European Defence Fund (EDF)

Call for proposals

EDF-2024-DA

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

Version 1.0
15 April 2024

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	15.04.2024	– Initial version.	
		–	
		–	
		–	

EUROPEAN COMMISSION
Directorate-General for Defence Industry and Space

DEFIS.A – Defence Industry

CALL FOR PROPOSALS

TABLE OF CONTENTS

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[1])

  – STEP Regulation 2024/795[2].

The call is launched in accordance with the Work Programmes 2024 Part II[3] and 2025 Part I[4] and will be managed by the **European Commission, Directorate-General for Defence Industry and Space (DG DEFIS)**.

⚠ Please be aware that, if selected, the Commission may decide that some projects are afterwards managed by entrusted entities such as, but not limited to, the European Defence Agency (EDA) or the Organisation Conjointe de Coopération en Matière d'Armement/Organisation for Joint Armament Co-operation (OCCAR). Management by OCCAR has already been identified for the project(s) relating to the topic EDF-2024-DA-C4ISR-MALE.

The call covers the following **topics**:

  – **EDF-2024-DA-C4ISR-AIMA-STEP: AI-based multifunctional aperture and transceiver**

  – **EDF-2024-DA-C4ISR-COMS-STEP: Defence multi-dimensional communication standard**

  – **EDF-2024-DA-C4ISR-SEEU-STEP: Small enhanced European UAS**

  – **EDF-2024-DA-C4ISR-MALE: Medium altitude long endurance RPAS**

  – **EDF-2024-DA-CYBER-NGCR-STEP: Next-Generation Cooperative Cyber Range**

  – **EDF-2024-DA-SPACE-EPW-STEP: Secure waveform for satellite communications**

  – **EDF-2024-DA-ENERENV-EEMC-STEP: Energy-independent and energy-efficient systems for military camps**

  – **EDF-2024-DA-AIR-NGRT: Next generation rotorcraft**

  – **EDF-2024-DA-GROUND-UGS-STEP: Multipurpose unmanned ground systems**

---

[1] 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).

[2] Regulation (EU) 2024/795 of the European Parliament and of the Council of 29 February 2024 establishing the Strategic Technologies for Europe Platform (STEP), and amending Directive 2003/87/EC and Regulations (EU) 2021/1058, (EU) 2021/1056, (EU) 2021/1057, (EU) No 1303/2013, (EU) No 223/2014, (EU) 2021/1060, (EU) 2021/523, (EU) 2021/695, (EU) 2021/697 and (EU) 2021/241 (OJ L, 2024/795, 29.2.2024).

[3] Commission Implementing Decision C(2024) 1702 final of 15.03.2024 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 II.

[4] Subject to adoption later in June 2024.

- **EDF-2024-DA-GROUND-BLOS: Beyond the line-of-sight close combat**

- **EDF-2024-DA-GROUND-AIFV: Next generation armoured infantry fighting vehicle**

- **EDF-2024-DA-NAVAL-FNP: Functional smart system-of-systems under an integral survivability approach for future naval platforms**

- **EDF-2024-DA-UWW-AHMS: Autonomous heavy minesweeping system**

- **EDF-2024-DA-SIMTRAIN-STME-STEP: Simulation and training for medical emergencies**

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 2024 part II and 2025 part I, this call covers thematic topics addressing **development actions** which will be implemented through actual cost grants.

STEP

The following topics contribute to the objectives of the Strategic Technologies for Europe Platform (STEP):

– EDF-2024-DA-C4ISR-AIMA-STEP: AI-based multifunctional aperture and transceiver

– EDF-2024-DA-C4ISR-COMS-STEP: Defence multi-dimensional communication standard

– EDF-2024-DA-C4ISR-SEEU-STEP: Small enhanced European UAS

– EDF-2024-DA-CYBER-NGCR-STEP: Next-Generation Cooperative Cyber Range

– EDF-2024-DA-SPACE-EPW-STEP: Secure waveform for satellite communications

– EDF-2024-DA-ENERENV-EEMC-STEP: Energy-independent and energy-efficient systems for military camps

– EDF-2024-DA-GROUND-UGS-STEP: Multipurpose unmanned ground systems

    – EDF-2024-DA-SIMTRAIN-STME-STEP: Simulation and training for medical emergencies.

Business coaching

The EDF also has a business coaching component. Successful SME beneficiaries will be offered business coaching, to accelerate their growth and guide them in their business challenges to reach the defence market.

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 (**generating knowledge**)	*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 (**integrating knowledge**)	65%	+ 10%	+ X% *(see table below)*	+ X% *(see table below)*	+ 10%	up to 100%
(c)	**Studies**, 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%

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		
(d)	**Design** 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)	**System prototyping[5]** 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)	**Testing** 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)	**Qualification[6]** of a defence product, tangible or intangible component or technology	70%	+ 10%	+ X% (see table below)	+ X% (see table below)	+ 10%	up to 80%
(h)	**Certification[7]** 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 **increasing efficiency** 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)
PESCO bonus	Project developed in the context of a project of the permanent structured cooperation (PESCO)[8]	+ 10%

---

[5] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[6] '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.

[7] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[8] 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).

Type of bonus	Condition	Bonus *(additional number of percentage points to the baseline funding rate)*
SME[9] bonus (non-cross border)	Proportion of eligible costs allocated to SMEs (beneficiaries, affiliated entities and subcontractors involved in the action; not associated partners)	+ % of the proportion of eligible costs allocated to non-cross-border SMEs[10] (up to maximum 5%)
SME bonus (cross-border)	≥ 10% (for the activity concerned)	+ twice the % of the proportion of eligible costs allocated to cross-border SMEs[11]
Mid-cap bonus	Proportion of eligible costs allocated to mid-caps[12] (beneficiaries, affiliated entities and subcontractors involved in the action; not associated partners) ≥ 15% (for the activity concerned)	+ 10%

⚠ 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)*

EDF-2024-DA-C4ISR-AIMA-STEP: AI-based multifunctional aperture and transceiver

---

[9] 'SMEs' means small and medium-sized enterprises as defined in the Annex to EU Recommendation 2003/361/EC.

[10] '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.

[11] '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.

[12] '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.

Objectives

General objective

To cope with multi-dimensional warfighting environments, modern militaries need relevant situational awareness across all domains. They also need to be able to both operate cross-domain capabilities, such as any-sensor-to-any-shooter networking, and prevent the enemy from doing so. This requires communications systems that can perform ad hoc networking in all domains in dynamically evolving tactical situations. Currently, this is done with mobile ad-hoc networking (MANET) data links.

As wireless solutions such as the Internet of Battlefield Things proliferate, the electromagnetic spectrum is likely to become an increasingly important source of situational awareness. Passive electronic monitoring, detection, classification and localisation of enemy radio frequency emitters is part of the recognised situational picture. Traditionally, this has been the task of electronic warfare (EW) units and their specific equipment providing electronic support (ES) to combat units.

To counter a detected threat, forces can use kinetic- (KE) and directed-energy (DE) means with their weapon systems, or electronic protection (EP) and attack (EA) if they have jamming systems, traditionally equipment carried and used by dedicated EW units. Before directing fire at detected targets, soldiers must mitigate the risk of friendly fire. At long ranges and in poor visibility, this requires radio communications with either self-positioning based Blue Force Tracking (BFT) or interrogation-based Identification Friend or Foe (IFF).

Today, MANET data links, ES receivers, jammers, BFT and IFF are separate pieces of equipment requiring decentralised control, separate installation space, power supply, cabling, antennas, etc. By combining these functionalities into a single autonomously controlled equipment, it would be possible to achieve better performance, higher reliability, lower weight and lower life cycle costs.

In addition to the aforementioned technological reasons for converged aperture, there is also a need for converged systems. The electromagnetic spectrum (EMS) is expected to continue to be contested, congested and constrained. Military use of the EMS is under serious pressure from the civil community. Civilian, dual-use and military applications intermingle in the EMS currently in use, challenging the freedom and security of operation (OPSEC) of military users. With Software Defined Radio (SDR) technology, systems are likely to be able to dynamically perform mission and threat analysis, situational awareness, positioning and navigation, and jamming. This means dynamic adaptation to prevailing conditions at machine speed. This would require AI-based operation at the device and system of systems (fleet/network) level in order to coordinate actions of several systems with minimal detectability and platform losses.

Specific objective

The specific objective of this topic is to design, develop and build a system that should:

– Accelerate command and control (C2) and enhance operational effectiveness by providing cross-domain mobile ad-hoc networking capabilities to the armed forces.

– Increase lethality by enabling faster firing and reducing the risk of collateral damages, including fratricide, by providing the means to detect and target the enemy and to locate, track and identify friendly forces.

– Reduce enemy lethality and increase own protection by avoiding detection with

AI-based emission control, stealthy waveforms and by jamming enemy communications.

- Provide autonomous mission management of several systems (including detection, jamming and targeting) within the network in order to improve survivability, and autonomously take actions to meet the mission objectives with the aid of AI.

- Be capable of operating in all weather conditions, in particular in the challenging Arctic environment and Global Navigation Satellite System (GNSS) denied areas.

Scope and types of activities

Scope

Proposals must address study, development and qualification of new generation scalable and cognitive (AI-controlled) multifunctional software defined (SD) transceiver for military use in manned and unmanned platforms. The ultimate objective of the proposals must be to achieve a qualified prototype for end-user demonstrations with a view to obtain end-user commitment for operational use.

Proposals may also provide a framework for the development of new standards, including proposals for intelligent and effective spectrum management, and prepare to contribute to future standards. The design approach should focus on building a system capable for series production and scalable for product families.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[13] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[14] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[15] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

– Studies:

  – Study different technological approaches, materials and study of end-user needs and requirement specifications including relevant applicable standards, such as NATO standards, which are eligible for all weather conditions, including for the northern and arctic environment.

– Design:

  – Design the architecture according to preferably NATO Architecture Framework (NAF) model 4.0[16];

  – Select applicable technologies;

  – Design the needed modules;

  – Integrate and provide a proof of concept.

– System prototyping:

  – Manufacture all functional modules and prototypes;

  – Ensure manufacturing ability with efficient supply chain.

– Testing:

  – Perform laboratory and field testing in relevant operational environment (e.g. HWIL[17], real spectrum), as well as functional testing, to:

---

[13] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[14] '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.

[15] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[16] AC/322-D(2018)0002-REV1/ENG/NHQD204550 (nato.int)

[17] Hardware in the loop.

- Evaluate system functions and EW performance (e.g. ESM, anti-jamming, jamming);

- Verify functions and properties against technical requirements;

- Validate requirements against operational needs and mission requirements.

- Analyse evaluation results and provide feedback for continuous design improvements.

Regarding the optional activities, proposals may also address, where applicable:

- Qualification:

  - Qualify the transceiver (functional, cyber, EW, environmental and electromagnetic compatibility (EMC)) for multi- and cross-domain use.

- Certification:

  - Ensure transceiver certifications by independent relevant body, such as authority or aircraft Original Equipment Manufacturer (OEM).

- Increasing efficiency:

  - Ensure smart power consumption, efficient transmitter power control and smart communications Radiofrequency (RF) spectrum usage;

  - Converge and integrate different functions to increase their control efficiency and maximise the operational endurance and survivability of smaller platforms.

The proposals should substantiate synergies and complementarities with foreseen, ongoing or completed activities, notably those described in the call topics PADR-EMS-03-2019[18] related to *Electromagnetic spectrum dominance*, as well as in EDF-2021-SENS-R-RADAR[19], EDF-2022-RA-SENS-ART[20] and EDF-2024-RA-SENS-ART related to *Advanced radar technologies.*

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

---

[18] Funding & tenders (europa.eu)
[19] Funding & tenders (europa.eu)
[20] Funding & tenders (europa.eu)

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).

For more information, please check *section 6*.

Functional requirements

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

A- <u>General functional requirements</u>

– The proposals should address the development of a new multifunctional transceiver which supports the following application-based functionalities: data link, secure digital voice, BFT, electronic support measures (ESM), EP and EA.

– The proposed design should be suitable for operations in future challenging environment and conditions, including operations in GNSS denied areas and under jamming, non-stop operations in all weather conditions, including arctic ones, and operations in congested, contested and constrained spectrum environments.

– The proposed design should support cooperation across the transceiver nodes (at least in surveillance and engagement) based on swarm intelligence operating in centralised and distributed architecture and address the needs for an AI-based mission management system of autonomous transceiver fleet.

– The design and architecture should be modular, Size, Weight, Power, and Cost (SWAP-C) scalable and support miniaturisation.

– The proposals should address convergence of common design for all platforms. The miniaturisation should lead to cost-effective manufacturing resulting in an affordable solution to all EU Member States and EDF Associated Countries, using various platforms with different requirements (future platforms as well as existing legacy platforms through Mid-Life Upgrades), also in the northern countries and arctic environment.

– The proposed system should support efficient and adaptive use of wide RF spectrum, transmission power, bandwidth and waveform features based on situational and operational conditions using artificial intelligence (AI) in analysis and control.

– System and hardware design should comply with open system architecture.

– Hardware and software architectures should support integration of several different software (SW)-based applications.

– Hardware should include low-cost solutions (e.g., sector antennas) and support high-performance solutions (e.g., active electronically scanned arrays (AESA)), possibly with the following capabilities:

– Beamforming with as high directivity as applicable;

– Covering the RF spectrum required for the targeted functionalities;

– Antenna solutions allowing for integration in platform structures (conformally when required). The proposed system should be compatible with applicable standards, such as NATO standards, and requirements and allow multi-domain interoperability in joint force operations.

B- Multifunctioning requirements

– Possibilities for the use of a direct conversion receiver should be included.

– Simultaneous multifunctionality of dynamic networking, secure digital voice, data link, BFT, ESM, EP/EA and transceiver control is the core feature of system requirements.

– RF and transceiver resource management and interoperability of two or more simultaneous applications (e.g., data link, ESM and EP/EA) should be controlled by a smart cognitive process, including for example:

  – Optimising the balance between unwanted RF emissions / interference between transmit-receive functions and communication requirements;

  – Continuous wideband RF sensing and application resource management.

– Transceiver should use simultaneously transmitting and receiving operation for all required tasks and functionalities.

  – The in-band full duplex (FD) mode may be utilised to improve spectrum usage efficiency.

– Proposals should include emissions control (EMCON) scheme in stealth operation conditions allowing network nodes to continue operation under restricted or no RF emission and continue active operation with acceptable delay.

– System positioning, navigation and timing and blue force tracking applications should use cognitive information fusion based on relevant sources to be provided by the proposed solution (such as GNSS, data link proportional navigation, ESM direction finding to known emitters and ground control support) and, when available, other sources (e.g., georeferencing (SAR, E/O visual and IR), stellar navigation, inertial, etc.).

C- Communication and networking requirements

– Networking should support multi- and cross-domain operations between different ground-based, airborne and naval platforms, as well as command and control entities.

– Networking should be scalable to different numbers of participants and applications, such as:

  – Real-time small-unit communications, e.g., swarming support;

  – Wide area information distribution for applications, such as blue-force tracking.

– Networking should support mesh topology with directional transmissions, providing self-configuration and self-healing capabilities.

– Networking should support smart datalink and dynamic traffic management according to user/mission policies/rules and overall situation.

– The system should be able to maintain connections to other nodes in the network in all possible directions (6 Degrees of Freedom (DOF) when using highly manoeuvrable platforms.

− The system should manage and control traditional passive antennas as well as active antenna beamforming and beam pointing (single/multiple) in 3D environment.

− Communication waveforms should provide robust Lower Probability of Intercept (LPI), Lower Probability of Detection (LPD), Lower Probability of Exploitation (LPE) and Interference/Jamming avoidance capabilities by using active, AI-based dynamic transmission control.

− Communication waveforms should use modern MIMO (Multiple-In Multiple-Out) beamforming techniques.

− The system should provide comprehensive support for Internet Protocol (IP) and commonly used networking standards.

− The system may support multiple loadable waveforms, including third party waveforms, and providing interoperability with other systems.

− The system may fulfil end-user communication and transmission security requirements, including support for Red/Black separation.

D- <u>Electronic warfare (EW) requirements</u>

− Signal detection and emitter recognition should be AI-based and should be capable of countering cognitive radars and threats with unknown waveforms.

− Signal detection, recognition and geolocation of targets and threats should support cooperative and distributed sensing to enhance detection of distant LPI/LPD targets.

− All system functions should be resilient to jamming and interference by EP, including, but not limited to:

  − Utilising selective directivity of antenna array (sector or active beamforming) which can reject (e.g., null steering) multiple jammers;

  − Adapting EP processing gain (bit rate and instantaneous bandwidth) by using cognitive spectrum management according to information transmission needs and operational situation;

  − Swarm level cognitive EP based on coordinated formation flying and use of data link (beam steering and routing);

  − By having high dynamic range receiver to allow observing and detecting signals with high dynamic in received power.

− System should be able to enable smart EA functions from single to multiple targets in coordinated manner with autonomous EA control process (e.g., AI-based), including, but not limited to:

  − Coordinated stand-in and stand-off jamming where all platforms within the jammed target's range are using different jamming strategies in a coordinated manner (brute force or intelligent jamming, i.e., noise or equivalent method or repeating jamming or equivalent)

  − Utilising antenna directivity (sector or active beamforming) to selectively transmit EA RF waveforms to directions of the targeted platforms.

Expected impact

The outcome should contribute to:

– Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

– Maintain and enhance European sovereignty and information superiority for critical communication systems and capabilities.

– Decrease dependencies from non-EU technologies and products to support long-term targets of EU Member States and EDF Associated Countries.

– Enhance and support EDTIB[21]'s goals and position in global markets.

– Facilitate multi- and cross-domain operations with increased information superiority capabilities from various Member States and EDF Associated Countries.

– Comply with the joint forces' needs of manned and unmanned platforms and of command entities, at all operational levels.

– Support enhanced, safe and secure operations in friendly and hostile environment with new innovative modular, scalable, and multiuse interoperable RF transceiver technologies and adaptive use of radio frequencies assisted by Artificial Intelligence algorithms and characteristics.

– Equip troops and platforms of various sizes and domains with beyond the state-of-art interoperable and multifunctional communication and electronic warfare systems that are suitable for demanding tactical operations also in GNSS denied environment and arctic climate conditions.

– Enable the joint forces of the Member States and EDF Associated Countries for secure, timely and accurate data transfer and communication in multi- and cross-domain environments combined with efficient ESM and EP/EA capabilities.

– Expand EDTIB's capabilities to produce new highly innovative and interoperable communication and information systems based on tactical multifunctional software defined radio and networks, as well as new generation systems that enhance survivability and operations in future battlefield.

EDF-2024-DA-C4ISR-COMS-STEP: Defence multi-dimensional communication standard

Objectives

General objective

5G is a technology originally developed to address the ongoing rapid pace of digital transformation of the different vertical industries in the civilian world. It is continuously being developed through standardisation activities in 3GPP[22], and new releases with extended features of the standard are approved approximately every 18 to 24 months.

---

[21] European defence technological and industrial base.
[22] 3rd Generation Partnership Project.

To ensure a technological edge in military use of 5G, it is important to capitalise on the continued momentum of new releases and associated features relevant for military operations. In 2016, resilience in civil communication systems was listed by NATO as one of seven baseline requirements that each Member State should measure their level of preparedness. In November 2019, this requirement was updated by NATO Defence Ministers, who stressed the need for reliable communications including 5G.

To address this statement and ensure a higher degree of robustness and resilience in military operations when operating in the tactical edge, the militaries should be able to exploit and seamlessly interact with civilian infrastructure to ensure uninterrupted services for tactical command and control applications.

This topic focuses on system level integration and orchestration of 5G technologies for seamless interaction of private military and public 5G networks. Hence, the overall objective is to support the need for an always connected concept enabling military applications to roam securely through a mix of private and public networks. To achieve this, there is a need to study, develop and demonstrate how the military can exploit seamless and uninterrupted transfer of secure applications and services in a coverage area served by a mix of private military and public 5G networks, including BLoS (Beyond Line of Sight) through Non-Terrestrial Network (NTN) communication systems integrated in 3GPP standard.

Specific objective

The specific challenge of this topic is to demonstrate robust and dynamic operational capabilities of 5G connectivity solutions matching the military needs for tactical command and control applications and services.

The solution should always be connected via a hybrid form of networks, while ensuring secure communications, using tactical networks, private military and public 5G networks and other federation solutions. The use of flexible reach back solutions such as 5G NTN is also necessary to reach shared centralised cloud services.

Within this context, secure integration of commercial and military hardware, software and services is a fundamental challenge that must be addressed on both a technological and a commercial level.

Scope and types of activities

Scope

Proposals must address the development of either integrated private-public 5G system architectures for military operations, or private military 5G networks, or public 5G services for military applications.

Moreover, proposals should lead to the development and demonstration of case-agnostic technical products and services, applicable to military operations across all dimensions of warfare. The demonstrations should be performed in relevant operational environments and cover all aspects from devices, infrastructure, security, and simplified orchestration of the overall system.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[23] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[24] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[25] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

Accordingly, the proposals must cover at least the following tasks as part of studies mandatory activities:

– Perform feasibility studies to explore the feasibility of new or improved technologies, products, processes, services, and solutions for 5G military applications.

– Study the concept of 5G Network-as-a-Sensor[26], targeting future capabilities of using a mix of private and public 5G networks for RF reconnaissance enabled by third party applications through an Open RAN[27] API[28].

---

[23] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.
[24] '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.
[25] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.
[26] 5G Network-as-a-Sensor may have the potential to serve as a sensor to detect and locate jammers, detect false base stations (based on reports from users' equipment), detect drones, etc.
[27] Radio Access Network.
[28] Application programming interface.

- Set up simulation or emulation tools of mobile networks and/or associated applications, enabling improved understanding of current network situations (i.e., analysis) as well as of future configurations and deployments (i.e., predictions).

- Demonstrate that 5G works for private networks in different frequency bands, such as ISM[29] bands (5G, for 5G unlicensed), in NATO bands (e.g., 4400-5000 MHz, 225-400 MHz, etc.).

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of communications, notably those described in the call topic EDF-2021-C4ISR-D-COMS[30] related to *Robust defence multi-dimensional communications*.

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).

For more information, please check *section 6*.

Functional requirements

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

A- Operational requirements:

- Ensure that troops and military assets are always best connected with interoperability capabilities to use multiple networks.

- Provide worldwide connectivity through the integration of 5G NTN.

- Dedicated 5G defence slices in public networks for tactical command and control applications.

- Robust, resilient, secure, and manageable roaming across private and public network.

