December 2022

ARTES 4.0 Strategic Programme Line

"Space Systems for Safety and Security" (4S)

Work Plan 2023

1. Introduction

Our society and economy are increasingly dependent on secure telecommunications networks. These networks are required for the secure operation of critical infrastructures, governmental services or in transport. They may constitute a systemic point of failure with major safety and security threats, particularly during disruptions caused by natural or human-made disasters or by cyberattacks. Satellite communications can provide a secure space component as a self-standing element or in complement to the terrestrial telecommunications system.

In 2019, ESA Member States decided to focus their efforts on this domain by the creation of a Strategic Programme Line named "Space Systems for Safety and Security (4S)" under the ESA ARTES (Advanced Research in Telecommunications Systems) programme. The 4S Strategic Programme Line objective is to support the development of Next Generation Satcom Systems aimed at providing secure, safe and sovereign communications for governmental/institutional and public regulated services and ensuring resilience to society's critical digital infrastructures.

As part of the 4S strategic action, the rolling Work Plan aims to support the development of critical technologies deemed essential to support the future implementation of safety and security satcom systems.

In September 2022, a further 17 Work Plan activities were approved and added to the rolling Work Plan. The full list of activities can be found in Annex I and described in Annex II

2. Implementation

The following implementation will be followed:

Phasing: phasing of the contractual activities may be considered depending on the risks associated with the development, the maturity of the technologies, and potential early market perspectives.

Parallel contracts: in accordance with the ARTES 4.0 Specific Implementing Rules for the Generic Programme Line "Core Competitiveness", proposals that have not ranked first in

the Tender evaluation, may be re-considered for award of a parallel contract under the following conditions:

- The proposal is ranked at least “good” (60)
- The proposed technology is innovative and technically mature
- The starting TRL is lower than 4.
- The delegations concerned reconfirm their support for the proposal.

Procurement Policy: the following procurement policies are foreseen for the proposed activities:

C: Activities in open competition without any further restrictions.
C1: Activities in open competition limited to non-Large System Integrators (LSIs) as prime. LSIs are allowed to participate as sub-contractors.
C2: Activities are in open competition, where a significant participation of non-LSIs is requested.
C3: Activities restricted to SMEs & R&D organisations, preferably in cooperation.
C4: Activities in open competition, subject to the SME subcontracting clause.

The full definition of these procurement policies is provided in document ESA/IPC(2005)87, rev.4.

Implementation Category: The activities comprising this work plan are designated as either B (Baseline) or R (at the Request of Delegates). The assignment of activities into these implementation categories is not a declaration of technological, commercial, or programmatic priority. Instead, it simply indicates whether an activity requires a prior request from a Delegation for the ITT to be generated and released. This categorisation could, for example, be related to a limited industrial landscape for the proposed activity.

Activities identified as B will be issued according to the schedule published (and regularly updated) on the ESA-STAR website and ESA ARTES web site: https://artes.esa.int/artes-planned-activities-summary-table. B activities for which industry and Participating States declare an interest will be given precedence when preparing Invitations To Tender (ITT). Such interest can be notified directly to the ARTES 4S Programme Office via the contact email address: artes-4S@esa.int.

Activities designated Implementation Category R will only be initiated either:
• On the explicit request of at least one delegation; or
• On the initiative of the Executive following consultation of the JCB.

Annex I: SUMMARY TABLE FOR THE 4S WORK PLAN 2023

ESA-initiated Invitations to Tender:

Activity Ref.	Title	Cost	Classification	Cost (K€) (Classification B)	Cost (K€) (Classification R)	Proc. Policy
	1. SYSTEM/ NETWORK / PROTOCOLS					
	1.1 System, Networking and Management					
3A.172	Resilient and secure multimedia communications from unmanned aerial/maritime vehicles using multiple unreliable networks	600	R	0	600	C1
3A.173	Resilient distributed network management for secure satellite constellations	500	B	500	0	C
3A.180	Secure and application-selective multicasting in multi-layer satellite constellation networks	500	B	500	0	C
	Subtotal			**1000**	**600**	
	1.2 Security and Cryptography					
3D.013	Multi-purpose Quantum Key Distribution receiver for optical ground stations	950	B	950		
3D.014	Anti-jamming techniques using artificial intelligence for frequency hopping waveforms	500	R	0	500	C
3D.015	Cyber resilience framework for space communication systems	400	B	400	0	C
3D.016	Scalable public key infrastructure concept for large constellation secure communications	500	B	500	0	C
3D.017	Lightweight post-quantum key exchange protocol for IP data transfers over satellite	600	B	600	0	C
3D.018	Security assessment, testing and validation capability for innovative secure communications and quantum technologies	1500	B	1500	0	C
3D.019	Cyber-range testbed for satellite communications physical and data link layers	750	B	750	0	C
	Subtotal			**4700**	**500**	
	2. SPACE SEGMENT - PLATFORM					
	2.1 Command and Data Handling					
4G.041	Ka-band radio frequency front-end resistant to intentional interference for secure TT&C	600	B	600	0	C
	Subtotal			**600**	**0**	

