A Cybersecurity Competence Network with leading research, technology, industrial and public competences

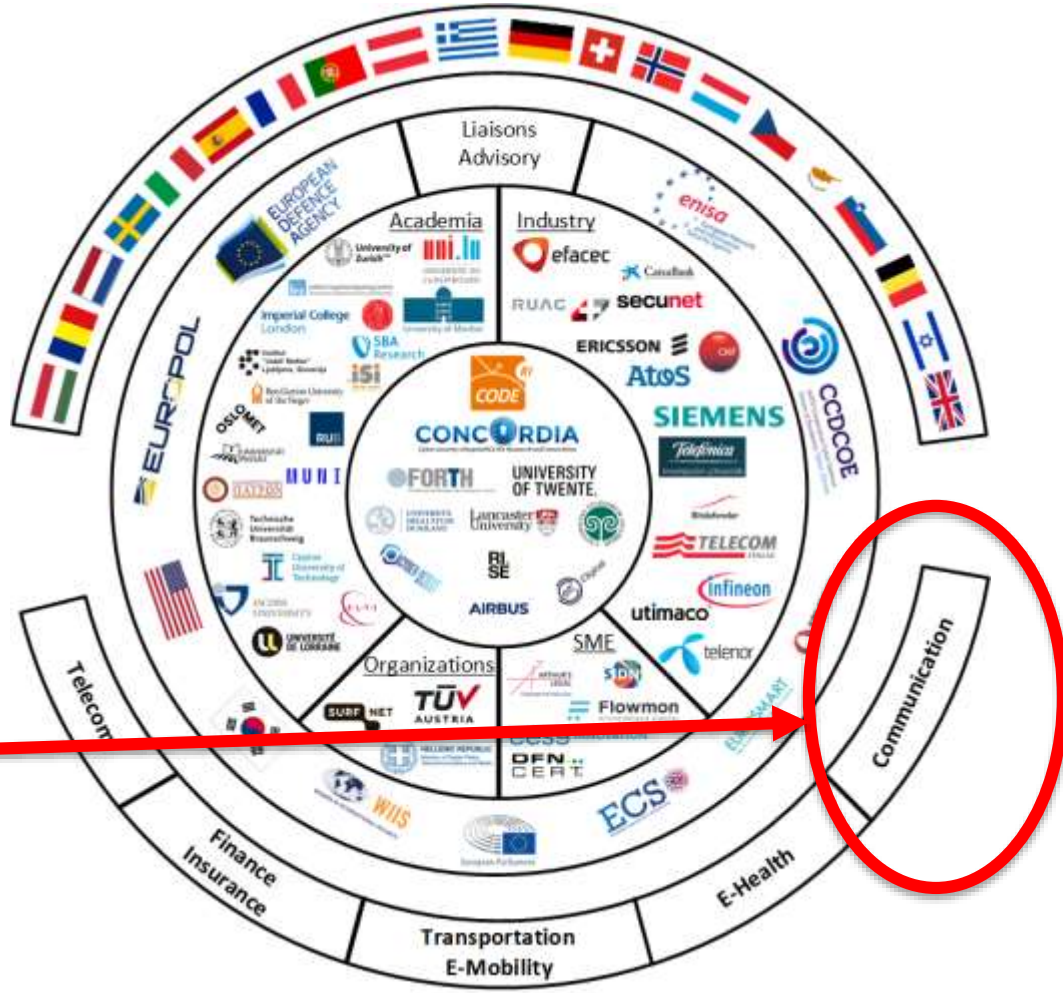
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Objectives

- Integration of fragmented European cybersecurity competences
- Building the European Secure, Resilient and Trusted Cybersecurity Ecosystem
- Bringing expertise to European policy makers and industry
- Providing CONCORDIA's cybersecurity roadmap for Europe
- Developing new, innovative market ready cybersecurity solutions
- Scaling up existing research and innovation with virtual labs and services
- Establishing an European Education Ecosystem for Cybersecurity

Current Consortium

- Current consortium with 53 official partners:
- Representing **16 EU member states** and **3 Horizon 2020 associated** countries + UK
- Project duration: 48 months (2019-2022)
- EC funding contribution: 15.998.737,50 €
- 5 industrial pilots:
  - Telecom
  - Finance/Insurance
  - Transportation/E-Mobility
  - E-health
  - Vehicular communication



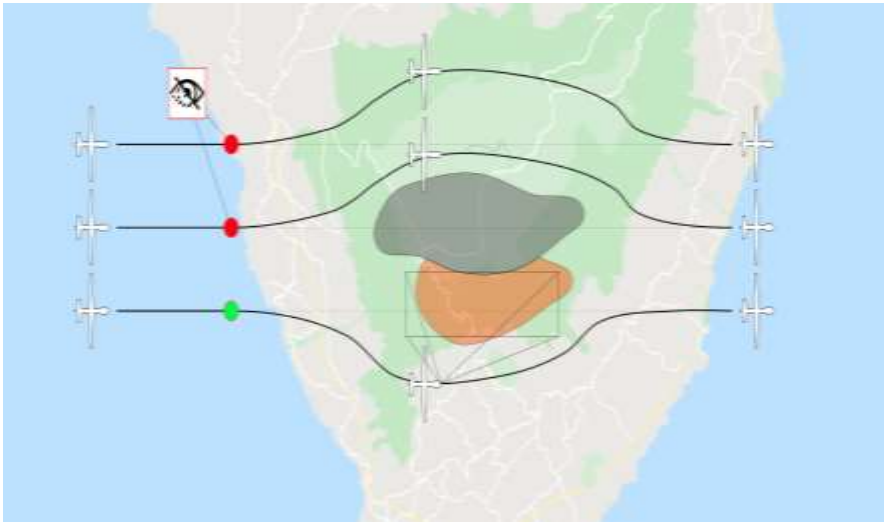
Operational Scenarios

Urban air mobility:

- Highly dynamic, heterogeneous environment
- Conflicting individual goals
- Vehicles not equally trustworthy
- Collaboration required with untrusted/ partially trusted vehicles for collision avoidance

Firefighting:

- Collaborative air/ground mission
- Participants unknown a priori
- Different capabilities of vehicles
- Plethora of attack paths due to common goal



Use Case 1: Secure Authentication

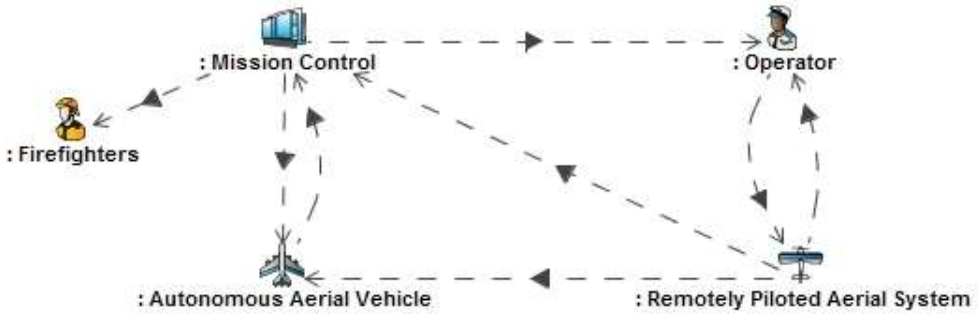
- Establishment of a secure link
- Essential for further interaction
- Implementation in HW
- Local authentication key storage
- System-on-chip with FPGA fabric

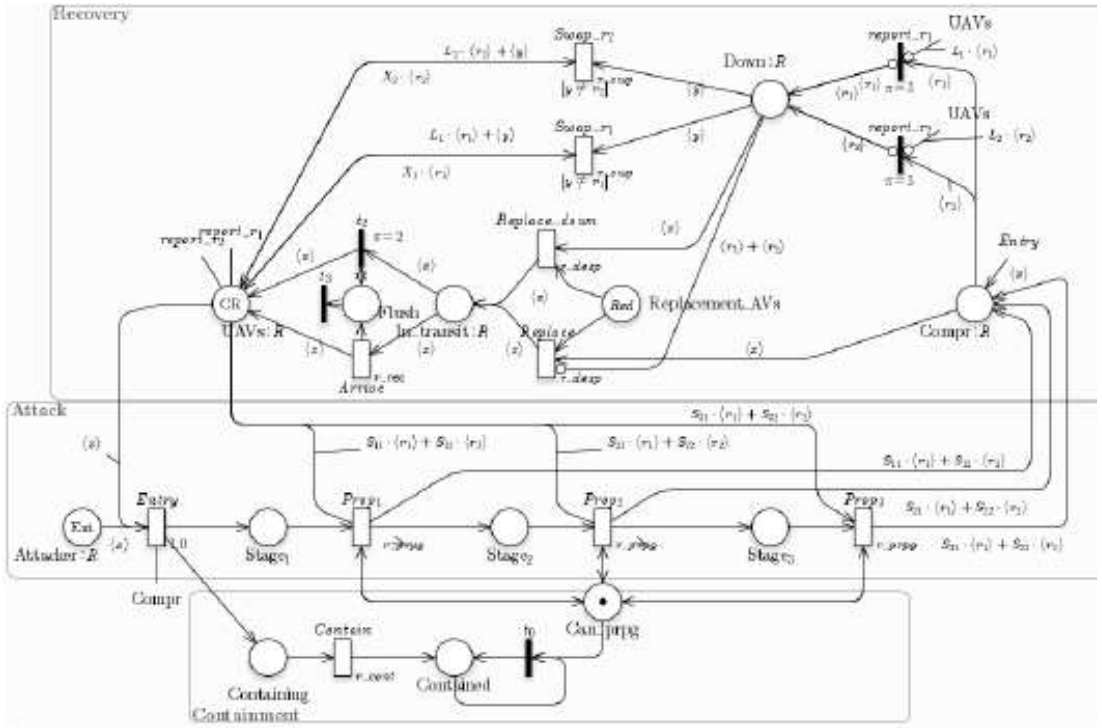
Use Case 2:Trustworthiness

- Performing joint mission together (e.g. formation flight)
- Prerequisite: authentication and established secure link
- Trust level determines level of interaction
- Based on the **urban air mobility scenario**
- Establishing, monitoring and adapting trust policies in reaction to past and present behaviour
- Integration of spatial policies and trust assessment

UC3: Ad-Hoc Networking and Resilience

- Based on firefighting scenario
- Evaluation of resilience of heterogeneous fleet of air and ground vehicles to attacks
- Network simulation, functionality, attack progression, impact on mission objectives, recovery strategies





Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020