---

[29] Industrial, scientific, and medical.
[30] Funding & tenders (europa.eu)

– Robust tactical applications and services that can operate locally even when communication with central services is lost.

– Making use of existing civilian networking infrastructure in military operations.

– Allow military private mobile networks operate as extensions of public mobile networks whenever feasible with demands on roaming and interconnect.

– End-to-end military-grade SIM[31] encryption (i.e., through the GSMA[32] standard IoT SAFE[33]).

– Access to terrestrial-based navigation services when GNSS[34] signals are subjected to jamming (e.g., through 5G positioning).

– Automated and simple network setup and operation by military personnel (e.g., through self-organising networks).

– Handling federation and interconnection of private and public 5G networks according to the framework of Federated Mission Networking (FMN).

– Ensure transmission security (LPI[35]/LPD[36]) to protect from interception and exploitation in the spectrum (e.g., spread spectrum, frequency hopping).

– Support of civil-military communication via interworking of military 5G solutions and public solutions, as required for defence operations.

– Leveraging interoperability with LTE[37]/5G support.

B- Technical requirements:

– Utilising 3GPP 5G standards (5G RAN, 5GC[38]) and connected applications (e.g., NR[39], network slicing, FWA[40], NTN).

– 5G Stand-alone solution for tactical network.

– Redundancy and security for critical solutions, especially solutions considering the needs in terms of confidentiality, integrity, and availability, when facing threats (including cyber threats) corresponding to the military use cases for active cyber defence.

– Interoperability and integration with existing military infrastructure, including through usage of military frequencies for private military 5G applications.

– Leveraging commercial 5G networks and technologies (e.g., network slicing, edge computing, 5G NTN, Open RAN, D2D[41], IoT SAFE[42], etc.).

– Compatible with different frequency bands (e.g., ISM, NATO, etc.), including with Dynamic Spectrum Sharing.

---

[31] Subscriber Identification Module.
[32] Global System for Mobile Communications Association.
[33] Internet of Things SIM Applet For Secure End-2-End Communication.
[34] Global Navigation Satellite System.
[35] Low probability of interception.
[36] Low probability of detection.
[37] Long term evolution.
[38] 5G Core network.
[39] New Radio.
[40] Fixed wireless access.
[41] Device to device.
[42] Internet of things SIM Applet For Secure End-to-End Communication.

Expected impact

The outcome is expected to contribute to:

– Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

– Create a European ecosystem for secured 5G devices and infrastructures, including hybrid networks (utilising both civilian and military radio technologies), configuration and management tools and cyber security fit for military use.

– Prepare the ground for the use in defence operations of next generation communication standards (e.g., 6G).

– Demonstrate the adaption of an appropriate industry standard to military needs.

– Orchestrate services across multiple administrative domains through the concept of federation.

– Provide worldwide 5G connectivity for operations through the integration of NTN.

EDF-2024-DA-C4ISR-SEEU-STEP: Small enhanced European UAS

Objectives

General objective

Despite the extensive use of COTS[43] UAS[44] in recent conflicts and continued technological development, these systems serve the purpose of rapid and relatively low-cost deployment of assets and effectors in times of extreme need. As with all such systems, there is a lack of key requirements and an overall development and sustainability frameworks that meets the real needs of defence users at the tactical level in the EU Member States and EDF Associated Countries. It should be noted, however, that large UAS are always challenging to operate due to their specific needs, e.g., regarding facilities, maintenance and support.

Anticipated advances in miniaturisation and communication protocols are likely to provide sufficient ground for improvements in the area of small UAS[45] for defence applications and their associated payloads, including weapons, without the stringent need for large UAS. Such activities are embedded in very promising prospects for further industrial and operational development.

Against this background, this topic aims to have a direct impact on the tactical operational effectiveness of armed forces in multi-domain operations (air, land and maritime). In addition, the outcome of this topic is also expected to improve the intervention capacity of relevant national or European agencies.

Specific objective

In particular, this topic intends to contribute to address the following specific challenges that small UAS are prone to:

---

[43] Commercially available off-the-shelf.
[44] Unmanned Aerial Systems, including Remotely Piloted Aircraft Systems.
[45] i.e., Class I RPAS (>15 kg and <150 kg) according to NATO STANAG 7232, Ed. 1, 13 Jan 2020, ATP 3.3.8.1. Training of unmanned aircraft systems (UAS) operators.

–   Low UAS signatures and extended operational ranges;

–   Operate autonomously and automatic, including with assisted piloting considerations;

–   Miniaturisation of sensors and payloads, including potential weapons and communication systems;

–   Operational capability and survivability in contested, congested and challenging (e.g., weather) airspace.

Scope and types of activities

Scope

Proposals must address the development of a small UAS with advanced ISTAR[46] capabilities, such as real-time imagery intelligence, and possibly kinetic capabilities, capable of operating in support of the widest possible range of military operations.

In addition, proposals should address the development of a multi-role approach that explores compatibility between different payloads and configurations, in particular through an Interoperable Modular and Scalable Architecture (IMOSA) approach to allow interchangeability of components and interoperability between different solutions, including a "plug and play" capability for sensors and possible effectors.

As the small UAS cannot support sets of different sensors due to weight, space and power limitations, the possibility of standard interfaces should be explored to allow the selection and integration of a variety of specific sensors to be used in different configurations depending on the mission, and to facilitate the use in defence, civil and dual-use configurations.

In addition, proposals may also address the potential synergy for use by law enforcement and other governmental use.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)

---

[46]   Intelligence, surveillance, target acquisition, and reconnaissance.

	Types of activities (art 10(3) EDF Regulation)	Eligible?
(d)	**Design** 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)	**System prototyping**[47] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[48] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[49] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

Accordingly, the proposals must cover at least the following tasks as part of mandatory studies activities:

– Develop integration with Combat Management System (CMS) in line with a common standard protocols (e.g. foreseen NATO STANAG 4817).

– Study electromagnetic compatibility in order to integrate the system in a combat system without interferences

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of small and tactical RPAS, notably those described in the call topic EDIDP-ISR-TRPAS-2019[50] related to *Development of a low-observable tactical RPAS with the capability to provide near real time information and with modern self-protection* and in the call topic EDF-2023-DA-C4ISR-TRPAS[51] related to *Tactical RPAS*.

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:

---

[47] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[48] '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.

[49] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[50] Funding & tenders (europa.eu)

[51] Funding & tenders (europa.eu)

- 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).

For more information, please check *section 6*.

Functional requirements

The proposed product and technologies may elaborate on mature and already proven solutions, when available and applicable, and should meet the following functional requirements:

- **Performance requirements**: The prototyped new small UAS platform should:

  - Be of Vertical Take-Off and Landing (VTOL) type, while being:

    - Able to take-off and land automatically in a conscripted area with its own means (i.e., without using external equipment such as net or catapult), e.g., from and to a ship single spot flight deck;

    - Compatible with the performance characteristics of a fixed-wing aircraft, especially regarding speed, range, and endurance, during cruise phases and in over-target flight, meaning:

      - An operational autonomy of at least 10 hours;

      - An operational range of at least 200 km Line Of Sight (LOS);

      - A cruising speed of at least 50 kts.

  - Be equipped with sustainable propulsion system/powertrain, possibly using alternative fuel (e.g., electric propulsion, heavy fuel (JP5) engine, multi fuel engine);

  - Have a reduced acoustic signature to limit detection, recognition and direction finding of the small UAS;

  - Sustain steady winds ≥25 knots with gust of 30 kts;

  - Fly in moderate rain conditions ≥ 5 mm/h;

  - Be able to operate in a temperature range between -20°C and +49°C;

  - Be able to carry a payload of up to 20kg with structural mounting points by design;

- − Be compliant with IP[52] 66 standard;

- − Include a plug and play capability in order to provide flexibility to users.

- **Airspace integration:** The system should be designed and equipped to enable safe deconfliction, transit and operations BLoS[53] in non-segregated airspace.

- **Airworthiness:** The system, including its design, development and construction, should be compliant with applicable standards with a view to future certification.

- **Operational requirements:** The system should:

  - − Have an automated mission profile, configured in real-time, before and during flight;

  - − Have an autonomous flight mode, where the UA[54] could adapt its flight path and take decisions based on the sensing of the environment/scenario;

  - − Have a fly-by-wire assisted flight mode where a human pilot can intervene using a pilot console;

  - − Be capable of automatically taking-off and landing, using its own means;

  - − Include a Manned-Unmanned Teaming (MUM-T) capability;

  - − Be able to operate in swarming formations;

  - − Be resilient to cyber-attacks;

  - − Be operated via a control station with the smallest footprint possible;

  - − Be aero transportable by and launched from e.g., light transport aircraft;

  - − Have a very reduced logistic footprint;

  - − Have the smallest crew for operation possible, considering the remote crew (i.e., remote pilots, systems, cameras and datalink operators), take-off and landing support crew, assistance crew;

  - − Control and monitoring unit software should allow e.g., but not limited to, geofencing, automatic NOTAM[55] creation based on requested flight area, input/upload of areas of interest or limitation (e.g., NOTAM or area of operation), PoI in the MAP, the map layers should be always updated and allow for military and civil maps and charts, the waypoint type navigation should draw the actual flight path of the UAS.

- **Survivability:** The developed small UAS should be able to operate in a contested environment with enemy anti-access/area denial (A2/AD)

---

[52] According to International Electronical Commission (IEC - https://www.iec.ch/) standard 60529 on Degrees of protection provided by enclosures (IP Code).
[53] Beyond the Line-of-Sight.
[54] Unmanned Aircraft.
[55] Notice to airmen.

capabilities, in particular UAS with return and pickup considerations, e.g., via increased protection on the UAS, redundancy and low signatures.

– **Optical gyro-stabilised spread spectrum multi-sensor**: A multi-spectrum sensor suite for small UAS should be capable of visualising, geo-referencing, and tracking multiple moving points of interest (POIs) in adverse weather and visibility conditions.

– **Improved sensing and ISR[56] and targeting systems**:

  – The system should include radar sensors SAR (Synthetic Aperture Radar) and LIDAR (Laser Imaging Detection and Ranging);

  – The development of smaller and more precise systems for ISR and targeting, as well as direction of indirect fires, should be addressed;

  – The system should include electro-optical, infrared (IR) sensors and target illumination (e.g., laser pointer, buddy lasing) capabilities;

  – The system should be able to auto-track fixed and moving targets and support the overall targeting cycle;

  – The system should provide IMINT[57] support to land forces.

– **Communications:**

  – The development of wideband BLoS communications for Small UAS (WB[58] BLOS LEO[59]) combined with Advanced Beamforming LoS with Direction Finding Capabilities, based on the new constellations for LEO satellite communications, should be addressed;

  – The system should be equipped with:

    – Radio receiver and transmitter;

    – An integral Communications sub-system for BLoS UAS C4I[60] datalinks and telemetry transmission;

    – An aerial communications relay and mesh network node payload to enhance or facilitate communications between other ground-based users;

    – An IFF[61] Mode 5/S and ADS-B[62] transponder aerial identification device that can be switched according to operational needs.

– **Artificial Intelligence / machine learning for autonomous and assisted piloting**:

  – The development of an intelligent module on the ground station / control and monitoring unit to process big amounts of data into actionable intelligent information should be addressed, as small UAS can incorporate a limited processing capacity.

---

[56] Intelligence, surveillance and reconnaissance.
[57] Imagery intelligence.
[58] Wideband.
[59] Low Earth orbit.
[60] Command, Control, Communications, Computers, & Intelligence.
[61] Identification Friend and Foe.
[62] Automatic dependent surveillance-broadcast.

- The system should be capable of flying in manual and automatic modes for flight plans and waypoints, with an autopilot capable of maintaining orbital trajectories while observing points, and automatic take-off and landing capability (including safe landing in case of emergency situations).

- The solution developed should be capable of **swarming operations**, acting in a coordinated way and controlled by a single control and monitoring unit.

- **Interoperability**: The developed solution should be interoperable with common standards in force, such as JISR[63] standards (e.g., NATO STANAG 4559[64]), UAV[65] interoperability standards (e.g., NATO STANAG 4586[66]) and C4I[67] interoperability standards.

- The proposed solution should be **affordable by design**, in terms of acquisition and lifecycle costs, including the overall operating, logistics and maintenance costs.

- **Electronic warfare:** The system may include:

    - VHF/UHF jammer capability;

    - Small jammer disposal capability;

    - Automated hold and track of an electromagnetic source.

- **Supply carrier and precision delivery:** The system may include the following capabilities:

    - Airborne launched capability;

    - Automated delivery of cargo;

    - Beacon capability for discoverability.

- **Miniaturised weaponry**: The development of miniaturised weapons may be considered to eventually get weapon-capable small UAS, hence paving the way for a solution to develop small kinetic capability against e.g., lightly armoured targets, including e.g., loitering munitions, small calibre guided missiles and small calibre torpedoes.

- **CBRN**[68] **surveillance**: The developed small UAS may be able to have a standoff or remote CBRN detector as a payload to allow remote detection of CBRN threats, alerting the unit to the proximity of a contaminated threat and allowing time to take protective action.

Expected impact

The outcome is expected to contribute to:

- Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

---

[63] Joint Intelligence, Surveillance and Reconnaissance.
(https://www.nato.int/cps/en/natohq/topics_111830.htm)
[64] NATO NSO NSDD (nato.int) https://nso.nato.int/nso/nsdd/main/standards?search=4559
[65] Unmanned aerial vehicle.
[66] Standard Interfaces of UA Control System (UCS) for NATO UA Interoperability - AEP-84 Edition A https://nso.nato.int/nso/nsdd/main/standards?search=4586
[67] Command, Control, Communications, Computers, & Intelligence.
[68] Chemical, biological, radiological and nuclear.

– The emergence of a commonly agreed EU standard for small UAS to allow a wider European application, interchangeability of sensors and modules, together with adaptability to various types of missions.

– Define commonly agreed EU defence requirements for small UAS.

– Reduce the current dependencies on non-European UAS suppliers.

– Reduce the fragmentation of UAS fleets in European armed forces and reduce the procurement and maintenance costs through economies of scale.

– Promote the interoperability between European armed forces.

– Foster an active European market for the development of interoperable and interchangeable sensors.

– Exploit the synergy with other than defence applications.

EDF-2024-DA-C4ISR-MALE: Medium altitude long endurance RPAS

Objectives

General objective

The 'Medium Altitude Long Endurance Remotely Piloted Aircraft System' (MALE RPAS) is an indispensable capability to facilitate international conflict prevention and crisis management in all phases of operations – especially in the field of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR). Member States and EDF Associated Countries (MS) have already used various types of MALE RPAS in recent operations to provide detection, identification and communication. MALE RPAS could also have a dual use potential.

The EU commonly agreed priorities underline the permanent need to track ships, aircraft and other systems across a wide area of airspace by means of interoperable unmanned surveillance systems capable of operating in all and adverse weather conditions and all types of environments, with assured data integrity. To operate in all types of operational environments, RPAS must be integrated into air traffic management (ATM).

As part of a versatile and robust MALE RPAS, the system should consider the option to incorporate the means for an effective neutralisation of targets that posed a threat to the mission being carried out.

Today, most of the ISR capabilities of the MS rely on non-EU manufacturers in order to carry out their missions. However, due to the sensitive nature of military operations and the restrictions on technology transfer that prevent MS and EDF Associated Countries from fully benefiting from platform adaptation, the development of a fully European MALE RPAS is key to reduce dependency on non-EU solutions and to ensure sovereignty in this area of ISTAR.

It is an overarching objective to strengthen European sovereignty in this strategically relevant area. Hence, this topic is expected to result in a step-changing programme in line with the commonly agreed EU defence objectives and ensuring European strategic autonomy and technological competitiveness in a broad sense.

Specific objective

MALE RPAS reconnaissance includes optical, infrared, radar and signal intelligence sensors and generates geoinformation data. The sensors for optical, infrared and radar reconnaissance are usual configuration parts of a MALE system. As signal

intelligence is often classified for national eyes only, it would be preferable to develop a common pod design, which is suitable to contain the national electronics. The integration effort into the MALE system can be shared with a common pod design. This pod design is also a suitable baseline for additional future sensors.

The ultimate objective is to develop, produce and sustain a system that provides this critical defence capability to respond to future security challenges.

In addition, a strong European supply chain is intended to be developed at all levels to promote the European Defence Technological and Industrial Base (EDTIB) in the long term. The supply chain should not be a pre-determined black box, but is expected to be open to competitive suppliers in a largely open tendering process, with the suppliers for mission-critical or security-relevant systems intended to be EU-based.

Scope and types of activities

Scope

Proposals must address a prototype of a fully European MALE RPAS with an innovative ISTAR and armed ISTAR capability to exceed the capabilities of comparable current systems and the capabilities of systems available at the entry into service time or, at least, be comparable with them. The prototype must be tested with a view to further qualification and certification activities.

Proposals must also address the design and prototype of a common sensor pod for the European MALE RPAS, without affecting the timeline of ongoing activities related to the development of MALE RPAS.

In addition, proposals should address the enhancement of a multi-role approach for the MALE RPAS available with different sensor pod configurations.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[69] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[70] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[71] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

–   Studies:

–   Set up the configurations to be recognised in the design.

–   Define a set of requirements considering the whole products cycle, to be assessed and accepted by supporting MS and EDF Associated Countries.

–   Provide an overview on a suitable configuration for signal intelligence pods for MALE RPAS.

–   Identify, analyse and mitigate critical technical risks especially regarding integration and certification considerations.

–   Perform a life-cycle-cost-analysis and management.

–   Design:

–   Cover detailed design activities after the Preliminary Design Review (PDR) until the System Test Readiness Review (STRR) of the MALE RPAS.

–   Complete a full design process for a common sensor pod to be used with the MALE RPAS.

–   System prototyping:

–   Prototype the MALE RPAS.

–   Prototype a common sensor pod to be used with the MALE RPAS.

---

[69]   'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[70]   '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.

[71]   'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Testing:

    - A flight test campaign must assess certification and qualification considerations for the European MALE RPAS including the common sensor pod.

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of MALE RPAS, notably those described in the EDIDP Work Programme for 2019 and 2020 with reference to the *development of European Medium-Altitude Long-Endurance Remotely Piloted Air System (MALE RPAS)*.

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).

    For more information, please check *section 6*.

Functional requirements

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

A- Regarding the detailed design of the MALE RPAS, the solution should**:**

- Include innovative ISTAR and armed ISTAR capabilities.

- Include widespread types of sensors:

    - Electro-Optical/Infrared;

    - SAR (Synthetic Aperture Radar) with GMTI (Ground Moving Target Indicator) capability;

    - Automatic Identification System function;

    - Personal Locator System.

- Include state-of-the-art means of communications:

    - Secured V/UHF;

    - Air Data Terminal;

- − Tactical datalinks, e.g., L16/JREAP[72] and VMF (Variable Message Format) functionalities;

- − Provision for future ATM and Aeronautical Telecommunication Network (ATN).

- − Include reliable and high-bandwidth C2[73]-/Data-links:

  - − Wideband Beyond Line-of-Sight Data Link;

  - − Wideband Line of Sight Data Link;

  - − Narrowband Beyond Line-of-Sight Data Link;

  - − Narrowband Line of Sight Data Link.

- − Address armament integration considerations.

- − Include an automatic Take-Off and Landing System.

- − Address growth potential considerations:

  - − For ATI equipment (Air Traffic Integration in non-cooperative traffic);

  - − Provisions for future payloads within the scope of ISTAR and armed ISTAR.

- − Ensure long-endurance ISTAR operations (no less than 26 hours).

- − Be certifiable (acc. to STANAG 4671 Ed. 3, Draft Sept 2014[74]).

- − Include a ground Control Station taking latest HMI-related scientific expertise into account.

- − Be transportable by air, land and sea standard means.

B- Regarding the development of a pod for the European MALE RPAS, the solution should**:**

- − Study signal intelligence configurations for MALE RPAS, specific for European MALE RPAS for a common pod design for European MALE RPAS supporting MS and EDF Associated Countries.

- − Analyse possible other sensor configurations, like geoinformation data generation for a common pod design.

- − Perform risk management for the development of a common pod, especially for integration, certification and qualification issues.

- − Create a set of requirements to be assessed and accepted by supporting MS and EDF Associated Countries.

- − Design a common pod shell according to the set of requirements with a Critical Design Review.

- − Produce a system prototype for flight test campaign with the European MALE RPAS.

---

[72] Joint Range Extension Applications Protocol.
[73] Command and control.
[74] NSO NSDD (nato.int)

- Define and perform a flight test campaign to prepare for further qualification and certification of the European MALE RPAS, and report the outcome in a flight test report

Expected impact

The outcome should contribute to:

- European sovereignty for ISR platforms.

- The emergence of a certifiable and air traffic integrated European MALE RPAS.

- Improve interoperability of EU Member States Armed Forces.

EDF-2024-DA-CYBER-NGCR-STEP: Next-Generation Cooperative Cyber Range

Objectives

General Objective

Cyber range technologies have seen notable uptake over the last decade. They form a cornerstone of cyber defence training and testing. The objective of this topic is to take further the ongoing cyber range technology roadmap by designing and implementing next-generation solutions. The key consideration is on the cooperative approach in developing and using those cyber range technologies, thereby facilitating joint capability development.

Technological investments and developments have so far mostly focused on various fundamental needs such as visualisation, scoring, realistic scenarios, and federation. Separate mature technological building blocks exist in modern cyber and IT solutions. However, these developments have yet to be consolidated into the context of cyber ranges for defence purposes, in a manner such as the PESCO project *Cyber Ranges Federation*.

Specific objective

This topic aims to address the remaining challenge on design and development of solutions that deliver notable progress vis-à-vis the current state-of-the-art, including in view of wider technology landscape. This means that focus has to shift from creating cyber ranges that fulfil basic needs to cyber ranges that target next-level capability requirements. Therefore, the specific objective is about the use of cyber ranges for trainings and exercises. The proposed solutions, however, can benefit also other cyber range use-cases such as product development and penetration testing. Therefore, considerations of such use-cases may be taken into account for developing the solutions.

Scope and types of activities

Scope

The next-generation cooperative cyber range capability must address at least the following issues:

1. Set up of trainings and exercises with classified information, especially for cross-border exercises by EU Member States and EDF Associated Countries.

Although the use of classified information in national exercises and trainings is not a new phenomenon, it is, firstly, still absent from the capabilities of many nations and, secondly, there is no existing solution that offers an EU-wide, cross-border classified

capability. Such a capability could help various countries in using this functionality which they otherwise would not be able to use and it would provide a currently unavailable solution to conducting exercises across nations, including for topics such as information sharing and ensuring confidentiality of related data. This would also benefit the EU's military structure, e.g., EU Military Staff, European Defence Agency and others.

