



**A3S'2019**  
**IEEE International Workshop on Automobile Software Security and Safety**  
**July 22-26, 2019**  
**Sofia, Bulgaria**  
<https://qrs19.techconf.org/workshops/a3s>

## Call for Papers

### Program Chairs

Mohammad Zulkernine  
*Queen's University, Canada*  
Ryo Kurachi  
*Nagoya University, Japan*  
Dennis Kengo Oka  
*Synopsys, Inc., USA*

### Program Committee

Onur Altintas  
*Toyota Info Technology Center, Japan*  
Jeremy Bryans  
*Coventry University, UK*  
Tsvika Dagan  
*Tel Aviv University, Israel*  
Mohamad Gharib  
*University of Florence, Italy*  
Javier Gozalvez  
*Miguel Hernández University of Elche, Spain*  
Bogdan Groza  
*Polytechnic University of Timișoara, Romania*  
Giambattista Grusso  
*Polytechnic University of Milan, Italy*  
Jérémie Guiochet  
*University of Toulouse, France*  
Talal Halabi  
*Queen's University, Canada*  
Anwar Haque  
*Western University, Canada*  
Mohammad Asadul Hoque  
*East Tennessee State University, USA*  
Shahreaz Iqbal  
*Security Compass, Canada*  
Clifford Liem  
*Irdeco, Canada*  
Stefan Murvay  
*Polytechnic University of Timișoara, Romania*  
Jan Pelzl  
*Applied University of Hamm-Lippstadt, Germany*  
Miguel Sepulcre  
*Miguel Hernández University of Elche, Spain*  
Alexey Vinel  
*Halmstad University, Sweden*  
Albert Wasef  
*EsCrypt, Canada*  
Andre Weimerskirch  
*Lear Corporation, USA*

The last decade has witnessed an increased level of sophistication within embedded software running on different types of automobiles. Automobiles are classified as critical systems, as their failure could directly impact human safety or lead to loss of valuable assets, making their security and safety a major concern for users and designers. The automobiles or vehicles are primarily software controlled and communicate with each other, the cloud, and the transportation infrastructure via wireless networks. Given that, the underlying software that controls their operations and integrated communication technologies must be safe and secure.

The A3S workshop seeks to bring together researchers and practitioners working toward the improvement of security and safety of software solutions in the automobile sector by discussing recent developments and current challenges and exchanging their research findings and experiences. The workshop welcomes papers and presentations in the field of automobile software, dealing with vehicle software security and safety.

The list of topics includes, but is not limited to:

- Automobile software vulnerability assessment, risk analysis, and attack models
- Architecture, design, and implementation of secure and automobile software
- Design of secure information systems and software applications for vehicles
- Vehicle operating system security
- Availability, reliability, and fault tolerance in automobile software
- Automobile software testing, verification, and validation
- Automobile software security and safety evaluation methodologies and metrics
- Automobile software penetration testing, forensics, and events monitoring
- Automobile software standardization, certification, and interoperability
- Secure intra-vehicle, vehicle-to-vehicle, and other vehicular communications
- AI and machine learning for connected and autonomous vehicles
- Practical experiences, empirical studies, and testbeds for automobile software
- Industrial experiences and best practices for automobile software development

### Submission

Authors are invited to submit original unpublished research papers as well as industrial practice papers. Simultaneous submissions to other conferences are not permitted. Detailed instructions for electronic paper submission, panel proposals, and review process can be found at <https://qrs19.techconf.org/submission>.

### Important Dates:

**Submission of papers due: May 20, 2019 (extended)**

**Author notification: June 1, 2019 (extended)**

Camera-ready papers due: June 10, 2019

Workshop dates: July 22-26, 2019