SAFECOMP 2018

international conference on computer safety, reliability & security

18-21 September, Västerås, Sweden

Conference Program and Practical Information

18-21 September, 2018

SAFECOMP 2018
Aros Congress Center
Munkgatan 7, 772 12 Västerås, Sweden
email : safecomp18@mdh.se
http://www.es.mdh.se/safecomp2018

Welcome to SAFECOMP 2018

On behalf of the whole organizing committee, it is my pleasure to welcome all participants to the 37th International Conference on Computer Safety, Reliability & Security – SAFECOMP 2018.

The European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7), established the SAFECOMP Conference in 1979. It has since contributed to the state-of-the art through the knowledge dissemination and discussions of important aspects of computer systems of our everyday life. With the proliferation of embedded systems, the omnipresence of Internet of Things and commodity of advanced real-time control systems, our dependence on the safe and correct behavior is ever increasing. Currently, we are witnessing the beginning of the area of truly autonomous systems, perhaps with the driverless cars as the most well-known to the non-specialist, where the safety and correctness of their computer systems are already being discussed in the mainstream media. In this context, it is clear that the relevance of the SAFECOMP conference series is increasing.

The international program committee, consisting of 56 members from 15 countries, received 63 papers from 24 nations. Of these, 20 papers were selected to be presented at the conference resulting in an acceptance rate of 31.7%. The review process was thorough with at least 3 reviewers with ensured independency, and 20 of these reviewers met in person in Munich, Germany in April 2018 for the final discussion and selection. Our warm thanks go to reviewers who offered their time and competence in the program committee work. We are grateful for the support we received from the PC member Mario Trapp, Fraunhofer ESK, who generously hosted the PC meeting.

The conference features three keynotes: “Software Engineering for Safety in Molecular Programmed Systems” by Robyn Lutz, Professor of Computer Science at Iowa State University; “Reviews?! We do that! Cross-domain reuse of engineering knowledge and evidence” by Uma Ferrell, software and airborne electronic hardware Designated Engineering Representative for the US Federal Aviation Administration; “Experiences from the industry, design and application of a control system platform for safety of machinery”, by Richard Hendeberg, specialist in functional safety at Epiroc Rock Drills AB.

As in the previous years, the conference is organized as a singletrack conference, allowing intensive networking during breaks and social events, and participation in all presentations and discussions. The conference also includes a fast abstracts session, giving the opportunity to new ideas and work in progress to bloom in a fertile soil. The Fast abstracts proceedings are published in the HAL repository.

Finally, the conference also includes a panel session, focusing on stimulating an interactive discussion with the audience around the main theme of SAFECOMP 2018, i.e., “Cross and intra domain reuse of engineering and certification artefacts: challenges and opportunities”.

As it has been the tradition for many years, the day before the main-track of the conference is dedicated to 5 regular workshops: DECSoS, ASSURE, SASSUR, STRIVE, WAISE. Papers from these are published in a separate LNCS volume (11094).

We would like to express our gratitude to the many who have helped with the preparations and running of the conference, especially Friedemann Bitsch as publication chair, Erwin Schoitsch as workshop chair, Jérémie Guiochet as fast abstracts chair, Alexander Romanovsky as publicity chair, and not to be forgotten the local organization and support staff, Irfan Sljivo, Lena Jonsson, Martina Pettersson, Elena Rivani, Linda Claesson, and Gunnar Widforss.

For its support, we wish to thank Mälardalen University, represented by the School of Innovation, Design and Engineering and, more specifically, by the research group Certifiable Evidences & Justification Engineering. We also wish to thank all other supporting institutions.

Without the support from the EWICS TC7 headed by Francesca Saglietti this event could not have happened. We wish the EWICS TC7 organization continued success, and we are looking forward to being part of this also in the future.

Finally, the most important persons to whom we want to express our gratitude are the authors and participants. Your dedication, effort and knowledge are the foundation of the scientific progress. We hope you will have fruitful discussions, gain new insights, as well as in all ways have a memorable time in Västerås.
To conclude, I wish to highlight that, despite the descent of Autumn, Västerås in September is still alive and kicking and hosts various cultural events (e.g., Kulturnatt, Autumn Festival in the Open Air Museum, etc.) in a spectacular display of Autumn colours.

Barbara Gallina
General chair & Program Co-Chair

MÄLARDALEN UNIVERSITY
SWEDEN

Conference Program

Overview

	Tuesday 18 September	Wednesday 19 September	Thursday 20 September	Friday 21 September
	WORKSHOP DAY	SAFECOMP DAY 1	SAFECOMP DAY 2	SAFECOMP DAY 3
	SUPPORTING INSTITUTIONS EXPOSITION			
8:00-8:45	REGISTRATION	REGISTRATION	REGISTRATION	REGISTRATION
8:45-9:00		**WELCOME**		
9:00-10:00	Workshops: DECSoS, SASSUR, ASSURE, STRIVE, WAISE	**KEYNOTE TALK 1** Robyn Lutz	**KEYNOTE TALK 2** Uma Ferrell	**KEYNOTE TALK 3** Richard Hendeberg
10:00-10:30		Coffee break	Coffee break	Coffee break
10:30-11:00	Coffee break	**SESSION 1** Automotive safety standards and cross-domain reuse potential	**SESSION 4** Verification	**SESSION 7** Fault tolerance
11:00-12:00				
12:00-12:30		**EXPOSITION OVERVIEW**		
12:30-13:30	Lunch break	Lunch break	Lunch break	Lunch break
13:30-14:00				
14:00-14:30		**SESSION 2** Autonomous driving and safety analysis	**EWICS PRESENTATION**	**SESSION 8** Safety and Security risk
14:30-15:30			**SESSION 5** Multi-concern assurance	
15:30-16:00	Coffee break	Coffee break		CLOSING SESSION & Introduction to SAFECOMP 2019
16:00-16:30		**SESSION 3** Fast abstracts and poster presentations	**SESSION 6** Panel discussion	
16:30-17:00				
17:00-17:30				
17:30-17:45				
17:45-18:30			Bus to Eskilstuna	
18:30-19:00		GUIDED CITY TOUR		
19:00-19:30			Mingle at Munktellmuseet	
19:30-20:00		WELCOME RECEPTION @Hotel PLAZA (Skrapan)		
20:00			CONFERENCE DINNER at Munktellmuseet	

Conference Program

Wednesday 19 September 2018

Room: Hörsalen

8:00-8:45 REGISTRATION

8:45-9:00 WELCOME (by Barbara Gallina)

KEYNOTE TALK 1 by Robyn Lutz (Chair: Irfan Sljivo)

9:00-10:00 Software Engineering for Safety in Molecular Programmed Systems.
Robyn Lutz, Iowa State University, USA

10:00-10:30 Coffee break

SESSION 1: Automotive safety standards and cross-domain reuse potential (Chair: Ewen Denney)

10:30-11:00 Automotive Safety Practices vs. Accepted Principles (Practical Experience Report).
Philip Koopman.

11:00-11:30 A Generic Method for a Bottom-Up ASIL Decomposition.
Alessandro Frigerio, Bart Vermeulen and Kees Goossens.

11:30-12:00 Assurance Benefits of ISO 26262 Compliant Microcontrollers for Safety-Critical Avionics.
Andreas Schwierz and Håkan Forsberg.

