Cranfield University
Centre for Autonomous and Cyber-Physical Systems
School of Aerospace, Transport and Manufacturing

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

## 19th Meeting of PNT Advisory Board

## June 28-29, 2017, Baltimore, MD

# “Cyber-Physical Security Aspects of Robust PNT”

SPACE-BASED POSITIONING NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

SPACE-BASED POSITIONING NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

SPACE-BASED POSITIONING NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

SPACE-BASED POSITIONING NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

SPACE-BASED POSITIONING NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

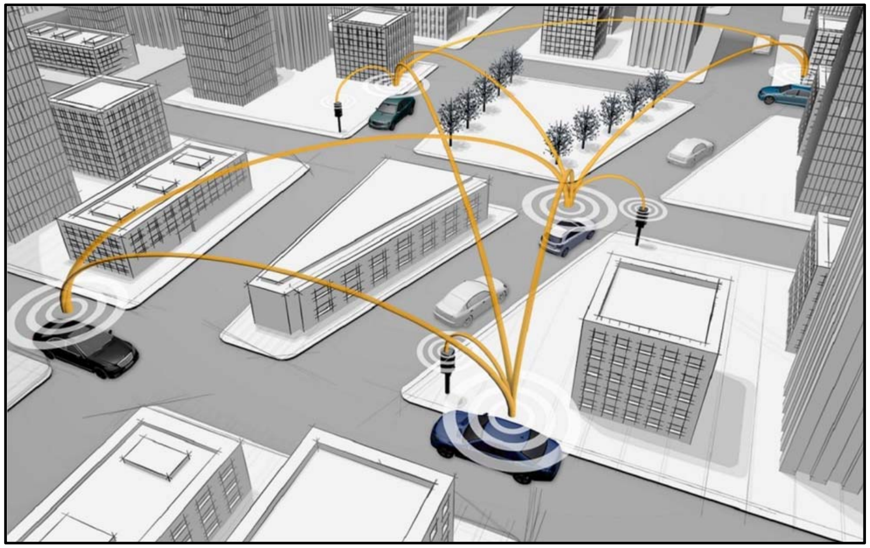
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

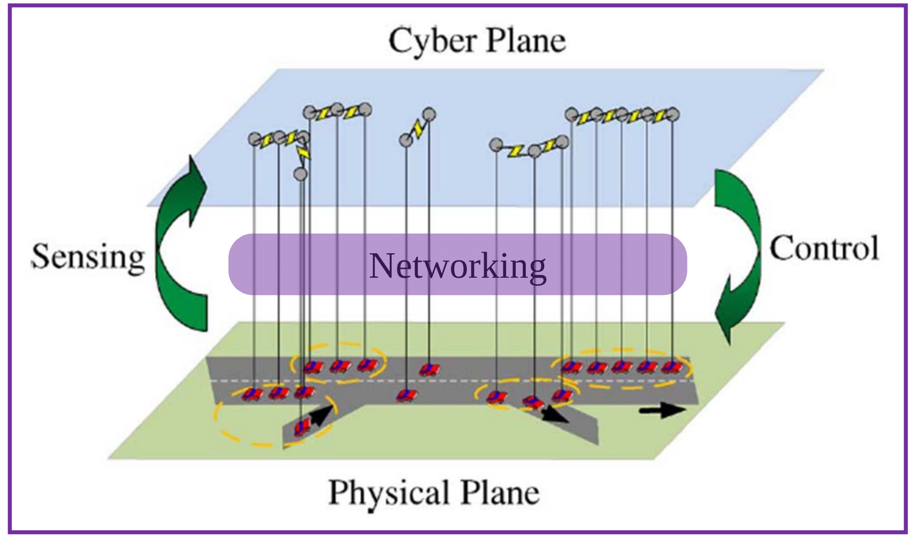
# Motivation and background:

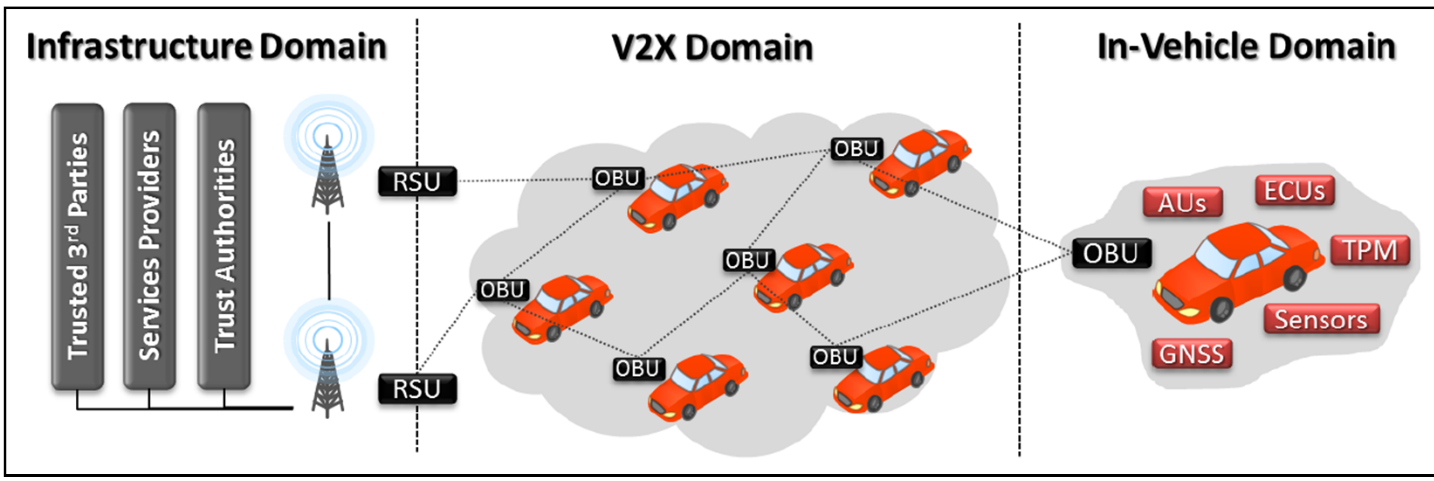
## *Connected drones and driverless cars*
## *or Cyber-Physical Systems*

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# CAVs: Connected – networking dynamics





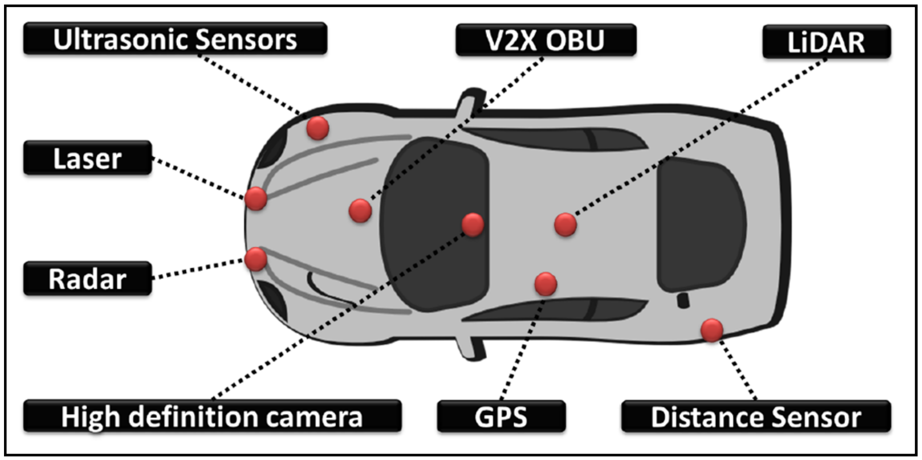



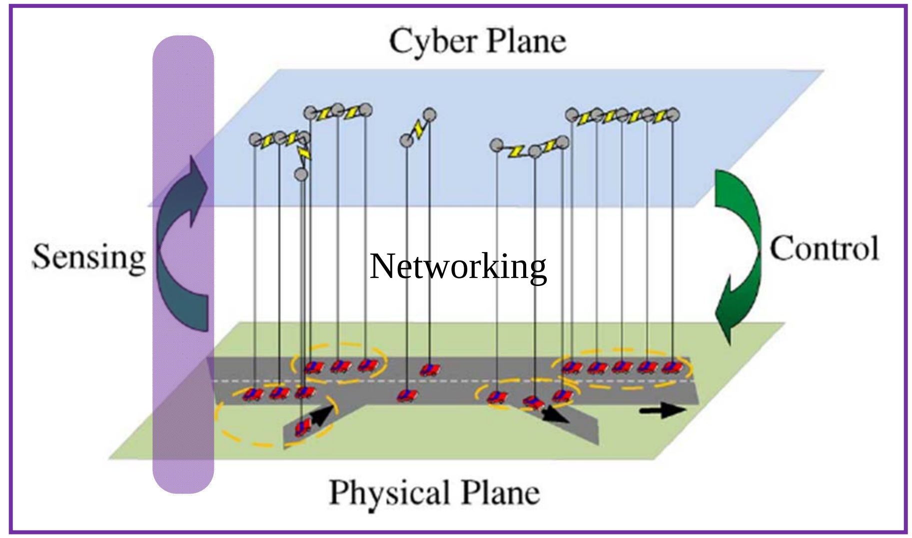

**Variable latencies**
radio channels
&
packet traffic

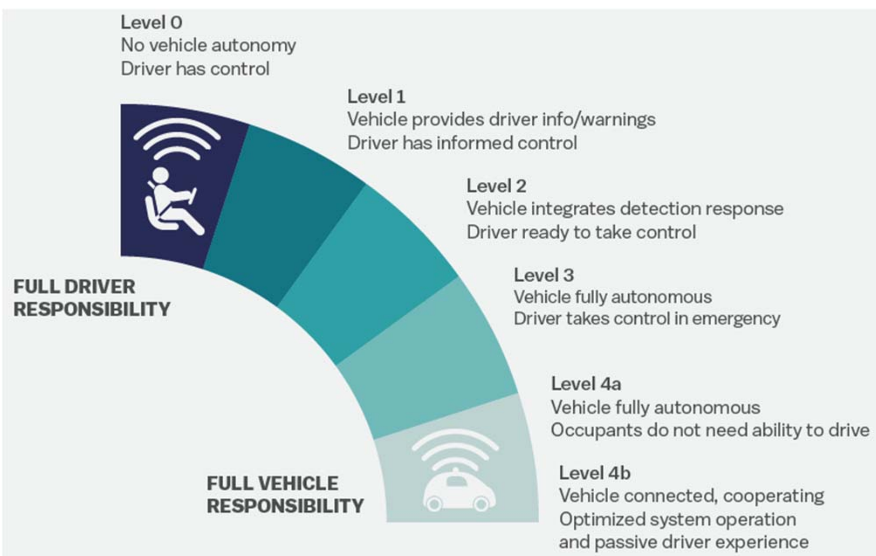
Centre for Autonomous and Cyber-Physical Systems
School of Aerospace, Transport and Manufacturing

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

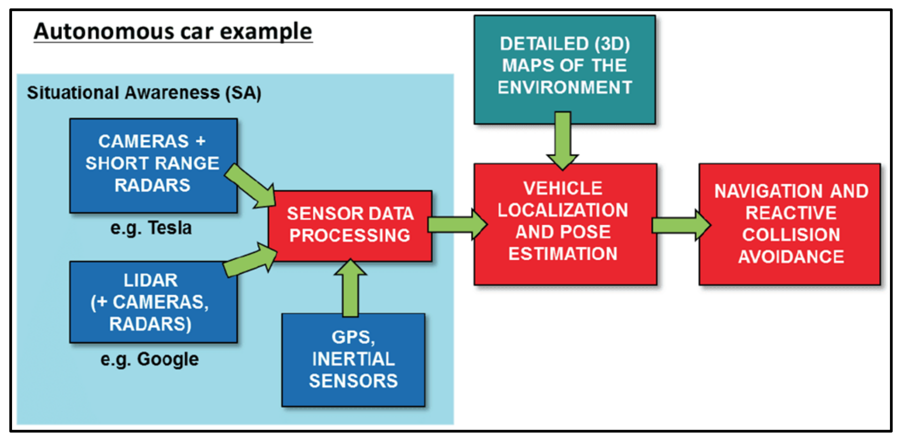
# CAVs: Autonomous – perception dynamics




