# **TAS-S Overview:** Bridging Gaps Between Makers and Users

*Lancaster University, Cranfield University*

Researchers: Dr. Anders af Wåhlberg, Pierre Ciholas, Dr. Oscar Gonzalez Villarreal, Dr. Yi Li , Alvaro Lopez, Dr. Luke Moffat, Dr. Andrew Sogokon, Dr. Zhuangkun Wei, Dr. Zhengxin Yu, Dr. Burak Yuksek.

Engineering and Physical Sciences Research Council

TAS-S

## What is Autonomy?

The ability to effectively conduct a mission with varied levels of absence of human intervention including completely unsupervised operations.

## Autonomous System

- Perceive environment
- Make decision
- Actuate a movement

**Coordination**
- Homogenous / heterogenous fleet operations.
- Resource sharing between assets.
- Maximising the operation effectiveness, safety and security.

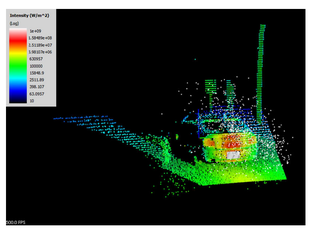
**Control**
- Command tracking with minimum error and appropriate dynamics.
- Adaptation mechanism for different conditions.
- Verifiable closed-loop dynamics and stability for trustworthiness.

**Decision Making**
- Making predictions about physical and environmental phenomena.
- Trustworthy and reliable actions as the system and environment changes

**Learning Enabled**
- Acquiring environmental data and behavioural adaptation in real-time.
- Provable safety and robustness.

**Dynamic**
- Real-time adaptation capability.
- Responsive for environmental, dynamical and operational variations

## UKRI TAS-S Trustworthy Autonomous System node in Security

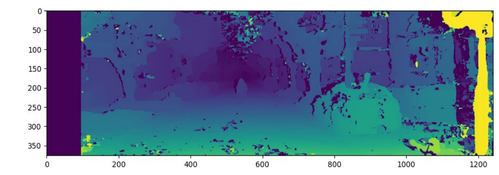


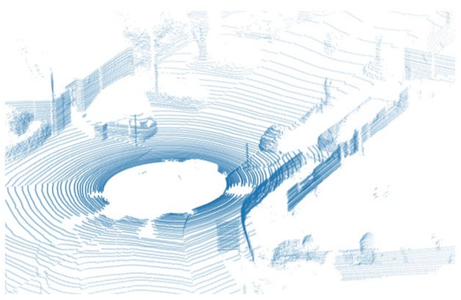
What is trust is performative?
From lack of alternatives
What ways can trust be done differently?

How and/or why do publics trust processes such as this?