EXPOSITION OVERVIEW

12:00-12:30 Exposition overview

12:30-14:00 Lunch break

SESSION 2: Autonomous driving and safety analysis (Chair: Elena Troubitsyna)

14:00-14:30 Structuring Validations Targets of a Machine Learning Function applied in Automated Driving.
Lydia Gauerhof, Peter Munk and Simon Burton.

14:30-15:00 Multi-Aspect Safety Engineering for Highly Automated Driving - Looking beyond functional safety and established standards and methodologies. *Patrik Feth, Rasmus Adler, Takeshi Fukuda, Tasuku Ishigooka, Satoshi Otsuka, Daniel Schneider, Denis Uecker and Kentaro Yoshimura.*

15:00-15:30 A Model-Based Safety Analysis of Dependencies Across Abstraction Layers. *Christoph Dropmann, Eike Thaden, Mario Trapp, Denis Uecker, Rakshith Amarnath, Leandro Avila Da Silva, Peter Munk, Markus Schweizer, Matthias Jung and Rasmus Adler.*

15:30-16:00 Coffee break

SESSION 3: Fast abstracts 30' + Posters Presentation 60' (Chair: Jérémie Guiochet)

16:00-16:30 Fast abstract talks

16:30-17:30 Fast abstract posters

18:30-19:30 GUIDED CITY TOUR

19:30 Social Event: Conference Welcome Reception at Hotel Plaza

Conference Program

Thursday 20 September 2018

Room: Hörsalen

8:00-9:00 REGISTRATION

KEYNOTE TALK 2 by Uma Ferrell (Chair: Barbara Gallina)

9:00-10:00 Reviews?! We do that! Cross-domain reuse of engineering knowledge and evidence.
Uma Ferrell, MITRE Corporation, USA

10:00-10:30 Coffee break

SESSION 4: Verification (Chair: Francesca Saglietti)

10:30-11:00 Formal verification of signalling programs with SafeCap.
Alexei Iliasov, Dominic Taylor, Linas Laibinis and Alexander Romanovsky.

11:00-11:30 Deriving and Formalising Safety and Security Requirements for Control Systems.
Elena Troubitsyna and Inna Vistbakka.

11:30-12:00 Optimal Test Suite Generation for Modified Condition Decision Coverage using SAT solving.
Takashi Kitamura, Quentin Maissonneuve, Eun-Hye Choi, Cyrille Valentin Artho and Angelo Gargantini.

12:00-12:30 Efficient Splitting of Test and Simulation Cases for the Verification of Highly Automated Driving Functions. *Eckard Böde, Matthias Büker, Ulrich Eberle, Martin Fränzle, Sebastian Gerwinn and Birte Kramer.*

12:30-14:00 Lunch break

14:00-14:30 EWICS PRESENTATION

SESSION 5: Multi-concern assurance (Chair: Erwin Schoitsch)

14:30-15:00 Roadblocks on the Highway to Secure Cars: An Exploratory Survey on the Current Safety and Security Practice of the Automotive Industry. *Michael Huber, Michael Brunner, Clemens Sauerwein, Carmen Carlan and Ruth Breu.*

15:00-15:30 Safe and Secure Automotive Over-The-Air Updates. *Thomas Chowdhury, Eric Lesiuta, Kerianne Rikley, Chung-Wei Lin, Eunsuk Kang, Baekgyu Kim, Shinichi Shiraishi, Mark Lawford and Alan Wassyng*.

15:30-16:00 Dependability Analysis of the AFDX Frame Management Design.
Venesa Watson and Mahlet Ermias.

SESSION 6: Panel discussion

16:00-17:30 Panel discussion

17:45 BUS to ESKILSTUNA. The bus leaves from Aros Congress Center

18:30-20:00 Mingle at MUNKTELLMUSEET

20:00-22:30 Social Event: Conference dinner at MUNKTELLMUSEET

22:30 Departure from Eskilstuna back to Aros Congress Center

Conference Program

Friday 21 September 2018

Room: Hörsalen

8:00-9:00 REGISTRATION

KEYNOTE TALK 3 by Richard Hendeberg (Chair: Kenji Taguchi)

9:00-10:00 Experiences from the industry, design and application of a control system platform for safety of machinery.
Richard Hendeberg, Epiroc Rock Drills AB, Sweden

10:00-10:30 Coffee break

SESSION 7: Fault tolerance (Chair: Alexander Romanovsky)

10:30-11:00 Efficient On-Line Error Detection and Mitigation for Deep Neural Network Accelerators.
Christoph Schorn, Andre Guntoro and Gerd Ascheid.

11:00-11:30 Random Additive Control Flow Error Detection.
Jens Vankeirsbilck, Niels Penneman, Hans Hallez and Jeroen Boydens.

11:30-12:00 Fault-Tolerant Clock Synchronization with only Two Redundant Paths.
Zoha Moztarazdeh.

12:00-12:30 MORE: MOdel-based REdundancy for Simulink.
Kai Ding, Andrey Morozov and Klaus Janschek.

12:30-14:00 Lunch break

SESSION 8: Safety and security risk (Chair: António Casimiro)

14:00-14:30 Diversity in Open Source Intrusion Detection Systems.
Hafizul Asad and Ilir Gashi.

14:30-15:00 Inter-Device Sensor-Fusion for Action Authorization on Industrial Mobile Robots. *Sarah Haas, Andrea Hoeller, Thomas Ulz and Christian Steger.*

15:00-15:30 Towards a Common Ontology of Safety Risk Concepts for Railway Vehicles and Signaling.
Bernhard Hulin, Hermann Kaindl, Roland Beckert, Thomas Rathfux and Roman Popp.

15:30-16:00 CLOSING SESSION & Introduction to SAFECOMP 2019

Fast Abstracts Program & Posters

Wednesday 19th September 2018 16:00-17:30

- A very First Glance on the Safety Analysis of Self-learning Algorithms for Autonomous Cars.
  Tim Gonschorek, Marco Filax, and Frank Ortmeier.
- Tailoring the Method Set in IEC 61508-3 Ed2.
  Nicholas Mc Guire, Andreas Platschek.
- Models adaptation at runtime: enhancing the safety of software systems in uncertain scenarios.
  Miren Illarramendi, Leire Etxeberria, Xabier Elkorobarrutia, Goiuria Sagardui
- Safety-Security Assurance Framework (SSAF) in Practice.
  Nikita Johnson, Tim Kelly.
- Dependable Perception of Infrastructure-Based Automation.
  Florian Geissler, Ralf Gräfe, Rainer Makowitz and Michael Paulitsch
- Agreements of an Automated Driving System.
  Martin Skoglund, Fredrik Warg, Behrooz Sangchoolie.
- Effectiveness of Hamming SEC/DED Code in Harsh Electromagnetic Environments.
  Jonas Van Waes, Jens Vankeirsbilck, Jeroen Boydens, Jonas Lannoo and Davy Pissoort.