**Variable latencies** sensing / processing dynamics

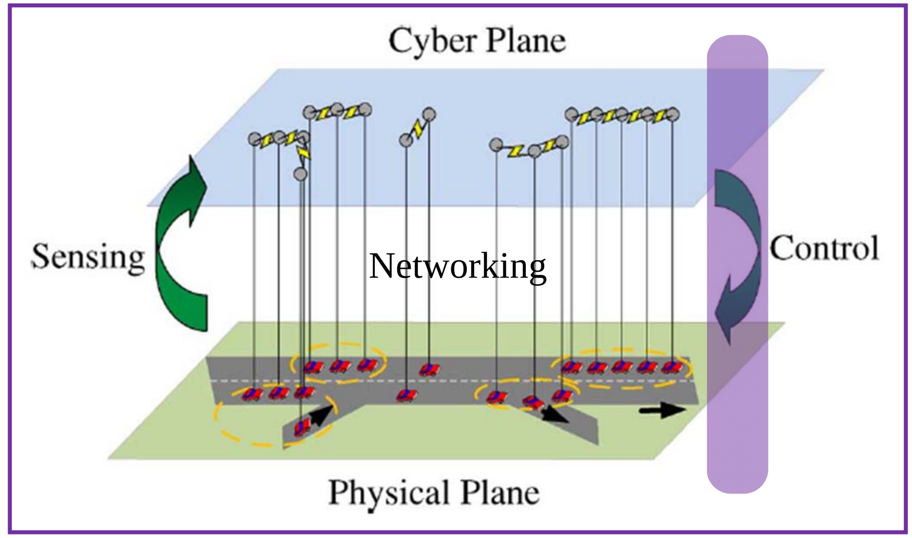


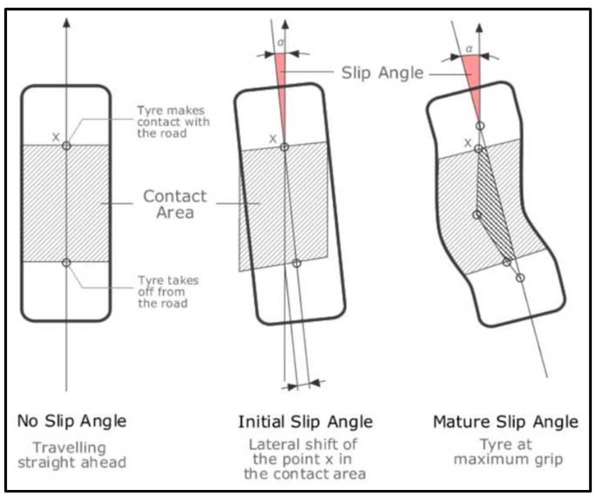
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

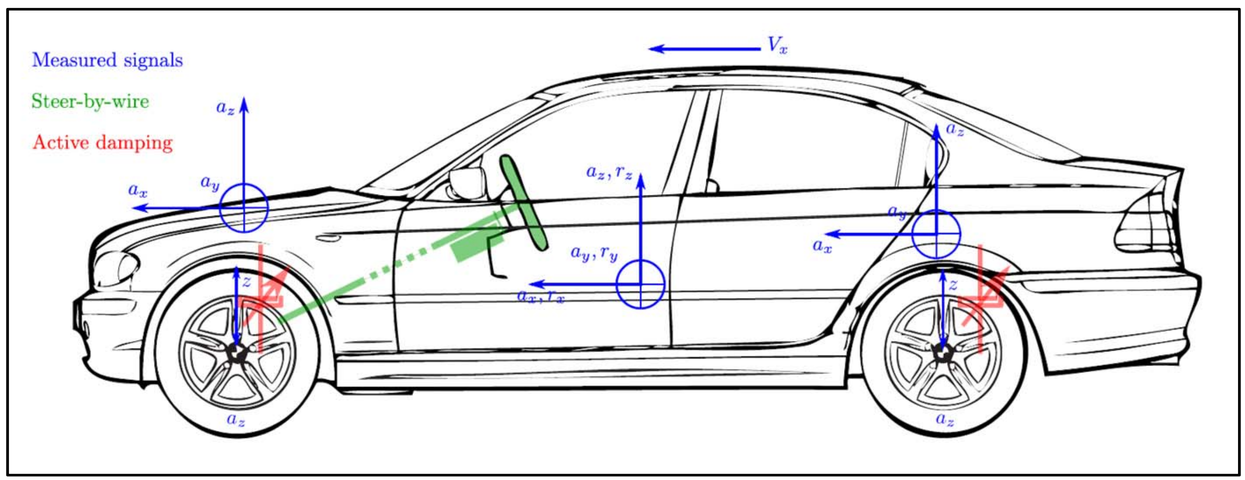
# CAVs: Physical – actuation dynamics

ABS (Anti-lock Braking System)
MSR (Mechanical Slip Regulation)
EDL (Electronic Differential Lock)
ASR (Anti Slip Regulation)
ESP (Electronic Stability Program)
TPM (Tyre Pressure Monitor)
→ CAN (Controller Area Network)

