In attack to MEMS, the attacker exploits

- the physical world to trick the sensor into detecting a phenomena that does not exist
- the digital world, by capturing the drone and modifying its firmware
- the physical world by tampering the hardware itself

Let us consider the CUSUM statistic update, and consider a value $z_i(k) = |y_{received} - y_{estimate}| - b_i$, where the received signal is the actually received signal, the estimate is the output of the model and the last term is a compensation parameter. The nonparametric CUSUM statistic at time k is given by $S_i(k) = (S_i(k-1)+z_i(k))^+$. Let us assume that $S_i(0) = 0$, that $b_i = 1$, and that the detection rule triggers an alarm when $S_i(k)$ is greater than 10.

Assuming that the process is such that the received signal is constant = 1, if an attacker starts an attack against sensor i such that the reported measurement is always twice the expected value, then

- after 5 steps, the anomaly detector triggers the alarm
- after 6 steps, the anomaly detector triggers the alarm
- the detector does not work as the compensation parameter is too high

In attacks to the sensors used in an ICS, the attacker needs to

- launch a DoS attack as the only means to be effective
- create attacks that lie within the operational range of sensors to be stealthy
- create attacks that lie outside the operational range of sensors to be stealthy

In an industrial plant, segmentation

- is only applied at the control network, as corporate network is already segmented
- refers to the process of grouping sensors according to their functionalities
- occurs at layer three thanks to a router device

A SAE Level-4 autonomous driving indicates

- full automation with the vehicle performing all driving tasks in all conditions
- conditional automation, where the vehicle can perform most of the driving task
- high automation where the vehicle performs all driving tasks under specific circumstances and in geofenced areas

A saturation attack to a LiDAR

- precision of the time measurements of the senors
- is a Denial of Service attack that leverages the limits in the linear region of sensors
- is a Denial of Service attack that leverages the limits in the operational range of sensors

Annulla la scelta

In a reduced headway attack

- the car ignores the predefined headway policy and closely follow the preceding vehicles
- the attacker injects a fake location in the communication and reduces the headway of a victim vehicle
- the attacker causes the following (victim) vehicle to increase its distance from the preceding vehicle

In CACC

- the vehicle uses a radar and a controller to automate acceleration tasks
- the vehicle uses information from the preceding vehicle in a feed-forward loop
- the sensed distance from the preceding car is reported to the controller, which acts on the speed to maintain a minimum safety distance

An ECU is

- an in-vehicle network bus-based standard
- an embedded systems that control one or more (sub)system(s) in a car
- a counter value that can be used to implement the bus-off attack

Clear my choice

In order for the bus-off attack to be effective, the attacker achieves precise synchronization by

- ○ detecting the ID of the packet of interest of the victim ECU
- ○ detecting in real-time the presence of the target packet
- ○ leveraging the periodicity of messages and priorities