

# SafeComp 2019

## 38<sup>th</sup> International Conference on Computer Safety, Reliability and Security

**Turku, Finland**

**10 - 13 September 2019**

**Conference Programme**





## Welcome to SAFECOMP 2019

On behalf of the organizing and program committee, it is our pleasure to welcome all participants to the 38th International Conference on Computer Safety, Reliability & Security – SAFECOMP 2019. The European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7), established the SAFECOMP Conference in 1979. Since then, it has been continually contributing to the state-of-the-art through the knowledge dissemination and discussions of safety and security aspects of computer systems and their impact on our lives. Modern safety-critical systems are becoming increasingly complex and interconnected. They start to rely on the technologies, such as artificial intelligence, that have not been used in the safety-critical domain before. This opens a wide range of engineering and certification problems, which are to be discussed at the conference.

The special theme of SAFECOMP2019 is “Safety and security of autonomous systems”. Autonomy – the ability of the system to operate for extended periods of time without human intervention – becomes a much sought-after property of modern computer-based systems. Self-driving cars, unmanned aerial vehicles (drones), autonomous ships and trains as well as variety of robots are the well-known examples of autonomous systems. A wide range of issues associated with development, verification and validation of safety of autonomous safety-critical systems are discussed in the invited talk “An Open, Transparent, Industry–Driven Approach to AV Safety” by Jack Weast (Intel, USA), the industrial panel, as well as a number of technical presentations.

Another actively discussed theme is the role of security in the safety-critical context. The invited talks by Professor Ross Anderson (University of Cambridge, UK) “The Sustainability of Safety, Security and Privacy” and Professor Marco Vieira (University of Coimbra, Portugal) “Trustworthiness Benchmarking of Safety Critical Systems” as well as several technical presentations address this recently emerged topic.

SAFECOMP 2019 has a strong technical program built of 21 technical papers published in Lecture Notes for Computer Science (LNCS) volume 11698 by Springer. The international program committee consisting of 57 members from 14 countries worked hard to review 65 submitted papers received from 23 countries. Each paper was thoroughly reviewed and discussed at the program committee meeting in Newcastle upon Tyne, UK in April 2019. The acceptance rate of SAFECOMP 2019 was 32%. We would like to thank the program committee members and the external reviewers for their hard work and active participation in the review process.

Following the tradition, SAFECOMP 2019 is organized as a single-track conference to promote an open discussion and intensive networking. The conference features an industrial panel on “Safety and security of autonomous systems”. We are grateful to the panel moderator Prof. Philip Koopman (Carnegie Mellon University, USA and Edge Case Research co-founder) and the panelists Dr. Simon Collart-Dutilleul (Institut Français des Sciences et Technologies des Transports, de l’Aménagement et des Réseaux IFSTTAR, France), Dr. Jelena Frtunikj (BMW, Germany), Dr. Timo Latvala (Space Systems Finland) and Jack Weast (Intel, USA) for agreeing to share their ideas and openly discuss this challenging topic. Finally, the conference program also includes a fast abstracts session, giving the authors an opportunity to present new ideas and discuss a work in progress.

The main conference is preceded by 5 regular workshops: DECSoS, ASSURE, SASSUR, STRIVE and WAISE publishing their papers in LNCS volume 11699. We would like to thank the workshop

chairs Ilir Gashi (City University London, UK) and Erwin Schoitsch (AIT Austrian Institute of Technology) for their hard work on coordinating workshops organization.

We are grateful to our sponsors and the supporting institutions, especially EWICS TC7 headed by Francesca Saglietti. We also express our sincere gratitude to Wärtsilä Land and Sea Academy for organizing the interesting technical guided tour. We would like to express our tahnks to the many who have helped with the preparations and running of the conference, in particular the publication chair Dr. Friedemann Bitsch (Thales, Germany) and the local organization team of Åbo Akademi University, Finland especially Inna Vistbakka and Amin Majd.

Finally, we would like to thank all the authors and participants – without you this event count not happen. We hope that you will enjoy the technical program, social events and the beautiful city of Turku.