Committees

EWICS TC7 Chair: Francesca Saglietti (Univ. of Erlangen-Nuremberg, DE)

General Chair: Barbara Gallina (Mälardalen University, SE)

Program Co-Chairs

Barbara Gallina (Mälardalen University, SE)

Amund Skavhaug (The Norwegian University of Science and Technology, NO)

Workshop Chair: Erwin Schoitsch (AIT Austrian Institute of Technology, AT)

Publication Chair: Friedemann Bitsch (Thales Deutschland GmbH, DE)

Local Organizing Committee

Irfan Sljivo (Mälardalen Universit, SE)
Elena Rivani (Mälardalen University, SE)
Gunnar Widforss (Mälardalen University, SE)
Lena Jonsson (Mälardalen University, SE)
Martina Pettersson (Mälardalen University, SE)
Linda Claesson (Mälardalen University, SE)

Publicity Chair: Alexander Romanovsky (Newcastle University, UK)

Fast Abstract Chair: Jérémie Guiochet (LAAS-CNRS, Univ. Toulouse, FR)

International Program Committee

Uwe Becker (Draeger Medical GmbH, DE)
Peter G. Bishop (Adelard, UK)
Friedemann Bitsch (Thales Deutschland GmbH, DE)
Robin Bloomfield (City University London, UK)
Sandro Bologna (Associazione Italiana Esperti Infrastrutture Critiche, IT)
Andrea Bondavalli (University of Florence, IT)
Jens Braband (Siemens AG, DE)
Anna Carlsson (OHB SE, SE)
António Casimiro (University of Lisbon, PT)
Peter Daniel (EWICS TC7, UK)
Ewen Denney (SGT / NASA Ames Research Center, USA)
Felicita Di Giandomenico (ISTI-CNR, IT)
Wolfgang Ehrenberger (Hochschule Fulda, DE)
Massimo Felici (Deloitte Consulting & Advisory, BE)
Uma Ferrell (MITRE Corporation, USA)
Fancesco Flammini (Linnaeus University, SE)
Barbara Gallina (Mälardalen University, SE)
Ilir Gashi (CSR, City University London, UK)
Janusz Górski (Gdańsk University of Technology, PL)
Jérémie Guiochet (LAAS-CNRS, FR)
Maritta Heisel (University of Duisburg-Essen, DE)
Chris Johnson (University of Glasgow, UK)
Bernhard Kaiser (Assystem Germany GmbH, DE)
Karama Kanoun (LAAS-CNRS, FR)
Johan Karlsson (Chalmers University of Technology, SE)
Phil Koopman (Carnegie-Mellon University, USA)
Floor Koornneef (Delft University of Technology, NL)
Timo Latvala (Space Systems Finland Ltd, FI)
Bev Littlewood (City University London, UK)
Silvia Mazzini (Intecs, IT)
John McDermid (University of York, UK)
Frank Ortmeier (Otto-von-Guericke Uni. Magdeburg, DE)
Michael Paulitsch (Intel, AT)
Holger Pfeifer (Technical University of Munich, DE)
Thomas Pfeiffenberger (Salzburg Research Forschungsgesellschaft m.b.H, AT)
Peter Popov (City University London, UK)
Laurent Rioux (Thales R&T, FR)
Alexander Romanovsky (Newcastle University, UK)
John Rushby (SRI International, USA)
Francesca Saglietti (University of Erlangen-Nuremberg, DE)
Christoph Schmitz (Zühlke Engineering AG, CH)
Erwin Schoitsch (AIT Austrian Institute of Technology, AT)
Christel Seguin (Office National d'Etudes et Recherches Aérospatiales, FR)
Amund Skavhaug (The Norwegian University of Science and Technology, NO)
Mark-Alexander Sujan (University of Warwick, UK)
Kenji Taguchi (CAV Technologies Co., Ltd., Japan)
Stefano Tonetta (Fondazione Bruno Kessler, IT)
Mario Trapp (Fraunhofer Institute for Experimental Software Engineering, DE)
Elena Troubitsyna (Åbo Akademi University, FI)
Fredrik Törner (Volvo Car Corporation, SE)
Martin Törngren (KTH Royal Institute of Technology, SE)
Pieter van Gelder (Delft University of Technology, NL)
Marcel Verhoef (European Space Agency, NL)
Jonny Vinter (RISE Research Institutes of Sweden, SE)
Helene Waeselynck (LAAS-CNRS, FR)

Sub-Reviewers

Matthieu Amy (LAAS-CNRS, FR)
Milan Battelino (OHB Sweden, SE)
Victor Bos (Space Systems Finland Ltd, FI)
Bill Drozd (Carnegie-Mellon University, USA)
Sam George (Adelard, UK)
Didem Gürdür (KTH Royal Institute of Technology, SE)
Denis Hatebur (University of Duisburg-Essen, DE)
Dubravka Ilic (Space Systems Finland Ltd, FI)
Lola Masson (LAAS-CNRS, FR)
Viorel Preoteasa (Space Systems Finland Ltd, FI)
Irum Rauf (Åbo Akademi University, FI)
Behrooz Sangchoolie (RISE Research Institutes of Sweden, SE)
Paulius Stankaitis (Newcastle University, UK)
Kimmo Varpaaniemi (Space Systems Finland Ltd, FI)
Inna Vistbakka (Åbo Akademi University, FI)
Andrzej Wardziński (Gdańsk University of Technology, PO)
Xinhai Zhang (KTH Royal Institute of Technology, SE)

MÄLARDALEN UNIVERSITY SWEDEN

Conference Keynote Talks

KEYNOTE TALK 1

Software Engineering for Safety in Molecular Programmed Systems

Robyn Lutz, Iowa State University, USA
Wednesday 19 September 2018, 9:00 - 10:00

Abstract: Molecular programming uses the computational power of DNA and other biomolecules to create nanoscale systems. Many of these envisioned nano-systems are safety-critical, such as diagnostic biosensors that detect contaminants, drug capsules that dispense medicine when they encounter diseased cells, and configurable nano-robots. Challenges to the safety engineering of the nano-systems include their probabilistic behavior, their very small size, the very large number of them that execute at once, and the dynamic environment in which they operate. Designs need to assure safe outcomes from highly fault-prone devices, hampered by the difficulty of defining the limits of their safe operation.

I organize the talk around our interdisciplinary team's development of an essential safety building block for programmed molecular systems– an embeddable, reusable, molecular Runtime Fault Detector. I describe how we harnessed goal-oriented requirements and risk analyses, reaction network modeling, and probabilistic model checking to specify, analyze, and verify the safety requirements and design for this new nano-system. Finally, I suggest that a similar approach also may be helpful in the safety engineering of non-molecular systems composed of highly distributed, autonomous, fault-prone components operating in dynamic environments.

Biography: Robyn Lutz is a professor of computer science at Iowa State University. She was also on the technical staff of Jet Propulsion Laboratory, California Institute of Technology, from 1983 to 2012, most recently in the Software System Engineering group. Her research interests include safety-critical software systems, product lines, and the specification and verification of molecular programmed nanosystems. She is an ACM Distinguished Scientist. She was program chair of the International Requirements Engineering Conference in 2014, general chair in 2006, and currently serves on its steering committee. She has served two terms as an associate editor of IEEE Transactions on Software Engineering and on the editorial boards of the Journal of Software Testing, Verification and Reliability, the Journal on Software and System Modeling, and the Requirements Engineering Journal.