	3. SPACE SEGMENT - PAYLOAD						
	3.1 Payload - System and Architecture						
5A.082	Breadboarding of critical technologies for a multi-beam satellite receiver for aircraft MODE-S signals	900	R		900		C
	Subtotal			**0**		**900**	
	3.2 RF Repeater and Signal Processing						
5C.481	Radio spectrum situational awareness functions embedded in telecommand/telemetry receivers	600	B	600	0		C
5C.482	Highly integrated beamforming networks for governmental X-band applications	1200	B	1200	0		C
5C.483	Robust timing and synchronisation techniques for secure communications	800	B	800	0		C
	Subtotal			**2600**		**0**	
	4. USER TERMINALS						
	4.1 Professional User Terminals						
7A.073	Array Antenna with Directional Modulation for secure governmental satcom User terminal	750	B	750	0		C
	Subtotal			**750**		**0**	
	4.2 User Terminal Mobile						
7C.078	Time reference for portable terminals used in secure communications	700	B	700	0		C
	Subtotal			**700**		**0**	
	TOTAL (k€)			**10350**		**2000**	

Annex II: DETAILED DESCRIPTION OF NEW ESA-INITIATED ACTIVITIES PROPOSED FOR THE 4S WORK PLAN

1. System/Network/Protocols

1.1. System, Network and Management

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3A.172	Resilient and secure multimedia communications from unmanned aerial/maritime vehicles using multiple unreliable networks	600	R
Objective:	The objective of this activity is the design and demonstration of network protocols that can use multiple unreliable satellite and terrestrial networks for increased resilience and security for retrieval of multimedia data with multiple QoS classes from drones and unmanned maritime vessels.		
Targeted Improvements:	This technique will allow at least 50% increase in the number of UAVs (Unmanned Aerial Vehicles) that can be supported in the same satellite network.		
Description:	Sending high-quality secure video streams, clips and photos from unmanned mobile platforms, at sea or in the air, beyond the range of local radio links, require use of communication networks that cover air and sea, in addition to land. In addition, there may be additional data sources on board these platforms such as AIS (Automatic Identification System) receiver, Emergency Position Indicating Radio Beacon (EPIRB), and maritime radar. Providing high-availability, high-capacity networks in such remote regions is costly. Thus, there is a market need for protocols that can jointly use multiple low-availability, low-cost networks for increased resilience. Security is also important and splitting the information across multiple networks may increase security resilience to interception, and resilience to jamming. Satellite communication complements terrestrial networks, such as 3G, 4G and 5G. However, in a mobile context, coverage changes, and choosing how to use, select and combine, multiple heterogenous networks can quickly become a complex challenge. In a dynamic and changing mobile situations, like drones flying beyond line of sight, predicting capacity of individual network branches based on history does not guarantee stability in the future. There are already multipath transport protocols, access traffic switching/steering/splitting protocols, and protocols integrating network coding with Torrent protocol that can jointly use multiple networks. The proposed activity shall design and demonstrate such protocols for secure and resilient multimedia communications from unmanned mobile platforms with multiple data sources with varying levels of QoS in latency, availability, security, etc. The key engineering challenges are design of algorithms that dynamically select networks, schedule packets, optimise protocol configurations as a function of current network conditions and required latency/availability/security QoS levels for each application. Such algorithms shall be implemented to achieve high throughput in real time with possibly constrained computational resources on board the aforementioned mobile platforms. The work shall demonstrate solutions for video streaming via at least one satellite link and two separate cellular networks simultaneously using a mobile platform, and demonstrate that stable, adaptive HD and possibly 4K video streaming in near-real-time is possible using the selected technology. It shall demonstrate that when capacity is sufficiently high, both live video and transmission of other sources of data such as earlier requested video clips, high-definition photo content, maritime radar data etc. is possible. It shall demonstrate resilience to cellular networks that have low availability.		
Deliverables:	Summary report, simulation software, demonstration testbed.		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	N/A		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3A.173	Resilient distributed network management for secure satellite constellations	500	B
Objective:	The objective of this activity is to investigate different network management architectures and design options to propose alternatives to a centralised network management in a context of a secure satellite constellation.		
Targeted Improvements:	Enable distributed network management techniques for future secure satellite constellations, not existing today		
Description:	Current Satellite Constellation systems rely on a centralised network control centre defining the use of resources in terms of frequency channels, service coverage per satellite as well as routing through the Inter Satellite Links (ISLs) to users and gateways. This approach is dependable on the availability of the control segment. This approach is not optimal for secure networks, where the network needs to be resilient to unavailability of the control centre caused by faulty states or malicious attacks. The aim of this activity is to identify strategies for a distributed network management for NGSO and multi-orbits (GSO and NGSO) satcom systems for secure communications not relying on a central control centre. While the need for distributed control has not been highly considered so far, the increasing concerns on resilience of secure telecommunication services makes this topic truly relevant nowadays. Despite its novelty in the world of satcoms, the problem to be solved shows some analogy to the terrestrial ad-hoc networks, and therefore this project will consider what has been done in this field. The activity will develop techniques for distributed network management of satellite constellations and illustrate their figure of merits using a software demonstrator. The main engineering tasks of the activity will be to develop distributed network management strategies for such systems, with a focus on a route meshed traffic through the satellite network including ISLs. Trade-offs shall be performed to identify at which layer the routing shall be performed and identify the most promising approach among connection or connectionless. Radio Resource Management for the user links will be implemented in a distributed way so that the satellite network can identify its frequency plan and instantaneous service coverage avoiding intra system interference. The system will need to manage service requests from users in a distributed way based on signalling on the control plane avoiding users being left unserved or avoiding multiple satellites registering the same user.		
Deliverables:	Summary report and simulation software		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	Yes		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3A.180	Secure and application-selective multicasting in multi-layer satellite constellation networks	500	B
Objective:	The objectives of the activity are the design, development and demonstration of secure multicasting, routing and secure group management protocols in satellite constellation networks involving thousands of NonGEO and GEO satellites.		
Targeted Improvements:	Increased user traffic plane efficiency (30%) and allow for a more secure user traffic plane		
Description:	Synchronisation of Content Delivery Network (CDN) edges, data centres, blockchain ledgers are examples of some use cases for multicasting in satellite networks. Multicasting via GEO satellite systems may also be invaluable for efficient batch configuration and software update of NonGEO satellites in the network. Multi-layer satellite constellation networks with GEO and NonGEO satellites allow to selectively use GEO satellites for unicast/multicast connectivity within the network. The large coverage provided by GEO satellites in addition allows to decongestion inter-satellite link network among NonGEO satellites. However, in order to leverage multi-orbit satellite systems in these scenarios, application-selective unicast/multicast routing protocols, traffic engineering algorithms, and secure multicast group management protocols must be developed and demonstrated in such networks. Traffic engineering and route selection are particularly hard in the presence of end-to-end aggregate flows where application types and QoS of individual streams are obfuscated due to end-to-end encryption. The proposed activity shall investigate solutions in collaboration with relevant cybersecurity partners. There is already a rich literature proposing solutions for these problems for terrestrial networks. Adaptations and optimisations of these solutions are still missing for multi-layer satellite constellation networks where thousands of satellites are involved. Such large constellations pose specific challenges for protocol scalability and efficiency. The key engineering challenges are the design of application-selective unicast/multicast routing protocols with intelligent traffic engineering functions at edge and intermediate nodes, and the design of multicast group and key management protocols. The work shall design solutions for these problems, evaluate their performances in software simulators, and validate them in demonstration testbeds that are representative of the HW platforms available on board the satellites.		
Deliverables:	Summary report, simulation software, demonstration testbed.		
Estimated current TRL:	3		
Target TRL:	5		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

