Cybersecurity Test & Evaluation Facility for Belgian future space and air transportation systems

”CyTEF”

Alexander Borghgraef
Royal Military Academy

CyTEF Consortium Partners

Royal Military Academy:

The Royal Military Academy (RMA) is a military university teaching establishment, responsible for the academic, military and sports training of the future officers of the Belgian Defence and of friendly countries. It has a legal personality different from that of the Belgian State, which makes it possible to sign (research) contracts with institutional or private partners. All the research activities in the RMA that are not funded by the Belgian Defence are run by the RMA with its own legal personality, the so-called RMA Patrimony. Although the Patrimony has its own employees, all the members of the academic personnel of the RMA are entitled by law to work on the projects of the Patrimony. RMA will act as the prime contractor in the CyTEF Project.

VITROCISET
a LEONARDO company

m3 SYSTEMS
BELGIUM

UNIFLY®

RHEA
GROUP
ENGINEERING THE WORLD WITH YOU

AIRobot

CyTEF Consortium Partners

Vitrociset: Vitrociset Belgium is present in Belgium at ESA Redu since 1982 and with its 160 employees operates in Ground Data Systems, Space operations, Engineering Services and Ground Infrastructure Deployment and Maintenance. In the field of satellite navigation, VTCB is responsible for the operations and maintenance of the first level of the 16 Galileo Remote Sites under the GSOP contract, and main contributor to Galileo 2nd Generation System Engineering activities with ESA. The company is involved in cybersecurity for satellite communications and operations (ESEC Redu).

RHEA Group: Established as a space systems and solutions company in 1992, RHEA has a trajectory of over 25 years offering systems, solutions and services in the space sector. The RHEA Group operates in ten countries with more than 500 employee specialists from diverse fields of engineering; the Security Division developed the existing ESA Cyber Range in REDU and has direct experience in the delivery of cybersecurity analysis of cyber threat hunting services, security risk management processes, security best practices and security standards, as well as extensive experience in the fields of space systems and security of space systems.

CyTEF Consortium Partners

M3 Systems: M3 Systems Belgium is an SME created in 2004 and is part of the MISTRAL group with two other SMEs. It is specialized in radio-navigation for critical applications. As part of the critical applications of interest for M3 Systems Belgium, the impact of radio-navigation performances and vulnerabilities for UAVs operations. In this context, M3 System Belgium relies on the long endurance fixed-wing UAV platform manufactured by Boreal, also part of the MISTRAL group.

AIRobot: Airobot makes capturing, sharing and visualizing data easy for organizations that need a lot of data. We turn drones into flying robots to automatically collect information in a fast, safe and consistently accurate way. We have developed the AiroCore: a complete flight and payload management core which allows to remotely connect to the drone via a multitude of wireless technologies including 4G/LTE. The AiroCore is the heart of our Mapper, an all-weather, industrial flying robot built for high accurate data collection missions.

Unifly: Unifly is the global leading provider of Unmanned Traffic Management (UTM) software technology. We connect authorities with drone pilots so drones can integrate into the airspace safely. With our platform, authorities can see the drones, manage the airspace and approve the flights. Drone pilots can see if they are allowed to fly, plan their flights and request approval. We also made BLIP, our electronic license plate for drones.

CyTEF Goals

CyTEF's primary goal is to provide cybersecurity research, test and evaluation services which address the changing threat landscape to the Space and Air Transportation Systems in Belgium, and most particularly possible cyber-attacks on UAS command-and-control, payload data and navigation systems.

The Cybersecurity Test & Evaluation Facility (CyTEF) in Redu, integrated with a dedicated Belgian industrial foothold and the DronePort UAS aerodrome with segregated airspace available, can represent the Belgian solution to address the security threats and unlock the huge market of drone powered security solutions.

Cyber Security concerns of UAS

- Cyber-Security in any kind of drone powered application is a growing concern. There are a number of security challenges in the use of UAS; in case of BRLOS,most of them are related with jamming or spoofing of GNSS signals and Command and Control channels – C2.

- Attacks on UAS navigation systems can compromise the determination of the PNT of the drone and put the entire drone operation at risk. This may involve both causing a DoS on the drone GNC system or causing a (controlled) error in it.

- Cyber-attacks can involve the Communication channel – C3 as well and VLOS operation are relevant as well due to the potential Radio Frequency link loss caused by malicious intent.

