## OCSOs related to attacks on Software/Hardware Architecture

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | **Level of integrity** | | |
| **Low** | **Medium** | **High** |
| **OCSO #1 \_Software/Hardware**  Identify and authenticate the entity(\*) trying to access to the GCS and autopilot  Keyword: **identification and authentication**  *Note: An entity could be a human, or a component (hardware/software)* | Optional | - 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 | - Same as Medium  Additionally:  - Define processes/mechanics to identify and authenticate **the component** trying to access the GCS and the autopilot. |
|  | **Example**  - Password is used to verifier user’s identity when someone tries to access to GCS/autopilot | **Example**  - The autopilot uses the Private key Infrastructure to verify the other component such as GPS, ABS-B. |
| **OCSO #2\_Software/Hardware**  Manage the entity’s authorization.  Keyword: **authorization management**  *Note 1: This objective focuses on the operational procedures to define/ allocate/ modify/ revoke the entity’s authorization.*  *Note 2: An entity could be a human, or a component (hardware/software)* | Optional | - Define the rights of each person in its organization, who could interact with the autopilot and GCS.  - Define the process/mechanics to allocate/modify/revoke the rights of each person.  - These activities should align to **OSO# 01,** which require to define the duties and responsibilities of the operator’s personnel | - Same as Medium  Additionally  - Define the process/mechanics to allocate/modify/revoke the rights of a component when it interacts with others. |
|  | **Example**  The authorization of each person is defined as follows:  - Manager  - Pilot could access to GCS to monitoring and control the vehicle.  - Maintenance staff could access to autopilot and download data after and before the flight.  In order to have the rights of maintenance staff, a person has to ask the manager for these rights. | **Example**  - The GCS PC has an identification and a key to connect to the autopilot. The identification and the key are installed on this PC by the manufacture. |
| **OCSO #3\_Software/Hardware**  For each entity (\*) accessing to GCS or autopilot, ensure that it could only carry out the authorized actions.  Keyword: **authorization control**  *Note: An entity could be a human, or a component (hardware/software)* | Optional | - Define process/mechanics to restrict the actions that a **person** could carry out to his allocated rights. | - Same as Medium  Additionally  - Define process/mechanics to restrict the actions that **other components** could carry out to their rights |
|  | Example  - Depending on the role of a user, the GCS could provide a specific Human-machine interface that let the user perform the authorized action | Example  - The connection *port* of the autopilot allows the GPS module to send position data to the autopilot only, but not to read the data from the autopilot |
| **OCSO #4\_Software/Hardware**  Detect the unauthorized entity (\*) from modifying the data/ information stored in the GCS and the autopilot.  Keyword: **Integrity**  *Note1: This objective refers to the case that the protection mechanics defined in OCSO #3 are bypassed*  *Note 2: An entity could be a human, or a component (hardware/software)* | Optional | - 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. | - Same as Medium  Additionally  - Define security mechanics to protect the integrity of source **code and hardware** of the autopilot and the GCS |
|  |  | **Example**  - The autopilot and the GCS generate an encrypted hash to protect the integrity of the flight plan. | **Example**  - A supplemental controller is used to control the integrity of the source code stored on the autopilot. |
| **OCSO #5\_Software/Hardware**  Prevent the unauthorized entity (\*) from accessing to the data/information stored in the GCS and the autopilot.  Keyword: **Confidentiality**  *Note 1: This objective refers to the case that the protection mechanics defined in OCSO #3 are bypassed*  *Note 2: An entity could be a human, or a component (hardware/software)* | Optional | - Define security mechanics to protect the confidentiality of the data/information stored in the GCS and the autopilot. | - Same as Medium |
|  | **Example**  - AES algorithm is used to protect the confidentiality of flight plan |  |
| **OCSO #6\_Software/Hardware**  Analyze the abnormal behavior on software/hardware after the flight (post-flight inspection)  Keyword: **abnormality detection** | Analyze the abnormal behavior on software/hardware after the flight to detect abnormal behavior in the post-flight inspection.  *Note: this activity should align to the OSO #6 of the SORA methodology, which requires to define a post-flight inspection procedure.* | - Same as Low | - Same as Low |
| Example  - After the flight, the pilot shall analyze the flight data and flight command recorded during the flight.  - Supporting the above activity, the autopilot and GCS shall record the data and event during the flight. |  |  |
| **OCSO #7\_Software/Hardware**  Partition the software/hardware architecture into different “zones” with different levels of criticality.  Keyword: **hardware/software partition** | Optional | - 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. | - Same as Medium |
| . | **Example**  - The GCS includes 2 PC with two different software. One PC is used to control and observe the aircraft. This PC is critical for the UAS. The other one is used to control the payload. This functionality is less critical. |  |