Moreover, such a capability can be used by nations internally, e.g., for its different security agencies both in defence and national security to increase interoperability.

2. Set up of trainings and exercises covering the entire chain of cyber defence operations from planning through conduct up to review, including by utilising realistic mission networks.

Most large-scale technical cyber exercises that are currently conducted do not sufficiently cover all relevant aspects of cyberspace operations. While such aspects are sometimes covered in non-technical exercises, these tend to not sufficiently well incorporate technical cyber defence teams. As a result, truly comprehensive and effective exercises are difficult to deliver.

The aspects that surround these technical activities (e.g., operation planning, legal considerations) and which complement incident management (e.g., intelligence activities) require different scenarios and different technical exercise environments in comparison to existing capabilities. The latter also includes the challenge of creating realistic federated mission networks for training purposes.

Key aspects in this entire chain are also the analysis of the performance of the cyber operators and the scoring of cyber security situational awareness.

3. Leveraging Artificial Intelligence throughout the delivery of trainings and exercises (e.g., for Blue, Red, White and Green Teams)

The use of AI in different phases and parts of cyber exercises and trainings has been researched and developed to an extent. This includes, for example, AI-based scenario generation[75], and AI-based Red/Blue Teams with hybrid skills (human + AI-based attack/defend strategies (developed in different private companies). AI also plays a pivotal role in generating comprehensive situational awareness for the development of realistic federated missions.

In the area of federated missions, which employ multiple teams operating from different locations, AI technologies could help to identify the operational deficiencies within each team member, informing subsequent training customisation and generating tailored scenarios.

It is clear that AI can assist in these and in other parts of cyber capability development. The proposals are expected to provide AI-based solutions that target all major parts of cyber exercise and training delivery, as well as AI-based solutions for the performance evaluation of the trainees using the hybrid skills.

4. Set up of trainings and exercises that leverage the concept of digital twins.

Digital twins[76] as a concept has a long history. The use of such solutions in cyber exercises has also been targeted previously but not with results that have been

---

[75] Such as ENISA November 2021: Foresight challenges: A study to enable foresight on emerging and future cybersecurity challenges.

[76] A Digital Twin is a virtual representation of a connected physical asset, American Institute of Aeronautics and Astronautics (AIAA), "Digital Twin Definition & Value," 2020.

sufficiently persistent or useful. Therefore, the challenge remains on developing digital twins or other high-fidelity simulations that have a reasonable cost-effectiveness – given that a common dilemma in such simulations is finding a balance between cost of creating such digital copies and the learning impact that those simulations can offer on top of more standardised ways for IT/OT system and network simulations. One possible avenue for successful balancing of these requirements may be witnessed in the space domain, given its increased need for simulations and testing.

5. Develop or facilitate a framework for accreditation of training centres and personnel skill levels.

The solutions should include a proposal on how to establish certified practices for accreditation of training centres (cyber ranges) and skill levels (personal and team certificates). The solution should take into account EU-wide accreditation schemes. However, these should allow for national specificities. Where possible, existing standards, such as relevant NATO practices, should be used.

6. Cross-cutting items

All solutions must address the **challenge of sharing and pooling cyber range capabilities** in a coordinated manner between cyber range providers. This challenge may be best addressed by using and enhancing existing initiatives and projects. Moreover, this sharing and pooling can be demonstrated, for example, via the implementation of the project's solutions in different cyber ranges through federation. If federation as an approach is used, it is expected that the proposals also cover the business and management side of the federation. This could, for example, formalise in the development of model cooperation agreements that mimic actual needs and have been developed with processes similar to actual processes (twin environments).

Where existing or new cyber range and cyber exercise standards (e.g., for scenario development and game net creation) are covered, the proposal must address the challenge of achieving a wide user-based of the standard. Proposing the use of any such standards without clearly addressing the way forward may invalidate the whole part of the proposal related to such standards because the success of a standard is as much dependent on the community as the standard's actual content.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)

Types of activities (art 10(3) EDF Regulation)		Eligible?
(d)	**Design** 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)	**System prototyping**[77] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[78] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	**Certification**[79] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

– Studies:

- Identification of additional challenge(s) with a comparable level of complexity as those specifically listed above (scope, items 1-6).

- Definition of capability statements for the solutions to all of the items in the scope (1-6).

- Assessment of the feasibility of achieving the capability as per the capability statements.

- Based on the feasibility assessment, definition of the most appropriate technical requirements for the solutions.

– Design:

- Design of the solutions for each of the listed items in the scope (1-6).

– System prototyping:

- Development of one or more system prototypes for each of the solution that target the items in the scope (1-6).

– Testing:

---

[77] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[78] '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.

[79] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Testing of all of the prototypes developed under system prototyping.

- Testing of one or more system prototypes at least in:

  - One new live-fire cyber demonstration with 3 or more EU Member states/EDF Associated Countries, organised by the consortium

  - One existing live-fire cyber demonstration with 3 or more EU Member states/EDF Associated Countries (e.g., in an exercise that is part of a series where at least one exercise has been held and where the exercises are held irrespective of the current topic).

- Qualification:

  - Qualification of the system, systems or system components for one or more of the system prototypes;

In addition, the proposals should cover at least the following tasks:

- Studies:

  - A supply chain analysis in the area of cooperative cyber range technologies, addressing critical dependencies for the EDTIB.

- Design:

  - Design of the solutions to items relevant for future cyber ranges beyond the mandatory items stated in the scope and in the mandatory tasks.

- Prototyping:

  - One or more prototypes of the designs to items relevant for future cyber ranges beyond the mandatory tasks.

- Testing:

  - Testing of the prototypes beyond the mandatory tasks in at least one live-fire cyber exercise.

- Certification:

  - Certification of the system, systems or system components which are used for the purpose of using classified information.

  - Certification of the system, systems or system components which are used for the purpose of delivering complete cyber operations trainings and exercises. Also, a proposal for accreditation schemes both for training centres and personal certificates (on skill) should be included.

The proposals may cover at least the following tasks:

- Qualification:

  - Qualification of any systems beyond the mandatory tasks.

- Certification, with the meaning of Validation, Verification & Evaluation (VV&E):

  - VV&E of the system, systems or system components which are used for

the purpose of leveraging the concept of digital twins.

- VV&E of the system, systems or system components which are used for the purpose of leveraging AI.

- VV&E of system prototypes designed and delivered beyond the mandatory tasks.

The proposals should substantiate synergies and complementarities with foreseen, ongoing or completed activities, notably those described in the call topic EDF-2021-CYBER-D-IECTE[80] on *Improved efficiency of cyber trainings and exercises*, as well as with activities conducted under Horizon Europe (e.g., DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE[81]).

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).

For more information, please check *section 6*.

Functional requirements

The proposed solutions and technologies should meet the following functional requirements in support of cyber ranges capabilities:

- The proposal should meet the common requirements for next generation cooperative cyber range as defined by supporting armed forces.

- The proposal should enable use of classified information.

- The proposal should provide a complete cyber operations trainings and exercises environment.

- The proposal should be able to measure the performance of the cyber operators, as well as to allow for the scoring of cyber security situational awareness.

- The proposal should, by leveraging AI enabled technologies:

---

[80] Funding & tenders (europa.eu)
[81] Funding & tenders (europa.eu)

- Be able to identify operational lacks within each team member before the organisation of the training exercise.

    - Be able to enrich the training environment by the use of Green/White/Blue/Red teams with features such as hybrid skills (human + AI), game net components, environment enriching user simulation, dynamic amendments of training deliveries, etc.

    - Be able to provide performance evaluation of the trainees using the hybrid skills;

- The proposal should leverage digital twins (may include cyber physical elements), as part of the realistic federated missions to be defined in the different trainings, enabling red teams with AI-based tools to attack the digital asset and blue teams with AI-based tools to defend the digital asset.

- The proposal should enable federating cyber ranges through:

    - Standard solutions to all challenges, which should contain functionalities for sharing and pooling of resources and federation of cyber ranges. For example, through concepts methods, tools, and standards such as HLA[82], or as developed in the context of the call EDF-2021-CYBER-D-IECTE.

Expected impact

The outcome should contribute to:

- Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

- Strategic autonomy of EDTIB in the area of cooperative cyber ranges.

    - Fostering the technological cooperation of industries in the field of cooperative cyber ranges.

- Interoperability of EU Member States and EDF Associated Countries Armed Forces:

    - In the area of cyber defence for cyber mission planning and execution, including through the use of classified information and high-fidelity simulations such as digital twins within the training process;

    - Between civil and military actors;

    - Common requirements and harmonisation of capability development.

EDF-2024-DA-SPACE-EPW-STEP: Secure waveform for satellite communications

Objectives

General objective

In today's military applications supported by satellite communications, security, information assurance and link efficiency are inextricably linked. Military operations are becoming more complex as conflict areas grow more dispersed on a global scale,

---

[82] SISO standard: High Level Architecture for distributed simulation, training and exercises.

a

with a growing need to support a diversity of on-the-move, on-the-pause and fixed platforms. At the same time, security threats are becoming more apparent, raising concerns that nations, terrorist groups, criminals and individual hackers can jam, interrupt and endanger military operations.

In satellite communications, most individual nations cannot generate significant capabilities by themselves. Instead, European nations can generate increased capabilities through cooperation and collaboration. Several pooling and sharing initiatives have already been kicked off in the European defence context to face challenges related to the fragmentation of supply and demand, the assured secure access to satellite communications and the changing environment.

The complexity of dispersed military operations translates into requirements to have access to complex global satellite communication networks with a mix of different satellite constellations, networks and services to support a wide variety of military applications. Security and resilience are key features of today's military satellite networks and are paired with efficiency to cope with the increased data demand of bandwidth hungry services such as ISR and situational awareness, the growing use of on-the-move applications, and the need for seamless end-user experience during operations. However, military satellite communication networks with these wide-ranging requirements face an increased risk of ill-intentioned acts and cyber-attacks such as jamming, signal spoofing and interception attempts.

A key element to tackle this security challenge is the implementation of a protected, resilient and secure satellite communication waveform for fully transparent[83], processed transparent[84] and the new generation processed interactive transponders[85], which at the same time responds to the operational requirements and allows for interoperability during joint operations with allies.

The great majority of Member States do not have independent access to secure satellite communication waveforms, although they also engage in military operations in a national or multinational (EU, NATO, UN peacekeeping, etc.) context. The investment for developing a protected waveform cannot be carried out by a single nation alone and requires a multinational development approach in a European context with the aim to establish a European Protected Waveform (EPW).

Specific objective

This topic aims specifically at further developing a European interoperable protected waveform for satellite military communications that can be used by different EU nations individually or together in a joint operational context (EU, NATO, multi-nation missions). Such European Protected Waveform (EPW) should in particular target efficiency, security, affordability and interoperability of satellite communications. The

---

[83] Transparent transponder: a satellite transponder performing fully analogue handling of the received signals. It re-transmits (repeats) the signals without modifying the received waveforms. A transparent transponder is also known as a bent pipe transponder.

[84] Processed transparent transponder: a satellite transponder performing digital processing of the received signals. It re-transmits (repeats) the signals without modifying the received waveforms. It includes a Digital Transparent Transponder (DTP). Signal processing allows to manage the apportionment and switching of the transponder bandwidth resources.

[85] Interactive Transponder: a satellite transponder, based on digital Software Defined Radio (SDR) technology On Board Processor (OBP), capable of dynamic/adaptive signals regeneration by demodulation and re-modulation of received signals. Signal processing allows to manage the apportionment and switching of the transponder bandwidth resources. The interactive functionalities hosted on-board can provides dynamic routing of data traffic between satellites via inter-satellite links and/or inter-beams/inter-channels, according to a dynamic on-board generated control plane. Furthermore, it could be able to host higher level functions devoted to assist satellite network control and management (i.e., network control centre and/or Traffic Resource Management (TRM)). Interactive transponder is also capable to downlink in regenerative and transparent modes.

EPW should be license-based and flexibly adapted according to the application, service or platform (fixed, on-the-move or on-the-pause) during peacetime or in operations.

Next to the waveform, related technologies should be developed to increase the security and resilience (via integrated multi-layered approach) and adopt the EPW on on-board processing satellites as well as to cater for next-generation technologies.

The targeted development should therefore be undertaken with five key considerations in mind:

1/ European autonomy and cooperation between Member States

The EPW should be capable of increasing the autonomy of Europe and of reducing the dependence on non-European satellite communication technologies for military operations with mission critical and sensitive information. At the same time, it should allow for interoperability between EU nations in a joint operational context to support the exchange of mission critical information and improve the efficiency of the operations.

2/ Affordable and efficient satellite services

The EPW should be affordable and include the latest efficiency satellite communication waveform, networking and equipment technologies to save OPEX (reduce bandwidth costs, require less resources for planning) and CAPEX (reduce equipment cost) compared to current existing expensive (proprietary) military satellite modems. The EPW should include already available innovative Commercial Off-The-Shelf (COTS) satellite communication technologies (e.g., DVB-S2X waveform standard) in combination with the latest security and resilience technologies. There should no longer be a trade-off between the efficiency of the waveform and security. As such, high throughput demands should be achieved even with small satellite terminals using a limited amount of satellite bandwidth.

3/ Flexibility and scalability

The EPW should be portable on different modems with different form factors (board, modem, terminal), different platforms (fixed, on-the-move, on-the-pause) and be used across multiple types of satellite communication networks, different types of satellite constellations (LEO, MEO, GEO, HEO, high-throughput satellites, spot beams, regional and global beams), transponders (fully transparent-, processed transparent- and processed interactive, including software defined radio ones) and different network architectures (VSAT, point-to-point, mesh). At the same time, the EPW should be operational in different satellite frequency bands (at least C-band, X-band, Ku-band and Ka-band) and exchange, broadcast, multicast, unicast or relay a large range of satellite services and applications, including those requiring low latency, from low to very high data rates.

4/ Innovation

The EPW development should not just be a copy and paste of existing waveform solutions, licenses and technologies. The EPW proposal should be ambitious and innovative, combining the individual strengths of different nations and different members in the European satellite communication industry. The EPW programme should be open to support future requirements and capabilities needed.

5/ Security and resilience

The main feature of the EPW should be the increase in protection and resilience of the waveform to ensure secure information exchange over satellite for mission critical

communications. Based on different threat analysis and Concept of Operations (CONOPS) definitions, the EPW development should focus on building satellite links that are resistant to electronic- and cyber-attacks, such as jamming, signal spoofing, eavesdropping and interception attempts. In addition, satellite link outages caused by rain fade, atmospheric and extra-atmospheric (relevant space weather events) conditions, or on-the-move communication challenges should be reduced to a minimum. The EPW activity should investigate how different security levels can be offered towards different military end users depending on their security requirements, their daily operations and the budgets available.

Scope and types of activities

Scope

Proposals must address system prototyping of the baseband equipment (satellite modem), the on-board satellite active transponder and ancillary systems, as well as the testing of all prototypes (modems, on board active transponders and ancillary systems) operating the EPW in a controlled and operational military environment.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (optional)
(d)	**Design** 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 (optional)
(e)	**System prototyping**[86] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)

---

[86] '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)	**Qualification**[87] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[88] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

– System prototyping:

– Develop a breadboard of an SDR Interactive Transponder implementing the EPW enhanced secure mechanisms that includes some of the components and electrical and functional (including digital) performances in order to reach TRL 6;

– Implement the EPW in SDR/ground-based equipment.

– Testing:

– Verify the SDR Interactive Transponder prototype in an end-to-end representative laboratory environment, including anti-jamming capability, user access control (authorised user admission and unauthorised user rejection), signals activity masking, ability to operate in GNSS-degraded or denied environment;

– Test end-to-end service in laboratory environment;

– Demonstrate end-to-end service in satellite environment (TRL 6).

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of satellite communication for defence applications, notably those described in the call topic EDF-2021-SPACE-D-EPW related to *a European protected waveform and accompanying technologies for resilient satellite communications against jamming*[89], as well as with those described in the European Defence Industrial Development Programme (EDIDP) work programme 2019-2020 relating to the European Secure Software defined Radio (ESSOR)[90] and those targeted by the new EU Secure Satellite Constellation[91] IRIS².

Moreover:

– projects addressing activities referred to in point (d) above must be based on harmonised defence capability requirements jointly agreed by at least two

---

[87] '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.

[88] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[89] Funding & tenders (europa.eu)

[90] See section 4.5.2 of EDIDP work programme:
https://ec.europa.eu/docsroom/documents/34515/attachments/3/translations/en/renditions/native

[91] IRIS² (europa.eu)

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).

For more information, please check *section 6*.

Functional requirements

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

System requirements:

– The EPW should be accessible to small, mid-sized and large Member States and EDF Associated Countries seeking to embrace today's and future challenges related to increased throughput demand over satellite, dispersed theatres, joint operations, mobility and new security threats;

– In accordance with this integrated multi-layered security and resiliency approach for military satellite networks, the EPW development should fulfil requirements at the level of the waveform, the baseband equipment (terminals, modems, hubs, networks) and end-to-end satellite network level including multi-band/multi-frequency terminals, anti-jamming technologies, interference mitigation, network diversity, network security and cyber technologies. The demarcation point is the edge router of the satellite network which connects the hubs, gateways and modems with outside networks or the internet.

– Additionally, it should be feasible to implement the EPW also on existing and operational telecommunication satellites;

– The EPW should be resilient and maximise service availability to ensure continuity of seamless operations;

– The EPW should have performances considering the throughput demands of today and the future;

– The EPW should support pooling and sharing service models of both waveform and equipment that can be implemented for different operations;

– The EPW should apply to the best extent possible the set of applicable standards of 5G non-terrestrial network (5G NTN) within 3GPP[92] and take into

---

[92] See 3GPP TS 38.101-5 v18.3 (for user end equipment) and 3GPP TS 38.108 v18.0 (for satellite access node) available here www.3gpp.org/ftp/Specs/archive/38_series/.

account the new use cases and technologies linked to Machine-to-Machine (M2M), Internet-of-Things (IoT), orchestration, cloud-services, the connected soldier and smart defence.

Protected Waveform Requirements:

- The EPW should be defined as a standard to enable interoperability in joint operations.

- Terminals from multiple vendors should be able to support the EPW and be compatible with it;

- The EPW should be affordable, based on the best practices of COTS and government or military-grade waveforms;

- The EPW should implement the most efficient SATCOM technologies to obtain the best performance out of a satellite link;

- The EPW should support a range of different multi-orbit satellite constellations ((V)HTS, wideband, military, commercial, government, HEO, GEO, MEO, LEO), satellite architectures (pure transponder, partially or fully processed) and frequency bands (C-band, X-band, Ku-band, [mil- and civ-] Ka-band) with extension to Q-/V-band to support future SATCOM constellations) and have the capability to roam across the different satellite networks in a seamless manner;

- The EPW should be easy to port on other software defined modems or hubs;

- The EPW should be flexible to support multiple governmental and defence applications that require different levels of security and latency;

- The EPW should implement functionality to support (a growing amount of) on-the-move and on-the-pause platforms connected over the satellite with a need for mobility features (Doppler compensations, spreading modulation, small and flat antenna support, beam switching, beam hopping, etc.);

- The EPW should be able to operate in GNSS-denied environments;

- The EPW should provide adequate protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping;

- The EPW should mask and obscure traffic patterns across the satellite link that could give away activity-related information on ongoing operations and assets;

- The EPW should consider a wide range of throughput requirements and satellite bandwidth sizes (symbol rates) and automatically adapt to changing environments and service requirements;

- The EPW should offer seamless services over resilient satellite links against fading and shadowing effects, unintentional and intentional interference such as jamming (fixed and sweeping);

Multi-layered security & resilience requirements (extended capabilities):

The EPW should be embedded in an integrated multi-layered security and resilience approach to increase the protection of mission critical military or governmental satellite networks. As such, an overall approach needs to be envisaged to align the EPW development with the complementary security and resiliency technologies for ground and space segments, leading to the following additional requirements:

The EPW should be integrated into a larger multi-layered security & resilience architecture that:

- Contains anti-jamming technologies that allow to detect, mitigate, prevent and predict jamming efforts by 3rd party adversaries. This could be tackled through spectrum monitoring, geolocation and network management technologies working together with nulling or interference excision technologies as well as Anti-Jam waveform capabilities as Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum and beam forming technologies;

- Allows for network diversity, redundancy and geo-redundancy technologies to increase the resilience of the satellite network as well as for multi-access capabilities (hybrid LTE/5G/etc.) with intelligent routing;

- Can dynamically steer its radiation pattern accordingly to connect to another satellite in a different frequency and satellite orbit to increase network resiliency. Fixed, on-the-move and on-the-pause land-based and maritime terminals, man packs and antenna systems, including airborne terminals and antenna systems installed on rotary wings (RW), need to be considered as well as different types of antenna technologies (e.g., parabolic, electronically steered, phased array, flat antennas, etc.). The secure connection and interface between antenna system and baseband needs to be taken into account as well;

- Includes network and ground segment technologies that improve the cyber hardening of all satellite vulnerable subsystems including protection against possible hacking, network intrusion, etc.

- Includes protection technologies against hostile action (e.g., jammers, intrusion and eavesdropping) for critical satellite datalinks, improving signals protection and integrity;

- Provides future proof interfaces and complementarity to upcoming disruptive security technologies such as quantum-safe encryption, self-healing networks, etc.;

- Is open towards upcoming and existing EU-based pooling and sharing programs (e.g., GovSatCom) and satellite constellations (EU Secure Space Connectivity System initiative currently under study) and ready to be integrated in these concepts.

Baseband equipment requirements (hubs, modems):

The right implementation of the terminal is likely to determine the success of the EPW. The flexibility and the affordability of the terminal are key considerations.