Alexander Romanovsky  
Program Committee Co-chair



Elena Troubitsyna  
General Chair and Program Committee Co-chair

# Conference Program

## Overview

	Tuesday 10 September	Wednesday 11 September	Thursday 12 September	Friday 13 September
	WORKSHOP DAY	SAFECOMP DAY 1	SAFECOMP DAY 2	SAFECOMP DAY 3
SUPPORTING ORGANISATIONS EXPOSITION				
8:00 – 8:50	Registration	Registration	Registration	Registration
8:50 – 9:00		Welcome		
9:00 – 10:00	Workshops  DECSoS ASSURE SASSUR STRIVE WAISE (Individual schedules)	Keynote talk 1	Keynote talk 3	Session 6
10:00 – 10:30		Coffee break	Coffee break	
10:30 – 11:00		Session 1	Session 4	Coffee break
11:00 – 11:30				Fast abstracts session
11:30 – 12:00				
12:00 – 13:30		Lunch	Lunch	Lunch
13:30 – 14:30		Keynote talk 2	Industrial panel	Session 7
14:30 – 15:00		Session 2	EWICS Session	
15:00 – 15:30			Coffee break	Closing
15:30 – 16:00		Coffee break	Session 5	Coffee break
16:00 – 16:30				
16:30 – 17:00		Session 3		
17:00 – 17:30				
17:30 – 18:00				
18:00 – 18:30				Guided tour in Turku Castle and conference banquet
18:30 – 19:00		Visit to Wärtsilä Land and Sea Academy		
19:00 – 20:30	Welcome reception			
19:00 – 23:30				

# Conference Program

Wednesday 11 September 2019

## Room: AavaMeri

08:00–08:50 Registration

08:50–09:00 Welcome

### KEYNOTE TALK 1 by Marco Vieira (Chair: Elena Troubitsyna)

09:00–10:00 Trustworthiness Benchmarking of Safety Critical Systems.  
*Marco Vieira, University of Coimbra, Portugal.*

10:00–10:30 Coffee break

### SESSION 1: Formal verification (Chair: Maritta Heisel)

10:30–11:00 Model-Based Run-Time Synthesis of Architectural Configurations for Adaptive MILS Systems. *Alessandro Cimatti, Rance DeLong, Ivan Stojic and Stefano Tonetta.*

11:00–11:30 Towards Zero Alarms in Sound Static Analysis of Finite State Machines.  
*Josselin Giet, Laurent Mauborgne, Daniel Kästner and Christian Ferdinand.*

11:30–12:00 Formal Verification of Memory Preservation of x86–64 Binaries.  
*Joshua Bockenek, Freek Verbeek, Peter Lammich and Binoy Ravindran.*

12:00–13:30 Lunch at Restaurant Airisto

### KEYNOTE TALK 2 by Jack Weast (Chair: António Casimiro)

13:30–14:30 An Open, Transparent, Industry-Driven Approach to AV Safety.  
*Jack Weast, Intel, USA.*

### SESSION 2: Autonomous driving (Chair: Simon Burton)

14:30–15:00 Graceful Degradation Design Process for Autonomous Driving System.  
*Tasuku Ishigooka, Satoshi Otsuka, Kazuyoshi Serizawa, Ryo Tsuchiya and Fumio Narisawa.*

15:00–15:30 Forecast Horizon for Automated Safety Actions in Automated Driving Systems. *Ayhan Mehmed, Moritz Antlanger, Wlfried Steiner and Sasikumar Punnekkat.*

15:30–16:00 Autonomous Vehicles Meet the Physical World: RSS, Variability, Uncertainty, and *Proving Safety*. *Philip Koopman, Beth Osyk and Jack Weast.*

16:00-16:30 Coffee break

**SESSION 3: Safety and reliability modeling (Chair: Andrea Bondavalli)**

16:30–17:00 A SysML Profile for Fault Trees — linking safety models to system design.  
*Kester Clegg, Mole Li, Alan Grigg, David Stamp and John McDermid.*

17:00–17:30 Efficient Model-level Reliability Analysis of Simulink Models.  
*Kai Ding, Andrey Morozov and Klaus Janschek.*

17:30–18:00 SafeDeML: On Integrating the Safety Design into the System Model.  
*Tim Gonschorek, Philipp Bergt, Marco Filax, Frank Ortmeier, Jan von Hoyningen-Huene and Thorsten Piper.*

18:30-20:30 Visit to Wärtsilä Land and Sea Academy



# Thursday 12 September 2019

## Room: AavaMeri

08:00–09:00 Registration

**KEYNOTE TALK 3 by Ross Anderson (Chair: Alexander Romanovsky)**

09:00–10:00 The Sustainability of Safety, Security and Privacy.  
*Ross Anderson, University of Cambridge, UK.*

10:00–10:30 Coffee break

**SESSION 4: Security engineering and risk assessment (Chair: Frank Ortmeier)**

10:30–11:00 Digital Forensics in Industrial Control Systems.  
*Robert Altschaffel, Stefan Kiltz, Prof. Dr. Jana Dittmann and Mario Hildebrandt.*

11:00–11:30 Towards Trusted Security Context Exchange Protocol for SDN based Low Latency. Networks. *Abdul Ghafoor, A Qudus Abbasi and Zaheer Abbas Khan.*

11:30–12:00 Dynamic risk assessment enabling automated interventions for medical cyber–physical systems. *Fabio Luiz Leite Junior, Rasmus Adler and Daniel Schneider.*

