



Systems, Software and Safety 2019

System and software safety in electronic systems is becoming increasingly central in many industries and indeed as part of often critical societal infrastructure. The systems become ever more complex, connected and autonomous — and the software continues to grow. This poses many challenges even for mature organizations, requiring approaches that go beyond established best practices.

The Scandinavian conference on safety critical systems and software has become a central meeting place for Scandinavian safety experts from industry, public and academic organizations. It is an opportunity to share experiences and make new contacts. The conference features a first day with distinguished keynotes, industrial and research presentations, followed by a second day of parallel workshops, advanced presentations and tutorials about different challenges, techniques, standards and methods. At the end of the first day the conference dinner provides opportunities to establish further contacts among the participants.

Warm Welcome!

Nicolas Martin-Vivaldi, Addalot
nicolas.martin-vivaldi@addalot.se
 0706 800 521

Martin Törngren, KTH/ICES
martin@md.kth.se
 08-790 63 07

www.addalot.se

www.ices.kth.se

TIME 22-23 October 2019

PLACE Spårvagnshallarna, Stockholm

ORGANIZERS Addalot Consulting AB, KTH and ICES

COST (excl. VAT): **Early bird**** **Late**

Two days*	3500:-	4200:-
Only Day 1*	2000:-	2400:-
Only Day 2	1500:-	1800:-

*Conference dinner is included.

**Early bird price before

15 September (extended)

Student discount : 50%

Final registration: 15 October

Full program and registration

<http://safety.addalot.se/>

addalot
 QUALITY IMPROVEMENT

ICES 
 Innovative Centre for Embedded Systems

First version 190616

Monday 22 October - Plenary day

Time	Content	Presenter
08:30-09:00	Registration and coffee	
09:00-09:15	Welcome and introduction	Nicolas Martin-Vivaldi/ Martin Törngren
09:15-10:15	Keynote: System Lifecycle Operational Governance	Nick McDonald Trinity College Dublin
10:15-10:40	Coffee	
10:40-11:20	Is the actual safety of E/E systems in automotive vehicles generally known?	Carl Bondesson, Scania
11:20-12:00	Safety cage : an approach for safe machine learning systems	Sankar Raman Sathyamoorthy, QRTECH AB
12:00-13:00	Lunch	
13:00-14:00	Keynote: System safety principles from 1999; challenges for 2019?	Dr David Pumfrey, University of York
14:00-14:35	Conflict as Software Levels Diversify	Fredrik Asplund, KTH
14:35-15:00	Coffee	
15:00-15:40	CCPE - A methodology for predicting mismatches in human-machine interaction	Lars-Ola Bligård, Chalmers University of Technology
15:40-16:20	Safety management - practice and compliance in safety critical product development and service production	Pernilla Ulfvengren, KTH
16:20-17:00	The challenges for today's functional safety engineer - A view based on railway, automotive and machinery industry	Yin Chen, Combitech



Nicolas Martin-Vivaldi
Addalot Consulting



Martin Törngren
KTH



Nick McDonald
Trinity College Dublin



Carl Bondesson
Scania



Sankar Raman
Sathyamoorthy
QRTECH AB



Dr David Pumfrey
University of York



Fredrik Asplund
KTH



Lars-Ola Bligård
Chalmers



Pernilla Ulfvengren
KTH



Yin Chen
Combitech

Tuesday 23 October - Parallel tracks 08:30-17:00

<p>Workshop: Design of dependable systems – fundamentals of Aircraft safety Kristina Forsberg and Håkan Forsberg, SAAB and MDH We address requirements and responsibilities in the aviation industry, e.g. EASA certification specifications CS25.1309 and acceptable means of compliance AMC 25.1309 for large airplanes. Who is responsible to assess that correct level of safety is achieved? Both process and design assurance are addressed. The workshop will discuss the reported unsafe condition of Boeing 737 MAX.</p>	<p>Workshop: System Lifecycle Operational Governance, Nick McDonald, Fredrik Asplund, Pernilla Ulfvengren What principles should inform system lifecycle governance? Theory often defines problems as insoluble; yet, pragmatic solutions are needed. A discussion will be structured around five interlinked challenges: 1. Understanding system performance 2. The reliability of change 3. Strategic management of operational risk 4. Design for operations 5. Governance based on evidence Underlying each is are contradictions to be overcome through the collective experience of the participants.</p>	<p>Tutorial/Workshop ISO 26262 – overview and challenges – Even-André Karlsson, Addalot In this tutorial/workshop we will give an overview of ISO 26262 with some practical experiences. The workshop will be interactive, where we expect the participants to bring their experience and challenges for discussion.</p>
<p>Workshop: System safety principles from 1999; challenges for 2019? David Pumfrey, Martin Törngren, Stefan Norrwing In this workshop we will discuss in more detail David's 9 principles and 2 new analysis methods. We will describe how they have been used, and also discuss their applicability for new challenges that more complex systems face, e.g. autonomy, AI, connected systems, and systems of systems. The workshop will be interactive involving participants to share experience and challenges.</p>	<p>In-depth presentations: Hazard Analysis of a Fleet of Autonomous Machine using STPA -A Case Study, Stephan Baumgart, Volvo Construction Equipment AB, MDH Preventing Omission of Key Evidence Fallacy in Process-based Argumentations, Barbara Gallina, MDH Implicit Safety -A Concept for SW SEooC, David Baca, NXP Facilitating Automated Compliance Checking of Processes against Safety Standards, Julieth Patricia Castellanos Ardila, MDH Variant Management and Change Impact Analysis in Safety-oriented Process-Product Lines, Barbara Gallina, MDH</p>	<p>Tutorial/Workshop ASPICE – overview and challenges – Nicolas Martin Vivaldi, Addalot In this tutorial/workshop we will give an overview of ASPICE with some practical experiences. The workshop will be interactive, where we expect participants to bring their experience and challenges for discussion.</p>

addalot
QUALITY IMPROVEMENT

Cices 
Innovative Centre for Embedded Systems