KEYNOTE TALK 2

Reviews?! We do that! Cross-domain reuse of engineering knowledge and evidence

Uma Ferrell, MITRE Corporation, USA
Thursday 20 September 2018, 9:00 - 10:00

Abstract: Both industry and certification authorities have reason to be excited about the benefits and opportunities of reusing and building products for more than one domain such as aviation and automobiles. Cross-domain reuse in an increasingly complex world can inject novel technologies to conventional domains to increase safety. Such opportunities come with social and ethical responsibilities for the safe use of a product in the target environment, not just whether the product and evidence are acceptable to certification authorities. The evidence may be wrongly presented based only on the equivalency in the use of expected language in pertinent standards. The evidence should be based on the actual accomplishments met and whether those accomplishments are applicable towards design assurance and safety in the target domain and environment.

Cross-domain reuse has many considerations. This talk is focused only on safety and security. Obviously, consideration of reuse must include functionality, use of standards in that domain, and certification concerns. All these considerations have undercurrents of safety as well as security. Let us focus further on three topics:

- **Derivation of risk**: Derivation of risk depends on the target domain and the human/system use of the product. Also, the acceptable level of risk tolerance is inherently different in different domains. Aviation is one of the few domains where safety risk tolerance is codified. As stewards of safety in this society, we need to be aware of the real idea behind certification, and promulgate a safety culture to take responsibility for safe cross-domain use of the product throughout the product life
- **Appropriate use of evidence**: While acceptability for certification is important, the knowledge and evidence for why a product is acceptable is even more important. Evidence may have been produced in a previous domain that appears to be usable in a target domain. Only the basis for that evidence may have a different interpretation and implication in the target domain because the terminology for even simple terms such as "reviews" may not have the same meaning in different domains. Further, the same functionality may be used in diverse ways in the two domains

- **Importance of systems engineering**: There are certainly considerations that may be codified and delegated to checklists. But blind use of checklists makes a poor substitute for domain knowledge and engineering. Cross-domain use does not just mean that one could deploy a product. Continued safe use of the product in the target domain has specific implications for maintenance of the product as well as maintenance of the system of which the product is just one component. For example, an electro-mechanical system may need adjustments to maintenance cycles depending on the characteristics of the component commanding the mechanical actions. In general, we must make sure that component engineering is within the context of system safety and security.

Opportunities of cross-domain reuse indeed come with responsibilities to understand, analyze, and engineer the product. Appropriate reuse considered in the system context can be a powerful tool to introduce newer technologies to solve complex problems.

Biography: Uma Ferrell is excited for the opportunity to share her experiences in engineering systems using cross domain and intra domain knowledge. Her perspectives have benefited from continuous learning through authoring standards, teaching, and researching as well as working with different cultures, and in different domains. Uma is a software and airborne electronic hardware Designated Engineering Representative (DER) for the US Federal Aviation Administration. She is a certification subject matter expert at the MITRE Corporation working on the US Federal Aviation Administration's certification transformation, and Global Positioning System (GPS) navigation for aviation. In addition, she is working on innovative methods of certification for the artificial intelligence in Urban Air Mobility systems, and codification of small Unmanned Aircraft Systems Type Certification. She is also devising a proof-of-concept for an integrated safety and cybersecurity analysis in complex software systems. Uma started her career building mission critical systems for space. After working in technical leadership positions for different companies, Uma co-founded Ferrell and Associates Consulting, Inc. a certification and aviation safety consultancy where she worked as a Chief Executive Officer and a principal for 17 years. Uma holds a Master's degree in Electrical Engineering from Johns Hopkins University, a Master's degree in Solid State Physics, BSc (Hons) in Physics, BSc (Physics, Chemistry and Mathematics) from Bangalore University. Uma is one of the technical editors for the third edition of the Digital Avionics Handbook, published in 2014 by CRC Press. Uma is also on the editorial board of American Society for Quality (ASQ) Software Quality Professional Journal. She also reviews technical books for ASQ. When she is not preoccupied with thoughts on safety culture, new technology, certification, and standards, Uma loves to play Indian classical music.

KEYNOTE TALK 3

Experiences from the industry, design and application of a control system platform for safety of machinery

Richard Hendeberg, Epiroc Rock Drills AB, Sweden

Friday 21 September 2018, 9:00 - 10:00

Abstract: Epiroc Rock Drills AB is a global manufacturer of mining and construction machinery. These highly automated machines operates in an incredibly harsh environment where reliability and availability is paramount. In this presentation, Richard Hendeberg – Specialist functional safety, talks about Epiroc's control systems platform and work with safety of machinery. How a modular design, componentization of software and standardization on hardware modules has led to an efficient reuse of engineering efforts and an automation platform which is used throughout Epiroc's entire range of machinery. In his presentation, Richard also describes Epiroc's journey with safety of control systems, leading up to the integration of safety functions into the existing control system platform. The challenges of designing safety functions for a harsh environment and why availability of the machine might be as important for the safety of the operator as the reliability of the safety function.

Biography: Richard Hendeberg works as a specialist in functional safety at Epiroc Rock Drills AB. He holds a master of science in electronics from the University of Örebro. Richard has worked with design and development of both machinery and systems, including radio- and tele-remote control system and autonomous Load Haul Dump machines. In his current role, Richard supports all divisions within Epiroc Rock Drills AB with matters regarding product legislation, international and regional standards and safety of machinery. He develops strategies and processes for safety management as well as methodologies and tools for risk assessment, design and evaluation of safety functions. Richard holds certifications as machinery safety expert from both the Swedish standards institute and TÜV Nord. He participates as expert in relevant ISO and CEN technical committees for autonomous machinery and safety of control systems.

Welcome to SAFECOMP 2018 Workshop Day

The SAFECOMP Workshop Day has for many years preceded the SAFECOMP Conference, attracting additional participants. The SAFECOMP Workshops have become more attractive since they started generating their own proceedings in the Springer LNCS series. This meant adhering to Springer's guidelines, i.e., the respective international Program Committee of each workshop had to make sure that at least three independent reviewers reviewed the papers carefully. The selection criteria were different from those for the main conference since authors were encouraged to submit workshop papers, i.e., on work in progress and potentially controversial topics. In total, 49 regular papers (out of 73) were accepted.

Three of the five workshops are sequels to earlier workshops, which shows continuity of their relevance to the scientific and industrial community:

- ASSURE 2018 – 6th International Workshop on Assurance Cases for Software-Intensive Systems, chaired by Ewen Denney, Ibrahim Habli, Ganesh Pai, and Richard Hawkins
- DECSoS 2018 – 13th ERCIM/EWICS/ARTEMIS Workshop on Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems, chaired by Erwin Schoitsch and Amund Skavhaug
- SASSUR 2018 – 7th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems, chaired by Alejandra Ruiz, Jose Luis de la Vara, and Tim Kelly

Finally, two new workshops are part of SAFECOMP for the first time (a third new proposal was withdrawn in the end):

- STRIVE 2018 – First International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms, chaired by Gianpiero Costantino and Ilaria Matteucci
- WAISE 2018 – First International Workshop on Artificial Intelligence Safety Engineering, chaired by Huascar Espinoza, Orlando Avila-García, Rob Alexander, and Andreas Theodorou;

The workshops provide a truly international platform for academia and industry.

It has been a pleasure to work with the SAFECOMP chair, Barbara Gallina, and with the publication chair, Friedemann Bitsch, the workshop chairs, Program Committees, and the authors. Thank you all for your good cooperation and excellent work!