1.2. Security and Cryptography

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.013	Multi-purpose Quantum Key Distribution receiver for optical ground stations	950	B
Objective:	The objective of the activity is the development and testing of a multi-purpose ground Quantum Key Distribution (QKD) Optical Receiver including a compact decoding set-up for secure key material generation. Key output is the standardization of interfaces a) from the telescope of the optical ground station and b) to the customer key management system.		
Targeted Improvements:	The main target improvement of this activity is the optimisation of the interoperability of quantum key distribution systems.		
Description:	The activity will include the following tasks: selection and justification of the most suitable technology and design to comply with the SAGA and EuroQCI system, performance, and programmatic requirements; address the advantages and technological challenges of selected QKD protocols with respect to detectors; designing and building the QKD multi-purpose Optical receiver prototype based on an outcome of the trade-offs; testing and validation of the prototype; test and demonstration of the QKD Optical receiver secure rate material generation using a QKD transmitter system; analysing the data and assessing the impact on the secure rate generation for a space to ground QKD link; assessment of space qualification possibility of the developed receiver including a preliminary assessment for the key age and security impacts.		
Deliverables:	Summary report, Interface Control Documents, prototype of QKD optical receiver, monitoring and control SW modules		
Estimated current TRL:	3		
Target TRL:	5		
Technology harmonised:	Yes - 2022 - Optical communications for space		
Dependency:	None		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	12 - Ground Station Systems and Networks		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.014	Anti-jamming techniques using artificial intelligence for frequency hopping waveforms	500	R
Objective:	The objective of the activity is to design, develop and test an advanced anti-jamming concept for frequency hopping waveforms, using sensing and Artificial Intelligence (AI) to predict and mitigate more efficiently the effects of narrowband jamming.		
Targeted Improvements:	Improve by a factor of at least 2 the anti-jamming performance (i.e., fraction of time in the channel without being jammed)		
Description:	Governmental communications require to be protected against jamming scenarios, such as low power narrowband jammers, which are typically addressed using frequency hopping secured waveforms. Those use a synchronisation mechanism and a hopping sequence, rendering unpredictable the frequency at which the signal is being emitted at a given time. Such hopping sequences are mostly based on pseudo-random sequences, which do not take into account the jammer behaviour. Recently, extensive literature can be found that aim to increase the resilience of frequency hopping by applying AI/ML techniques on jammer sensing and use it to tune the waveform parameters, with promising results. This activity will design and develop a new frequency hopping waveform concept, based on jamming sensing and artificial intelligence to improve the anti-jamming performance. Critical parts of the protocol such as secured synchronisation between emitter and receiver, behaviour of "smart" jammers, and performance of jamming sensing, shall be addressed. The waveform will be validated on a physical layer, real time test bed emulating the scenarios of governmental communications, and jammers relevant to the level of threat and protection identified for such communications.		
Deliverables:	Summary report, frequency hopping enhanced waveform system concept and real-time test bed		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	02 - Space System Software		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.015	Cyber resilience framework for space communication systems	400	B
Objective:	The objective of the activity is to develop a space centric framework for cyber information exchange, a threat and vulnerability assessment tool, and sets of reference security blueprints for future product implementations.		
Targeted Improvements:	The immense majority of attacks use known security breaches: this framework will help defuse at least 85% of common attacks.		
Description:	There is a growing need to increase the cyber resilience of space systems supporting critical missions in the areas of crisis management, surveillance, and key infrastructures. To ensure an efficient protection in terms of confidentiality, integrity, and availability, it is crucial for any cyber strategy to cover the security pillars of technology, people, processes, and environment all together. This will boost the cyber-readiness of the industry. With a scope limited to satellite communications, the activity objective is to gather the critical building blocks for a common understanding of cyber, to federate relevant stakeholders and to enable the development of preventative countermeasures at technological and administrative levels. The cyber resilience framework will cover the following three pillars: 1. Exchange - space cyber threat intelligence platform; 2. Analyse - space threat and vulnerability framework; 3. Implement - common security blueprints for space systems and their components. For the first pillar the activity will study how the European satcom stakeholders can be brought together in a common forum to exchange satcom cyber intelligence; increase their awareness; facilitate assessment; and enhance compliance with cybersecurity standards. Following the Space ISAC approach, the study shall survey the relevant stakeholders, identify the best governance model, define a list of resources and services to be offered in priority by the platform, and propose an implementation roadmap. The second pillar will develop a common knowledge base of cybersecurity risk management and of adversary tactics and techniques adapted to satcom ground and space segments. For that purpose, existing frameworks such as MITRE ATT&CK and NIST IR8270 will be used as a starting base. A self-assessment tool will be produced for the industry to evaluate their cyber security risks in an easy and comprehensive way. The third pillar will address the topic of cybersecurity certification for satcom systems and shall be inspired by ENISA's candidate EUCC scheme, based on the Common Criteria framework. Building on top of the 2nd pillar framework, it will identify relevant satcom components, such as user terminals and gateways, and develop preliminary sets of security requirements. The blueprints shall be developed for future use and tailoring in commercial/governmental satcom projects. This activity is fully in line with the safety and security pillar of ESA Agenda 2025. In order to promote the use of security standards across the space industry and help start-up and SMEs to offer trusted products and services, software shall be delivered under an ESA Software Public Licence (Type 2).		
