SAIl: 6

OCSL: 2

🡪 OCSO 🡪 medium

**OCSO #1 \_Software/Hardware**

1. Define processes/mechanics to identify and authenticate the person trying to access to the GCS and the autopilot.

***Operational***

*- To access to the GCS/autopilot, a person has to have an account (including Id + password)*

***Technical***

*- GCS computer shall verify the Id and the password of an account. There could be two levels of verification. At first level, the operation system (linux/windows) of GCS computer shall verify the account information. At the second level, the GCS software shall verify the account information by itself.*

*- The autopilot shall not have any physical interface that provides a direct access. The unique way to access to the autopilot is via the GCS.*

1. Define process/mechanics to create/modify/delete a person’s identification

***Operational***

*- The manager is in charge of managing (create/modify/delete) staff/pilot accounts.*

*- The manager has an admin account for GCS (Operation system and GCS software) to access to admin interface. Using this interface, the manager could create/modify/delete a staff/pilot account.*

*- The pilot accounts is valid during a period of time defined by the manager.*

***Technical***

*- The GCS software have an ‘manager interface that allow the manager to* *create/modify/delete staff/pilot accounts.*

**OCSO #2\_Software/Hardware**

1. Define rights of each person who could interact with the UAS.

***Operational***

*- The manager could modify/create/delete staff/pilot accounts.*

*- The primary pilot could*

*+ Send command to the vehicle from the GCS (taking off, landing, flying following a plan, fail-safe, and going to a defined point).*

*+ Create a flight plan on GCS and upload it to the autopilot.*

*+ Access to flight information (altitude, position, attitude, battery info, communication status).*

*+ Control manually the vehicle.*

*+ Access to video captured by the camera.*

*+ Access to logged files to perform post-flight analysis.*

*- The secondary*

*+ Access to flight information (altitude, position, attitude, battery info, communication status).*

*+ Access to video captured by the camera.*

*+ Control manually the camera.*

1. Define the process/mechanics to allocate/modify/revoke the rights of each person.

***Operational***

*- Depending on the role of each person, the manager gives her/him a pilot account or a support staff account.*

**OCSO #3\_Software/Hardware**

1. Define process/mechanics to limit the actions that a person could carry out to his rights.

***Technical:***

*-**The GCS software provides three different interfaces according to three types of user account*

*+ Manager interfaces*

*+ Primary pilot interfaces*

+ *Secondary pilot interfaces*

*- The manager and pilots will use these interfaces to interact with the UAS. To access these interfaces, the user has to have an account.*

**OCSO 4:**

1. Define security mechanics to protect the integrity of the flight plan, the flight parameters (PID parameters, filter Kalman parameters, sensors calibrations, etc.) and recorded data (video data, log data) stored in the GCS and the autopilot.

***Technical:***

- The GCS shall use an encrypted hash to protect the integrity of video data stored in its memory.

- The GCS and the autopilot shall use an encrypted hash to protect the integrity of logged data and flight plan stored in their memories.

- The autopilot does not have any modifiable flight parameters. The flight parameters is unchangeable. All flight parameters is embed into source code of the autopilot.

- The flight plan is protected by a encrypted hash

**OCSO 5:**

1. Define security mechanics to protect the confidentiality of the data/information stored in the GCS and the autopilot.

***Technical:***

- The GCS shall store the video data in the form of encrypted data.

- The GCS and the autopilot shall store logged data and the flight plan in the form of encrypted data.

**OCSO #6\_Software/Hardware**

1. Analyze the abnormal behavior on software/hardware after the flight to detect abnormal behavior in the post-flight inspection.

***Operational:***

*- The pilot and support staff will analyze the log-files stored in GCS and autopilot after each flight.*

***Technical***

*- During the flight, the GCS and the autopilot shall record the flight data (altitude, position, attitude, battery info, communication status) into log-files.*

*- During the flight, the GCS and the autopilot shall record the pilot commands into log-files .*

*- During the flight, the GCS and the autopilot shall record the change of autopilot’s state (arm, disarm, takeoff, landing, fly at automatic mode) into log-files.*

**OCSO #7\_Software/Hardware**

1. Partition the software/hardware architecture into different “zones” with different levels of criticality. Some hardware/software could be vulnerable to cyberattack than the others, but they provide functionality less critical than the others.