- A Software Defined Mode type of baseband equipment should be pursued;

- The baseband infrastructure (hubs and modems) should cover multiple architecture types of networks (point-to-point, point-to-multipoint, mesh) and satellite (wideband, spot beam, mix of both, transparent, processed) architectures;

- The EPW should operate on Software Defined hardware from different vendors to be selected by nations, government and defence agencies or institutions, depending on their preference or acquisition processes;

- The EPW should include the ability to receive and transmit various modulation

methods using a common set of hardware;

- The EPW should be future-proof, easy to upgrade and change configurations (over-the-air) and offer the ability to alter functionality by downloading and running new software at will, in order to repurpose the modem for new applications;

- The EPW should be affordable and include the latest efficiency satellite waveform, networking and equipment technologies to save OPEX (reduce bandwidth costs, save resources for planning) and CAPEX (save on equipment cost) compared to existing expensive military satellite modems;

- The EPW should consider Size, Weight and Power (SWaP) constraints for on-the-pause and on-the-move platforms and unmanned systems. Modems and terminals should be easy to transport and deployed and use a minimum amount of power;

- The EPW should be deployable in different environment conditions and on different platforms (land, sea or air);

- The EPW should be available in different form factors (OEM cards, rack units or rugged terminals);

- The EPW should be transparent for national encryption standards and externally encrypted data, and capable of integrating on-board modules for encryption technology.

On-board Transponder requirements:

- The EPW should consider different transponder technologies including next generation ones (i.e., fully transparent transponder; processed transparent transponder; new generation processed interactive transponder).

- The EPW processed transponder should contribute to improve link performance; adoption of (individual) gain adjustment mechanism for dynamic power level control needs to be considered.

- The EPW interactive transponder should be able to support operation in GNSS-denied environments by implementing enhanced mechanisms dedicated to the network elements synchronisation and aided fast signal acquisition.

- The EPW interactive transponder should improve the Low Probability of Detection (LPD) and Low Probability of Interception (LPI) factors.

- The EPW interactive transponder must provide protection against intrusion and jamming.

- The EPW interactive transponder must deny connectivity for unauthorised transmission attempts by guaranteeing exclusive access to the satellite resource.

- The EPW interactive transponder should be able to implement enhanced mechanism, addressed in the EPW project, devoted to decoupling the transmission schemes between downlink and uplink signals in order to de-correlate uplink and downlink signals activity and prevent eavesdropping and activity monitoring for ongoing operations and assets.

- The EPW interactive transponder architecture should be designed maximising the employment of Software Defined solutions in order to perform future

upgrade/changes of configuration.

Expected impact

The outcome should contribute to:

- Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

- The availability of a critical enabler for CSDP operations and missions in providing scalable secure and resilient communications in peacetime and during operations with protection against intrusion, hacking, jamming, traffic monitoring and eavesdropping;

- Full interoperability between different demanders and suppliers of satellite communication in support of military operations and missions;

- Secure, guaranteed and affordable access to satellite communications for all Member States and EDF Associated Countries;

- Strongly increase European autonomy in satellite communication for defence users and remove dependency on support from outside the EU for the transmission and exchange of mission critical and sensitive information;

- State-of-the-art technological solution in line with the latest satellite innovations and initiatives such as 5G, small LEO/MEO satellites, connected vehicles and Internet of things.

EDF-2024-DA-ENERENV-EEMC-STEP: Energy-independent and energy-efficient systems for military camps

Objectives

General objective

The future battlefield is likely to be dominated by weapon systems, platforms and devices that require electric energy. This type of battlefield, previously purely oil-based from cradle to grave, to integrate energy management technologies, buffer storage resources and a camp/weapon system interface in a constrained and contested tactical environment, is in need of a comprehensive review of its energy production and distribution. It requires the implementation of a coherent and efficient energy network, from the energy production systems at operational level to the soldiers at tactical level, through all the layers of the distribution systems.

In parallel, the EU defence sector has to start its digital and green energy transition to contribute to the EU net-zero greenhouse gas emissions target by 2050 and to anticipate growing energy costs linked to the vulnerability of fossil fuel supplies becoming increasingly scarce and disputed.

This development entails major risks for military activities. The multiplication of low-carbon energy sources and the risk of more complex logistics are an additional challenge for manoeuvres. It is also an opportunity to meet the growing demand for future weapons systems, platforms and devices.

An energy-independent and energy efficient deployable military camp, as part of the future electric battlefield, is the first step towards an operational and tactical integrated energy supply chain. It serves as a starting point, hub for innovative electric energy generation and efficient distribution throughout all levels. This includes initial definitions of interface between the stationary components (operational level) and the mobile components (tactical level) of the electric battlefield.

As the role of the military camps, as an energy provider has been emphasised, scaling-up of its technological bricks (energy generation, storage and distribution) needs to be amplified while covering a wide range of operational scenarios.

Specific objective

The specific objective of this topic is to substitute the fossil fuel dependency reduction in military deployable camps (support and mobility) without any drop of operational performances, in a context of increasing electrical energy demand in the battlefield. Moreover, investigation on the return of experience of the demonstration stage, should include specifications of a whole concept of energy independent and efficient deployable camps. Furthermore, the ability to support the diminution of their fossil fuel consumptions while maintaining operational performances, avoiding logistics, security burden and reducing logistics footprint should be validated.

Scope and types of activities

Scope

Proposals must address a full-scale operational demonstrator of a deployable camp fulfilling interoperability between inter-allied armies and NATO, with a modular and easily deployable energy system and adaptable energy mix.

Proposals must pursue the feasibility study of different technologies to answer to the identified needs of the Member States and EDF Associated Countries while ensuring the interoperability of systems and taking into consideration opportunities such as autonomy or resilience. As innovative solutions evolve rapidly, the proposals should update results generated through the latest research in this domain. In addition, proposals should demonstrate the effectiveness of logistics and maintenance in different scenarios (e.g., Host Nation Support, Contractor Support to Operations or by military themselves).

Proposals must design and produce the solutions (production, storage and management modules, including control and command interfaces, communication protocols, and operational simulation and planning systems). In order to ensure their safe use, functional tests must be performed before the demonstration stage.

Proposals must address physical experiment of the most critical technological modules deployed in military camps, especially the most vulnerable ones toward harsh environmental conditions and demanding operational scenarios, including resilience against electronic warfare, cyber-attacks and electromagnetic pulse.

Proposals must split the demonstration of the technological modules in different locations hosted by several Member States in different representative environment (cold/warm weather, dust, number of occupants, deployment duration, type of mission, etc.). In addition, the proposals must validate a wide range of operational use cases and assess the adaptability of the technology for the deployment in different scenarios. Adding up, they should ensure testing, validation and qualification of the overall concept through simulation activities in real military context including in harsh conditions. Furthermore, the ability of the energy architectures and protocols endorsed to operate in civil-based (non-rugged) solutions should be demonstrated. The demonstration should cover the simulation and planning tools.

The focus must be on military use-cases, taking into account specific harsh military environment (cold/heat/dust), different deployments and conflict intensities (including the shift from low-intensity conflict to high-intensity warfare), different deployed infrastructures, different life-time phases of the camp (storage, building, operation and redeployment phase) and military heavy constraints (logistic, maintenance, training, risk management, unmanned).

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[93] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[94] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(h)	**Certification**[95] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

– Studies:

– Study activities must build on ongoing, completed civil-based and military research and follow as well new solutions available on the market (hydrogen/synthetic fuels, non-fossil fuels from renewable sources, smart grid, microgrids, self-healing power systems, etc.) to

---

[93] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[94] '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.

[95] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

validate the feasibility of deploying such solutions in operations areas. Some specific areas must be covered:

- Study the emerging technological solutions becoming available on the market;

- Analyse hydrogen or hydrogen based synthetic fuels to include recent development on substances identified as storage medium for hydrogen as ammonia, toluene, salt and solid matter, and assess the possibility to be employed in overseas camp (UxV, soldiers wearables, etc.);

- Analyse smart grid integrating hybrid and electric vehicles in the camp scope, including fast charging systems, vehicle to grid concepts, wireless and fast charging docking for UxV;

- Analyse heat recovery systems for increasing energy efficiency of power generators, thermal energy storages, i.e., water or phase change material (PCM)/ latent heat storages and waste treatment systems, including wastewater;

- Analyse data monitoring tools (including meters) and management technologies, interface with tactical management systems as battlefield management and situational awareness tools;

- Perform an accurate energy performance diagnosis;

- Identify and select key technological solutions for a demonstration action: existing industrial solutions and adapting civilian products identified that are part of the energy independent and efficient deployable camps concept;

- Study of the added value of Artificial Intelligence (AI) for the camp's energy management system and to prevent, detect and to respond to cyberattacks;

- Study and implement up to date technological solutions in order to allow the forces to reduce fossil fuel consumption in military deployable camps;

- Study the ability for such technological solutions to operate in a military context by integrating the logistics and financial aspect, and collateral benefits;

- Study and update the risk assessment from demonstration actions: vulnerability, electromagnetic compatibility, detections of such systems, spare parts needs, possible collateral damages in case of destruction, cyberattacks, training;

- Identify the needs of the interested Member States and EDF Associated Countries for demonstration actions;

- Define aspects of standardisation of hardware and software interfaces (i.e., through the use of middleware or other) to allow the creation of a military camp in which different modules can be integrated through standard interfaces in accordance with Operational Energy Concept milestones (e.g., the draft available on the NATO Energy Security Centre of Excellence website) and

the environmental protection for military camps (e.g., the NATO operations environmental protection best practices).

– Design:

  – Design and define energy efficient deployable camp architectures following preliminary existing research concepts in this area and covering the complete energy chain too;

  – Design and production of the energy modules (production, storage, management modules, as well as electrical and control/command equipment, communication protocols, operational simulation and planning tools);

  – Design a camp energy simulation and planning platform and validate its capacity to represent operational situations. The simulation and planning platform must be designed in a way that it can be updated and provide the ability to add new modules/characteristics of power sources, energy storages and consumers;

  – Design and set-up a full-scale operational demonstrator of a deployable military camp as the starting point of an energy supply chain, to validate the concept in operational conditions, and to support the development of a new advanced European capability for supplying electric energy on the battlefield;

  – Design should ensure that the outcomes of the proposals must include the definition of an EU energy efficient deployable camp standard, with a special interest on standardisation of hybrid and electric heavy vehicles supply and powering systems at the camp. Proposals must also pursue the development of the tool to predict and simulate energy production/consumption and determinate the most efficient camp architectures for planning activities;

  – Design should safeguard specifically the capacity to on-site produce, transport, store, distribute and use green hydrogen or green hydrogen based synthetic fuels in military context and to power supply in field operations;

  – Integrate individual tests at component/equipment level to ensure safety.

– System prototyping:

  – Functional testing of the energy modules at real power levels (test bench at full size) in order to confirm the global safety of the solutions, test the interoperability and connectivity of each module and test non-nominal electrical scenario (stress tests, breakdown, network resilience and reconfiguration).

– Testing:

  – The testing activities must involve the identification of key players in this domain, to ensure the inclusion of the European armies need addressing specific operational scenarios and different hypothesis of engagement. A special attention must be given to the technological modules which show vulnerability towards harsh environment or carrying potential risk to be operated in fields operations.

- The testing must include the design of the appropriate experimental approach to demonstrate the capacity of the technological solutions to be operated in military context covering different deployment scenarios, with at least:

    - Geographic and climatic regions including at least an Arctic region, a continental climate region, an arid climate region and a tropical region;

    - Validate requirements against operational needs and mission requirements;

    - Perform the tests in specific harsh environments: extreme heat and cold, dust, high humidity

- Test the use of hybrid and full electric vehicles, including military, logistic and construction vehicles (e.g., forklifts, excavators, cranes, ground moving equipment, etc.) that are used in the build-up phase, the operational phase, and the redeployment phase of a deployable military camp, including the evaluation and simulation of the use and possible impact on fuel reduction of those machines as part of the camp microgrid system (e.g., as extra energy storage and/or grid balancing).

- Test the capacity to power hybrid and electric vehicles, including construction equipment (e.g., forklifts, excavators, cranes, ground moving equipment, etc.) and military platforms (e.g., UxV, robots, DEW, soldiers, etc) in operations.

- Test the capacity to produce, transport, store, distribute and use alternate non-fossil fuels from renewable sources to explore the convenience of integrating fossil fuels with zero or low impact on the carbon footprint in the military environment.

- Different existing concepts of deployment for overseas operations, at least including deployed force infrastructure.

- Three scenarios reflecting different number of camps occupants: 50 personnels, 250 personnels and 2000 personnels;

- A peacetime and low-intensity scenario and a high-intensity war scenario demonstrating the energy network's capacity for reconfiguration;

- A test preparation and coordination between industrial partners and hosting Member States, by defining an adequate Data Collection Plan. In addition, ensure security and proper analysis of the data collected;

- Demonstrator testing, both tactics and logistics (including maintenance);

- Individual tests at component and equipment level to ensure safety (e.g., CE certification).

- To prove the performance of the capacity, the testing must be performed following realistic operational conditions, for a representative period for each demonstrator module. Physical testing must be completed with simulation activities (e.g., SIMEX - Simulation Exercise) through the digital model elaborated. The testing must be organised in collaboration with the supporting Member states and EDF Associated

Countries (e.g., in collaboration with NATO "Capable logisticians" exercise and with the Permanent Structured Cooperation (PESCO) and Energy Operational Function EOF[96] partners) to articulate the interoperability of the solutions with the allies.

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of energy-efficient systems for military camps, notably those described in the call topic EDF-2021-ENERENV-D-EEMC[97] related to *Energy independent and efficient systems for military camps*.

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).

For more information, please check *section 6*.

Functional requirements

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

– Lower the fossil fuel dependency of deployable camps and foster their energy autonomy and improve the use of an extensive energy mix, including a growing share of renewable energy;

– Improve the energy autonomy of the camp: use of renewable sources, production and storage of its own electricity or sustainable fuel, integration of smart electricity grid and energy management system, implementation of cogeneration of power and heat from different non-fossil sources, including renewable sources (i.e., combination of solar panels and heat pumps), with a minimum of maintenance and cost-efficient solutions;

– Improve the deployment of hydrogen solutions in operational areas particularly in terms of onsite production (from renewable sources) transportation and storage;

– Improve the operational capacity of the camp: reducing the noise and detection/signature, reducing the logistical convoys in fossil fuels and

---

[96] https://www.pesco.europa.eu/project/energy-operational-function/
[97] Funding & tenders (europa.eu)

integration of the energy awareness inside battle management systems;

– Improve the energy supply of current, future weapon systems, operational energy planification with digital twins, machine learning, and AI technologies;

– Promote plug-and-play and easy-to-use solutions in order to limit human resources burden and be effective maintainable,

– Be modular and be integrated in extensive military operational configurations, from foreground infrastructure to equipment deployed close to the threats,

– Be protected against military risks and natural disasters, taking into account climate change effects;

– Be easily and rapidly transportable (even air-transportable), deployable and removable without involving a lot of labour force, in different geographic and climatic regions from arctic to tropical regions, housed in ISO containers (e.g., an ISO 20 feet container type "1C" or under);

– Be compliant with cyber-defence and cyber-security requirements;

– Be agile and easily reconfigurable with open interfaces and communication protocols allowing the integration of future solutions and use of civil-based (non-robust) solutions deployed in harsh operational circumstances (e.g., in a downgraded mode);

– Be based on components developed and manufactured in Europe in order to foster the European autonomy and sovereignty;

– Be interoperable between allied armies and NATO and be tested in a representative military environment;

– Be compliant with relevant national, European and global regulations and standards.

Expected impact

The outcome must contribute to:

– Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

– Improving the armed forces autonomy, resilience, interoperability and capabilities in operations to support the growing needs of electrical energy for the weapons systems in the battlefield,

– A decrease in the total costs of ownership of deployed capacities and supporting the growing needs of electrical energy for the weapons systems in the battlefield,

– Enhancing the competitiveness and innovation capacity of the EU defence industry in the area of new energies,

– Completing the global European strategy for renewable and sustainable energy, hence tackling the climate change,

– Adapting to civilian sustainable energy technology, military requirements and develop European standards,

– Improving the logistics processes and the ability to perform effective

maintenance.

EDF-2024-DA-AIR-NGRT: Next generation rotorcraft

Objectives

General objective

The importance of rotorcraft in military operations is widely recognised as one of the most important VTOL[98] assets/systems. Military rotorcraft act like workhorses of the battlefield, performing a variety of missions such as armed reconnaissance, strike, combat, combat and ordinary search-and-rescue (SAR), MEDical EVACuation (MEDEVAC), CASualty EVACuation (CASEVAC), utility, air assault and close aerial support, all of which are critical to the success of military operations.

After decades of European involvement in counter-insurgency type of operations, recent conflicts have marked the return of high-intensity confrontations very close to European Union territory, recalling that although military helicopters are key assets, they require careful mission planning and operations to be efficient and survivable.

On the longer term, rotorcraft is foreseen to be even more critical as future combat theatres are likely to take place in congested urban environment, mostly in littoral regions, and to involve a wide range of long-range strike capabilities (artillery, short range ballistic missiles) combined with a shortened OODA[99] loop made possible by the massive global deployment of networked C4ISR[100] assets.

Current capability forecast assessments at European and NATO levels show that the helicopter fleets will have to be renewed as of 2035-2040. The main objective is therefore to provide the EU Member States and EDF Associated Countries with a European solution that meets the European market and military needs in the field of rotorcraft.

Specific objective

This topic is intended to lead to a step improvement in EU VTOL capability with a view to future EU/NATO rotorcraft programmes (EIS 2035/2040+). Moreover, developed technologies should also be used for upgrades of legacy platforms, where applicable.

Scope and types of activities

Scope

Proposals must address future technologies and rotorcraft architectures with a view to the launch of a new European collaborative capability development programme in the field of next generation rotorcraft by 2030.

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)*:

---

[98] Vertical Take-Off and Landing.
[99] Observe – Orient – Decide – Act.
[100] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

	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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[101] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[102] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[103] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (mandatory)

Accordingly, the proposals must cover at least the following tasks as part of the studies and design mandatory activities:

– Assess adequate elements and criteria underpinning the convergence towards a single vehicle architecture and assess the related operational concepts for high performance military VTOL platforms, including;

  – Fundamental work on EU defence community needs as provided by EU Member States and EDF Associated Countries, with a special focus on logistics, serviceability and training;

  – Assessment of the preliminary technical specifications, concept studies and sizing for major sub-systems (including, but not limited to, propulsion, core avionics, mission system(s), role equipment and

---

[101] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[102] '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.

[103] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

general systems);

– Feasibility analysis and preliminary requirements review (PRR) of rotorcraft architectures to confirm the technical, programmatic, industrial and market feasibility of the solution(s), with a view to further development and industrialisation and production phases;

– Rotorcraft design study consisting of an assessment of vehicle architectures, with a maturity target allowing a System Specification Review (SSR);

– Coordination of technology acquisition efforts to integrate key future capability streams since early concept phase (e.g., modularity, interoperability, interchangeability, manned-unmanned teaming (MUM-T), survivability, design-to-cost);

– Address key technologies and system architectures for next generation VTOL platforms up to TRL[104] 4-6, in particular regarding:

– Design and manufacturing technologies to:

– Reduce acquisition and upgrade costs, using an EU Modular and Open Rotorcraft System Architecture;

– Reduce maintenance costs while providing a significantly higher operational and fleet availability than existing helicopters (e.g., utilising mature and already proven solutions wherever possible, harmonised maintenance programme, etc.).

– Technologies towards lower-emission production and operation, as well as reduced consumption of energy resources;

– Technologies to improve the operational capability and thus create an operational advantage in the area of:

– Performance of the platform (e.g., range, endurance/autonomy, payload, speed, manoeuvrability, etc.);

– Enhanced survivability in contested environments, such as technologies towards minimised signature (e.g., IR, radar, acoustic, visual, etc.);

– Improved connectivity and interoperability;

– Adaptability for rapid reconfiguration according to the mission requirements;

– Improved interchangeability of components between different aircraft configurations and/or between different helicopter operators;

– Manned-unmanned teaming and automation level to reduce crew workload;

– Multi-domain (air, land and maritime) capability aspects;

– Ability to conduct distributed operations to sustain potentially

---

[104] Technology readiness level

protracted confrontations.

– Perform ground and flight demonstrations of systems and technologies, relying on technology demonstrators and available assets, as well as on laboratory testing.

– In terms of programme activities:

- – Prepare the required industrial activities to develop and exploit the military capacity to be selected and the interoperability requirements;

- – Establish the preliminary programme management and the system engineering plans;

- – Establish the overall programme schedule and roadmap, including possible relationships with other projects;

- – Perform a costing evaluation exercise;

- – Perform a market assessment review;

- – Identify risks and constraints related to implementation, costs, schedule, organisation, operations, maintenance, production and disposal;

- – Identify key technological aspects and plan for their maturation within the programme plan;

- – Establish methods to ensure the simplest feasible technical solution to the operational requirement and to establish methods to harmonise and optimise the maintenance programme.

– In terms of activities related to the operational environment, contribute to:

- – The refinement of a concept of operations (CONOPS) and Main Attributes List provided by the supporting EU Member States and EDF Associated Countries.

- – The definition of the sustainment model (i.e., number of planned flight hours, layout of bases, deployments), in line with guidance from the supporting EU Member States and EDF Associated Countries.

- – The definition of a baseline for aircraft logistic support, in accordance with the supporting EU Member States and EDF Associated Countries provisions.

– Provide a proposal for a best candidate solution based on a complete value analysis covering performances, costs, risks, modularity, availability, manufacturability, safety, consistency with Member States and EDF Associated Countries operational needs, with jointly defined detailed criteria and hypotheses.

In addition, the proposals must cover at least the following tasks in view of the increasing efficiency mandatory activities:

– Maximise maintenance operations to be performed at operational level and minimise depot level maintenance (with regard to aircraft components and aircraft ground equipment);

– Minimise calendar and flight hour maintenance limits while maximising on-condition maintenance;

– Minimise utilisation of components subject to limitations (e.g., REACH legislation[105] or any other import/export regulation), potentially affecting the procurement of spare parts;

– Implement as many already certified systems and maintenance metrics as possible;

– Provide targeted production and maintenance plans to be worked on at all stages of the development/design phase.

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of rotorcraft, notably those described in:

– The call topic EDF-2021-AIR-R-NGRT[106] related to Future Operating Environment (FOE) and Future Operating Concepts (FOC) for *Next generation rotorcraft technologies*.

– The call topic EDF-2021-AIR-D-CAC[107] related to *European interoperability standard for collaborative air combat* as regards to collaborative air combat and manned-unmanned teaming aspects.

– The call topic EDF-2023-DA-AIR-SPS[108] related to *Self-protection systems* as regards to survivability aspects.

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).

For more information, please check *section 6*.

---

[105] Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) (OJ L 396 30.12.2006, p. 1).
[106] Funding & tenders (europa.eu)
[107] Funding & tenders (europa.eu)
[108] Funding & tenders (europa.eu)

Functional requirements

The proposed product and technologies should meet the Main Attributes List defined by the supporting EU Member States and EDF Associated Countries and the following functional requirements:

A- Ground rig test, laboratory tests and/or specimen demonstration of:

– The system architecture, based on a maximal proportion of existing system components, modified where applicable to include new interfaces, and combined in a system integration laboratory to test the architectural backbone and system interconnections.