**Variable latencies** sensing / processing dynamics

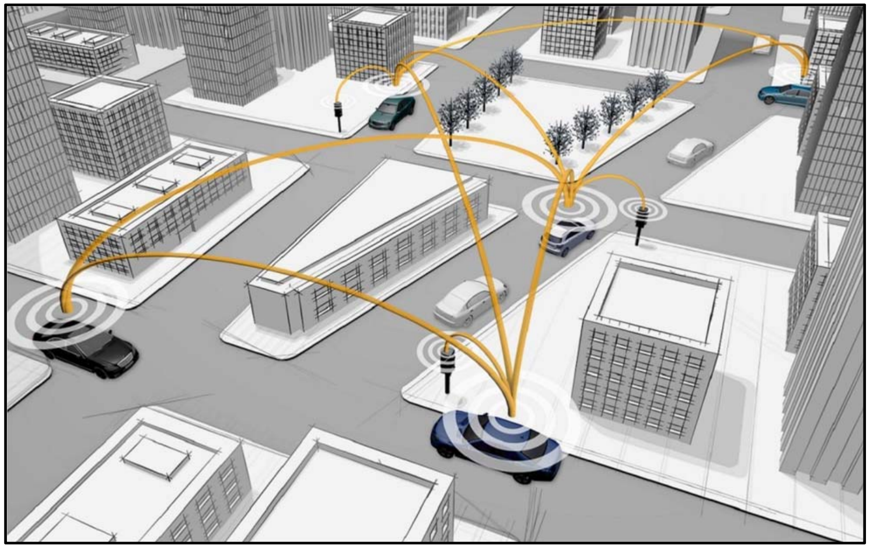


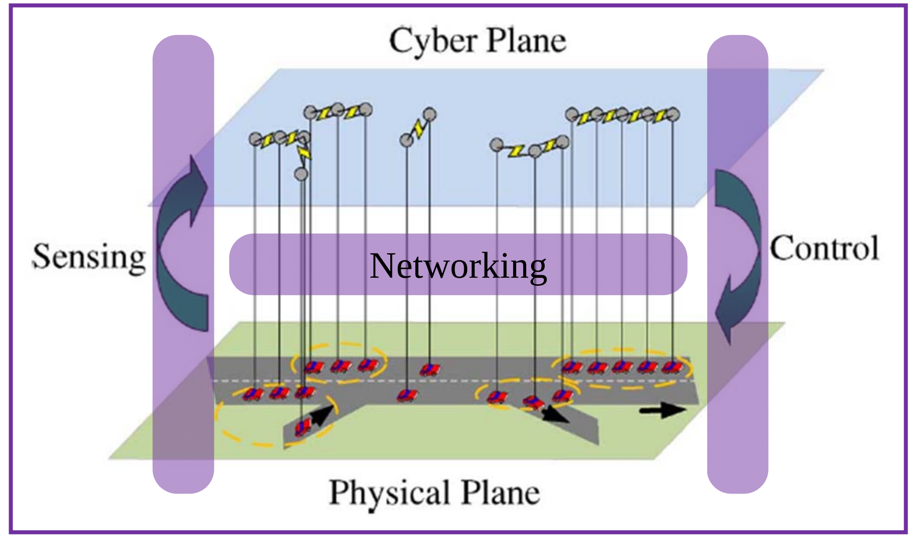



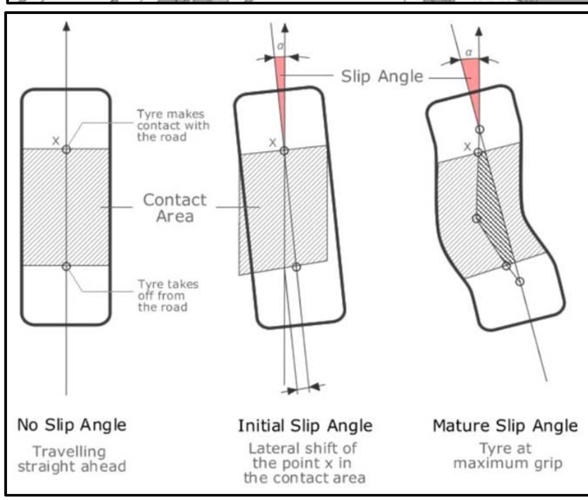



Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

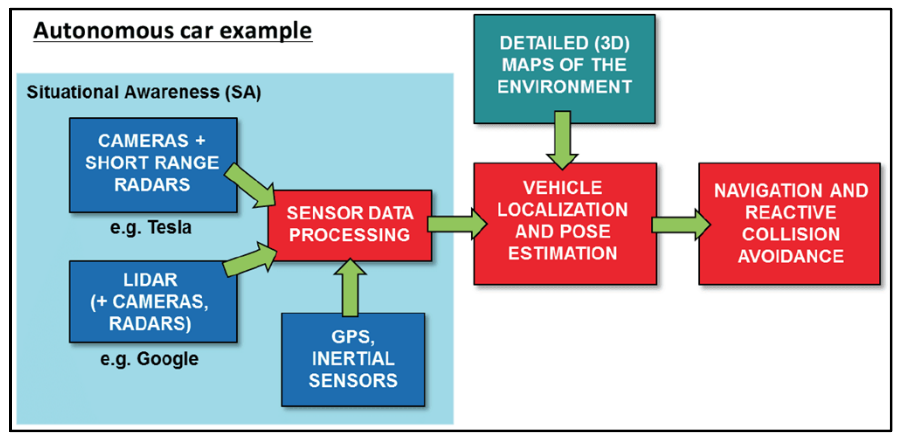
# CAVs: Cyber-Physical System dynamics





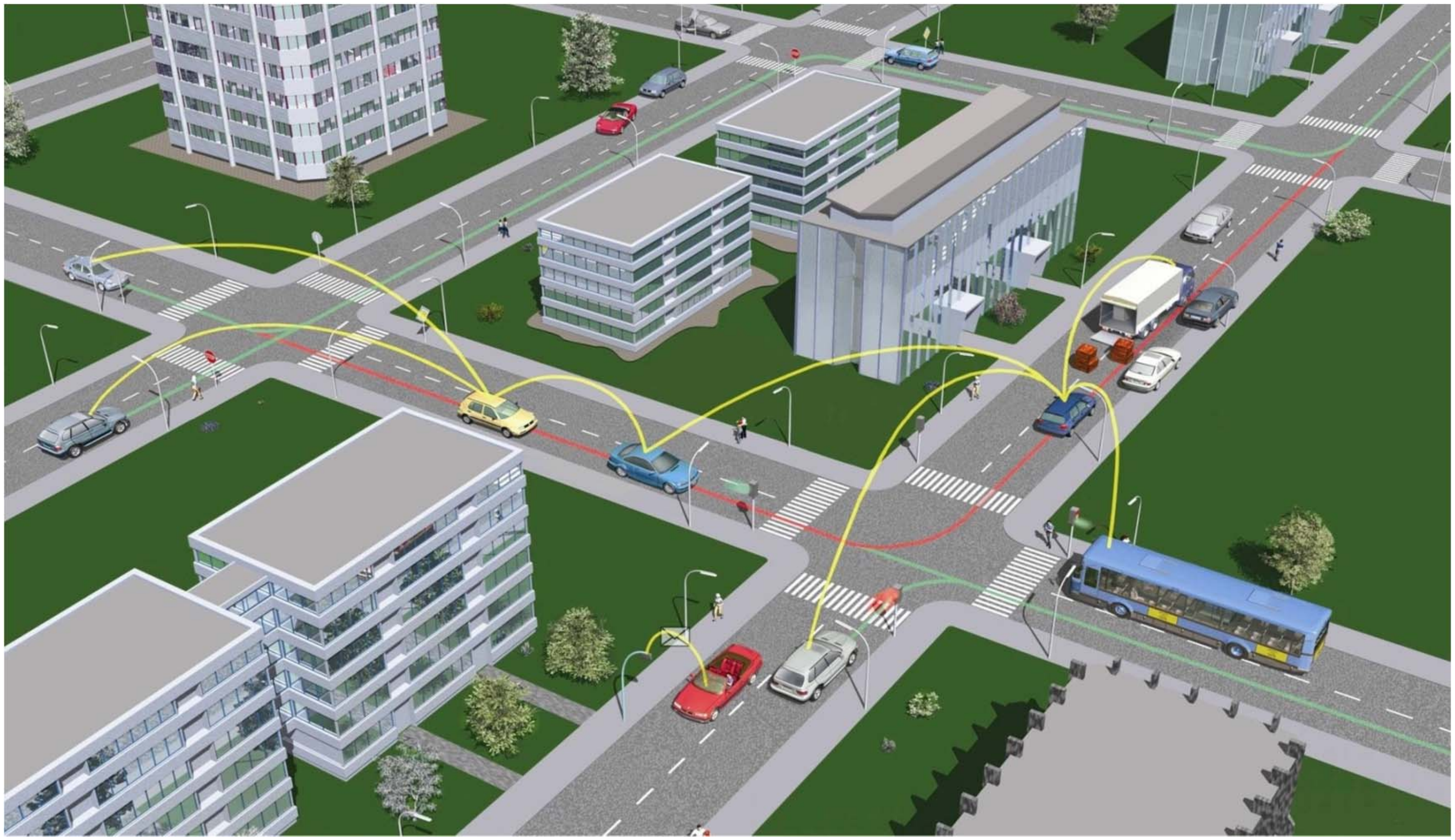

**Joint dynamics**
of
networking,
sensing,
&
control
resulting in
**variable latencies**



Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# CAVs: PNT-based safety messages exchange

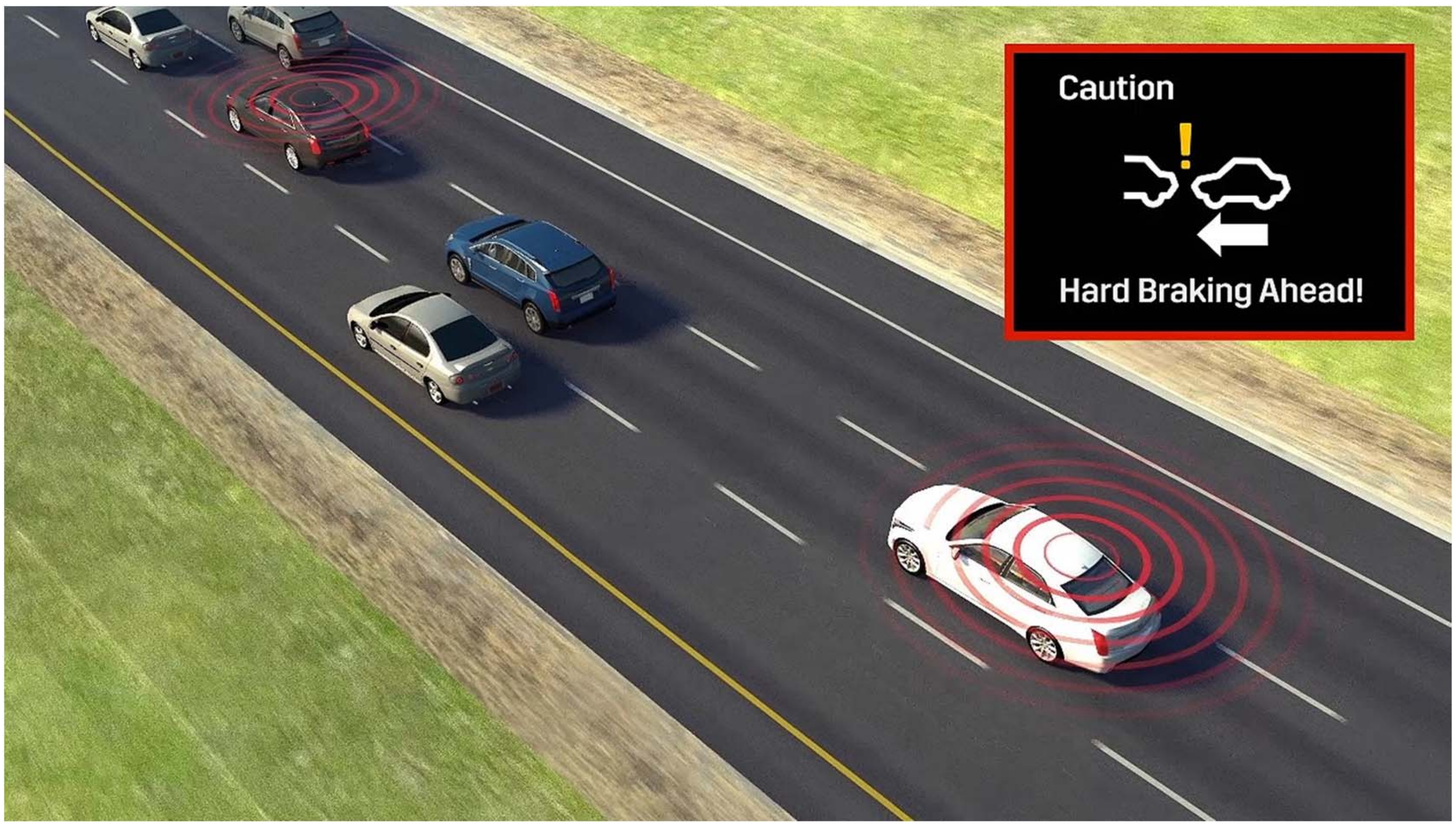
Connectivity for co-operative road safety assumes that CAVs minimise the use of the ambient communication infrastructure. The CAVs perform short-range V2V communications by forming a vehicle ad hoc network (VANET), symbolised below by the yellow multi-hop message passing (green / red lines are the intended paths of CAVs).



Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# CAVs: PNT-based safety messages exchange ctnd

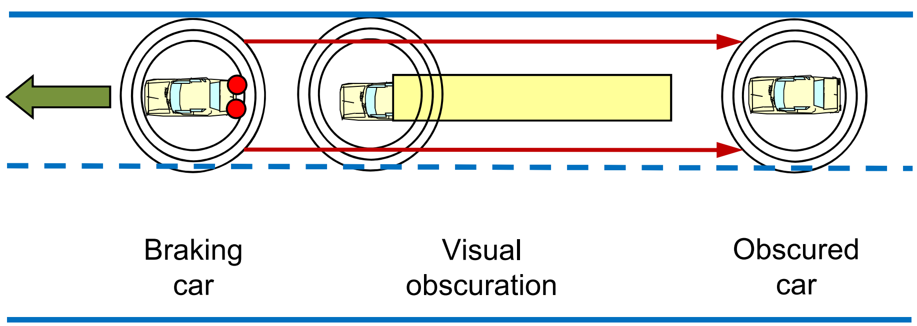
The most important use of connectivity in CAVs is to use V2V communications to exchange safety messages. The radio messages will have an effective range of a few hundred metres, allowing extension of situation awareness well beyond the line of sight. The illustration below shows that the brake lights of the black car are obscured by the blue car and hence the cameras of the white car cannot see them; however, the safety message can be quickly received.



Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Scenario: ETSI use case C.1.1.1

**ETSI use case C.1.1.1: Emergency electronic brake lights**
One-way safety message; max latency: 100 ms; min refresh rate: 10 Hz




**Application name:** Road hazard warning.

**Short description:** This use case consists for any vehicle to signal its hard breaking to its local followers. In such case, the hard braking is corresponding to the switch on of emergency electronic brake lights.

**Usage:** Warn all following vehicles of a sudden slowdown of the traffic so limiting the risk of longitudinal collision.

**Communication mode:** Time limited periodic messages broadcasting on event.

http://www.etsi.org/

## Robust PNT?

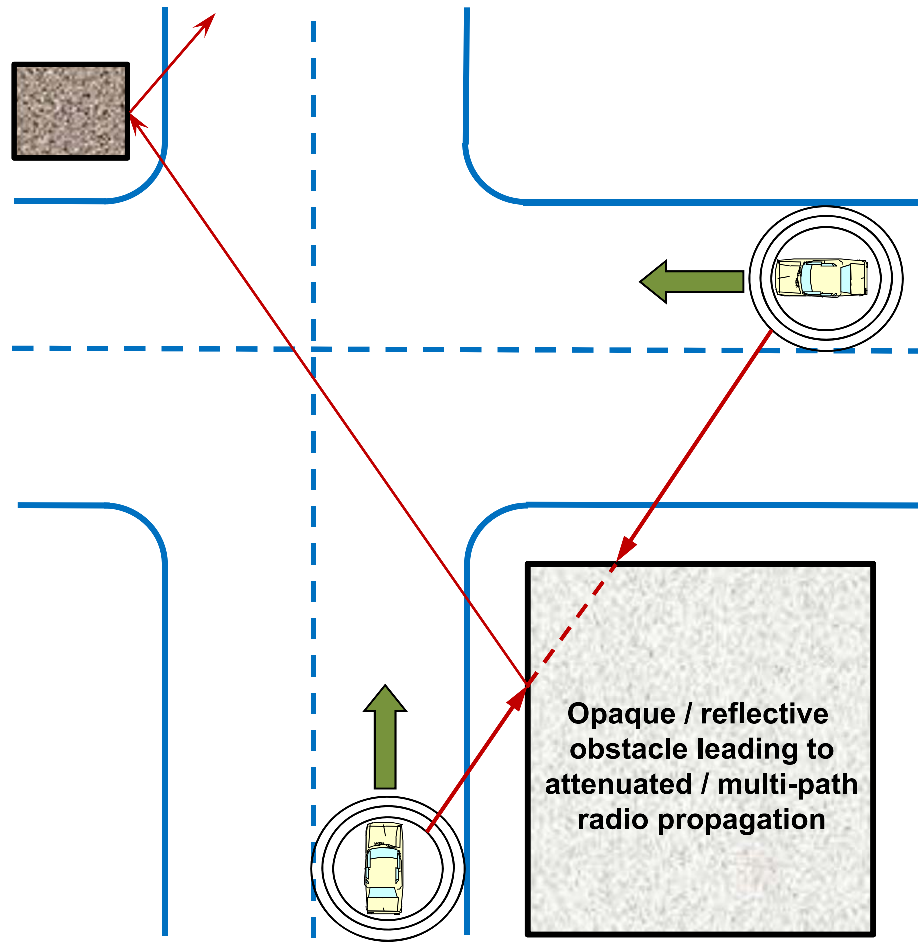
**Main requirements:**

- Capability for a vehicle, from the emergency electronic brake lights activation, to broadcast in V2X decentralized environmental notification messages.
- Capability for concerned vehicles to receive and process V2X decentralized environmental notification messages.
- Minimum frequency of the periodic message: 10 Hz.
- Critical time (latency time less than 100 ms).

