

Workshop on Safety Critical Systems and AI

Date: 2024-10-28

Time: 9:00 AM - 5:00 PM

Location: Mälardalen University in Västerås, Room: Beta

The Trusted Smart Systems strategic profile area at MDU is pleased to in collaboration with the Competence Centre CoDig invite you to a one-day workshop on **Safety Critical Systems and AI**. Join us for a one-day workshop that brings together leading academic researchers and industry experts to explore the latest advancements and challenges in this crucial field.

This is a free-of-charge event, including lunch and refreshments.

Registration required: [link to registration page](#)

Unlock the Future of Safety-Critical Systems with AI

The intersection of artificial intelligence (AI) and safety-critical systems represents both a challenge and a transformative opportunity. As AI technology rapidly advances, its integration into systems that society relies on—such as autonomous vehicles, healthcare, and industrial automation—brings forth critical questions about safety, reliability, and trust. How can we harness the potential of AI while ensuring that these systems remain secure and resilient?

This event will delve into three core themes:

- **AI and Safety:** Assess the dual nature of AI in safety-critical systems. We will explore how AI can both enhance and pose risks to safety in various domains, including autonomous vehicles, industrial systems, and healthcare.
- **AI and Cybersecurity:** Discover how AI is reshaping the cybersecurity landscape, potentially enhancing defenses while also introducing new vulnerabilities.
- **Trustworthy AI in Society:** Engage in discussions about the ethical, legal, and societal implications of AI, and what it means to develop systems that are not only effective but also trustworthy and aligned with societal values.

The workshop features keynote addresses from prominent experts, breakout sessions tailored to each theme, and a closing panel that will synthesize the insights and propose pathways forward.

Why Attend?

- **For Researchers:** Connect with peers, gain insights into the latest research, and explore collaborative opportunities in AI and safety-critical systems.
- **For Industry Professionals:** Learn about cutting-edge research that could impact your industry, discuss practical challenges, and network with leading academics and other industry leaders.

Don't miss this opportunity to contribute to shaping the future of AI in safety-critical systems. Together, we can navigate the complexities and ensure that AI serves as a force for good in society.

Agenda:

Morning Session:

- **9:00 - 9:20:** Registration and Welcome Coffee
- **9:20 - 9:30:** Opening address
- **9:30 - 10:15: “Automotive safety standards for AI and related open issues”**
Keynote by Prof. Simon Burton, U. of York
- **10:15 - 10:35: “AI in critical systems – a business sector perspective”**
Mikaela Näslund, Vice President Research & Development, Westermo
- **10:35 - 10:55: “Ensuring AI Integrity: The Critical Role of Reliability, and Validation”**
Prof. Masoud Daneshtalab, MDU
- **10:55 - 11:15:** Coffee Break
- **11:15 - 11:35: “Open challenges in cybersecurity”**
Prof Kai Rannenber, Goete U. Frankfurt
- **11:35 - 11:55: “Confidential AI”** Prof. Shahid Raza, MDU
- **11:55 - 12:15: “AI - what may be its (unintended) societal consequences?”**
Prof. Jonas Stier, MDU
- **12:15 - 12:35:** Speaker 7 (to be announced) – 2nd presentation on societal implications
- **12:35 - 13:30:** Lunch Break

Afternoon Session:

- **13:30 - 15:00:** Breakout Session 1: AI and Safety
- **13:30 - 15:00:** Breakout Session 2: AI and Cybersecurity
- **13:30 - 15:00:** Breakout Session 3: Trustworthy AI in Society
- **15:00 - 15:30:** Coffee Break
- **15:30 - 16:45:** Panel Discussion:
Where do we go from here? - Insights and findings from Breakout Sessions
- **16:45 - 17:00:** Closing Remarks

About the speakers



Simon Burton holds the chair of Systems Safety at the University of York, UK and is the Business Director of the Centre for Assuring Autonomy. He achieved his PhD on the topic of the verification of safety-critical software in 2001. Professor Burton has worked in various safety-critical industries, including 20 years managing R&D organisations in automotive companies. More recently, he was Scientific Director for Safety Assurance at the Fraunhofer Institute for Cognitive Systems (Fraunhofer IKS) until December 2023. Professor Burton is convener of the ISO working group ISO TC22/SC32/WG14 “Road Vehicles—Safety and AI”.



Masoud Daneshtalab is professor at Mälardalen University, specializing in algorithm-hardware co-design, embedded-friendly and reliable AI, and interconnection networks. He has made significant contributions to AI, system architectures, and reliability, earning prestigious awards such as the Marie Skłodowska-Curie Fellowship and multiple research grants. His collaborations with leading companies like Saab, Volvo, Ericsson, and Scania highlight his ability to bridge academic research with industry needs. Masoud has authored over 200 publications and has developed open-source tools that enhance AI reliability and performance, especially in safety-critical systems.



Mikaela Näslund is an experienced executive with over 25 years in management and project leadership across global companies. Currently serving as Vice President of R&D at Westermo AB, she manages an international team of 150 developers. Previously, she held senior roles at Mycronic AB, overseeing a workforce of 400 across nine countries. Mikaela holds a Master of Science in Mechanical Engineering from KTH and an MBA from Uppsala University. She specializes in driving innovation in industrial communication solutions and advancing global platform development.



Kai Rannenberg holds the Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt since 2002 and is a Visiting Professor at the National Institute for Informatics (Tokyo) since 2012. He achieved his PhD at Freiburg University on IT Security Evaluation Criteria and the protection of users and subscribers in 1998. Until 2002 Kai was working with the System Security Group at Microsoft Research Cambridge on „Personal Security Devices & Privacy Technologies“. Since 1991 Kai is active in ISO/IEC standardization, first in JTC 1/SC 27/WG 3 “Security evaluation criteria”. 2007 he became Convenor of SC 27/WG 5 “Identity management and privacy technologies”.



Shahid Raza is a cybersecurity expert specializing in IoT Security and serves as Chair Professor of Cybersecurity at the University of Glasgow, UK. He is also affiliated with Mälardalen University (MDU), Sweden, as a Professor in Cybersecurity, and with RISE Sweden as Research Director of Cybersecurity. Previously, Shahid led the Cybersecurity Unit at RISE Sweden, establishing it as one of Sweden's largest technical cybersecurity groups. He co-founded Cybercampus Sweden (cybercampus.se), the RISE Cyber Range, and the Swedish Cybersecurity Research and Innovation Node (cybernodel.se). He holds a Swedish Docentship from Uppsala University, a PhD from Mälardalen University, and an MSc from KTH, all in cybersecurity.



Jonas Stier is a sociologist and a professor of social work at Mälardalen University in Sweden. His research mainly revolves around identity, diversity, intercultural interactions, and the digital transformation of society and people. Stier has a long track-record of collaboration and co-creation with civil society, industry and the public sector, for instance within the Horizon 2020-project *Accomplishh*. Moreover, he has held two professorships in intercultural studies and sociology and is one of the founders of addai.org – a policy initiative on artificial intelligence.