## OCSO related to attacks on Communication:

| **Description** | **Level of integrity** | | |
| --- | --- | --- | --- |
| **Low** | **Medium** | **High** |
| **OCSO #8\_ Communication**  Prevent a non-authorized entity (\*) from accessing to the data/information within the communication between the GCS and the aircraft  Keyword: **Confidentiality**  *Note: An entity could be a human, or a component (hardware/software)* | - Define mechanics to ensure the confidentiality of each data transmitted via **communication equipment.** | - Same as Low  - Define mechanics to ensure the confidentiality of each message transmitted between the GCS software and the autopilot software. (**applications level**) | - Same as Medium |
| **Example**  - In a simple case, the GCS and autopilot communicate together via a pair of radio modules. The confidentiality of data is protected based on the encryption algorithm and frequency hopping mechanics provided by this module. | **Example**  - The GCS software and the autopilot software have their mechanics to protect the confidentiality of the message transmitted between them. |  |
| **OCSO #9\_ Communication**  Prevent a non-authorized entity from modifying the data/information within the communication between the GCS and the aircraft  Keyword: **Integrity**  *Note: It’s to ensure that the data have not been modified in terms of content, time (prevent replay attack), and source.* | - Define mechanics to ensure the integrity of each data packet/message transmitted via **communication** **equipment**. | Same as Low  Additionally  - Define mechanics to ensure the integrity of each message transmitted between the GCS software and the autopilot software. (**communication between applications**) | - Same as Medium |
| **Example**  - In a simple case, the GCS and autopilot communicate together via a pair of radio modules. The integrity of data is protected based on the encryption algorithm provided by this module. | **Example**  - The GCS software and the autopilot software have their mechanics to protect the confidentiality of messages transmitted between them. |  |
| **OCSO #10\_ Communication**  **Detect abnormalities**  in the communication channels between the GCS and the aircraft during the operation  Keyword: **abnormality detection** | - Define parameters used to measure the performance of communication channels.  - The GCS displays the defined parameters  - Establish a security instruction that the pilot could use to detect a drop in communication channels' performance by observing communication channels' status.  At a low level, the abnormalities refer to only the drop in **communication performance.**  These activities should align to the OSO #6, which require the operator to identify the communication characteristics | - Same as Low | - Same as Low  Additionally  - Define mechanics to detect the abnormalities automatically in the communication channels  At this level, the abnormalities refer to the drop in communication performance and the content of the messages/packet transmitted via the communication channels. |
| **Example**  The parameters used to evaluate the communication quality are signal strength, drop-packet ratio, and bitrate. These parameters will be displayed to the pilot.  - An instruction which describes the popular attacks that could be detected by observing the parameters. |  | **Example**  **-** Using a firewall in case the communication of UAS is based on a complex network involving the other applications, operations, or systems |
| **OCSO #11\_ Communication**  Maintain a minimum communication performance  Keyword: **Availability** | - A plan or a procedure that permits the user, pilot, to re-establish the communication or maintain several essential services in case of recognizing a drop in communication performance. | - Same as Low  - Define the mechanics to re-establish the communication or maintain several essential services in case of a drop in communication performance. | - Same as Medium |
| **Example**  - In case of a drop in communication performance, the pilot should change the communication frequencies. | **Example**  - In case of a drop in communication performance, the communication module shall transmit the important information /message /packet (such position, attitude information, pilot command information) in priority. |  |
| **OCSO #12\_ Communication**  Analyze abnormalities in communication channels after the flights (post flight inspection)  Keyword: **abnormality detection** | - Define parameters used to diagnostic the performance of communication channel after each flight. These parameters will be recorded on both the autopilot and the GCS.  - Establish a security instruction that the pilot or maintenance staff could use to detect abnormalities by inspecting the log. | - Same as Low | - Same as Low |
|  | Example  - The autopilot and GCS record the parameters: Package lost percentage, the signal strength, delay time.  - The GCS provides an interface that allows the pilot/staff to analysis the recorded data. |  |  |
| **OCSO #13\_ Communication**  Partition the communication system into different channels.  Keyword: **Communication partition** | Optional | Partition the communication system into different channels according to the criticality levels and vulnerability levels of transmitted data. | Same as Medium |
|  | For example  - The communication system is partitioned into two channels. One is used to transmit flight data, which is critical. Another one is used to transmit the video data, which is less critical**.** |  |

## OCSO related to attacks on Sensors

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | **Level of integrity** | | |
|  | **Low** | **Medium** | **High** |
| **OCSO #14\_Sensor**  Detect abnormal behaviors of sensors due to attacks  Keyword: **abnormality detection** | - Define the characteristics of sensors (about output value, sampling frequency, noise) and their acceptable threshold. The excess of these thresholds is considered abnormal behavior. | - Same as Medium  Additionally  - Define mechanics to detect abnormal sensors data by analyzing the consistency and the coherence between the data from different sensors. | Same as Medium |
| **Example**  - An acceptable threshold for data from the accelerometer such as +- 3m/s2. The data out of this scope could be considered a possible attack. | **Example**  - Compare position data from GPS with data from IMU and a stereo-camera to detect GPS spoofing |  |
| **OCSO #15\_Sensors**  Ensure the availability of the sensor data under attack.  Keyword: **Availability** | - Define the solution to protect sensors against the interference from the environment (The attacker could manipulate the output of the accelerometer sensor by using the interference at its resonant frequency ) | - Same as Low  Additionally  - Define mechanics or architectures that provide redundancies of sensor data | Same as Medium |
|  | **Example**  - The accelerometer (IMU at large) is shelled within a metal box to defense against the interference at resonant frequencies | **Example**  **-** In the case that the GPS is unreliable, the data from the camera could provide position data alternatively |  |

.