12:00–13:30 Lunch at Restaurant Airisto

**Industrial Panel: Safety and Security of Autonomous Systems (Moderator: Phil Koopman)**

13:30–15:00 Industrial Panel

*Panelists*

*Simon Collart-Dutilleul (Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux IFSTTAR, France)*

*Jelena Frtunikj (BMW, Germany),*

*Timo Latvala (Space Systems Finland)*

*Jack Weast (Intel, USA)*

15:00–15:30 EWICS TC7 presentation lead by *Francesca Saglietti*

15:30–16:00 Coffee break



**SESSION 5: Safety argumentation (Chair: Ewan Denny)**

16:00–16:30 Devil's in the detail: Through–life safety and security co–assurance using SSAF. *Nikita Johnson and Tim Kelly.*

16:30–17:00 Automated Evidence Analysis of Safety Arguments using Digital Dependability Identities. *Jan Reich, Marc Zeller and Daniel Schneider.*

17:00–17:30 A Pattern for Arguing the Assurance of Machine Learning in Medical Diagnosis Systems. *Chiara Picardi, Richard Hawkins, Colin Paterson and Ibrahim Habli.*

18:00-23:30 **Conference banquet**

**18:00            Bus departs from the conference venue.**

**18:30–19:30 Guided tour in the medieval part of Turku Castle**

**19:30–20:00 Welcome drink**

**20:00–23:00 Conference banquet in the King's hall**

**23:05            Bus departs towards the conference venue**

# Friday 13 September 2019

## Room: Submarina (underground floor)

08:30–09:00 Registration

### SESSION 6: Verification and validation of autonomous systems (Chair: Philippe Palanque)

09:00–09:30 Practical Experience Report: Engineering Safe Deep Neural Networks for Automated Driving Systems. *Jelena Frtunikj*.

09:30–10:00 Fitness Functions for Testing Automated and Autonomous Driving Systems. *Florian Hauer, Alexander Pretschner and Bernd Holzmüller*.

10:00–10:30 Increasing Trust in Data-Driven Model Validation – A Framework for Probabilistic Augmentation of Images and Meta-Data Generation using Application Scope Characteristics. *Lisa Joeckel and Michael Klaes*.

10:30–11:00 Coffee break

### FAST ABSTRACT SESSION (Chair: Alexander Romanovsky)

11:30–12:00 Fast abstracts

- Towards Safe-by-Design Artificial Intelligence Systems. *Nataliya Yakymets*.
- Signal-based Hazard Analysis and Risk Assessment. *Dariusz Szymanski, Tilmann Ochs and Galvani Alves de Lacerda*.
- AQUAMON – A dependable Monitoring Platform based on Wireless Sensor Networks for Water Environments. *António Casimiro, José Cecílio, Pedro Ferreira, Anabela Oliveira, Paula Freire, Marta Rodrigues, Luís Almeida*.
- Towards assessing the risk of the effect of augmented reality on human failures. *Soheila Sheikh Bahaei and Barbara Gallina*.
- Towards a holistic assurance methodology: From component to information assurance. *Arash Khabbaz Saberi, Andre Smulders, and Johan J. Lukkien*.

12:00–13:30 Lunch at Restaurant Airisto

### SESSION 7: Interactive systems and design validation (Chair: Barbara Gallina)

13:30–14:00 Brace Touch: a Dependable, Turbulence-Tolerant, Multi-Touch Interaction Technique for Interactive Cockpits. *Philippe Palanque, Andy Cockburn, Léopold Désert-Legendre, Carl Gutwin and Yannick Déléris*.

14:00–14:30 Spectrum–Based Fault Localization in Deployed Embedded Systems with Driver Interaction Models. *Ulrich Thomas Gabor, Simon Dierl and Olaf Spinczyk.*

14:30–15:00 BACRank: Ranking Building Automation and Control System Components by Business Continuity Impact. *Herson Esquivel–Vargas, Marco Caselli, Erik Tews, Doina Bucur and Andreas Peter.*

15:00–15:30 **CLOSING SESSION and Introduction to SAFECOMP 2020**

15:30–16:00 **Closing coffee**

## Committees

### EWICS TC7 Chair

Francesca Saglietti University of Erlangen-Nuremberg, Germany

### General Chairs and Program Co-chairs

Alexander Romanovsky, Newcastle University, UK  
Elena Troubitsyna, KTH - Royal Institute of Technology, Sweden  
and Åbo Akademi, Finland

### General Workshop Chairs

Iilir Gashi CSR, City University London, UK  
Erwin Schoitsch AIT Austrian Institute of Technology, Austria