Deliverables:	Summary report and roadmap, space attack framework and self-assessment tool, technical security blueprints		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	N/A		
Dependency:	None		
S/W Clause:	ESA Software Community Licence		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.016	Scalable Public Key Infrastructure concept for large constellation secure communications	500	B
Objective:	The objective of the activity is to study, design, develop and test a scalable and future proof Public Key Infrastructure (PKI) concept for a telecommunications system based on a large constellation including concept of interconnection with other space and terrestrial systems. The PKI shall allow the authentication of users (on ground and in space) by means of asymmetric cryptography (classical and post-quantum) as well as the definition of groups and hierarchy of users. A test bed shall be developed to fully evaluate the developed concept for a large constellation.		
Targeted Improvements:	Enabling independent authentication service as needed for secure communications based on large constellation not existing today		
Description:	In the traditional GEO communication satellites, the satellite is a relay between the user and the ground gateway. The security of communication between the user segment and the gateway can be managed by a pre-shared secret. With the increase of broadband users, the increase of on-board capabilities and the development of satellite-based services, a flexible way to manage the confidentiality and authentication between all actors is needed. Currently the connection in the World Wide Web is secured through a PKI. A similar solution, but with independent certification authorities, is needed for telecommunication systems with many actors, allowing the secure and authenticated exchanges with users and with other systems. In addition, the advent of Post Quantum Cryptography (PQC) requires a careful study in terms of protocols adaptations and certificates signing process, taking into account the constraints of space systems. The activity targets the design of an independent PKI suitable for large constellation systems, also allowing the secure interconnection with other space and ground services and systems and capable to support “hybrid certificates” using classical cryptography and PQC. In particular, the PKI shall have a flexible and independent way to manage the key distribution using asymmetric cryptography, manage different multicast groups in a hierarchical manner and have synergy with other satellite-based services. Moreover, the activity shall evaluate different alternatives to digitally sign the certificates (e.g., using different schemes for different scenarios), considering the challenges of SATCOM environment (e.g., latency, limited power) and the state of the art of PQC. Such PKI will be validated with the development of a software testbed. Such software testbed shall simulate a communication system including gateways, satellites, and users. It shall emulate the behaviour of the PKI, evaluating as a minimum key distribution latency, bandwidth overhead due to authentication and peak bandwidth during specific operations such as key revocation. Moreover, it shall implement a proof of concept of a user and a server that authenticate the communication based on the designed PKI. The activity will start with a critical review of the requirements, taking into account the connections with other space systems, the synergy with different services (e.g., navigation, timing, and situational awareness) and the management of different multicast groups in a hierarchical manner. Subsequently, there shall be an analysis and trade-off to design a secure, efficient, and flexible PKI. The trade-off shall include different aspects such as flexibility, expandability, independency, and optimisation with respect to space systems constraints. Moreover, it shall consider whether can be an advantage the use of satellites in different orbits as part of the key infrastructure for key distribution in case of disaster recovery, ensuring business continuity. A definition of Key Performance Indicators (KPI) to evaluate different solutions shall be provided. Finally, the activity will output a software testbed to validate the designed PKI and evaluate its performance based on the set of defined KPI.		
Deliverables:	Summary report and scalable public key infrastructure concept and software testbed		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.017	Lightweight post-quantum key exchange protocol for IP data transfers over satellite	600	B
Objective:	The objective of the activity is to implement and test a lightweight version of the Internet Key Exchange version 2 (IKEv2) key exchange mechanism that includes post-quantum cryptographic key exchanges. The activity will implement an open-sourced reference implementation of the protocol and perform assessment in a satcom simulator of the protocol on realistic use cases (processing power, data being transferred, latency, available bandwidth, etc.).		
Targeted Improvements:	Improved security with an actual protocol implementation of the newly standardised Post Quantum Cryptography (PQC) primitives. 50% reduction in the overhead of data transmission thanks to the use of direct IPSec tunnels (that use IKEv2 as their key exchange) instead of encapsulation of packets over satellite links.		
Description:	IKEv2 (Internet Key Exchange v2), used for the IP Security (IPSec) protocol, is one of the pillars of secure Internet. There is currently an effort from the ground telecommunication standardisation body IETF to integrate Post Quantum Cryptography (PQC) capabilities into new versions of the IKEv2 key exchange protocol. To allow for the use of IPSec tunnels over satellite links, but without the overhead of operating them within conventional satellite data link layers, satellites need to be able to negotiate keys in the IPSec protocol. Nevertheless, some trade-offs are unique to usage in the satellite telecommunication world. To ensure widespread adoption in the satellite telecommunication community, and that adaptations to the key exchange protocol necessary for usage in satellite links could be back-ported into the terrestrial protocol, the space industry needs to release a Request For Comments (RFC) document that will formalise the proposed protocol. This activity will identify the key factors that make a post-quantum IP communications over satellite "efficient" (for example reduced overhead, size, latency etc.), and adapt the state of play in PQC for ground telecommunications in order to release an RFC-like document specifying a space-specific PQC-ready IKEv2 key exchange protocol. Then a reference implementation of this proposed standard will be specified, implemented, and tested in a suitable satcom simulator. To encourage fast and widespread adoption of this technology among commercial satellite operators (to allow them to be ready for the mass adoption of PQC in the ground telecommunication world) and allow for the collective maintenance and security patching of a sensitive key exchange protocol, it is proposed to release the software developed in this activity under the ESA community Weak Copyleft (type 2) licence.		
