Cyber-Physical Resilience for Unmanned Aerial Systems



Unmanned aerial systems (UAS) are increasingly used in applications such as inspection, logistics, and surveillance. As these systems become more connected and autonomous, they are also exposed to a variety of cyber and physical threats. Attacks such as sensor spoofing, communication interference, or malicious manipulation of control systems may affect the safe operation of drones and other autonomous platforms.

Existing research has investigated individual security mechanisms such as secure communication protocols, anomaly detection in telemetry data, or sensor integrity verification. However, cyber-physical resilience often depends on the interaction between multiple data sources, including on-board sensors, communication links, and environmental information. Understanding how these data sources can be used to detect disruptions or abnormal system behavior remains an open challenge.

The goal of this thesis is to investigate how different data sources can be used to evaluate and improve the cyber-physical resilience of UAS systems. The student will identify relevant operational scenarios and determine which types of data can support resilience monitoring. Experimental proof-of-concept implementations using machine learning techniques will be developed to demonstrate how these data sources can be used to detect anomalies or disruptions.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Farhad Aghili	farhad.aghili@sirris.be	office Sirris-Heverlee
	Laurens Le Jeune	laurens.lejeune@sirris.be	office Sirris-Heverlee
	Roozbeh Sarenche	roozbeh.sarenche@kuleuven.be	office B01.13
Nature of the work:	25% literature, 35% theoretical work, 40% software		
Number of students:	1		

 © 2026 – 2027 COSIC