– Critical structural and dynamic components to collect experimental data for preliminary validation activities of design concepts, in support to the rotorcraft architecture assessment.

– Technologies enhancing survivability capacities of structural elements.

– Aerodynamics performances through experimental aerodynamics campaigns to demonstrate aerodynamic effects and behaviours of the platform in various mission conditions.

– Aerodynamic tests on non-linear behaviours to collect de-risking elements on critical aero-elastic effects.

– Technologies supporting the ability to adopt dispersed operations for long time (validation of the technologies developed by simulation).

B- In-flight demonstrator of:

– Interoperability capability to support mid- and long-term compatibility of EU rotorcraft with future multi-domain and air combat collaborative systems and leverage on results from simulation;

– Collaborative combat and MUM-T[109] capacities.

C- In-flight demonstrations of technology bricks, focusing on bricks providing an operational advantage:

– Modular architecture for control system (from pilot inputs to moving surfaces) to be tested at the end of specific design activities;

– Survivability elements to reduce the risk of encounter, detection, acquisition, as well as hit, penetration and kill, such as those induced by self-protection capabilities, in coherence with hardware and/or software solutions already developed in this field, provided that they are made available for testing, even in their simplified configurations and shapes;

– Future on-board energy/power capability and related energy/power management possible architectures.

D- Simulation of technology bricks, focusing on those providing an operational advantage, such as:

– Rotors and rotating controls, in combination with ground demonstrators;

---

[109] Manned-UnManned Teaming.

- Technologies supporting the ability to adopt dispersed operations for long time (to be validated in rig-test demonstrator);

- Survivability capabilities linked to low signature/detectability assessment (of various types, e.g., acoustic/dB, radar, IR etc.), connectivity and System of Systems (SoS) capabilities;

- Survivability capability technologies, systems and structures, such as structural protection for ballistic damage tolerance, impact/crash resistance, on-site repairing of ballistic damage, etc.;

- Maintenance, including dispersed maintenance technologies (e.g., non-destructive testing, simplified repair, etc.) and enhanced by the concept of "smart maintenance" to enable predictive maintenance approaches to replace the conventional scheduled tasks with an aircraft tailored maintenance. This new approach relies on the continuous collection and analysis of aircraft data through advanced engineering techniques, empowered by digital-twin technologies and applied-AI techniques;

- Airframe and structural components modularity to allow for fast vehicle re-configuration.

- Control laws impacting platforms manoeuvrability capabilities to be demonstrated through digital tools, such as digital-twin or available ground simulators, and as a consequence, improving survivability potential.

E- Cross-cutting requirements:

- Based on operational scenarios & threat environment 2030+ (i.e., multi-domain connectivity), to be assessed though both studies and virtual simulation as appropriate;

- Affordability, in terms of acquisition and lifecycle costs, including the overall operating costs and maintenance costs (e.g., easier and less labour-intensive maintenance in terms of methods, tools and personnel required) to remain below similar solutions available on the market;

- Operations in hostile environment (e.g., battlefield/federated battlefield simulations) and dispersed maintenance concepts;

- Multi-mission capability and flexibility for operating different kind of military missions and possibly reconfigurable for supporting civilian needs;

- Cargo capability to carry the necessary equipment for the execution of the various missions as required in the CONOPS and Main Attributes List defined by the supporting EU Member States and EDF Associated Countries;

- State-of-the-art development to ensure availability and reliability of the platform and avoid obsolescence concerns;

- Sustainability along the entire product lifecycle: from the conception / production by means of digitalisation up to the product use with reduced environmental footprint due to e.g., advanced propulsion system, low weight and more efficient flight capabilities.

Expected impact

The outcomes should contribute to:

- Prepare 2035/2040+ horizon, building European capabilities for new EU/NATO

rotorcraft/VTOL programmes, fully compatible to future multi-domain combat collaborative systems.

  − Develop technologies and concepts usable for upgrade of legacy platforms, where applicable.

  − Support the competitiveness and excellence of the EDTIB, as well as the autonomy and sovereignty of EU and EDF Associated Countries, in the field of military rotorcraft.

  − Increase the effectiveness and efficiency of EU Member States and EDF Associated Countries Armed Forces.

  − Enhance the strategic autonomy and competitiveness of the EU Member States and EDF Associated Countries and their DTIB willing and able to develop new technologies for inclusion in future EU/NATO rotorcraft programmes.

EDF-2024-DA-GROUND-UGS-STEP: Multipurpose unmanned ground systems

Objectives

General objective

The use of Unmanned x (generic) Vehicles (UxVs) in military operations represents one of the most important innovations of recent years. Undoubtedly, UxVs exploitation is likely to grow in the coming years with the massive introduction of other autonomous systems in different domains (land, air, sea, space, cyber) and the increase of capabilities to work collaboratively between systems (swarms) and people.

Indeed, intelligent and effective cooperation between military assets (UxVs, different types of vehicles and their operators, and dismounted soldiers) within Close Combat Operations is needed to increase the overall Battlespace effectiveness, while reducing loss of life, the risk of collateral damage and lowering the cognitive burden placed upon operators.

Therefore, deploying autonomous and swarm-based military assets in a framework of cooperation between manned and unmanned systems (manned-unmanned teaming) is a very important capability that can enable enhanced ISTAR, survivability, situation awareness, mobility, lethality, logistics and training, and increase the probability of battlefield combat success.

This would allow the rapid development of capacities implying an incremental approach of capabilities milestones for current and future land systems and upgrades of legacy systems.

Specific objective

The use of such UxV systems has a direct impact in reducing the exposure of human operators and soldiers to associated risks. Such systems can radically improve the efficiency and performance of the tactical unit to provide tactical/ operational superiority and offer robust and reliable solutions in very demanding conditions.

Thus, the aim of this topic is to develop an unmanned modular system of systems capable of supporting dismounted, mechanised and motorised infantry in all types of European geographic and operational land environments, including denied environments, in adverse light and weather conditions with evolving levels of autonomy and robustness.

The overarching goal of this topic is to contribute to the maturing, testing and verification of the Unmanned Ground Systems (UGS) capability, so that the

technology is expected to be ready for integration into the European armed forces by 2030. Therefore, to ensure wide acceptance and efficient use of the systems, it is pertinent to study, analyse and develop:

– Detailed capability provision assessment for integration into force structures for supporting dismounted, mechanised, and motorised infantry.

– Novel concepts for Human Machine Teaming to enable closed hatch and long-range usage of system capabilities with regards to ethical and legal aspects of combat operations. These concepts should allow a significantly reduced cognitive workload for UGS operator(s) by improving the efficiency and effectiveness of the control, direction, monitoring, and supervision of unmanned systems through the development and application of artificial intelligence and assisted functions.

– Enhanced manned-unmanned and unmanned-unmanned teaming capacities of UGSs through advancements in multirobot and swarming technology.

– Modular design and open architectures (regarding platforms, autonomous functions, as well as effector, sensor and other payloads management) with standard interfaces to enable Through Life Capabilities Management (TLCM) in terms of interoperability, scalability, maintainability, availability, robustness and resilience. This should ensure transferability of technology with other manned and unmanned (including drive-by-wire legacy) platforms.

– Federated digital-twin framework would favour this TCLM management and may provide improved training environment for UGS navigation and other mission specific algorithms.

– State-of-the-art equipment and secure information availability to enable enhanced ISTAR, Survivability, Situational Awareness, Mobility, Lethality, Logistics and Training to ensure Battlefield Superiority.

– Self-air-defence (against NATO Class I UAVs), in support of dismounted soldiers, with automatic designation by on-board electro-optical sensors and related data fusion.

Additional enablers for the wide acceptance and use of the Systems are:

– Formation of UGS related R&D ecosystem/community that facilitates continuous innovation, synergies and inclusion of deep-tech start-ups, Technology and system testing, Evaluation, Verification and Validation (e.g., cross-border TEVV procedures, trust).

– Practical testing in a scenario-based exercise (48+ h) with infantry units.

Scope and types of activities

Scope

Proposals must address the development of a multipurpose Unmanned Ground System of systems with lethal effectors and solutions for systems integration and manned-unmanned teaming. This system must integrate the following abilities:

– Enhance situational awareness and force protection of ground units, their combat effectiveness, endurance, mobility, and autonomy, and enable faster deployment.

– Support dismounted, mechanised, and motorised infantry in all types of European geographic and operational land environments, including denied

environments, in adverse light and weather conditions with evolving levels of autonomy and robustness.

– Significantly reduce cognitive workload for UGS operator(s) using artificial intelligence and assisted functions.

– Have a modular design and enhance interoperability with manned and unmanned platforms to ensure transferability of the relevant technology to other platforms (including existing manned vehicles) and simplify payload integration, with the aim of bringing together European industrial capabilities and define standard interfaces for the benefit of European defence.

– Enhance manned-unmanned and unmanned-unmanned teaming capacities of current UGS.

– Have the capability to analyse different weather conditions, terrain types and obstacles to increase the mobility of single UGS and UGS teams.

The proposal must also provide analysis on the following topics:

– A fully autonomous targeting process and efficient effector(s) management and use against multiple types of targets, and include mobility solutions for engagement, target delegation and other relevant aspects of effector usage.

– The ethical and legal aspects of integrating combat-UGS in the European armed forces (if needed, research to support recommendations/decisions on ethical and legal aspects related to integration of combat-UGS in the EU Armed Forces and their interaction with human beings in the land domain should be included).

Proposals should also integrate the development and TLCM support of equipment (hardware or software) designed to enable personnel to function within different manned-unmanned operational modes and environments, able to be deployed in the digitised Battlefield where all land system assets are available to operate in coherence and demonstrating the following abilities:

– To interconnect in real time within the Battlefield and in a fully secured way with an extended set of systems supported by an intelligent TLCM solution concept.

– To be integrated seamlessly in the digitised systems (e.g., power supply, situational awareness, targeting process) manned or unmanned as and when needed during combat missions.

– To adopt real-time cooperative functionality and enhance Battlefield combat superiority, adaptation and effectiveness with measurable impacts of actions.

– To cooperate within the Battlefield while being able to sustain connectivity and interact with other assets (dismounted troops, UxVs, manned vehicles, swarms, long range support).

– To enable a versatile use in order to be deployed for a large spectrum of close combat operations and provide superior and optimised operational capability in hostile and harsh environment.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[110] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[111] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[112] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (mandatory)

Accordingly, proposals must cover at least the following tasks:

– **Studies** to critically analyse the essence of Intelligent Behaviour and Ethics within Land Operations, while understanding the necessary coherence and integration between different enablers to provide state-of-the-art equipment and information superiority for Battlefield success:

– Consider the ethical and legal aspects of integrating combat-UGS in the European armed forces (if needed, research to support recommendations/decisions on ethical and legal aspects related to integration of combat-UGS in the EU Armed Forces and their interaction with human beings in the land domain should be included).

---

[110] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.
[111] '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.
[112] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Provide an analysis and present possible solutions for an autonomous targeting process and efficient effector(s) management and use against multiple types of targets, and include mobility solutions for engagement, target delegation and other relevant aspects of effector usage. The system must meet standing law as required, with focus on the principles of discrimination, proportionality and caution in International Humanitarian Law (IHL) – e.g., by providing the possibility to override the systems autonomous engagement by a "human in the loop" manual function in order to meet standing law as required.

- Provide modular platforms design able to support dismounted, mechanised and motorised infantry in all types of European geographic and operational land environments, including denied environments, in adverse light and weather conditions with evolving levels of autonomy and robustness. This implies modular design and enhance interoperability with manned and unmanned platforms in order to ensure transferability of the relevant technology to other platforms (including existing manned vehicles) and simplify payload integration, in order to bring together European industrial capabilities and define standard interfaces for the benefit of European defence. This also implies significantly reduced cognitive workload for UGS operator(s) through maximum use of artificial intelligence and assisted functions.

- Provide manned and unmanned platforms and intelligent swarms of platforms with advanced mobility capabilities. This implies developing systems for automation with the ability to perceive the environment and location in all weather and operational conditions (e.g., unstructured environments, GNSS denied, adverse weather conditions, etc.), and resilient communications to the operating position. In critical circumstances the autonomous decision making should be supported, using local platform status (HUMS) and knowledge.

- Consider line-of-sight (LOS) and beyond-line-of-sight (BLOS) support with Command-and-Control system that meets mission planning and management needs, being able to manage the information available before the mission and the information provided during execution (common operational picture), so that the operator can have situational awareness that allows taking operational decisions assisted by the system intelligence (information superiority).

- Consider resilient and secure communications and high-level cyber security to work simultaneously in different security environments and handle the information.

- Consider the definition of a predictive maintenance framework encompassing logistics (including across fleet), and in-Battlefield support, including equipment functional configuration and re-role for assets availability and capabilities resilience.

- Consider the definition of a training framework to ensure specialist personnel availability with all areas of the Battlefield.

- Consider the definition of digital-twin framework that provides improved TLCM support as well as training environment for UGS navigation and other mission specific algorithms.

- **Design** an interoperable modular UGS combat platforms framework to demonstrate infantry support by effective engagement, risk reduction,

sustainability and mobility, enabled by computerised processing technologies as well as study of the potential early exploitation of innovative technologies, through the:

- – Definition of an interoperable modular architecture and the relevant functions in terms of autonomy, effectors management and necessary modules.

- – Definition of the relevant functions for manned-unmanned and the unmanned-unmanned operation modes for balanced teaming and swarming, environment understanding and advanced decision-making support.

- – Definition of the relevant implementation and integration of functions into a modular open system architecture of the targeted vehicles (hardware, software, networks) and other assets, taking into account EU/NATO existing standards.

- – Definition of the relevant functions implementation within a unified, interoperable and self-sufficient adaptive command and control environment.

- – Definition of the security environment.

- – Definition of open solutions able to embed future sensors, effectors and their optimised systems integration.

- – Proposal for a test case as a basis for demonstration, simulation and prototyping.

- – System integration into the tactical cloud concept and the distributed processing that allows fostering information superiority.

- – **Develop, Prototype and Demonstrate** combat UGS capabilities and technology insertion to provide Intelligent Command and Control within an optimised cooperative environment of human-machine assets, whilst conforming to ethics, legal aspects, safety and security, through:

  - – Development of optimised solutions identified within the Design Framework:

    - – Integration in a system of systems demonstrator of all the proposed capabilities: multipurpose ground system of systems capable of supporting dismounted, mechanised and motorised infantry in all types of geographic and operational land environments, including denied environments, with evolving levels of autonomy and robustness.

    - – Risk mitigation potentially including early exploitation of dismounted troops.

  - – Presentation of study results and execution of a demonstration with a test scenario.

  - – A detailed plan for the subsequent project phases must be developed, including the identification of implementation priorities, according to the operational needs of the participating Member States.

- Develop technologies or assets **increasing efficiency across the life cycle** of UGS products and technologies, by substantiating synergies and complementarities with foreseen, ongoing or completed activities in the field of Unmanned Ground Systems, notably those described in the call topics EDF-2021-GROUND-D-UGVT[113] on *Unmanned ground vehicle technologies* and EDIDP-MUGS-2019[114] on *Multipurpose unmanned ground system*, as well as other activities conducted across the EU (e.g., iUGS PESCO[115], EDA Cat B Combat UGS project[116]).

The proposals may also cover:

- **Certification** and support to the definition of a Through Life Capabilities framework, enabling battlespace-ready equipment and personnel, infrastructure and organisation, maintenance and logistics, as well as the definition of a Capability Certification framework for operational deployment, encompassing hybrid functionalities within the (human-machine) system (e.g., in the case of dismounted troop providing support to operations).

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).

    For more information, please check *section 6*.

Functional requirements

The development of functions that enable upgrading a set of current vehicles or to be integrated into vehicles under development or future vehicles with the ability to embed advanced multi-technology sensors networks and advanced effector networks around a common and standardised manned/unmanned teaming capability.

This set of modular components is expected to provide Armoured Fighting Vehicles programs with initial capacity to operate within connected hybrid balanced manned/unmanned Battlefield teams with the following main functional requirements around common, standardised and novel manned-unmanned teaming with a modular and robust architecture:

---

[113] Funding & tenders (europa.eu)
[114] Funding & tenders (europa.eu)
[115] Integrated Unmanned Ground System (UGS) | PESCO (europa.eu)
[116] 10---combat-unmanned-ground-system-cugs.pdf (europa.eu)

– Ability to manoeuvre the unmanned vehicles as needed for the relevant functions both in autonomous and remote way, taking into account that:

– an unmanned ground system can be remotely driven from any position (manned vehicles, possibly moving, operational station, etc.);

– the operators must have a comprehensive understanding of the environment of remote unmanned systems;

– the operators must rely on assisted and autonomous functionalities with a special care in the reduction of collateral damage risks;

– the unmanned systems should be able to interact in terms of manoeuvre in combat situations within a manned-unmanned swarm;

– the unmanned systems should be able to rely on and switch between several alternative driving modes (e.g., remotely controlled driving, semi-autonomous driving and highly autonomous driving) and call humans into the loop if standing law requires it or the confidence level of the autonomous system gets below a specified level;

– the unmanned systems should be able to function as part of dismounted and motorised infantry in most relevant environments and capable of manoeuvring autonomously to pre-planned positions and formations, and operating in support to dismounted and motorised infantry operation, by fielding the following abilities:

– navigate in a GNSS signal-denied environment;

– autonomously calculate the optimal route and plan the path between two geographical points;

– generate trajectories for local navigation, adapting the path as needed and overcoming possible obstacles through "sense and avoid" technology;

– autonomously detect, identify, categorise and track relevant agents and elements from the environment (e.g., targets, potential threats or enemy units, allied units and civilians);

– autonomously follow dismounted soldiers and vehicles, moving in coordination with them.

– Ability to resort to advanced interaction modes to optimise the number of human operators depending on the interaction modes.

– Ability to understand and adapt to the operational and tactical environment to speed up the decision-making process of the operators by delivering a user-friendly and reliable decision-making support tool. This enables operators to remotely operate all payloads from any of the manned vehicles by:

– providing good situational awareness to the system operator;

– providing real-time trusted situational awareness information and information sharing inside a system swarm;

– allowing to remotely cooperate the effectors of relevant systems (manned and unmanned) in order to gain a tactical advantage and generate tactical options, taking into account the tactical required effects, the collateral damage constraints and the ethical and legal

aspects.

– Ability to integrate additional UxSs seamlessly and securely to drastically enhance capabilities in the following domains:

  – force protection against a large spectrum of threats by using specific individual or cooperative countermeasures provided by UxSs;

  – integration of Beyond Line Of Sight (BLOS) combat capabilities.

– Capability to enhance force protection and resilience through:

  – impossibility for the enemy to visually distinguish between manned and unmanned platforms:

    – to prevent external identification of a manned or unmanned vehicle to target it as a priority (does not apply to systems designed to be only used in unmanned mode);

    – to give access to this capacity without increasing the logistic footprint.

  – the improvement of short- and long-range sensors and effectors integration and real-time communication;

  – the interoperability with soldier systems based on EU/NATO standards and previous EDIDP and EDF Projects.

– Use of a diversity of sensors and technical equipment to ensure:

  – the availability of information from variety of data sources;

  – the ability to predict logistic resource requirements using real time data;

  – the ability to navigate primarily with passive sensor systems.

– Use of state-of-the-art system with modern, customisable and intuitive user interfaces that support operators in all their operational, technical and training needs – with particular emphasis put on deployability as the cornerstone of system design – enabling rapid adaptation, implementation, operation and embedded training.

– Ability to operate in all relevant European climate zones and in all areas where relevant EU missions could be conducted.

– Dynamic, scalable and resilient functions, efficiently embeddable in most of the existing ground combat vehicles systems, compliant with their different programme roadmaps and the obsolescence of their modules lifecycles.

– Functions designed to be able to support specified availability requirements to contribute to an open, scalable, highly available and transparent failover architecture.

– Functions designed to be proof against diminution of environmental sensing capability, hostile countermeasures, including the application opportunity in Global Navigation Satellite System (GNSS) denied operation environment.

– Cyber security aspects to be applied along all project phases, from requirements capture to system design and implementation, in order to ensure adequate resilience, survivability and information protection.

– The system, and especially its command and control (C2), should be able to provide resilient and reliable connectivity in EW hostile environment.

– Functions designed to be able to work simultaneously in different security environments and handle the information security requirements to properly control the information flows between these domains and with external systems. The system should be able to be integrated into environments that impose different security constraints on the exchange of information while remaining usable in an environment with low security constraints.

– Multi-level security to be applied to all systems, data and information access to enable secure multi-national cooperation.

– Functions to be designed in accordance with the modularity openness and standard interfaces principles in order to enable integration of new technological solutions and to enable maintenance, scalability, availability, resilience and obsolescence management.

– Employment of any effector should be in accordance with the requirements of IHL and other regulations with appropriate human control while sensors can potentially be employed autonomously to increase the potential capacity to gather data and increase situational awareness.

– Functions designed to comply or be able to comply with the operational procedures of the targeted vehicles, with ethical and environmental constraints as well as with logistic and defence programme efficiency requirements.

– The ability to shift a system into an unmanned configuration.

– The design to be modular and scalable for future upgrades and implementations of different autonomous functions and must ensure transferability of technology with defined interfaces with other manned and unmanned platforms.

– Digital twins to be available for integration with high-level digital training areas usable with existing simulation systems.

Expected impact

The outcome should contribute to:

– Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

– Develop critical enablers for Common Security and Defence Policy (CSDP) operations and develop concept of critical enablers for EU Battlegroup missions.

– Enhance UxS self-defence and cooperative force protection.

– Increase readiness and availability for equipment and personnel deployment of EU military missions.

– Reduce the possible number of casualties on friendly forces.

– Interoperability milestones for Member States' ground capacity programs.

– Improve situational awareness, resilience and security of EU operations.

– Create a reference for manned-unmanned teaming modes and functions to improve the capabilities of the European defence industry to develop and supply state-of-the-art ground systems.

– Reinforce adaptation and interoperability of EU Member States' armed forces.

– Strengthen the EU's strategic autonomy in military capabilities.

– Optimise interoperability and synchronisation between manned and unmanned platforms, and soldier systems.

– Reduce the impact of the logistic footprint.

