Intelligent Vehicle Dependability and Security

IFIP Working Group 10.4

1. Introduction

The purpose of this brief white paper is to inform interested stakeholders of the intentions of a project recently undertaken by Working Group 10.4 (Dependable Computing and Fault Tolerance) of the International Federation for Information Processing (IFIP). WG 10.4 was established by the IFIP General Assembly in October 1980, operates under the auspices of IFIP Technical Committee 10 (Computer Systems Technology), and has held semi-annual meetings since June,1981.

Through its workshops, its affiliations with larger conferences, and landmark publications by many of its members, WG 10.4 has contributed significantly to both R&D and application of highly dependable and secure computing systems. This new project is expected to require several years to complete, where its vision, mission, and goals are as follows.

2. Vision

The vision of the project is the realization of highly dependable and secure operation of intelligent vehicles (IVs), verified and validated with respect to strict dependability (particularly safety) and security requirements by rigorous state-of-the-art methods. Types of vehicle intelligence assumed in the vision are mainly those associated with SAE levels 3-5 (ADS) (per SAE Recommended Practice J3016, V 0620180), although level 2 (ADAS) may also be addressed with respect to certain issues.

3. Mission

In pursuit of this vision, the project's mission is to facilitate awareness and provide pro bono counsel to both automotive stakeholders and relevant standardization/regulatory bodies. Avenues for such provision include the invitation of researchers and government/industry stakeholders to workshops regarding specific IVDS issues. These will be organized either by WG 10.4 or jointly with other professional groups having similar interests, e.g., WGs in IFIP TCs such as TC 11 (Security) and TC-12 (AI), and IEEE TCs and ACM SIGs such as 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). Another important avenue is meeting with industry and government in their own environments, e.g., IV-related conferences and workshops organized by industrial groups and governmental agencies.

4. Goals

In keeping with the above-stated mission, the goals of the project correspond to acquiring and disseminating knowledge with respect to a number of important concerns regarding dependable and secure IVs. Other goals may surface as work on the project progresses.

4.1 Measures

Several interesting questions deserve consideration in this regard. Generally, what kind of measures are appropriate for assessing dependability and security during various phases of IV development and deployment? Are there dependability measures other than safety that need to be addressed in this context? What are the most useful measures of IV security? Can security of an IV be measured quantitatively? A number of publications (journal papers, conference papers, white papers and technical reports by government and non-profit organizations, etc.) have been published in this regard. However, most focus on safety and tend to reflect legacy thinking relating to safe SAE level-0 operation of vehicles.

4.2 Standards

Many standards for IV operation at various levels of automation already exist. These requirements are authored by various international bodies and national organizations in the Americas, Europe, and Asia. (Although not advertised as a standard, SAE J3016 is highly suggestive of what needs to be standardized.) These documents deserve to be studied carefully with regard to dependability and security requirements. In particular, are they consistent? Do they employ measures of the type addressed in goal 4.1? If so, are there stated bounds on measure values that need to be adhered to?

What's likely needed in this regard are dependability specifications of the type that have been applied to aircraft and spacecraft computing systems. For example, if failure is identified with a crash causing fatalities, the allowable failure rate (e.g., fatal crashes per hour) is no greater than a very small number such as 10^{-8}.

4.3 Employment of Machine Learning Algorithms

If a vehicle is intelligent then, de facto, it is artificially so, i.e., AI is employed, particularly the use of machine learning (ML) techniques. However, there are general concerns about the use of statistical ML algorithms in safety-critical applications and, hence, their use for IV control. Should employment of such algorithms therefore be avoided in IVs? If not, are there methods of insuring that unpredictable anomalies in outcomes are detected and their adverse effects on the IV are mitigated?

4.4 Key Design Methods

To satisfy strict dependability and security requirements, key design methods will need to be discussed with automotive stakeholders. These will certainly include techniques for tolerating both accidental and intentional faults that are familiar to the dependable computing community. Also included are techniques more specific to IV safety, e.g., those specified in ISO 26262. However, with regard to the concerns noted in goal 4.3, new methods may also be needed to tolerate the vagaries of non-determinism.

Since safe and secure operation of IVs transcends that of a single vehicle, system-of-systems behavior also needs to be considered, along with a hierarchy of related policies. In particular, attention should be given to highway flow control, the interaction of multiple vehicles and the potential for cascading error scenarios.

For example, to what degree does design diversity help or hinder achievement of goals? Could a common mode error or security flaw create gridlock or catastrophic failure? Are multiple discipline engineering solutions thoroughly integrated and analyzed? What is the potential for mode confusion and emergent behavior?

4.5 Assurance and Certification

IVs present some interesting problems with regard to assuring and certifying that dependability and security requirements are satisfied. These problems cut across all the usual means of verifying and validating safety-critical and security-critical systems. They are due, in part, to the fact that IVs are intelligent and, therefore less predictable than more usual deterministic systems. Indeed, what needs to be accomplished in this regard depends in no small extent on first resolving concerns expressed in goals 4.1-4.4. Finally, there's the question as to who is going to be responsible for such assurance and certification. Roles and responsibilities of regulatory, oversight and governance bodies need to be clearly articulated.

Contact

IVDS Project Lead Dr. Jay Lala: Jay_Lala@raytheon.com

Websites

IFIP: www.ifip.org

WG 10.4: https://www.dependability.org/wg10.4/index.html