Deliverables:	Summary report; Open-source implementation; Recommendations on an efficient use of the proposed protocol.		
Estimated current TRL:	3		
Target TRL:	5		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	ESA Software Community Licence		
Service Domain:	5		
Technology Domain:	01 - On-Board Data Systems		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.018	Security assessment, testing and validation capability for innovative secure communications and quantum technologies	1,500	B
Objective:	The objectives of the activity are to identify the needs and requirements for new security assessment capabilities for satcom systems and their components, define related architectural solutions and develop prototypes of the main components of these capabilities.		
Targeted Improvements:	Enabling testing, verification, and validation of advanced technologies in the domain of cybersecurity, modern telecom, and quantum security (Quantum Key Distribution, Quantum Random Number Generator, etc) for enhancing secure satellite telecommunications in ESA Member States.		
Description:	In an increasingly digital world, security concerns are becoming driving market needs. New approaches, like the use of COTS in space potentially bring vulnerabilities of the IT world into space. New technologies, e.g., 5G, interconnect further terrestrial networks with space, increasing even more the attack surface. As threats are continuously evolving, it is crucial that innovative security solutions and technologies for satcom are designed and developed. These solutions will for instance rely on post-quantum cryptography, quantum key distribution, quantum randomness, etc. A major step in the development of these solutions is to perform a comprehensive security assessment, testing and validation of the solutions and of their integration in satellite telecommunications components. Due to the specificities of the targeted products, protocols and services, the existing security assessment solutions are not enough to address these security assessment needs. These new needs can be achieved using virtualised representative, cost-effective security assessment laboratories that will emulate the targeted environment(s). Such environments can also be used to support the definition and validation of new security standards, as well as validating whether new solutions satisfy standard/certification requirements. Several initiatives in ESA MSs are also currently under preparation for the development and deployment of non-geostationary/multi orbit constellations satcom systems for providing secure and non-secure services. These systems of systems will rely on complex and innovative security architectures to be designed and validated. The objective of this activity is in a first step to identify and consolidate the needs in the Industry of ESA MSs for new operational security assessment, testing, verification, and validation capabilities arising from the development of innovative security solutions to be used in current and future satellite communications. Testing and validation capabilities will include new technologies like quantum ones (e.g., QKD). Validation shall be performed against relevant standards and certification frameworks. Such capability may also be envisaged to support the design, testing and validation of the complex security architectures and components of the upcoming satellite constellations systems. Opened to private actors as well as in support to on-going ESA projects, this capability could undertake assessment at any stage of development of the target solutions. Following a comprehensive system study including market opportunity and cost analysis, the second step of the activity will be dedicated to the prototyping of the pertinent capability elements, including those in support of future standardisation such as for QKD.		
Deliverables:	Summary report; prototype of security assessment, testing and validation capability components		
Estimated current TRL:	3		
Target TRL:	5		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
3D.019	Cyber-range testbed for satellite communications physical and data link layers	750	B
Objective:	The objective of the activity is to study, design and develop a cyber testing tool to support a comprehensive analysis of security and privacy risks of satellite communication systems. A testbed comprising computers, custom software in order to probe terminals for vulnerabilities, communication channel emulators, will be developed.		
Targeted Improvements:	Enabling data link and physical layer vulnerability testing and training in simulated satcom environments.		
Description:	In an increasingly digital world, security and privacy concerns are becoming driving market needs both for consumers and businesses. In order to achieve sustained competitive advantages for the coming decade, satellite communications need to adopt state-of-the-art security technologies and processes including security by design, trusted components, third-party validation and comprehensive testing and training. A method to achieve comprehensive testing and training consist of making use of virtualised but realistic environments known as cyber-ranges. This technology allows to experience real-world threats, assess security risks and validate security mitigation techniques in a safe and cost-effective laboratory environment. However, the scope of a cyber-range does usually not go below the network layer: it is indeed assumed that an attacker has some sort of an IP connectivity to the system under attack. This results in an artificially reduced attack surface in the simulation that is not realistic for a satellite communications scenario, especially since the availability of low cost - RF capabilities in the recent years. The objective of this activity is to close this gap by developing a cyber test tool compatible with commercial satellite communication systems, with a focus on the data link and physical layer emulation, and that can be integrated into an existing cyber-range environment. The tool's capabilities will cover the control, management, and data plane of forward and return links of common satcom waveforms and implement a modular architecture, including in the frame of this project DVB-S2 and RCS2. It is envisaged that the development would allow other waveforms to be incorporated in a later commercial phase. The environment will be able to assess not only threats against the satcom system owner, but also against the privacy of its users' data. The activity will end up with a demonstration of the tool in a cyber-range and showcase a predefined list of satcom threat scenarios.		
Deliverables:	Summary report; full hardware prototype that demonstrates the functionality in the relevant environment.		
Estimated current TRL:	3		
Target TRL:	6		
Technology harmonised:	TN/A		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	08 - System Design & Verification		

