Hackathon challenge:

Exceeding the speed limit on the roads while failing to keep a proper distance from other road users has been a major problem on Polish roads. Recently, the Polish Parliament has adopted a law that requires keeping a minimum distance between vehicles. Article 19 point 3a of the Polish Road Traffic Law- (*Prawo o ruchu drogowym)* states that the distance between cars expressed in meters shall be defined as not less than half of the number determining the speed of the vehicle the driver is driving, expressed in kilometers per hour, e.g., if the distance between two cars is 50 metres, that means that it is forbidden to exceed the speed of 100km/h The idea is fully justified and necessary, however at the moment, violation of this legal provision is difficult to detect.

In order to monitor the distance between cars, the police traffic officers consider using drones and GNSS navigation. Unfortunately, communication with the drone can be disrupted for a variety of reasons, such as spoofing (an attempt to fool a GNSS receiver by emitting a false GNSS signal from the Earth's surface) and jamming (intentional interference with the GNSS signal resulting in loss of accuracy and potentially loss of positioning capability). Both jamming and spoofing seem to pose a serious threat these days. In consequence, they can even affect traffic safety, as well as law enforcement.

The challenge is to develop a **concept of a spoofing and jamming resistant telemetry system used by drones**. The architecture of this system will guarantee the reliability of drones monitoring road traffic in Polish cities.

The key features of such a system will be as follows:

- Improving the effectiveness of spoofing detection;

- Meeting traffic safety standards;

- High system integrity and high security level;

- Real-time operation.

The concept of a telemetric system should include the following aspects:

- technical - the structure of the system should be defined by using the points described above and presented in a diagram. Groups should present a scheme and features of the system used by "road drones" with the highest possible degree of protection against spoofing and jamming phenomena. Participants should select technologies performing the tasks of the system from those already existing and justify the choice. The system should benefit from the technologies of navigation, telecommunications, and digital networks, sensorics and telemetry.

- usability - the presentation should demonstrate the economic benefits for the user (public administration). Groups should perform the analysis of time and financial commitment to the project as well as justify the cost of realization of their concepts.