### Publication Chair

Friedemann Bitsch, Thales Deutschland GmbH, Germany

### Local Organizing Committee

Elena Troubitsyna, Åbo Akademi, Finland  
Minna Carla, Åbo Akademi, Finland  
Christel Engblom, Åbo Akademi, Finland  
Inna Vistbackka, Åbo Akademi, Finland

### International Program Committee

Uwe Becker, Draeger Medical GmbH, Germany  
Peter G. Bishop, Adelard, UK  
Friedemann Bitsch, Thales Deutschland GmbH, Germany  
Jean-Paul Blanquart, Airbus Defence and Space, France  
Sandro Bologna, Associazione Italiana Esperti Infrastrutture Critiche, Italy  
Andrea Bondavalli, University of Florence, Italy  
Jens Braband, Siemens AG, Germany  
Simon Burton, Robert Bosch GmbH, Germany  
António Casimiro, University of Lisbon, Portugal  
Mads Dam, KTH - Royal Institute of Technology, Sweden  
Peter Daniel, EWICS TC7, UK  
Ewen Denney, SGT/NASA Ames Research Center, USA  
Felicita Di Giandomenico, ISTI-CNR, Italy  
Wolfgang Ehrenberger, University of Applied Science Fulda, Germany  
John Favaro, Intecs, Italy  
Francesco Flammini, Linnaeus University, Sweden  
Simon Fuerst, BMW Group, Germany  
Barbara Gallina, Mälardalen University, Sweden  
Iilir Gashi, CSR, City University London, UK  
Anatoliy Gorbenko, National Aerospace University, KhAI, UK

Janusz Górski, Gdańsk University of Technology, Poland  
Jérémie Guiochet, LAAS-CNRS, France  
Hans Hansson, Mälardalen University, Sweden  
Mats Heimdahl, University of Minnesota, USA  
Maritta Heisel, University of Duisburg-Essen, Germany  
Constance Heitmeyer, Naval Research Laboratory, USA  
Alexei Iliasov, Newcastle University, UK  
Christopher Johnson, University of Glasgow, UK  
Rajeev Joshi, Automated Reasoning Group, Amazon Web Services, USA  
Karama Kanoun, LAAS-CNRS, France  
Joost-Pieter Katoen, RWTH Aachen University, Germany  
Phil Koopman, Carnegie-Mellon University, USA  
Peter Ladkin, University of Bielefeld, Germany  
Timo Latvala, Space Systems Finland Ltd., Finland  
Simin Nadjm-Tehrani, Linköping University, Sweden  
Mattias Nyberg, Scania, Linköping University, Sweden  
Frank Ortmeier, Otto-von-Guericke Universität Magdeburg, Germany  
Philippe Palanque, ICS-IRIT, University Toulouse, France  
Michael Paulitsch, Intel, Austria  
Holger Pfeifer, Technical University of Munich, Germany  
Peter Popov, City University London, UK  
Laurent Rioux, Thales R&T, France  
Matteo Rossi, Politecnico di Milano, Italy  
Francesca Saglietti, University of Erlangen-Nuremberg, Germany  
Christoph Schmitz, Zühlke Engineering AG, Switzerland  
Erwin Schoitsch, AIT Austrian Institute of Technology, Austria  
Christel Seguin, Office National d'Etudes et Recherches Aérospatiales, France  
Håkan Sivencrona, Zenuity AB, Sweden  
Oleg Sokolsky, University of Pennsylvania, USA  
Kenji Taguchi, CAV Technologies Co., Ltd., Japan  
Stefano Tonetta, Fondazione Bruno Kessler, Italy  
Martin Törngren, KTH - Royal Institute of Technology, Sweden  
Mario Trapp, Fraunhofer Institute for Experimental Software Engineering, Germany  
Tullio Vardanega, University of Padua, Italy  
Marcel Verhoef, European Space Agency, The Netherlands  
Jonny Vinter, RISE Research Institutes of Sweden, Sweden  
Hélène Waeselynck, LAAS-CNRS, France

# Conference Keynote Talks

## KEYNOTE TALK 1

### Trustworthiness Benchmarking of Safety Critical Systems

Professor Marco Vieira, University of Coimbra, Portugal

Wednesday, 11 September 2019, 9:00-10:00

**Abstract.** Trustworthiness is a paramount concern for users and customers in the selection of a software solution, specially in the context of complex and dynamic environments, such as Cloud and IoT.

However, assessing and benchmarking trustworthiness (worthiness of software/service for being trusted) is a challenging task, mainly due to the variety of application scenarios (e.g., safety-critical, business-critical), the large number of determinative quality attributes (e.g., safety, security, performance), and last, but foremost, due to the subjective notion of trust and trustworthiness.

In this talk, we will address trustworthiness as a measurable notion and discuss approaches for the assessment and benchmarking of software systems. The main goal is to better understand how trustworthiness scores can be computed and the main components involved in a trustworthiness benchmarking process.