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Scenario: ETSI use case C.1.5.4

**ETSI use case C.1.5.4: Intersection collision warning**
Two-way safety message; max latency: 100 ms; min refresh rate: 10 Hz




**Application name:** Co-operative awareness.

**Short description:** This use case allows that there is a risk of collision at an (un)controlled intersection and vehicles in the affected area are informed in order to mitigate the risk.

**Usage:** Avoid longitudinal collision.

**Communication mode:** Prevent/mitigate collision between vehicles.

## Robust PNT?

**Main requirements:**

- Capability for vehicles to broadcast V2X co-operative awareness messages and to receive and process V2X co-operative awareness messages.
- Accurate positioning of vehicles on digital maps.
- Minimum frequency of the periodic message: 10 Hz.
- Critical time (latency time less than 100 ms).

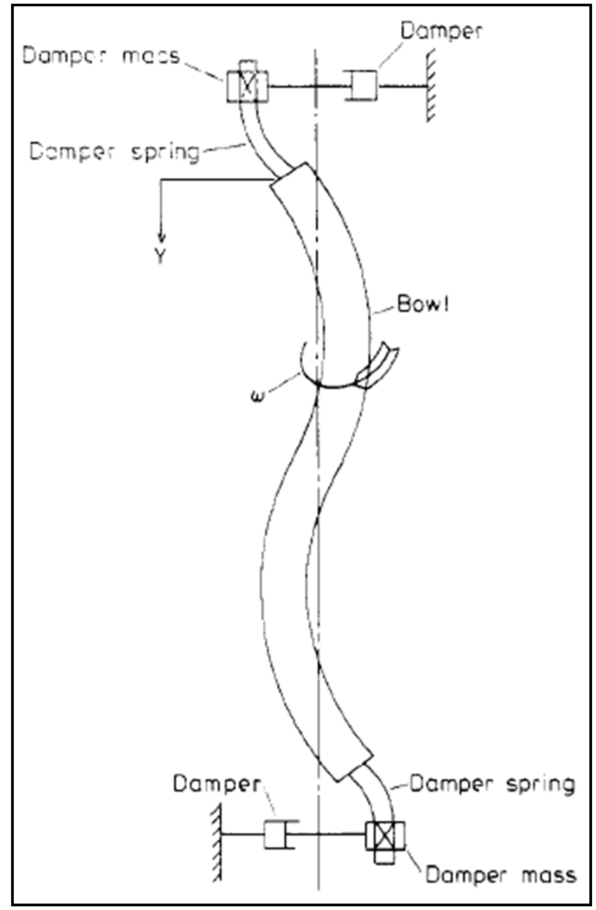
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Cyber-Physical Security:

## *From factory floor to multi-modal transport*

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

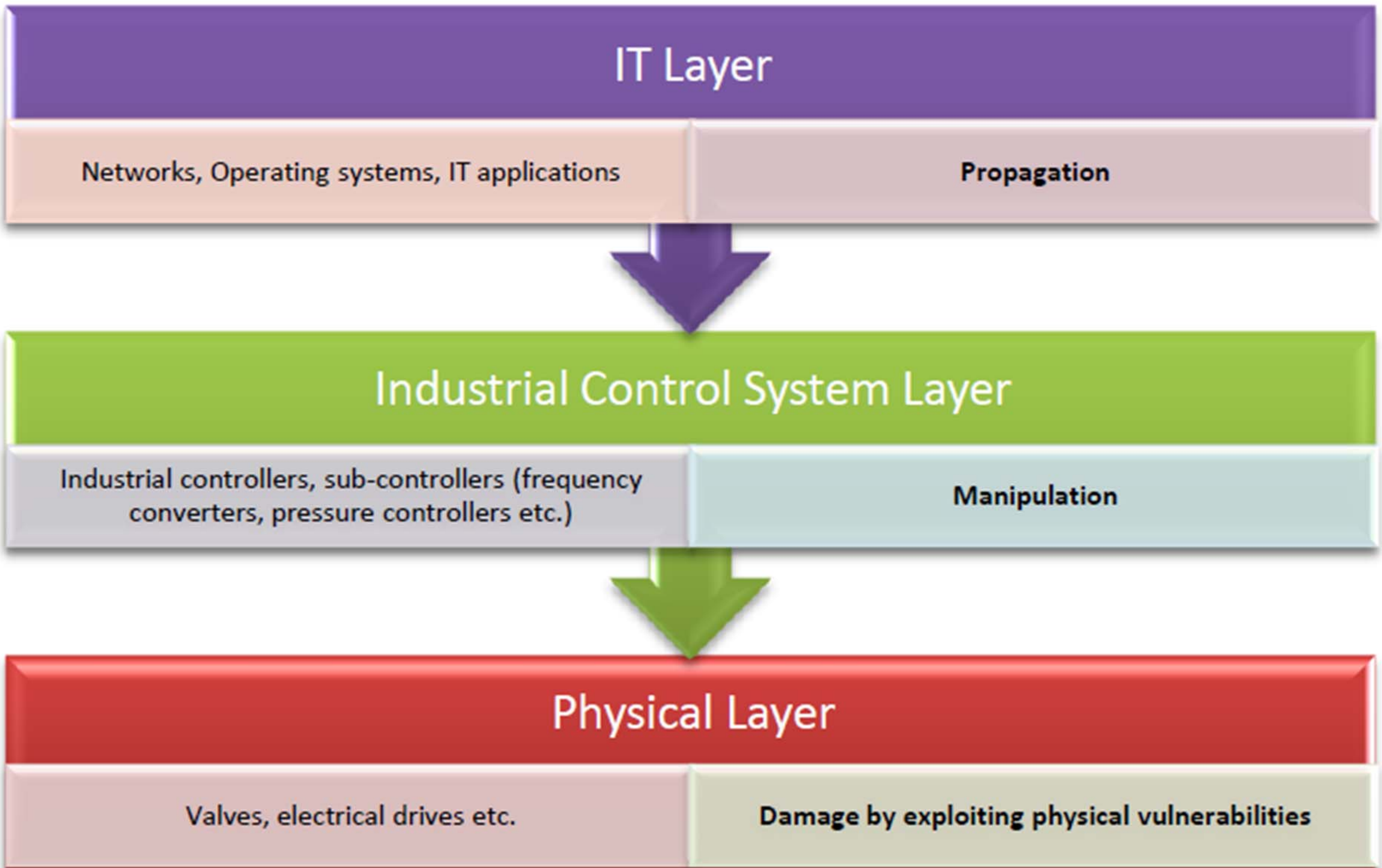
# Stuxnet: "To kill a centrifuge"




Centrifuges have a large length to diameter ratio which can result in standing wave patterns or **critical modes** which may result in excessive vibration and wall stresses, leading to mechanical failure.

Centre for Autonomous and Cyber-Physical Systems
School of Aerospace, Transport and Manufacturing
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# The three layers of a cyber-physical attack

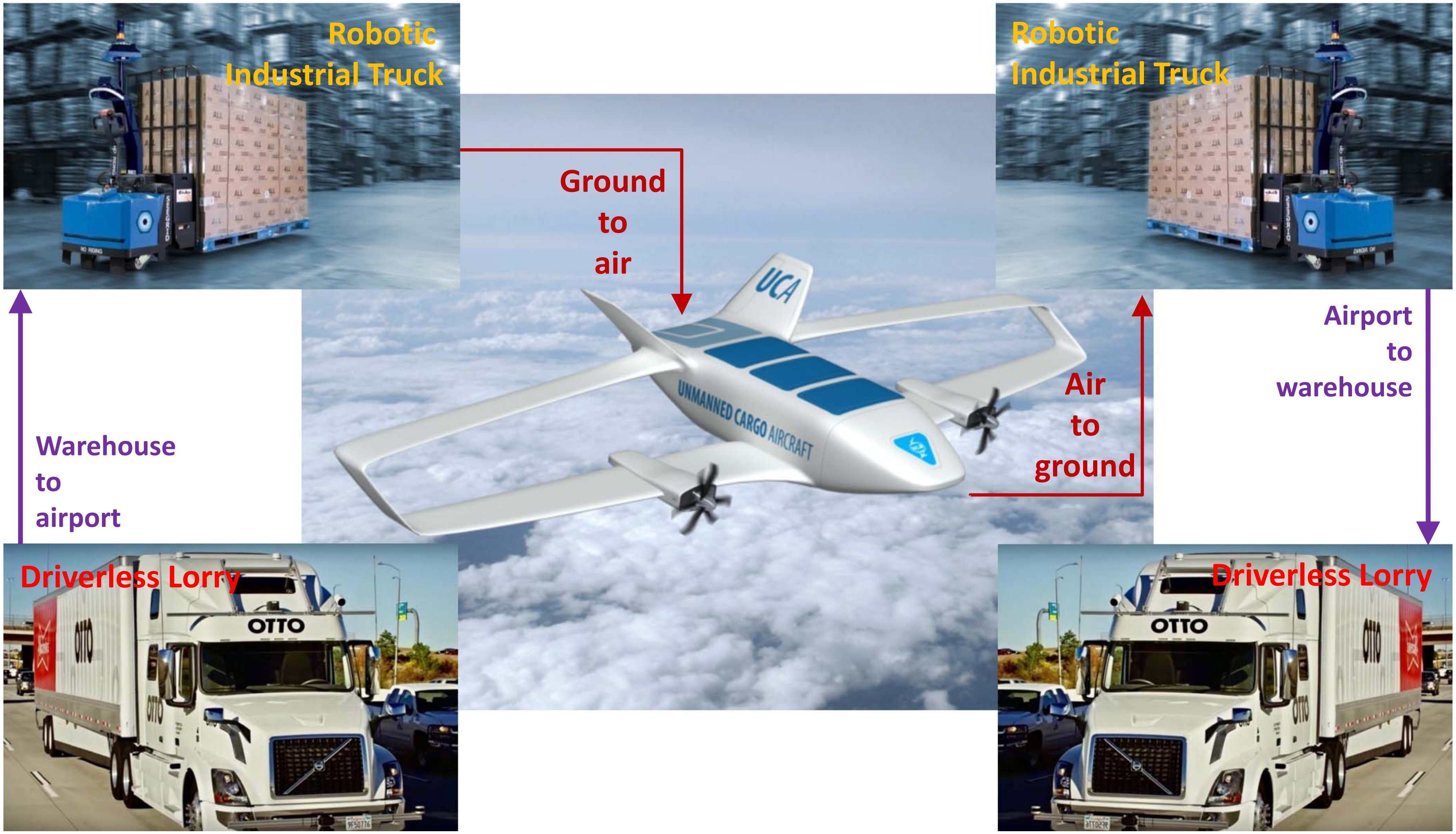


Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Challenge: Unmanned Traffic Management


Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Challenge: Autonomous multi-modal transport