September 2018 Erwin Schoitsch

Workshop Program

DECSoS — 13th International ERCIM/EWICS/ARTEMIS Workshop on "Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems"

Room: 105

08:00-09:00 Registration

Welcome and Introduction

09:00-09:30 ERCIM/EWICS/ARTEMIS DECSoS Workshop: European Research and Innovation Initiatives in the Area of Cyber-Physical Systems and Systems-of-Systems (Selective Overview);
by Erwin Schoitsch and Amund Skavhaug

SESSION 1: Testing for Trusted Safety-Critical Systems

09:30-10:00 A Testbed for Trusted Telecommunications Systems in a Safety Critical Environment;
by Ian Oliver, Gabriela Limonta, Borger Vigmostad, Aapo Kalliola, Yoan Miche, Silke Holtmanns and Kiti Muller

10:00-10:30 Constraint-based Testing for Buffer Overflows;
by Loui Al Sardy, Francesca Saglietti, Tong Tang and Heiko Sonnenberg

10:30-11:00 Coffee break

SESSION 2: Cooperative Systems Safety & Security

11:00-11:30 Multi-Layered Approach to Safe Navigation of Swarms of Drones;
by Inna Vistbakka, Amin Majd and Elena Troubitsyna

11:30-12:00 Dynamic Risk Management for Cooperative Autonomous Medical Cyber-Physical Systems;
by Fabio Luiz Leite Junior, Daniel Schneider and Rasmus Adler

12:00-12:30 Towards (semi-)automated synthesis of runtime safety models: A safety-oriented design approach for service architectures of cooperative autonomous systems;
by Jan Reich and Daniel Schneider

12:30-13:30 Lunch break

SESSION 3: Safety & Cybersecurity Systems Engineering

13:30-14:00 Co-Engineering-in-the-Loop;
by Thomas Gruber, Christoph Schmittner, Martin Matschnig and Bernhard Fischer

14:00-14:30 STPA Guided Model-Based Systems Engineering;
by Uwe Becker

14:30-15:00 A Quantitative Approach for the Likelihood of Exploits of System Vulnerabilities;
by Siddhartha Verma, Thomas Gruber, Peter Puschner, Christoph Schmittner, and Erwin Schoitsch

15:00-15:30 Safety and Security in a Smart Production Environment;
by Reinhard Kloibhofer, Erwin Kristen and Stefan Jakšić

15:30-16:00 Coffee break

SESSION 4: Dependability of Advanced Networks/IoT

16:00-16:30 Survey of Scenarios for Measurement of Reliable Wireless Communication in 5G;
by Matthias Herlich, Thomas Pfeiffenberger, Jia Lei Du and Peter Dorfinger

16:30-17:00 Application of IEC 62443 for IoT Components;
by Abdelkader Shaaban, Erwin Kristen and Christoph Schmittner

17:00-17:30 Dependable Outlier Detection in Harsh Environments Monitoring Systems;
by Goncalo de Jesus, António Casimiro and Anabela Oliveira

Workshop Program

SASSUR — 7th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems

Room: 110

9:30-9:35 Welcome

KEYNOTE TALK by Thor Myklebust

9:35-10:30 Evolutionary development and frequent releases of safety systems.
Thor Myklebust (SINTEF, Norway)

10:30-11:00 Coffee break

Paper presentation & discussion (1)

11:00-12:30 - Fault Trees vs. Component Fault Trees: An Empirical Study.
Tim Gonschorek, Marc Zeller, Frank Ortmeier, and Kai Höfig.

- Comparing Risk Identification in Hazard Analysis and Threat Analysis.
Hideaki Nishihara and Kenji Taguchi

12:30-13:30 Lunch break

Paper presentation & discussion (2)

13:30-15:30 - Towards Risk Estimation in Automated Vehicles using a Fuzzy System.
Leonardo Gonzalez, Enrique Martí, Isidro Calvo, Alejandra Ruiz, and Joshue Perez.

- Integration Analysis of a SEooC Transmission Unit for Automated Driving Vehicles.
Georg Macher, Markus Bachinger, Andreas Kager, Michael Stolz, and Christian Kreiner.

- In Search of Synergies in a Multi-Concern Development Lifecycle: Safety and Cybersecurity.
Martin Skoglund, Fredrik Warg, and Behrooz Sangchoolie.

15:30-16:00 Coffee break

Paper presentation & discussion (3)

16:00-16:45 - Challenges in Assuring Highly Complex, High Volume Safety-Critical Software.
John Macgregor and Simon Burton

Industrial Panel: Trends and Needs for Future Assurance of Safety-Critical Systems

16:45-17:45 **Panelists**:

- Lauren Fabre (Critical Systems Labs, Canada)

- Javier Ibañez-Guzmán (Renault, France)

- Thor Myklebust (SINTEF, Norway)

17:45-18:00 Closing

Workshop Program

ASSURE — 6th International Workshop on Assurance Cases for Software-intensive Systems

Room: 108

08:00-09:00 Registration

SESSION 1: Introduction, Keynote, and Confidence Assessment

09:00-09:10 Welcome and Introduction

ASSURE 2018 Organizers

KEYNOTE TALK by Robin Bloomfield

09:10-10:00 Assurance Cases: Mindsets, Methodologies, and Convergence.
Robin Bloomfield (Adelard LLP, and City University, London)

10:00-10:30 Research on the Classification of the Relationships Among the SameLayer Elements in Assurance Case Structure for Evaluation.
Biao Xu, Minyan Lu, Tingyang Gu and Dajian Zhang.

10:30-11:00 Coffee break

SESSION 2: Patterns and Processes

11:00-11:30 The Assurance Recipe: Facilitating Assurance Patterns.
Justin Firestone and Myra Cohen.

11:30-12:00 Incorporating Attacks Modeling into Safety Process.
Amer Surkovic, Dzana Hanic, Elena Lisova, Aida Causevic, Kristina Lundqvist, David Wenslandt and Carl Falk.

12:00-12:30 Assurance Case Considerations for Interoperable Medical Systems.
Yi Zhang, Brian Larson and John Hatcliff.

12:30-13:30 Lunch break

SESSION 3: Tools and Automation

13:30-14:00 Two Decades of Assurance Case Tools: A Survey.
Mike Maksimov, Nick Fung, Sahar Kokaly and Marsha Chechik.

14:00-14:30 MMINT–A: A Tool for Automated Change Impact Assessment on Assurance Cases.
Nick Fung, Sahar Kokaly, Alessio Di Sandro, Rick Salay and Marsha Chechik.

14:30-15:00 D–Case Steps: New Steps for Writing Assurance Cases.
Yuto Onuma, Toshinori Takai, Tsutomu Koshiyama and Yutaka Matsuno.

15:00-15:30 Continuous Argument Engineering: Tackling Uncertainty in Machine Learning based Systems.
Fuyuki Ishikawa and Yutaka Matsuno.

15:30-16:00 Coffee break

SESSION 4: PANEL – What are Assurance Case Tools For?

16:00-17:15 The panel discussion

17:15-17:30 Conclusion and Wrap–Up
ASSURE2018 Organizers

Workshop Program

STRIVE — 1st International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms

Room: 107

08:00-09:00 Registration Desk

09:15-09:30 Opening

KEYNOTE TALK by Mathias Johanson

09:30-10:30 Connected vehicles: challenges and opportunities.
Mathias Johanson

10:30-11:00 Coffee break

SESSION 1: In-vehicle Security

11:00-12:30 - Counter Attacks for Bus-off Attacks.
Daisuke Souma, Akira Mori, Hideki Yamamoto and Yoichi Hata.

