6th Scandinavian Conference on System and Software Safety 21-22 May, Stockholm

Systems, Software and Safety 2018

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!

TIME 21-22 May 2018

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 16 March
Student discount : 50%

Final registration: 15 May

Full program and registration

http://safety.addalot.se/

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

Final version 180207

Monday 21 May - Plenary day

Time	Content	Presenter
08:30-09:00	Registration and coffee	
09:00-09:10	Welcome and introduction	Nicolas Martin-Vivaldi/ Martin Törngren
09:10-10:10	**Keynote: Assurance Points in Software Development**	**Prof. Peter Bernard Ladkin, Bielefeld University**
10:10-10:30	Coffee	
10:30-11:05	How does a Safety Standard Change the Safety Work?	Anna Beckman, Scania
11:05-11:40	Software Defenses Against Hardware Failure	Chris Hobbs, QNX Software Systems
11:40-12:15	SMILE – Safety analysis and verification & validation of MachIne LEarning based systems	Cristofer Englund, RISE Viktoria
12:15-13:10	Lunch	
13:10-14:10	**Keynote: Safety of intended functionality - Status, open issues and ways forward**	**Dr Håkan Sivencrona, Zenuity**
14:10-15:10	**Keynote: Safety of Autonomy: Challenges and Strategies**	**Professor John McDermid, University of York**
15:10-15:30	Coffee	
15:30-16:05	Machine learning in automotive software development - opportunities and challenges	Miroslaw Staron, Chalmers / University of Gothenburg
16:05-17:05	**Keynote: Cyber-Risk Assessment Framework encompassing safety and security**	**M.Sc. Jonathan Roberts, Rolls-Royce**


Nicolas Martin-Vivaldi
Addalot Consulting

Martin Törngren
KTH



Peter Bernard Ladkin
Bielefeld University

Anna Beckman
Scania



Chris Hobbs, QNX
Software Systems

Cristofer Englund
RISE Viktoria



Håkan Sivencrona,
Zenuity

John McDermid,
University of York



Miroslaw Staron
Chalmers
University of
Gothenburg

Jonathan Roberts
Rolls-Royce


Tuesday 22 May - Parallel tracks 08:30-17:00

Frontiers in Safety:

- Towards generating ECSS-compliant fault tree analysis results via ConcertoFLA, Zulqarnain Haider, Mälardalens Högskola
- A Tool for Analyzing Safety and Security of Java Programs, Narges Khakpour, Linnaeus University
- Towards Increased Efficiency and Confidence in Process Compliance, Julieth Patricia Castellanos Ardila, Mälardalens Högskola
- Open Source in Functional Safety products, Nicolas Martin-Vivaldi, Addalot

Workshop: Security and Safety
John McDermid and Jonathan Roberts.
Following up on the presentation from the previous day the Cyber-Risk Assessment Framework (CRAF) will be further illustrated by the use of real-world incidents.
Participants will be given the opportunity to use the CRAF to elicit undiscovered risk related to safety and security in an example system.
The results will be discussed with an eye towards what is missing in current engineering practice.

System Safety training: Why-Because Analysis, Ontological Hazard Analysis, and Risk Analysis
Full day training course with Prof. Dr. Peter Bernard Ladkin
The course is divided into three modules:
1. The Counterfactual Test (CT) and Why-Because Analysis (WBA) Introducing the CT and its use in causal analysis of incidents with WBA. An incident description will be provided, from which participants will construct a Why-Because Graph.
2. Ontological Hazard Analysis (OHA). Applying OHA using OPRA, followed by a system description provided for participants to apply OHA.
3. Risk Analysis. Use of event trees to delineate possible outcomes of hazards; evaluate of likelihood and severity and their combination.
Written course materials will be provided.
The tutorial is based partly on examples in the draft book, Digital System Safety.
Causalis Ingenieurgesellschaft will issue a certificate of successful completion for active participants.

Workshop: Users, HMI and Safety
Christin Lindholm, LTH
Patrik Moberg, Siemens Digital Factory Division
Medical devices and other industrial system are becoming more sophisticated, contain more software and are used by new and different user groups – often with limited training or infrequent. A major challenge is to assure safety and prevent harm. By involving users in the risk management process, we can lower the risk of errors. In this workshop we will discuss challenges and experiences from safety work in this kind of systems.

Workshop: Safety engineering for highly automated vehicles
Martin Törngren and Sofia Cassel, ARCHER FFI project,
Automated driving for higher levels of automation represents a drastic departure from current vehicle design by introducing unprecedented complexity as part of safety critical systems. The workshop focuses on presenting issues and results concerning methods and techniques for

- dealing with risk,
- verification and validation,
- architectural design methods

addalot
QUALITY IMPROVEMENT

Chces
Innovative Centre for Embedded Systems
KTH VETENSKAP OCH KONST