2. Space Segment – Platform

2.1. Command and Data Handling

Activity Ref.	Activity Title	Budget (kEuro)	Classification
4G.041	Ka-band radio frequency front-end resistant to intentional interference for secure TT&C	600	B
Objective:	The objective of the activity is to design, manufacture and test a Scaled Engineering Model of rugged Ka-band RF front-end for secure TT&C applications that will enable technologies for mitigation of intentional interference		
Targeted Improvements:	Ability to operate under severe Radio Frequency Interference		
Description:	TT&C is a key equipment for all satellites since it provides the umbilical cord to the control station(s). It has to operate in an RF environment that tends to become increasingly congested and interference prone, whether intentionally or non-intentionally. For secure communications such as government satellites, techniques like spread spectrum and CDMA (Code Division Multiplexing Access) etc., may help but on the condition that the RF receiver front-end still operates in a linear regime. Operation in linear regime means that signal is not distorted, and decoding is possible as it should meet minimum required Signal to Noise ratio. For secure communications, increasing linear power dynamic range by 20 dB will allow decoding of CDMA and spread spectrum signals. Therefore, by moving from GaAs (Gallium Arsenide) to GaN (Gallium Nitride) technology, such rugged Ka-band RF front ends are possible which can operate under intentional or unintentional radio frequency interference. Recent developments have proven that GaN technology can provide a much-improved linearity as well as higher power handling as compared to more traditional GaAs technology used in all current TT&C implementation. To realise Rugged Ka-band RF front end in GaN technology to enable secure communications due to their linearity and high-power handling capability is the primary aim of this activity.		
Deliverables:	Summary report and Scaled Engineering Model of rugged Ka-band RF front-end		
Estimated current TRL:	3		
Target TRL:	5		
Technology harmonised:	N/A		
Dependency:	None		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

3. Space Segment – Payload

3.1. System and Architecture

Activity Ref.	Activity Title	Budget (kEuro)	Classification
5A.082	Breadboarding of critical technologies for a multi-beam satellite receiver for aircraft MODE-S signals	900	R
Objective:	The objective of the activity is to design, develop and test payload technologies compliant with multi-beam receivers for satellite-based air traffic surveillance. Critical breadboarding will be carried out to demonstrate the concept suitable for use on small satellites in LEO or MEO.		
Targeted Improvements:	50% reduced payload power consumption, mass and volume compared to current technology. Increase the probability of message detection by a factor of 2		
Description:	The World Radiocommunication Conference (WRC) in 2015 made a primary allocation of frequency band 1087.7 to 1092.3 MHz for satellite reception of Secondary Surveillance Radar (SSR) messages transmitted by the aircraft. By detecting these MODE-S broadcast messages and recording their arrival time, on multiple spacecraft it is possible to accurately determine the position of the aircraft, without relying on the aircrafts knowledge of its location, thus creating an independent surveillance system. It has already been established that small satellites in LEO can detect these types of signals from aircraft. Because of practical geometric limitations to the problem, it is challenging to detect aircraft in highly congested airspaces, although it is critical to maintain the overall service quality. Thus, any receiver will need to be multi-beam to segment the coverage areas into smaller region. This activity aims to design and develop the critical technologies that are needed to implement a multi-beam MODE-S Receiver suitable for small platforms while meeting the technical requirements for the RF, baseband processing and time stamping. This activity will design, manufacture and test breadboard models of the key technologies for a multi-beam MODE-S broadcast messages receiver in frequency range 950 to 1100 MHz, including the accurate timestamping of the time of arrival of individual messages. The breadboard(s) will also be used to test and evaluate the performance in the presence of multiple messages with low Signal to Noise Ratio (SNR).		
Deliverables:	Summary report and breadboard model of critical transceiver subsystems for a MODE-S surveillance receiver		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