EDF-2024-DA-GROUND-BLOS: Beyond the line-of-sight close combat

Objectives

General objective

The performance of land combat systems has proved decisive in recent conflicts, since the availability of mobile (tactical and strategical mobility) precision systems able to provide the necessary high degree of accuracy, efficiency and reactivity, are becoming increasingly important to avoid widespread collateral damage and reduce exposure of friendly forces. In particular, it is essential for Member States' armed forces to provide combat units with increased engagement capabilities without being spotted and with a high level of success and survivability.

Specific objective

Beyond Line Of Sight (BLOS) engagement is the capability of firing at a target not directly seen by the effector, based on information given by a remote sensor. The Beyond Line Of Sight (BLOS) capability offers tactical advantages, as mobile units acquire an increased engagement capability with higher kill probability and without being spotted by the adversary.

To succeed in a BLOS-firing mission, reconnaissance, intelligence, and adequate preparations is likely essential. A technical system design (i.e., incorporating command and control, mobility, survivability, lethality, intelligence and endurance) for BLOS must be versatile against future alterations pending an evolving hostile threat. A BLOS system design therefore needs to be future-proof regarding robustness and security to motivate investments in resources and funds for the anticipated period of life.

In this context, some requirements are becoming increasingly important: provide the land and coastal combat units with an increased engagement capability and with a very high degree of success and survivability; discriminate between threats that are not always clearly identified and visible before firing; defeat targets that may mask or unmask at the last moment; avoid widespread collateral damage; providing conditions for a high level of survivability by low exposure as well as reachability with precision strikes over an area.

Scope and types of activities

Scope

Proposals must address:

– the development of innovative technologies of interest to improve the

performance of the capability;

- the update of BLOS collaborative close combat architecture for the integration of new technologies / capabilities;

- the development of effect management functions for BLOS capability;

- the development or the integration of a BLOS battlefield training system for collaborative training indoor, outdoor and being able to use force on force;

- the development of a common interface concept for dismounted system integration in light and medium vehicles and system compatibility with, but not limited to, ring mounted version;

- the demonstration of a BLOS collaborative engagement that:

  - should include firing from a dismounted version (possibly mounted on a light vehicle);

  - may include firing from a BLOS system integrated into a battlefield vehicle (deployed in a tactical situation).

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[117] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)

---

[117] '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)	**Qualification**[118] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[119] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

- Integrating Knowledge

    - Perform a threat assessment, taking into account the modern battlefield, lessons learned from current peer-to-peer conflicts, and deployed or about to be deployed advanced technologies.

    - Develop research activities for maturing identified technologies.

- Studies:

    - Feasibility studies concerning proposed technologies.

- Design:

    - Develop technologies suite to reach TRL 6.

    - Preliminary definition and design of the final product and technology.

    - Detailed definition of the final product and technology.

    - Critical Design Review (CDR).

    - Testing of product, tangible or intangible component or technology.

The proposals should substantiate synergies and complementarities with foreseen, ongoing or completed activities, notably those described in the call topics EDF-2021-GROUND-D-3CA[120] on *BLOS collaborative close combat architecture* and EDIDP-NGPSC-2019[121] on *Upgrade of current and development of next generation ground-based precision strike 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)

---

[118] '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.

[119] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

[120] Funding & tenders (europa.eu)

[121] Funding & tenders (europa.eu)

– 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).

For more information, please check *section 6*.

Functional requirements

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

– The architecture should allow Collaborative Close Combat using Line of Sight (LOS) or BLOS firing modes at different ranges and using mounted, dismounted and integrated European missile systems.

– The BLOS system should be coordinated at a tactical level.

– The system should operate with cooperation means such as a communication network of participants or the European Battle Management Systems.

– The system should allow for employment within land and amphibious/littoral naval force structures, e.g., light and motorised infantry, mechanised units, and amphibious assault units.

– The system should be quick into and out of engagements (BLOS and LOS) with a short time from transport, through deployment, preparations, engagement and redeployment, allowing for use in highly dynamic manoeuvre scenarios.

– Design should consider common maintenance concepts for cost-effective solutions for availability within Europe.

– The BLOS system should be reliable and safe.

– The data links should be cyber robust, the cyber aspects being fully controlled by Member States.

– The system should be capable of operating in climate zones that are of interest to the EU Member States and EDF Associated Countries with a "one applies to all" way of usage.

– Effect management functions should be explored and possibly improved.

– The system should provide automated deployment and engagement planning support.

– The system should be able to operate in a Global navigation satellite system (GNSS)-denied environment.

– The BLOS system should have an associated battlefield training system for indoor and outdoor exercises with focus on force-to-force training.

− System design should take into account forces' limited availability of time for training to operate the capability.

− The system should allow for robust positioning, navigation and guidance.

− The system should provide automated support for target detection and acquisition.

− When doing re-design and design, concern should be taken to existing concepts to minimise the cost of ownership for future upgrades of the capability.

Expected impact

The outcome is expected to contribute to:

− Bring a significant operational differentiator and contribute to enhanced interoperability between armed forces of Member States;

− Develop and increase the maturity of innovative technologies specifically adapted to BLOS engagement;

− Increase EU industry capabilities on BLOS architecture, components and technologies;

− Consolidate European business consortium able to offer competitive solutions for the global market;

− Decrease dependence on non-EU technologies and products.

EDF-2024-DA-GROUND-AIFV: Next generation armoured infantry fighting vehicle

Objectives

General objective

The Global Strategy for the European Union's (EU) Foreign and Security Policy defines an integrated approach to conflicts "at all stages of the conflict cycle, acting promptly on prevention, responding responsibly and decisively to crises, investing in stabilisation and avoiding premature disengagement when a new crisis erupts".

In order to support and, if necessary, enforce, the above approach, a credible deterrent is required to be rebuilt in terms of land combat capability with a priority focused on armoured vehicles in general and, in particular, on Armoured Infantry Fighting Vehicles.

Specific objective

Armoured Infantry Fighting Vehicles (AIFV) remain a pivotal element of land military manoeuvre, both in a conventional warfare context as well as in the asymmetric one, thanks to the combination of protection, mobility, and firepower. Nonetheless, AIFVs currently numbered in the fleet inventories of the EU Member States are to some extent either ageing or obsolete and, therefore, the same States face the compelling need to modernise their in-service platforms and replace those of them approaching the end of their operational life. There is also a need to accelerate the acquisition and increase the size of the AIFV fleets updating some of the new requirements stemming from the war in Ukraine and the new threat scenarios. Against this background, the upgrade of the current and development of the next generation armoured infantry fighting vehicle capable of outstanding operational effectiveness and mission success

in all possible future scenarios are highly necessary.

Modularity, reduced crew workload, the integration of automatic systems, Manned-Unmanned Teaming (MUM-T), and increased survivability must guide design considerations.

Scope and types of activities

Scope

Proposals must address studies and design for the upgrade of current armoured infantry fighting vehicles and the development of next generation armoured infantry fighting vehicle technologies, with desirable outputs for legacy platforms, including enabling and green technologies (eco-design or sustainable technologies), leading to a system level capable of outstanding operational effectiveness and mission success in all possible future scenarios. Furthermore, they must take into account aspects such as mobility, deployability (tactical and strategic ones), autonomy, firepower, maintainability, survivability and cyber security.

Thematic scope of the activities to be supported is preliminary studies, system analysis and early development phases. It includes considerations of the system in operational perspective and identification of specific subsystems that define the future operational environment and purpose of system within the future battlefield.

Moreover, proposals should include development efforts of a new common European "Armoured Infantry Fighting Vehicle" (AIFV), and when feasible have a high commonality with solutions in other future European combat vehicles.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[122] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[123] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[124] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

- Studies

    - Concept of Operation (CONOPS) definition, feasibility study and architecture definition, including the definition of operational requirements and critical capabilities;

    - Cost-benefit analysis against technology solutions defined during the project;

    - System Specification (SSS and SSDD) providing a detailed system and sub-systems description, including the development of harmonised requirements and vehicle system architecture;

    - System Requirement Review (SRR).

- Design

    - Concept and Preliminary Design Review (PDR).

The proposals should substantiate synergies and complementarities with foreseen, ongoing or completed activities, notably those described in the call topics related to ground combat capabilities and possibly related to manned and unmanned platforms under EDF and EDIDP.

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)

---

[122] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[123] '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.

[124] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

– 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).

For more information, please check *section 6*.

Functional requirements

The proposed activities should focus at least on a subset of functions for AIFV (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, including asymmetric theatres, with the minimum possible degradation of performance due to extreme environmental conditions and type of terrains, as defined in the relevant standards, and in compliance with EU/NATO standards;

– Be capable of conducting operations in Chemical, Biological, Radiological and Nuclear (CBRN) environment (to be also considered in the design phase);

– Be capable of handling the specific requirements that comes from conditions in special areas context:

– Comprising soft soil (marshland) and deep snow mobility capability;

– Impact from heavy snow, wind and low temperatures, implying e.g., ice build-up, blocking of sensors;

– Be able to act with own resources in low logistic support situations;

– Be capable of handling short standoff distances (<150m) with short time to engagement of target;

– Long shooting distance BLOS in covered terrain (e.g., forest);

– APS functionality in covered terrain (forest);

– Be capable of handling the specific requirements coming from the MOUT (Military Operations on Urbanised Terrain) context:

– Capability to detect threats in high elevations;

– Capability to engage and defeat threats in high elevations and short stand-off distances;

– APS functionality within high elevations and short stand-off distances;

– Capability to obtain situational awareness within an urban environment;

– Have a modular design which allows different mission capabilities relying on

high subcomponent commonality among different variants;

– Be designed to facilitate the possible future evolution into an "optionally manned" remotely controlled AIFV. Remote off-board control is expected to be assisted by on-board automatic functions, intended to reduce the workload for the remote operators in charge of the control so that, with the long-term goal that a single operator might control an AIFV. To be noted that the firing of any of the weapons equipping the AIFV must always remain under human control;

– Adaptive crew environment and support architectures, open and modular to enable the introduction of innovative technologies as soon as they become mature, in accordance with EU/NATO standards on Vehicle Architecture;

– Be designed with crew comfort and ergonomics in mind;

– Have 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;

– The vehicle be designed for being operated by a minimal crew (maximum 3), and the crew be given the maximum possible level of protection and survivability chance;

– The vehicle should be capable of hosting a fully combat geared infantry squad of 8 members (with 6 members being the minimum admissible threshold), and they must be given the maximum possible level of protection and survivability chance;

– Ensure interoperability with unmanned ground platforms and facilitate MUM-T (Manned-Unmanned Teaming) with adequate LOI (Level of Interoperability), and interoperability with Unmanned Systems (UAS/UGV). The interoperability for unmanned ground platforms may be in accordance with EU/NATO standards.

– Integrable and interoperable with a family of similar support platforms (system of systems);

– The complete vehicle (i.e., hull and turret), in full combat order, should be transportable in an in-service aircraft. The vehicle must have the possibility to dismantle components (e.g., additional armour) for transportation in smaller aircraft;

– The weight and the overall dimensions of the complete vehicle in full combat order must guarantee lethality, mobility (both tactical and strategic) and protection factors, together with a high power/weight ratio;

– Take into account constraints due to EU Member States and EDF Associated Countries' roads, railways, tunnels and bridges in order to meet transportability requirements; air transportability/ air drop should also be considered according to commonly applicable EU/NATO standards;

– Feature a maximum speed of at least 70 km/h on paved roads, at least 50 km/h (aiming at 65 km/h) on all off-road terrain and an operational range of not less than 600 km averaged on different type of terrains;

– Feature a wading depth without preparation of at least 1.50 m, a trench crossing capability of at least 2 m and an obstacle/step crossing capability of at least 0.7 m, and a ground clearance of at least 0.4 m;

– Feature a high "Operational Availability" to be capable to perform the assigned

missions;

— Provide effectors to engage modern AIFVs and MBTs with precise "fire-on-the move" capability at greater distances than current systems;

— Provide effectors to engage modern AIFV and MBT under LOS, NLOS and BLOS conditions;

— Provide capabilities to engage UAVs and perform air defence self-protection;

— Feature sophisticated C-UAS/C-SWARM/C-RAM capabilities to perform platform protection aiming at reducing the number of systems (e.g., multi mission system, or handing over some functions to other support platforms);

— Support smart/programmable ammunition;

— Ability for the vehicle of automatic threat detection, identification and tracking, including ability to handle multiple threats, and target distribution - enabling sensor-to-effector allocation (hard- and soft-kill capabilities), to support the decision-making process and ensure a rapid engagement;

— Have real-time and unified information and data presentation, provided by the sensors deployed on the platform and from external networks (including other combat support platforms) with low latency times;

— Have advanced PNT (Position Navigation and Timing) system (with inertial navigation capability) in order to ensure trusted PNT for the platform even in challenging GNSS 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 must also be considered;

— Feature an optimised trade-off between mobility, firepower, and protection;

— Provide protection against the following threats: mines and improvised explosive devices (IED), electronic warfare (EW) and cyber-attacks/offensive Cyber Electromagnetic Activities (CEMA), and at least 30 mm "Armour Piercing Fin Stabilised Discharging Sabot" (APFSDS) and other direct threats likely to become known over the whole duration of the project according to STANAG 4569 Protection Levels for Occupants of Armoured Vehicles Level;

— Feature a capability to counter direct threats, such as: Rocket Propelled Grenades (RPG) (including those with a functionality of disposable anti-tank rocket launcher like RPG-30), "High Explosive Anti-Tank" (HEAT) Munitions, "Anti-Tank Guided Missile" (ATGM; including 3rd generation ATGM with high angle of attack – e.g., NLOS and top attack), loitering ammunition and Unmanned Aerial Systems (UAS) and APFSDS (125 mm) according to STANAG 4686 DAS;

— 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.,: hybrid engines) and take into account other aspects of green technologies (e.g.,: total life CO_2 footprint, use of other materials, recycling, micro-grid management);

— Operate in silent mode for at least 10 km and extended silent watch with low thermal signature for at least 24 hours;

- Store and supply high density and power of electric energy for sensors, effectors and weapons;

- Have a range between 5% and 10% of growth potential without changing the assigned power/weight ratio;

- Be equipped with technologies to ensure enhanced Situational Awareness (SA), e.g.,: advanced display devices products, "transparent armour" concepts, allowing visualisation of the environment around the vehicle; automatic surveillance, detection, reconnaissance and identification;

- Have advanced 360 degrees 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 (including Friend or Foe, Battlefield Combat identification) of the vehicle status 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 vehicle mission system should be interoperable with other command and control systems, including the dismounted soldier command and control system, increasing the protection and effectiveness of soldiers once they get out from the vehicle in the combat zone. The interoperability may be in accordance with EU/NATO standards;

- Have a multi-sensor suite for threat detection and target acquisition (including, but not limited to: electro-optical sensors, acoustic sensors and radar), whose data should be available for Situational Awareness (SA) technologies and effectors through the fire control system, according to STANAG 4754[125] - NATO generic vehicle architecture (NGVA)s;

- Have 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;

- Feature static or dynamic on-board simulation for training (embedded);

- Be able to perform battle damage assessment without compromising survivability;

- Be able to monitor the health of the system and make the actual system performances data promptly available to the C2 systems, allowing to perform conditions-based maintenance.

Expected impact

The outcome should contribute to:

- Fill the majority of technology gaps identified in the "Overarching Strategic Research Agenda" concerning the armoured vehicles domain;

- Reduce, through commonality and mass production, the acquisition and lifecycle costs and create employment in each MS;

- Remove dependency from non-EU technologies and products;

- Reinforce interoperability of EU MS Armed Forces;

---

[125] https://nso.nato.int/nso/nsdd/main/standards?search=4754

- Reduce the logistic footprint and costs of EU Missions and Operations aiming at the implementation of infologistic systems;

- Competitiveness, efficiency and innovation capacity of the European defence technological and industrial base, as expected long-term effects enabled by the supported action;

- A common understanding and knowledge of technological basis as input to subsequent high level requirement analysis for next generation AIFV systems;

- Contribute to the defence and security interests of the EU and its Member States;

- Contribute to the EU strategic autonomy level of ambition;

- Contribute to Europe's resilience and European technological sovereignty;

- Contribute to European industrial autonomy;

- Contribute to excellence with the demonstration of a significant advantage over existing products or technologies.

EDF-2024-DA-NAVAL-FNP: Functional smart system-of-systems under an integral survivability approach for future naval platforms

Objectives

General objective

Evolving operational environment and threats require the development of cutting-edge maritime technologies, solutions, and systems, which should be able to operate interconnected in a fully integrated way under challenging multi-domain (i.e., land, aerial, surface, subsurface, and cyber) threat conditions.

Naval platforms trends are based on technologies, standards, solutions, and systems, all designed from the start to work integrated together in a coherent manner, ensuring the survivability of the platform against emerging threats. Therefore, the main objective of this topic is to identify, define, design, and develop them, to be integrated on future European naval platforms.

The topic should act as a real enabler for both the European naval industry and the EU Navies. In that context, it should be very inclusive to be adapted to the most European Navies' needs for their future naval platforms. It will allow EU Navies to remain at the forefront of technology, to maximise interoperability and the survivability by design, to operate with technological superiority, and to increase EU strategic autonomy. At industrial level, this topic should be an instrument for the European industry to assess and reinforce its ability to develop and support emerging key technologies.

Specific objective

The specific objective of this topic is to define the common operational requirements of the System of Systems (SoS) framework and the essential elements of the next generation of European naval platforms. Such a SoS framework is expected to embrace the supporting infrastructure including interfaces, data, and common and specific services. It must identify the technological needs for the future development of European naval platforms with special attention on emerging technologies, promising solutions, and the increased resilience of naval vessels when facing the most sophisticated threats by near real-time evaluation of survivability.

In particular, the topic should contribute to solve these specific challenges:

–   The capability to operate interconnected in a fully integrated way, under challenging multi-domain (i.e., land, aerial, surface, subsurface and cyber) threat conditions.

–   The definition and the design of the core architecture of the future European naval platforms by a SoS approach.

–   The analysis of naval vessels survivability aspects on an operational level, considering its three key aspects (i.e., susceptibility, vulnerability, and recoverability) under an integral approach, leading to a resilient ship.

This topic aims to identify and define essential elements for future European naval platforms as functional system building blocks by specifying a full set of new technologies, solutions, and systems to be fitted on board, covering the following main areas:

–   Four pillars:

–   **Combat System.** New threats based on emerging technologies lead to the development of combat systems with enhanced sensors collaborating under an extended top-side concept that increase the detection capability, in time and accuracy, as well as new weapons/effectors able to face them, based on decision making algorithms to allow shorter reaction time to engage those threats. The UxVs[126] are to be integrated into the Combat System as an extension of the detection and defence capability. In terms of survivability, specific challenges to susceptibility are the required countermeasures, both hard-kill and soft-kill, and their deployment, together with the ability to predict and manage where a missile or a torpedo might impact the vessel, as an important interface between susceptibility and vulnerability. UxVs should be also analysed in relation to ship survivability.

–   **Communication and Information System.** Solutions need to be sought to meet emerging challenges in this area such as the management of a big volume of data transmitted at high speed (comparable to 5G and ahead) in a very demanding operational theatre, the integrity and cybersecurity of the data, and the EU naval tactical cloud integrated in a military multidomain operations cloud. Special consideration should be made on anti-access/area denial (A2/AD) scenarios, defining embarked cloud capabilities to support the edge operation of joint forces overseas. Attention must also be paid to complete loss of connectivity due to denial or due to stealth reasons.

–   **Enhanced Platform Management System**. New threats and evolving technologies should lead to redefine the current concept of naval platforms to ensure enough and adequate power generation, as well as a proper top-side compatible with new weapons and UxV launch and recovery systems (LARS) on board. In the same way, future naval platforms should address efficient platform control and management, as well as increased power supply needs for future weapons and sensors, and new energy technologies to achieve the European Green Deal objectives. In addition, ship signature management, smart damage control, and survivability aspects should be considered because countermeasures, both hard-kill and

---

[126] Any one of the four categories of unmanned vehicle: ground, air, surface, or undersea.

soft-kill, and their deployment, or the impact of hypersonic missile or torpedo affect the vulnerability of the platform (e.g., a successful hard-kill engagement might result in debris hitting the ship, the success soft-kill deployments strongly affect the ship signatures). The impact of such events should be studied, and technical solutions to withstand the physical and system damage should be identified.

– **Navigation System.** Solutions should be sought for increased safety during navigation, independent satellite positioning system, accurate inertial navigation system, autonomous operations and multi-manned and unmanned, underwater, surface, and aerial vehicles coordinated navigation.

– One transversal area linked to the four pillars:

– **Survivability Advisory System Foundation**. The evolving threat landscape should result in a need for an advisory capability to assist in the setting of the ship signature management system, the deployment of hard-kill and soft-kill countermeasures, the adjustment of the ship's signature for hit-point management, the post-hit damage assessment, the remaining capability including strength and systems, and the deployment of recovery actions to regain functionality. This should also allow for future task group advisory capabilities, where high value assets should be protected by the task group, and the survivability of the task group is expected to be optimised due to advice across the task group.

Proposals should design a SoS framework: Solutions should be sought based on a service-oriented architecture or any other evolution, that might sustain the above-mentioned areas. It should include transversal capabilities like for instance, Artificial Intelligence (AI) Based Decision Making, Digital Twin, Federated Mission Networking, Through-Life Support based on virtual reality and remote systems monitoring, Cyberwarfare, or Survivability

Scope and types of activities

Scope

Proposals must address:

– The definition of common operational requirements of the essential elements for the future European naval platforms, covering the main areas (i.e., Combat System, Communication and Information System, Enhanced Platform Management System and Navigation System) under an integral survivability approach (i.e., Survivability Advisory System Foundation);

– The development of a concept of a SoS framework, typically based on a service-oriented architecture or any other evolution that might sustain the concerned areas;

– The definition of a modular, interoperable, scalable, and flexible concept design to support an architecture that should provide a versatile solution for answering future Navies´ needs and trends;

– The identification of emerging technologies that should respond to the operational needs of the future naval platforms, including integrated operational data-, messaging-, telecom-communication systems;

– The design of a tool for the management of the ship signature while advising on the status and solutions for timely and accurate deployment of

countermeasures, both active (e.g., advanced jammers, signature manipulators) and passive (e.g., flares, chaff, corner cubes), coordinated with hard-kill solutions, and including the prediction and management of the hit-point;

– The assessment of existing solutions and the consideration of new damage control systems where appropriate through automated systems, crew actions, and recovery of systems, while performing predictions of the state of the ship after incidents, likely based on AI that processes sensor readings/information and imaging;

– The design of an operational guidance system to support the Navigation System for ship operations with a damaged and undamaged ship (e.g., advice for helicopter operations, UxV deployment);

– The identification of the priorities on technologies to be further develop in the future, as well as the level of maturity to be achieved for the associated elements;

– The analysis of a tool for the European naval industry to assess and reinforce its ability to develop and support emerging key technologies;

– The operational assessment and the analysis of the technical viability, as well as the evaluation of the feasibility of the baseline concepts;

– The design of a joint technology demonstrator and to de-risk potential further activities in the future.

