observe the environment surrounding the UAS, detect traffic, informs the pilot, assess risk of collision and when appropriate generate a new flight path to avoid collision.

As a key enabler for air traffic integration (ATI) of UAS, DAA effectively provides the remote pilot with the ability to perform the required duties regarding safety hazard of conflicting airborne aircraft. Through collection and fusion of sensor data, the remote pilot obtains awareness of traffic, while assisted by collision avoidance (CA) and remain well clear (RWC) functions, preventing the unmanned aircraft to be involved in a collision hazard or, if so, allowing manoeuvre to avoid a collision even in case of lost pilot action.

Therefore, the general objective of this topic consists in reaching a consistent level of maturity allowing to integrate the envisioned European DAA capabilities into the maximum possible UAS within the various Member States and EDF associated countries (Norway) fleet in order to allow for UAS operation in the airspace anywhere and at any time.

#### **Specific objective**

The specific objective of this topic is to take the necessary steps towards a standardised, qualified and certified DAA solution to be integrated in many different UAS, hence allowing a full integration for civil and military airspace and U-space<sup>66</sup> services where applicable, and operational use of current and near-term platforms to be used, such as MALE RPAS.

---

<sup>66</sup> Set of services and procedures to support safe, efficient and secure access to airspace for Unmanned Aircraft Systems (UAS).

Scope and types of activities**Scope**

The scope of the topic is to provide a fully standardised, qualified and certifiable DAA solution for UAS. The DAA solution should aim at fully integrating RPAS in the general airspace (A-G classes) without any limitations regarding operation in the airspace including in TMA<sup>67</sup>. This is to be achieved by involving all the relevant key-stakeholders regarding airspace integration in Europe (i.e., EUROCAE<sup>68</sup>, EASA<sup>69</sup>, EUROCONTROL<sup>70</sup>, SESAR<sup>71</sup>, ANSPs<sup>72</sup>, pilot organisations and ICAO<sup>73</sup>).

The outcome should be a standard for DAA systems emanating from a fully developed DAA solution. This solution must be validated by simulation and under real flying conditions, allowing integration in various UAS, including MALE RPAS and tactical RPAS.

The overarching scope of this topic will be to push the DAA solution (conflicting airborne traffic) for UAS into designs for full operational capability without any UAS specific restrictions in European airspace including in TMA. The designs must be European standardised and recognised in Europe by relevant authorities and stakeholders. The DAA solution must be designed to be integrable for both MALE and tactical RPAS classes. The DAA solution design must be made for aeronautical use on aircraft and as such be subject to qualification and certification.

**Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)

<sup>67</sup> Traffic Monitoring and Analysis.

<sup>68</sup> European Organisation for Civil Aviation Equipment.

<sup>69</sup> European Union Aviation Safety Agency.

<sup>70</sup> European Organisation for the Safety of Air Navigation.

<sup>71</sup> Single European Sky ATM (air traffic management) Research.

<sup>72</sup> Air Navigation Service Provider.

<sup>73</sup> International Civil Aviation Organisation.

Types of activities (art 10(3) EDF Regulation)		Eligible?
(e)	<b>System prototyping</b> <sup>74</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>75</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	<b>Certification</b> <sup>76</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - establish an inventory of past and existing projects and solutions worldwide for the DAA function, analyse their strengths and weaknesses in order to make sure DAA will come to state-of-the-art solutions;
  - specification of facilities, test conditions, measurements, instrumentation, analysis of ongoing and future regulation requirements, data analytic capabilities, environment, engineering development sites and analysis processes, which better serve the testing, prototyping, qualifying and certifying procedures to follow;
  - specification of the system integration procedures which facilitate the accommodation of system updates and the integration of new innovative functional capabilities;
  - assessment of the possibility to define a common site for demonstration, testing, analysing and training purposes, using the same or interoperable facilities;
  - study collision avoidance manoeuvre dedicated to low-speed performance RPAS;
  - provision of drawings, reports, analyses, certification plan and data in view of future approval and certification of the system by supporting Member States and EDF associated countries (Norway) authorities.

<sup>74</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>75</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>76</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Design:
  - preparation of a detailed test and evaluation master plan;
  - elimination of deficiencies identified and incorporate possible new features to upgrade the configuration accordingly;
  - defining system architecture to make a consistent set of sub-functions of the DAA solution for MALE and tactical RPAS;
  - feasibility of tactical RPAS applications:
    - DAA adaptations to tactical RPAS operations;
    - certification considerations for tactical RPAS;
  - sensors:
    - minimising the weight/volume of the sensors/system applying a SWaP<sup>77</sup> approach;
  - provide validation and standardisation of DAA;
  - provide resources to obtain European standards;
  - standardisation:
    - support the standardisation in terms of maintaining the already available standards based on the feedback from testing;
    - complementing standards with new elements stemming from the activities.
- System prototyping:
  - definition and build/update of the “engineering development model” version of the pre-production prototype, to evaluate the performance of the system;
  - prototype the system with environment constraints level (e.g. vibrations, temperature, RTCA<sup>78</sup>/EUROCAE DO160) corresponding to different RPAS classes (e.g. MALE RPAS, Tactical RPAS, rotorcraft UAS as optional).
- Testing:
  - testing of the system as a unified whole, in terms of performance, compatibility, reliability, maintainability, availability and safety;
  - system performances and behaviour tested and validated in environments of European air traffic and international air traffic including relevant parameters;
  - validation of the DAA solution;
  - verification of system components to prove feasibility;

---

<sup>77</sup> Size, Weight, and Power

<sup>78</sup> Radio Technical Commission for Aeronautics



- checking that the software meets the system requirements and its compatibility with the hardware;
  - execution of simulations, to evaluate the performance, effectiveness and compatibility between the prime defined mission and specific oriented segments of the system;
  - execution of field tests in a realistic operational environment, to verify the system's performance in different realistic scenarios including collision avoidance scenarios;
  - verification of interoperability with the remoted pilots, in terms of data link characteristics, communication protocols and human-machine interfaces efficiency;
  - diagnostic on discrepancies, faults and non-conformities with the wished system requirements and behaviour and quick response by a remedial plan of actions.
- Qualification:
- checking that the system meets its operational requirements to effectively accomplish its mission and user needs;
  - evaluation of all elements of the system on an integrated basis;
  - evaluation of all major interfaces among the different subsystems or subfunctions of the DAA;
  - assessment of the possible impact of the DAA system to other closely related operating systems of the UAS;
  - derivation, evaluation, and application of possible upgrading changes to the system's configuration;
  - provision of evidence for further environmental qualification;
  - final identification of detailed plan for certification of UAS equipped with DAA;
  - obtain full recognition of the DAA solution and DAA related standards including regulatory conditions, AMCs<sup>79</sup> or other MOC<sup>80</sup>.

In addition, the proposals must substantiate synergies and complementarity with activities described in the call topic EDIDP-ISR-DAA-2019 targeting the *development of a European Detect and Avoid (DAA) function based on new sensors and processing for RPAS integration into air-traffic management*, as well as the European Defence Agency's Mid-air collision avoidance system (MIDCAS) project and SESAR.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)

---

<sup>79</sup> Acceptable Means of Compliance.

<sup>80</sup> Means of Compliance.

- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement
- and
- based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed product and technologies should meet the following functional requirements, in line with capability requirements as jointly agreed by supporting Member States and EDF associated countries (Norway):

- a DAA solution to allow operation in all airspace classes (including TMA) and at any time without UAS specific restrictions;
- a DAA solution that can be certified (military and civil) for the intended operation with involvement of relevant stakeholders for respectively certification and scenario definition;
- fulfil every given requirement resulting from the standardisation efforts in cooperation with the relevant stakeholders in ATI in Europe;
- identify and assess detailed additional common requirements in accordance with needs of EU Member States and EDF associated countries (Norway) while ensuring the harmonisation of international requirements and potential military specific requirements on DAA systems;
- enable UAS navigation in airspace without constant inputs from remote pilots, thanks to an agreed and final version of a standard for detect and avoid;
- enable participation of UAS to the same operation with other manned and unmanned aircraft;
- detect and avoid cooperative and non-cooperative traffic by providing traffic information, as well as, when appropriate, providing alerts and guidance, and performing avoidance manoeuvres while not creating another dangerous situation with other aircraft;
- ability to execute either CA or RWC manoeuvres. Alerts and guidance of RWC manoeuvres as a second layer of conflict management, when separation is the responsibility of the remote pilot. Execution of collision avoidance as third and last layer of conflict management, to protect the aircraft from collision in an imminent collision hazard;
- provide interoperability with CA systems (ACAS<sup>81</sup>/TCAS<sup>82</sup>) on manned and unmanned aircraft;
- execute manoeuvres complying with the existing rules and regulations for

---

<sup>81</sup> Airborne collision avoidance system.

<sup>82</sup> Traffic collision avoidance system.

manned aircraft;

- operate without interfering or counteracting the normal execution of ATC<sup>83</sup>;
- an intruder detected by different sensors to be processed in a way that it is only displayed to the pilot as a single intruder following sensing data fusion;
- use miniaturised non-cooperative sensors for smaller UAS compatible/compliant with minimal operational performance standards (MOPS);
- support coordination with other DAA hazard detection systems to assure appropriate actions when different hazards are present at the same time;
- fulfil civil and military requirements for different categories of RPAS with initial focus on MALE and tactical RPAS;
- be integrable (minimising the customisation process) in different categories of RPAS;
- perform its intended functions in en-route and Terminal Manoeuvring Area (TMA);
- obtain system performances and behaviour validated:
  - with models representative for European air traffic and international air traffic including relevant parameters. (e.g. Monte Carlo simulations);
  - in environments of European air traffic and international air traffic including relevant parameters (man-in-the-loop simulations).

### Expected impact

The outcome should contribute to:

- UAS/RPAS access to civil and military airspace with full operational capability regarding DAA for the hazard of conflicting airborne traffic without any UAS/RPAS specific restrictions in European airspace including in TMA;
- new and more flexible uses of UAS operational exploitation, due to the drastic safety margins increase;
- improved civil / military cooperation to airspace management;
- availability to the European industry of an improved toolbox of DAA functions, for the purpose of airborne conflict management;
- improved UAS radar and electro-optical (EO)/infrared (IR) sensor detection, tracking and identification capabilities;
- European standardisation of RPAS/UAS DAA technology for the benefit of the EU and EDF associated countries;
- increased European industrial capability and competitiveness in UAS and autonomous systems.

---

<sup>83</sup> Air Traffic Control

## **EDF-2023-DA-SENS-GRID: Sensor grid**

### Objectives

#### **General Objective**

Driven by the changing geopolitical situation, Europe is facing new and evolving threats that are smaller, faster, and more diverse, with increased manoeuvrability, in greater numbers and with denial-of-service capabilities. There is a strong need to detect and characterise challenging targets. Those include small size, high speed, low signature (stealthy) targets and targets in congested and contested electromagnetic environments, e.g. urban environments. There are various examples of such challenging targets that necessitate different configurations and range of active and passive sensors to be detectable such as UAS, hypersonic or ballistic missiles, stealth targets, swarms, etc.

Most of our potential adversaries have gained technological and operational knowledge in a number of sensor's capabilities, including both active and passive sensing. It is obvious that the technological lead in sensors will provide a definite technological advantage for the fast and accurate shaping of situational awareness and battlefield management.

Moreover, European standards for the Concepts of Operations and Rules of Engagement aim at achieving positive target identification before any use of weapons to reduce fratricide and avoid unintended casualties or destruction. Optimal use of sensors in an architecture could increase the level of confidence to have accurately recognised and (if possible) identified a real threat with a low false alarm probability.

#### **Specific objective**

The EU Member States and EDF associated countries (Norway) already own or are developing a variety of high-end sensor equipment and weapon systems for defence against challenging targets. However, in most cases even at national level and most importantly at European level, existing systems still follow stand-alone concepts, that is not considering fusion of data from distributed networks of sensors and especially not cooperation between sensors. For the specific application of naval surveillance, efforts are addressing the exchange and fusion of plots of targets created by the different sensors, through domain-specific communication systems (e.g. through call EDF-2022-DA-NAVAL-NCS). There is the necessity for complementary efforts.

Indeed, facing new and challenging threats, requires building an even more collaborative real-time sensor network, where particular sensors' capabilities will be optimally combined through a flexible architecture.

Such an integrated sensor network solution should encompass passive and active surveillance techniques based on different types of sensors working in different bands of the electro-magnetic spectrum (electro-optical and radio frequency) in order to collect information in a broad spectrum. Advantages of both stationary and mobile sensor platforms could be exploited, e.g. through sensor dynamic resource management. Information processing suitable for detection of new threats should be supported both close to the sensor and – after transferring the data – at a more central processing unit, where signal and data fusion could create a complete situational picture.

This approach is expected to considerably improve the military capabilities in detecting, tracking, recognising and eventually identifying novel challenging targets in the battlespace by increasing the probability of target detection, as well as track stability and creating a continuous real-time situational picture. This will provide a technologically competitive advantage in the fields of situational awareness, mission

planning, support of decision making and eventually even fire control.

### Scope and types of activities

#### **Scope**

The proposals must address the establishment of a European Architecture Framework for multiple interoperable and collaborating sensors. Efforts should aim at overall sensor performance optimisation (e.g. in terms of coverage, accuracy and efficient use of electromagnetic spectrum) against diverse and evolving challenging threats. The Architecture Framework should enable the integration and optimal use of EU Member States and EDF associated countries (Norway) sensor assets that exist or are under development and collaborative use of the sensors data.

The architecture framework must be capable of integrating radar sensors and it should be capable of integrating other types of sensors such as electro-optical, acoustic or others with various modes of operation, such as ground-based and airborne, passive and active, stationary and mobile. The proposals may not include efforts on the integration of space assets that would create unnecessary duplications with ongoing and planned projects but may prepare the future combination of the different research and development results in the future.

The proposals should include aspects of flexible architectures and dynamic asset and resource management for real-time planning of sensor grids adaptable to different tasks, threats and situations. The proposals may not address the development of new sensors.

The proposals should address aspects of data exchange and data fusion between sensors and command centres. The proposals may provide the creation and maintenance of a shared common picture of available sensors and effectors.

The proposals must address surveillance tasks and tracking and aim at improved accuracy of threat detection, tracking and classification of targets. Activities proposed may extend to the field of fire control to advanced effectors in a network. The proposals must be suited to support Integrated Air & Missile Defence (IAMD) operations. Additionally, the proposed architecture framework should be capable of addressing other types of targets or domains of application (e.g. drone detection, swarm detection).

The proposals must address cybersecurity aspects as integral part of the architecture consideration.

In addition, the proposals must substantiate synergies and complementarity with foreseen, ongoing or completed activities in the field of Integrated Air & Missile Defence, notably those performed or foreseen in the context of the PESCO initiative TWISTER and the call topics EDF-2021-AIRDEF-D-EATMI and EDF-2022-DA-SPACE-SBMEW, as well as other projects in the field of radar technologies, e.g. in the EDA framework.

The proposals should take into account projects with related challenges concerning the integration of heterogeneous sensors, such as the call US-03-2019 of the Preparatory Action on Defence Research, which addressed the integration of heterogeneous drone-carried sensors, and the establishment of a collaborative surveillance network such as in the call topic EDF-2022-DA-NAVAL-NCS, by aiming at complementary outcomes. The proposals should also ensure compatibility with ongoing projects in other frameworks, in particular efforts to establish surveillance networks in the NATO context.

The proposals may not particularly focus on the use of over-the-horizon radars using

sky-wave propagation as addressed by the call topic EDF-2021-DIS-RDIS-OTHR.

### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

<b>Types of activities</b> (art 10(3) EDF Regulation)		<b>Eligible?</b>
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (mandatory)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>84</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>85</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>86</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - define operationally realistic use cases (i.e. threat descriptions, sensor grid constellation, communication network requirements...) and define

<sup>84</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>85</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>86</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- adequate performance indicators;
- definition and modelling of objectives, tasks and threats to determine assignments and settings of sensors, and optionally effectors;
- execute and analyse performance simulations to evaluate the potential added value of the architecture;
- investigate a concept for sensor planning and dynamic resource management on different command levels, based on available or new dynamic resource management solutions.
- Design:
  - integrate sensor planning and dynamic resource management in the architecture framework;
  - describe the top-level architecture;
  - define the communication network architecture and requirements;
  - establish the required Quality-of-Service needs for contributing sensors;
  - define the timing and geographic positioning needs for operating a sensor grid;
  - include or establish a protocol enabling flexible integration and elimination of assets from the network;
- System prototyping:
  - prepare a prototype implementing the architecture;
- Testing:
  - perform a demonstration of the added-value of the architecture using various European assets;
  - analyse the results in terms of quality of service and key performance indicators.

Additionally, the proposals should cover the following tasks:

- Studies:
  - to investigate modern signal processing, advanced sensors and data fusion and decision support (e.g. using artificial intelligence, machine learning) to achieve better target information extraction and complementarity between different sensors;
- Design:
  - adaptation of existing C2 interfaces.

The proposals may also cover the following tasks:

- Design:
  - to design the necessary algorithms to achieve better target information extraction and complementarity between different sensors, using

modern signal processing, advanced sensors and data fusion and decision support;

- System prototyping:
  - establishment of new user interfaces.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed development should meet the following functional requirements:

- the architecture should be able to incorporate information from sensors being used within the Member States and EDF associated countries (Norway);
- the architecture should use the available information to optimally set up its attached sensors, given a certain task and taking into account sensors' spatial diversity, complementary sensing geometries and measurement error statistics;
- the architecture should have a certain level of control over its attached sensors (e.g. concerning their modes of operation);
- the solution should enable data fusion from multiple and possibly moving sensor nodes as well as information transmission to multiple potentially mobile military command centres;
- the architecture should be scalable and be able to establish small networks (a few sensors locally) to large networks of sensors (large amount of sensors placed in multiple countries);
- the architecture solution should be able to assess its current performance;
- the solution should allow dynamic and real-time planning of the integration and configuration of heterogeneous sensors to adapt the sensors grid to the mission;
- the solution should be able to adapt the network and sensors' settings to optimise the performance of each sensor by taking advantage of information



gathered by other sensors. Each sensor of the grid should be able to compensate some of the detection and discrimination limitations of the others, thus offering better overall performance;

- the solution should improve the detection, classification, identification and continuous tracking of single and multiple airborne, ground and seaborne threats (such as small size, high speed, low contrast, camouflaged, in degraded visual environment, in an urban environment, UAS/UAV/Drones, hypersonic/ballistic missiles, stealth targets, cruise missiles, etc.);
- the solution should be adaptable towards future threat evolutions;
- the solution should be in line with operational doctrines and systems of EU Member States and EDF associated countries (Norway). The resulting architecture and standards need to be open for all EU Member States and EDF associated countries (Norway);
- the solution should be compatible with efforts to establish surveillance networks in the NATO context;
- the solution should support efficient electromagnetic spectrum management;
- the solution should mitigate performance limitations caused by intentional or non-intentional interference in the electromagnetic spectrum, e.g. through the use of multiple sensors and communication systems operating in diverse spectrum bands, through adapting sensors settings, etc.;
- the architecture framework should take into account cybersecurity;

Optionally, the solution may be able to make use of threat libraries to support different types of sensors to detect and classify targets.

### Expected impact

The outcome should contribute to:

- enhancing information superiority and situational awareness at European level by achieving effective, robust and efficient target surveillance and reconnaissance;
- performing a major step towards a European Integrated Air & Missile Defence (IAMD), contributing to European strategic autonomy and complementing capabilities of NATO allies;
- enhancing the cooperation of armed forces of EU Member States and EDF associated countries (Norway) and increase the interoperability among different sensors at European level.