**Biography.** Marco Vieira is a Full Professor at the University of Coimbra, Portugal. His current research interests include dependability and security assessment and benchmarking, fault injection and vulnerability & attack injection, robustness and security testing, online failure prediction, and software verification and validation, subjects on which he has authored or co-authored more than 180 papers in refereed conferences and journals. He has coordinated several research projects, both at the national and European level. Marco Vieira has served as PC-chair of the major conferences in the dependability area and acted as referee for many international conferences and journals.

## KEYNOTE TALK 2

### **An Open, Transparent, Industry-Driven Approach to AV Safety**

Jack Weast, Intel, USA

Wednesday, 11 September 2019, 13:30-14:30

**Abstract.** The rules of the road today are all focused around one key element: drivers. Licensing, insurance, traffic laws - everything assumes vehicles are operated under the control of a human. For driverless vehicles, this presents a dilemma: How can you tell which car is at fault in an accident? More importantly: How can self-driving and human-driven cars co-exist safely?

At Intel and Mobileye, saving lives drives us. But in the world of automated driving, we believe safety is not merely an impact of AD, but the bedrock on which we all build this industry. And so we proposed Responsibility-Sensitive Safety (RSS), a formal model to define safe driving and what rules an automated vehicle, independent of brand or policy, should abide to always keep its passengers safe. We intend this open, non-proprietary model to drive cross-industry discussion; let's come together as an industry and use RSS as a starting point to clarify safety today, to enable the autonomous tomorrow.



**Biography.** Jack Weast is a Sr. Principal Engineer and the Chief Systems Architect for Automated Driving Solutions at Intel. In his nearly 20 year career at Intel, Jack has built a reputation as a change agent in new industries with significant technical contributions to a wide range of industry-first products and standards in complex heterogeneous high performance compute solutions in markets that are embracing high performance computing for the first time. With an End to End Systems perspective, Jack combines a unique blend of embedded product experience with a knack for elegant Software and Systems design that will accelerate the adoption of Autonomous Driving. Jack is the co-author of *UPnP: Design*

*By Example*, is an Adjunct Professor at Portland State University and is the holder of 23 patents with dozens pending.



## KEYNOTE TALK 3

### **The Sustainability of Safety, Security and Privacy.**

Ross Anderson, University of Cambridge, UK.

Thursday, 12 September 2019, 9:00-10:00

**Abstract.** Now that we're putting software and network connections into cars and medical devices, we'll have to patch vulnerabilities, as we do with phones. But we can't let vendors stop patching them after three years, as they do with phones. So in May, the EU passed Directive 2019/771 on the sale of goods. This gives consumers the right to software updates for goods with digital elements, for the time period the consumer might reasonably expect.

In this talk I'll describe the background, including a study we did for the European Commission in 2016, and the likely future effects. As sustainable safety, security and privacy become a legal mandate, this will create real tension with existing business models and supply chains. It will also pose a grand challenge for computer scientists.

What sort of tools and methodologies should you use to write software for a car that will go on sale in 2023, if you have to support security patches and safety upgrades till 2043?



**Biography.** Ross Anderson is a professor of Security Engineering at the Computer Laboratory of University of Cambridge, UK. He is one of the pioneers and world leaders in security engineering. Ross Anderson's mission is to develop the discipline of security engineering, which investigates how systems can be made robust in the face of malice, error and mischance. He has made pioneering contributions to many subdisciplines, including peer-to-peer-networks, hardware tamper resistance and cryptographic protocols.

Ross was a designer of the block cipher Serpent, and he has worked on many applications with diverse protection requirements such as payment networks, power-line communications, goods vehicle tachographs and clinical information systems. Ross is the author of the standard text *Security Engineering: A Guide to Building Dependable Distributed Systems* (2008) and regularly contributes to a blog on security research, *Light Blue Touchpaper*. He has also chairs the *Foundation for Information Policy Research*.

# Workshop Program

## DECSoS – 14<sup>th</sup> International ERCIM/EWICS/ARTEMIS Workshop on “Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems”

Co-hosted by the ARTEMIS/ECSEL projects AQUAS, AutoDrive, Productive4.0, iDev40, AfarCloud SECREDAS, ARROWHEAD-Tools and Comp4Drones

### Room Aava

9:00 – 10:30 Registration

10:30 – 11:00 Coffee Break

#### Welcome and Introduction

11:00 – 11:30 ERCIM/EWICS/ARTEMIS DECSoS Workshop: European Research and Innovation Projects in the Field of Cyber-Physical Systems and Systems-of-Systems (Selective Overview) by *Erwin Schoitsch and Amund Skavhaug*.

