On control engineering, reliability and smart infrastructure enabling safer autonomous vehicle operation

Cranfield University

Professor Argyrios Zolotas
Centre for Autonomous and Cyber-Physical Systems

… Cranfield University…

1946 Cranfield College of Aeronautics

1969 The Cranfield Institute of Technology

1993

- Cranfield is situated in Bedfordshire, England

- Between London and Birmingham

- **Cranfield is ranked in the world's top 30 institutions for the subject area 'Engineering – Mechanical, Aeronautical' (2024 QS World University)**

Cranfield University
Cranfield
MK43 0AL, UK

Contents

- Preamble (background)
- Control engineering and reliability
- Autonomy and the role of infrastructure in validation
- Towards autonomous systems certification

Autonomous and Cyber-Physical Systems Centre

Our Centre develops the technology behind autonomous vehicles which operate in the air, on land, at sea and in space.

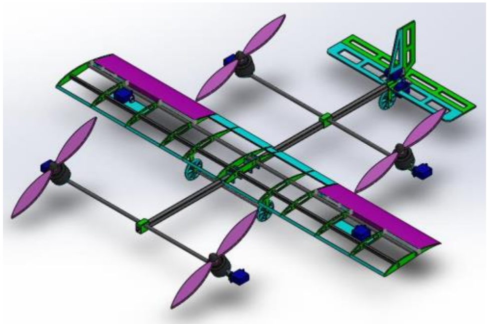
Additional expertise is in the field of UAS Traffic Management, focusing on safe integration of UAS in national airspace.

We have an outstanding international reputation for the quality of our work and our capability of performing both theoretical and experimental studies

Novel UAS Design and Green Air Vehicles

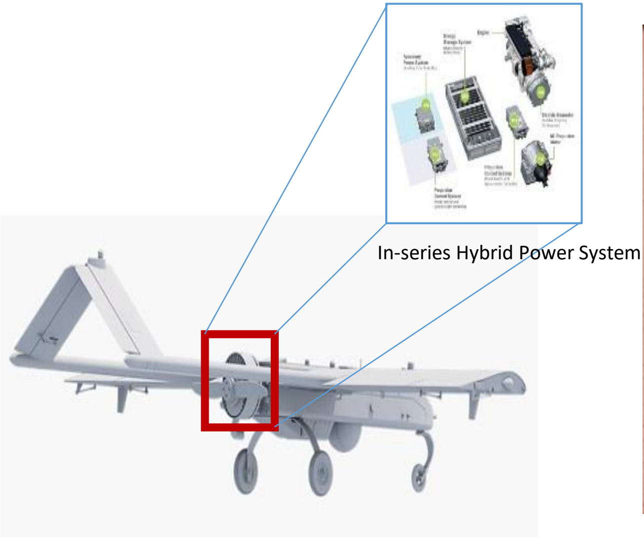
System Centric Aerospace Research

Variable pitch for 4+ rotor UAS

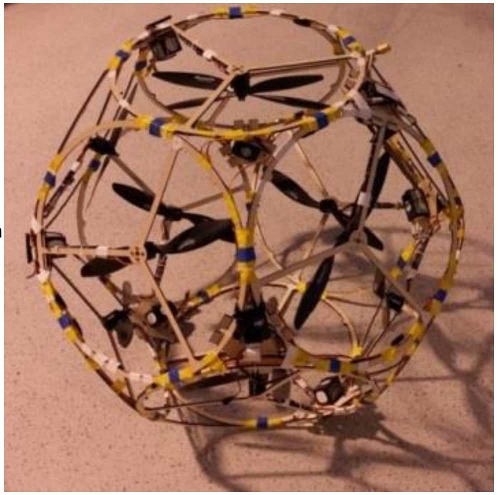


BVLOS UAS

Hybrid Fuel Cell
Aerial Platforms



Hybrid Electric Aerial Platforms



**Development of a Novel
Polyhedral Mult-copter**

AEROSPACE TECHNOLOGY INSTITUTE

AS UR AUTONOMOUS SYSTEMS UNDERPINNING RESEARCH

Aerospace Growth Partnership NATEP

Advanced Mobility Ecosystem Consortium

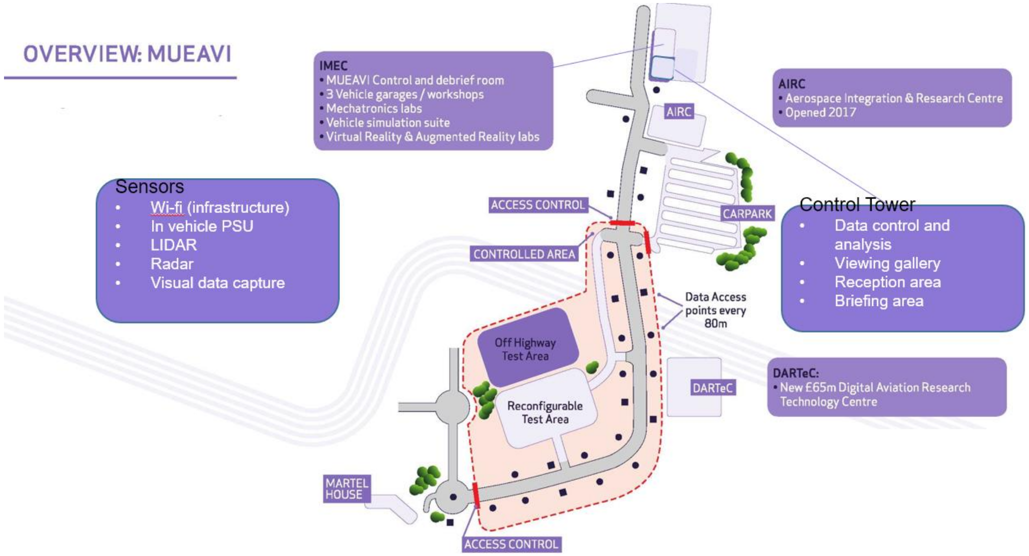
UKRI Innovate UK

Future Flight Challenge Programme

Developing new ecosystem to demonstrate the commercial and operational viability of Advanced Air Mobility (AAM) flying taxi and accelerate the net zero target.

ATKINS Member of the SNC-Lavalin Group · CATAPULT Connected Places · Cranfield University · Heathrow · VERTICAL · Skyports · NATS · NEURON · virgin atlantic

CAV projects participation



HUMAN DRIVE

https://humandrive.co.uk/

NISSAN MIRA Cranfield University HITACHI Inspire the Next

aimsun. UNIVERSITY OF LEEDS SBD highways england

CATAPULT Transport Systems ATKINS

CORAM
CONNECTED ON-ROAD AUTONOMOUS MOBILITY

Propelmee Cranfield University CATAPULT Transport Systems

Control Engineering and Reliability

8

Control Engineering = enabling technology

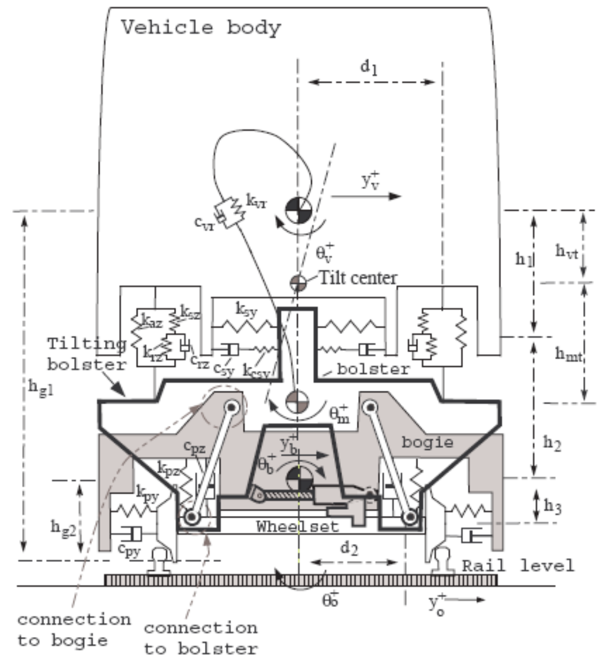
Example: Advanced control of Tilting Trains