3.2. RF Repeater and Signal Processing

Activity Ref.	Activity Title	Budget (kEuro)	Classification
5C.481	Radio spectrum situational awareness functions embedded in telecommand/telemetry receivers	600	B
Objective:	The objective of the activity is to develop RF situational awareness functions for telemetry and telecommand receivers. Algorithms and a testbed shall be developed and experimentally tested in laboratory conditions based on several representative operational cases.		
Targeted Improvements:	Enabling interference and signal identification and classification using telecommand and telemetry signals.		
Description:	Information obtained from RF (Radio Frequency) data can be used to enhance the situational awareness of a Telecommunications satellite, offering information onboard that cannot be obtained via other sensors. Examples of such information include unintentional communication signals (from other spacecraft), intentional jamming signals, and unexpected interference from EM (Electromagnetic) sources within the satellite itself (e.g., harmonics or intermodulation products from other RF emitters of the same satellite, or leakage from internal sources such as cabling, connectors, switches). This activity plans to add RF situational awareness as an additional function in TT&C/TCR/PCC communications units. This can be achieved for instance by monitoring and processing an IF (Intermediate Frequency) signal within the bandwidth of the receiver chain of a transponder or transceiver based on software-defined radio (SDR) architectures. The IF raw samples at the ADC (Analogue-to-Digital Converter) can then be used to perform signal detection and classification (based on type of interference signal, type of modulation scheme, etc.) using an RF surveillance monitor that employs advanced signal processing that could be based on machine learning techniques. Machine learning techniques will be traded-off against classical techniques that use conventional algorithms for autonomous detection and classification of the main signal characteristics (modulation type, symbol rate, code rate), e.g., FFT-based parallel correlation, symbol signal-to-noise ratio estimation, parallel demodulation channels, etc.). Criteria for this trade-off will include the computational complexity, performance, cost, and suitability for this user case. A breadboard will implement the selected RF situational awareness concept, and, under a number of representative test cases, it will help evaluate the complexity and validate the performance of the RF surveillance monitor functions and algorithms. In addition, an (updated) transponder/transceiver architecture will be proposed that shows how this concept can be integrated in current transponder/transceiver designs (covering mechanical, electrical, front-end, digital and interface aspects). Finally, a Test Bed that allows to monitor, control, and test the RF situational awareness breadboard with a suite of representative test scenarios will also be implemented.		
Deliverables:	Summary report, technical data package, breadboard and testbed.		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	Yes - TT&C Transponders and Payload Data Transmission		
Dependency:	None		
S/W Clause:	Yes		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
5C.482	Highly integrated beamforming networks for governmental X-band applications	1,200	B
Objective:	The objective of the activity is to pack in a monolithic microwave integrated circuit (MMIC) the many separate ICs that are currently used in the hybrid approach to RX/TX beamforming in X band. The single chip solution will replace the hybrid approach, in a move similar to what happened in Ku/Ka and Q bands.		
Targeted Improvements:	Increased degree of integration thanks to implementation in Si/SiGe technology: 50% reduction of mass and size, volume production and functional modularity		
Description:	Active antenna payloads in the X-band government secure communications traditionally rely on hybrid integration of beamforming networks that involve multi-chip and printed circuit board implementation of individual RF functions. It is not unusual to see beamforming modules at X-band built out of hundreds of microwave integrated circuits each with a dedicated RF function in each of TX and RX direction and interconnected using bulky and costly technologies. This solution results in high payload volume and mass, which is not compatible with the objectives of the next generation satcom payloads. In the more commercially attractive Ku and Ka bands, this method has been replaced by a single-chip or a single package implementation, with one monolithic microwave integrated circuit (MMIC). This solution will allow a substantial increase in the maximum number of beams that can be generated by a single payload, however, there is no European solution on the market in the X-band. Development of highly integrated beamforming solution will be the objective of this activity. Although this domain has been for several decades traditionally represented by III-V technologies, it is expected that the SiGe BiCMOS or Silicon on Insulator technologies will offer the best performance trade-offs and commercial viability. Reference GEO and LEO active antenna payload shall be proposed, and various beamforming approaches shall be assessed, covering analogue, digital and hybrid beamforming architectures. The activity shall investigate different on-board transmit and receive array antenna concepts for the user uplink using a multi-node integrated BFN and shall also study different BFN architectures and integration technologies. As an outcome of the activity, a breadboard of the multi-node integrated beamforming network, including microwave signal conditioning functions, shall be produced and characterised covering both, transmit and receive X-band satcom. In this activity, a number of custom beamforming MMICs shall be designed, manufactured, and tested stand alone as well as a part of beamforming demonstrator modules.		
Deliverables:	Summary report and breadboards of each MMICs and demonstrator of overall beamforming network.		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	Yes		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