## **EDF-2023-DA-CYBER-CSA: Full-Spectrum Cyber Situational Awareness for enhanced Cyberspace Operations Support**

### Objectives

#### **General objective**

According to the EU Military Vision and Strategy on Cyberspace as a Domain of Operations<sup>87</sup>, cyberspace comprises the distinct but interrelated physical layer, logical

---

<sup>87</sup> ST11926/21 (16.09.2021)

layer and cognitive layer, which cannot be considered independently, but is one facet of the triad cyberspace, electromagnetic environment and cognitive environment. Pointing to the same direction, NATO's doctrine for cyberspace operations described cyberspace in terms of three layers: physical, logical and cyber persona, where Cyberspace Operations (CO) always include the logical layer, but may also include activities or elements from the other two layers.

Military activities in cyberspace may comprise two overarching missions: to protect and defend their own cyberspace (national level, EU level, Coalition level, etc.) and conduct COs. In this context, Cyber Situational Awareness (CySA) describes the capability of perceiving, reasoning and projecting knowledge of the elements in the battlespace necessary to make well-informed decisions, putting emphasis on the cyber situations and their propagations to planned missions. Commanders need to acquire CySA at strategic, operational and tactical levels in order to make informed decisions on how to operate in cyberspace towards enhancing mission assurance and achieve cyber effects to support mission objectives. On the other hand, a holistic and human-understandable representation of the whole situation is needed.

### ***Specific objective***

Previous national and EU initiatives have addressed the conceptualisation and development of technologies for the acquisition of situational awareness by focusing on the logical sub-layer of cyberspace (software, services, networks, interfaces, etc.) but there is a raising demand of military-focused solutions able to holistically understand the cyberspace as a whole, taking into account all the layers.

The military operations in cyberspace possess complexity intrinsically linked to the challenge of understanding in real time the state of the different data processing planes in which its various actors coexist, as well as the relationship with the lines of effort, tasks and objectives of the missions they enable, where allies, enemies, unknown and neutral entities may coexist. These military operations extend the scope of the conventional understanding of situations in Cyber-Physical Systems (CPS) towards covering the understanding of the dependencies between the cyberspace and the COs context, the latter comprising Lines of Operation (LOOs) and their dependencies, Decisive Conditions (DCs) and how effects triggered by cyber situations may be derived on them, cyber Centres of Gravity (CoGs), missions in or through cyberspace, mission-enabling capabilities linked to cyber assets, etc., and impact/effect dimensions related with kinetic battle domain (air, land, space, sea) or hybrid propagations (information, political, economic, social, environmental, etc.). Developing mission-centric CySA capabilities able to assist human decision-makers while preserving the commander's intent is considered a challenge, which is amplified by the difficulty of understanding the different sub-layers of cyberspace as a single environment and considering the hybrid effects consequent of cyber situations.

### ***Scope and types of activities***

#### ***Scope***

The proposals must focus on developing capabilities for mission-centric CySA, which as a System of Systems (SoS), must comprise independent enablers able to act jointly towards facilitating human decision-making through synergies between them. The proposals should address challenges in all the following areas:

- Full-spectrum cyber situational awareness:
  - facilitating human decision-makers understanding of the cyberspace spectrum as a whole, including physical (hardware, geographical, Electromagnetic Spectrum, etc.), logical (software, networks, etc.) and cyber persona (Human-Machine Interfacing, cognitive, psychological,

social) assets, conditionings, impacts and effects.

- Decision, command, and control support:
  - identification and assessment of creative and flexible options (CO's Areas of Operation (CoAs), countermeasures, etc.) and opportunities to accomplish missions in or through cyberspace. The proposals should bring CySA to assist decision-making under full-spectrum operational friction, including uncertainty when faced with a thinking and adaptive enemy, which may operate on conventional but also hybrid measures. CySA also facilitates understanding the effect and stress of COs on human actors;
  - associating full-spectrum cyber situations and opportunities with objectives, strategies and initiatives of actors operating within the CoAs (considering features such as interest, responsibility, influence, etc.). Among others, this includes assessing the status of mission essential assets, recognition of players in the operational environment, or developing a joint Situational Awareness (SA). As part of the characterisation of the mission, all instruments of power should be taken into account (approaches such as PMESII<sup>88</sup> or PESTLE<sup>89</sup>). Mission Engineering (ME) may be considered with a view to help determining and analysing the composition and status of decisive cyber conditions that support or impact own missions, while assisting the assessment of opportunities on neutral/adversarial missions, centres of gravity and CoAs;
  - capability orchestration enabling deployability within joint forces, and adapted to decision-makers at all war levels. This includes adapting to collaborative environments like joint and/or combined operations at the national, EU and NATO levels. Capability to dynamically adapt to the operational context in agreement with different human intervention profiles.
- Interoperability:
  - the results should enable interoperability with EU-level and NATO-level C2 initiatives.

### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (see *Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No

<sup>88</sup> Political, Military, Economic, Social, Information, Infrastructure (PMESII).

<sup>89</sup> Political, Economic, Sociological, Technological, Legal and Environmental (PESTLE).

Types of activities (art 10(3) EDF Regulation)		Eligible?
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (Optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (Mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (Mandatory)
(e)	<b>System prototyping</b> <sup>90</sup> of a defence product, tangible or intangible component or technology	Yes (Mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (Optional)
(g)	<b>Qualification</b> <sup>91</sup> of a defence product, tangible or intangible component or technology	Yes (Optional)
(h)	<b>Certification</b> <sup>92</sup> of a defence product, tangible or intangible component or technology	Yes (Optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (Optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- studies and design of a holistic CySA enabling solution able to orchestrate EU cyber defence-related capabilities towards achieving full-spectrum awareness for assisting COs in or through cyberspace, on a mission-centric perspective;
- studies and design of specific CySA capabilities to discover and assess opportunities in or through cyberspace in the context of multi-domain operations, and to support commanders to benefit from them;
- studies and design of specific CySA enabling capabilities for an easy full-spectrum understanding of cyber frictions, adversarial postures and their effects according to the commander's intent, with emphasis on mission characterisations, analysis and implementation;
- System prototyping: demonstrators on the previous area's points.

<sup>90</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>91</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>92</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

In addition, the proposals should cover the following tasks:

- testing of complementary large-scale demonstrators supported by national and EU end-users on tactical, operational and strategical storylines;
- explore the recent advances of edge processing in order to ensure independent functionality and partly-offline reduced human intervention especially at the tactical level as MSOCs and MNOCs often use low quality air gapped networks.

The proposals must also substantiate synergies and complementarity with activities described in the call topics EDIDP-CSAMN-SSS-2019 and EDF-2021-CYBER-R-CDAI, and in other relevant EU ongoing activities.

The proposals must give due consideration to design principles and implement a specific ethics-focused approach during the development, deployment and/or use of AI-based solutions, e.g. by the Assessment List for Trustworthy AI (ALTAI), in order to develop procedures to detect and assess the level of potential ethical risks and address them.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposals must be supported by a set of capability requirements as agreed by a group of Member States or EDF associated countries (Norway). The proposals must give evidence of coherence between the proposed activities and the requirements by the Member States and EDF associated countries (Norway).

The proposals should aim to provide:

- a full-spectrum Recognised Cyberspace Picture (RCyP), combining cyberspace, electromagnetic environment and cognitive environment, that is able to assist human decision-makers from a mission-centric perspective;
- capability to analyse RCyP information and forecast combined effects for Cyberspace Operations, based on monitored, collected, shared and fused data from multiple sources and authorities, and derived from different battlespace dimensions;
- ability to share information and cooperate with different stakeholders prior,

during and after mission execution;

- interoperability with EU Cyberspace Operations;
- capabilities to discover, track, identify, and assess both threatening situations (for mitigation) and mission-centric opportunities (for exploitation), in order to make successful Cyberspace Operations.

### Expected impact

The outcome should contribute to:

- a stronger, more competitive and technologically independent European Defence Technological and Industrial Base (EDTIB) when it comes to solutions for cyber defence capabilities, cyberspace operations and Cyber Situational Awareness;
- improved situational awareness, resilience and security of EU Cyberspace Operations;
- reduction of the minimum reaction time for deployment and increased feasibility of EU military missions;
- improved interoperability and future capabilities of EU Member States and EDF associated countries (Norway) forces in the area of cyber defence for cyber mission planning and execution;
- improved interoperability of C2 systems;
- better cooperation of EU Member States and EDF associated countries (Norway), research and industrial actors towards defining a common vision on Cyberspace Operations.

## **EDF-2023-DA-CYBER-DAAI: Deployable Autonomous AI Agent**

### Objectives

#### **General objective**

Artificial intelligence (AI) begins to transform cybersecurity. Recent advances in machine learning (ML) techniques could enable ground-breaking capabilities in the future, including defences that automatically interdict attackers and reshape networks to mitigate offensive operations. ML combined with AI could shape cyber operations in ways that drive more aggressive and destabilising engagements between state actors. Therefore, it is valuable to anticipate how adversaries might adapt their tactics and strategies, and to determine what challenges might emerge for defenders.

The field of AI is at a critical crossroad. Globalisation and industrialisation of AI is intensifying, while the ethical and regulatory issues of these technologies are multiplied. AI has moved from an emerging technology to a mature technology, which is no longer dealing with a speculative part of scientific research, but instead something that has real-world impact, both positive and negative. The importance of AI in cyber operations has been noticed by many nations. AI is a strategic technology that could prove incredibly consequential for the competitiveness of the EU, its Member States and EDF associated countries (Norway).

#### **Specific objective**

Today's conversations on AI in military affairs concentrate on various variants of "narrow" artificial intelligence. Current discussions on AI often primarily concentrate

on ML, which is the process of using algorithms to learn from data. Much of the most exciting progress in recent years has leveraged deep learning, a technique that involves the use of layers of artificial neural networks, which are inspired by the structure of the human brain.

At a basic level, AI involves software that leverages data for learning but also requires hardware to harness the power of significant computing capabilities to enable that process. It is inherently challenging to define what AI is or can achieve when the field is so dynamic and evolving so rapidly. For the time being, AI/ML techniques are often limited by the availability of data, although this may change with advances in the use of synthetic data, real-life cyber exercises, data lakes and techniques that leverage reinforcement learning, such as the capability to learn from self-play alone.

The main challenge of this topic is to establish an investigative approach on an area of autonomous deployable AI creation, with the intention to broaden artificial intelligence perspective in cyber defence in the EU.

### Scope and types of activities

#### **Scope**

The proposals must focus on the development of an autonomous and adaptive deployable AI agent. All proposed activities must ultimately support the creation of an AI agent that is able to conduct automated and semi-automated incident management on different cyber defence systems for the entire process of the incident management cycle. The solutions must support human operators, analysts and decision-makers at technical, tactical, operational, strategic and political level. In addition, solutions are expected to contribute to enhanced cyber situational awareness, increased military infrastructure resilience and improved protection against AI-based and other advanced cyber threats.

The work should identify gaps for achieving an autonomous AI agent for military systems. The final result should build on a general-purpose AI agent that can be deployed in different operating environments.

The work should also address the gap of learning data sets through the use of live-fire exercises, data lake concepts and self-learning algorithms. Access to the data sets should be planned in a decentralised way to allow the solution to be deployable. This implies, that new architectures and solutions should be considered in achieving decentralisation, utilising and enhancing for example AI-powered edge computing.

The assessment of the proposed solution must be evaluated during live-fire exercises with a method allowing comparison of the developed AI agent against actual defending teams. This means using learning data from different exercises, but also data feeds from the exercise itself, where the AI agent is competing.

#### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No

Types of activities (art 10(3) EDF Regulation)		Eligible?
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>93</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>94</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>95</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - the proposed activities must include feasibility studies drawing upon real-world scenarios and live-fire exercises in order to ensure that developed solution and techniques are fit-for-purpose.
- Design:
  - the proposed solutions must include creation of AI-based techniques for detecting and understanding adversarial activity;
  - the proposed solution must include creation of AI-based techniques for building knowledge about own protected ICT systems (e.g. a “cyber record” with current and historical information). This must include collecting, linking and fusing different kinds of information about the system hardware, software, and the relationship between them.

<sup>93</sup> ‘System prototype’ means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>94</sup> ‘Qualification’ means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>95</sup> ‘Certification’ means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.



Previously used analysis should enhance the more generalised AI solution.

- System prototyping:
  - the proposed solutions must demonstrate the creation of AI-based information collection and storage systems that dynamically adapts its collection and storage strategy to the situation as continuously analysed and perceived by the system;
  - the proposed solutions must be able to conduct automated and semi-automated incident management on different cyber defence systems for the entire process of the incident management cycle.
- Testing:
  - the proposed solutions must be tested in a live fire-exercise against real defenders.

In addition, the proposals should cover the following tasks:

- Studies:
  - the proposals should reuse previously created reference systems or develop new ones and appropriate test cases to generate training data and evaluate the efficacy of different solutions, both with and without human operators interacting with the system.
- Design:
  - the proposed solutions should include creation of AI-based techniques for detecting and understanding adversarial activity tasks on:
    - analysing and triaging alarms, conducting forensics, utilising external information with varying levels of trust (e.g. threat intelligence);
    - leveraging behavioural analytics, performing kill-chain detection and analysis, assessing potential attacker intentions;
    - monitoring applications and communication activities, analysing malware;
  - the techniques should be intended for both real-time and non-real-time detection and analysis, involve multi-disciplinary approaches, use data from endpoints, networks and the cloud, and leverage distributed computing and data processing for real-time scalability;
  - the creation of AI-based techniques for building knowledge about own protected ICT systems (e.g. a “cyber record” with current and historical information) should utilise previously used analysis to enhance the more generalised AI solution;
  - AI agent architecture should consider decentralised data sets with new state-of-the-art hardware;
  - the proposals should include functional modules for mapping threat actors based on common frameworks like MITRE and RICHDATA.

The proposals must also substantiate synergies and complementarity with activities

described in the call topics EDIDP-AI-2020, EDF-2021-CYBER-R-CAI, and with other relevant EU ongoing activities.

The proposals must give due consideration to design principles and implement a specific ethics-focused approach during the development, deployment and/or use of AI-based solutions, e.g. by the Assessment List for Trustworthy AI (ALTAI), in order to develop procedures to detect and assess the level of potential ethical risks and address them.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposals must be supported by a set of capability requirements as agreed by a group of Member States or EDF associated countries (Norway). The proposals must give evidence of coherence between the proposed activities and the requirements by the Member States and EDF associated countries (Norway).

In addition, the intended final outcome should at least:

- be able to work autonomously in the deployed environment, but also allow manual interruption and reasoning of the decision process;
- be able to create AI-based information;
- be able to collect and store needed information in dynamic big data and data lake concepts in a decentralised manner;
- be deployable and it should be possible to deploy the solution in different environments with all needed components;
- Use CTI (Cyber Threat Intelligence) and technical information exchange platforms (such as MISP, HIVE) in order to enrich data sets and information of ongoing cyber activities.
- include an architecture that is open, modular, scalable, resilient and highly available.

### Expected impact

The outcome must contribute to:

- a stronger, more competitive and technologically independent European Defence Technological and Industrial Base (EDTIB) when it comes to solutions for next generation cyber defence capabilities;
- enhanced security for the EU, its Member States and EDF associated countries (Norway) by ensuring capable defence measures against AI-based cyber attacks;
- alleviating human resource availability problems;
- advanced preparedness to counter emerging threats for critical infrastructure providers and to enhance military mobility.

### **EDF-2023-DA-SPACE-SSA: Initial operational capacity for Space situational awareness C2 and sensors**

#### Objectives

European cooperation on military space situational awareness (SSA), including the development of a common Space Surveillance Network (SSN), interoperable military SSA Command and Control centres, exploitation tools and new SSA sensors, is recognised as a key solution to enhance Space Domain Awareness (SDA) of EU Member States, EDF associated countries (Norway) and the EU. A SSA capability, based on the capabilities of the Member States and EDF associated countries (Norway) and taking into account interoperability and standards developed between NATO members, is crucial to assess the space situation. This capability, focused on the needs and requirements of the EU Member States and EDF associated countries (Norway) defence end-users, is required to characterise and identify intentional threats against the EU, its Member States and EDF associated countries (Norway) space infrastructure and may also, as a side effect, complement and extend current and future EU Space Surveillance and Tracking (EU SST) services provided by dual-use sensors.

The main challenges faced by a European approach of military SSA are:

- to harmonise the requirements for a shared Recognised Space Picture (RSP) among supporting Member States and EDF associated countries (Norway) (sMS) focusing on defence users' needs thus increasing cross-country military coordination;
- to characterise space activities which represent potential threats against sMS space systems, thus contributing to the deterrence of space attacks and to the support to space operations;
- to achieve a larger degree of European autonomy on military SSA and to safeguard European interests in space.

#### **General objective**

The general objective of this topic is to develop interconnected military SSA centres with their respective sensors to foster a larger degree of European autonomy with respect to awareness of the situation in space in order to contribute to a RSP, and support space operations, taking also benefit of relationships which may be established with other partner nations and organisations and their capabilities.

### ***Specific objective***

The specific objective of this topic is to develop military SSA sensors, command and control centres and Space Surveillance Network initial operational capability among the SMS.

### ***Scope and types of activities***

#### **Scope**

The proposals must address the development of a military SSA capability broken down into two components:

- sensors and data processing for detection, tracking, identification and characterisation of space objects in LEO, MEO and GEO orbits;
- Space Situational Awareness Command and Control (SC2) centres, able to manage the sensors and the processing of collected data, including fusion of data processed at sensor level, and a space surveillance network (SSN) interconnecting military SSA C2 centres allowing the sharing of data;

able to:

- allow SSA sensor planning, data management, processing and sharing inside and between military Space Situational Awareness C2 Centres of SMS in accordance with an agreed data policy up to SECRET level;
- provide the basis for a shared, and consequently enhanced RSP and support space operations through added-value services to SMS;
- share data with military Space Situational Awareness centres of NATO allies.

The proposals must cover at least the following sensors:

- ground-based optical sensors. This item should include:
  - photometer;
  - spectrophotometer;
  - laser ranger;
  - high frequency imager;
  - polarimetric imager;
  - adaptive optics;

This may also include multiband imager (from visible to IR).

- ground-based RF sensors. This item should include:
  - radar sensors in monostatic configuration, including tracking and surveillance radars with characterisation capabilities;
  - radar sensors in multistatic configuration;
  - Inversed Synthetic Aperture Radar (ISAR) imaging radars (considering multidimensional imaging);
  - passive radio-frequency;

- space-based sensors as hosted payloads for big satellites and small satellites and as only payloads for small satellites for LEO, MEO and GEO. This item should include:
  - optical, including multi-band/hyperspectral imaging systems;
  - radar;
  - passive radio-frequency.

### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>96</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>97</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	<b>Certification</b> <sup>98</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

<sup>96</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>97</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>98</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

The proposals must cover at least the following tasks as part of the mandatory activities:

- the further development of military SSA C2 systems (including qualification for some functions) able to operate in an environment up to SECRET;
- the further development of military SSA ground-based sensors both optical and RF (including qualification for some of them) and definition of formats of data that are common to each type of sensors and compatible with the SSA C2 / SSN;
- under the framework of an agreed data policy, increase the modularity of the system architecture, flexibility of use, and responsiveness of the SSN (including qualification for some functions) through the combination and optimisation of resources (sensors and processing services), with the ability to handle data and/or information up to SECRET;
- further study and design of new space-based SSA sensors interoperable with SSA C2 systems.