- Clear commercial benefit of tilting trains substantial reduction in journey
- Increasing speed by 30% but maintain acceptable ride quality levels on same track!
- Concept: vehicle tilts inwards on curved section of the rail track (corners)
- Commercial tilt controllers use precedence information (from precedent vehicle sensors with appropriate delays) or track database (GPS)
- Complex schemes, inter-vehicle signal connections train performance optimised for specific route, direction-sensitive, fault detection difficult, track databases require often update
- Work on simpler local/'per vehicle' controller structures possible via advanced/modern control concepts

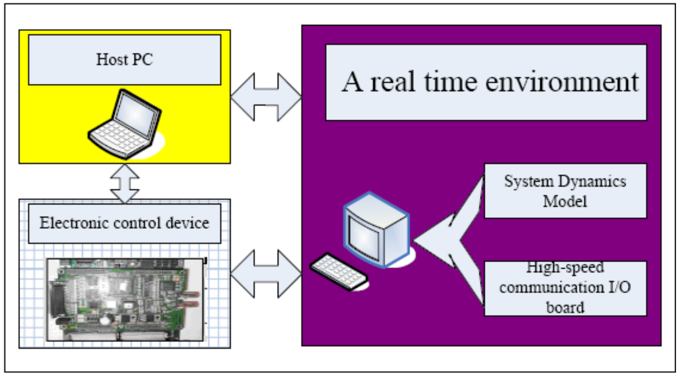
Control Engineering = enabling technology

Advanced control of Tilting Trains

- Fundamental study of tilt control concept
- Detailed modelling of end-view (Linear/Non-Linear)
- Rigorous analytical investigation of nulling-tilt problem
- Development of an assessment approach of dynamic tilt controllers' performance
- Employing robust H-inf controllers and estimator-based solutions
- Extensions to simplified tilt control with fuzzy control correction
- Incorporation of dual actuator studies (both tilt and active lateral) to further enhance performance
- Hardware-in-the-Loop studies
- Use of fractional control based enhancements



End-view model with tilting bolster



Reliability and path to autonomy

AI-based fault tolerant control with multiple sensing / actuating capabilities and validation with assured solutions (i.e. Kalman filters)

STRUCTURE OF THE DATA USED FOR THE iFD TRAINING

Actuator/ Sensor Set Number	Actuator/ Sensor Status	Training data										Estimated sensor/actuators signals									
		y_1	y_2	y_3	$\cdots$	y_{n_y}	u_1	u_2	u_3	$\cdots$	u_{n_u}	$\hat{y}_1$	$\hat{y}_2$	$\hat{y}_3$	$\cdots$	$\hat{y}_{n_{\hat{y}}}$	$\hat{u}_1$	$\hat{u}_2$	$\hat{u}_3$	$\cdots$	$\hat{u}_{n_{\hat{u}}}$
1	Healthy sets:	$D^1_{y_1^1}$	$D^1_{y_2^1}$	$D^1_{y_3^1}$	$\cdots$	$D^1_{y_{n_y}^1}$	$D^1_{u_1^1}$	$D^1_{u_2^1}$	$D^1_{u_3^1}$	$\cdots$	$D^1_{u_{n_u}^1}$	$D^1_{\hat{y}_1^1}$	$D^1_{\hat{y}_2^1}$	$D^1_{\hat{y}_3^1}$	$\cdots$	$D^1_{\hat{y}_{n_{\hat{y}}}^1}$	$D^1_{\hat{u}_1^1}$	$D^1_{\hat{u}_2^1}$	$D^1_{\hat{u}_3^1}$	$\cdots$	$D^1_{\hat{u}_{n_{\hat{u}}}^1}$
	$\mathcal{Y} = y_1, y_2,\dots,y_{n_y}$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
	$\mathcal{U} = u_1, u_2,\dots,u_{n_u}$	$D^1_{y_1^k}$	$D^1_{y_2^k}$	$D^1_{y_3^k}$	$\cdots$	$D^1_{y_{n_y}^k}$	$D^1_{u_1^k}$	$D^1_{u_2^k}$	$D^1_{u_3^k}$	$\cdots$	$D^1_{u_{n_u}^k}$	$D^1_{y_1^k}$	$D^1_{\hat{y}_2^k}$	$D^1_{\hat{y}_3^k}$	$\cdots$	$D^1_{\hat{y}_{n_{\hat{y}}}^k}$	$D^1_{\hat{u}_1^k}$	$D^1_{\hat{u}_2^k}$	$D^1_{\hat{u}_3^k}$	$\cdots$	$D^1_{\hat{u}_{n_{\hat{u}}}^k}$
2	Faulty set:	$c^2_{y_1^1}$	$D^2_{y_2^1}$	$D^2_{y_3^1}$	$\cdots$	$D^2_{y_{n_y}^1}$	$D^2_{u_1^1}$	$D^2_{u_2^1}$	$D^2_{u_3^1}$	$\cdots$	$D^2_{u_{n_u}^1}$	$c^2_{\hat{y}_1^1}$	$D^2_{\hat{y}_2^1}$	$D^2_{\hat{y}_3^1}$	$\cdots$	$D^2_{\hat{y}_{n_{\hat{y}}}^1}$	$D^2_{\hat{u}_1^1}$	$D^2_{\hat{u}_2^1}$	$D^2_{\hat{u}_3^1}$	$\cdots$	$D^2_{\hat{u}_{n_{\hat{u}}}^1}$
	y_1	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
		$c^2_{y_1^k}$	$D^2_{y_2^k}$	$D^2_{y_3^k}$	$\cdots$	$D^2_{y_{n_y}^k}$	$D^2_{u_1^k}$	$D^2_{u_2^k}$	$D^2_{u_3^k}$	$\cdots$	$D^2_{u_{n_u}^k}$	$c^2_{\hat{y}_1^k}$	$D^2_{\hat{y}_2^k}$	$D^2_{\hat{y}_3^k}$	$\cdots$	$D^2_{\hat{y}_{n_{\hat{y}}}^k}$	$D^2_{\hat{u}_1^k}$	$D^2_{\hat{u}_2^k}$	$D^2_{\hat{u}_3^k}$	$\cdots$	$D^2_{\hat{u}_{n_{\hat{u}}}^k}$
3	Faulty set:	$c^3_{y_1^1}$	$c^3_{y_2^1}$	$D^3_{y_3^1}$	$\cdots$	$D^3_{y_{n_y}^1}$	$D^3_{u_1^1}$	$D^3_{u_2^1}$	$D^3_{u_3^1}$	$\cdots$	$D^3_{u_{n_u}^1}$	$c^3_{\hat{y}_1^1}$	$c^3_{\hat{y}_2^1}$	$D^3_{\hat{y}_3^1}$	$\cdots$	$D^3_{\hat{y}_{n_{\hat{y}}}^1}$	$D^3_{\hat{u}_1^1}$	$D^3_{\hat{u}_2^1}$	$D^3_{\hat{u}_3^1}$	$\cdots$	$D^3_{\hat{u}_{n_{\hat{u}}}^1}$
	y_1, y_2	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
		$c^3_{y_1^k}$	$c^3_{y_2^k}$	$D^3_{y_3^k}$	$\cdots$	$D^3_{y_{n_y}^k}$	$D^3_{u_1^k}$	$D^3_{u_2^k}$	$D^3_{u_3^k}$	$\cdots$	$D^3_{u_{n_u}^k}$	$c^3_{\hat{y}_1^k}$	$c^3_{\hat{y}_2^k}$	$D^3_{\hat{y}_3^k}$	$\cdots$	$D^3_{\hat{y}_{n_{\hat{y}}}^k}$	$D^3_{\hat{u}_1^k}$	$D^3_{\hat{u}_2^k}$	$D^3_{\hat{u}_3^k}$	$\cdots$	$D^3_{\hat{u}_{n_{\hat{u}}}^k}$
4	Faulty set:	$c^4_{y_1^1}$	$c^4_{y_2^1}$	$D^4_{y_3^1}$	$\cdots$	$D^4_{y_{n_y}^1}$	$c^4_{u_1^1}$	$D^4_{u_2^1}$	$D^4_{u_3^1}$	$\cdots$	$D^4_{u_{n_u}^1}$	$c^4_{\hat{y}_1^1}$	$c^4_{\hat{y}_2^1}$	$D^4_{\hat{y}_3^1}$	$\cdots$	$D^4_{\hat{y}_{n_{\hat{y}}}^1}$	$c^4_{\hat{u}_1^1}$	$D^4_{\hat{u}_2^1}$	$D^4_{\hat{u}_3^1}$	$\cdots$	$D^4_{\hat{u}_{n_{\hat{u}}}^1}$
	y_1, y_2, u_1	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
		$c^4_{y_1^k}$	$c^4_{y_2^k}$	$D^4_{y_3^k}$	$\cdots$	$D^4_{y_{n_y}^k}$	$c^4_{u_1^k}$	$D^4_{u_2^k}$	$D^4_{u_3^k}$	$\cdots$	$D^4_{u_{n_u}^k}$	$c^4_{\hat{y}_1^k}$	$c^4_{\hat{y}_2^k}$	$D^4_{\hat{y}_3^k}$	$\cdots$	$D^4_{\hat{y}_{n_{\hat{y}}}^k}$	$c^4_{\hat{u}_1^k}$	$D^4_{\hat{u}_2^k}$	$D^4_{\hat{u}_3^k}$	$\cdots$	$D^4_{\hat{u}_{n_{\hat{u}}}^k}$
5	Faulty set:	$c^5_{y_1^1}$	$D^5_{y_2^1}$	$D^5_{y_3^1}$	$\cdots$	$D^5_{y_{n_y}^1}$	$c^5_{u_1^1}$	$c^5_{u_2^1}$	$D^5_{u_3^1}$	$\cdots$	$D^5_{u_{n_u}^1}$	$c^5_{\hat{y}_1^1}$	$D^5_{\hat{y}_2^1}$	$D^5_{\hat{y}_3^1}$	$\cdots$	$D^5_{\hat{y}_{n_{\hat{y}}}^1}$	$c^5_{\hat{u}_1^1}$	$c^5_{\hat{u}_2^1}$	$D^5_{\hat{u}_3^1}$	$\cdots$	$D^5_{\hat{u}_{n_{\hat{u}}}^1}$
	y_1, u_1, u_2	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
		$c^5_{y_1^k}$	$D^5_{y_2^k}$	$D^5_{y_3^k}$	$\cdots$	$D^5_{y_{n_y}^k}$	$c^5_{u_1^k}$	$c^5_{u_2^k}$	$D^5_{u_3^k}$	$\cdots$	$D^5_{u_{n_u}^k}$	$c^5_{\hat{y}_1^k}$	$D^5_{\hat{y}_2^k}$	$D^5_{\hat{y}_3^k}$	$\cdots$	$D^5_{\hat{y}_{n_{\hat{y}}}^k}$	$c^5_{\hat{u}_1^k}$	$c^5_{\hat{u}_2^k}$	$D^5_{\hat{u}_3^k}$	$\cdots$	$D^5_{\hat{u}_{n_{\hat{u}}}^k}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
n_{yu}	Faulty sets:	$c^{n_{yu}}_{y_1^1}$	$c^{n_{yu}}_{y_2^1}$	$\cdots$	$c^{n_{yu}}_{y_{n_y-1}^1}$	$D^{n_{yu}}_{y_{n_y}^1}$	$c^{n_{yu}}_{u_1^1}$	$c^{n_{yu}}_{u_2^1}$	$\cdots$	$c^{n_{yu}}_{u_{n_u-1}^1}$	$D^{n_{yu}}_{u_{n_u}^1}$	$c^{n_{yu}}_{\hat{y}_1^1}$	$c^{n_{yu}}_{\hat{y}_2^1}$	$\cdots$	$c^{n_{yu}}_{\hat{y}_{n_y-1}^1}$	$D^{n_{yu}}_{\hat{y}_{n_{\hat{y}}}^1}$	$c^{n_{yu}}_{\hat{u}_1^1}$	$c^{n_{yu}}_{\hat{u}_2^1}$	$\cdots$	$c^{n_{yu}}_{\hat{u}_{n_u-1}^1}$	$D^{n_{yu}}_{\hat{u}_{n_{\hat{u}}}^1}$
	$y_1,\dots,y_{n_y-1}$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
	$u_1,\dots,u_{n_u-1}$	$c^{n_{yu}}_{y_1^k}$	$c^{n_{yu}}_{y_2^k}$	$\cdots$	$c^{n_{yu}}_{y_{n_y-1}^k}$	$D^{n_{yu}}_{y_{n_y}^k}$	$c^{n_{yu}}_{u_1^k}$	$c^{n_{yu}}_{u_2^k}$	$\cdots$	$c^{n_{yu}}_{u_{n_u-1}^k}$	$D^{n_{yu}}_{y_{n_u}^k}$	$c^{n_{yu}}_{\hat{y}_1^k}$	$c^{n_{yu}}_{\hat{y}_2^k}$	$\cdots$	$c^{n_{yu}}_{\hat{y}_{n_y-1}^k}$	$D^{n_{yu}}_{\hat{y}_{n_{\hat{y}}}^k}$	$c^{n_{yu}}_{\hat{u}_1^k}$	$c^{n_{yu}}_{\hat{u}_2^k}$	$\cdots$	$c^{n_{yu}}_{\hat{u}_{n_u-1}^k}$	$D^{n_{yu}}_{\hat{y}_{n_{\hat{u}}}^k}$