In addition, the proposals should substantiate synergies and complementarities, while avoiding unnecessary duplication, with activities described in previous call topics under EDIDP and EDF programmes.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (mandatory)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[127] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[128] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[129] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

- Integrating knowledge:

    - Illustrate an integral overview of available and to be developed technologies fitting in a future European System of Systems.

- Studies:

    - Identification and definition of the systems and the subsystems that may be considered essential elements for the future European naval platforms, according to the main areas.

    - Development of the Concept of Operations (CONOPS) under the direction of the participating Navies.

    - Defining operational requirements including threat analysis and assumptions, under the direction of the participating Navies, and derive use-cases (vignettes) as a common basis for the project.

    - Establishing the guidelines for an integral survivability approach, leading to solutions to be applied in the design phase of a vessel.

    - Defining the guidelines for the main areas (i.e., Combat System, Communication and Information System, Enhanced Platform Management System, Navigation System, and Survivability Advisory System Foundation) and for the SoS framework.

    - Elaboration of a comprehensive roadmap, identifying technologies to be considered and developed for the future European naval platforms, and

---

[127] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[128] '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.

[129] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

prioritising the developments on technologies and the associated elements for subsequent phases and the target TRLs[130] to be achieved.

- Tools for analysis of the European industrial capabilities to support current and emerging key technologies.

- Design:

  - Conceptual design of the essential elements and the framework to equip the future European naval platforms, considering the following aspects:

    - Identifying target architecture baseline concepts for SoS.

    - Identifying specific and common baseline services for the next generation of naval systems.

    - Assessing operational, technical, and programmatic feasibility of the baseline concepts, optimising naval vessel survivability.

    - Identifying a demonstrator of the common framework with the possibility to incorporate specific elements to perform partial tests for risk reduction and technology consolidation.

  - Tools for assessment of European industrial capabilities with the elaboration of an up-to-date map on skills and knowledge, processes, facilities, and equipment needed to design, develop, manufacture, repair and support key technologies and products for next generation of European naval platforms.

In addition, the proposals should cover the following tasks:

- System prototyping:

  - A prototype for the SoS framework should be developed, including some representative pillar functionality, in addition to some capability focused on the Survivability Advisory System Foundation. It should be developed to demonstrate the proof-of-concept between participating Navies.

- Testing:

  - Testing some performances of the prototype.

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

---

[130] Technology readiness level.

> 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).

For more information, please check *section 6*.

Functional requirements

The proposed SoS framework should:

– Be modular, interoperable, scalable, flexible, and adaptable to the requirements of the Navies;

– Be based on a service-oriented architecture and include the common and specific services for the essential elements;

– Consider the available government developed applications;

– Cover the main challenges for the next generation of European naval platforms while allowing the incorporation of new developments to face the future needs and threats, and serving the basement for future developments.

The conceptual design should consider new and promising technologies to:

– Shorten reaction times to engage the new threats like hypersonic missiles, or small targets that may appear in swarms, using the aid of decision-making algorithms;

– Enhance integration of new types of weapons based on conventional and non-conventional reaction means, as laser and direct energy weapons, or electromagnetic rail-gun weapons;

– Incorporate an integral missile defence, ballistic missile defence capability, and an integral anti-torpedo system;

– Integrate UxVs in combat system as an extension of detection and defence capability;

– Manage a big volume of data transmitted to high speed in very demanding operational scenarios;

– Ensure the integrity and security of data;

– Enhance the platform control capabilities such as ship signature management, smart damage control, or higher survivability, while harmonising requirements across the disciplines of susceptibility, vulnerability and recoverability;

– Increase the power supply needs for future weapons and sensors;

– Provide advanced navigation processing to improve the own-ship estimated position and navigation data even in GNSS[131] denied environment, considering

---

[131] Global navigation satellite system

other positioning methods like astronomical exploration and localisation;

- Facilitate a SoS approach by identifying transversal capabilities such as AI-based decision making, digital twin, federated mission networking, through-life support based on virtual reality and remote systems monitoring or cyberwarfare, that substantiates an integral conception of the ship systems.

Expected impact

The outcome should contribute to:

- the commonality of European naval systems to increase interoperability and interchangeability among European defence naval industries and Navies;

- an integrated survivability of naval vessels, more resilient against future threats, and with a reduced size and safer crew;

- promoting the EU strategic autonomy in the naval sector, configuring naval forces that respond to national and European strategic needs and trends;

- reducing the development and maintenance cost of future systems throughout their life-cycle;

- developing innovative systems, more efficient, scalable, and adaptable to different naval platforms.

EDF-2024-DA-UWW-AHMS: Autonomous heavy minesweeping system

Objectives

Uncrewed systems are a familiar asset in naval capabilities, and they are being increasingly adopted. These types of assets and the technologies that go with them have the potential to offer a diverse mission set, minesweeping being one of them. The maritime drones and their payloads currently used and integrated by the navies operate with different levels of autonomy and endurance. This topic aims to enhance naval minesweeping capabilities by pushing the design and level of the autonomy of particularly maritime drones. Furthermore, this topic addresses sweep gear and sweep sources for minesweeping operations adjoining the higher level of autonomy. In this context the drone/platform and its payload/sweeping gear form the minesweeping system.

Minesweeping is traditionally performed using mechanical or influence sweep sources towed behind a highly specialised and expensive crewed platform (minesweeper). Evolving technologies, such as autonomous features, offer new solutions to the minesweeping systems. These solutions in concert with new operational concepts offer European navies the opportunity to maximise the benefits of common development. Typically, a distinction can be made between drones with towed signature sources and those with integrated sources installed aboard.

The size and capability of a minesweeping drone and its payload are defined by the operational needs. These needs vary in environmental aspects from inshore operations with short transit and limited operation times in sheltered areas to operations in unsheltered areas potentially exposed to heavy wind and large waves with long standoff distances. The variation in operational needs with respect to the subject of protection can be from smaller merchant vessels and military vessels with reduced underwater signatures to large civilian merchants with significant underwater signatures.

The underwater signature and the shock resistance of the minesweeping system is a crucial part of its design and a fundamental feature of minesweeping operations.

The objective of this call is to reach at least technology readiness level 6 for a minesweeping system (platform/drone and payload designed for it)[132].

Scope and types of activities

Scope

The proposals must target minesweeping systems (platform/drone and payload/sweeping gear) with autonomous features that are capable of performing influence sweeping in open-sea conditions against mines that target large merchant vessels (such as Landing Platform Dock (LPD), Ro-Ro vessels etc. up to around 200m length). The proposals must investigate and develop capable and cost-effective drone systems for influence minesweeping. This includes the interfaces to enabling systems such as launch and recovery (LARS) of the sweep system and command and control (C2) systems (including planning and evaluation tools).

The proposals may include solutions that include modified mechanical minesweeping operations.

Furthermore, the proposals must address reducing time (improved effectiveness) and risk for personnel and materiel in minesweeping operations. Development of uncrewed systems and autonomous features are seen as enablers in this regard. Improvements must address at least vehicle design regarding underwater signatures, propulsion system, and shock resistance to benefit both operational quality and efficiency. Improvements should also address features such as low maintenance effort, survivability, endurance, and modularity.

The proposals should address multi-purpose functions with the aim of supporting additional Naval Warfare operations, such as, but not limited to, Anti-Submarine Warfare (ASW), Intelligence, surveillance and Reconnaissance (ISR), and Maritime Evacuation Operations. This may imply that features, such as, but not limited to, LARS, interaction with several autonomous underwater vehicles (AUVs), operation in Global Navigation Satellite System (GNSS) denied environments, towing of sonar systems, and use of mine disposal systems are incorporated.

The outcome should benefit a European interoperable and interchangeable NMCM Future Sweeping System designed with incremental capabilities to counter current and new mine threats consisting of enhanced intelligent platforms. Furthermore, the outcome should address the development of influence sweep source demonstrators for relevant underwater signatures (such as acoustic, magnetic, pressure and electric).

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 (**generating knowledge**)	No

---

[132] A functional version of the product working on a realistic environment able to draw conclusions on the technical and operational capabilities of the product (Horizon Europe).

	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[133] of a defence product, tangible or intangible component or technology	Yes (optional)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (optional)
(g)	**Qualification**[134] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[135] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

- Studies:

    - Research and studies on relevant signature levels, characteristic and frequencies as well as sweep tactics.

    - Defining the sweep signatures in the acoustic, magnetic, pressure and electric field. The research must be supported by simulation and experimentation.

    - Simulations must include at least mine influence sweeping, including multi sweep, in order to estimate the effectiveness against various mines.

        - Simulations must include at least the most basic mine setting and target selection features.

---

[133] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[134] '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.

[135] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

- Design:

    - Design, development, fabrication and integration of demonstrator signature sources, including, but not limited to, features on available energy, mechanical interface and shock requirements.

    - Design of minesweeper drone.

    - Design of uncrewed LARS of towed sweep sources if the proposed design includes towed sweep sources.

    - Design of minesweeping systems and sub-systems with attention to at least the following characteristics:

        - Shock resistance from underwater explosions.

        - Automated ship systems prepared for autonomy interfacing.

        - Non-magnetic materials and/or degaussing systems for reduced magnetic underwater signature.

        - Hybrid propulsion including battery powered electric propulsion for reduced underwater signature.

        - Resilience and robustness.

        - Autonomous detection of mine firings.

        - Environmental conditions (sea state, temperature etc.).

        - Uncrewed operations with the possibility of crewed operations in transition phases to-from operation or regulatory demand.

        - Digital infrastructure, and communication security.

        - Data and information security.

    - Design in support of autonomous features for drones including at least the following characteristics[136]:

        - Navigation including COLREGS[137] (collision avoidance) and GNSS denied situations (implies low derivation error).

        - Situational awareness.

        - Joint sweep operations with cooperating drones in formation.

        - Fault handling.

        - Mission planning, including interface to higher level operational planning tools.

---

[136] The use of best practice definitions, for instance the guide for UMS handling, operations, design and regulations developed by the SARUMS (Safety and Regulations for European UMS) ad-working group of the European Defence Agency, is advisable.

[137] Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs) (imo.org)

- The design of the autonomous features must be in accordance with international and national laws and regulations, including, where applicable, regulations for autonomous vessels[138] and class guidelines from international providers of classification.

- Design of user interface for maintenance, monitoring, and information exchange for minesweeping operations with drone.

- Design verification must include technical and functional tests of key technology components (such as sweep signature sources, drone sub-systems, autonomy and command and control systems) in a representative operational environment.

The proposals should cover at least the following tasks:

- Studies:

  - A supply chain analysis in the area of minesweeping solutions with autonomous features addressing critical dependencies for the EDTIB.

- Design:

  - The design should include alternative payloads for NMCM operations:

    - AUV operations with transport and LARS, also including underwater communication with AUV and position aiding.

    - Towing of mine hunting sonar systems.

    - Remote operation of mine disposal systems from drone.

    - Support vessel role equipment for mine clearance divers.

    - Role equipment for underwater surveillance (mission module) in support of barrier operations necessary to protect ongoing mine clearance operations.

    - Supporting vessel for mine jamming operations.

  - Communication systems to operate uncrewed systems with crewed systems including interworking and interoperability of applications & data.

  - Digital infrastructure and cyber security by design.

    - The digital infrastructure and security measures depend on the configuration/architecture of the System setup (System of Systems). This needs to be tested in isolated component and subsystem tests, as well as total systems tests.

- System prototyping:

  - The proposals should include technical system prototyping for a minesweeping system, including drone and influence sweep sources for relevant underwater signatures (any, some, or all of signatures such as acoustic, magnetic, pressure and electric).

---

[138] Including constrained manoeuvrability and towed gear.

A final demonstration should serve as an instrument to show to the military community the results of the targeted development activities, present potential military value and identify technology shortfalls that need to be addressed in subsequent activities in nations and in EU.

The design and development methodology should comply with NATO Architecture Framework (NAFv4)[139].

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).

For more information, please check *section 6*.

Functional requirements

The proposed solutions for a minesweeping system should meet the following functional requirements:

– The proposals should meet the common requirements for future minesweeping systems as defined by supporting Member States.

– The solutions should be capable of minesweeping in the tactics mine setting mode (MSM) against different mine types and in target simulation mode (TSM) for the simulation of various ship types, in particular large merchant vessels (such as LPD, Ro-Ro vessels etc. up to around 200m length).

– The solutions should be capable to operate in an open sea, as well as confined and shallow environment at moderate to rough sea state.

– The solutions should be capable to operate continuously (independently without replacement, recharging, reloading) in sweeping mode for at least 36 hours and in transit mode at least 72 hours.

Expected impact

The outcome should contribute to:

– Strategic autonomy of EDTIB in the area of minesweeping systems.

---

[139] NATO - NATO Architecture Framework, Version 4

- Fostering the technological cooperation of industries in the field of uncrewed sweeping drones and signature sources.

  - Interoperability of EU Member States Armed Forces:

    - System definition and proof of concepts for a future European minesweeping system.

    - Common requirements and harmonisation of minesweeping concepts.

EDF-2024-DA-SIMTRAIN-STME-STEP: Simulation and training for medical emergencies

Objectives

General objective

Medical (support) personnel often have limited access to extensive Prolonged Field Care (PFC) training due to a wide variety of factors. Studies to evaluate hospital preparedness have shown that good response plans can be developed for complex medical training scenarios (such as radiation exposure response), and that medical providers can be trained to follow these plans if the given training is realistic in its delivery.

Effective military medical training and readiness for PFC require decision training, performance of individual medical procedures and excellent teamwork skills in austere conditions of fast changing battlefield conditions of large-scale symmetrical conflict or natural disaster. Military medical training based on both computer-generated, hybrid and physical teaching materials creates advantage to development of cost-effective training courses for the military and civilian medical (support) personnel population and paramedics.

European Union has already started its efforts for developing military medics' innovative training solutions, focused on Field Care and Role 1 scenarios. In order to take full advantage of military medics training simulation, additional operational scenarios and functionalities in a virtual reality environment have to be developed and integrated into a network of federated toolbox which provides interconnection and joint access to simulation systems that are supporting different but mutually complementing simulation methods like mixed, augmented, hybrid, part task trainers, logistics, manikins and medical equipment, but currently are unevenly distributed in the European market for the medical personnel and paramedic training.

Specific objective

The topic aims to address the current operational challenges facing military medical personnel in the EU Member States (MS) and EDF Associated Countries, including in and out of areas of deployment.

Scope and types of activities

Scope

Proposals must address the development of a prototyped solution for a federation of available and enhanced medical simulation systems that support military medical curriculum and are connected to a (at best AI-based) feedback system (that may include real medical and health-data as benchmarking) that enables to see integrated picture of all training related information.

Proposals must therefore address:

– **Medical Training Modules**: The Medical Training Modules are designed to impart knowledge in military medicine to trainees. At present, the guidelines are anchored in Tactical Combat Casualty Care, serving as vital training curricula for both medical and non-medical personnel in civilian and military contexts. Looking ahead to future battlefield situations, insights from Ukraine underscore the importance of updating existing guidelines with a Prolonged Casualty Care environments. This adaptation is essential in preparing Europeans to confront diverse battlefield scenarios. Training modules can provide realistic, scenario-based learning experiences covering trauma, infections, and radiation exposure. They extend across various environments, including battlefield tranches, vehicles, and aircraft, offering comprehensive multi-modal and interdisciplinary training. The integration of virtual and mixed technologies elevates the delivery of educational content and learning retention. The overarching focus is effective communication, coordination, and preparedness for non-medical professionals in dynamic settings of the battlefield.

– **Supporting elements enabling Military Medical Training Multi-Modular Simulation Federated network**: The Military Medical Training Multi-Modular Simulation Federated network employs advanced technologies to create a comprehensive and realistic training environment. This includes cloud-based solutions for simultaneous management of large casualties, integration of digital computer simulated casualties for dynamic scenarios, physical simulated patients for hands-on training, and physical manikin systems replicating human responses. Crucially, seamless data exchange between computer-generated simulations and physical systems ensures a cohesive training experience. The interconnected federated network allows collaborative exercises across different locations, with real-time monitoring and feedback enhancing the learning process. Scalability, customisation, and integration of virtual, mixed, and augmented reality technologies contribute to an immersive and adaptable training platform for military non-medical and medical professionals.

– **Integration with Real World**: The integration of 5G technology into medical education signifies a transformative approach for European Union medical training centres. This integration facilitates the delivery of educational content with high-speed, low-latency connectivity, enabling real-time and immersive learning experiences. Learning analytics tools add a data-driven dimension, offering insights into individual and collective learning patterns. Augmented reality serves as a powerful teaching aid, particularly for Definitive Surgical Trauma Care, enhancing trainees' understanding through virtual overlays in the real-world environment. This comprehensive integration fosters scalable and distributed training solutions, promotes remote collaboration, and ensures standardisation and quality assurance across diverse training centres. The result is a cutting-edge educational paradigm that leverages advanced technologies to elevate the efficiency, accessibility, and effectiveness of medical training throughout the European Union.

In addition, the proposals must address concept development for interconnectivity of Military Medical VR Training Simulation Modules to a Battle Management System's simulation[140], including interface to a MS Battle Management System's simulation.

Moreover, proposals should address how real data and AI can be used to create an as

---

[140] Battle Management System's simulation here is meant to address MedC2 (Medical Command and Control) features to facilitate medical regulating and patient flow management as part of Battlefield Management (simulation).

realistic as possible environment facing medical, medical logistic and C2[141] challenges and provide suggestions to improve real life scenarios.

In addition, proposals may address the analysis of trainees' stress levels and hesitations and provides feedback.

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 (**generating knowledge**)	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 (**integrating knowledge**)	Yes (optional)
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory)
(d)	**Design** 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)	**System prototyping**[142] of a defence product, tangible or intangible component or technology	Yes (mandatory)
(f)	**Testing** of a defence product, tangible or intangible component or technology	Yes (mandatory)
(g)	**Qualification**[143] of a defence product, tangible or intangible component or technology	Yes (optional)
(h)	**Certification**[144] of a defence product, tangible or intangible component or technology	Yes (optional)
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	Yes (optional)

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

---

[141] Command and control

[142] 'System prototype' means a model of a product or technology that can demonstrate performance in an operational environment.

[143] '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.

[144] 'Certification' means the process by which a national authority certifies that the product, component or technology complies with the applicable regulations.

a) Medical Training Modules

- Studies:

  - Research analyse and define the existing military medical curriculum, focusing on identifying key areas for potential improvements and adaptations to meet the requirements of European Member States. An updated military medical curriculum framework, incorporating interactive and engaging content elements that reflect the diverse training needs and scenarios of EU Member States and EDF Associated Countries.

  - Review and assess existing MEDEVAC protocols and procedures, identifying areas for enhancement and integration into the virtual simulation environment, with a specific focus on logistics and casualty flow simulation medical regulating and MedC2.

  - Explore current practices and methodologies in Prolonged Field Care (PFC), and prolonged casualty care, focusing on understanding the necessary sustainment skills and training requirements for improving overall preparedness for armed forces medics and paramedics. Tactical Combat Casualty Care must be core of the training module.

  - Investigate and analyse various CBRNE scenarios, with a specific emphasis on burn injuries related to radiation exposure, aiming to develop comprehensive training modules that address recognition, decontamination, and effective trauma treatment strategies.

- Design:

  - Develop a scalable and dynamic simulation model for MEDEVAC scenarios (with a focus on tactical MEDEVAC manoeuvre elements), incorporating operational environment complexity logistical complexities and casualty flow dynamics to provide an immersive and realistic training experience for military medical personnel.

  - Design an integrated Prolonged Field Care (PFC) and Prolonged casualty care, based on the skills and equipment[145] of the medical (support) personnel module within the virtual reality training platform, focusing on the implementation of advanced medical procedures and treatments beyond conventional planning timeframes, emphasising critical decision-making and response strategies.

  - Create immersive and detailed CBRNE training simulations, incorporating lifelike scenarios and interactive modules that simulate various aspects radiological incidents, emphasising comprehensive training in recognition, decontamination, and effective treatment protocols.

- Prototyping:

  - Develop a functional prototype of the MEDEVAC simulation model (with a focus on tactical MEDEVAC manoeuvre elements), testing its capabilities in simulating realistic logistical and casualty flow scenarios,

---

[145] Focusing on personnel medical equipment (« backpack », TACEVAC, etc.) and additional on medical devices (e.g., patient monitors).

and validating its effectiveness in providing an immersive training experience for military medical personnel. (expected to reach TRL 7)

‒ Create a prototype of the Prolonged Field Care (PFC) and prolonged casualty care module within the virtual reality training platform, testing and validating advanced medical procedures and treatments beyond conventional planning timeframes, and assessing its effectiveness in improving critical decision-making and response strategies. (expected to reach TRL 7)

‒ Build interactive prototypes of the CBRNE training simulation, testing lifelike scenario and interactive module that simulate various aspects of radiological incident, and assessing the effectiveness of the training in recognition, decontamination, and effective treatment protocols. (expected to reach TRL 7)

‒ Testing:

  ‒ Perform rigorous testing of the military medical curriculum framework, assessing its effectiveness in addressing the diverse training needs and requirements of European Member States, and soliciting feedback from key stakeholders for further improvements.

  ‒ Test the MEDEVAC simulation model in simulated scenarios (with a focus on tactical MEDEVAC manoeuvre elements), assessing its ability to accurately simulate logistical and casualty flow dynamics, and soliciting feedback from military medical personnel for further enhancements and adjustments.

  ‒ Perform comprehensive testing of the Prolonged Field Care (PFC) module within the virtual reality training platform, evaluating its effectiveness in simulating advanced medical procedures, treatments and therefore also the usage of personal and/or vehicle specific medical equipment beyond conventional planning timeframes, and gathering feedback from trainees for further refinements.

  ‒ Conduct rigorous testing of the CBRNE training simulation, assessing their effectiveness in simulating realistic radiological incident, and soliciting feedback from trainees to ensure comprehensive training in recognition, decontamination, and effective treatment protocols.

b) Supporting elements enabling Military Medical Training Multi-Modular Simulation Federated network:

‒ Studies:

  ‒ Conduct a comprehensive literature review and analysis of the current state of Military Medical Training Multi-Modular Simulation Federated networks and associated technologies.