In addition, the proposals should cover the following tasks:

- as part of testing, the interconnection of a sub-set of highly matured sensors with the above-mentioned SSA C2/SSN systems, to provide the basis for the creation of a shared RSP;
- the testing of SC2, SSN and selected sensors in an operational environment, involving at least two military SSA centres located in two EU Member States or EDF associated countries (Norway);
- for SSN, development (design, prototyping, testing) of high added-value tools to support joint multinational and multisensor planning, operations, data sharing and simulation activities;
- for photometer, further development, prototyping and test;
- for spectrophotometer, further development, prototyping and test including, developing observation strategies, testing in multiple sites, training of the machine learning capability based on measurements;
- for laser ranger, further development, prototyping and test allowing automation, compliance with laser safety regulation, remote control, availability of a European laser source, daylight operations and simulations;
- for high frequency imager, further development, prototyping and test allowing improved image quality, a more automated system and daylight operations;
- for polarimetric imager, further development, prototyping and test;
- for adaptive optics for high resolution imagery, further development, prototyping and test, including robustness increase, calibration automation and exploitation ease;
- for imaging radar, further development, prototyping and test including hardware and software development of a multistatic architecture;
- for tracking and surveillance radars with characterisation capabilities, further development, prototyping and test of characterisation modules, also through simulation;

- for passive radio-frequency, further development, prototyping and test allowing maximum coverage (both through antennas and bands monitoring);
- for radar sensors in multistatic configuration, further development, prototyping and test also with the objective to evaluate, also through simulation, the number and the geographical distribution of sensors;
- study and design of space-based SSA systems and missions in different orbits (LEO, MEO and GEO) with different sensors (optical, radar and passive radio-frequency);
- the development of technologies and assets increasing efficiency across the lifecycle (e.g. lower production, operational, maintenance, repair and overhaul or disposal costs) for the sensors, SC2 and SSN;
- the testing, in a real operational and multinational environment, of some of the integrated military SSA/SSN solutions, composed of interoperable C2 capabilities, exploitation tools and sensors.

The proposals must substantiate synergies and complementarity with foreseen, ongoing or completed activities in the field of SSA, notably those performed or foreseen in the context of the call topics EDIDP-SSAEW-SC2-2020<sup>99</sup> and EDIDP-SSAEW-SSAS-2020<sup>100</sup>, as well as in the context of the EU SST framework<sup>101</sup>. The proposals should also, where relevant, substantiate synergies and complementarity with the activities foreseen within the call topic EDF-2023-RA-SPACE-PSA.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement
 and
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

Military SSA capabilities to be developed should contribute to the following main functions:

<sup>99</sup> Advanced Space Command and Control (SC2) capability to process and exploit SSA data generated from sensors and catalogues to provide a complete space picture (edidp\_call-texts-2020\_en.pdf (europa.eu)).

<sup>100</sup> Enhanced SSA sensors for accurate identification and characterisation of existing Geostationary Earth Orbit (GEO) and Low Earth Orbit (LEO) public and private assets (edidp\_call-texts-2020\_en.pdf (europa.eu)).

<sup>101</sup> <https://www.eusst.eu>

- detection, surveillance and tracking of objects from, to and in space with a focus on the timely detection of anomalous/potential hostile manoeuvres and threats;
- identification, characterisation, including behaviour/pattern of life recognition, and classification of objects and activities (such as active spacecraft, rocket body, debris, etc.) from, to and in space, including resident space objects and, where possible, launching activities through RF, thus enabling attribution of space actions or behaviours;
- sharing of data between military SSA centres allowing the establishment of a more complete RSP;
- delivery of services to military space operators (e.g. support to threat surveillance and protection of space-based assets).

### Expected impact

The outcomes should contribute to:

- making military SSA Command and Control (SC2) centres and sensors for EU Member States and EDF associated countries (Norway) available and their assets interoperable;
- ensuring consistency of the SC2 centres with existing national SSA C2 centres;
- enhancing cooperation between undertakings across Member States and EDF associated countries (Norway);
- achieving better performance while reducing costs and avoiding unnecessary duplications.

The expected outcomes of military SSA systems are to:

- contribute to the security and defence of the space domain and space assets that support the EU, its Member States and EDF associated countries (Norway) operations and missions;
- enable secure space operations;
- contribute to the protection of military, national and EU security interests (Common Security and Defence Policy, military operations, protection of populations);
- support the Member States and EDF associated countries (Norway) that are operating launching sites and/or military satellites.

## **EDF-2023-DA-MATCOMP-MJR-CBDIN: Technologies and processes for maintenance, joining and repair through an innovation test hub**

### Objectives

#### **General objective**

The increasing requirements for future military systems demand not only improved performance but also economic and ecological improvements. In order to meet these requirements in the area of structures and construction methods, modular and multi-material designs or the integration of functions are considered as particularly promising. For example, the combination of different materials such as fibre composites and metals shows a very high potential for performance enhancement



with simultaneous economic and environmental advantages. To exploit the potential of such new material technologies in military systems, suitable, high-performance and technically mature joining technologies are required. Additionally, new sensorised materials might enable new certification procedures for joining technologies.

Given the harsh environment in which military systems have to operate and the increase risk of damage during operation, the operability and survivability of platforms depend on fast, efficient and reliable repair methods. The advantages of new materials technologies can only be fully exploited if adequate repair technologies are available and could, ideally, be used in the field.

Due to the complexity of today's systems not only the procurement is capital-intensive but the maintenance also generates considerable costs and the need for significant logistic support. Developing new methods that can decrease the effort to fulfil the operational needs without any negative effect on safety will result in advantage for both civil and military operators. Advances in repair and maintenance technologies will also reduce the environmental footprint of defence equipment. An example for new concepts of maintenance, are technologies involving the use of in-structure or on-structure health monitoring sensors, such as those addressed by the call EDF-2021-NAVAL-R-SSHM. To make such concepts useable for future military systems they need to be matured, repair and maintenance aspects should be taken into account and most importantly, the technologies need to be tested and qualified.

There are several technologies under development in national and European projects addressing the area of maintenance, joining and repair. Research and Development projects often lead to a technology readiness level (TRL<sup>102</sup>) of approximatively 4, meaning that new technologies show potential for use in future military applications and have been validated in a lab. However, these technologies have not yet been tested at demonstrator level (TRL 6/7) and therefore cannot yet be considered useable in military products. The gap between technological proof-of-concept and (at least partially) qualified solutions is often difficult to overcome for innovative solutions. New sources of funding must be found, as further maturation efforts can often not be covered by research funding. At the same time, connections must be established with certification entities, planned defence projects and potential end users, often still unaware of the new technological opportunities. Because of these challenges, summarised as 'valley-of-death', new defence products are often delayed in their transfer into new defence products or even abandoned, although the technologies show large potential for future applications. Specific support to overcome the valley-of-death will enable the use of (partially) qualified and certified technologies in next generation military systems to produce, operate and maintain them at a fraction of cost of current systems.

### ***Specific objective***

This topic will provide support to collaborative development activities to setup demonstrator platforms and test candidate technologies for maintenance, joining and repair, in order to propel those technologies' maturity and allow them to be approved and/or qualified.

There will only be a limited number of innovative technologies directly available within a selected consortium. Therefore, the consortium will be requested to reach out to third parties across the EU and EDF associated countries, in particular SMEs, including start-ups, to test a broad spectrum of technological solutions and give those

---

<sup>102</sup> Definitions of Technology Readiness Levels can be found in the context of Horizon 2020 work programmes, e.g. [https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014\\_2015/annexes/h2020-wp1415-annex-g-trl\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf)

innovative players the opportunity to demonstrate the potential of their ideas to relevant players in the defence application field. As a tool to enable this open innovation approach, funding for financial support to third parties (FSTP) will be integral part of the awarded grant. The consortium will be required to organise calls to third parties to select and award start-ups and SMEs. The selected third parties will be offered the opportunity and financial support to test their solutions, receive technical mentoring and other relevant acceleration services for a specific time period.

Therefore, the specific objective of this topic is twofold. The first is the development of a new test environment for testing and the improvement of technologies up to certification level. The second is the creation of a cross-border defence innovation network that encompasses players that would otherwise not have the means to access EDF actions, thereby further enhancing innovation capacity and competitiveness of the European Defence Industrial and Technological Base.

The consortia responding to the call may include a large variety of entities, such as military or civil test centres, research institutes, universities, industry, certification authorities, accelerators or incubators as well as other organisations that can play a role in the establishment or certification of new technologies for repair, joining and maintenance or that can support the associated innovation support measures targeted towards third parties receiving financial support.

### Scope and types of activities

#### **Scope**

This topic aims at supporting the technological maturation of various joining or repair or maintenance technologies, including the associated processes.

The proposals must address the setup of a suitable demonstrator platform as a test environment which offers the possibility to test, qualify and certify technologies covering the fields of joining, repair and maintenance. This may include the establishment of adequate test protocols. The platform may be focussing on one of the defence application domains air, land or naval or the combination of land and naval domains. The demonstrator platform should be a generic system suitable for this domain (e.g. a plane, a ship, a truck, etc.). The proposals may involve the set-up of a new platform or the partial modification of existing systems to be used as a demonstrator platform, e.g. by replacing individual parts and components or by integrating additional functions, sensors, etc. In addition, various parts or components may be manufactured multiple times to cover different technologies.

The proposals must test various joining or repair or maintenance technologies or combination of them. The considered technologies should have reached the stage of experimental proof-of-concept (TRL 3) or, preferably laboratory validation (TRL 4) but may also have been already validated in a relevant environment (TRL 5). The proposals must address the technological maturity of promising technologies to lead them towards qualification and certification. This must encompass all tests and approvals to achieve the demonstration of the technology in a relevant or operational environment (TRL 6 or 7). The considered technologies must encompass technologies that are not available within the consortium. Technologies must be relevant for military applications but may include technologies originally developed for civil applications. Technologies adequate for 'in-field' repairs should be considered.

The proposals must describe how entities with expertise on the relevant technologies know-how will be supported, including the proposed implementation conditions for FSTP. Beneficiaries of FSTP that contribute with a joining or repair or maintenance technology must receive financial support to prepare a sample of their technology, to attend and support the testing of their technological sample, and to technologically improve their solution. FSTP may also be provided to entities that contribute with

analysis and measurement capacities, technology-specific expertise, innovative tools, or support the manufacturing of technology test samples or components necessary for testing. The proposals must include technical mentoring for the selected beneficiaries of the FSTP as well as the set-up of additional measures to support the beneficiaries' business case.

Although the proposals may consider joining and repair technologies that are applicable and involve the use of additive manufacturing processed parts, the proposals must not focus on the improvement of additive manufacturing processes themselves, as those are covered by the call EDF-2021-DIS-RDIS-AMD. The proposals may not target minor improvements of technologies not having achieved a proof-of-concept (below TRL 3).

### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (mandatory)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>103</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>104</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	<b>Certification</b> <sup>105</sup> of a defence product, tangible or intangible component or technology	Yes (optional)

<sup>103</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>104</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>105</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

Types of activities (art 10(3) EDF Regulation)		Eligible?
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Design:
  - design of a test environment to test and certify technologies for joining, repair or maintenance, including the demonstrator platform;
  - design of components based on innovative technologies for joining, repair or maintenance to be integrated in the demonstrator platform.
- System prototyping:
  - prototyping of a demonstrator platform for various joining or repair or maintenance technologies or combination of those.
- Testing:
  - testing at component and demonstrator level of various joining or repair or maintenance technologies or combination of those that may be developed by entities selected through a call for FSTP at component level.
- Qualification:
  - preparation of documentation and reviews necessary for qualification of the technology or component, e.g. TRL reviews.

In addition, the proposals should cover the following tasks:

- Design:
  - design of digital mock-up or digital twin and simulation of manufacturing and assembly.
- Qualification:
  - qualification of joining or repair or maintenance technologies.

The proposals may also cover the following tasks:

- Design:
  - partial testing of samples of innovative technologies at component level to prepare their integration in the demonstrator platform;
  - support of multi-disciplinary design optimisation;
  - adaptation of the platform design in accordance with the outcome of a call for FSTP.

Concerning the implementation of the FSTP, the proposals must cover the following tasks:

- Integrating knowledge:
  - technical mentoring of beneficiaries selected through sub-calls to receive financial support to third parties.
- Studies:
  - screening and identification of landscape of suitable candidates from various sectors, including those that have not been active in the defence sector before, for the sub-calls organised by the consortium providing FSTP;
  - preparation of the call documentation to issue up to two sub-calls for FSTP;
  - organisation of up to two sub-calls for FSTP;
  - selection and award of beneficiaries for FSTP;
  - offering of an entrepreneurship class on doing business in the defence domain to beneficiaries of FSTP calls;
  - setting up of collaboration and networking activities for beneficiaries of FSTP and other SMEs.

Up to EUR 3 600 000 of the total topic budget may be allocated to FSTP. However, the FSTP in the proposals should target but not exceed 12% of the requested EU contribution. The FSTP can NOT be provided through services offered by the consortium directly.

The FSTP should be issued in up to two distinct calls, with a target from minimum 10 and up to 30 recipients (third parties) per call and where:

- the recipients must be established in the EU or in EDF associated countries
- the recipients must not be subject to control by non-associated third countries or non-associated third-country entities

The calls must be open, published widely (to ensure a clear EU outreach) and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality and must remain open for at least two months.

The outcome of the calls must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final recipient legal names and countries.

The beneficiaries may be involved in any type of task within the proposal. Possible tasks at the level of the calls for third parties may include:

- feasibility studies on alternative solutions, life-cycle analysis (LCA) as well as life-cycle cost analysis (LCCA)
- preparation of sample repair, joining, maintenance technologies to be tested
- analysis support
- measurement capacities

- manufacturing capacities to support the testing or the sample preparation
- support of multi-disciplinary design optimisation.

The FSTP must target in priority SMEs (including start-ups)<sup>106</sup>. Participation of entities other than SMEs can only be accepted where no SMEs are available to demonstrate the capacity or expertise needed for the project during its lifetime.

The FSTP should include various entities from different Member States and EDF associated countries (Norway) and different sectors, including those not active in the defence sector.

The FSTP calls should aim to ensure a balance between experienced SMEs and newcomers.

Certification at company-level or approval as production organisation is not mandatory, but specific business coaching should be provided to non-certified companies.

Your project application must clearly specify:

- the objective and the mix of proposed support, including a fixed list of the different types of activities for which a third party may receive financial support
- the maximum amount to be granted to each recipient (may not exceed EUR 60 000) and the method for calculating the exact amount of the financial support
- the payment arrangements for payments to the recipients
- the criteria for awarding financial support
- the potential results to be obtained
- the roles and responsibilities of the consortium with regard to the management of FSTP
- a clear methodology allowing to measure the FSTP's contribution to the innovation performance of the supported SMEs in the short-term, e.g. via indicators such as numbers of new or significantly improved products (goods and/or services), processes, new marketing methods, or new organisational methods, and to its impact on resource efficiency and/or turnover.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries

---

<sup>106</sup> Applicants for FSTP must have self-assessed their SME status. The consortium should perform checks on the basis of random sampling in accordance with the criteria as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC.

that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement

and

- based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed solutions and technologies should meet the following functional requirements:

- The demonstrator platform should be modular in order to integrate different technological alternatives for the same or different components or parts;
- The technologies and processes should cover a broad range of innovative solutions. It should cover at least 4 out of the 6 following technologies, without being limited to those:
  - novel materials and multi-material constructions in particular the combination of fibre composites with other materials;
  - multi-functional structures with embedded and integrated sensors (e.g. optical fibres), antennas, vents or any other structure combining mechanical performance and additional functionality;
  - joining technologies applicable for the combination of similar and dissimilar materials, in particular co-bonding, adhesive bonding and welding;
  - repair methods for multi-material and composite structures, e.g. patch-repair, cold-spray process...;
  - inspection technologies applicable during maintenance and for in-situ measurement during the use of a product, like structural health monitoring (SHM);
  - maintenance, repair and operation processes with a high degree of automation covering defect analysis, repair process and quality inspection.
- The technologies considered in the proposals should meet the following requirements:
  - the technologies should have the potential to reduce the production costs or the total costs of ownership by reducing the costs and efforts for maintenance and repair;
  - processes considered should have the potential of a high degree of automation, of a high rate of digital data handling and of information storage and availability at production, maintenance and repair stages;
- The FSTP should:
  - be organised in one or two calls to third parties selecting a target of minimum 10 and up to 30 entities per call, depending on the industrial

landscape of the targeted domain, whereas each third party may be supported with up to EUR 60 000 for a maximum 6-month long acceleration programme that encompasses the associated tasks;

- provide the third parties the opportunity to demonstrate their knowledge, technologies, capabilities and products;
  - foster the possibilities for future involvement of these third parties in the European defence community;
  - provide the third parties with necessary knowledge on doing business in defence domain, in particular with respect to protection of IPR, IPR strategies, export control and other specificities of the defence sector;
  - provide networking and collaboration activities that facilitate collaboration amongst innovators and between innovators and end-users (including industry and public bodies) throughout the maturation of their product or technology;
  - be accompanied by a clear methodology allowing to measure the FSTP's contribution to the innovation performance of the supported SMEs in the short-term, e.g. via indicators such as numbers of new or significantly improved products (goods and/or services), processes, new marketing methods, or new organisational methods, and to its impact on resource efficiency and/or turnover;
  - aim at a wider impact on innovation performance of the supported entities in the medium-term.
- The proposals should clearly delineate the expected contributions from the main beneficiaries as well as from the third parties, to ensure their coherence and impact.

#### Expected impact

The outcome should contribute to:

- increased technological maturity of new processes and technologies to be implemented in future military systems to improve their performance, reliability and competitiveness;
- faster development of new systems including an improved flexibility for usage;
- reduction of repair and maintenance costs and increased lifetime for defence systems;
- reduction of logistics footprint, involving actions of transport, maintenance and repair, in particular for operations in harsh environment;
- reduction of the environmental footprint of defence systems throughout their life-cycle;
- strengthening of the European industrial leadership by reinforcing value chains that integrate innovative solutions from SMEs, including start-ups, along and across existing value chains;
- improvement of the business environment and collaboration opportunities for innovative start-ups and SMEs in the defence domain by supporting open innovation and involving innovative actors and customers from different sectors and countries;



- leveraging and complementing support for innovation which may be provided by national or regional authorities and/or by private investors (as follow-up investments) and fostering cross-fertilisation between sectors.

## **EDF-2023-DA-AIR-STFS: Smart technologies for next generation fighter systems**

### Objectives

#### **General objective**

New generation manned and unmanned military aerial platforms require enhanced avionics able to support new architectures and functions, while providing higher performances, safety and cyber resilience.

Against this background, new solutions regarding, for instance, hardware (HW), software (SW, including operating systems, middleware, system services, etc.) and framework, need to be defined in order to comply with new requirements for processing, network, interfaces, storage, power supply, etc.

Military aerial platforms, from fighters to helicopters and other specific mission platforms, could benefit from the application of civil technology breakthroughs and standards. However, they require dedicated solutions to comply with specific military requirements (e.g. SWAP<sup>107</sup>, multi-level security data flow, real time reactive response, etc.).

In particular, modular architectures for avionics are widely recognised as key to reduce development cycles and costs and to increase interoperability in multi-industrial collaborative development, compared to classical federated systems. Therefore, the concept of core integrated modular avionics has been already defined in the civil aviation market.

