6th International Workshop on Safety and Security of Intelligent Vehicles - SSIV 2020

João Carlos Cunha
Coimbra Polytechnic - ISEC
Centro de Informática e Sistemas da Universidade de Coimbra
Portugal
jcunha@isec.pt

Kalinka Branco
Universidade de São Paulo
Brazil
kalinka@icmc.usp.br

Michaël Lauer
Univ. de Toulouse
LAAS-CNRS
France
mlauer@laas.fr

Mobile robot systems, like aerial and ground vehicles, have been receiving an increased number of electronic components, connected through wireless networks and running embedded software over the last years. This strong integration between dedicated computing devices, i.e. the physical environment, dedicated computing devices, and networking, composes a Cyber-Physical System (CPS). CPS have thus become part of common vehicles, accessible to everyone, such as automobiles or unmanned aerial vehicles (UAVs). Furthermore, as processing power increases and software becomes more sophisticated, these vehicles gain the ability to perform complex operations, becoming more autonomous, efficient, adaptable, comfortable, safe and usable. These are known as Intelligent Vehicles (IV).

A prominent representative of Intelligent Vehicles are automobiles which are now able to offer active safety, adaptive cruise control, park assistance, automatic climate control, navigation support and, in a near future, vehicle to vehicle communication. With networking capabilities, the myriad of devices inside the vehicles become part of the IoT (Internet of Things) world.

These systems are classified as critical, since failure events may cause the loss of human lives or high-value assets, meaning that safety is one of the main concerns for developers and users. However, the combination of high mobility and wireless communications has further increased the exposure of such systems to malicious threats and to faults deriving from uncertain connectivity or communication timeliness. Non-functional requirements like security and real-time operation have thus become harder to fulfill, creating new challenges to these safety-critical embedded systems. The environment of humans will continue to evolve to interactive IoT that is going to include mobile (flying, driving, floating, rolling, diving, walking, etc) objects that raises numerous challenging issues. Observing the current trend in the development of self-driving cars, one can only infer that artificial intelligence (through machine learning) is going to play a crucial role in the future intelligent vehicle. However, the complexity of such algorithms decreases their level of trust and integrating them in critical systems is a far-reaching research issue. Even advanced hardware components like multi-core processors, GPUs, or FPGAs that represent a formidable opportunity to deploy complex functionalities in intelligent vehicles, they raise new difficulties for certification, verification of real-time properties, safety and security.

The vast range of open challenges to achieve Safety and Security in Intelligent Vehicles (with or without connection with the Internet) is a fundamental reason that justifies the numerous research initiatives and wide discussion on these matters, which we are currently observing everywhere. Therefore, this workshop will keep its focus on exploring the challenges and interdependencies between security, real-time, safety and certification, which emerge when introducing networked, autonomous and cooperative functionalities.

This is the sixth edition of SSIV, planned to run in València, Spain, co-located with 50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Previous editions took place in Rio de Janeiro, Brazil (2015), Toulouse, France (2016), Denver, USA (2017), Luxembourg (2018), and Portland, USA (2019).

However, due to the COVID-19 situation, this year the conference will run all-digital, as the remaining events of DSN. SSIV 2020 will run for 3.5 hours, allowing people from all over the world to participate in a more convenient time. The workshop is organized in 3 sessions that include the presentations of the 9 accepted papers, and one panel:

- **Session 1** is devoted to **Artificial Intelligence and Adaptive Systems**, and includes 3 paper presentations addressing topics of AI and reliability, adaptive data selection and distributed decision-making.
- **Session 2** is devoted to **Dependability and Security Analysis** and includes 3 presentations addressing Hazard and Risk Analysis, Cybersecurity and Fault Injection.
- **Session 3** is devoted to **Architecture and Deployment**, and includes 3 presentations addressing human-drone communication, fault tolerant architecture and enforcement of flight and privacy restrictions.
- The **Panel Session** features selected speakers that promote a discussion about "Challenges in Safety and Security of Intelligent Vehicle".

We would like to express our gratitude to the Program Committee members of SSIV 2020 for their hard work and dedication in providing insightful feedback to the authors, and also to the DSN 2020 conference Organizing Committee for their support in the setup and arrangements of the Workshop, mainly in this pandemic time, keeping safety and well-being of all conference participants as a priority.

For further information, visit: sites.google.com/view/ssiv.