#### SESSION 1: Safety & Security Analysis

11:30 – 12:00 Comparative Evaluation of Security Fuzzing Approaches. *Loui Al Sardy, Andreas Neubaum, Francesca Saglietti and Daniel Rudrich*.

12:00 – 12:30 Assuring compliance with protection profiles with ThreatGet. *Magdy El Sadany, Christoph Schmittner and Wolfgang Kastner*.

12:30 – 13:30 Lunch at Restaurant Airisto

#### SESSION 2: Safety/Security/Privacy Systems Co-Engineering

13:30 – 14:00 A Survey on the Applicability of Safety, Security and Privacy Standards in Developing Dependable Systems. *Lijun Shan, Behrooz Sangchoolie, Peter Folkesson, Jonny Vinter, Erwin Schoitsch, Claire Loiseaux (invited paper)*.

14:00 – 14:30 Combined Approach for Safety and Security. *Siddhartha Verma, Thomas Gruber and Christoph Schmittner*.

14:30 – 15:00 Towards Integrated Quantitative Security and Safety Risk Assessment. *Jürgen Dobaj, Christoph Schmittner, Michael Krisper and Georg Macher*.

15:00 – 15:30 Coffee Break

#### SESSION 3: IoT Applications

15:30 – 16:00 Potential use of safety analysis for risk assessments in Smart City Sensor network Applications. *Torge Hinrichs and Bettina Buth*.

16:00 – 16:30 Increasing Safety of Neural Networks in Medical Devices. *Uwe Becker*.

16:30 – 17:00 Smart Wristband for Voting. *Martin Pfatrish, Linda Grefen and Hans Ehm*.

# Workshop Program

## SASSUR – 8<sup>th</sup> International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems

### Room Lumi

9:00 - 9:15 [Welcome](#)

9:15- 10:00 **Keynote:** Model-based safety assurance in industrial practice - Quo vadis? *Mark Zeller*

10:00 - 10:30 The SISTER approach for Verification and Validation: a lightweight process for reusable results. *Andrea Ceccarelli, Davide Basile, Andrea Bondavalli, Lorenzo Falaj, Alessandro Fantechi, Sandro Ferrari et al.*

10:30 - 11:00 [Coffee break](#)

11:00 - 11:30 Automotive Cybersecurity standards - relation and overview. *Christoph Schmittner, Georg Macher.*

11:30 - 12:00 A Runtime Safety Monitoring Approach for Adaptable Autonomous Systems. *Nikita Bhardwaj Haupt, Peter Liggesmeyer.*

12:00 - 12:30 Structured Reasoning for Socio-Technical Factors of Safety-Security Assurance. *Nikita Johnson, Tim Kelly.*

12:30 – 13:30 [Lunch at Restaurant Airisto](#)

# Workshop Program

## ASSURE – 7th International Workshop on Assurance Cases for Software-intensive Systems

### Room Pisara

#### SESSION 1: Welcome and Keynote

9:00 - 09:10 Welcome and Introduction, ASSURE 2019 Organizers

9:10 - 10:00 **Keynote:** Assurance cases in an era of smart and collaborative cyber-physical systems – pain points and ways forward. *Prof. Martin Törngren.*

10:00 - 10:30 Assurance Case Tools.

10:30 - 11:00 [Coffee Break](#)

#### SESSION 2: Research Papers

11:00 - 11:30 Contract-based Modular Safety Cases for Incremental Certification of Product Lines. *Damir Nesic and Mattias Nyberg.*

11:30 - 12:00 Combining GSN and STPA for safety arguments. *Celso Hirata and Simin Nadjm-Tehrani.*

12:00 - 12:30 A modelling approach for system life cycles assurance. *Shuji Kinoshita, Yoshiki Kinoshita and Makoto Takeyama.*

12:30 – 13:30 [Lunch at Restaurant Airisto](#)

# Workshop Program

**STRIVE – 2<sup>nd</sup> International Workshop on Safety, security and pRivacy in automotiVe systEMs**

## Room Lähde

09:15-09:30 Opening

09:30-10:30 DEMO: CANDY CREAM - haCking infotAiNment AnDroid sYstems to Command instRument clustEr via cAn data fraMe. *Gianpiero Costantino and Ilaria Matteucci.*

10:30-11:00 Coffee Break

### SESSION 1: In-vehicle Security (Chair: *Gianpiero Costantino*)

11:00-11:30 CarINA - Car sharing with IdeNtity based Access control re-enforced by TPM. *Bogdan Groza, Lucian Popa and Pal-Stefan Murvay.*

11:30-12:00 Combining Safety and Security in Autonomous Cars Using Blockchain Technologies. *Lucas Davi, Denis Hatebur, Maritta Heisel and Roman Wirtz.*