- The risk implied by both C2/3 cyberattacks can involve: loss of the aircraft, loss of mission data or alteration / corruption of the information collected, or injuries to people, damage to third party property and infrastructure

CyTEF Objectives

- **Demonstrate an proof of concept for an end-to-end Cybersecurity Test & Evaluation Facililty (CyTEF) for UAS**
  - with access to a segregated airspace for UAS
  - allowing for scenarios from VLOS microdrone to BRLOS tactical UAS operations
  - conducting both simulated and real in-flight assessments
  - applying the ISO/IEC 15408 *“Common Criteria for Information Technology Security Evaluation”* (Common Criteria) methodology to assess the EAL (Evaluation Assurance Level) of the UAS

- **Develop national standards and procedures for UAS navigational and cyber-security.**

- **Allow for the testing of new technologies early in the development cycle.**
- **Leverage access to space facilities and a segregated airspace, as well as existing cybersecurity expertise and infrastructure (ESEC, DronePort, ARTEMIS,CSCE,Cyber Range)**

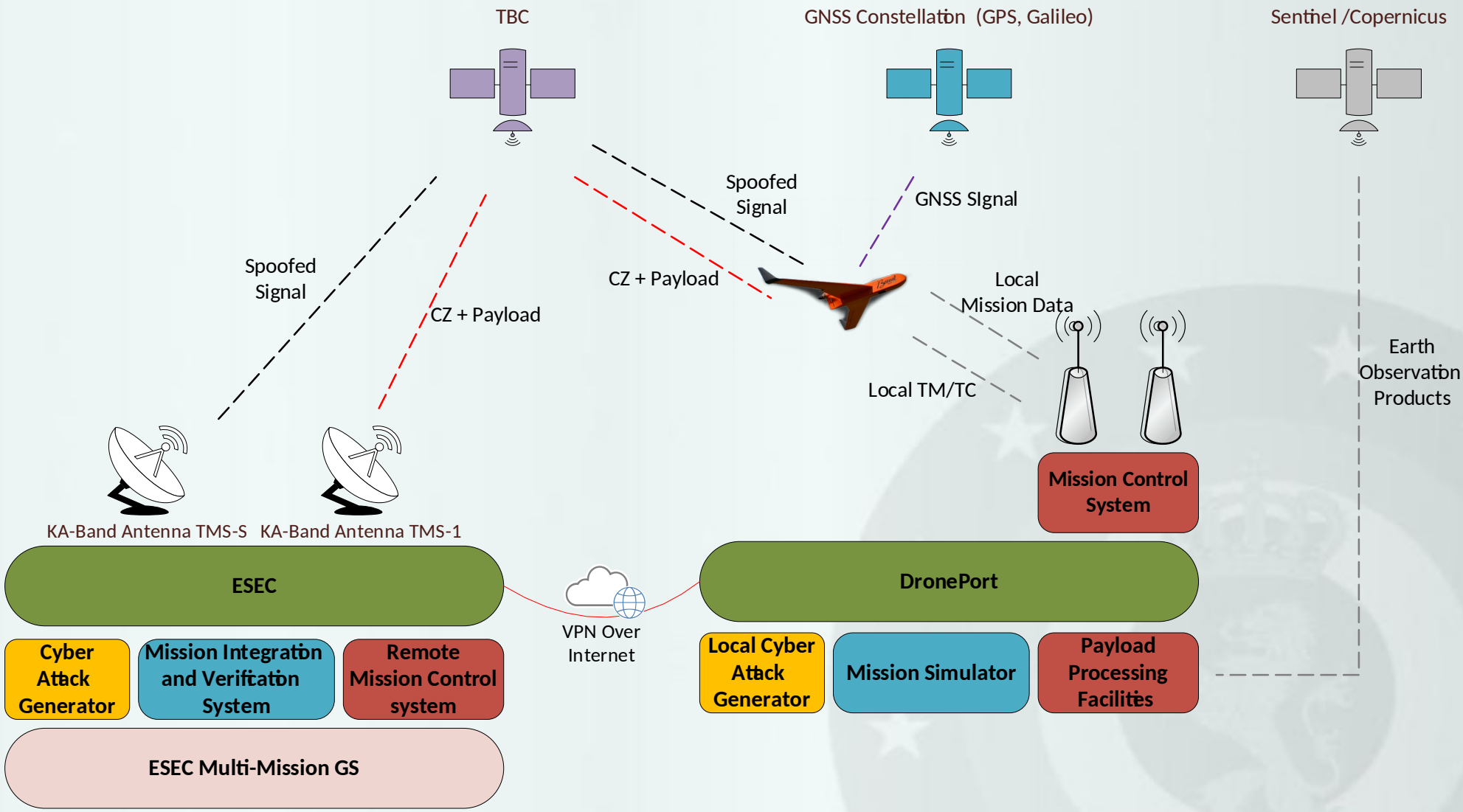
Preliminary market targets

- **Customers:**
  - UAS system and module manufacturers
  - UAS service providers
  - Payload manufacturers
  - Airport authorities and UTM manufacturers

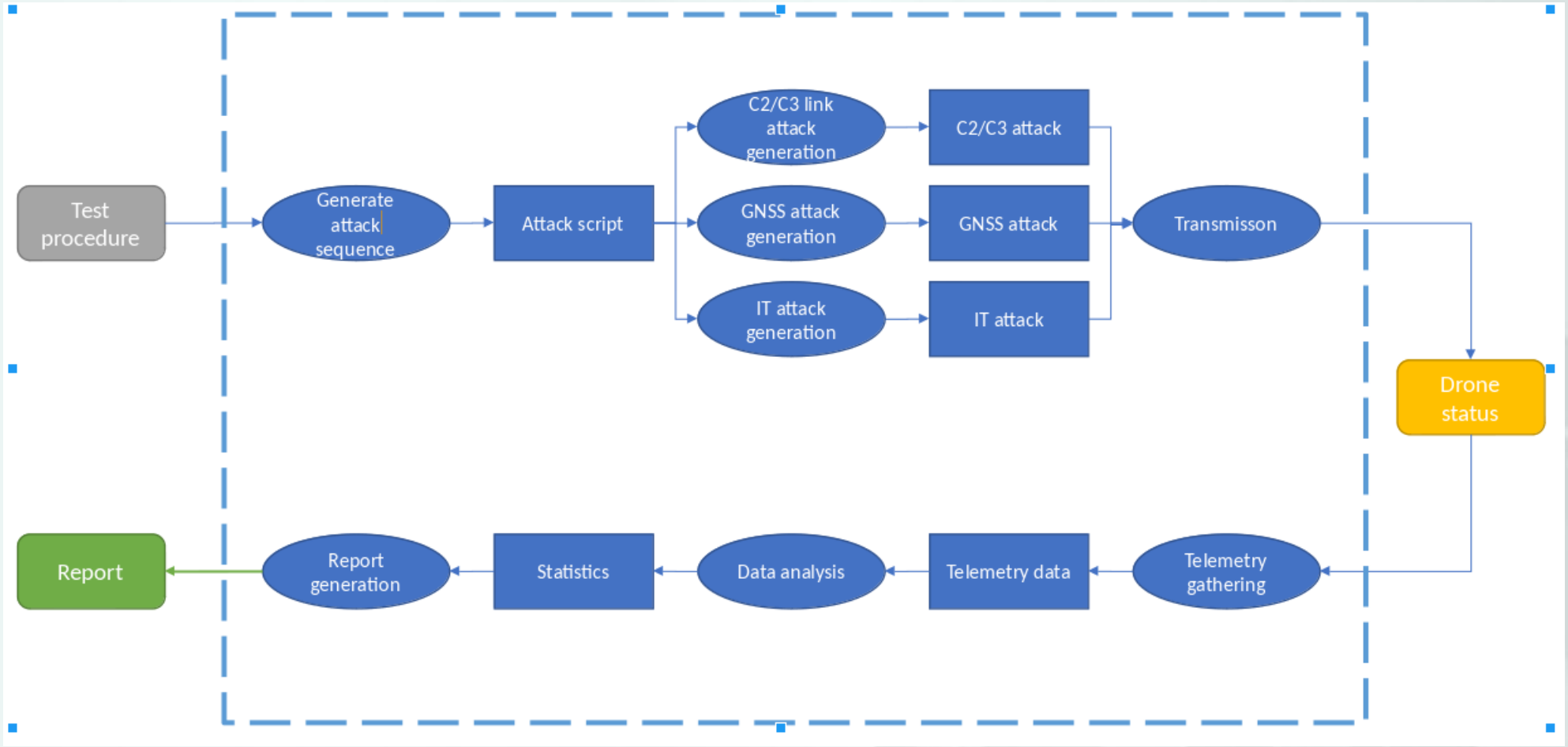
- **Users**:
  - Government entities (Skeyes/DGTA, Civil Protection, Defense, Homeland security, Law enforcement, Municipalities