However, the next generation military aerial platforms, both manned and unmanned, will operate through a system-of-systems approach which implies much higher data sharing and processing needs than in the civil market, as well as new specific requirements in terms of development cycle (cf. need for faster adaptability of mission solutions applying DevSecOps<sup>108</sup> type of development, but also involvement of more industrial entities) and in terms of defence-related missions.

The general objective is then to exploit the knowledge and solutions conceived for civil purposes in the application of such technologies on various military platforms in accordance with defence requirements.

#### **Specific objective**

The challenge of this topic is to study, design and demonstrate, within a 3-year timeframe, key components for a next generation military integrated modular avionics (NG-MIMA) for various military platforms able to operate in the tough digital battlefield as foreseen in the future.

### Scope and types of activities

#### **Scope**

The proposals must address the study and the development of key technologies

---

<sup>107</sup> Size, Weight, and Power.

<sup>108</sup> Development, security and operations concept, which integrates security aspects into every phase of the development life cycle.

supporting the next generation of military integrated modular avionics (NG-MIMA). The proposals should consider multiple military aerial platforms that should operate in a defence air cloud context, both manned and unmanned, including other than fighters.

Use cases analysis and identification of the NG-MIMA key technologies must be addressed and possible future architectures, including possible applicable methodologies and processes, should be described.

In addition, the proposals should include proofs of concept, demonstrations and even prototyping of a selection of the envisioned key technologies to be determined according to the studies to be performed, hence paving the foundations for future development actions in this area. The proposals may consider simulations and model-based system engineering.

In any case, the use of EU and EDF associated countries (Norway) technologies without restrictions from non-associated third countries must be highly prioritised, leveraging on sovereign European technological components, systems and know-how.

The proposals should target at least TRL 4 (component and/or breadboard in laboratory environment) for the key technologies addressed.

### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>109</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (optional)

<sup>109</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

Types of activities (art 10(3) EDF Regulation)		Eligible?
(g)	<b>Qualification</b> <sup>110</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>111</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - perform gap analysis to identify the standardisation needs beyond the international standards already widely used in this domain or beyond ongoing activities conducted at national, multinational or EU level;
  - provide a use case analysis and identification of requirements, including regarding the key technological components identified for possible future architectures for NG-MIMA. This task should consider other related initiatives at national or EU level;
  - provide a list of requirements and KPIs<sup>112</sup> for new generation computing architecture (e.g. performance, low SWaP<sup>113</sup>, cyber resilience, etc.), exploring segregation of military avionics, as well as flexible and hot reconfiguration capabilities;
  - study multi-level computing solutions to be able to run all functions including safety critical and highly demanding computing requirements, such as AI<sup>114</sup>-based functionalities;
  - study certifiable multi-level real-time operating systems oriented to these new levels of manycore computing solutions;
  - study the process, framework and tools required for NG-MIMA.
- Design:
  - include HW<sup>115</sup> and SW<sup>116</sup> architectures and interfaces able to execute not only different levels of safety critical functionality but also mission functionality;
  - include on-board deterministic high-speed data buses and consolidated backwards compatible with legacy ones;

<sup>110</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>111</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

<sup>112</sup> Key Performance Indicators.

<sup>113</sup> Size, Weight and Power.

<sup>114</sup> Artificial intelligence.

<sup>115</sup> Hardware.

<sup>116</sup> Software.

- include high-performance graphics capability for the computing solution and its interfaces;
- include packaging, powering and connecting technology requirements and solutions.

In addition, the proposals must substantiate synergies and complementarity with relevant activities described in the call topic EDF-2021-AIR-D-CAC on *European interoperability standard for collaborative air combat*.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed product and technologies should meet the following functional requirements:

- Multi-functional avionics should:
  - be based on a scalable reference architecture to pave the way for standardisation of interfaces and stacking avionics systems;
  - include high-speed and performing data buses and protocols, including packaging standards;
  - provide the capability regarding high-speed data sharing and regarding assets interoperability throughout the EU as well as with NATO air defence arsenals;
  - include real-time operating system for on-board safety and mission (both critical and non-critical in terms of safety) systems, with multi-level capabilities;
  - include HW and SW complying with multi-safety and multi-mission (both critical and non-critical);
  - be purposely built with a view to comply with security classification with multi-level security segmentation;
  - allow for integration into supportive HW that would facilitate

certification by military authorities in the future (cf. machine learning, in particular deep learning algorithms);

- provide for real-time computation and sharing capability orchestration, e.g. including process, tools and framework to support the development in a multi-industrial workshare and taking into account DevSecOps type of upgrade;
  - provide a high integrity deterministic avionic network with the necessary redundancy to connect various computing nodes and consider solutions when different platforms are engaged;
  - provide a sufficient level of compatibility in order to operate a variety of heterogeneous assets, manned and unmanned, during air operations.
- The system should include data processing and visualisation capability with:
- state-of-the-art high-performance and ad-hoc HW and SW infrastructure, that allows processing, interfaces and visualisation of tactical data in real time.
- The embedded data processing and networking capacity may:
- integrate HW with high data processing, notably through AI applications;
  - provide AI-based functional standard interfaces and system monitoring.

#### Expected impact

The outcome is expected to contribute to:

- significantly reducing the number of computer packages in an aircraft, hence leading to a decreased SWaP;
- the creation of a European ecosystem for next generation integrated modular avionics for defence platforms, hence fostering the development of European technological sovereignty in this area;
- enhancing the ability to trigger modern and faster innovation towards a European air cloud, currently bottlenecked by the absence of a common NG-MIMA concept;
- increasing platform flexibility and modularity with a common open architecture, fostering the use and integration of new disruptive technologies;
- reducing time and costs for iterations of services that require underlying new integrated modular avionics, such as multi-domain mission systems, enhanced collaborative situational awareness and real-time tactical information sharing.

### **EDF-2023-DA-AIR-SPS: Self-protection systems**

#### Objectives

##### **General objective**

The main objective of the next generation self-protection systems (SPS) is to increase survivability of fixed-wing and rotary-wing, combat or non-combat aircraft in hostile environments.

SPS is to face a wide, heterogeneous and evolving spectrum of hostile and directly

threatening systems of surveillance, as well as to prioritise risks in the operational area and select the proper reaction mode through a network of distributed capabilities exploiting sensor nodes of various type inter/intra platforms. It should be reconfigurable depending on the mission and the platform targeted. It should also be able to self-adapt while operating, based on scenario monitoring and mission assets availability.

### ***Specific objective***

When operating in semi-permissive or even non-permissive environments, fixed- and rotary- wing platforms face a large spectrum of hostile systems of surveillance and direct threats, which are continuously improving their technology and effectiveness.

Recent events in Ukraine and Syria clearly call for not neglecting any high intensity scenario and question the current self-protection capabilities of fixed- and rotary-wing, combat and non-combat platforms. Surface-to-air and air-to-air missiles with a wide range of guiding systems (RF<sup>117</sup>, optronics) and a wide range of associated surveillance/warning systems are to be considered, as well as hostile fires and unmanned aerial vehicles (UAV).

The specific objective is to develop an enhanced SPS able to protect against:

- direct threats (e.g. missiles, loitering munition, RPG<sup>118</sup>, etc.);
- indirect threats (e.g. surveillance/acquisition/tracking systems also with Low Probability of Intercept (LPI) radar capability;
- new proliferating types of threats, such as those in the field of loitering munitions, directed energy weapons (DEW) and cyber electromagnetic activity (CEMA) capabilities.

### ***Scope and types of activities***

#### ***Scope***

The proposals must address the design, prototyping and testing of a new generation of integrated self-protection system, designed to protect both fixed- and rotary-wing, combat and non-combat platforms, with very high efficiency, in view of allowing the usage of these platforms for mission accomplishment even in contested airspace.

#### ***Types of activities***

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

<b>Types of activities</b> (art 10(3) EDF Regulation)		<b>Eligible?</b>
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No

<sup>117</sup> Radiofrequency

<sup>118</sup> Rocket-propelled grenade.

Types of activities (art 10(3) EDF Regulation)		Eligible?
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>119</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>120</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>121</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- design of a detailed self-protection system (Critical Design Review - CDR);
- prototyping and testing (on board of existing end-user platforms) of a self-protection system modular version, integrating sensors and effectors of sufficient technological maturity (e.g. full wideband digital radar warning receiver, multispectral threat warner);
- testing to be conducted either on a large and fixed wing aircraft or on a medium size helicopter in order to demonstrate:
  - versatility of the system architecture on fixed- and rotary-wing assets;
  - ability of the proposed system to meet the high-level requirements as jointly agreed by the supporting Member States and EDF associated countries (Norway);

<sup>119</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>120</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>121</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- feasibility of collaborative self-protection capability allowing the exchange of data with cooperative platforms, to perform sensing and jamming, in order to achieve better performances than a stand-alone platform, taking into consideration the possible level of classification of such data;
- technical maturation of lower technological readiness level (TRL) sensors and effectors, leading to at least TRL 7.

In addition, the proposals must substantiate synergies and complementarity with activities described in the call topic EDIDP-ACC-SPS-2020 *Self-protection systems for fixed and rotary wing aircraft*.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed product and technologies should meet the following functional requirements:

1) The system should:

- be designed to equip both fixed-wing and rotary-wing aircraft with appropriate modularity to cope with specific threat list/platform signature/platform kinematics/platform installation and integration constraints;
- be based on an open architecture and international standards widely used in this domain (hardware interfaces, software interfaces, protocols and communication links);
- protect its own sensitive data and software (e.g. from cyberattacks);
- embed compatibility management features to ensure compatibility with other emitters and receivers on board the platform and/or other aircraft involved in a mission;
- have ways to remove any doubt concerning the source of the alleged hostile system, before alerting the crew;
- provide for, but not limited to, an automatic mode elaborating suggested



countermeasures, including coordinated countermeasures (e.g. manoeuvres, expendables and jamming) that can be implemented without a man in the loop if automatic mode is selected;

- be compatible with new-generation platform systems architecture (e.g. next generation rotorcraft, future mid-size tactical cargo) and legacy platforms.

2) Regarding protection against direct threats, the system should:

- detect that the aircraft or other aircraft they are flying with, are being engaged by direct threats and provide warning to the mission and/or avionics systems of the aircraft;
- protect the aircraft from direct threats providing identification of such direct threats and elaborating the appropriate coordinate countermeasures;
- provide features to counter the direct threats elaborating the most appropriate combination of countermeasures (e.g. expendables, jamming, directed energy weapon and manoeuvres);
- detect incoming threats, perform classification and suggest optimal combination of reactions in terms of countermeasures and escape manoeuvres considering assets available on the single platform and considering the availability of collaborative platforms;
- gather intelligence regarding the direct threats characteristics and fire posts locations and be able to detect changes in those characteristics and locations;
- classify threats, to support sensor system behaviour in complex, congested, cluttered, contested, connected and constrained operational electromagnetic environment.

3) Regarding indirect threat detection and protection, the system should:

- gather and record indications that the aircraft or other aircraft they are flying with, are detected by any hostile surveillance systems and provide warning through the mission and/or avionics systems of the aircraft;
- detect that the aircraft or other aircraft of the group are being tracked by any hostile systems and provide warning to the mission and/or avionics systems of the aircraft;
- provide features to disturb the detection and tracking by both passive and active surveillance systems of the enemy;
- suggest, considering the availability of collaborative platforms, the optimal combination of disturbances to interrupt the acquisition chain of enemy sensors;
- gather intelligence regarding indirect threats characteristics and locations and be able to detect differences with expected Electronic Order of Battle (EOB) or changes with reference to previously recorded EOB;
- perform collaborative self-protection with the ability to share collected information with cooperative platforms in networked operations, exchanging ESM<sup>122</sup> and ECM<sup>123</sup> data with other platforms to achieve a faster and more

---

<sup>122</sup> Electronics Support Measures.

<sup>123</sup> Electronic Countermeasures.

accurate operational situational awareness than with a single platform, taking into account the possible level of classification of such data;

- classify indirect threats during the development of the system, to support sensor system behaviour in complex environment.

### Expected impact

With reference to currently available self-protection systems, the outcome is expected to contribute to:

- increasing coverage in term of threat types (e.g. new generation seekers, multiple homing threats, networked LPI radar systems, new generation directed energy weapons and loitering munitions, hostile fires/small calibre, RPG);
- ensuring EU autonomy in the survivability capability;
- versatility by covering a wide range of platforms and saving costs in integration, installation and maintenance, as well as specific development through modular design.

## **EDF-2023-DA-AIRDEF-CUAS: Counter unmanned aerial systems**

### Objectives

#### **General objective**

Unmanned aerial system (UAS), including cheap commercial off-the-shelf (COTS) and easy to assemble UAS components are widely available and their popularity is even growing. Traditional surveillance systems often fail to cope with these flying objects because of their characteristics. Indeed their low speed make them challenging to detect with conventional radars. Their low altitude allows them to hide amongst trees or behind natural or artificial obstacles, and their very small radio-frequency (RF)/radar cross-section (RCS), as well as their thermal and acoustic signatures make them difficult to detect. Additionally the high manoeuvrability of some machines makes their movement hard to track once detected, and their increasing on-board processing capabilities (e.g. automated and vision-based navigation, use of artificial intelligence) makes them more resilient to some counter-UAS (C-UAS) systems that rely on RF detection and jamming.

In addition, current C-UAS technology is largely ineffective against military grade UAS (such as loitering munitions), swarms and flocks of drones and threats that may emerge in the short to medium term, also considering that the use of cellular networks (4G, 5G or beyond) will increase the speed, stability and immediacy of intercommunication between aircraft and control stations. Moreover, while some systems may be effective against a variety of UAS threats, the costs of engagement may be prohibitive to counter large-scale attacks.

#### **Specific objective**

The specific objective of this topic is to:

- tackle safety and security concerns (e.g. malevolent users attempting deliberately hostile missions such as the use of explosive payloads, ISR<sup>124</sup>);
- consider the various threats in their environmental and operational context as

---

<sup>124</sup> Intelligence, Surveillance, Reconnaissance

mitigation options may vary from different scenarios (e.g. depending on the size of the area to protect, the value of the unit to protect, the reaction time required and the need to minimise fratricide and collateral damages);

- provide a suite of solutions to comply with a broad set of rules of engagement (ROEs), each adapted to the surrounding environment and the operational scenarios (including the transition from peace-time to war-time), including from a sensing perspective;
- cover fixed (i.e. continuous protection of Forward Operating Bases (FOB), critical infrastructures, 24/7, at reasonable operational and maintenance costs), deployed (i.e. quick deployment with minimum logistic support, as well as rapid integration of additional sensors and effectors within a recognised open architecture, for tactical military activities as well as civil events) and mobile (i.e. protection of mobile units/elements) applications;
- include a set of various C-UAS capabilities, such as navigation systems spoofing, RF jamming, kinetic effectors (soft/hard with lethal or non-lethal effects), catch or hit-to-kill by a swarm subset or direct energy weapons (e.g. high-power lasers and/or microwaves);
- improve identification and classification capabilities of the system.

### Scope and types of activities

#### **Scope**

The proposals must address the development of a C-UAS system, from a detailed design (i.e. critical design review) up to a system prototype to be tested and qualified in relevant defence operational scenarios, demonstrating its ability to:

- with a selection of passive and active sensors, detect, track, classify, identify, support decision making and counter class I<sup>125</sup> UAS (single and/or multi-UAS) through an optimal selection and activation of relevant effectors using multiple technologies;
- ensure effective protection of critical defence infrastructure, installations and assets;
- operate with limited impact on existing communications or position and navigation infrastructures.

In addition, the proposals may address other operational scenarios, if deemed relevant.

#### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

---

<sup>125</sup> Cf. Classification referred to in NATO STANAG 4670 Minimum training requirements for unmanned aircraft systems (UAS) operators and pilots

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>126</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>127</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	<b>Certification</b> <sup>128</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory qualification activities:

- the proposals must address the qualification of the prototype to be developed, based on use cases jointly agreed by the supporting Member States and EDF associated countries (Norway);
- in particular, the proposals must address the provision of drawings, reports, analyses, certification plan and data in view of future certification of the system by the supporting Member States and EDF associated countries (Norway) authorities.

In addition, the proposals must substantiate synergies and complementarity with activities described in the call topic EDIDP-CUAS-2020 *Counter Unmanned Air*

<sup>126</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>127</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>128</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

### *Systems (UASs) capabilities.*

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed product and technologies should meet the following functional requirements:

1) The C-UAS system should include battlefield management features, providing for the following capabilities:

- ensure effectiveness of the protection of moving units and assets (e.g. ground formations, convoys, ships located in the vicinity of a harbour or coastal patrolling);
- facilitate the interaction of C-UAS system with security and defence systems for fixed, deployed and mobile assets;
- consider non-static, effector-dependent danger areas in order to reduce risk of blue-on-blue or collateral damage, when protecting groups of moving objects (e.g. convoys, formations);
- ensure robustness and high availability, without being saturated in case of multiple threats (i.e. either single or multiple UAS units, either uncoordinated or operating as a team or as a single system, including swarms);
- provide an extended range of operational performances (e.g. extended ranges for surveillance, detection, identification and neutralisation) to face possible improvements of UAS threats;
- require minimum operator effort for decision making;
- neutralise the threat with focus on semi-autonomous (or even manual) technical solutions (HITL);
- in critical scenarios, where extremely high tempo and/or high threat volume prohibit the use of human sound judgement, provide options for temporarily

allowing automatic C-UAS engagements with specified effectors in defined areas, within the LOAC<sup>129</sup> and relevant ROE;

- offer all-weather, 24/7 operational capability, in a wide variety of climate conditions;
- provide simulation and training features in realistic scenarios;
- provide real-time playback functions for mission analysis, training and other purposes;
- require limited logistic support for deployment and maintenance.

2) Regarding command and control (C2), the C-UAS system should be able to:

- plan and monitor subsystems missions and conditions;
- merge information from heterogeneous sensors;
- report about any internal or external elements that could affect the system performances;
- evaluate the possible engagement approaches to the operator, coordinate the engagement approach selected by the operator and report on the resulting outcomes;
- balance the autonomous processing of information across the adopted sensors and timely report to a central Battle Management/C2 system in order to reduce operational manpower load and bottlenecks;
- generate, disseminate and update real-time operational picture and alerts;
- integrate multilayer C2 system with cross-security-domain approach;
- allow subsystems dynamic deployment and multi-instance integration;
- provide a range of selective engagement and mitigation alternatives with the ability to evaluate mission success probabilities and potential resulting drawbacks;
- compute success probability, time to complete the neutralisation and drawback probabilities, depending on the characteristics of the effectors, for each of the possible neutralisation approaches;
- integrate and connect all the sensors and the effectors in a local C2 station;
- implement data fusion and automatic procedures and rules in order to focus human operations on action, resources coordination and cooperation. A user-friendly interface should be provided.

3) Regarding sensors, C-UAS should:

- enable omnidirectional detection (e.g. rotating or staring) while also being capable of limiting the detection to a sector of choice;
- include the capability of detection for non-cooperative UAS, including autonomous, in the suite of sensors, as well as various technologies for

---

<sup>129</sup> Law of Armed Conflict

detection and tracking (e.g. EO<sup>130</sup>/IR<sup>131</sup>, RF<sup>132</sup>, acoustic);

- provide dynamic scalability of sensors and effectors using communication protocols that allow plug-and-play deployment.