k is the total number of samples at each actuator/sensor set.

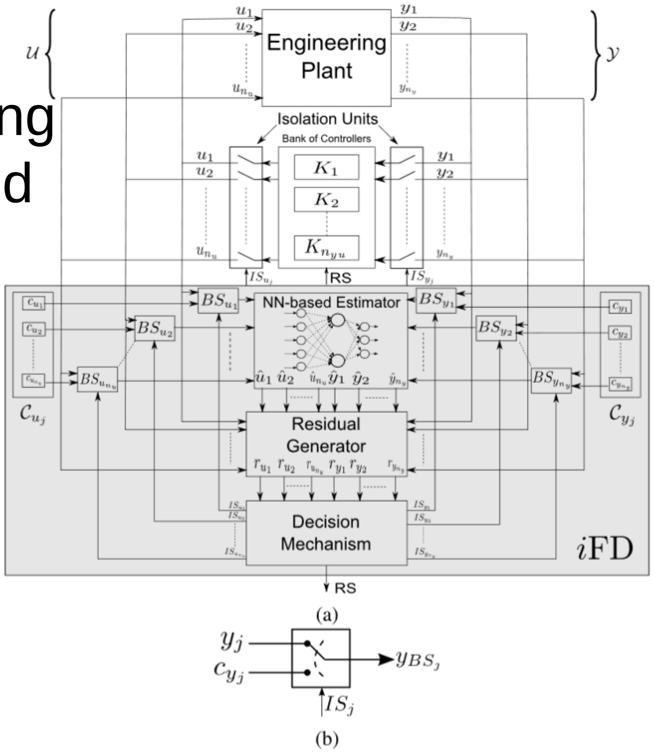


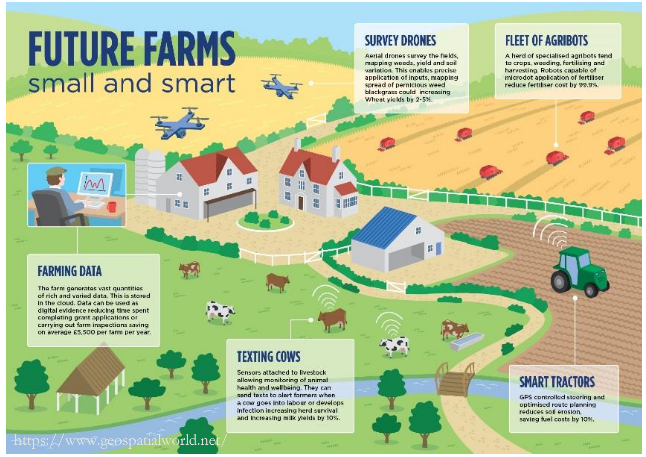
Fig. 2. (a) General diagram of actuator/sensor FDI with the proposed iFD. (b) BS operation.