- **Application**:
  The test range will validate resilience and robustness of UAS against cyber vulnerability in critical missions such as:
  - Disaster monitoring (forest fires, floods, earthquakes)
  - Asset monitoring (coastal patrol, pipleline, power line and solar panel inspections)

CyTEF System Concept



CyTEF Functional Architecture



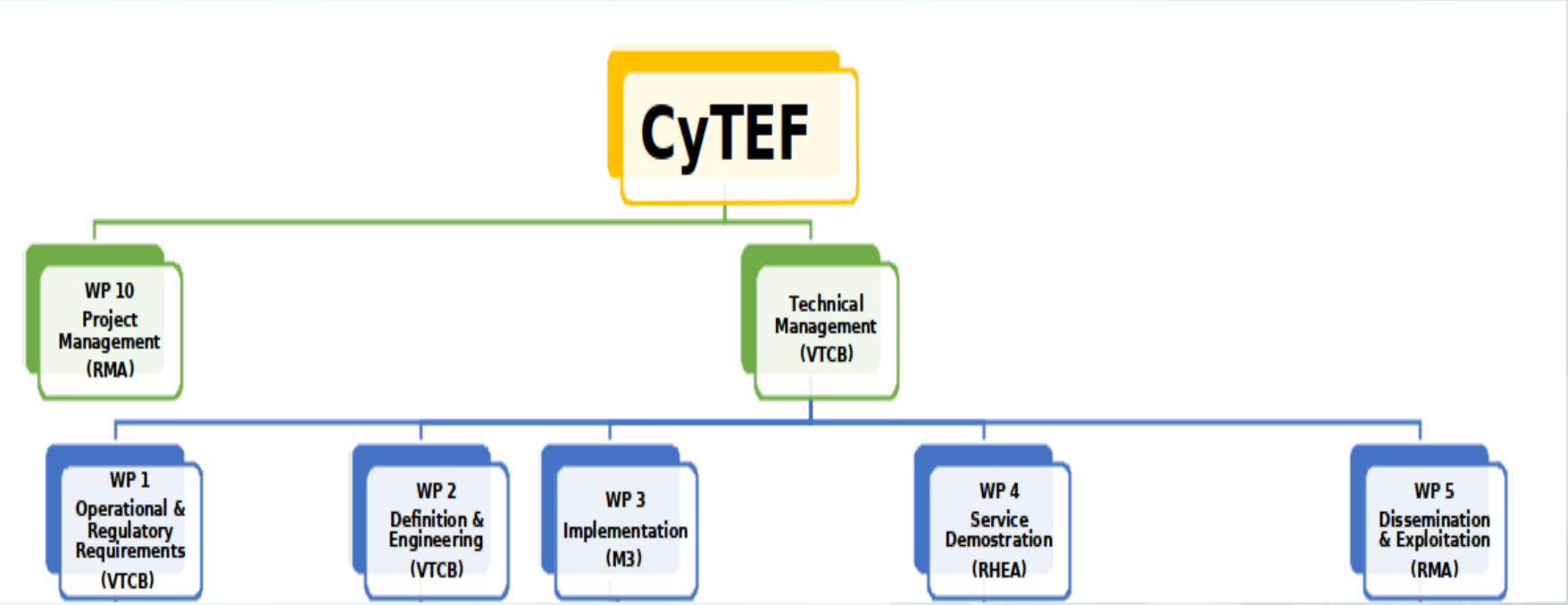
CyTEF Work Breakdown Structure

Project Status: Approved

Kickoff date: 31/01/2020

End date: 31/01/2022

Work organization:



CyTEF Trial: ESEC and DronePort

ESEC Redu

DronePort

DronePort cage

CyTEF Trial: UAS

AIRobot Mapper

DJI Phantom RTK

DJI M200

Boreal UAS

Thanks for your kind attention

Questions?