4) In terms of data and information processing, the proposed solution should:

- enable machine learning to allow using recorded signals or signatures in order to enhance the performance of target recognition and identification;
- integrate, process and display different information sources for classification/identification (e.g. sensors information, ACO<sup>133</sup>, civil UTM/ATM<sup>134</sup> information...).

5) In terms of interfaces and interoperability, the C-UAS system should:

- be based on an open, flexible, modular and scalable architecture based on a plug-and-play component approach which allows deployment of specific configurations adapted to the threat scenarios;
- provide standard interfaces and interoperability with relevant foreseen UAS systems (e.g. U-space<sup>135</sup>) and higher air defence C2 elements or other units.

### Expected impact

The outcome should contribute to:

- consolidating and validating doctrine and CONOPS<sup>136</sup> in the field of C-UAS;
- developing a comprehensive C-UAS capability for the EU and EDF associated countries;
- reducing the minimum reaction time compared with current systems;
- enhancing situation awareness and protection of critical areas and strategic assets;
- ensuring interoperability with existing security and defence systems in order to easily adapt to current monitoring systems;
- further increasing the effectiveness of C-UAS technologies/systems to be able to better counter the current and future UAS threat (including the use of MOTS<sup>137</sup> UAS and swarms).

## **EDF-2023-DA-GROUND-MBT: Main battle tank platform systems**

### Objectives

#### **General objective**

Main Battle Tanks (MBT) remain a pivotal element of land military manoeuvre,

---

<sup>130</sup> Electro-optical.

<sup>131</sup> Infrared.

<sup>132</sup> Radio-frequency.

<sup>133</sup> Airspace control order.

<sup>134</sup> Unmanned Aerial Traffic Management/Air Traffic Management.

<sup>135</sup> Set of services and procedures to support safe, efficient and secure access to airspace for Unmanned Aircraft Systems (UAS).

<sup>136</sup> Concept of operations.

<sup>137</sup> Modified Off-The-Shelf.

especially in a conventional warfare context, thanks to their unique combination of protection, mobility, and firepower. Nonetheless, MBTs currently numbered in the fleet inventories of the EU Member States and EDF associated countries (Norway) are either ageing or obsolete and, therefore, the latter face the compelling need to modernise their in-service platforms and replace those of them approaching the end of their operational life. Against this background, the upgrade of current and development of future main battle tank technologies capable of outstanding operational effectiveness and mission success in all possible future scenarios are highly necessary.

### ***Specific objective***

To this end, it is of key importance for future European MBT systems to:

- be designed to operate in all environments, including urban and symmetrical high intensity warfare, counter peer or near peer and asymmetrical threats, by operating dispersed in the context of multi-dimensional operations;
- have a higher level of protection, enhanced stealth capability, enhanced survivability in all environments against symmetric and asymmetric threats, and resilience against cyber- and electronic warfare-attacks;
- have a higher capability of detecting and identifying threats at greater distances;
- be operated by a smaller crew, compared to present/today's designs, allowing the system to be lighter, more compact, and agile;
- be equipped with advanced command and control system that supports the crew with situational awareness, target acquisition, target engagements, target handover, battle space management, data- and information sharing;
- be able to cooperate with adjacent manned and unmanned robotic assets;
- rely on a superior firepower to engage and win symmetrical duels, as well as to conduct urban and asymmetrical operations successfully;
- rely on advanced mobility (e.g. higher speed, better manoeuvrability in all terrains, new operating modes such as silent mode), a lower fuel consumption, greater operational range and autonomy, and supply the increased electric demand of on-board equipment and weapons;
- be prepared to be operated unmanned in the future.

### ***Scope and types of activities***

#### ***Scope***

The proposals must address studies and design for the upgrade of current and development of future main battle tank technologies, including enabling and green technologies, leading to a system level, capable of outstanding operational effectiveness and mission success in all possible future scenarios. Furthermore, the proposals must take into account aspects such as mobility, deployability, autonomy, firepower, protection and cybersecurity.

#### ***Types of activities***

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):



Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>138</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	<b>Qualification</b> <sup>139</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>140</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - Assist supporting Member States and EDF associated countries (Norway) in the definition of the Concept of Operation (CONOPS), feasibility study and architecture definition;
  - System Specification (SSS<sup>141</sup> and SSDD<sup>142</sup>) providing a detailed system and sub-systems description;
  - System Requirement Review (SRR).

<sup>138</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>139</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>140</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

<sup>141</sup> System/Sub-system Specification.

<sup>142</sup> System/Sub-system Design Description.

- Design:
  - Preliminary Design Review (PDR).

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed activities should focus at least on a subset of functions for MBT (e.g. among mobility, energy, observation, protection, human-machine interaction and/or firepower) and meet the following functional requirements:

- be capable of performing its missions by day, night and in adverse weather conditions, in worldwide crisis/war scenarios, with the minimum possible degradation of performance due to extreme environmental conditions and types of terrains, as defined in the relevant standards. Operations in Chemical, Biological, Radiological and Nuclear (CBRN) conditions should be considered in the design too;
- feature a maximum speed of at least 80km/h on paved roads, at least 50km/h on smooth and rugged terrain (apart of paved roads) and an operational range of not less than 600km averaged on different types of terrains;
- feature a wading depth without preparation > 1.20m, a wading depth with snorkel > 5.00m, a trench crossing capability > 3.00m and a climbing capability > 1.10m;
- feature a high operational availability to be capable to perform the assigned mission in at least 85% of calls to duty;
- provide direct firepower to engage modern MBT at greater distances with precise “fire-on-the move” capability than current systems;
- provide firepower to engage modern MBT under BLOS conditions;
- support smart/programmable ammunition;
- automatic threat detection, identification and tracking, including ability to handle multiple threats, and target distribution across the military network

enabling sensor-to-effector allocation;

- real-time and unified information and data presentation, provided by the sensors deployed on the platform and from external networks with low latency times;
- advanced Positioning, Navigation and Timing (PNT) system in order to ensure trusted PNT for the platform even in challenging GNSS<sup>143</sup> contested and denied environment;
- feature a low detectability and electromagnetic signature e.g. ultraviolet (UV), visible, infrared (IR) (from Short-Wavelength Infrared (SWIR) to Long-Wavelength Infrared (LWIR)), radar, laser, and acoustic. Detection and signature recognition by multi- and hyperspectral sensors are also to be considered;
- feature an optimised trade-off between mobility, firepower, and protection;
- provide protection against the following threats: mines and Improvised Explosive Device (IED), Rocket Propelled Grenades (RPG) (including those with a functionality like RPG-30), "High Explosive Anti-Tank" (HEAT) munitions, "Anti-Tank Guided Missile" (ATGM; including 3<sup>rd</sup> generation ATGM with high angle of attack), loitering ammunition and Unmanned Aerial Systems (UAS), Electronic Warfare (EW) and cyber-attacks, and at least 125mm "Armour Piercing Fin Stabilised Discharging Sabot" (APFSDS) and other direct threats likely to become known over the whole duration of the project;
- feature an Active Protection System (APS) capable to counter direct threats, including ATGM and APFSDS (125mm) ammunition, also with the aim to reduce weight of passive and reactive armour;
- feature sophisticated counter-UAS (C-UAS) / counter-swarm capabilities to perform platform protection;
- be capable of reducing the reliance on fossil fuel, foster reduction of dependency on combustion engines by means of electrical or alternative propulsion systems (e.g. by using hybrid engines) and take into account other aspects of green technologies (e.g. total life CO<sub>2</sub> footprint, use of other materials, recycling);
- operate in silent mode and extended silent watch with low thermal signature;
- store and supply high density and power of electric energy for sensors, effectors and weapons;
- not exceed for the complete vehicle (i.e., hull and turret), in full combat order, the following maximum acceptable weight and overall dimensions: 70 tons, 2.5m (H) - 10.0m (L) - 3.8m (W) - 0.55m (ground clearance) meters (hull length: 7.0m);
- meet transportability requirements and constraints due to EU Member States and EDF associated countries (Norway) roads, railways, tunnels and bridges; air transportability/drop should also be taken into account;
- a range between 5% and 10% of growth potential without changing the assigned power/weight ratio;

---

<sup>143</sup> Global Navigation Satellite System.

- ensuring interoperability with unmanned ground platforms and Manned-Unmanned Teaming (MUM-T) with adequate Level of interoperability (LOI), and interoperability with UAS;
- be equipped with technologies for enhanced Situational Awareness (SA), e.g. advanced display devices, “transparent armour” concepts, allowing visualisation of the environment around the vehicle, automatic surveillance, detection, reconnaissance, and identification;
- advanced 360° SA and decision-making systems to integrate, correlate and fuse video and data from the available sensors in the platform to provide an enhanced SA augmented reality picture of the environment of the vehicle and support the decision-making process through multimodal human-machine interfaces combining textual, vocal, acoustic, haptics, 2D and/or 3D visual information, and augmented / virtual reality devices. The system data and image processing include search and tracking, and object recognition;
- decision-making assistance: advanced crew information presentation capabilities including smart synthesis, prioritisation, and filtering, to keep the most relevant items, especially in the context of reduced crews;
- crew environment and support architectures should be adaptive, open and modular to enable the introduction of innovative technologies as soon as they become mature;
- be operated by a crew of not more than three;
- feature static or dynamic on-board simulation for training (embedded);
- reduced lifecycle costs compared to current MBT;
- be designed with crew comfort and ergonomics in mind;
- be able to perform battle damage assessment without compromising survivability;
- integrable and interoperable with a family of similar support platforms (system of systems);
- compliance with NATO requirements and standards.

### Expected impact

The outcome should contribute to:

- the defence and security interests of the EU and its Member States;
- the EU level of ambition in terms of strategic autonomy;
- EU resilience and technological sovereignty;
- EU industrial autonomy;
- excellence with the demonstration of a significant advantage over existing products or technologies.

## **EDF-2023-DA-GROUND-IFS: Long-range indirect fire support capabilities for precision and high efficiency strikes**

### Objectives

#### **General objective**

The increasingly complex geopolitical instability faced by the European Union, its Member States and EDF associated countries (Norway) requires continuous and unfragmented responses. To that purpose, the EDF promotes and contributes to the strategic autonomy and sovereignty of its Member States and EDF associated countries (Norway).

Considering the ongoing geopolitical situation, the objective of this study is to develop European solutions for 155mm (up to 52-calibre) and rocket artilleries adapted to the new threats by increasing the fire range compared to current systems while maintaining interoperability principle. The targeted solutions must be cost-driven based on the assumption of a symmetric high intensity battle.

#### **Specific objective**

Future capability and operational challenges in artillery require enhanced interoperability, agility, action range, accuracy, survivability, and security as well as ability to operate in adverse conditions and to obtain scalable effects while ensuring efficient maintainability, high level of operational readiness, and optimised life cycle cost. In this context and during the next coming years, the future generation of 155mm artillery projectiles and rockets (timeframe 2030) will be subject to numerous potential game-changing technologies, which are expected to enhance capabilities significantly.

The proposals must stimulate cross-border cooperation within the EU and with EDF associated countries and ensure the security of supply and strategic autonomy in a longer-term perspective.

The main objectives of this topic are to address challenges regarding precision, range (155mm shell: 80km with a minimum range of 50km; rocket: at least 150km), terminal effect and operation in stressful environment like GNSS-denied battlefield.

### Scope and types of activities

#### **Scope**

The proposals must address:

- a study of range-extending technologies;
- a parametric study of long range artillery ammunition requirements regarding further range increase, with identification of the compatibility between studied technologies and these future ammunitions, and identification of technological development roadmaps;
- the modular design of the major technologies including 155mm (up to 52-calibre) long range cargo ammunition;
- the prototyping of sub-systems.

#### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>144</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	<b>Qualification</b> <sup>145</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>146</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Study of sub-systems (in particular the propulsion sub-system) of 155mm (up to 52-calibre) artillery ammunition adapted to the existing European artillery guns. This study must include:
  - the parametric study of long range artillery ammunition requirements and limits (in terms of mass, propulsion, etc.) regarding further range increase (beyond the technologies to be designed and prototyped under this call topic), considering both current 155mm (up to 52-calibre) and future artillery guns (e.g. increase of the barrel length and chamber volume). In order to optimise further developments, this study should also include identification of the compatibility between studied

<sup>144</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>145</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>146</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

technologies and these future ammunitions, and the identification of technological development roadmaps;

- the provision of a roadmap for subsequent phases (e.g. qualification phase, anticipation of product optimisation during life cycle).
- Design:
  - design at sub-system level.
- System prototyping:
  - prototyping at sub-system level.

The proposals must substantiate synergies and complementarity with foreseen, ongoing, or completed R&D activities, notably those performed or envisaged in the context of EDF and its precursor programmes (e.g. EDIDP-NGPSC-PGA-2020 and EDIDP-NGPSC-LRIF-2020).

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement

and

  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposals should meet the following functional requirements:

- Modularity and interoperability:
  - interoperability between EU Member States, EDF associated countries (Norway) and NATO. Especially, the 155mm ammunition should be compliant with the Artillery JB MOU<sup>147</sup> and be testable in a proven 155mm (up to 52-calibre) artillery;
  - both rocket and 155mm (up to 52-calibre) ammunition should be developed following a modular approach (Canard Actuation System / Fin Actuation System, aerodynamic skeleton, seeker, etc.), with interface specifications and validation;

---

<sup>147</sup> NATO Joint Ballistics Memorandum of Understanding (JBMou).

- the ammunition should have a range of around 80km for the 155mm shell and at least 150km for the rocket. The minimum range for the 155mm shell is 50km but at least 60km should be pursued;
- the ammunition should provide a terminal effect with a metric precision below 10m (CEP@50) range, in all weather conditions and in a GNSS contested environment;
- terminal effect: the ammunition should integrate a high payload warhead that should be effective against soft targets, light vehicles, small building with the ability to attack the enemy (high pay-off targets) in depth, to strike a counter-fire. Accordingly, warhead and terminal effect should be optimised (scalable effect depending on target objectives); the use of insensitive explosive (HE IM<sup>148</sup>, MURAT 1\*<sup>149</sup>) is requested, as far as possible. When not possible, this has to be justified;
- the ammunition guidance and navigation should be GPS and Galileo compatible, without creating any restriction of use to EU Member States and EDF associated countries (Norway);
- the ammunition safety of use should be as high as possible, as per the best standards related to life duration and insensitiveness to aggressions. Compliance with NATO STANAG 4439 (related to insensitive munition) and STANAG 4187 (related to safety) is expected;
- the ammunition should be programmable to realise the mission, with minimum interference with the gun system;
- an integrated in-flight re-targeting capability (including mission change and/or a mission abort) should be assessed for the different categories of ammunition;
- terminal guidance should be affordable and effective against moving and stationary targets;
- terminal phase characteristics (i.e. fuse and warhead architecture) should be determined according to the kind of effect considered. Typical options for activation are impact, delayed impact (also against reinforced infrastructure, bunkers, etc.) and predefined altitude;
- high survivability against modern air defence systems;
- the ammunition should present a high robustness against jamming.
- The ammunition should consider storage constraints:
  - The ammunition availability should consider operational needs taking into account storage constraints due to the frequency of use of such type of projectiles (ammunition still effective within a 15-year duration to be compliant with other types of ammunition) with particular attention to:
    - increased capacity of power supply;
    - the robustness of the supply chain.

<sup>148</sup> High explosive insensitive munition.

<sup>149</sup> 1 star marked « Munitions à risques atténués ».



- The propellant charges should be studied with the intention of reducing wear, limiting dispersion and yet with increased firing distances.
- Performances should be achieved without modifying the requirement of existing European artillery rocket launchers and 155mm (up to 52-calibre) artillery guns.
- Every technology and component developed to address the above challenge should be capable of being integrated into an artillery rocket. Therefore, technical specifications at all stages should encompass the two categories of ammunition. It is expected that the stress put on compactness and resistance to the extreme thermo-mechanical environment of a 155mm artillery shell will enable technologies and components to withstand the environment of an artillery rocket as well.
- The modular architecture should allow, through flexibility and, if needed, specific subsystems, ammunition compatibility between EU Member States, EDF associated countries (Norway) and NATO countries and especially with existing European artillery rocket launchers and 155mm (up to 52-calibre) artillery guns.

### Expected impact

The outcome should contribute to:

- EU strategic autonomy;
- European technological sovereignty;
- the reinforcement of innovation on key capabilities;
- strengthening the European Defence Technological and Industrial Base (EDTIB);
- increasing interoperability and developing potential European standards.

## **EDF-2023-DA-NAVAL-MMPC: Modular and multirole patrol corvette**

### Objectives

#### **General objective**

Naval combat platforms and systems are essential assets to ensure maritime surveillance and presence at sea where needed with deterrent effect to grant maritime security, the respect of International Maritime Law, the defence of the sea lines of communications, and protect the interests of the EU, its Member States and EDF associated countries (Norway).

The main objective of this topic is to generate a new multirole and modular “second line class of vessels”<sup>150</sup>, able to increase current EU Member States and EDF associated countries (Norway) navies’ interoperability and capabilities mainly in terms of maritime situational awareness, surface superiority and power projection. Such units are due to carry out a large spectrum of naval operations ranging from peacetime and crisis time actions up to wartime operations.

The ambition is to drastically increase the flexibility and cost-effectiveness of that class of vessels, based on a reference core ship (baseline), while addressing the

---

<sup>150</sup> Limited Warship Unit according to NATO terminology.

common requirements of the supporting Member States and EDF associated countries (Norway), and the specific requirements of their variants.

### ***Specific objective***

The goal of this topic is to pursue the work already addressed in the EDF 2021 work programme under the call topic *multirole and modular offshore patrol vessel* (EDF-2021-NAVAL-D) aiming, this time, to complete the Critical Design Review (CDR), and start the development phase with the production of, at least, the platforms of several variants as prototypes and, at least, one per version.

The proposals should leverage the progress made in the context of the above-mentioned action aiming in particular, at building and structuring a common industrial working environment, and studying and reaching an initial design of the common baseline of the vessel.

Two different versions are considered:

- Full Combat Multipurpose (FCM) corvette equipped with a variety of systems to ensure adequate self-defence in all warfare scenarios and capable of integrating specific additional capabilities based on modular configurations;
- Long Range Multipurpose (LRM) corvette, with an extended endurance (compared with FCM) and equipped with a variety of systems to ensure adequate self-defence in specific warfare scenarios and capable of integrating specific additional capabilities based on modular configurations.

The main result should be the design of the two above-mentioned versions based on a common mono hull platform (reference core ship), and the integration of a combat system, specific for each variant, to enable the prototyping and testing activities.

### ***Scope and types of activities***

#### ***Scope***

The proposals must aim, based on the work addressed in the EDF 2021 work programme under the call topic *multirole and modular offshore patrol vessel* (EDF-2021-NAVAL-D), to:

- implement, maximise and strengthen the progress made in the context of the preceding above-mentioned action, in terms of common rules and standards;
- reach a mature and detailed design for each variant based on a common baseline (reference core ship) of this innovative class of warship to address the common requirements of the supporting Member States and EDF associated countries (Norway);
- provide digital models of the reference core ship and the two versions (FCM and LRM) with the possibility to add specific variants;
- develop, at least, the platforms of several variants as prototypes and, at least, one per version;
- perform initial trials and testing activities related to each prototype.