  ‒ Study the integration possibilities and challenges related to the exchange of data between computer-generated, physical manikin systems and medical equipment, emphasising the development of open standards for seamless data transfer and analysis.

  ‒ Research cloud-based solutions for managing large quantities of casualties simultaneously and the combination of digital computer simulated casualties, physical simulated patients and physical manikin

systems, with a focus on scalability, efficiency, and resource optimisation within a simulated training environment.

- Design:

    - Develop a detailed blueprint and architectural plan for the implementation of the Military Medical Training Multi-Modular Simulation Federated network, outlining the specific technical components and their interconnections.

    - Design an integrated data exchange system between computer-generated and physical manikin systems, and physical simulated casualties (with a digital device to simulate a casualty and thereby visible in the trainer) focusing on the development of standardised protocols and interfaces to facilitate seamless data transfer and interoperability between different simulation platforms and in addition to medical equipment.

    - Design the architecture of a cloud-based infrastructure for handling large quantities of casualties simultaneously, ensuring efficient resource allocation, data management, and communication protocols for seamless coordination and collaboration among various training centres and facilities.

- Prototyping:

    - Develop an initial prototype of the Military Medical Training Multi-Modular Simulation Federated network, integrating essential components and functionalities based on the design specifications and architectural plan (expected to reach TRL 6).

    - Construct a prototype of the data exchange system between computer-generated and physical manikin systems, testing its compatibility and effectiveness in facilitating seamless data transfer and interoperability between different simulation platforms (expected to reach TRL 7).

    - Develop a functional prototype of the cloud-based infrastructure for managing large quantities of casualties simultaneously, testing its efficiency in resource allocation, data management, and communication protocols for seamless coordination and collaboration among various training centres and facilities (expected to reach TRL 5).

- Testing:

    - Conduct extensive testing of the streaming software solution, evaluating its compatibility with 5G technology, and assessing its efficiency in delivering seamless and high-quality data transmission across various training locations and facilities within the European Union.

    - Test the cloud-based infrastructure for managing large quantities of casualties simultaneously, evaluating its efficiency in resource allocation, data management, and communication protocols, and soliciting feedback from training centre administrators for further improvements.

    - Conduct comprehensive system testing of the Military Medical Training Multi-Modular Simulation Federated network, evaluating its

performance, scalability, and interoperability across various simulated training environments and scenarios.

c) Integration with Real World:

- Studies:

    - Investigate and evaluate various learning analytics tools and systems, considering their applicability and effectiveness in tracking individual training progress and competency within the simulated environment.

    - Study the capabilities and limitations of 5G technology, particularly in relation to its potential integration for scalable and distributed training solutions across the European Union.

    - Investigate the current landscape of Augmented Reality surgical simulators and their applicability in providing training to different surgical capability levels (focusing on (r)DCS at Role 2 level, additional up to Role 4), focusing on the enhancement of surgical decision-making skills and techniques based on the specific guidelines.

- Design:

    - Design the architecture of a secure and efficient streaming software solution, leveraging 5G technology to enable seamless and high-quality data transmission across various training locations and facilities within the European Union.

    - Create a robust and user-friendly Learning Analytics Tool interface, integrating advanced tracking and monitoring features to provide real-time feedback and comprehensive data analysis capabilities for training administrators and instructors, but also the learning loop to use these data to enhance and/or simplify protocols.

    - Develop an augmented reality surgical simulation environment tailored to different surgical capability levels (focusing on (r)DCS at Role 2 level, additional up to Role 4) training, incorporating realistic surgical scenarios and procedures based on specific guidelines, emphasising hands-on training and decision-making skills for complex medical interventions.

- Prototyping:

    - Develop a prototype version of the streaming software solution, ensuring compatibility with 5G technology and validating its ability to deliver seamless and high-quality data transmission across various training locations and facilities within the European Union (expected to reach TRL 5).

    - Build a functional prototype of the Learning Analytics Tool interface, incorporating key tracking and monitoring features to allow for real-time data analysis and visualisation, enabling comprehensive insights for training administrators and instructors (expected to reach TRL 7).

    - Build a prototype of the augmented reality surgical simulation environment for training at different surgical capability levels (focusing on (r)DCS at Role 2 level, additional up to Role 4), testing and validating its effectiveness in providing hands-on training and decision-

making skills for complex medical interventions based on specific guidelines (expected to reach TRL 6).

– Testing:

 – Execute thorough testing of the Learning Analytics Tool interface, validating its tracking and monitoring capabilities, and ensuring its seamless integration with the training platform to provide real-time data analysis and comprehensive insights for training administrators and instructors.

 – Perform thorough testing of the data exchange system between computer-generated and physical manikin systems, assessing its compatibility and effectiveness in facilitating seamless data transfer and interoperability between different simulation platforms, and gathering feedback from system administrators and users for further enhancements.

 – Conduct comprehensive testing of the augmented reality surgical simulation environment for training at different surgical capability levels (focusing on (r)DCS at Role 2 level, additional up to Role 4), evaluating its effectiveness in providing hands-on training and decision-making skills for complex medical interventions based on the specific guidelines, and gathering feedback from medical professionals for further refinements and adjustments.

In addition, proposals must address the following cross-cutting design activity:

– Design a concept for interconnectivity of Military Medical VR Training Simulation Modules to a Battle Management System's simulation, including interface to a MS or EDF Associated Countries Battle Management System's simulation.

Proposals may also address the following cross-cutting activities:

– Study and Design a software decision support system elements, geared towards strategic planning of resource distribution, to training of operators using such resources to address multiple trauma victims in remote or poorly accessible theatres, and to the real-time support of decision making in the wake of an actually occurring accident. The technical specifications ought to include the class (types) of events addressed, the resources to be managed, the timeframe available for cognitive support delivery to the decision-maker. Test-beds, typically simulated (table-top or physical exercises) will have to be described and their relevance to the validation of the product detailed.

– Study and Design and create a stochastic (at its best AI-optimised) training simulation scenario, with multiple victims and realistic distribution of available resources, statistically adherent to disasters effectively recorded or to anticipated battlefield situations. It must include a learning loop on how to update these scenarios by real-life data of such incidents.

– Study and Design methods to augment situational awareness and decision support systems for decision-makers in real-time crisis development.

The proposals must substantiate synergies and complementarities with foreseen, ongoing or completed activities in the field of Simulation and Training, notably those described in the call topic EDIDP-SME-2020[146] related to *Simulation and Training*.

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).

For more information, please check *section 6*.

Functional requirements

The proposed product and technologies should enable medical (support) personnel and paramedics with regular joint and frequent access to lifelike, secure, immersive training environment from Care Under Fire throughout multiple levels of surgical capability (focusing on (r)DCS at Role 2 level, additional up to Role 4) and being designed to respond to the evolving training requirements for medics and paramedics both at individual and team levels, contributing for their readiness for national and multi-national missions.

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

a) Medical Training Modules:

– MEDEVAC: Connection between Field Care by MEDEVAC scenario to Role 1 and beyond to provide connection to a constructive simulation tool able to simulate logistics and the casualty flow and the (Med) C2 capability, including at least an interface to a MS battle management system.

– Prolonged Field Care (PFC)/ Prolonged Casualty Care: Creation of a layer of PFC to the existing virtual reality medical training scenarios to increase training complexity, stress factor for the trainees and improve readiness for the armed forces medics and paramedics. The content of this training should address sustainment skills for Field Care applied beyond doctrinal planning timelines (10-60-120 min) in order to decrease patient mortality and morbidity until the patient arrives at the next appropriate level of care.

– CBRNE: Developed training scenarios to include CBRNE injury sample with a

---

[146] Funding & tenders (europa.eu)

focus on burn injuries related to radiation exposure to teach how to recognise it, decontamination, trauma treatment and disposition.

– Large Quantities of Casualties for Simultaneous Care: Developed cloud-based capability to increase the amount of patients with up to 30 or more causalities.

b) Supporting elements enabling Military Medical Training Multi-Modular Simulation Federated network

– Military Medical Curriculum:

– Developed Prolonged Field Care military medical curriculum based on the available guidelines and research studies to enable unified set of instruction and ability to update those for the European Member States.

– Tactical Combat Casualty Care (TCCC) is a critical teaching curriculum that emphasises care under fire, tactical field care, and medical evacuation. Learnings from Ukraine, where prolonged field care has become necessary, underscore the need to adapt the curriculum. This requires incorporating provisions for sustained treatment beyond the initial phase, ensuring that combatants are equipped to handle extended care scenarios effectively.

– Additionally, the inclusion of Chemical, Biological, Radiological, and Nuclear (CBRN) elements in the curriculum is imperative. This means introducing comprehensive training in Personal Protective Equipment (PPE) usage, decontamination procedures, and the treatment of radiological exposure, to ensure troops are adequately prepared to manage diverse battlefield threats.

– Furthermore, the evolving protocols for medical evacuation, based on the insights garnered from Ukraine, should reflect a heightened emphasis on accommodating prolonged care scenarios and mitigating the risks associated with dynamic combat environments. This adjustment aims to optimise the efficiency and effectiveness of the evacuation process, prioritising the timely transfer of casualties.

– Learning Analytics Tool: Developed component to track individual training progress, competency, and proficiency across and between the toolboxes/systems of the federated network able to:

– Generate adaptive learning experiences that enable individually tailored training programs to increase learning retention and effects;

– Provide both distributed debriefing and AAR for training centres through the European Union, and an automated learning analytics system at scale for instructors and commanders.

– Scalability / Distribution via 5G: Developed streaming software from cloud services across European Union with 5G and beyond to integrate products and services into IT systems of end-users.

– Federated medical training network applying existing open and applicable standards and including the following features:

– Interoperability: Ensures seamless communication and data exchange between various medical training entities, promoting comprehensive and unified learning experiences.

– Versatile Learning Modalities: Facilitates diverse learning approaches,

including virtual, augmented, mixed, and extended reality, as well as constructive simulations, enabling trainees to acquire practical skills in a simulated environment.

- Robust Competency Tracking: Enables comprehensive monitoring and assessment of individual progress, competence assertion statements, and on-the-job experiences, ensuring a holistic approach to skill development and evaluation.

- Integrated Federated Network: Provides a unified ecosystem for medical training across multiple institutions and organisations, fostering collaboration and knowledge sharing among diverse stakeholders.

- Granular Data Tracking: Offers detailed tracking capabilities, allowing the monitoring of specific skills development, course completion, and individual performance, facilitating targeted interventions and personalised learning paths.

- Extensive Customisation Options: Empowers users to tailor the platform to specific training needs and organizational requirements, ensuring a tailored and effective learning experience for all participants.

- Learning Management System (LMS) should include comprehensive integration and tracking capabilities, ensuring seamless coordination and monitoring of learning activities within the network. The LMS should be fully integrated within the federated medical training network, allowing for streamlined data management and tracking of various learning events, including live events and simulations. Competence assertion statements should be collected through comprehensive after-action reviews, capturing detailed insights into trainee performance and skill development.

- Individual on-the-job experiences contributing to training and education should be meticulously tracked through the LRS, ensuring a comprehensive understanding of each learner's professional development. The APIs within the system should be fully open and enable seamless integration with external applications, promoting flexibility and interoperability. Data export functions should be provided to allow for data analysis and reporting outside the system.

- The results should excel in tracking very granular details, such as specific skills acquisition versus overall course completion, providing a nuanced understanding of trainee progress and proficiency. The results should also generate detailed reports and analytics, including performance metrics, skill mastery levels, and learning outcomes, which can be easily configured to meet the specific needs of different stakeholders.

- The result should offer extensive customisation options, enabling users to adapt the platform to diverse training requirements and institutional preferences. The result should be able to scale efficiently to accommodate approximately 30 000 concurrent users, ensuring seamless access and smooth user experiences across the network.

c) Integration with Real World:

- Data Exchange Between Computer-Generated and Physical Manikin Systems, physical simulated casualties and medical equipment provided with a digital simulation device. Integration with physical manikins in combination with centralised data analysis and distribution. Open standards and/or other simulation systems or their providers available to transfer scenario data between the systems.

- Integration with Augmented Reality simulators for training at different surgical capability levels (focusing on (r)DCS at Role 2 level, additional up to Role 4) in context. Surgical decision training and skills based on the specific guidelines.

Expected impact

The outcome should contribute to:

- Reduce dependencies on non-European suppliers by boosting the EDTIB and promoting the development of a European solution.

- Increase variations of military medical simulation training scenarios, providing better-prepared personnel both at individual and team's level, including distributed, multi-national team training.

- Enable one-stop toolbox of interconnected simulation systems that are currently dispersed across Europe to create unified environment for Prolonged Field Care military medical training, including mixed, augmented, hybrid, part-task trainers, logistics and manikins.

- Expanded immersive virtual reality simulation training environment for continuous education and maintenance of readiness for military medics critical for their missions, particularly in Prolonged Field Care circumstances with situations having high casualty numbers requiring treatment of polytrauma including CBRNE injury types.

- Significantly enhance availability, intensity, and speed of military medical personnel training.

- Reduce costs for military medical personnel cooperation training, particularly on cross-border training practices.

- Increase interoperability between paramedics, military medical (support) personnel and civilians both in military and natural disaster context.

- Provide more accessible training environments to strengthen cross-border civil–military medical forces collaboration for emergency preparedness, resulting in increased patient safety- enabled reuse of simulation data on user performance for strategic and tactical decision-making of national armed forces.

- Provide Military Medical Modelling & Simulation as a Service to the IT systems of the European Union Member States armies.

- Enhance European technological know-how in medical simulation systems strengthening European Defence Technological and Industrial Base (EDTIB).

3. Available budget

The estimated available call budget is **EUR 579 000 000**.

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

Topic	Topic budget	Fixed maximum number of projects
EDF-2024-DA-C4ISR-AIMA-STEP: AI-based multifunctional aperture and transceiver	**EUR 45 000 000**	No (but normally 1 expected)

Topic	Topic budget	Fixed maximum number of projects
EDF-2024-DA-C4ISR-COMS-STEP: Defence multi-dimensional communication standard	EUR 25 000 000	No (but normally 1 expected)
EDF-2024-DA-C4ISR-SEEU-STEP: Small enhanced European UAS	EUR 11 000 000	No (but normally 1 expected)
EDF-2024-DA-C4ISR-MALE: Medium altitude long endurance RPAS	EUR 100 000 000 excluding remuneration of OCCAR	No (but normally 1 expected)
EDF-2024-DA-CYBER-NGCR-STEP: Next-Generation Cooperative Cyber Range	EUR 48 000 000	No (but normally 1 expected)
EDF-2024-DA-SPACE-EPW-STEP: Secure waveform for satellite communications	EUR 25 000 000	No (but normally 1 expected)
EDF-2024-DA-ENERENV-EEMC-STEP: Energy-independent and energy-efficient systems for military camps	EUR 40 000 000	No (but normally 1 expected)
EDF-2024-DA-AIR-NGRT: Next generation rotorcraft	EUR 100 000 000	No (but normally 1 expected)
EDF-2024-DA-GROUND-UGS-STEP: Multipurpose unmanned ground systems	EUR 50 000 000	No (but normally 1 expected)
EDF-2024-DA-GROUND-BLOS: Beyond the line-of-sight close combat	EUR 25 000 000	No (but normally 1 expected)
EDF-2024-DA-GROUND-AIFV: Next generation armoured infantry fighting vehicle	EUR 25 000 000	No (but normally 1 expected)
EDF-2024-DA-NAVAL-FNP: Functional smart system-of-systems under an integral survivability approach for future naval platforms	EUR 45 000 000	No (but normally 1 expected)
EDF-2024-DA-UWW-AHMS: Autonomous heavy minesweeping system	EUR 30 000 000	No (but normally 1 expected)
EDF-2024-DA-SIMTRAIN-STME-STEP: Simulation and training for medical emergencies	EUR 10 000 000	No (but normally 1 expected)

The availability of the call budget still depends on the adoption of the budget 2025 by the EU budgetary authority.

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:	20 June 2024
Deadline for submission:	5 November 2024 – 17:00:00 CET (Brussels)
Evaluation:	November 2024 - May 2025
Information on evaluation results:	May 2025
GA signature[147]:	May - December 2025

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)

  - 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)

---

[147] In case of management by an entrusted entity, this timeframe may be different.

- declarations on procurement intent and common specifications (if the project covers system prototyping, testing, qualification or certification activities)

- ownership control declarations (including for associated partners and subcontractors involved in the action)

- 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.)*.

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

6. Eligibility

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[148] 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[149].

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'[150]. ⚠ 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 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 16th 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,

---

[148] '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.

[149] See Article 197(2)(c) EU Financial Regulation 2018/1046.

[150] For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.

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)[151] and entities covered by Commission Guidelines No [2013/C 205/05](#)[152])*. 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

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 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.

⚠ Moreover please take into account that development actions are subject to the following additional eligibility criteria:

- the consortium must demonstrate that the costs of the action that are not covered by the EDF funding are financed by other means *(e.g. Member States or associated countries' contributions or co-financing from legal entities)* — this is done by submitting the required co-financing declarations signed by your cofinancers *(see section 5 and instructions in the [template](#))*.

- proposals addressing design activities must include evidence that these activities are based on harmonised defence capability requirements jointly agreed by at least two Member States or EDF associated countries — this is done by submitting the harmonised defence capability requirements declarations signed by at least two Member States or EDF associated countries *(see section 5 and instructions in the [template](#))*.

- proposals addressing prototyping, testing, qualification or certification activities must include evidence that at least two Member States or EDF

---

[151] 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](#).
[152] 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).

associated countries intend to procure the final product or use the technology in a coordinated manner, including through joint procurement where applicable and that the actions are 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 — this is done by submitting the declarations on procurement intent and common specifications signed by at least two Member States or EDF associated countries *(see section 5 and instructions in the* template*)*.

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

- 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 not allowed 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: **must 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*).

For completing the ethics issues table in the Submission System, see *How to complete your ethics self-assessment*.

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](#)[153] and its implementing rules[154].

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

— 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.

---

[153] 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).
[154] See Article 27(4) EDF Regulation.

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.

ℹ️ 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[155]:

   – 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[156] (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)

   – 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[157]:

   – during the award procedure they misrepresented information required as a condition for participating or failed to supply that information

---

[155] See Articles 136 and 141 of EU Financial Regulation 2018/1046.

[156] 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.

[157] See Article 141 EU Financial Regulation 2018/1046.

- 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.

Priority order for proposals with same 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 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

Evaluation result and grant preparation

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. Proposals under topics EDF-2024-DA-C4ISR-AIMA-STEP, EDF-2024-DA-C4ISR-COMS-STEP, EDF-2024-DA-C4ISR-SEEU-STEP, EDF-2024-DA-CYBER-NGCR-STEP, EDF-2024-DA-SPACE-EPW-STEP, EDF-2024-DA-ENERENV-EEMC-STEP, EDF-2024-DA-GROUND-UGS-STEP and EDF-2024-DA-SIMTRAIN-STME-STEP that are eligible and exceed the evaluation thresholds will be awarded a Sovereignty Seal.

⚠ 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.

⚠️ For projects where the Commission decides on management by the European Defence Agency (EDA), the Organisation Conjointe de Coopération en Matière d'Armement/Organisation for Joint Armament Co-operation (OCCAR) or another entrusted entity, you will receive the evaluation result letter by us and then be invited to sign the grant with the relevant entrusted entity.

Business coaching

The EDF also has a business coaching component. Successful SME beneficiaries will be offered business coaching, to accelerate their growth and guide them in their business challenges to reach the defence market.

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[158] (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 topic 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

---

[158] In this section, 'cross-border SMEs or mid-caps' refer to SMEs or mid-caps which are established in Member States or EDF associated countries other than those where the legal entities cooperating within the consortium which are not SMEs or mid-caps are established.

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
Overall weighted (pass) scores	**37**	**55**	N/A

Each award criterion will be scored from 0 to 5 (half-points will be allowed) using the following scale:

0 — The proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

1 — Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.

2 — Fair. The proposal broadly addresses the criterion, but there are significant weaknesses.

3 — Good. The proposal addresses the criterion well, but a number of shortcomings are present.

4 — Very Good. The proposal addresses the criterion very well, but a small number of shortcomings are present.

5 — Excellent. The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

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[159]

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)

---

[159] In case of management by an entrusted entity, these rules may be different.

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 (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 (not allowed)

  - 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)[160]:Yes

- SME owner/natural person unit cost[161]: Yes

- subcontracting costs:

  - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries

- travel and subsistence unit cost[162]: 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: not allowed

  - internally invoiced goods and services (unit cost according to usual cost accounting practices)[163]: 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

---

[160] 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.

[161] 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).

[162] 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).

[163] 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.

–   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

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 normally:

- limited joint and several liability with individual ceilings — *each beneficiary up to their maximum grant amount*

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)*

- specific national security framework under Article 27(4) of the EDF Regulation: Yes

Ethics rules: *see Model Grant Agreement (art 14 and Annex 5)*

- specific ethics rules in Annex 5: Yes

IPR rules: *see Model Grant Agreement (art 16 and Annex 5):*

- list of background and background free from restrictions: Yes

- results free from restrictions: Yes

- ownership of results: Yes

- protection of results: Yes

- transfer and licensing of results: Yes

- rights of use on results: Yes

- for EDF Research Actions: access to results for policy purposes: Yes

- for EDF Research Actions: access to special report: Yes

- for EDF 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 (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 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.

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 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.

<div align="right">**Annex 1**</div>

<div align="center">**EDF types of action**</div>

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

<div align="right">**Annex 2**</div>

<div align="center">**Guarantees pursuant to Article 9(4) of the EDF Regulation**</div>

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*.

<div align="right">**Annex 3**</div>

<div align="center">**Security aspects**</div>

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
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	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)*
Bulgaria	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Croatia	TAJNO	POVJERLJIVO	OGRANIČENO
Cyprus	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Czech Republic	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG

France	SECRET SECRET DÉFENSE *(Note 2, see below)*	CONFIDENTIEL DÉFENSE *(Notes 2 and 3, see below)*	*(Note 4, see below)*
Germany ***(Note 5, see below)***	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
Ireland	SECRET	CONFIDENTIAL	RESTRICTED
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET	KUNFIDENZJALI	RISTRETT
Netherlands	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Poland	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	SECRETO	CONFIDENCIAL	RESERVADO *(Note 6, see below)*
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO *(Note 6, see below)*	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG

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.