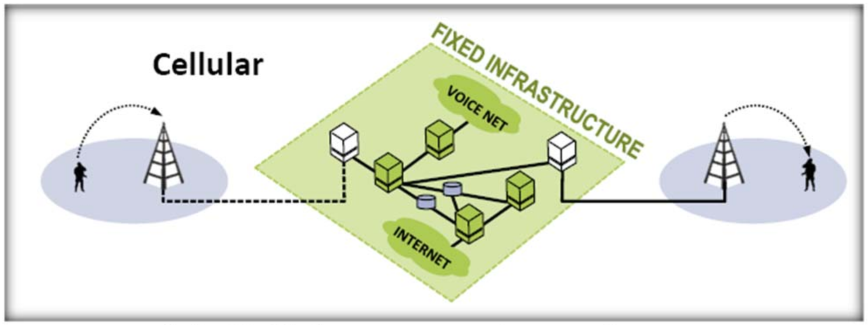
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Connected Autonomous Vehicles:

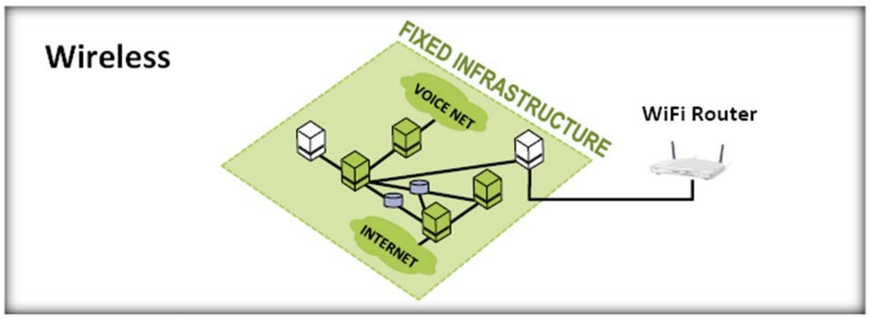
# *MANETs, VANETs and FANETs*

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

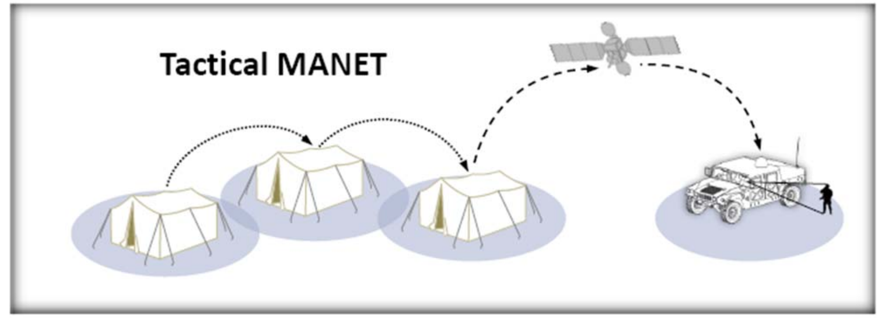
# Wireless networks: Fixed and ad-hoc



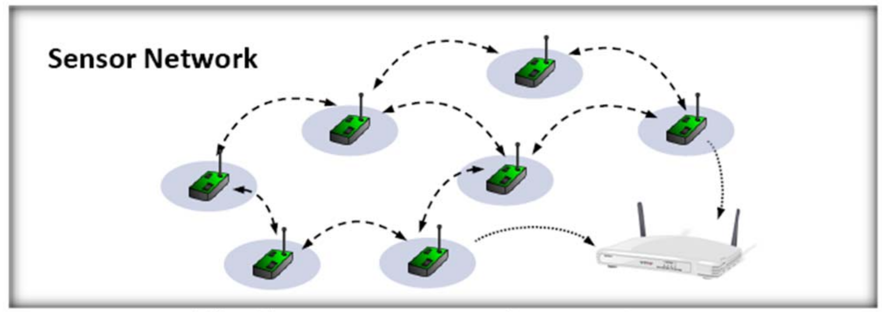

(a) Cellular network topology.




(b) Wireless network topology.




(c) Tactical MANET network topology.




(d) Sensor network topology.

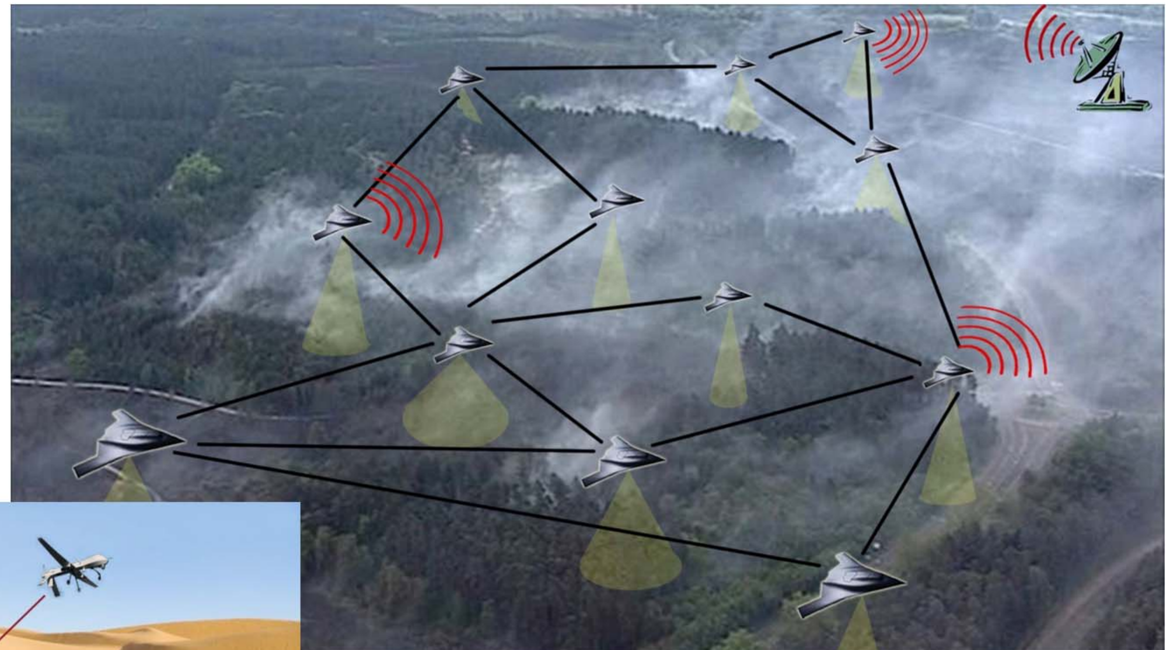
MANET = Mobile ad hoc network

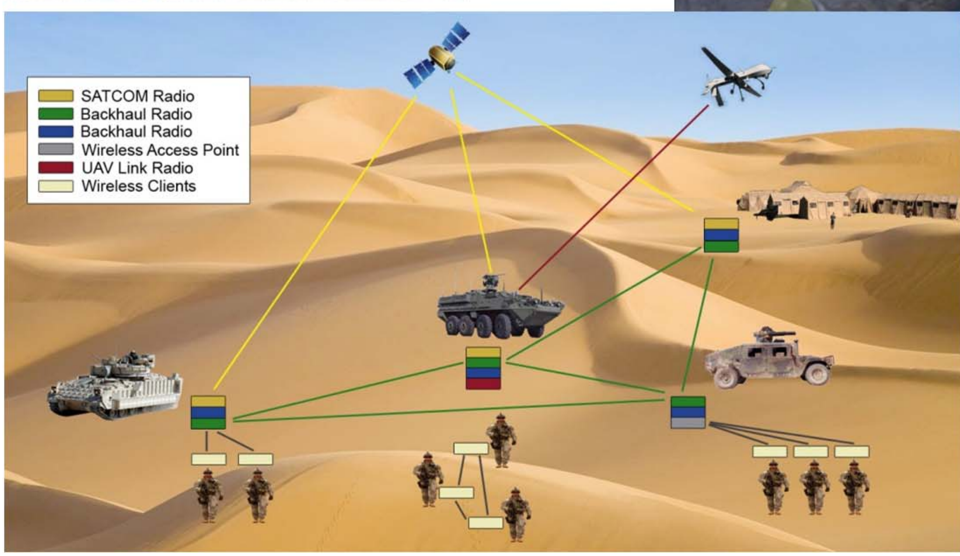
→ FANET = Flying ad hoc network

→ VANET = Vehicle ad hoc network

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Collaborating: UAVs (FANET) + UGVs (VANET)





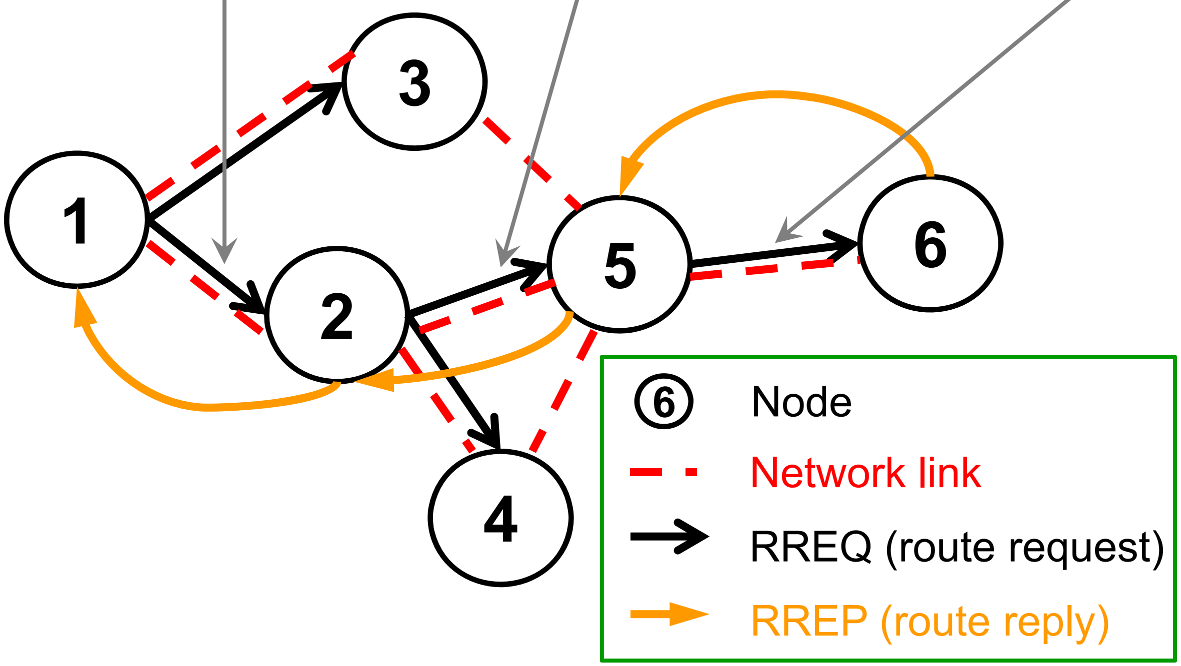

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# MANETs: Route discovery vs data messaging

