CHALLENGE 1

1. Entity posing the challenge

HABIC: ALCAD, BURDINOLA, DAISALUX, OJMAR

2. Challenge

How can we improve the digital protection of smart devices in the space equipment industry, and the cybersecurity of their connections?

3. Possible solutions that can be applied

- Cybersecurity: securing assets and cyber-intelligence
- Software and hardware security engineering
- Managing security and threat intelligence

4. Context

An increasing number of buildings and facilities labelled as being “smart” are controlled by BMS (Building Management Systems), or smart building management systems. **The technologies deployed in these buildings** (as in other non-smart buildings) provide high-value features with multiple benefits and efficiencies for their users, but **may also have significant cyber-risks associated with them**. These technologies are mainly divided between hardware (sensors, consoles, etc.) and software (mainly computer programmes with protocols). In this sense, the companies proposing this challenge are mainly hardware manufacturers (although they also design software) and they have proprietary protocols for connecting their devices.

Given the above, there is a growing **need to implement these technologies safely and securely** (and in the case of the companies proposing the challenge: emergency lighting - Daisalux, laboratory fume cupboards - Burdinola, telecommunication platforms - Alcad, smart locks - Ojmar), in order to avoid the risks of physical and cyber liability that could be caused by digital attacks. They include technologies that may sometimes have connections to the internal networks (servers) of the infrastructures in which they are integrated, such as hospitals, laboratories and other critical facilities and, therefore, they may be a very attractive initial access target for cyber attackers.

As a result, the **space equipment sector and its companies** face very specific risks when it comes to integrating their systems/products into the buildings for which they are intended. In this respect, the main problem is: **the low security of communication protocols between the equipment (device and controller) and infrastructures (servers)**, which need to incorporate more and better security measures such as encryption or authentication. Other problems/challenges identified in integrating these systems and products into buildings in a secure manner include: **lack of end-to-end network and cyber security monitoring and visibility**,

multiple disparate internet connections installed throughout the building without centralised control, poor **patch management** practices, and **insecure remote access processes**.

5. Subsidiary challenges and objectives

In view of this reality, the design of communication protocols is crucial, as is taking the appropriate security measures in this regard and the gateways for connecting them. Similarly, going back one step further, it is important to ensure the cybersecurity of the firmware that controls the sensor hardware that operates the equipment in question. To this end, the different phases that affect them, such as user control, use of firewalls, remote access via VPN, etc., need to be inspected.

In addition to implementing security measures on protocols, it is also very important to take general protection measures for systems into account, such as: password policies, appropriate network segmentation, securing equipment, and controlling the information provided by the system. In this case, bearing in mind that the companies proposing the challenge have proprietary protocols built in-house, and that they face some of the different problems outlined above, they envisage two types of collaborative project with startups:

1. **Digital forensic analysis/cybersecurity audits of devices/protocols/connections** to produce a risk map and prioritise actions, by carrying out diagnoses of the current situation and designing the securitisation of network protocols (encryption) in the event of any potential leaks/breaches detected. That could also lead to a project for:
    - **Setting up a cybersecurity operations centre** for preventing incidents, real-time monitoring and responding to threats.
    - **Implementing IDS/IPS*** (Intruder Detection Systems) or other hardware devices or software applications that use known intrusion signatures to detect and analyse incoming and outgoing network traffic for abnormal activity.
    - Providing **end-to-end cybersecurity or mitigation solutions** to prevent distributed denial of service (DDoS) attacks, preventing loss of connectivity for legitimate users and preventing servers and connections (Fire, Gate and Cloud) from being taken out of service.
    - **Authentication of access and communications** between network elements in a centralised or distributed manner **using low-cost devices**.
2. Secondly, it would be related to providing secure remote monitoring and maintenance services for installations and operating sensors through secured remote connections. Seeking to ensure security over the connection (which is different depending on the client: mobile card, parallel wifi network, etc.), and making the hardware (IoT) cybersecure, minimising the existence of open ports for system leaks.

**The operation of these types of services on low-cost microcontrollers/processors on local and central devices and external communications gateways will also be assessed.*