- Applications of pairing-based cryptography on automotive-grade microcontrollers.
Tudor Sebastian Andreica, Bogdan Groza and Pal-Stefan Murvay.

- Towards an Integrated Penetration Testing Environment for the CAN Protocol.
Giampaolo Bella and Pietro Biondi.

12:30-14:00 Lunch break

SESSION 2: Security in Vehicular Infrastructure

14:00-15:30 - Enhancing sensor capabilities of open-source simulation tools to support autonomous vehicles safety validation.
C.B.S.T. Molina, L.F. Vismari, T.Y. Fujii, J.B. Camargo Jr, J.R. de Almeida Jr, Rafia Inam, Elena Fersman, A. Hata and M.V. Marquezini.

- A security analysis of the ETSI ITS vehicular communications.
Alexandru Serban, Erik Poll and Joost Visser.

- Real-Time Driver Behaviour Characterization through Rule-based Machine Learning.
Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone and Gigliola Vaglini.

15:30-16:00 Coffee break

16:00 End of the Workshop

Workshop Program

WAISE — 1st International Workshop on Artificial Intelligence Safety Engineering

Room: 109

08:00-08:30 Registration Desk

KEYNOTE TALK by Philip Koopman (Chair: Huascar Espinoza)

08:30-09:30 Autonomous Vehicle Safety Technical and Social Issues. *Prof. Philip Koopman*

SESSION 1: Machine Learning Safety and Reliability (Chair: Orlando Avila-García)

09:30-10:30
- «Boxing Clever»: Practical Techniques for Gaining Insights into Training Data and Monitoring Distribution Shift, *Rob Ashmore and Matthew Hill*
- Mitigation of Policy Manipulation Attacks on Deep Q-Networks with Parameter-Space Noise, *Vahid Behzadan and Arslan Munir*
- What is Acceptably Safe for Reinforcement Learning?, *John Bragg and Ibrahim Habli*
- Debate Panel - Paper Discussants: *Jin Zhang, Rob Ashmore*

10:30-11:00 Coffee break

SESSION 2: Uncertainty in Automated Driving (Chair: Timo Latvala)

11:00-12:20
- Uncertainty in Machine Learning Applications - A Practice-Driven Classification of Uncertainty, *Michael Kläs and Anna Maria Vollmer*
-Towards a Framework to Manage Perceptual Uncertainty for Safe Automated Driving, *Krzysztof Czarnecki and Rick Salay*
- Design of a Knowledge-Base Strategy for Capability-Aware Treatment of Uncertainties of Automated Driving Systems, *Dejiu Chen, Kenneth Östberg, Matthias Becker, Håkan Sivencrona and Fredrik Warg*
- Uncertainty in Machine Learning: A Safety Perspective on Autonomous Driving, *Sina Shafaei, Stefan Kugele, Mohd Hafeez Osman and Alois Knoll*
- Debate Panel - Paper Discussants: *Hari Balaji*

12:20-13:20 Lunch - Poster Sessions

INVITED TALK by François Terrier (Chair: Orlando Avila-García)

13:20-13:50 Challenges in the Qualification of Safety-Critical Machine Learning-based Components, *Prof. François Terrier*

SESSION 3: Challenges in AI Safety (Chair: Rob Ashmorev)

13:50-14:50
- Considerations of Artificial Intelligence Safety Engineering for Unmanned Aircraft, *Sebastian Schirmer, Christoph Torens, Florian Nikodem and Johann Dauer*
- Could We Issue Driving Licenses to Autonomous Vehicles?, *Jingyue Li, Jin Zhang and Nektaria Kaloudi*
- Concerns on the differences between AI and system safety mindsets impacting autonomous vehicles safety, *Alexandre Moreira Nascimento, Lucio Vismari, Paulo Cugnasca, Joao Camargo Jr., Jorge Almeida Jr., Rafia Inam, Elena Fersman, Alberto Hata and Maria Marquezini*
- Debate Panel - Paper Discussants: *Huascar Espinoza*

SESSION 4: Ethically Aligned Design of Autonomous Systems (Chair: Rob Alexander)

14:50-15:30
- The Moral Responsibility Gap and the Increasing Autonomy of Systems, *Zoe Porter, Ibrahim Habli, Helen Monkhouse and John Bragg*
- Design Requirements for a Moral Machine for Autonomous Weapons, *Ilse Verdiesen, Virginia Dignum and Iyad Rahwan*
- Debate Panel - Paper Discussants: *Orlando Avila-Garcia*

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

SESSION 5: Human-Inspired Approaches to AI Safety (Chair: Andreas Theodorou)

16:00-17:00 - AI Safety and Reproducibility: Establishing Robust Foundations for the Neuropsychology of Human Values, *Gopal Sarma, Nick Hay and Adam Safron*

- A Psychopathological Approach to Safety Engineering in AI and AGI, *Vahid Behzadan, Arslan Munir and Roman Yampolskiy*

- Why Bad Coffee? Explaining Agent Plans with Valuings, *Michael Winikoff, Virginia Dignum and Frank Dignum*

- Debate Panel - Paper Discussants: *Ilse Verdiesen*

SESSION 6: Runtime Risk Assessment in Automated Driving (Chair: Jérémie Guiochet)

17:00-17:40 - Dynamic Risk Assessment for Vehicles of Higher Automation Levels by Deep Learning, *Patrik Feth, Mohammed Naveed Akram, René Schuster and Oliver Wasenmüller*

- Improving Image Classification Robustness using Predictive Data Augmentation, *Harisubramanyabalaji Subramani Palanisamy, Shafiq Ur Rehman, Mattias Nyberg and Joakim Gustavsson*

- Debate Panel - Paper Discussants: *Timo Latvala*

17:40-18:00 Wrap-up - Best Paper Award

General Information

VENUE: The conference will be held at Aros Congres Center (http://acc.se/). Aros Congress Center is one of Sweden's leading conference centres and it is situated in the city centre, just a stone's throw from Västerås Central Station and in the immediate vicinity of shops, restaurants and the concert hall.

Aros Congress Center
Munkgatan 7
722 12 Västerås
Sweden

ACC accessibility information available at https://www.acc.se/en/facilities/accessibility/

REGISTRATION DESK: All participants are requested to check in at the Registration Desk. The registration will be open every day from 08:00 until 18:00. The Registration Desk is located on the first floor (PLAN 1 in the ACC floor plan on the next page).

BADGE/TICKETS: All participants will receive a personal badge upon registration. Please wear the badge throughout the entire conference, including all sessions and social events. It will be easier for the staff to recognize you as a SAFECOMP participant.

Tickets are required for the visit to Munktellmuseet for the conference dinner on Thursday. These will be handed out during registration. Please bring your ticket for boarding the bus.

LUNCHES AND COFFEE BREAKS: Coffee and lunches are included in the registration fees. Coffee breaks will be held on the first floor, next to the Registration Desk. The lunch will be served on the ground floor in the restaurant hall located opposite of the main entrance door. Please see the floor plan of ACC on the next page.