12:00-12:30 Enhancing CAN security by means of lightweight stream-ciphers and protocols. *Aymen Boudguiga, Jerome Letaille, Renaud Sirdey and Witold Kludel.*

12:30 – 13:30 Lunch at Restaurant Airisto

### SESSION 2. Security in Vehicular Network and IoT (Chair: *Ilaria Matteucci*)

14:00-14:30 Analysis of Security Overhead in Broadcast V2V Communications. *Paul Kearney, Mujahid Muhammad, Adel Aneiba and Andreas Kunz.*

14:30-15:00 *You overtrust your printer.* *Giampaolo Bella and Pietro Biondi.*

15:00-15:30 Coffee Break

15:30 End of the Workshop

# Workshop Program

## WAISE – 2<sup>nd</sup> International Workshop on Artificial Intelligence Safety Engineering

### Room Meri

**8:30-9:00** Registration and welcome to WAISE 2019.

**9:00-10:00 KEYNOTE TALK SESSION (Chair: Simos Gerasimou)**

Safety Assurance of Autonomous Systems – bridging the gap between research and industry. *Apl.Prof.Dr.habil. Mario Trapp*

**10:00-10:10** Poster Pitching

Three Reasons Why: Framing the Challenges of Assuring AI, *Xinwei Fang and Nikita Johnson*.

Tackling Uncertainty in Safety Assurance for Machine Learning: Continuous Argument Engineering with Attributed Tests. *Yutaka Matsuno, Fuyuki Ishikawa and Susumu Tokumoto*

The Moral Machine: Is It Moral? *Alexandre Moreira Nascimento, Lucio Vismari, Anna Carolina Muller Queiroz, Paulo Cugnasca, Joao Camargo and Jorge Rady*.

**10:10-10:40** Coffee break - Poster Sessions

**10:40-11:20 SESSION 1: Standardisation and Certification**

A Safety Standard Approach for Fully Autonomous Vehicles. *Philip Koopman, Uma Ferrell, Frank Fratrick and Michael Wagner*

A Self-Certifiable Architecture for Critical Systems Powered by Probabilistic Logic Artificial Intelligence. *Jacques Robin, Raul Mazo, Henrique Madeira, Raul Barbosa, Daniel Diaz and Salvador Abreu*

### Debate Panel

**11:20-12:30 SESSION 2: Assuring AI-based Systems**

Open Questions in Testing of Learned Computer Vision Functions for Automated Driving. *Matthias Woehrle, Christoph Gladisch and Christian Heinzemann*.

An Abstraction-Refinement Approach to Formal Verification of Tree Ensembles. *John Törnblom and Simin Nadjm-Tehrani*.

Improving ML Safety with Partial Specifications. *Rick Salay and Krzysztof Czarnecki*.

### Debate Panel

**12:30-13:30** Lunch - Poster Sessions

**13:30-14:30** KEYNOTE TALK SESSION Zakaria Chihani

**14:30-15:30** SESSION 3: Uncertainty in AI-based Systems

Uncertainty Wrappers for Data-driven Models - Increase the Transparency of AI/ML-based Models through Enrichment with Dependable Situation-aware Uncertainty Estimates. *Michael Klaes and Lena Sembach.*

Bayesian Uncertainty Quantification with Synthetic Data. *Buu Phan, Samin Khan, Rick Salay and Krzysztof Czarnecki.*

Confidence Arguments for Evidence of Performance in Machine Learning. *Simon Burton, Lydia Gauerhof, Bibhuti Bhusan Sethy, Ibrahim Habli and Richard Hawkins.*

**Debate Panel**

**15:30-16:00** Coffee break - Poster Sessions

**16:00-16:40** SESSION 4: Safety of Autonomous Systems

RL-Based Method for Benchmarking the Adversarial Resilience and Robustness of Deep Reinforcement Learning Policies. *Vahid Behzadan and William Hsu.*

Adaptive Deployment of Safety Monitors for Autonomous Systems. *Nico Hochgeschwender.*

**Debate Panel**

**16:40-17:30** Towards a Body of Knowledge for Assured Robotics and Autonomous Systems

**17:30-17:45** Wrap-up - Best Paper Award



## General Information

**Venue:** Radisson Blu Marina Palace Hotel, Turku, Finland.

<https://www.radissonhotels.com/en-us/hotels/radisson-blu-marina-turku>

Address: Linnankatu 32, 20100 Turku, Finland.

**Registration desk:** Located in the lobby. Open from 8:00 till 18:00, every workshop and conference day.

**Badge/Tickets:** Each participant will receive a personal badge upon registration. Please wear the badge during the workshops and conference. Please show your banquet ticket before entering the bus to the conference banquet.