**RREQ**
ORIGINATING NODE: 1
TARGET NODE: 6

**RREQ**
ORIGINATING NODE:1
TARGET NODE: 6
FORWARDING NODE: 2

**RREQ**
ORIGINATING NODE:1
TARGET NODE: 6
FORWARDING NODES: 2,5

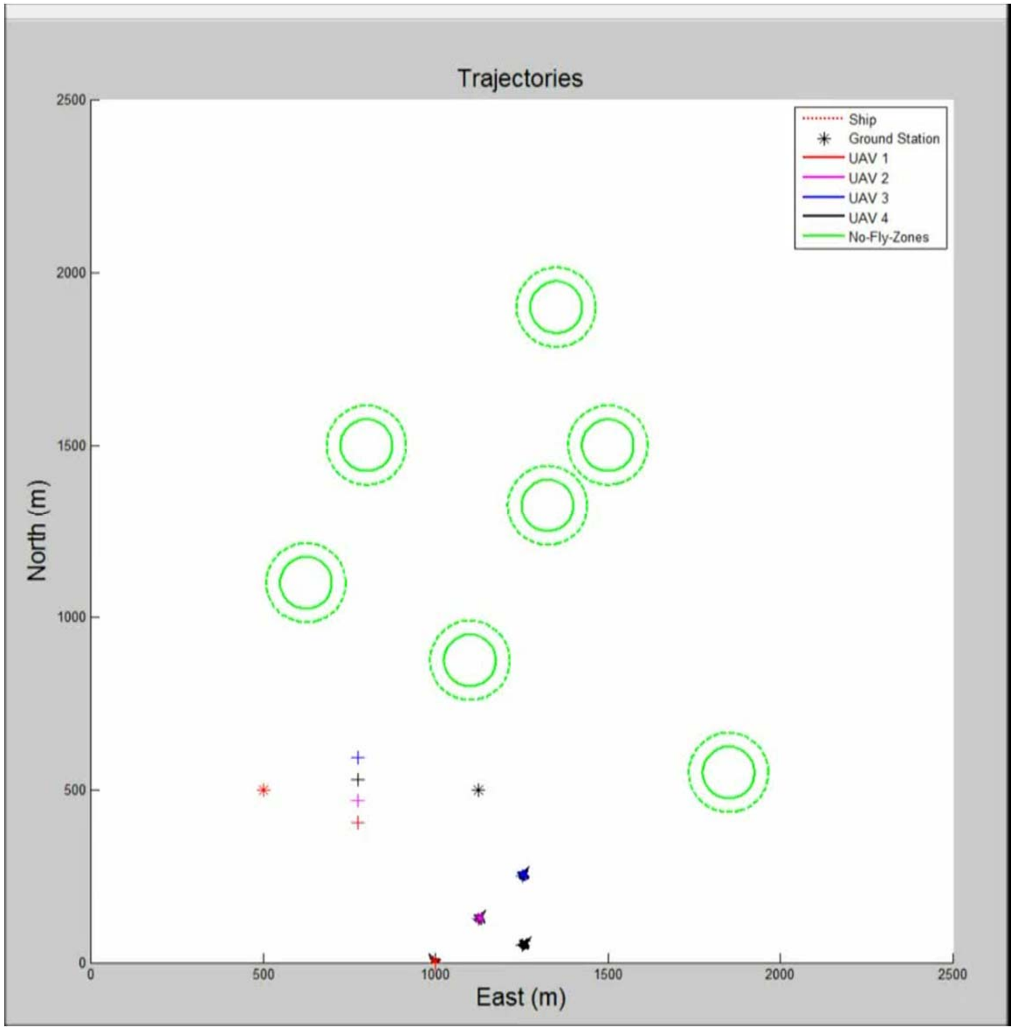



Due to ever-changing MANET topology, existence of routes for message-passing must be updated frequently. Hence, two types of data flow in MANETs: 1) route-discovery data, and 2) message data.

Deciding criticality of each (or both) type of data is application-dependent and is not well understood. A mix of event-driven and time-driven approaches is needed.

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# MANET: Path following vs network cohesion




MANETs are multi-hop networks with changing topology and weak infrastructure. The ***multi-hop*** character means that nodes (UAVs) cannot always communicate directly; instead, they must use other nodes as comms relays. The ***changing topology*** is due to motion of the nodes and ***weak infrastructure*** results from nodes alternately acting as comms relays or transceiving nodes.

Message-passing is the **cyber** aspect of MANETs whilst motion of the nodes is a **physical** phenomenon making MANETs Cyber-Physical Systems. The key challenge is the **joint dynamics** of path following (necessary for mission completion) and network cohesion (necessary for message passing), see simulation video on the left.

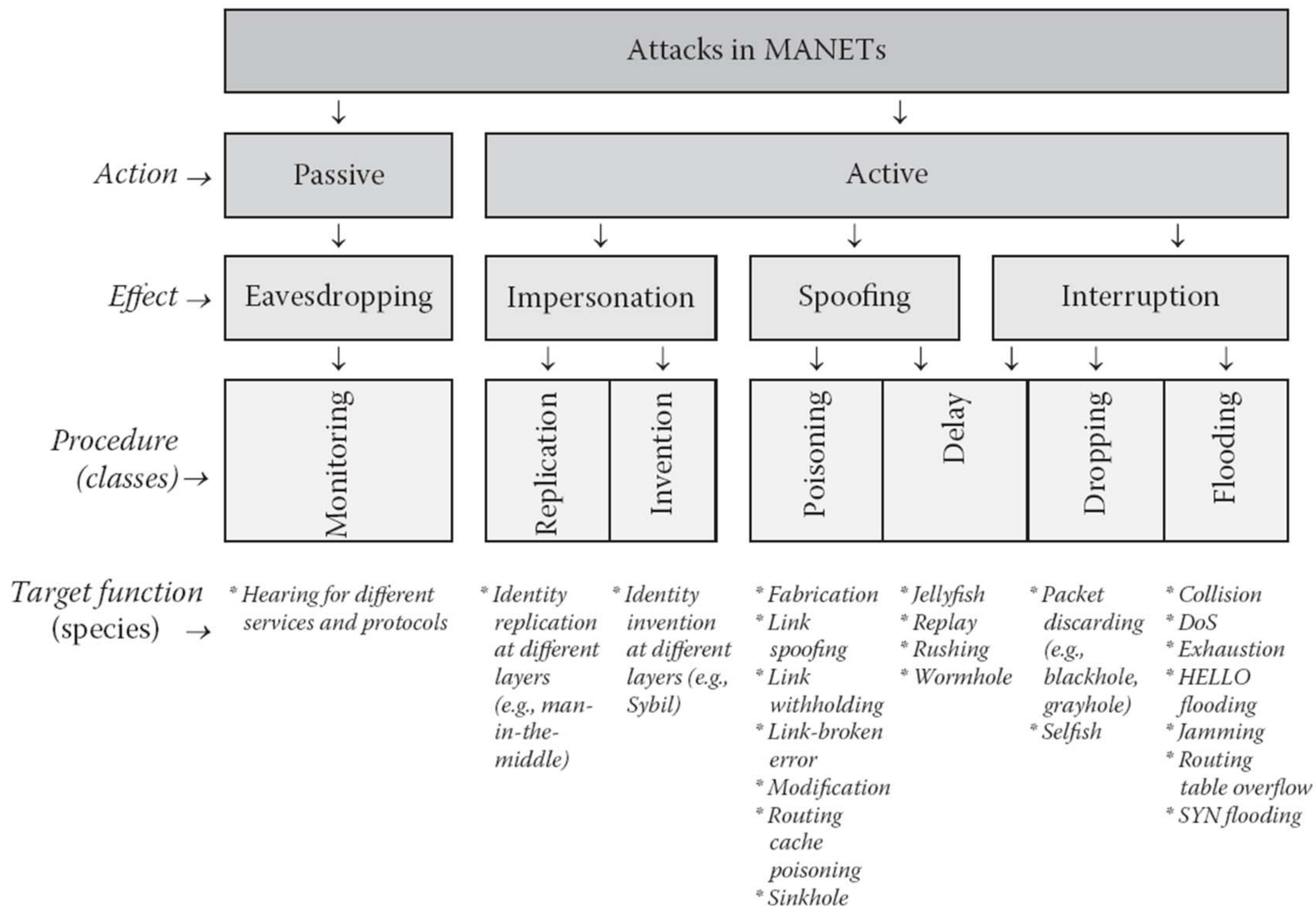
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Connected Autonomous Vehicles:

# *Cyber-Physical threats*

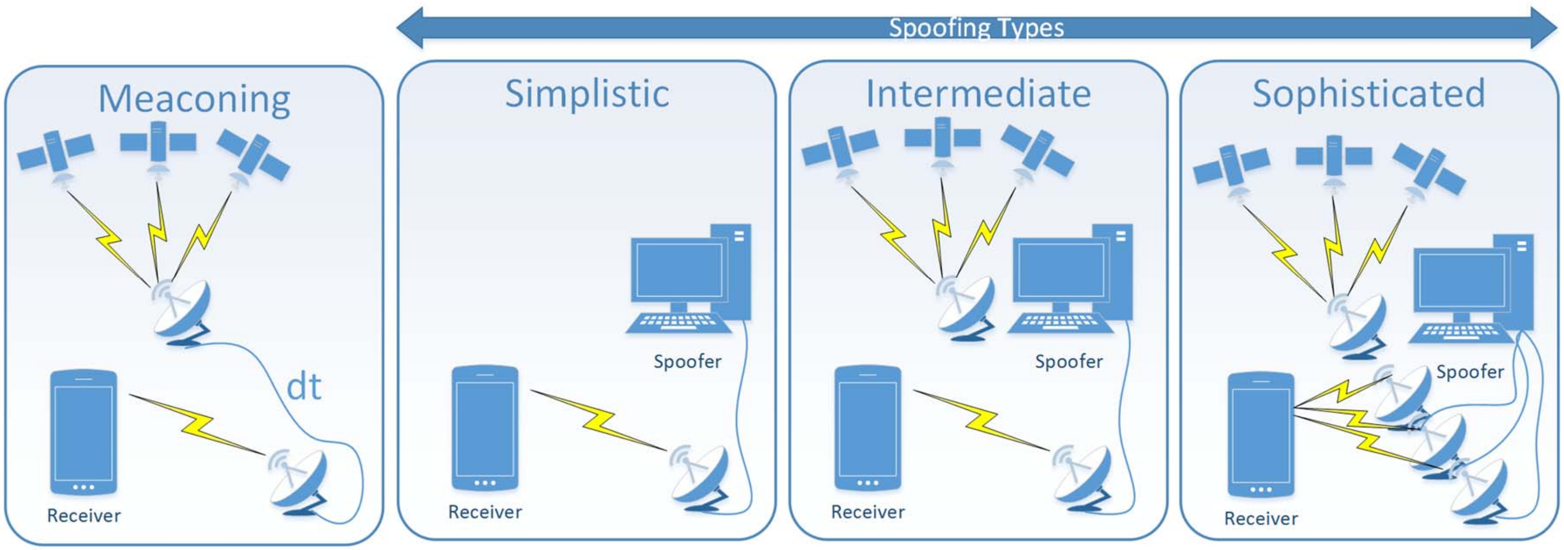
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Taxonomy of attacks on MANETs



Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Attacks on MANETs – How about PNT?




**Jamming** Blocking reception of the GNSS signal by deliberately emitting electromagnetic radiation to disturb user receiver by reducing the signal-to-noise level

**Meaconing** Rebroadcasting of delayed GNSS signal without any distinction between SIS from different satellites

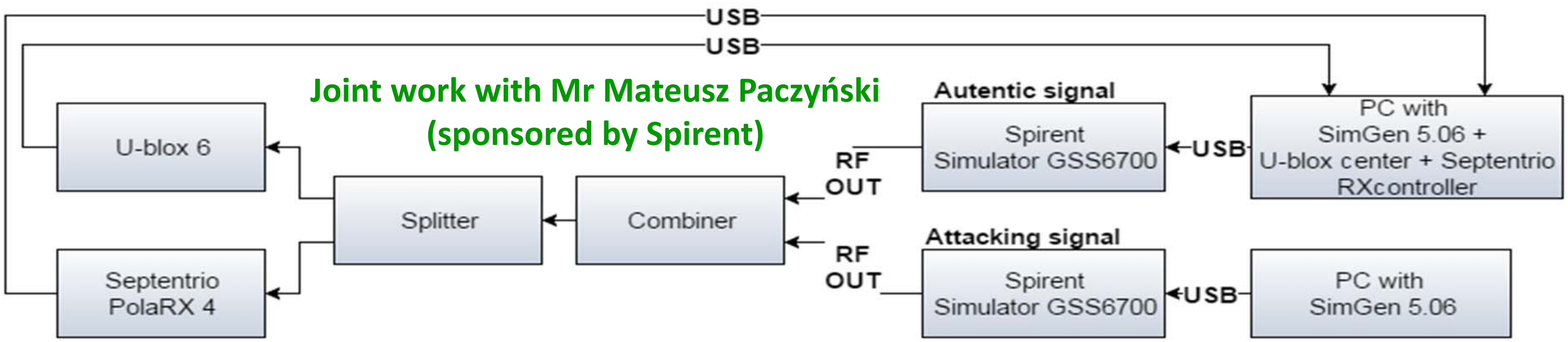
**Spoofing** Transmission of counterfeit GNSS-like signal, with the intent to produce a false position within the victim receiver without disrupting GNSS operations.