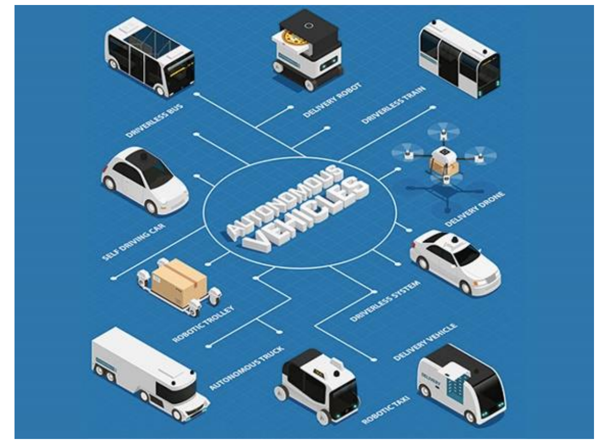
AI-based actuator/sensor fault detection with low computational cost for industrial applications https://ieeexplore.ieee.org/document/7111282/ , highlighted in World Industrial Reporter https://worldindustrialreporter.com/... enabling Simpler AI-Based Industrial Fault Detection Systems

Towards Autonomy and role of infrastructure

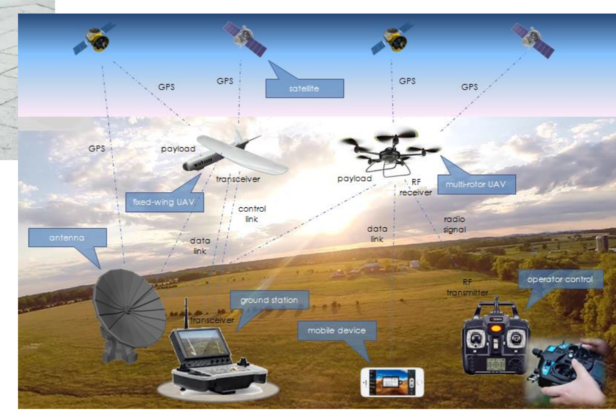
12

Autonomy and its complexity





IEEE spectrum



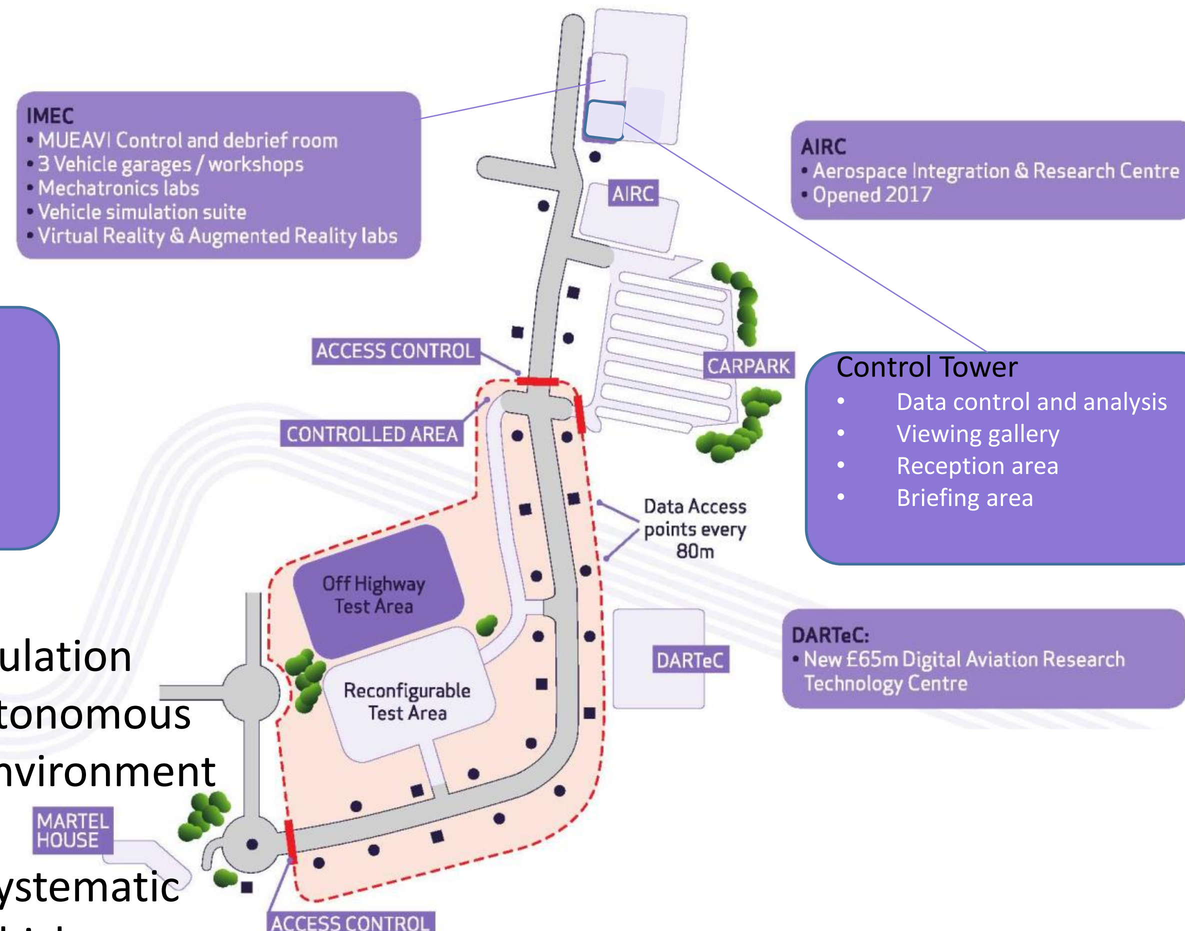
Infrastructure for Autonomous Vehicle validation

- Most infrastructures are focused either:
  - on real driving test at physical infrastructure
  - or software simulation in virtualized infrastructure
- Neither the real driving test can cover all possible scenarios of autonomous driving and human factors,
- nor the virtualized software simulation can generate a feasible model for practical on/off-road driving.
- Furthermore, future autonomous transport in smart cities requires comprehensive validation.

Cranfield's Multi-User Environment for Autonomous Vehicle Innovation(MUEVI)

OVERVIEW: MUEAVI

Sensors
- Wi-fi (infrastructure)
- In vehicle PSU
- LIDAR
- Radar
- Visual data capture



Control Tower
- Data control and analysis
- Viewing gallery
- Reception area
- Briefing area

An integrated testing and simulation infrastructure to meet the autonomous transport in complex traffic environment

has been built targeting the systematic validation for autonomous vehicles

MUEAVI Sensors

12 Plextek Radar:
- 33° FOV
- Detect human at 125 m
- 77 GHz

22 Overview Hydra camera:
- 1920x1080p resolution @ 25 fps
- Colour or B/W
- Pan and tilt movement: 0.05 degree to 180 degrees/sec on both axes
- 4 Dual camera with IR

