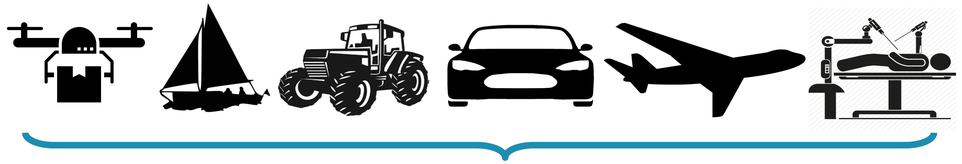
Wireless communication's robustness as one of the keys to bring safety to autonomous systems

Aleksandr Ovechkin, Tim Claeys, Dries Vanoost, Guy Vandenbosch, Davy Pissoort
ESAT-WaveCoRe , KU Leuven Bruges Campus

Plans for the deployment of Autonomous Systems (AS):



Ubiquitous implementation

Consequences of unsuccessful deployment:

All the problems endanger humans' life

Trust and safety problems

WP1

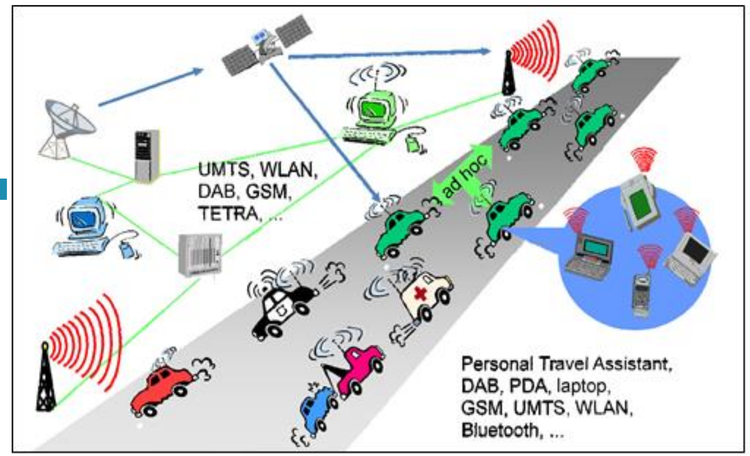
Early-stage researchers (ESRs):ESR1, ESR2, ESR3, ESR4

ESR5:

Electromagnetic disturbance (EMD)

Impaired communication

Safety-critical issue



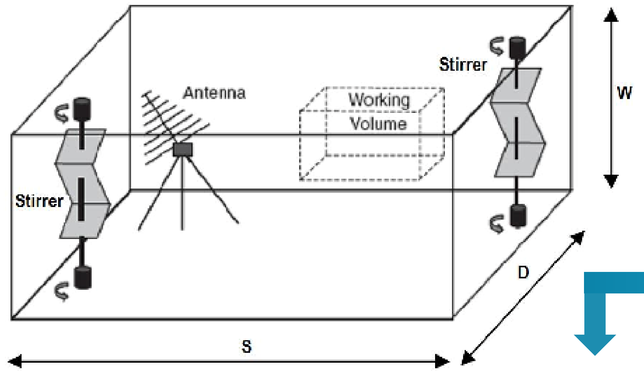
Objectives:

Increase the robustness of different wireless communication protocols for different types of EMD.

Expected results:

- Novel software and/or hardware-based techniques and measures
- Dependable wireless connectivity that is fault-tolerant or even fault-operational under diverse types of environmental stress

Reverberation chamber as a main tool to make wireless communication more resilient



Possibility to test many of the potential wireless protocols to be used in AS:

Allows to

Obtain main communication key performance indicators (KPIs):

- Packet Error Rate (PER)
- Communication latency
- Data throughput

Perform wireless co-existence tests

The SAS Project

Safer Autonomous Systems

Goal: make autonomous systems safer

Objectives:

Work Packages (WPs)

WP1

To integrate guaranteed safe behaviour directly into the architecture/design of the autonomous system

WP2

To prove by model-based safety-analysis techniques that the behaviour of an autonomous system remains safe under all possible conditions

WP3

To ensure that the safety-assurance strategies that combine the architectural/design measures with the evidence allow to have trust in the autonomous system, which is very likely to be learning and evolving

Acknowledgement

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.788.