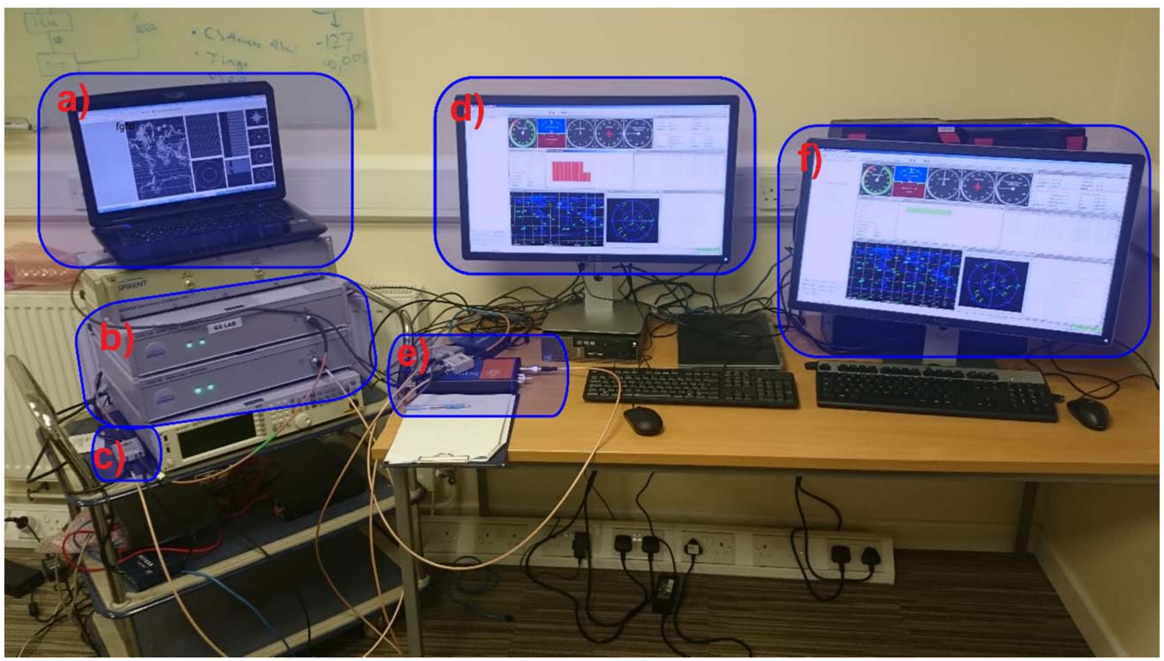
Centre for Autonomous and Cyber-Physical Systems
School of Aerospace, Transport and Manufacturing

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Example: Hardware-in-the-loop meaconing

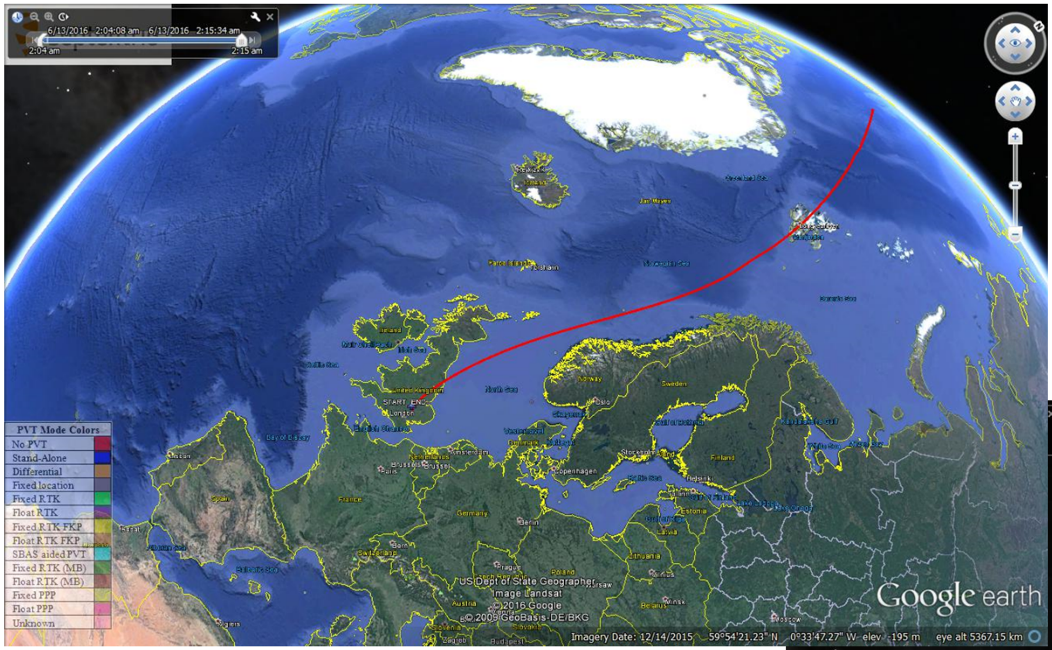
Joint work with Mr Mateusz Paczyński
(sponsored by Spirent)



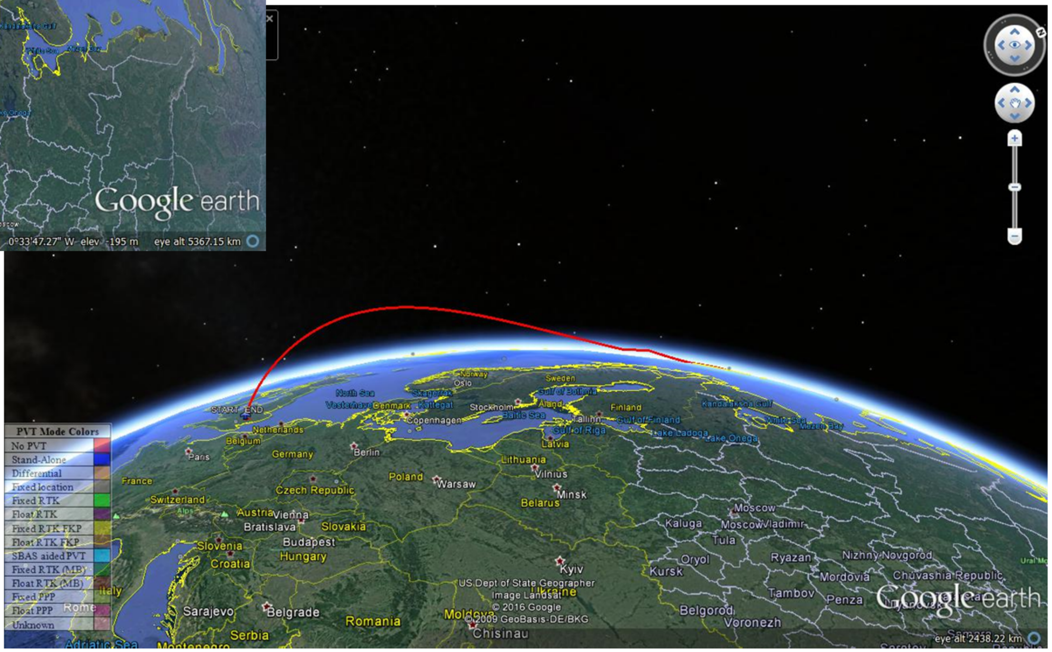
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Example ctnd: Effect of meaconing attack



- A delay between real and attacking signal was approximately 2 seconds
- During the attack RIAM and multipath option were disabled in the receiver

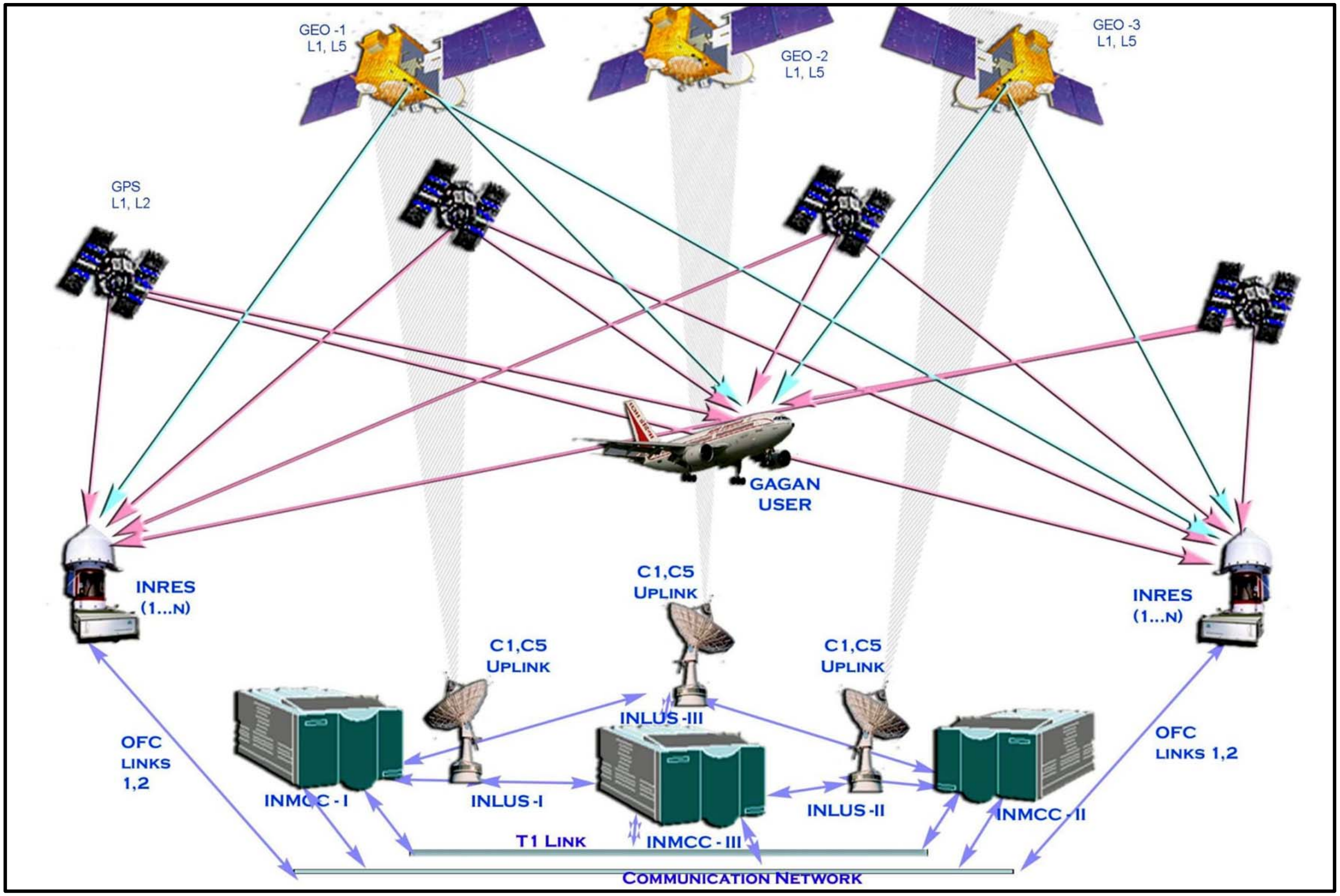
**Joint work with Mr Mateusz Paczyński (sponsored by Spirent)**