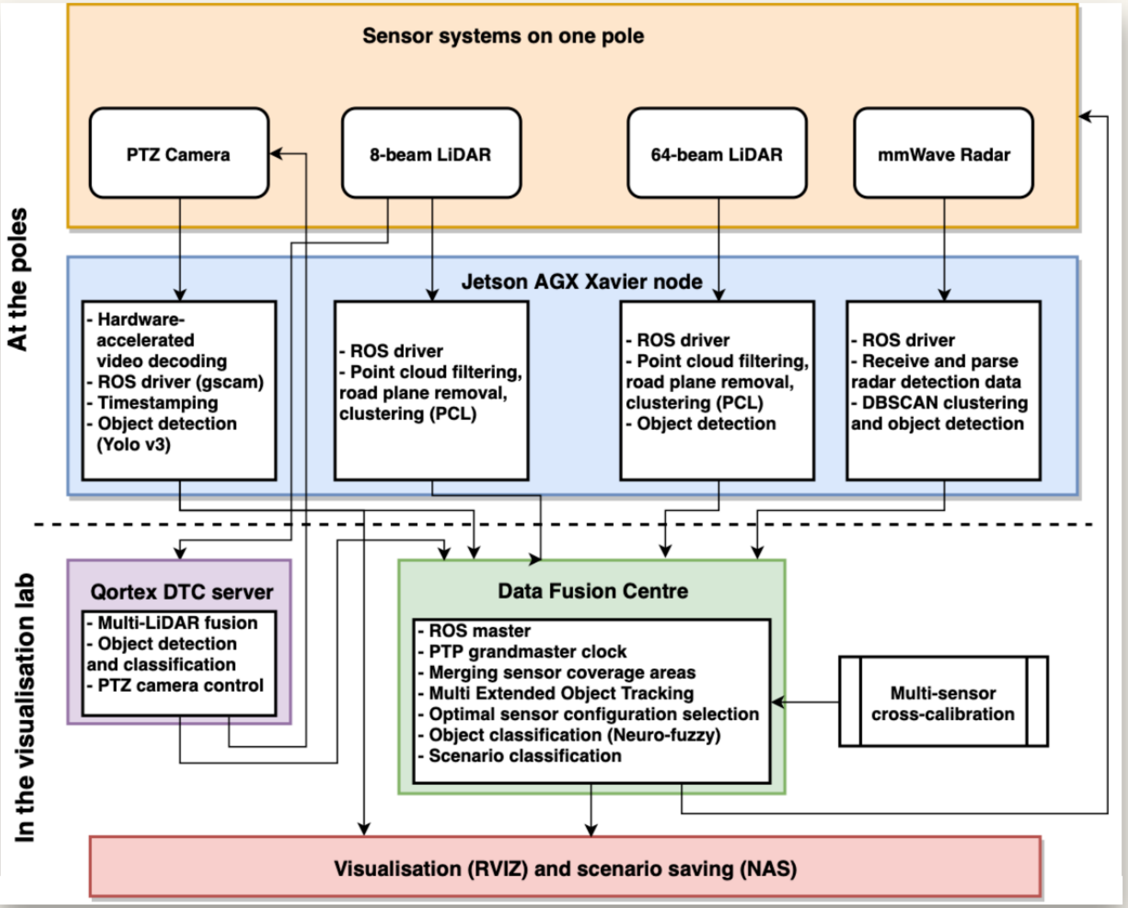
17 Quanergy M8 Lidar:
- 360° horizontal FOV and 20° FOV
- 8 layers, 5-20 Hz update frequency
- 1-150 m range

12 Ouster OS-1-64 Lidar:
- 360° horiz. FOV and 32.2° vert. FOV
- 64 layers, 10-20 Hz update frequency
- 0.5-120 m range

MUEAVI Sensors Deployment

System architecture

- The system architecture is split into two major physical sections where the different HW and SW modules operate:
  - poles
  - visualisation lab



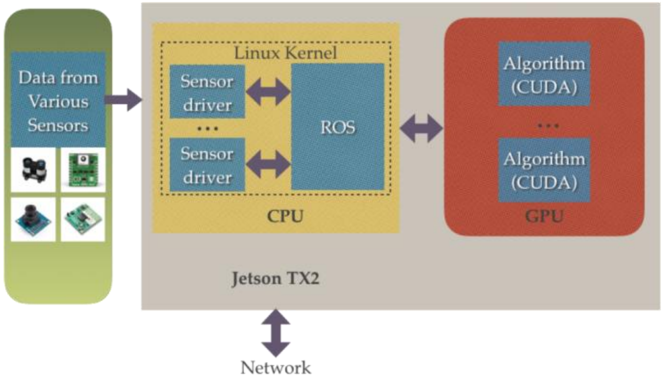
System architecture

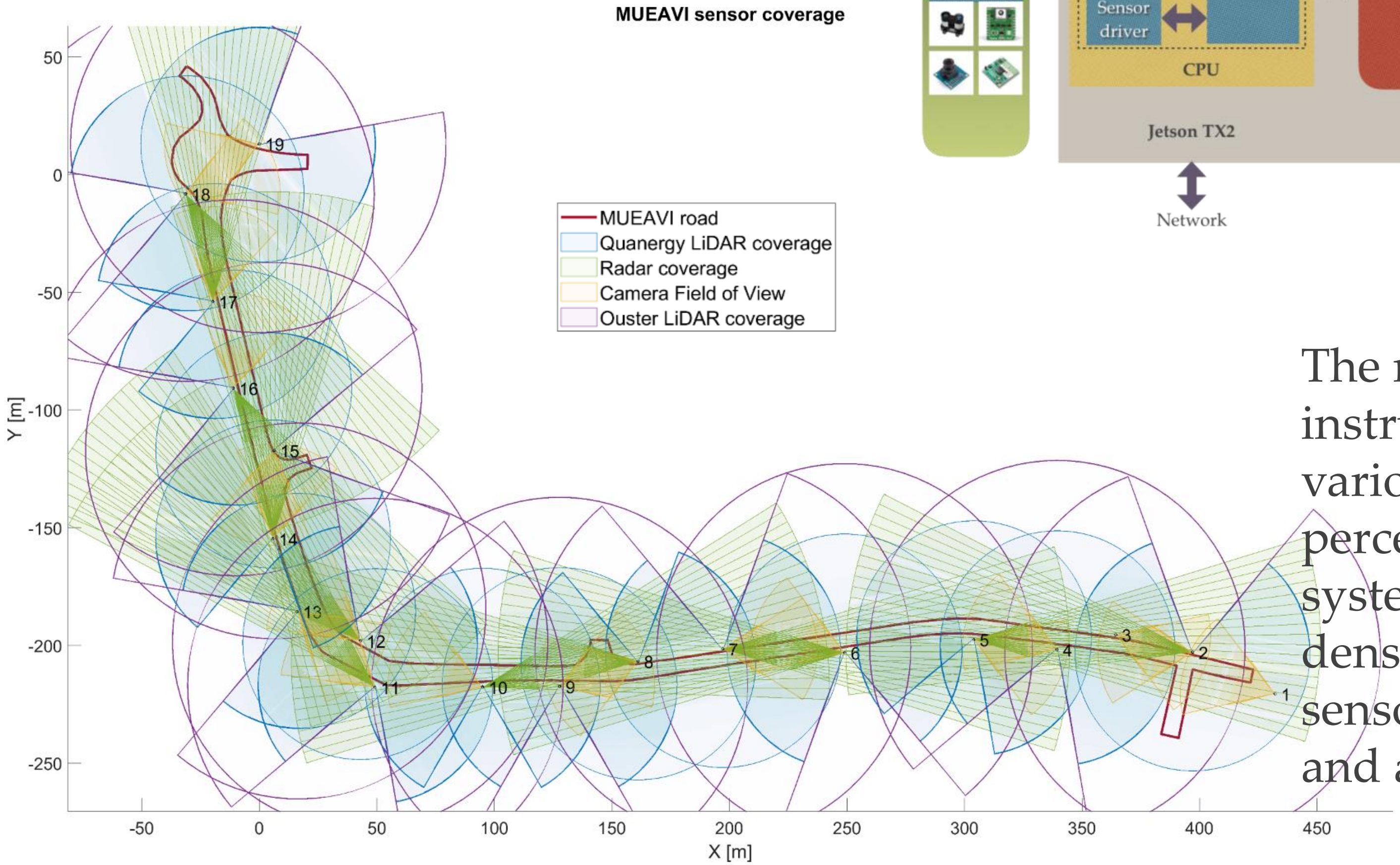
Data from various sensors entering a three stage architecture:

- **Preprocessing stage** includes packetizing and timestamping the data and setting up the infrastructure for data networking and transmission.
- **Main processing stage** where, object detection, trajectory tracking and data classification takes place.
- **Manipulation stage** performs data validation and completeness and forms data ready for visual representation, analysis and decision making.

