# 4th International Workshop on Safety and Security of Intelligent Vehicles - SSIV 2018

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
LAAS-CNRS
France
mlauer@laas.fr

Based on the fast growth of computational capacity in low power microprocessors and microcontrollers, autonomous vehicles (aerial, ground, underwater, etc) and mobile robot systems have been receiving an increased number of electronic components connected through wireless networks and running embedded software. This strong interaction between physical environments and dedicated computing devices composes a Cyber-Physical System (CPS). CPS has become part of common Autonomous Road Vehicles (ARV) or Unmanned Aerial Vehicles (UAV), likely to be commonplace and accessible to everyone in the near future. 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).

The overall motivation of building Intelligent Vehicles has been to make life safer, and more convenient and efficient. In an increasingly connected world, new levels of missions can be reached if IV can interact with each other and/or with remote users. Connected vehicles could provide up-to-date information and make intelligent decisions in cooperation with other vehicles or devices. However, these links have increased the exposure of IV to malicious threats opening new concerns related to security, on traditional safety-critical systems.

For such IV to become a reality, new research and development must be performed, addressing the needs of multidisciplinary approaches like integrated control systems, communication and network, security algorithms, artificial intelligence, verification and validation, neural networks, safety assessment and other technological concerns.

The first edition of SSIV took place in 2015 in Rio de Janeiro, Brazil, co-located with the 45th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). The success of this workshop motivated new editions, happening in the following years, also co-located with DSN: in 2016 in Toulouse, France; in 2017 in Denver, USA. This is the fourth edition of SSIV, taking place in Luxembourg, as part of DSN'2018. The 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 to intelligent vehicles.

12 papers have been submitted, authored by researchers and practitioners from 9 countries: Brazil, France, Germany, Italy, Romania, Spain, Taiwan, United Kingdom, and United States. After a careful peer review process, 6 full-length papers (8 pages) and 2 short papers (4 pages) were accepted to be presented at the Workshop. SSIV 2018 will run in a full day, organized in 4 sessions, including the presentations of the 8 selected papers, one invited talk, and one panel.

The invited talk will be featured by a distinguished keynote speaker, **Philippe Quéré**, an expert on cybersecurity process and conformity, involved, among others, on ISO/SAE 21434 Automotive Cybersecurity Engineering. Philippe has been involved for 10 years in the development of ISO 26262 Functional Safety standard. He joined Renault in 2005 in "advanced engineering" to work on software development. He took the lead of the team in 2010, and then led an Alliance convergence project with Nissan. Before joining Renault, Philippe has been involved in the development of embedded software for the consumer electronics and the automotive industry, working for car suppliers and manufacturers.

The four sessions will be organized as follows:

- **Session 1** features a **keynote** talk by Philippe Quéré, on the "Progress and possibilities of concrete links between functional safety and cybersecurity". The session also includes 2 paper presentations related to **functional safety** on the automotive domain.
- **Session 2** is devoted to **security** issues in particular through the topics of assessments, testing, and anomaly/intrusion detection.
- **Session 3** features papers on **evaluation and testing** in the automotive and unmanned aerial vehicles domains.
- **Session 4** is devoted to a **panel** where the invited panelists will promote a discussion on the "Challenges, current solutions and research directions regarding safety and security of intelligent vehicles".

We would like to express our gratitude to the Program Committee members of SSIV 2018 for their hard work and dedication in providing insightful feedback to the authors, and also to the DSN 2018 conference Organizing Committee for their support in the setup and arrangements of the Workshop.

For further information, visit: www.lsec.icmc.usp.br/ssiv.



DOI 10.1109/DSN-W.2018.00067