- Receiver attacked by 100-metre pseudorange 9-minute ramp
- Meaconing has strong effects without taking control of the receiver
- Ease of meaconer construction makes it potentially dangerous

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# EW + Cyber → Cyber-Physical Security ← Motion



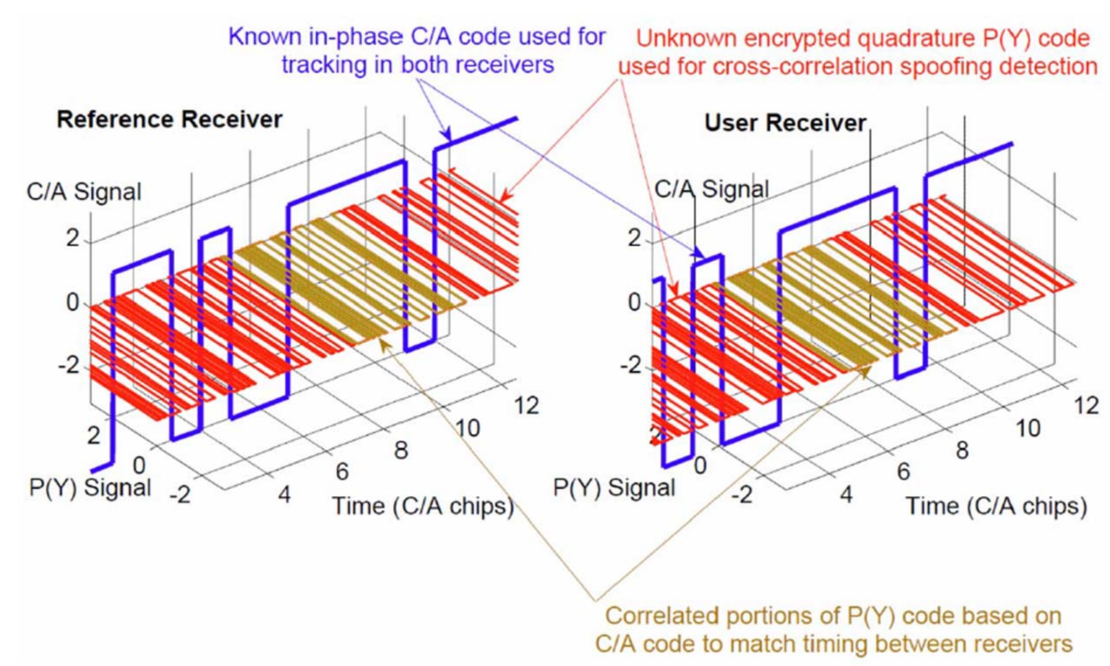
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Connected Autonomous Vehicles:

## *Cyber-Physical threat mitigation*

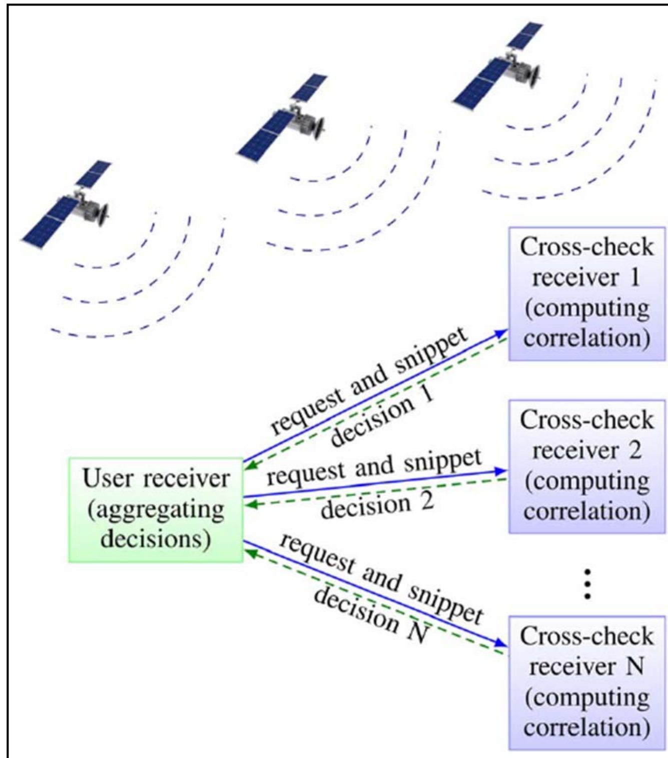
Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Robust PNT for MANETs – Cooperative peers




Spoofing detection by cross-correlation. The publicly known C/A signal and the encrypted P(Y) signal are modulated onto the GPS L1 carrier in-phase and quadrature. Each receiver tracks the C/A code and uses its phase and timing relationships to the P(Y) code to take a snippet of the same part of the P(Y) code. A high correlation will occur if the two snippets contain the same P(Y) code.

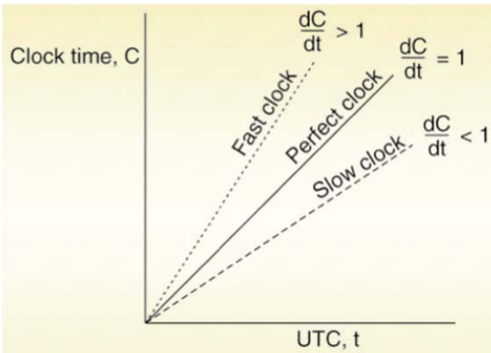
*IEEE Trans. Intelligent Transportation Systems, 2015, 16(4), 1794–1805*

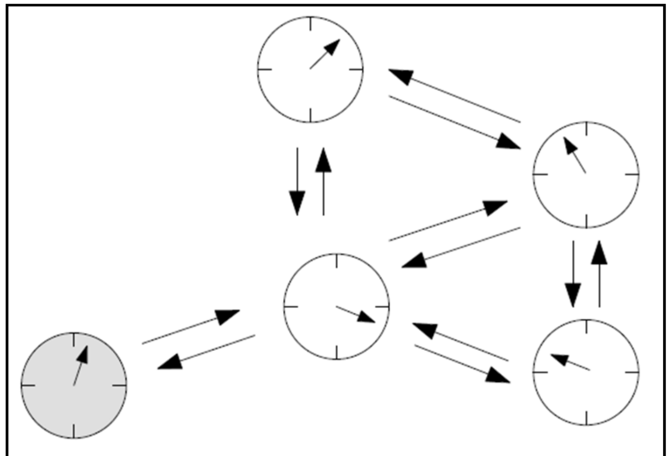



Each cross-check receiver computes the correlation between its own snippet and the one from the user receiver. The user receiver aggregates the decisions from all cross-check receivers.

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

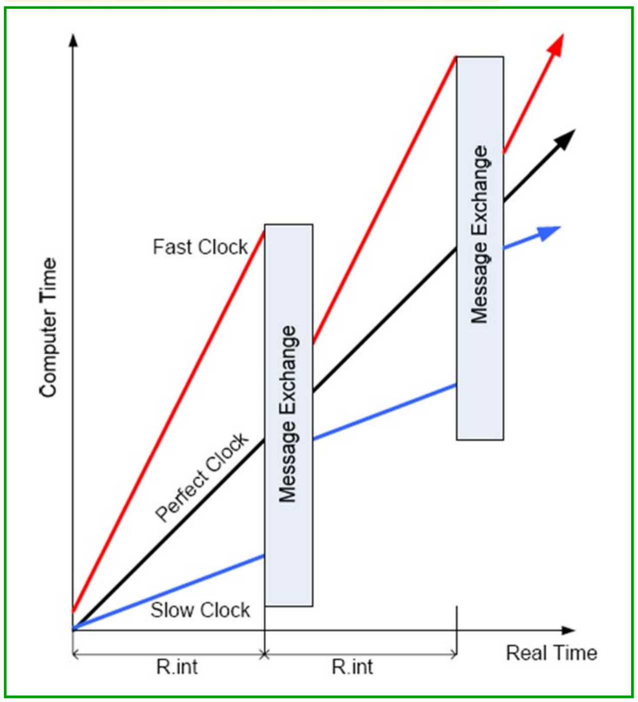
# Robust PNT for MANETs – Synchronisation

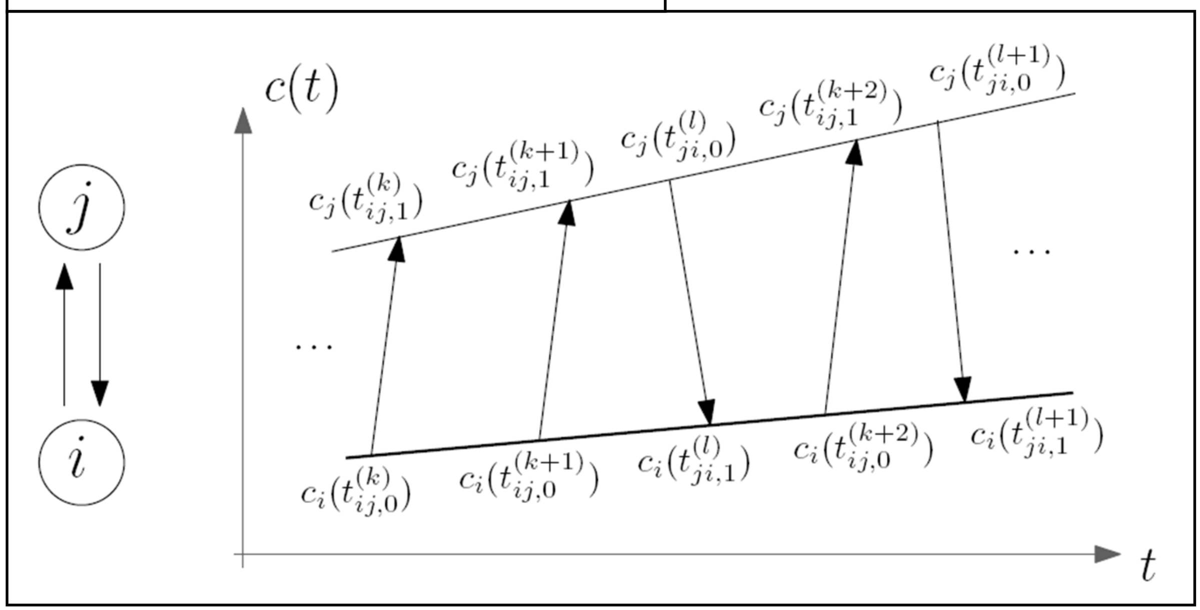


Cooperative synchronisation in wireless networks

IEEE Transactions on Signal Processing, 2014, 62(11), 2837–2849



Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Summary

- Connected Autonomous Vehicles (CAVs) are emerging on a large scale
- CAVs necessarily entail wireless networking of moving vehicles, resulting in MANETs
- Robust PNT is essential for motion planning for all MANETs arising in CAV applications
- CAVs are networked and function in real time, making them Cyber-Physical Systems (CPS)
- Wireless clock synchronisation with respect to physical time is a key CPS problem

Professor Rafał Żbikowski
r.w.zbikowski@cranfield.ac.uk

# Thank you for listening…

**…to our Dad—we don't!**