**Lunches and coffee breaks** are included in the registration fee. Coffee breaks will take place in the foyer next to the conference room. Lunches will take place at the restaurant Airisto.

**WIFI:** free wi-fi is available for all hotel guests and participants.

**CONTACTS:** safecomp2019@easychair.org

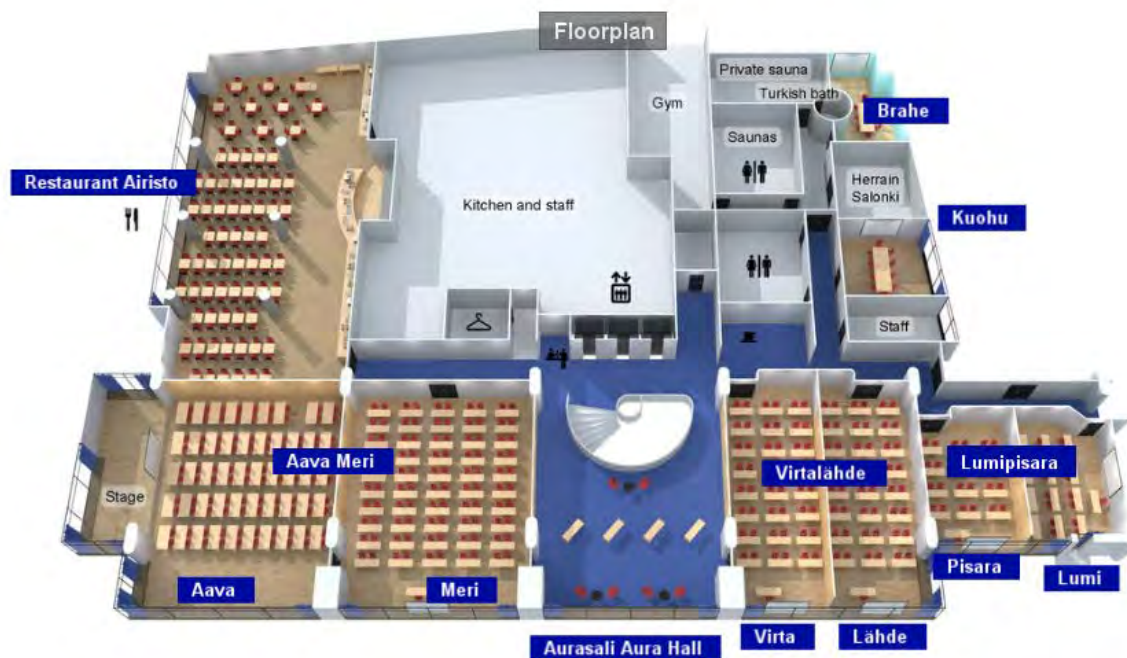
Phone: +358 2 215 4086

**Emergency number: 112**

**Liability:** The organising committee cannot accept any responsibility for personal accidents or loss/damage of private property. Please do not keep your personal belongings unattended.

**Lost and Found:** Please refer to the hotel reception or registration desk.

Floor plan:



## Social Events



**Tuesday 10 September 2019 19:00 – 20:30**

### Welcome reception at Turku City Hall

**Address: Aurakatu 2, Turku (650 meters from the conference venue)**

After welcome from City of Turku and short guided visit, refreshments and drinks will be served

**Wednesday 11 September 2019 18:30-20:30**

### Visit to Wärtsilä Land and Sea Academy

- Bus transportation to and from the conference venue
- Address: Stålarinkatu 45, Turku
- Guided tour 19:00-20:00

Wärtsilä Oyj Abp is a Finnish corporation which manufactures and services power sources and other equipment in the marine and energy markets. We will be guided through the training center, where the participants will have an opportunity to see the real engines and visit the hands-on area.

Please observe **NO PHOTOGRAPHY ALLOWED.**



**Thursday 12 September 2019 18:00 – 23:30**

### Guided tour and banquet in the Turku Castle

Bus transportation to and from the conference venue

#### Program

18:00: Bus departs from the conference venue.

18:30–19:30: Guided tour in the medieval part of Turku Castle (we will be split in four groups)

19:30-20:00 Welcome drink

20:00–23:00: Conference banquet in the King's hall

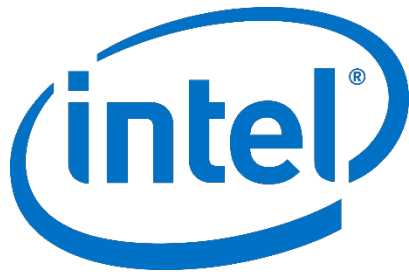
23:05: Bus departs toward the conference venue





# SAFECOMP 2019 Sponsors and Partners

## Gold sponsor



## Bronze Sponsors



EDGE CASE RESEARCH



## Partners

