Safety as a Data-Centric Design for Autonomous Vehicles

Data is at the core of the design of modern Safety-Critical Systems. Data is no longer only sensed and processed in the context of the control loops of such systems. It is also secured, stored, and transmitted for the sake of the decision-making processes required for higher levels of autonomy. Decomposing the problem domain into a Data-Centric point of view considers the modeling of constructs that will abstract the selected entities and their relationships according to the data they produce and consume, considering timing, safety, security, and persistency. The diagram below presents a top-view of components in Autonomous vehicles.

In this sense, many questions come to the mind when we consider safety in Autonomous vehicles. Some of them are listed below to instigate the discussion in this topic during the panel:

1. Data-Centric design:
   1. Domain decomposition into Data-Centric Design: Replacing tasks with Data!
   2. How to measure the trustfulness of data?
   3. How to measure data plausibility?
2. Safety Models
   1. Measuring safety in terms of safety distances and (discussion based on Responsibility Sensitive Safety!)
   2. Reachability Set Analysis (RSA) and the prediction strategies for nearby actors future states
3. Run-time Verification and Property Monitors
   1. Formal Methods integration with the system design
   2. Protection Mechanisms and Fault-Tolerance: How to integrate the knowledge from engineering into safety models?
4. Critical components Isolation and Security

Guilherme Mertens de Andrade is an Autonomous Racing Director at Ampera, in Federal University of Santa Catarina.

José Luis Conradi Hoffmann is a PhD student at Federal University of Santa Catarina (UFSC), where he is a member of the Software/Hardware Integration Lab (LISHA) since 2018. He received his M.Sc. degree in Computer Science in 2021, from the UFSC, Brazil. His research interests include Data-Driven Design of Critical Systems, Safety Verification, Formal Methods, Real-Time embedded systems, Machine Learning, IoT, and Security Protocols.

Leonardo Passig Horstmann is a Ph.D. candidate at Federal University of Santa Catarina (UFSC), where he is a member of the Software/Hardware Integration Lab (LISHA) since 2018. He received M.Sc. degree in Computer Science in 2021, from the UFSC, Brazil, and his research interests include Safety-Critical Systems, Mixed-Criticality Systems, Autonomous Systems, Real-Time embedded systems, multicore processors, Machine Learning, IoT, Misbehavior Detection, and security protocols.

Antônio Augusto Fröhlich is a Full Professor at the UFSC, where leads the Software/Hardware Integration Lab (LISHA) since 2001. With a Ph.D. in Computer Engineering from TU-Berlin, he has coordinated several R&D projects on embedded systems. Significant contributions from these projects materialized within the Brazilian Digital Television System and IoT technology for Energy Distribution, Smart Cities, and Autonomous Systems. He is a senior member of ACM, IEEE, and SBC.

Giovani Gracioli is an assistant professor at UFSC and associate researcher of LISHA since 2007. He holds a PhD degree in automation and systems engineering from UFSC. He has participated in several R&D projects in areas such as IoT, safe-critical embedded systems and autonomous vehicles. His research interests include critical embedded software and real-time operating systems.

Phone: +55 48 3721-9516  
e-mail: lisha@lisha.ufsc.br  
Web: https://lisha.ufsc.br/