#### ***Types of activities***

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>151</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	<b>Qualification</b> <sup>152</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>153</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Studies:
  - technical feasibility studies, if needed, to complete the initial design of the common platform;
  - technical feasibility studies related to the integration of the respective combat system including, but not limited to, sensors, processing and effectors, considering physical, combat management, and command and control perspectives in a multi-domain interoperability scenario, while designing a reference core ship as wide as possible;

<sup>151</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>152</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>153</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- industrial plan, encompassing the full production strategy for all variants.
- Design:
  - integration in the ship design of the technological bricks selected by supporting Member States and EDF associated countries (Norway);
  - detailed design of the reference core ship, platform and combat system integration, addressing the common requirements of the supporting Member States and EDF associated countries (Norway);
  - definition and detailed design of the two versions and specific variants in order to fulfil the needs and requirements of the supporting Member States and EDF associated countries (Norway). These designs will be completed to enable the production of FoCs<sup>154</sup> of each variant within the class of vessel;
  - design of the prototypes;
  - digital model of the variants.
- System prototyping:
  - produce, at least, the platforms of several variants as prototypes and, at least, one per version.
- Testing:
  - of components and system integration of the reference core ship;
  - initial trials of prototypes in harbour and, desirably, at sea.

The proposals may also cover the following tasks:

- Qualification:
  - qualification of the design of the reference core ship in its two versions to ensure consistency with the requirements of the supporting Member States and EDF associated countries (Norway).
- Certification:
  - certification activities of the detailed design of the reference core ship.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurement

---

<sup>154</sup> First-of-Class.

and

- based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposed developments for the reference core ship and its variants should meet the following functional requirements:

- the collection and analysis (technical-operational and value analysis) of each end-user's operational requirements (CONEMP<sup>155</sup>) to define the needs, including the ones related to the integration of the combat systems for all the variants;
- the demonstration of the completion of a detailed design and the integration of the relevant ship elements including the respective combat system through, for example, the production of technical documentation, drawings, or 3D digital models;
- the detailed design should be approved by classification societies;
- based on the designed reference core ship as a common baseline for the class of vessel, the differences between variants should be minimised as much as possible through innovative solutions like, for instance, the use of flexible areas and modular architectures. As well, in order to increase commonality between variants and to reduce non-recurring costs, the on-board systems should have, as much as technical and economically feasible, standardised functional and physical interfaces, with indication of buffer tolerances in terms of weight, dimensions and features for embarking specific systems or equipment;
- the physical and functional interfaces should be compliant with standards widely used in the naval domain (e.g. NATO STANAGS);
- provide advanced Human Machine Interfaces (HMI) supporting the operators in all their operational, technical and training tasks;
- green aspects should be properly considered to minimise the environmental impact (e.g. reduced global gas emissions, waste disposal) and be compliant with the requirements of most advanced legislation on environmental protection and prevention of pollution from ships.

The platform should:

- integrate innovative solutions, technologies or systems to enhance efficiency and the capabilities of the vessel at sea;
- provide an overall expected displacement of around 3 000 tons, with a draft enabling the ship to operate from minor/tender ports;
- provide a design able to integrate different combat systems for the different variants.

---

<sup>155</sup> Concept of Employment.

The integration of the combat systems should:

- be based on definition of common interfaces, when possible, between the platform and the combat system of the different variants;
- give due consideration to cybersecurity aspects;
- aim to optimise design, production and in service support costs;
- be able to easily integrate additional capabilities, manage weapon system configurations, interface with external systems through standardisation, and favour reconfiguration and continuous modernisation throughout the ship life-cycle;
- embrace the integration of different unmanned vehicles through standardised systems providing interfaces for sharing information in a collaborative way and based on standards widely used in the naval domain (e.g. STANAG 4817 on Multi-Domain Control System);
- enable the integration of systems to collect and manage information coming from local sensors, cooperative sources and, when applicable, non-cooperative sources.

#### Expected impact

The outcome should contribute to:

- a joint procurement of a cutting-edge modular and multirole patrol corvette class;
- a widened level of communality, interoperability and standardisation of the variants, maximising their integration at fleet level;
- strengthening the European industrial ecosystem by means of common methods, standards, rules and interfaces;
- enhancing the EU naval sector competitiveness, innovation, efficiency and technological autonomy, while promoting a wider cross-border cooperation in particular as regards SMEs and mid-caps;
- reinforcing trust as regards security of supply in the naval sector by shaping an initial nucleus of a truly European supply chain;
- the EU Green Deal and climate objectives.

### **EDF-2023-DA-UWW-ASW: Unmanned anti-submarine and seabed warfare**

#### Objectives

##### **General objective**

The resurgence of high intensity conflicts at the borders of the European Union, combined with new technologies and hybrid threats, is calling the EU, its Member States and EDF associated countries (Norway) to action. The vulnerability of critical maritime infrastructure, such as undersea cables and pipelines, requires resolute measures to ensure its safety and resilience.

The underwater domain (including the seabed and critical maritime infrastructure) is particularly prone to threats as it is largely unmonitored, uncontrolled and concealed. There is a need to perform an increasing number of operations at the same time to

face new generation of silent submarines and drones against the wide array of threats. Current solutions are not sufficient or efficient to deal with these new forms of threats. Unmanned systems are estimated to be the backbone of future solutions enabling European navies to deal with numerous simultaneous missions in larger areas of operations.

### ***Specific objective***

The specific objective of this topic is to develop and assess, in a real environment, unmanned platforms and other new assets along with traditional platforms to manage efficiently anti-submarine warfare (ASW) and seabed warfare (SBW) operations to face current and future threats in the new security context.

The aim is to progress in the ASW and SBW with unmanned systems beyond a concept phase to develop and test models or prototypes of UxVs (UAVs, USVs, UUVs, and other unmanned systems) with payloads which will enable ASW and SBW missions. The solution is expected to contribute to and enable an open and agile maritime warfare architecture. The aim is to reach at least a maturity level equivalent to technology readiness level 6 (TRL 6) on at least sub-system level. Higher technology readiness level in the prototyping phase and maturity towards a foreseeable system integration with open architecture are encouraged.

### ***Scope and types of activities***

#### ***Scope***

The proposals must address design, testing and prototyping activities through sea demonstrations of next-generation underwater warfare solutions.

The proposals should contribute to new ASW and SBW concepts and may leverage civil R&D results (synergies through spin-ins). The proposals should build on a System-of-Systems (SoS) approach that allows adaptations and additions beyond the proposed solution without manufacturer-specific restrictions. The proposals should consider collaborative ASW and SBW capabilities that are based on manned and unmanned assets, in a highly scalable and heterogeneous communication and information network with self-x-properties. Design and prototyping should include relevant simulations.

The areas concerned for development and improvement, and that must be addressed by the proposals are the following:

- new ASW and SBW concepts;
- detection, classification, identification, and tracking of underwater threats in demanding conditions (such as deep and very shallow waters, challenging seabed topography, and noisy environment);
- collaborative, all-node, all-payload, manned-unmanned teaming, including the necessary command, control (C2), and communication (C3);
- decision support for ASW and SBW operations and their enabling systems;
- enabling neutralisation of underwater threats.

Proposed solutions that address these areas should consider some or all of the following features:

- collaborative sensor systems concepts with enhanced capabilities for detection, classification, localisation and tracking of low signature underwater targets;

- UxVs with collaborative behaviour for improved performance in ASW and SBW operations;
- means for monitoring critical infrastructure;
- improving UxVs with, for example, enhanced seaworthiness, energy autonomy, decision autonomy, GNSS-independent navigation and automated payload processing;
- neutralisation solutions for emerging underwater threats, such as UxV:s and swarms;
- new and enhanced self-protection solutions, such as extended anti-torpedo protection using for example decoying or jamming solutions;
- mission autonomy of different degrees with partial or total remote or on-board processing;
- combat system architecture and associated applications (such as mission planning, mission management, situational awareness, tactical aid) for reduced human workload, enabling operations with manned and unmanned systems, improving connectivity and interoperability with the naval forces;
- underwater battlespace data solution to establish situational awareness in the underwater domain. Data analysis algorithms, including machine learning and AI, are required to manage ever larger volumes of (acoustic) data and support decision making;
- communication systems to operate unmanned systems with manned systems including interworking and interoperability of applications and data.

### **Types of activities**

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (*see Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)



Types of activities (art 10(3) EDF Regulation)		Eligible?
(e)	<b>System prototyping</b> <sup>156</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	<b>Qualification</b> <sup>157</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>158</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory activities:

- Design:
  - the proposals must use the NATO Architecture Framework methodology and digital twin approach to design a European interoperable ASW and SBW SoS;
  - non-proprietary standards on data/information exchange level for mission planning, mission supervision and communication to implement unmanned systems into joint/combined task forces.
- System prototyping:
  - the proposed solutions must be demonstrated under operational conditions.

In addition, the proposals should cover the following tasks:

- Design:
  - new UxV platforms with payloads for ASW missions;
  - new sensors including network topologies for threat detection and identification of emerging threats;
  - new breakthrough navigation and mission autonomy algorithms;
  - low cost solutions to provide surveillance capabilities of choke points and littoral waters.

<sup>156</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>157</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>158</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- System prototyping:
  - the proposed solutions should be demonstrated in various operational environments.
- Testing:
  - the proposed solutions should be tested in a simulated environment;
  - the proposed solutions should at least partially be tested under operational conditions.

The proposals must substantiate absence of duplication of activities and tasks described in the topic *Solutions to detect, identify, counter and protect against mobile manned, unmanned or autonomous underwater systems (including those operating at very high depths)* of the call *Underwater Control contributing to resilience at sea* under the European Defence Industrial Development Programme (EDIDP-UCCRS-MUAS-2020). The proposals must also give due consideration to sufficient human oversight of autonomous features in the solutions, as addressed e.g. by the United Nations Convention on Certain Conventional Weapons Group of Governmental Experts Lethal Autonomous Weapon Systems (CCW GGE LAWS) 11 guiding principles.

While conforming to all relevant national, EU, and international laws and regulations, the proposals may use available and relevant sources for topic specific standards and regulations. For example the “Safety and Regulations for European Unmanned Maritime Systems”.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

### Functional requirements

The proposals must be supported by a set of capability requirements as agreed by a group of supporting Member States and EDF associated countries (Norway). The proposals must be in line with the proposed activities and the requirements by the supporting Member States and EDF associated countries (Norway).

The outcome should at least:

- provide for enhanced detection, classification, identification, targeting and neutralisation of current and new underwater threats in challenging

environments;

- be able to perform missions 24/7/365 in the European maritime waters;
- be based on a modular and agile non-proprietary system-of-systems architecture.

### Expected impact

The outcome should contribute to:

- a stronger, more competitive and technologically independent European Defence Technological and Industrial Base (EDTIB) when it comes to solutions for next generation ASW and SBW capabilities;
- enhanced security for EU Member States and EDF associated countries (Norway) and more capable and interoperable forces performing ASW and SBW operations;
- a new European interoperable concept of operations for ASW and SBW.

## **EDF-2023-DA-UWW-MCMC: Future maritime mine countermeasures capability**

### Objectives

#### **General objective**

The maritime mine warfare domain is currently facing two critical challenges. On the one hand, uncertain geopolitical context makes it crucial for European navies to retain the necessary capabilities to keep European waters, critical infrastructure at sea, and sea lines of communications clear from an ever-evolving mine threat (such as buried mines, drifting mines, intelligent mines). To secure a sustainable European sovereignty in conventional military capabilities, the European defence stakeholders must understand the threat and develop appropriate interoperable and interchangeable solutions to mitigate the risk due to naval mines and underwater explosive devices and establish local maritime superiority in areas prone to mine warfare.

On the other hand, new technologies, especially the miniaturisation of the sensors and the level of autonomy on-board naval unmanned platforms, are enabling new operational concepts, such as so-called “stand-off” or semi-autonomous concept – that limit human exposure to danger. European navies have already started to embrace this challenge to maximise future interoperability and share the costs of these developments. Many current European mine countermeasures (MCM) systems are facing obsolescence of systems, and rapid evolving technologies in the underwater domain offer new solutions for Maritime MCM. These solutions enable also new operational concepts to be established.

#### **Specific objective**

The specific objective of this topic is to enable solutions that are easily deployable both on current (by retrofit) and future naval assets. The focus is on interoperability and interchangeability as from the design phase of the systems, including data-sharing. The aim is to provide capable and cost-effective technologies for MCM operations. These include enabling systems for mine warfare platforms (such as launch and recovery (LARS) and command and control (C2) systems), development of unmanned platforms, decision support, planning, and evaluation tools.

The focus is on improving effectiveness in difficult seabed conditions (such as cluttered seabed and deep waters) and against difficult naval mines (such as intelligent mines, stealth mines, buried and concealed mines, drifting mines, and rising or mobile mines), and on reducing time (increase efficiency) of the overall MCM operation. Development of unmanned systems and autonomous features are seen as enablers in this regard. Improvements may also be related to automated collaborative behaviour of UxV-based system of systems to benefit both operational quality and efficiency.

The outcome should benefit a European interoperable and interchangeable MCM future system designed with incremental capabilities to build successive systems to counter current and new mine threats consisting of a system of systems (SoS) with evolving and scalable toolboxes, and enhanced intelligent platforms. The aim is to reach a maturity level equivalent to at least technology readiness level 6 (TRL 6) on at least sub-system level.

### Scope and types of activities

#### **Scope**

The proposals must address design to qualification activities of next-generation MCM solutions which improve the quality and speed of MCM processes. The proposals must cover operations in demanding conditions. The proposals should consider and contribute to unmanned solutions and concepts.

The areas concerned for development and improvement, and that must be addressed are the following:

- performance of the MCM process in terms of quality and time using decision support capabilities;
- operational effectiveness and efficiency through extended autonomous behaviour and improved endurance of unmanned systems (UxV) both individually and as collaborative system of systems;
- detection and neutralisation of difficult naval mines (drifting mines, buried mines, stealthy mines) through improved sensors and/or vectors;
- extending operational MCM capability in battlespace and time, covering environment and factors such as difficult seabed terrain, high sea state, iced waters, non-permissive electromagnetic environment, in the water column from surface to maximum 1000m;
- improving reliability and robustness.

Proposed solutions that address these areas should consider some or all of the following features:

- decision support using sensor data fusion, big data analysis, data exploitation, and improvement of decision-making algorithms and tactical procedures;
- sensor and effector development utilising forms of Artificial Intelligence (AI) and swarm techniques;
- UxVs (UAVs, USVs, UUVs, and other stationary and mobile drones) complementary or embedded to the MCM organic system and interoperable with other naval force elements;
- UxV deployment, launch and recovery functions implemented for designed or designated vessels, craft of opportunity and shore infrastructure;

- joint multi-level (platform-unit-fleet) MCM mission management tools utilising for example AI and Big Data solutions to manage operations using multiple resources (manned and unmanned);
- communication systems to operate unmanned systems with manned systems, including interworking and interoperability of applications and data;
- digital infrastructure and cyber security by design.

### Types of activities

The following table lists the types of activities which are eligible for this topic, and whether they are mandatory or optional (see *Article 10(3) EDF Regulation*):

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence ( <b>generating knowledge</b> )	No
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies ( <b>integrating knowledge</b> )	Yes (optional)
(c)	<b>Studies</b> , such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	<b>Design</b> of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial test for risk reduction in an industrial or representative environment	Yes (mandatory)
(e)	<b>System prototyping</b> <sup>159</sup> of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	<b>Testing</b> of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	<b>Qualification</b> <sup>160</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	<b>Certification</b> <sup>161</sup> of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets <b>increasing efficiency</b> across the life cycle of defence products and technologies	Yes (optional)

The proposals must cover at least the following tasks as part of the mandatory

<sup>159</sup> 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

<sup>160</sup> 'Qualification' means the entire process of demonstrating that the design of the product, component or technology meets the specified requirements, providing objective evidence by which particular requirements of a design are demonstrated to have been met.

<sup>161</sup> 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

activities:

- Design:
  - the proposed solutions must be interoperable at various levels addressing and using existing or foreseen (known to be under negotiation) European and NATO standards;
  - the proposals must adhere to a technical design review milestone approach:
    - SRR (System Requirements Review) SWSR (Software Specifications Review);
    - SFR (System Functional Review)/SDR (System Design Review) PDR (Preliminary Design Review);
    - CDR (Critical Design Review) TRR (Test Readiness Review);
- System prototyping:
  - the proposed solutions must be demonstrated at sea under realistic environmental conditions with relevant mine targets and in an operational environment.

In addition, the proposals should cover the following tasks:

- Design:
  - the proposed solution should form a comprehensive next generation MCM concept supported by relevant European interoperable standards and architecture.
- System prototyping:
  - the proposed solutions should be demonstrated at sea under realistic environmental conditions with relevant mine targets and in various operational environments.
- Testing and qualification:
  - the proposed solutions should be tested in a simulated or controlled environment representing various use cases;
  - the proposed solutions must at least partially be tested and qualified in an operational environment.

The proposals must substantiate absence of duplication of activities and tasks described in the topic *Solutions to detect, identify, counter and protect against mine threats (including those operating at very high depths)* of the call *Underwater Control contributing to resilience at sea* under the European Defence Industrial Development Programme (EDIDP-UCCRS-MCM-2020). The proposals must also give due consideration to sufficient human oversight of autonomous features in the solutions, as addressed e.g. in the United Nations Convention on Certain Conventional Weapons Group of Governmental Experts Lethal Autonomous Weapon Systems (CCW GGE LAWS) 11 guiding principles.

Moreover:

- projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries (or, if studies within the meaning of point (c) are still needed to define the requirements, at least on the joint intent to agree on them)
- projects addressing activities referred to in points (e) to (h) above, must be:
  - supported by at least two Member States or EDF associated countries that intend to procure the final product or use the technology in a coordinated manner, including through joint procurementand
  - based on common technical specifications jointly agreed by the Member States or EDF associated countries that are to co-finance the action or that intend to jointly procure the final product or to jointly use the technology (or, if design within the meaning of point (d) is still needed to define the specifications, at least on the joint intent to agree on them).

#### Functional requirements

The proposals must be supported by a set of capability requirements as agreed by a group of supporting Member States or EDF associated countries (Norway). The proposals must give evidence of coherence between the proposed activities and the requirements by the supporting Member States and EDF associated countries (Norway). Development of capability requirements by supporting Member States and EDF associated countries (Norway) may take into account relevant work done in groups like the PESCO MAS MCM that try to forge a long term vision on the development of an interoperable European MCM Toolbox.

The proposals should develop a capability aiming to:

- provide enhanced MCM processes in challenging environments;
- enable an open, modular, and adaptable MCM system-of-systems suite;
- be able to operate 24/7/365 in the European maritime waters.

#### Expected impact

The outcome should contribute to:

- a stronger, more competitive and technologically independent European Defence Technological and Industrial Base (EDTIB) when it comes to solutions for next generation MCM capabilities;
- enhanced security for EU Member states and EDF associated countries (Norway) and more capable and interoperable forces performing MCM operations;
- a new European interoperable concept of operations for MCM;
- future extended sea-bed warfare capabilities.

### **3. Available budget**

The estimated available call budget is **EUR 714 500 000**.