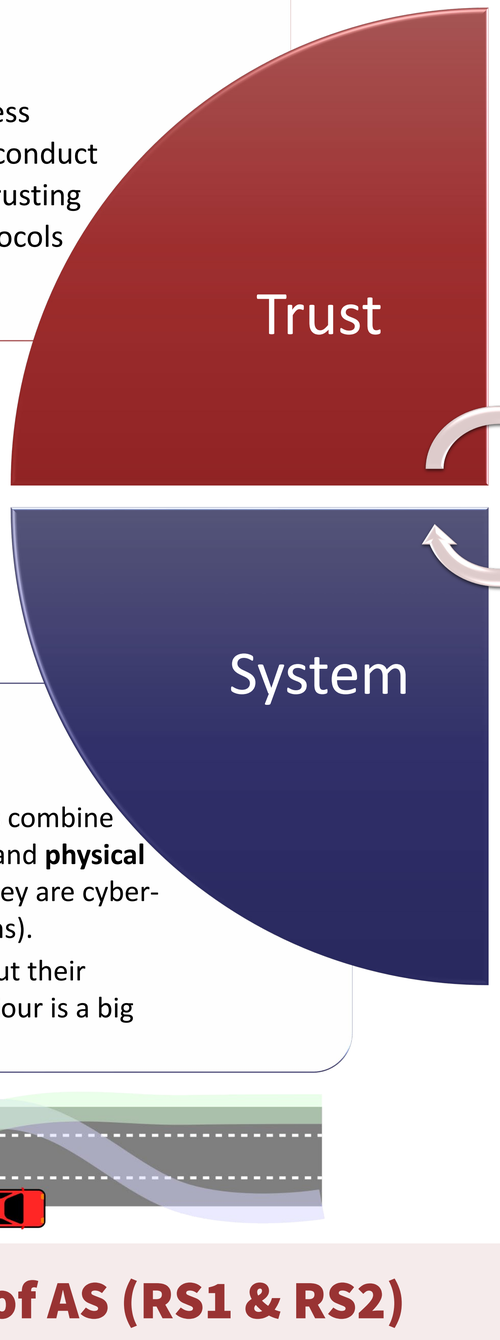
Factoring in resistance and dissent

- Expectation meeting reality
- Risk perception
- Verifiability
- Societal Readiness
- Trust as ethical conduct
- Other ways of trusting
- Indigenous Protocols

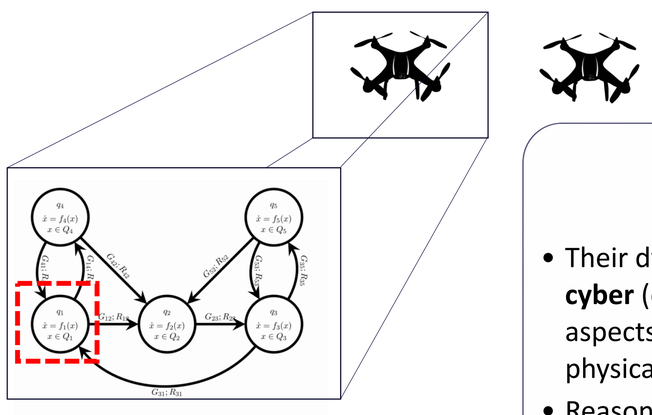




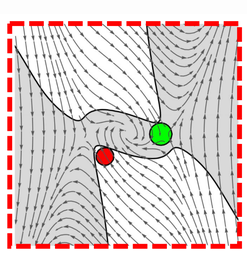
- Co-ordination & control
- Decision making
- Dynamic
- Learning enabled

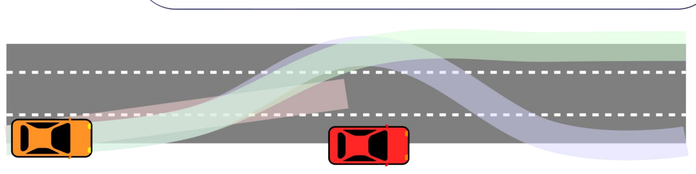



- Autonomous systems are often **networked** and operating in environments where they are exposed to attacks.

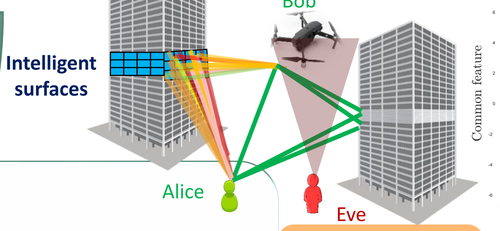


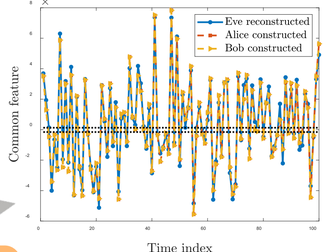
- Their dynamics combine **cyber** (digital) and **physical** aspects (i.e. they are cyber-physical systems).
- Reasoning about their physical behaviour is a big challenge.





- Security of Autonomous systems are from different layers, with specific attack vectors and countermeasures.