Activity Ref.	Activity Title	Budget (kEuro)	Classification
5C.483	Robust timing and synchronisation techniques for secure communications	800	B
Objective:	The objective of the activity is to design, manufacture and test a prototype of an on-board timing equipment for secure communications		
Targeted Improvements:	Enabling secure communications thanks to high accuracy and resilient timing synchronisation (sub microseconds)		
Description:	Governmental communications make use of secured waveforms, which implement modern techniques like frequency hopping or direct sequence spread spectrum and require a high level of performance for modem and network synchronisation. Current on-board synchronisation technologies based on quartz oscillators do not provide the required timing accuracy and robustness for such critical missions. The use of local oscillators disciplined to GNSS can achieve such performance requirements, but it can be subject to attacks such as GNSS jamming, deteriorating their performance. There is thus a need for more robust, high performance time synchronisation for secured communications. The introduction of solutions based on a combination of technologies (quartz oscillator, GNSS, chipscale atomic clock) with associated algorithms for control and integrity, offers the possibility to contemplate both high level of performance, with a high level of resilience. In this activity it is proposed to perform the design, development, and testing of a robust on-board timing solution. System aspects related to time synchronisation, in particular modem and network synchronisation, shall be considered as part of the design and a security risk analysis shall be performed to assess the necessary level of resilience needed for governmental communications (e.g., holdover period versus performance). A breadboard prototype, encompassing all critical components of the equipment, will then be tested and validated to demonstrate the required performance.		
Deliverables:	Summary report, breadboard prototype corresponding to TRL4		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		

4. User Terminals

4.1. Professional User Terminals

Activity Ref.	Activity Title	Budget (kEuro)	Classification
7A.073	Array Antenna with Directional Modulation for secure governmental satcom User terminal	750	B
Objective:	The objective of the activity is to develop a time modulated array antenna breadboard realising directional modulation to add an additional layer of security.		
Targeted Improvements:	Adding a physical layer of security to satcom user terminals. Improvement over standard array security by 3 orders of magnitude in terms of bit-error-rate (demonstrated on laboratory breadboards)		
Description:	With ever increasing demand for secure connections, this activity aims to add another layer of security (on top of/instead of encryption) on the air interface. When using traditional array antennas, the transmitted signal in desired and undesired direction are only different in power, which with sufficiently sensitive receivers makes it possible to eavesdrop. By utilising the right antenna topology, the signal can be distorted in antenna sidelobes; increasing the bit error rate in unwanted directions while keeping a clean link in the desired direction. This can also be realised while scanning the beam of the array, making this suitable for tracking satellites in all orbits. One way to achieve this is to use time modulated arrays (4D array), adding an extra degree of freedom that can be used to scramble the modulation off axis. With developments made for high-speed RF switches, a suitable bandwidth should be achievable to enable high speed satellite communication. The activity shall develop and breadboard (TRL4) a directional modulated array antenna suitable for a government satcom user terminal. The preliminary baseline working frequency should be in Ku-Band and above.		
Deliverables:	Summary report, array antenna prototype, hardware demonstrator (breadboard)		
Estimated current TRL:	3		
Target TRL:	4		
Technology harmonised:	No		
Dependency:	None		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	07 - Electromagnetic Technologies and Techniques		

4.2. User Terminal Mobile

Activity Ref.	Activity Title	Budget (kEuro)	Classification
7C.078	Time reference for portable terminals used in secure communications	700	B
Objective:	The objective of the activity is to design, develop and test a very low Size, Mass and Power (SWaP) device able to assure time and frequency stability from one to two order of magnitudes better than high performance devices (e.g., oven cooked crystal oscillators).		
Targeted Improvements:	Reduce the power consumption down to 100 mW for portable terminals		
Description:	Governmental communications feature the need to have high-performance synchronisation performance due to the use of complex waveforms, typically involving spread spectrum (direct sequence or frequency hopping). A highly accurate time reference becomes critical; to answer this need chip-Scale atomic clocks (CSAC) exist in the commercial market, in particular US products are available also for space applications. However, the available products in Europe are lacking behind in terms of power consumption, restricting some usages such as portable critical applications, in which external synchronisation may not be sufficient or not enough reliable. A power consumption reduction below 100 mW could enable these new usages and the feasibility of reaching such performance was demonstrated on paper through past ESA activities. The present activity will aim to perform the design, prototyping and testing of a time reference component able to address portable terminals secure communications. The activity shall address in particular the optimisation of the design, addressing thermal design, electronic and packaging so to define a design baseline and prove that performances are not compromised. A prototype, corresponding to TRL5, shall be developed.		
Deliverables:	Summary report and prototype corresponding to TRL 5		
Estimated current TRL:	4		
Target TRL:	5		
Technology harmonised:	Yes - Frequency and Time Generation and Distribution - Space & Ground		
Dependency:	None		
S/W Clause:	No		
Service Domain:	5		
Technology Domain:	06 - RF Systems, Payloads and Technologies		