Secure Operations of Trustworthy Autonomous Systems

Cranfield University, Lancaster University

Investigators: Weisi Guo, Gokhan Inalhan, Plamen Angelov, Antonios Tsourdos, Vasileios Giotas, David Hutchison
Research Fellows: Zhuangkun Wei, Oscar Villarreal, Burak Yuksel, Pierre Chiolis

Autonomous systems face numerous challenges in their operation, due to the uncertain and dynamic multi-layer attack surfaces

TAS-RS2 aims to solve following challenges:
- Modelling & addressing potential attacks in discrete mission, control and communication layers
- Study & address hybrid cascaded cross-layer threats in the dynamic AS space

RS-2A: Exposure to cyber-physical attacks by characterizing the attack surfaces, i.e., entry points and likelihoods across the mission surface in a technology & mission-invariant manner.

RS-2B: Provide quantifiable safety and feedback to the mission surface when the limits of secure controllability are compromised within a time horizon under current policies and adversarial situations.

RS-2C: Provide secure communications across the different layers in the informatics plane from detection of signals to networking.

Secure and real-time communications serve as the fundamentals for Autonomous Systems to achieve reliable control and mission delivery.

Key Challenges for Trustworthy Learning-based Mission Control under Security Constraints

- Real-Time Non-Convex Trajectory Optimisation for Path Planning under Uncertainty, Power Consumption, Dynamic Obstacle Avoidance and Communication Security Constraints
- Adaptive and Fault-Tolerant Learning-based Design for Mission Control to improve reliability of safety critical systems
- Supervisory Control for Anomaly Detection and Isolation Systems
- Intelligent Resource Allocation for Multi-UAV Design under Security Threats
- Reliable Self-Assessment under Learning-based Scenarios

Secure Physical Layer Security: using RECIPRO radio environment

Innovation: exploit unique, dynamic, reciproc CSIs between entities due to radio propagation nature

Advantages: low latency & complexity, using only physical channel properties:
- Randomness of wireless channel
- Superiority of legitimate over eavesdropper channels

Steps:
- Generate randomness using intelligent reflecting surface (IRS)
- Channel Probing between legitimate users
- Generate cipher keys using recipro CSIs

Adaptive Security Strategies:
- Deep Reinforcement Learning Based Adaptive Controls
- Continual Assurance
  - Detect and avoid
  - Learning enabled context

Interpretability => Explainable and Trustworthy AI
- Physics Informed Deep Learning
- Ability to identify system behaviour
- Explainable and Adaptive operation
- Anomaly detection/classification

Mission Control for Secure Trustworthy Autonomous Systems requires flexible but reliable real-time optimal decision making and monitoring to handle a wide range of attacks

Critical Tasks:
- Handling Communication Errors and Security Constraints
- Assessing Control Faults and Performance Limitations
- Handling Environmental Limitations (Uncertainty/Dynamic Obstacles/No-Fly zones)
- Avoiding and Handling Electronic/Electro-magnetically induced attacks
- Achieving Deterministic/Real-Time Performance for the Optimal Decision Making
- Handling and Detecting Security Threats under Learning-based Scenarios

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