***Technical***

*- On the ground, the GCS includes two separate PCs with two separate GCS software. One is used to control and command the flight. Another one is used to control and command the thermal camera.*

*- On the vehicle, the autopilot is designed for flight control. The camera control is performed by another computer.*

**OCSO #8\_ Communication**

1. Define mechanics to ensure the confidentiality of each data packet transmitted via **communication equipment.**

***Technical:***

*- The communication modules shall encrypt/decrypt the data before the data transmission / after data receipt (AES algorithm shall be used).*

1. Define mechanics to ensure the confidentiality of each message transmitted between the GCS software and the autopilot software. **(application level).**

**-** *The GCS software and the autopilot shall encrypt/decrypt their messages before the message transmission / after the message receipt (AES algorithm shall be used).*

**OCSO #9\_ Communication**

1. Define mechanics to ensure the integrity of each data packet/message transmitted via **communication equipment.**

***Technical:***

***-*** *The communication module implement a secured protocol which protects the integrity of transmitted data by using the encrypted hash.*

1. *Define mechanics to ensure the integrity of each message transmitted between the GCS software and the autopilot software. (communication between applications)*

*- The GCS software and the autopilot software implement the Mavlink v2 protocol. This protocol provides a mechanics to protect the integrity of transmitted message.*

**OCSO #10\_ Communication**

1. Define parameters used to measuring the performance of communication channels.

***Technical:***

*- The performance of communication channels is evaluated by the following parameters:*

*+ Percentage of package lost - measured by the GCS and the autopilot*

*+ Strength of signal –measure by the communication modules*

*+ Delay time – measured by the GCS and the autopilot*

1. The GCS display the defined parameters

***Technical:***

*- The GCS shall display the communication performance parameter to the pilot.*

1. Establish a security instruction which the pilot could use to detect a drop of performance of communication channels by observing the status of communication channels.

***Operational:***

*- The pilot observe the communication performance parameters and detect the abnormal based on the threshold defined by the drone constructor*

**OCSO #11\_ Communication**

1. Define Define the mechanics to re-establish the communication or maintain several essential services in case of a drop in communication performance.

***Technical:***

- *In case of performance drop, the GCS and the autopilot shall reduce the size of transmitted information and transmit in priority the critical information:*

*+ GCS sends to autopilot: pilot command data*

*+ autopilot sends to GCS: attitude, position data.*

*- Implement the redundancy of communication channel. In the case of performance drop, the critical shall be transmitted in an emergency channel (This channel is deactivated in normal situation and is only activated in the situation under attack. That is to prevent attackers discover this channel).*

**OCSO #12\_ Communication**

1. Define parameters used to diagnostic the quality of communication channel after each flights. These parameters will be recorded on both the autopilot and the GCS.

***Technical:***

*- These parameters are defined as in OCSO#10.*

1. *Establish a security instruction which the pilot or maintenance staff could use to detect abnormalities by inspecting the log.*

***Operational:***

*- The pilot and support staff analysis the communication performance after each flight*

***Technical:***

*- GCS and autopilot shall record the communication performance parameters during the flight into log files.*

**OCSO #13\_ Communication**

1. Partition the communication system into different channels according to the criticality levels and vulnerability levels of transmitted data.

***Technical:***

**-** The flight control/command data and the video data are transmitted within 2 separated channels. The communication channel for the control/command could have a low baud rate, use a strong encryption algorithm and has a low package lost rate. The communication for the video data could have a high baud rate, the package lost could be tolerant.

**OCSO #14\_ Sensor**

1. Define the characteristics of sensors (about output value, sampling frequency, noise) and their acceptable threshold. The excess of these thresholds is considered abnormal behavior.

***Technical:***

*- The thresholds are defined as follows*

*+ Acceleration < 3 m/s2*

*+ Angular speed < /s*

*+ Velocity\_GPS < 90 m/s*

*- In the case that these thresholds is exceeded, the autopilot shall sent an alarm to the GCS*

1. Define mechanics to detect abnormal behaviors of sensors based on the data from other sensors

***Technical:***

*- An embedded camera is used to provide an alternative position data source.*

*- The autopilot analyze the data from the embedded camera, the GPS and the IMU to detect the spoofing attack (especially the GPS spoofing)*

**OCSO #15\_Sensor**

1. Define the solution to protect all sensors against the interference from the environment (that could be or not artificial)

***Technical:***

*- The IMU is shelled to defense against the physical interference at resonant frequencies*

1. Define mechanics or architectures that provide redundancies of sensor data

**Technical:**

**-** *Triple**Redundancy of IMU*

**-** *Triple**Redundancy of GPS*

**-** *Embedded camera provides a redundant position data source*