Dependability and Security Imperatives for Intelligent Autonomous Systems

Background: Artificial intelligence (AI) technologies such as machine learning (ML) are rapidly being applied to a variety of unmanned systems. Prominent among these are autonomous automobiles, trucks, busses, robots, and aerial vehicles. The emphasis to date in research and development of such systems has focused on aspects of performance in perception (e.g., object recognition and classification using computer vision, speech recognition, and language understanding) and decision making (e.g., learning based path planning and control). On the other hand, such systems are typically being deployed in critical application domains such as transportation, healthcare and manufacturing. Use of AI, and particularly ML, in assisting the control of and communication between autonomous systems thus raises concerns regarding their dependability and security. One might hope to state and pursue R&D imperatives in this regard without reference to a particular type of system or application domain. However, a fundamental problem in this regard is that attributes of dependability are based on an underlying concept of "failure" (a transition from correct to incorrect service delivery). But characterizing failure of an AI-assisted system (whether or not autonomous) is difficult, since what's meant by correct (desired) or incorrect (undesired) service is elusive. Indeed, the notion of "service" implicitly calls for some knowledge of just who or what is being served. Thus, a statement of dependability imperatives for such systems appears to be necessarily application-dependent. Moreover, the same likely holds for attributes of security. In view of these considerations, the following project is proposed.

The Project: Although several interesting application domains might be considered, one that's currently the most pervasive in the United States, Europe, and Asia is transportation via automated vehicles (AVs). Technologies for the automated control of and communication between AVs are being developed worldwide. Indeed, among automotive technologies, they are reported to be among the most heavily researched. Moreover, AVs are already being deployed. The International Society of Automotive Engineers (SAE Int'l) has defined (Standard J3016, version 062018) six levels of automation for motor vehicles, ranging from level 0 (no automation) to level 5 (fully automated). Technical interests among members of WG 10.4 relate to each of the non-trivial levels (1-5) and, generally, the WG could have a substantial say regarding future dependability/security needs and precautions in this regard. More specifically, per the background cited above, we propose that emphasis be placed on the application of AI to AVs. As for dependability attributes, safety appears to be the most important concern. Accordingly, a failure of an intelligent AV is definable in terms of one of several recognized severity levels. As noted in a recent RAND report https://www.rand.org/pubs/research_reports/RR2662.html), these include contact between the vehicle and its outside environment, a crash resulting in property damage over a certain cost, a crash resulting in injury, in severe injury, and in death. Imperatives relating to other dependability and security attributes will likewise be addressed. This is a project that, via surveys of existing literature and interaction with AV and AI experts, seeks to recommend what needs to be done, what should be avoided, and what shouldn't be done until something else is accomplished. In short, it is aimed at identifying and justifying problems. It is NOT a joint research project that solves those problems.

Work Plan: Given this project is chosen by the Working Group at the Winter 2019 business meeting, the effort might proceed as follows. These are simply suggestions. Flushing out the details is part of what needs to be accomplished.

1) At the Winter 2019 meeting, decide on which aspects of dependable and secure intelligent AVs we should address. For example:

   a. Standards – Many already exist (some conflicting), both international standards and ones specific to countries in the Americas, Europe, and Asia.
   b. On-board vehicle technology -- There is a multitude of existing and proposed systems, where those for level 3-5 application are particularly interesting with respect to AI-assisted AVs.
   c. Inter-vehicle (V2V) and V2X technology – Again, a myriad of current and proposed methods and implementations, with interesting safety and security tradeoffs.
   d. Total system architecture – WG expertise regarding dependable and secure distributed systems (e.g., regard a connected group of AVs as a larger autonomous system) should be particularly useful in this regard.
   e. Infrastructure – Intelligent spaces such as smart intersections, smart highways, etc. (This could be included as part of aspect d. if that seems to be more appropriate.)
   f. Assurance – Special needs for measuring, analytic and simulation modeling, testing, verifying, and validating dependable and secure intelligent AVs.

2) Determine who should manage overall work on the project (10.4 Chair?) and ask for 10.4 volunteers to address various aspects chosen in step 1). And there's likely a need to designate a lead for each such task group. Hopefully, work can begin right after the Winter 2019 meeting. There's a great deal of activity regarding intelligent AVs that deserves to be surveyed in order to establish and justify resulting dependability and security imperatives. Other topics and corresponding task groups may emerge as a consequence.

3) Each task group should benefit from interaction with experts in related areas, either "offline" between meetings, or "online" by inviting them to subsequent meetings. Building on the Brazil 10.4 workshop held in Summer 2015 (Autonomous and Cooperative Intelligent Vehicles), the WG should organize specific workshops over the next couple of years devoted to topics being addressed by the task groups. These could include joint workshops with WGs in other IFIP TCs, e.g., TC 11 (Security) and TC-12 (AI), and interaction with relevant IEEE TCs and ACM SIGs. Some examples are the *TC on Self Driving Cars* (IEEE Intelligent Transportation Systems Society), *TC on Autonomous Ground Vehicles and Intelligent Transportation Systems* (IEEE Robotics and Automation Society), and the *SIG on Artificial Intelligence* (ACM).

4) Each task group (see Step 2)) prepares a summary of their imperatives along with justifications thereof. There is no set deadline for this. It depends mainly on the extent of the activity proposed for Step 3), which will likely require at least two years to accomplish.

Deliverable: The imperatives determined by each task group will be combined in a document edited by a subcommittee (TBD) but authored in the name of WG 10.4. This document will then be distributed to the wider CS/IT community (specifics also TBD) as well as major players in the intelligent AV arena.