Data exiting the three stage architecture are fed to a Model verification and validation stage, where a combination of dynamic system tests and formal verification for proving the correctness of intended algorithms is done.

MUEAVI sensor coverage



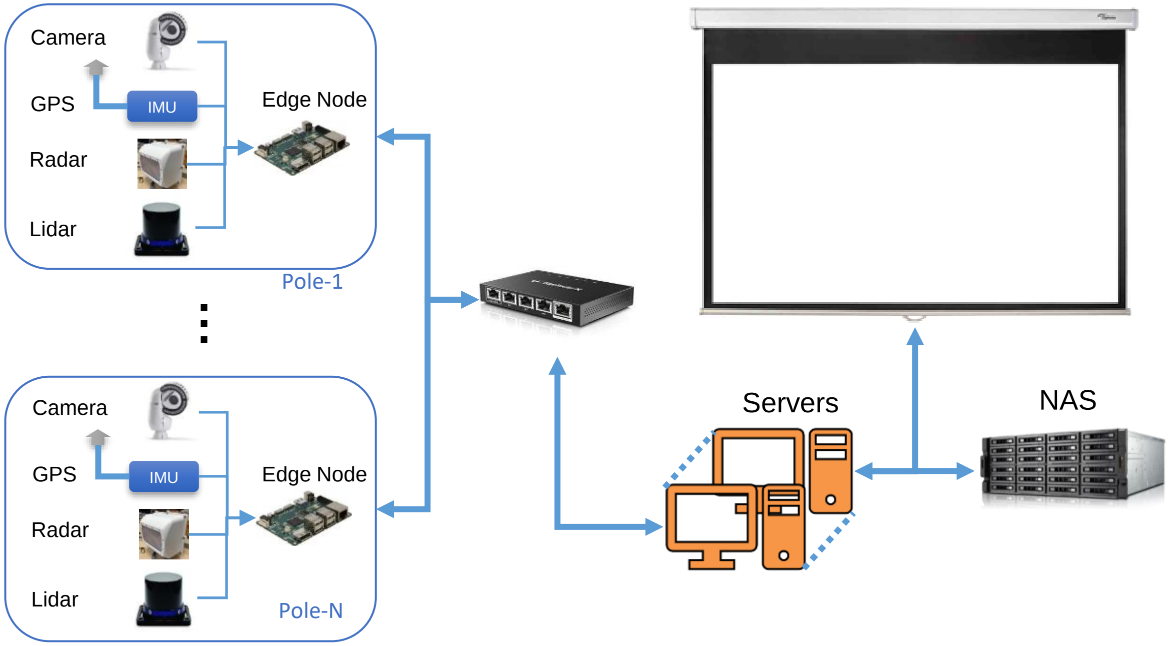


The road is richly instrumented with various types of perceptive sensor systems providing a dense and overlapping sensor coverage area on and around the road.

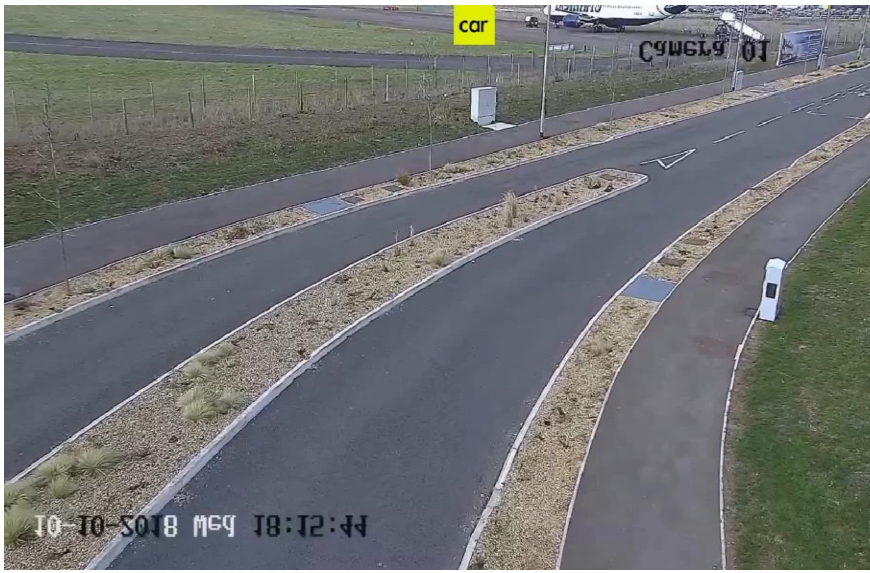
MUEAVI Infrastructure

Preprocessed data from the computing nodes are received in the MUEAVI Visualization Lab, where the centralized data fusion, adaptive, detection-based sensor combination selection, raw and processed data visualization and storage take place.

- Heterogeneous Sensor Network
- Embedded edge accelerator
- High performance computer-vision server
- High capacity streaming data storage server
- Multimedia projecting system

