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:

- Modeling & 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 linkages 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.

**RS-2B: Securing the Control Surface**

Autonomous Systems rely on the ability to conduct run time adaptations of control decisions over attacks or “perceived” attacks:

- Adversaries
- Environment uncertainties
- Degraded performance

**How to do this in a “trustworthy” fashion?**

- Safe
- Secure
- Reliable

**Attack Definitions**

- Sensing and Communication Errors
- Loss of an actuator
- Environmental conditions
- Electronic attacks
- Electromagnetic deception
- Injecting false pattern into data

**RS2-AS State Space**

- Lindeburg Region
- Uncertainty Envelope
- Design-Type Autonomy
- Network Layer
- Cross-Layer Security
- Delay Sensitive & Secure Networking in Communication Surface

**Dynamical V&V**

- Explainability of Flight Control Systems (FCS)
- Explainable Flight Control Systems

**Adaptive Security Strategies**

- Deep Reinforcement Learning Based Adaptive Controls
- Learn adaptation strategy through observation between reference model and the reality

**B. Explainability of the AI-Based FCS**

**Interpretability => Explainable and Trustworthy AI**

- Physics Informed Deep Learning
- Ability to identify system behaviour
- Generalization capability
- Anomaly detection/classification

**C. Adaptive Security Strategies**

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