WIFI information:
SSID: ACC WIRELESS
PASSWORD: 0211011000

CONTACTS: For any information or assistance during the event please refer to the STAFF members or contact:

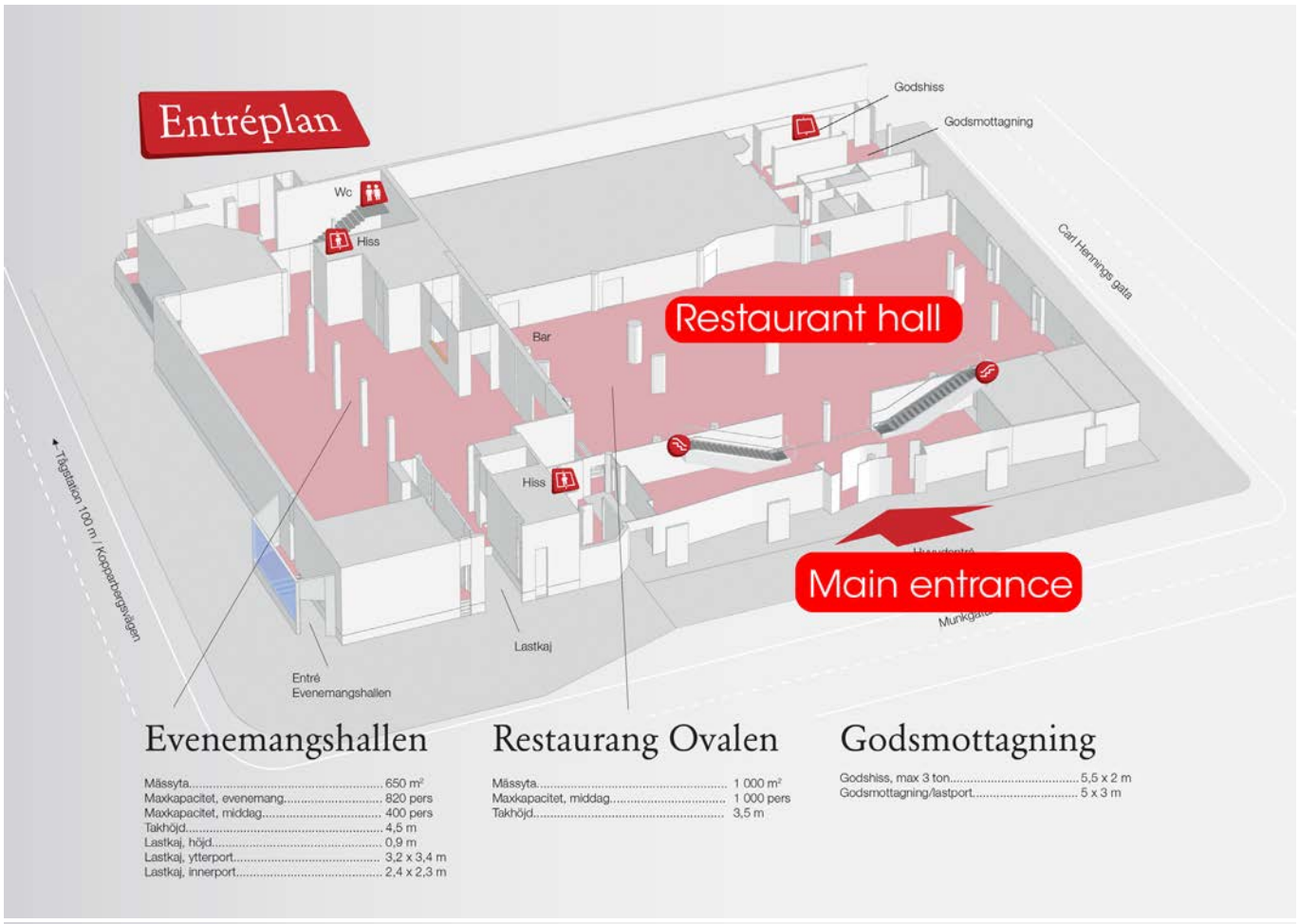
safecomp18@mdh.se
Tel.: +46-21-10 14 05

Additional useful numbers:
ACC reception: +46 21 10 11 00
Emergency number: 112

LIABILITY: The Organizing Committee cannot accept any responsibility for personal accidents or loss/damage of private property of participants (e.g.: luggage left at the reception desk). Participants are advised to take out insurance as they consider necessary.

LOST AND FOUND: For lost and found objects please go to the SAFECOMP Registration Desk or the ACC reception desk located opposite of the wardrobe and the Registration Desk.

Conference Venue Floor Plan



Evenemangshallen

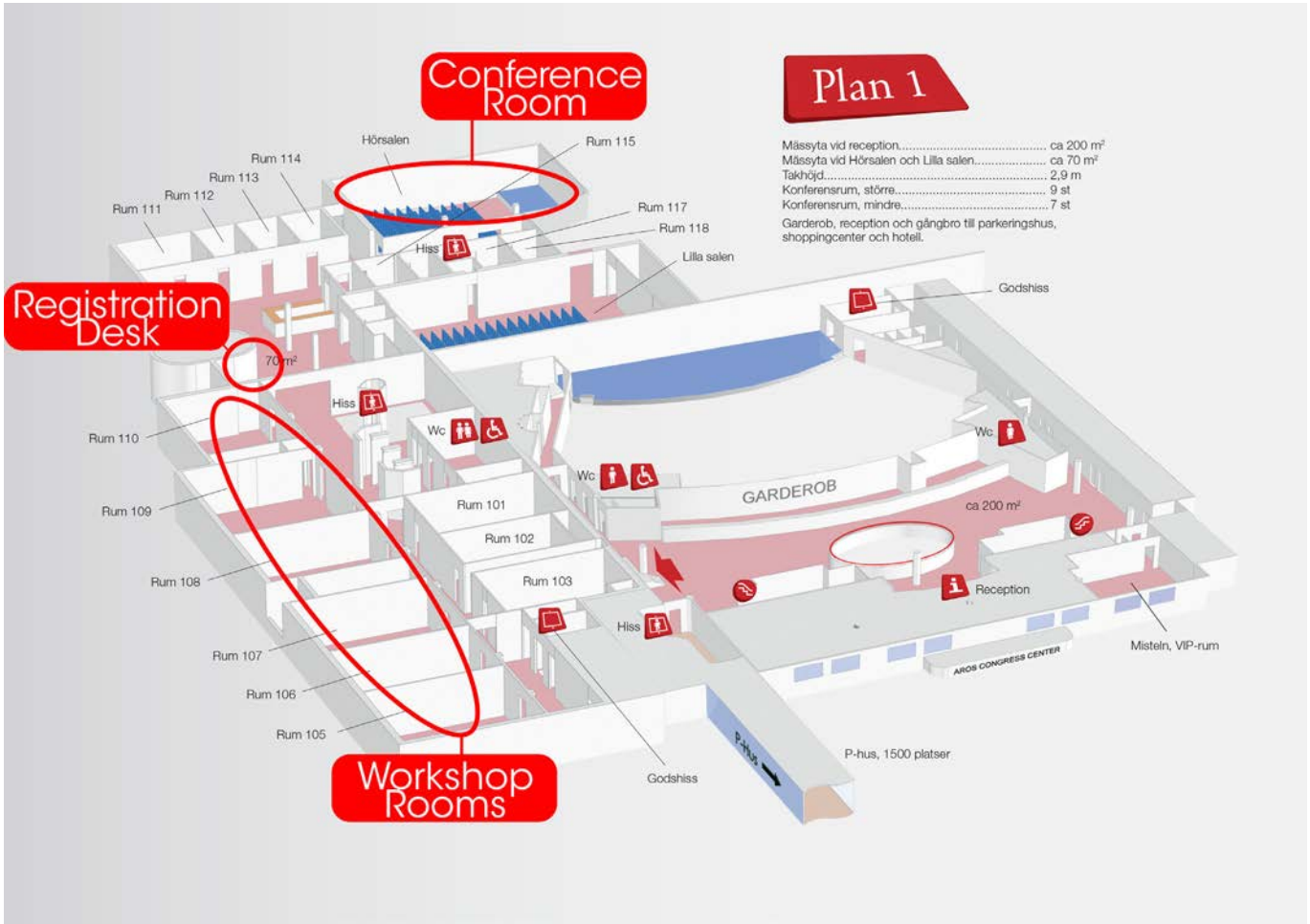
Mässyta	650 m²
Maxkapacitet, evenemang	820 pers
Maxkapacitet, middag	400 pers
Takhöjd	4,5 m
Lastkaj, höjd	0,9 m
Lastkaj, ytterport	3,2 x 3,4 m
Lastkaj, innerport	2,4 x 2,3 m

