SAIl → 6

OCSL →2

→ OCSO → medium

OCSO 1:

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

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

OCSO 2:

- Define rights of each person who could interact with the autopilot and GCS.

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

OCSO 3:

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

OCSO 4:

- Define security mechanics to protect of the modifiable parameter (e.g. flight plan, filter Kalman parameters, encrypted key) and recorded data (video data, log data) stored in the GCS and the autopilot.

OCSO 5:

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

OCSO #6_Software/Hardware

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

OCSO #7_Software/Hardware

- Partition the system into different software/hardware with different levels of criticality. Some hardware/software could be vulnerable to cyberattack than the others but they provide the functionality less critical than the others.

OCSO #8_ Communication

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

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

OCSO #9_ Communication

- Define mechanics ensure the integrity of each data packet/message transmitted via communication links.

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

OCSO #10_ Communication

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

- The GCS display the defined parameters

- 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.

At low level, the abnormalities refers to only the drop of **communication performance.**

OCSO #11_ Communication

- A plan or a procedure that permits the user, pilot, to re-establish the communication or maintain several essential service in case of recognizing a drop of communication performance.

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

OCSO #12_ Communication

- 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.

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

- All detected abnormalities need to be recorded and reported to manufacturer.

OCSO #13_ Communication

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

OCSO #14_ Sensor

- Define acceptable threshold for raw data from sensors: GPS, IMU, barometer, compass. The excess of this threshold is considered an abnormal behavior

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

OCSO #15_Sensor

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

- Define mechanics or architectures that provide redundancies of sensor data