Invitation to NIAG to Participate in IST-176: "**Federated Interoperability of Military C2 and IoT Systems**"

Introduction

Under the auspices of the NATO Science and Technology Organisation (STO), Nations, together with the NATO Communication and Information Agency, are conducting a three-year study examining the Federated Interoperability of Military C2 and IoT Systems. This builds on the work conducted earlier under IST-147 – Military Applications of IoT. The details of the scope of the current activity are defined in the attached approved Technical Activity Proposal (TAP).

The study commenced in May 2019. At the kick-off meeting it was realised that it could be of mutual benefit if a mechanism was found to include industry in the study as this was found to be very valuable in the IST-147 work. In particular, we believe that the benefits of such a cooperation could be:

- It would allow NATO to keep abreast of developments in industry in this fast moving area;
- It would allow NATO to potentially shape the industrial offerings as they develop to ensure they meet our military needs;
- It would allow NATO to influence industry standardisation activities to ensure that they take cognisance of military use cases;
- It would allow industry to understand the military context and use cases, and any specific needs of this domain; and
- It would allow industry to showcase their emerging products to not only the study team, but also to a wider NATO and national military audience as we have planned several demonstrations into the programme of work.

In order to engage industry in the study, the decision has been taken to do this through the NATO Industrial Advisory Group (NIAG). By working with the NIAG, a recognised NATO body, the following advantages have been identified compared to other potential mechanisms:

- The right expertise can be engaged, but without bringing in industrial bias; and
- A simple proven mechanism can be used to engage industry.

In order for the first advantage to be realised, and to be seen to be realised, it is necessary that a number of industries participate so that no one company can dominate the advice provided.

Current IST-176 team members include: POL (Lead), DEU, ESP, ITA, NLD, NOR, POL, USA, NCI Agency, FIN and CHE.

Scope

The objectives of the study, identified in the attached TAP, are:

1. To examine existing IoT standards, as well as existing STANAGs, architectures, and best practices to better understand how to integrate commercial and civilian IoT technologies and capabilities into Military C2 and Logistics systems, and in particular NATO's Federated Mission Networking (FMN) architecture.
2. To further define the use-cases/scenarios, interfaces, and practical usability of IoT based solutions for HADR operations in future Smart City environments and to assist in realizing Collaborative Resilience.
3. To explore the challenges of discovery of commercial IoT capabilities and services, given the relative lack of standardization.

4. To identify security challenges and develop mitigation strategies for those challenges when interfacing military C2 and civilian IoT infrastructures and when performing fusion with or otherwise relying on data coming from various sources of information.
5. To experiment and demonstrate, through proof-of-concept trials, the benefits and ability to integrate civilian IoT and military C2 systems, especially in the context of providing Collaborative Resilience.
6. To potentially engage in standardization activities in the civilian space, for example the IEEE Smart Cities initiatives.
7. To organize workshops at conferences to engage with commercial IoT activities.

The study is defining an overall scenario, of significance to NATO, based around a deployed base with both an Airport of Debarkation (APOD), Maritime Port of Debarkation (MPOD), medical facilities, etc. Around this overall scenario the study will explore the benefits, risks, and potential mitigations, using short vignettes. This work is ongoing.

Implementation

Participation in the IST-176 study would be done using a similar model to the way that was used in IST-147, which differs from the 'normal' NIAG approach. For this study, we are seeking a direct partnership with NIAG industries; that is, the participating industries would form part of the study team and participate directly in the programme of work of the study, contributing in areas aligned to their expertise and interest. Under this model industries would pay 100% of their own costs, as does any Nation or NATO body that participates. The industries would participate and contribute to the execution of the study, under the direction of the study leader, including team meetings and demonstrations. Prior to publication of the report or reports, input, recommendations and conclusions would be sought equally from industry as from other study members; however, in cases of disagreement final recommendations would be decided by the study chairman on advice of the national study team members. Anyone contributing to the report or reports would be equally listed as authors, regardless of their affiliation.

Also coordinated through the study, the team intends to organise Special Sessions at conferences, such as the IEEE World Forum on IoT, as a way to disseminate results to a broad community.

Invitation

NIAG is invited to nominate between six and eight suitable companies for participation in the IST-176 study. As a guide, the nominated companies should have the following characteristics:

- Be willing to make a commitment to participate in the study for the duration; that is, until April 2022, making contributions to the successful conclusion;
- Be willing to nominate a lead investigator who will attend the meetings (foreseen as two a year) and monthly, or more frequent, WebEx sessions where progress is reviewed and activities coordinated. The lead investigator will be responsible for coordinating activities internal to the company they represent;
- Be good team members, willing to participate and share information and experience in a constructive way, within the boundaries of commercial disclosure;
- Have a strong interest and expertise in an area related to IoT, such as: sensors, security, communications, big data analysis, actuators, decision making, etc.; and
- Optionally, have an interest and experience in the military domain.