Specific budget information per topic can be found in the table below:

Topic	Topic budget	Fixed maximum number of projects
<b>EDF-2023-DA-MCBRN-FCS: Federating CBRN systems</b>	<b>EUR 15 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-C4ISR-LCOM: Laser communications</b>	<b>EUR 17 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-C4ISR-TRPAS: Tactical RPAS</b>	<b>EUR 42 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-C4ISR-DAA: Detect and avoid</b>	<b>EUR 40 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-SENS-GRID: Sensor grid</b>	<b>EUR 27 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-CYBER-CSA: Full-Spectrum Cyber Situational Awareness for enhanced Cyberspace Operations Support</b>	<b>EUR 20 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-CYBER-DAAI: Deployable Autonomous AI Agent</b>	<b>EUR 26 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-SPACE-SSA: Initial operational capacity for Space situational awareness C2 and sensors</b>	<b>EUR 100 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-MATCOMP-MJR-CBDIN: Technologies and processes for maintenance, joining and repair through an innovation test hub</b>	<b>EUR 30 000 000</b> excluding remuneration of EDA	No
<b>EDF-2023-DA-AIR-STFS: Smart technologies for next generation fighter systems</b>	<b>EUR 30 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-AIR-SPS: Self-protection systems</b>	<b>EUR 33 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-AIRDEF-CUAS: Counter unmanned aerial systems</b>	<b>EUR 43 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-GROUND-MBT: Main battle tank platform systems</b>	<b>EUR 20 000 000</b>	No
<b>EDF-2023-DA-GROUND-IFS: Long-range indirect fire support capabilities for precision and high efficiency strikes</b>	<b>EUR 27 000 000</b>	No (but normally 1 expected)
<b>EDF-2023-DA-NAVAL-MMPC: Modular and multirole patrol corvette</b>	<b>EUR 154 500 000</b> excluding remuneration of OCCAR	No (but normally 1 expected)
<b>EDF-2023-DA-UWW-ASW: Unmanned anti-submarine and seabed warfare</b>	<b>EUR 45 000 000</b>	No (but normally 1 expected)



Topic	Topic budget	Fixed maximum number of projects
<b>EDF-2023-DA-UWW-MCMC: Future maritime mine countermeasures capability</b>	<b>EUR 45 000 000</b>	No (but normally 1 expected)

We reserve the right not to award all available funds or to redistribute them between the call priorities (i.e. topics), depending on the proposals received and the results of the evaluation.

#### 4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	22 June 2023
<u>Deadline for submission:</u>	<u>22 November 2023 – 17:00:00 CET (Brussels)</u>
Evaluation:	November 2023 – May 2024
Information on evaluation results:	June 2024
GA signature <sup>162</sup> :	June – December 2024

#### 5. Admissibility and documents

Proposals must be submitted before the **call deadline** (see *timetable section 4*).

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the [Search Funding & Tenders](#) section). Paper submissions are NOT possible.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System (⚠ NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:

- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities), the ethics issues table and the summarised budget for the project (*to be filled in directly online*)
- Application Form Part B — contains the technical description of the project (*to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded*)
- mandatory **annexes and supporting documents** (*templates available to be downloaded from the Portal Submission System, completed, assembled and re-uploaded together with Application Form Part B*):
  - detailed budget table (EDF DA)

<sup>162</sup> In case of change in the management mode for a given action (see Section 3 of the EDF Work Programme), this timeframe may be different.

- participant information (including previous projects, if any)
- list of infrastructure, facilities, assets and resources
- cofinancing declarations (if the requested EU grant does not cover the total eligible costs of the project)
- actual indirect cost methodology declarations (if actual indirect costs used)
- harmonised capability declarations (if the project covers design activities)
- declarations on procurement intent and common specifications (if the project covers system prototyping/testing/qualification/certification activities)
- ownership control declarations
- PRS declaration (if the project requires access to Galileo PRS information).


Please note that the amounts entered into the summarised budget table (filled in directly online) must correspond to the amounts calculated in the detailed budget table. In case of discrepancies, the amounts in the online summarised budget table will prevail.

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that the participants comply with the conditions for receiving EU funding (especially eligibility, financial and operational capacity, exclusion, etc.). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable, accessible and printable**.

Proposals (Part B) are limited to maximum **100 pages**, counting the work package descriptions. Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents (*for legal entity validation, financial capacity check, bank account validation, etc.*).

 For more information about the submission process (including IT aspects), consult the [Online Manual](#).

## 6. Eligibility

Applications will only be considered eligible if their content corresponds wholly (or at least in part) to the topic description for which it is submitted.

### Eligible participants (eligible countries)


In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
  - EU Member States (including overseas countries and territories (OCTs))
  - non-EU countries:
    - listed EEA countries ('EDF associated countries', see [list of participating countries](#))

- have their executive management structure established in eligible countries
- must not be subject to control by a non-associated third country or non-associated third-country entity (unless they can provide guarantees – see *Annex 2* - approved by the Member State or EDF associated country where they are established)

Beneficiaries and affiliated entities must register in the [Participant Register](#) — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Other entities may participate in other roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc. (*see section 13*).

 Please note that, in EDF, subcontractors involved in the action<sup>163</sup> and associated partners must also comply with the above-listed conditions concerning establishment and control.


Associated partners which are not established in one of the eligible countries (or which are subject to control by a non-associated third country or non-associated third-country entity) may however participate exceptionally if certain conditions are fulfilled (*not contravene EU and MS security and defence interests; consistent with EDF objectives; results not subject to control or restriction by non-associated third countries or non-associated third-country entities; no unauthorised access to classified information; no potential negative effects over security of supply of inputs which are critical for the project*), subject to agreement by the granting authority and without any funding under the grant.

### *Specific cases*

**Natural persons** — Natural persons are NOT eligible (with the exception of self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

**International organisations** — International organisations are not eligible, unless they are international organisations whose members are only Member States or EDF associated countries and whose executive management structure is in a Member State or EDF associated country.

**Entities without legal personality** — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons<sup>164</sup>.

**Associations and interest groupings** — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'<sup>165</sup>.  Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

**Subcontractors involved in the action** — Subcontractors with a direct contractual relationship to a recipient (*i.e. beneficiary or affiliated entity*), other subcontractors to

<sup>163</sup> 'Subcontractors involved in the action' means subcontractors with a direct contractual relationship to a beneficiary or affiliated entity, other subcontractors to which at least 10 % of the total eligible costs of the action are allocated, and subcontractors which may need access to classified information in order to carry out the project.

<sup>164</sup> See Article 197(2)(c) EU Financial Regulation [2018/1046](#).

<sup>165</sup> For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation [2018/1046](#).

which at least 10 % of the total eligible costs of the action is allocated, and subcontractors which may need access to classified information in order to carry out the action.

Following the [Council Implementing Decision \(EU\) 2022/2506](#), as of 16<sup>th</sup> December 2022, no legal commitments (including the grant agreement itself as well as subcontracts, purchase contracts, financial support to third parties, etc.) can be signed with Hungarian public interest trusts established under Hungarian Act IX of 2021 or any entity they maintain. Affected entities may continue to apply to calls for proposals. However, in case the Council measures are not lifted, such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties). In this case, co-applicants will be invited to remove or replace that entity and/or to change its status into associated partner. Tasks and budget may be redistributed accordingly.

EU restrictive measures — Special rules apply for certain entities (*e.g. entities subject to [EU restrictive measures](#) under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)*<sup>166</sup> and entities covered by Commission Guidelines No [2013/C 205/05](#)<sup>167</sup>). Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

 For more information, see [Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment](#).


### Consortium composition

For all topics under this call, proposals must be submitted by:

- minimum 3 independent applicants (beneficiaries; not affiliated entities) from 3 different eligible countries.

### Eligible actions and activities

Eligible actions and activities are the ones set out in section 2 above.

 Please note that the evaluation will also take into account how the proposals address the 'must', 'should' and 'may' requirements included in the subsections 'Scope and types of activities' and 'Functional requirements'. Failing to address a 'must' may give grounds to consider the proposal out of scope; failing to address a 'should' may give grounds for impacting the scoring negatively; addressing a 'may' may give grounds for impacting the scoring positively.

The following actions and activities are not considered as eligible for funding under this call:

- projects that do not implement the objectives set out in Article 3 of the EDF Regulation
- projects that do not concern new defence products or technologies or the upgrade of existing defence products or technologies

<sup>166</sup> Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the [EU Sanctions Map](#).

<sup>167</sup> Commission guidelines No [2013/C 205/05](#) on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

- projects that do not relate to at least one of the types of activities set out in Article 10(3) of the EDF Regulation
- projects that do not cover the mandatory types of activities set out in section 2
- projects that concern products and technologies whose use, development or production is prohibited by international law
- projects that concern the development of lethal autonomous weapons without the possibility for meaningful human control over selection and engagement decisions when carrying out strikes against humans (with the exception of the development of early warning systems and countermeasures for defensive purposes).
- projects where background or results:
  - would be subject to control or restriction by a non-associated third country or non-associated third-country entity, directly, or indirectly through one or more intermediate legal entities, including in terms of technology transfer
  - and, for pre-existing information (background), this would impact the results.

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).


Projects must comply with EU policy interests and priorities (*such as environment, social, security, industrial and trade policy, etc.*).

Financial support to third parties:

- is mandatory for the topic EDF-2023-DA-MATCOMP-MJR-CBDIN. For the conditions, see *section 2*.
- is not allowed in all other topics under this call.

#### Geographic location (target countries)

Proposals must relate to activities taking place in the eligible countries (*see above*).

 Please note that moreover, in EDF, only infrastructure, facilities, assets and resources which are located or held in an eligible country may be used. Other assets, infrastructure, facilities or resources may be used only exceptionally if certain conditions are fulfilled (*no competitive substitutes are readily available; not contravene EU and MS security and defence interests; consistent with EDF objectives; results not subject to control or restriction by non-associated third countries or non-associated third-country entities*), subject to agreement by the granting authority and without any funding under the grant.

#### Duration

Project duration:

- for all topics: between 12 and 48 months

Projects of longer duration may be accepted in duly justified cases. Extensions are possible, if duly justified and through an amendment.

### Project budget

Project budgets (maximum grant amount):

- for all topics under this call: should not exceed the budget available for the topic (*see table in section 3*)

This does not however preclude the submission/selection of proposals requesting other amounts. The grant awarded may be lower than the amount requested.

### Ethics

Projects must comply with:

- highest ethical standards (including highest standards of research integrity) and
- applicable EU, international and national law.

Proposals under this call will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

### Security

Projects involving classified information must undergo security scrutiny to authorise *funding* and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

Projects where the Member States of the participating beneficiaries and affiliated entities decide to establish a specific security framework under Article 27(4) of the EDF Regulation, will be subject to this specific security framework and classified foreground information (results) generated by the project will be under the originatorship of these Member States.

If no such specific security framework is set up by the signature of the grant agreement, the security rules will be governed by Commission Decision [2015/444](#)<sup>168</sup> and its implementing rules<sup>169</sup>.

These rules provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
  - created or accessed only on premises with facility security clearing (FSC) from the competent national security authority (NSA), in accordance with the national rules
  - handled only in a secured area accredited by the competent NSA

<sup>168</sup> See Commission Decision 2015/544/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).


<sup>169</sup> See Article 27(4) EDF Regulation.

- accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know
- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving classified information may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission)
- disclosure of classified information to third parties is subject to prior written approval from the granting authority.

Please note that facility security clearing may have to be provided before grant signature. The granting authority will assess the need for clearing in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearing.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables (*e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc.*).

Beneficiaries must ensure that their projects are not subject to third-country/international organisation security requirements that could affect implementation or put into question the award of the grant (*e.g. technology restrictions, national security classification, etc.*). The granting authority must be notified immediately of any potential security issues.

 More information on security aspects can be found in Annex 3.

## 7. Financial and operational capacity and exclusion

### Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all these projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the [Participant Register](#) during grant preparation (*e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc.*). The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information



- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities (*see below, section 10*)
  - prefinancing paid in instalments
  - (one or more) prefinancing guarantees (*see below, section 10*)
- or
- propose no prefinancing
  - request that you are replaced or, if needed, reject the entire proposal.

 For more information, see [Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment](#).

### Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the 'Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project.
- description of the consortium participants (including previous projects, if any).

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Public bodies, Member State organisations and international organisations are exempted from the operational capacity check.

### Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate<sup>170</sup>:

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct<sup>171</sup> (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

---

<sup>170</sup> See Articles 136 and 141 of EU Financial Regulation [2018/1046](#).



- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- guilty of irregularities within the meaning of Article 1(2) of EU Regulation [2988/95](#) (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant).

Applicants will also be rejected if it turns out that<sup>172</sup>:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

## 8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, *see sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each budget envelope; *see section 3*) against the operational capacity and award criteria (*see sections 7 and 9*) and then ranked according to their scores.

For proposals with the same score (within a budget envelope) a **priority order** will be determined according to the following approach:

Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:

- 1) Proposals will be prioritised according to the scores they have been awarded for the criterion 'Excellence and potential of disruption'. When these scores are equal, priority will be based on scores for the criterion 'Innovation and technological development'. When these scores are equal, priority will be based on scores for the criterion 'Competitiveness'. When these scores are

---


<sup>171</sup> Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain advantage.

<sup>172</sup> See Article 141 EU Financial Regulation [2018/1046](#).

equal, priority will be based on scores for the criterion 'Creation of new cross-border cooperation'

- 2) If necessary, any further prioritisation will be based on the number of Member States or EDF associated countries, in which applicants involved in the proposal are established

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

 No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc.*

**Grant preparation** will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending will be considered to have been accessed and that deadlines will be counted from opening/access (see also [Funding & Tenders Portal Terms and Conditions](#)). Please also be aware that for complaints submitted electronically, there may be character limitations.

## 9. Award criteria

The **award criteria** for this call are as follows:

### 1. Excellence and potential of disruption (5 points)

- Excellence of the overall concept and soundness of the proposed approach for the solution, including main ideas, technologies and methodology
- Compliance of the proposal with the objectives, scope and targeted activities), functional requirements and expected impact of the topic as set out in section 2
- Extent to which the objective and expected outcome of the proposed project differs from (and represents an advantage at strategic, technological or defence operational level over) existing defence products or technologies, or has a potential of disruption in the defence domain

### 2. Innovation and technological development (5 points)

- Extent to which the proposal demonstrates innovation potential and contains ground-breaking or novel concepts and approaches (*e.g. new products, services or business and organizational models*), new promising technological improvements, or the application of technologies or concepts previously not applied in the defence sector
- Integration of existing knowledge and previous or ongoing R&D activities in the defence and/or civil sectors, while avoiding unnecessary duplication

- Extent to which the innovations or technologies developed under the proposal could spin-off to other defence applications and products

### **3. Competitiveness (5 points)**

- Foreseen competitive advantage of the product/technology/solution vis-a-vis existing or planned products/technologies/solutions across the EU and beyond, including consideration given to the balance between performance and cost-efficiency of the solution
- Potential to accelerate the growth of companies throughout the EU, based on an analysis of the EU internal market and the global market place, indicating, to the extent possible, the size and the growth potential of the market it addresses, as well as expected volumes of sales both within and outside of the EU.
- Strength of the IP strategy (*e.g. patents*) associated with the solution to support the competitiveness and growth of the applicant companies

### **4. EDTIB autonomy (5 points)**

- Extent to which the proposed project will contribute to the autonomy of the European defence technological and industrial base (EDTIB) by increasing the EU's industrial and technological non-dependency from third countries
- Beneficial impact that the proposed activities will have on the strength of the European security of supply, including the creation of a new supply chain
- Extent to which the project outcome will contribute to the defence capability priorities agreed by Member States within the framework of the Common Foreign and Security Policy (CFSP), and in particular in the context of the [Capability Development Plan](#) (EDA version releasable to the industry); where appropriate, extent to which the proposal addresses regional or an international priorities which serve the security and defence interests of the EU as determined under the CFSP and do not exclude the possibility of participation of Member States or EDF associated countries

### **5. Creation of new cross-border cooperation (5 points)**

- Extent to which the proposed project will create new cross-border cooperation between legal entities established in Member States or EDF associated countries, in particular SMEs and mid-caps, especially compared to former activities in the technological area of the call and taking into account the specificity of the market
- Planned future cross-border cooperation between legal entities established in Member States or EDF associated countries and cooperation opportunities created by the proposed activities
- Extent to which SMEs and mid-caps which cooperate cross-border participate substantially, and industrial or technological added value brought by them

**6. Lifecycle efficiency (5 points)**

- Improvement in terms of the efficiency across the lifecycle in comparison to existing solutions; for example, improvement in terms of cost-effectiveness by lower production, operational, maintenance, repair and overhaul or disposal costs and/or potential simplification of processes or combination with existing processes for procurement, maintenance and disposal.

**7. Member State cooperation (5 points)**

- The contribution to the further integration of the European defence industry throughout the Union through the demonstration by the recipients that Member States have undertaken to jointly use, own or maintain the final product or technology in a coordinated way.

**8. Implementation (5 points)**

- Effectiveness and practicality of the structure of the work plan (work breakdown structure), including timing and inter-relation of the different work packages and their components (illustrated by a Gantt chart, Pert chart or similar)
- Usefulness and comprehensiveness of the milestones and deliverables of the project; coherence and clarity of the criteria for reaching the milestones, which should be measurable, realistic and achievable within the proposed duration
- Appropriateness of the management structures and procedures, including decision-making mechanisms, to the complexity and scale of the project; quality of the risk management, including identification and assessment of the project specific critical risks, which could compromise the achievement of the stated project's objectives and detail of proposed risk treatments (*e.g. mitigation measures*)
- Appropriateness of the allocation of tasks and resources between consortium members, ensuring that all participants have a valid and complementary role; allocation of the work share that ensures a high level of effectiveness and efficiency for carrying out the project.

Award criteria	Minimum pass score	Maximum score	Weighting
Excellence and potential of disruption	n/a	5	2
Innovation and technological development	n/a	5	1
Competitiveness	n/a	5	1
EDTIB autonomy	n/a	5	2
Creation of new cross-border cooperation	n/a	5	2
Lifecycle efficiency	n/a	5	1
Member State cooperation	n/a	5	1
Implementation	n/a	5	1

Award criteria	Minimum pass score	Maximum score	Weighting
Overall weighted (pass) scores	37	55	N/A

Maximum points: 55 points.

There is no minimum pass score for individual criteria.

Overall threshold: 37 points.

Proposals that pass the overall threshold will be considered for funding — within the limits of the available budget (i.e. up to the budget ceiling). Other proposals will be rejected.

## 10. Legal and financial set-up of the Grant Agreements<sup>173</sup>

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on [Portal Reference Documents](#).

### Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement (*Data Sheet, point 1*). Normally the starting date will be after grant signature. A retroactive starting date can be granted exceptionally for duly justified reasons — but never earlier than the proposal submission date.

Project duration: *see section 6 above*

### Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

The following deliverables will be mandatory for all projects:

- progress reports (every 6 to 12 months, to be agreed during grant agreement preparation)

### Form of grant, funding rate and maximum grant amount

The grant parameters (*maximum grant amount, funding rate, total eligible costs, etc.*) will be fixed in the Grant Agreement (*Data Sheet, point 3 and art 5*).

Project budget (maximum grant amount): *see section 6 above*.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs

<sup>173</sup> In case of change in the management mode for a given action (see Section 3 of the EDF Work Programme), these rules may be different. For the topics EDF-2023-DA-MATCOMP-MJR-CBDIN and EDF-2023-DA-NAVAL-MMPC, the EDF work programme already foresees that the resulting grants will be managed by entrusted entities.

(eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted* costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement (*see art 6 and Annex 2 and 2a*).

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of activities and participants (*see section 2*).

Grants may in principle NOT produce a profit (i.e. surplus of revenues + EU grant over costs). Where the no-profit rule is activated in the Grant Agreement, for-profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount (*see art 22.3*).

Moreover, please be aware that the final grant amount may be reduced in case of non-compliance with the Grant Agreement (*e.g. improper implementation, breach of obligations, etc.*).

### Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement (*Data Sheet, point 3, art 6 and Annex 2*).

#### *Budget categories for this call:*


- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties (allowed only for topic EDF-2023-DA-MATCOMP-MJR-CBDIN)
  - D.2 Internally invoiced goods and services
- E. Indirect costs

#### *Specific cost eligibility conditions for this call:*

- personnel costs:
  - average personnel costs (unit cost according to usual cost accounting practices)<sup>174</sup>: Yes
  - SME owner/natural person unit cost<sup>175</sup>: Yes
- subcontracting costs:

<sup>174</sup> [Decision](#) of 27 February 2023 authorising the use of unit costs for staff costs and costs for internally invoiced goods and services for specific actions under the European Defence Programme.

<sup>175</sup> Commission [Decision](#) of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7115).

- country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
  - travel and subsistence unit cost<sup>176</sup>: No (only actual costs)
  - equipment costs:
    - depreciation + full cost for listed equipment (for all topics)
  - other cost categories:
    - costs for financial support to third parties: allowed only for the grants related to the following topic:
      - EDF-2023-DA-MATCOMP-MJR-CBDIN: maximum amount per third party is EUR 60 000,
    - internally invoiced goods and services (unit cost according to usual cost accounting practices)<sup>177</sup>: Yes
  - indirect cost:
    - flat-rate: 25% of the eligible direct costs (categories A-D, except subcontracting costs, financial support to third parties and exempted specific cost categories, i.e. internally invoiced goods and services and PCP procurement costs)
- or
- actual costs
-  The indirect cost method selected will be fixed for the project and cannot be changed later on.
- VAT: non-deductible VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
  - other:
    - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
    - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
    - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible
    - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible
    - other ineligible costs: Yes, costs related to the use of assets, infrastructure, facilities or resources located or held outside the eligible countries are not eligible (even if their use was authorised, *see section 6*).

### Reporting and payment arrangements

<sup>176</sup> Commission [Decision](#) of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

<sup>177</sup> [Decision](#) of 27 February 2023 authorising the use of unit costs for staff costs and costs for internally invoiced goods and services for specific actions under the European Defence Programme.



The reporting and payment arrangements are fixed in the Grant Agreement (*Data Sheet, point 4 and art 21 and 22*).


After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **55%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/starting date/financial guarantee (if required) — whichever is the latest.

For projects of more than 18 months, there may be one or more **additional prefinancing payments** linked to a prefinancing report and one or more **interim payments** (with detailed cost reporting).

In addition, you will be requested to submit one or more progress reports not linked to payments.

**Payment of the balance:** At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All payments will be made to the coordinator.

 Please be aware that payments will be automatically lowered if one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement (*see art 22*).

Please also note that you are responsible for keeping records on all the work done and the costs declared.

### Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement (*Data Sheet, point 4*). The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are formally NOT linked to individual consortium members, which means that you are free to organise how to provide the guarantee amount (*by one or several beneficiaries, for the overall amount or several guarantees for partial amounts, by the beneficiary concerned or by another beneficiary, etc.*). It is however important that the requested amount is covered and that the guarantee(s) are sent to us in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement.

### Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and



thresholds for each certificate are fixed in the Grant Agreement (*Data Sheet, point 4 and art 24*).

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement (*Data Sheet point 4.4 and art 22*).

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up to their maximum grant amount*
- unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*
- or
- individual financial responsibility — *each beneficiary only for their own debts*.

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary).

Provisions concerning the project implementation

Security rules: *see Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- background and list of background: Yes
- protection of results: Yes
- limitations to transfers and licensing: Yes
- rights of use on results: Yes
- for Research Actions: access to results for policy purposes: Yes
- for Research Actions: access to special report: Yes
- for Research Actions: access rights to further develop results: Yes

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5):*

- additional communication and dissemination activities: Yes

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5):*

- specific rules for EDF actions: Yes
- specific rules for PCP Grants for Procurement: No
- place of performance obligation for PCP Grants for Procurement: No
- specific rules for Grants for Financial Support: No
- specific rules for blending operations: No

### Other specificities

n/a

### Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).

 For more information, see [AGA — Annotated Grant Agreement](#).

## **11. How to submit an application**

All proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

### **a) create a user account and register your organisation**

To use the Submission System (the only way to apply), all participants need to [create an EU Login user account](#).

Once you have an EULogin account, you can [register your organisation](#) in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).


### **b) submit the proposal**

Access the Electronic Submission System via the Topic page in the [Search Funding & Tenders](#) section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 2 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B and Annexes through a password-protected single zip archive:
  - Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and add to the zip archive as a PDF
  - Annexes (*see section 5*). Download the templates, and add to zip archive as PDFs (— unless other format specified).

The zip archive must be submitted password-protected (using AES-256 encryption method), with a size of less than 100 MB. The password (and any other passwords used in the documents) must be communicated before the deadline for submission to the following email address: [DEFIS-EDF-PROPOSALS-PWD@ec.europa.eu](mailto:DEFIS-EDF-PROPOSALS-PWD@ec.europa.eu) (together with the proposal ID and the name of the zip archive).

 If your proposal includes **classified information**, please contact us at [DEFIS-EDF-PROPOSALS@ec.europa.eu](mailto:DEFIS-EDF-PROPOSALS@ec.europa.eu) — well in time before the deadline, in order to arrange the delivery of the classified documents. Please be aware that such documents **MUST NOT** under any circumstances be submitted online through the Funding & Tenders Portal.

The proposal must keep to the **page limits** (see *section 5*); excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System otherwise the proposal might be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (see *section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the [IT Helpdesk webform](#), explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the [Online Manual](#). The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

## 12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- [Online Manual](#)
- FAQs on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)
- [Portal FAQ](#) (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

### Contact

For individual questions on the Portal Submission System, please contact the [IT Helpdesk](#).

Non-IT related questions should be sent to the following email address: [DEFIS-EDF-PROPOSALS@ec.europa.eu](mailto:DEFIS-EDF-PROPOSALS@ec.europa.eu).

Please indicate clearly the reference of the call and topic to which your question relates (see *cover page*).

## 13. Important



### IMPORTANT

- **Don't wait until the end** — Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions (*e.g. congestion, etc.*) will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System** — By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the [Portal Terms & Conditions](#).
- **Registration** — Before submitting the application, all beneficiaries, affiliated entities, associated partners must be registered in the [Participant Register](#). The draft participant identification code (PIC) (one per participant) is mandatory for the Application Form.  
If your project applies for the SME/Mid-cap bonuses, registration (draft PIC and SME self-assessment wizard) is also mandatory for all participants claiming SME/Mid-cap status (beneficiaries, affiliated entities and subcontractors involved in the action; *see section 2*).  
Moreover, registration (draft PIC) is required for entities that must submit an ownership control assessment declaration (beneficiaries, affiliated entities, subcontractors involved in the action and associated partners).
- **Consortium roles** — When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.  
The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs per beneficiary/affiliated entity must be justified in the application and may be accepted by the granting authority if the topic is not subject to a fixed subcontracting limit (*see section 10*).
- **Coordinator** — In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any).
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.

- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.
- **Balanced project budget** — Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully (*e.g. own contributions, income generated by the action, financial contributions from third parties, etc.*). You may be requested to lower your estimated costs, if they are ineligible (including excessive).
- **No-profit rule** — Grants may in principle NOT give a profit (i.e. surplus of revenues + EU grant over costs). Where the no-profit rule is activated in the Grant Agreement, this will be checked by us at the end of the project.
- **No double funding** — There is a strict prohibition of double funding from the EU budget (except under EU Synergies actions). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances be declared to two different EU actions.
- **Completed/ongoing projects** — Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).
- **Combination with EU operating grants** — Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice (see [AGA — Annotated Grant Agreement, art 6.2.E](#)).
- **Multiple proposals** — Applicants may submit more than one proposal for *different* projects under the same call (and be awarded a funding for them).  
Organisations may participate in several proposals.  
BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw one of them (or it will be rejected).
- **Resubmission** — Proposals may be changed and re-submitted until the deadline for submission.
- **Rejection** — By submitting the application, all applicants accept the call conditions set out in this Call Document (and the documents it refers to). Proposals that do not comply with all the call conditions will be **rejected**. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, it must be replaced or the entire proposal will be rejected.
- **Cancellation** — There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.
- **Language** — You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, see *section 12*).

- **Transparency** — In accordance with Article 38 of the [EU Financial Regulation](#), information about EU grants awarded is published each year on the [Europa website](#).

This includes:

- beneficiary names
- beneficiary addresses
- the purpose for which the grant was awarded
- the maximum amount awarded.

The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection** — The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the [Funding & Tenders Portal Privacy Statement](#).

## Annex 1

### EDF types of action

EDF uses the following actions to implement grants:

#### Research Actions

**Description:** Research Actions (RA) target activities consisting primarily of research activities, in particular applied research and where necessary fundamental research, with the aim of acquiring new knowledge and with an exclusive focus on defence applications.

**Funding rate:** 100%

**Payment model:** Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

#### Development Actions

**Description:** Development Actions (DA) target activities consisting of defence-oriented activities primarily in the development phase, covering new defence products or technologies or the upgrading of existing ones, excluding the production or use of weapon.

**Funding rate:** variable per activity (rates depend on activity and bonuses for SME and mid-cap participation and PESCO)

**Payment model:** Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

#### PCP Grants for Procurement

**Description:** PCP Grants for Procurement (PCP) target activities that aim to help a transnational buyers' group to strengthen the public procurement of research, development, validation and, possibly, the first deployment of new solutions that can significantly improve quality and efficiency in areas of public interest, while opening market opportunities for industry and researchers active in Europe. Eligible activities include the preparation, management and follow-up, under the coordination of a lead procurer, of one joint PCP and additional activities to embed the PCP into a wider set of demand-side activities.

**Funding rate:** variable (to be defined in the work programme)

**Payment model:** Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — payment of the balance

#### Lump Sum Grants for Research Actions

**Description:** Lump Sum Grants (LS-RA) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature) on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented, only part of the lump sum will be paid.

Lump Sum Grants for Research Actions cover the same type of activities as Research Actions and follow — where relevant — similar rules (*e.g. for funding rates, etc.*).

**Funding rate:** 100%

**Payment model:** Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

### **Lump Sum Grants for Development Actions**

**Description:** Lump Sum Grants (LS-DA) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature) on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented, only part of the lump sum will be paid.

Lump Sum Grants for Development Actions cover the same type of activities as Development Actions and follow — where relevant — similar rules (*e.g. for funding rates, etc.*).

**Funding rate:** variable per activity (rates depend on activity and bonuses for SME and mid-cap participation and PESCO)

**Payment model:** Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment

### **Framework Partnerships (FPAs) and Specific Grants (SGAs)**

#### **FPAs**

**Description:** FPAs establish a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

**Funding rate:** no funding for FPA

#### **SGAs**

**Description:** The SGAs are linked to an FPA and implement the action plan (or part of it). They are awarded via an invitation to submit a proposal (identified beneficiary action). The consortium composition should in principle match (meaning that only entities that are part of the FPA can participate in an SGA), but otherwise the implementation is rather flexible. FPAs and SGAs can have different coordinators; other partners of the FPA are free to participate in an SGA or not. There is no limit to the amount of SGAs signed under one FPA.

**Funding rate:** depending on the type: 100% or variable per activity

**Payment model:** Prefinancing — (x) additional prefinancing payment(s) — (x) interim payment(s) — final payment



**Annex 2****Guarantees pursuant to Article 9(4) of the EDF Regulation**

All calls under the EDF Programme are subject to ownership control restrictions, meaning that they exclude the participation of legal entities which are established in the EU territory or in an EDF associated country, but are controlled by a non-associated third country or non-associated third country legal entity.

Thus, for the purposes of participating in EDF actions, beneficiaries, affiliated entities, associated partners and subcontractors involved in the action must not be subject to control by a non-associated third country or non-associated third-country entity and undergo an ownership control assessment procedure before grant signature.

Entities that do not comply with this requirement may however exceptionally nevertheless participate, if they can provide guarantees approved by the Member State/EDF associated country in which they are established. Such guarantees must be provided at the latest by grant signature.


The guarantees must provide assurance to the granting authority that the participation of the entity will not contravene the security and defence interests of the EU and its Member States as established in the framework of the Common Foreign and Security Policy (CFSP) pursuant to Title V of the TEU, or the objectives set out in Article 3 of the EDF Regulation. They must also comply with the provisions on ownership and intellectual property rights (Articles 20 and 23 of the EDF Regulation).

They must in particular substantiate that, for the purposes of the action, measures are in place to ensure that:

- **control** over the legal entity is not exercised in a manner that would restrain or restrict its ability to carry out the action and to deliver results, that would impose restrictions concerning its infrastructure, facilities, assets, resources, intellectual property or knowhow needed for the purposes of the action, or that would undermine its capabilities and standards necessary to carry out the action
- **access** by a non-associated third country or non-associated third-country entity to sensitive information relating to the action is prevented and the employees or other persons involved in the action have national security clearance issued by a Member State or an EDF associated country, where appropriate
- **ownership** of the intellectual property arising from, and the results of, the action remain within the beneficiary or affiliated entity during and after completion of the action, are not subject to control or restriction by a non-associated third country or non-associated third-country entity, and are neither exported outside the EU/EDF associated countries nor accessible from outside the EU/EDF associated countries without the approval of the Member State/EDF associated country in which the legal entity is established and in accordance with the objectives set out in Article 3 of the EDF Regulation.

The guarantees may refer to the fact that the legal entity's executive management structure is established in the EU/EDF associated country or, if considered appropriate, to specific governmental rights in the control over the legal entity.

If considered appropriate by the Member State/EDF associated country, additional guarantees may be provided.

 For more information, see also [\*Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls.\*](#)

## **Annex 3**

### **Security aspects**

#### **Introduction**

Pursuant to Article 27(4) of the EDF Regulation, in case the implementation of the grant involves the handling of classified information, Member States on whose territory the beneficiaries and affiliated entities are established must decide on the originatorship of the classified foreground information (results) generated in the performance of the project. For that purpose, those Member States may decide on a specific security framework for the protection and handling of classified information relating to the project and must inform the granting authority. Such a security framework must be without prejudice to the possibility for the granting authority to have access to necessary information for the implementation of the action.

If no such specific security framework is set up by those Member States, the security framework will be put in place by the granting authority in accordance with Decision 2015/444.

In either case, the security framework will be put in place at the latest by the signature of the Grant Agreement.

The applicable security framework will be detailed in the security aspect letter (SAL) which will be annexed to the Grant Agreement.

When you implement a classified grant, please bear in mind the following key rules.

#### **Access to classified information**

The creation, handling or access to information classified CONFIDENTIAL or SECRET (or RESTRICTED where required by national rules) on the premises of a participant is only possible if a valid Facility Security Clearance (FSC) at the appropriate level exists for the premises. This FSC must be granted by the National Security Authority (NSA/DSA) of the participant concerned.

The participant must hold a duly confirmed FSC at the appropriate level. Until a secured area is in place and accredited by the national NSA, the handling of classified information above RESTRICTED level on their premises is not allowed.

Access to and handling of classified information for the purposes of the project must be limited to individuals with a need-to-know and which are in possession of a valid personnel security clearance.

At the end of the Grant Agreement when EUCI is no longer required for the performance of the grant, the participant must return any EUCI they hold to the contracting authority immediately. If authorised to retain EUCI after the end of the grant, the EUCI must continue to be protected in accordance with Decision 2015/444.

#### **Marking of classified information**

Classified information generated for the performance of the action must be marked in accordance with the applicable security framework, as described in the SAL.

Grants must not involve information classified 'TRES SECRET UE/EU TOP SECRET' or any equivalent classification.

## Other provisions

Where a participant has awarded a classified subcontract, the security provisions of the grant agreement must apply *mutatis mutandis* to the subcontractor(s) and their personnel. In such case, it is the responsibility of the participant to ensure that all subcontractors apply these principles to their own subcontracting arrangements.

All security breaches related to classified information will be investigated by the competent security authority and may lead to criminal prosecution under national law.

## Table of equivalent security classification markings

	Secret	Confidential	Restricted
<b>EU</b>	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
<b>Austria</b>	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
<b>Belgium</b>	SECRET (Loi du 11 Dec 1998) or GEHEIM (Wet van 11 Dec 1998)	CONFIDENTIEL (Loi du 11 Dec 1998) or VERTROUWELIJK (Wet van 11 Dec 1998)	(Note 1, see below)
<b>Bulgaria</b>	СЕКРЕТНО	ПОВЕРЛИВО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
<b>Croatia</b>	TAJNO	POVJERLJIVO	OGRANIČENO
<b>Cyprus</b>	ΑΠΟΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΟ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ ABR:(ΠΧ)
<b>Czech Republic</b>	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
<b>Denmark</b>	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
<b>Estonia</b>	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
<b>Finland</b>	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG

<b>France</b>	SECRET SECRET DÉFENSE (Note 2, see below)	CONFIDENTIEL DÉFENSE (Notes 2 and 3, see below)	(Note 4, see below)
<b>Germany</b> (Note 5, see below)	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
<b>Greece</b>	ΑΠΟΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΟ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ ABR:(ΠΧ)
<b>Hungary</b>	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
<b>Ireland</b>	SECRET	CONFIDENTIAL	RESTRICTED
<b>Italy</b>	SEGRETO	RISERVATISSIMO	RISERVATO
<b>Latvia</b>	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
<b>Lithuania</b>	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
<b>Luxembourg</b>	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
<b>Malta</b>	SIGRIET	KUNFIDENZJALI	RISTRETT
<b>Netherlands</b>	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
<b>Poland</b>	TAJNE	POUFNE	ZASTRZEŻONE
<b>Portugal</b>	SECRETO	CONFIDENCIAL	RESERVADO (Note 6, see below)
<b>Romania</b>	STRICT SECRET	SECRET	SECRET DE SERVICIU
<b>Slovakia</b>	TAJNÉ	DÔVERNÉ	VYHRADENÉ
<b>Slovenia</b>	TAJNO	ZAUPNO	INTERNO
<b>Spain</b>	RESERVADO (Note 6, see below)	CONFIDENCIAL	DIFUSIÓN LIMITADA
<b>Sweden</b>	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIIG

**Notes:**

**Note 1 Belgium:** 'Diffusion Restreinte/Beperkte Verspreiding' is not a security classification in Belgium. Belgium handles and protects RESTREINT UE/EU RESTRICTED information and classified information bearing the national classification markings of RESTRICTED level in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

**Note 2 France:** Information generated by France before 1 July 2021 and classified SECRET DÉFENSE and CONFIDENTIEL DÉFENSE continues to be handled and protected at the equivalent level of SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL respectively.

**Note 3 France:** France handles and protects CONFIDENTIEL UE/EU CONFIDENTIAL information in accordance with the French security measures for protecting SECRET information.

**Note 4 France:** France does not use the classification 'RESTREINT' in its national system. France handles and protects RESTREINT UE/EU RESTRICTED information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union. France will handle classified information bearing the national classification markings of RESTRICTED level in accordance with its national rules and regulations in force for 'DIFFUSION RESTREINTE'. The other Participants will handle and protect information marked 'DIFFUSION RESTREINTE' according to their national laws and regulations in force for the level RESTRICTED or equivalent, and according to the standards defined in the present document.

**Note 5 Germany:** VS = Verschlusssache.

**Note 6 Portugal and Spain:** Attention is drawn to the fact that the markings RESERVADO used by Portugal and Spain refer to different classifications.