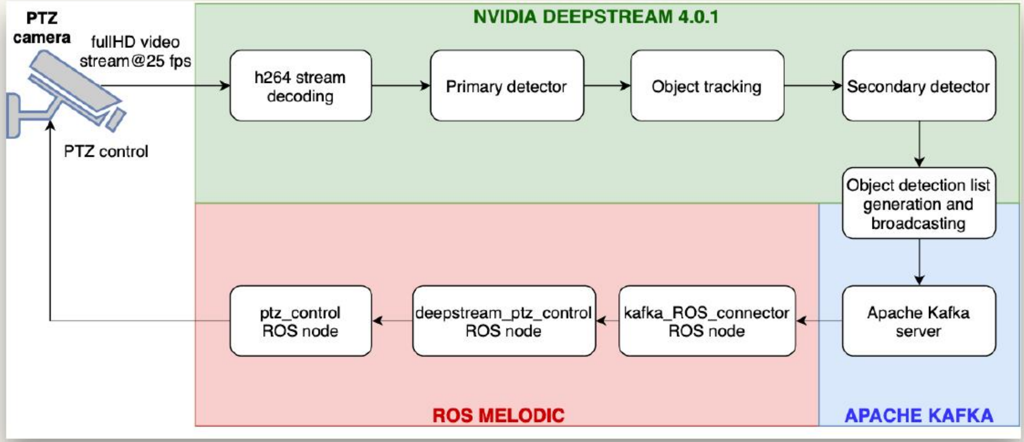


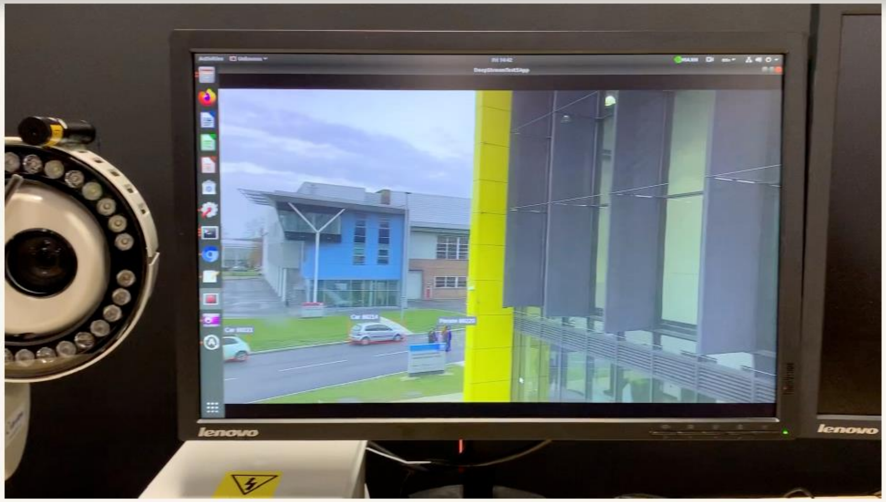
MUEAVI Sensor Demonstration - Camera



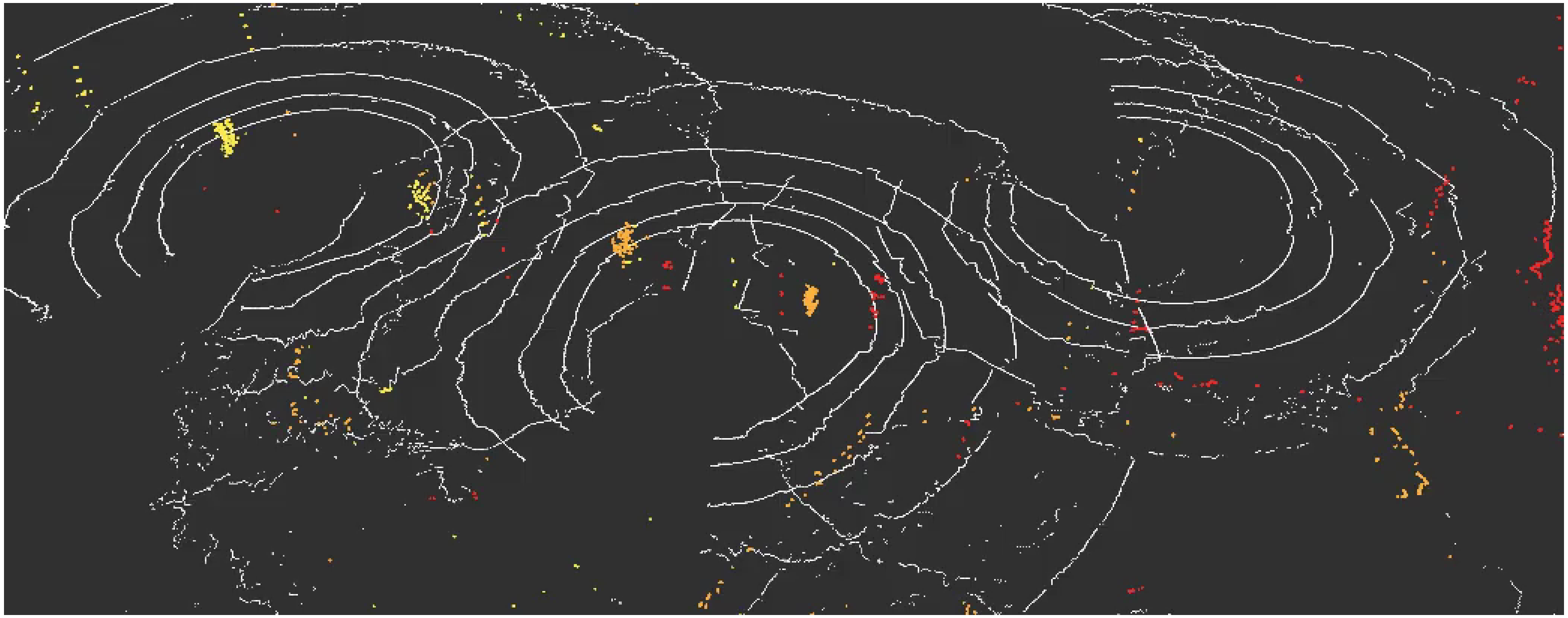
Camera tracking scenario (control engineering element within)

- The camera tracking receives a video stream and outputs PTZ commands to the camera based on the detected objects.
- A (closed) control loop is formed by a pipeline structure comprising of three main stages:
  - NVIDIA Deepstream 4.0.1 engine,
  - Kafka apache server,
  - ROS nodes.

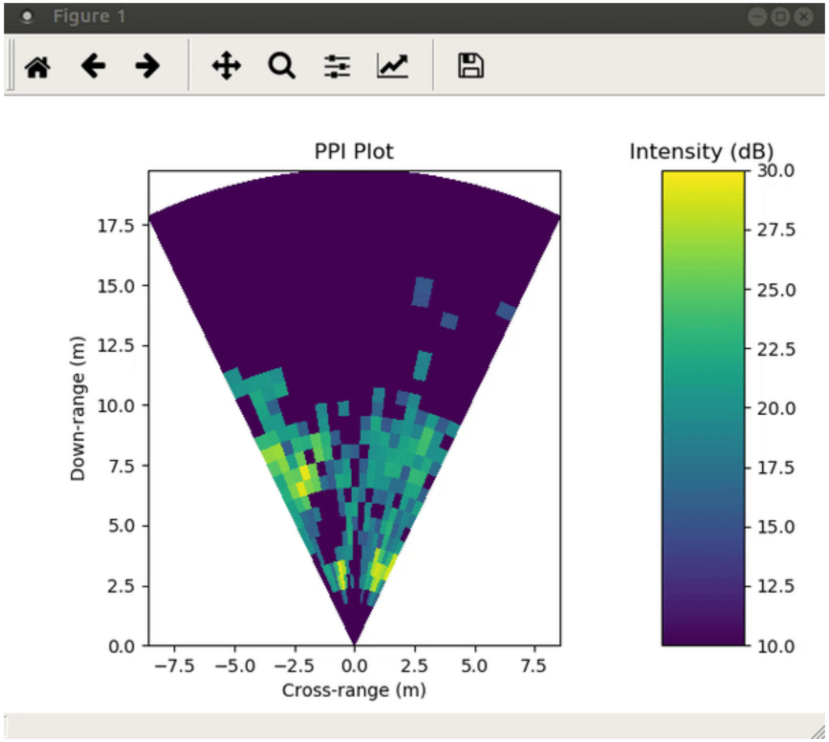




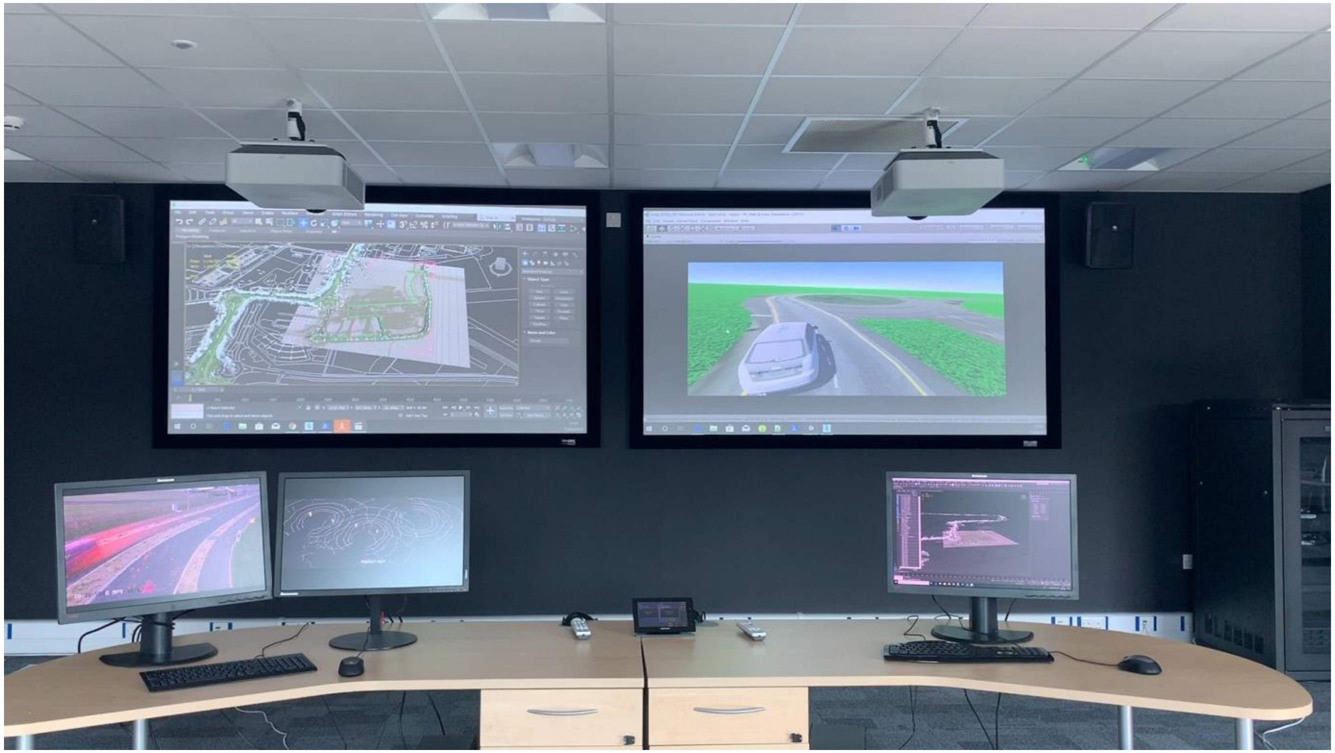
MUEAVI Sensor Demonstration - Lidar



MUEAVI Sensor Demonstration - Radar



MUEAVI Visualization Lab Demonstration



Enabler Verification, Validation, Certification of Autonomous Systems

Dynamic Decision Making Modelling

Formal methods

- Solid mathematical techniques
- Quantifiable answers to questions related with reliability of systems
- 3 parts: Modelling/Specification/Verification