- Four layers of security
- **Attacks vectors** – Information leakage, Spoofing, Jamming, Tampering of privilege
- **Countermeasures**- Cryptography, (quantum, physical, mathematical), authentication, Federate differential privacy

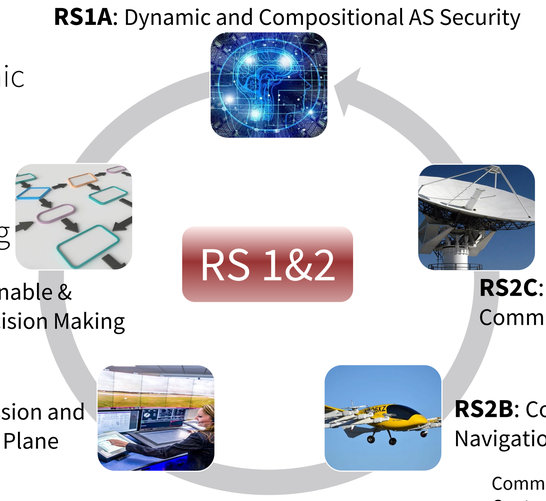
| | |
|---|---|
| App Layer | Learning based method to prevent malicious uses, protect data privacy |
| Network Layer TCP, UDP | Internet protocol and socket security |
| Access Layer Virtual, Mac | Authentication against spoofing and sniffing |
| Physical Layer: control, comms | Protect channels from contamination (jamming, spoofing), and prevent information leakage |



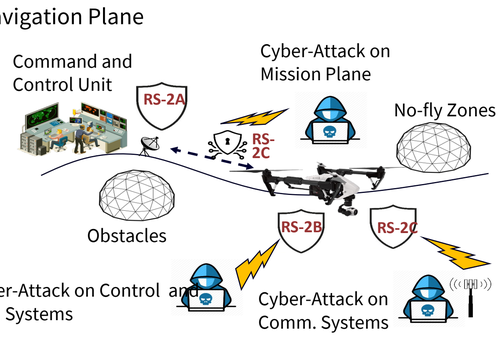

## Secure Usage and Operation of AS (RS1 & RS2)

## Secure Operation and User of AS (RS2 & RS3)

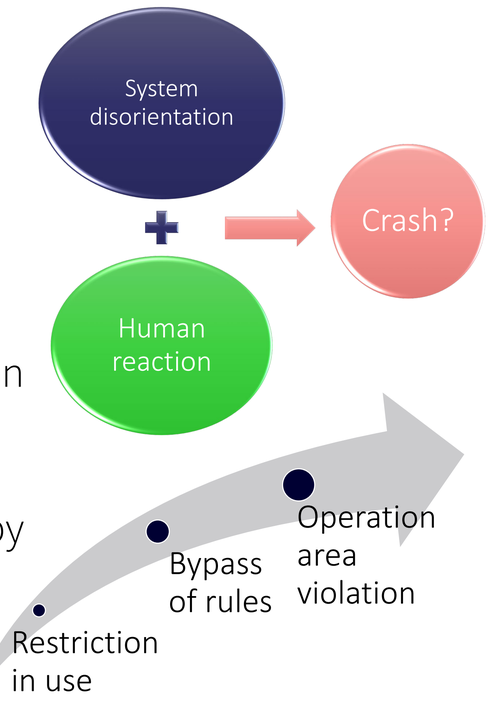
### RS1: Secure Usage
- Adaptive and dynamic ML framework
- Robust learning & Detection
- Safe decision making




### RS2: Secure Operation
- Mission
- Control and Navigation
- Communication




### RS3: Secure User
- Individual Behavioural Adaptation
- Organizational Processes
- Ethical & Legal Security Ecosystem




- If an attack disorientates a vehicle, how does the human react?
- How should the system react to an attack situation to enable the human to safely handle the situation?
- Can autonomous systems be misused through violation of rules by provision of faulty information by users?

Lancaster University
Cranfield University
UKRI Trustworthy Autonomous Systems Hub

This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]