Restaurang Ovalen

Mässyta	1 000 m²
Maxkapacitet, middag	1 000 pers
Takhöjd	3,5 m

Godsmottagning

Godshiss, max 3 ton	5,5 x 2 m
Godsmottagning/lastport	5 x 3 m



Plan 1

Mässyta vid reception	ca 200 m²
Mässyta vid Hörsalen och Lilla salen	ca 70 m²
Takhöjd	2,9 m
Konferensrum, större	9 st
Konferensrum, mindre	7 st

Garderob, reception och gångbro till parkeringshus, shoppingcenter och hotell.

MÄLARDALEN UNIVERSITY SWEDEN

Social Events

GUIDED CITY TOUR

WHEN

Wednesday 19th September 2018, 18:30 – 19:30

WHERE

We start in front of Aros Congress Center

Munkgatan 7, 772 12 Västerås, Sweden

DETAILS

We divide in 2 groups in front of the ACC and each group follows their tour guide around the city. We finish the tour in front of Hotel Plaza where you can join for the welcome reception.

WELCOME RECEPTION AT HOTEL PLAZA

WHEN

Wednesday 19th September 2018, 19:30

ADDRESS

Kopparbergsvägen 10, 722 13 Västerås, Sweden

HOW TO GET THERE

1 minute walking from Aros Congress Center

Social Events

VISIT TO MUNKTELLMUSEET: GUIDED TOUR AND DINNER

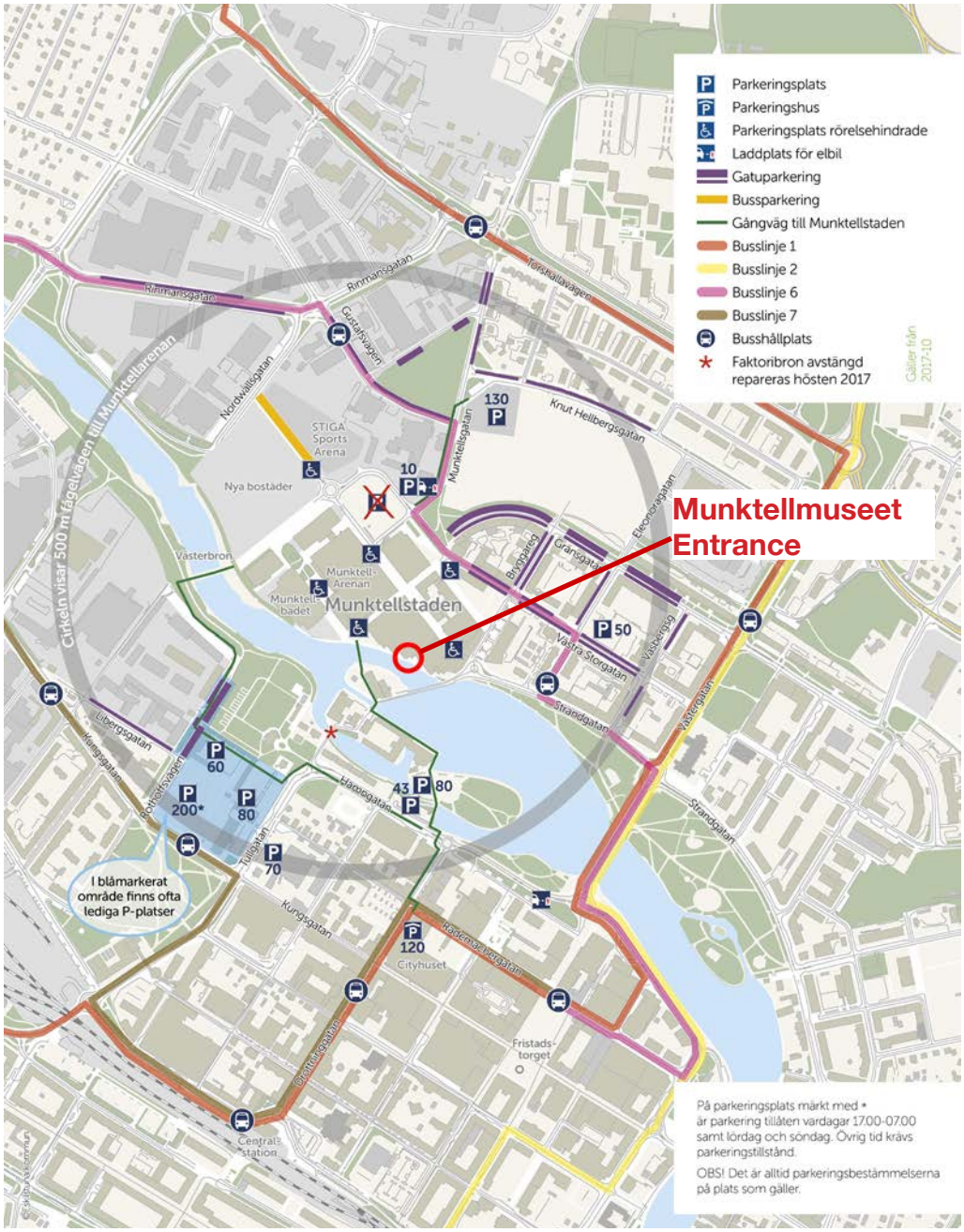
WHEN

Thursday 20th September 2018

HOW TO GET THERE

The bus will start from Aros Congress Center at 17:45.
The Munktellmuseet visit will start at 18:30 with mingling.
The conference dinner starts at 20:00. If you plan to reach Munktellmuseet by car (around 40 minutes from ACC):

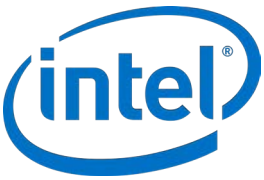
Visit address: Munktellstorget, 633 43 Eskilstuna, Sweden
GPS coordinates:
RT90: X: 6584191, Y: 1540061
WGS84: Lat N 59° 22′ 35″ Lon E 16° 30′ 35″
Decimal: 59.3765, 16.5099



SAFECOMP 2018 Partners

Custom Sponsors

Silver Sponsors



Bronze Sponsors