Formal modelling techniques

: Message Sequence Charts, Finite State Automata, Petri Nets, and Kripke models

Kripke model

- Can represent real world uncertainty formally
- Is a triple, M=(W, R, L)

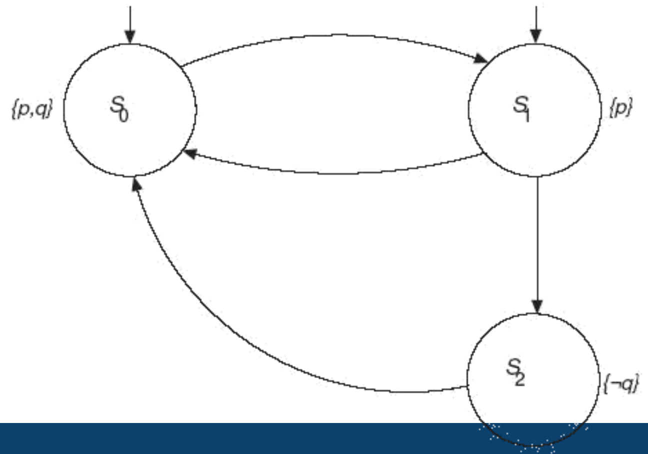
  W: possible worlds

  R: accessibility relation

  $R \subseteq W \times W$

  L: labelling function

  $L: W \rightarrow P(Atoms)$



Verify multi-vehicle Operations

Model Checking

- Automated procedure for verifying finite state concurrent systems
- Exhaustive (or symbolic) search of the system's state-space
- Determines the truth value of the specification in question
- Produce an error trace in case of *no* answer

Model checker	Description
Simple Promela Interpreter (SPIN)	Developed for verification of protocols and software check LTL properties
Symbolic Model Verifier (SMV)	Implement the OBDD (Ordered Binary Decision Diagram)-based symbolic model checking techniques for CTL
Model Checker for Multi-Agent Systems (MCMAS)	Developed to verify the multi-agent systems Specify the logic including not only temporal operators but also epistemic, correct behavioural, and strategic operators $IS = \langle (L_i, Act_i, P_i, t_i)_{i \in \{1,\cdots A\}}, (L_E, Act_E, P_E, t_E), I, V \rangle$

Department of Informatics & Systems Engineering – Centre for Autonomous Systems

Extracting properties as LTL formulae

Reachability analysis, can be written in LTL as follows:

$$\Box \left[\bigwedge_{i=1}^{N} \overset{a}{\underset{l}{X}}_i \, \mathcal{U} \, (x_i, y_i) \in \left([x_{goal}, x_{end}], [y_{goal}, y_{end}] \right) \right]$$

The formula can be read as:

"all vehicle continue moving until they reach the area designated as the goal area."

Safety properties are represented in LTL as follows:

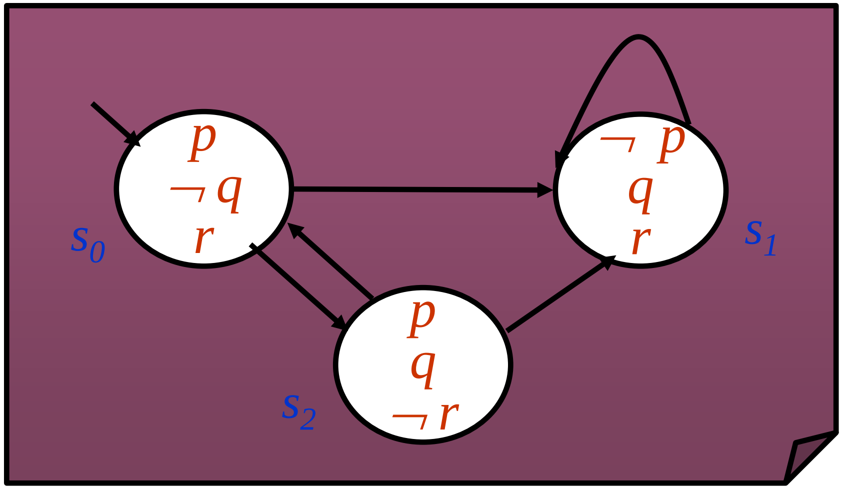
$$\Box \neg \left[\bigwedge_{\substack{i,j=1 \\ i \neq j}}^{N} \sqrt{(x_{i2} - x_{j2})^2 + (y_{i2} - y_{j2})^2} < L_D \right]$$

The formula can be read as:

"no two vehicles can ever come closer than a pre-specified separation boundary."

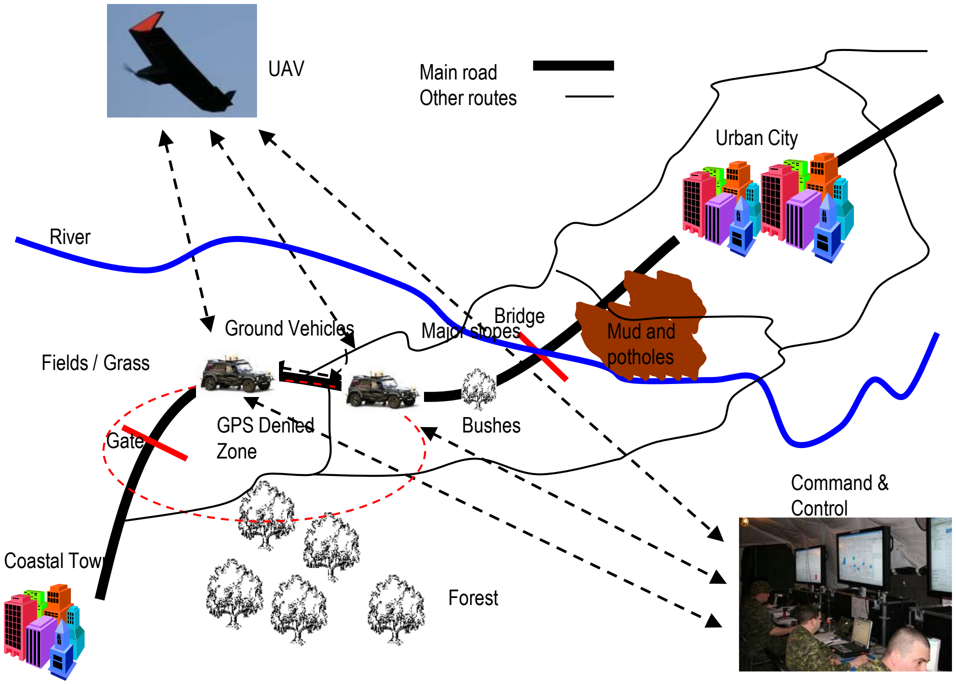
J. Choi and A. Tsourdos "Verification of Decision Making Behaviour for Heterogeneous Multi-Agent System", AIAA Guidance, Control and Navigation Conference 2011

Supporting Certification of Autonomous Systems



Key questions remain:

- Representing uncertainty and goal functions in decision-making
- Optimising architecture for scalability and robustness
- Decentralised / Centralised decision making



Department of Informatics & Systems Engineering – Centre for Autonomous Systems

On control engineering, reliability and smart infrastructure enabling safer autonomous vehicle operation

…for listening!

Professor Argyrios Zolotas
Centre for Autonomous and
Cyber-Physical Systems