



TAS Autonomous Systems Security Node

First External Stakeholders Group (ESG) Workshop,

Monday, 29th March 2021

TAS-S, as the security node in the EPSRC's *Trustworthy Autonomous Systems* (TAS) programme, held its first External Stakeholders Group (ESG) workshop on 29th March 2021. The TAS-S stakeholders, as an international representation of prominent autonomous systems leaders, numbered about 50 participants from 30 academic, governmental and industrial organizations. The full-day event provided the TAS-S investigators and its external stakeholders with a critical opportunity to network, albeit virtually, as the collective TAS-S team!

The morning session presented the objectives and planned activities for the three inter-linked research strands of the TAS-S project. Each of these strands addresses a diversity of basic-research and practitioner-relevant themes of AS security, that are collaboratively conducted by the researchers across Lancaster and Cranfield Universities. The research strands (RS) are:

- **RS1: Securing the AS “Usage” Environment: Establish the fundamental AS “usage” framework for providing and assessing multi-layered, multi-dimensional adaptive AS security in dynamic mixed mode environments.**
 - Theme A: Dynamic and Compositional AS Security
 - Theme B: Explainable & Verifiable Decision Making
- **RS2: Securing the AS “Operations” Environment: Ascertain exposure (and their consequent mitigation) of AS “operations” to cyber-physical attacks by characterizing the attack surfaces (i.e., entry points and likelihoods) across the mission, control and information surfaces in a technology and mission-invariant manner.**
 - Theme A: Security in the Mission and Operational Surface
 - Theme B: Securing the Control Surface
 - Theme C: Securing the Cross-Layer Networking Surface
- **RS3: Securing the AS “Users” Environment: Develop novel socio-technical, legal and regulatory approaches to ascertain and mitigate AS threats to provide a secure AS “user” environment.**
 - Theme A: Behaviour Adaptation as a Basis of Security by Design
 - Theme B: Organizational Socio-Technical Mitigation
 - Theme C: Ethics and governance of AS security

The afternoon session provided the stakeholders an opportunity to present their activity profiles, challenges and TAS-S expectations. The presenters included Airbus, Academia Sinica-Taiwan, AIT-Austria, Arthur's Legal-Netherlands, BAE Systems, Edge Case Research/Carnegie Mellon University-USA, HM Coastguard, Raytheon, RISE-Sweden, Thales, TTTech-Austria, Leonardo Helicopters, Boeing Europe, Catapult, GE Aviation, Lockheed Martin and Highways England.

The subsequent breakout sessions discussed the ethical, legal and social issues involved over the use of autonomous systems. Questions around the socio-technical interplay involved in designing and testing the systems, the regulatory and liability implications for the AS mission decisions and related societal considerations over the AS usage were identified as some of the key considerations warranting focussed research. Although these issues are obviously far too complicated to be resolved in a single session, they raised an excellent set of research issues and highlighted the diversity and complexity of the challenges ahead. A number of these socio-technical aspects, including prioritizing key research needs, were subsequently discussed in the panel on "Priorities for AS Security – The Road Ahead"

The workshop closed with the TAS-S Advisory Group's reflections on the workshop discussions, and suggested issues for future deliberation.

