# NTNU CCIS and SFI NORCICS Joint Conference 2024

November 21st 2024, Clarion Hotel The Hub Oslo

**Program:**

| Time | Description/title |
|---|---|
| 08:30 - 09:00 | **Registration, coffee, exhibition, mingling** |
| 09:00 - 09:30 | **Welcome**<br>Ingrid Schjølberg, Dean Faculty of Information Technology and Electrical Engineering NTNU, Chair of the CCIS and NORCICS Boards<br>Basel Katt, Head of Department of Information Security and Communication Technology NTNU<br>Peggy Sandbekken, Director NTNU CCIS<br>Sokratis Katsikas, Professor NTNU and Centre Director SFI NORCICS |
| 09:30 - 09:50 | **Keynote: *A unified approach to cyber-physical testing***<br>Jon Leistad, Senior Project Manager/Coordinator EDF project FACT, Kongsberg Defence & Aerospace |
| 09:50 - 10:10 | **Group work: *Cybersecurity testing in the merged cyber and physical spaces*** |
| 10:10 - 10:30 | Summary in plenary by selected groups |
| 10:30 – 11:00 | **PhD/PostDoc/Researcher pitches** |
| 11:00 - 11:30 | Exhibition, coffee, mingling |
| 11:30 - 12:20 | Lunch break |
| 12:20 - 12:40 | **Keynote: *How may cybersecurity risks impact the design of safety instrumented systems?***<br>Mary Ann Lundteigen, Professor Engineering Cybernetics NTNU |
| 12:40 - 13:00 | **Group work: *Exploring the Interplay of Safety, Security, Reliability and Resilience in IT-OT integration*** |
| 13:00 - 13:20 | Summary in plenary by selected groups |
| 13:20 - 13:30 | Technical break |

| | |
|---|---|
| 13:30 - 13:50 | **Keynote:** ***Is evaluating emerging threats in an objective way possible? Practical lessons from the world of critical infrastructure***<br>Izabela Hawrylko, Head of Customer Success, Omny Security |
| 13:50 - 14:10 | **Group work:** ***Secure Industry 5.0 and Industry 6.0: Identifying Emerging Threats and Addressing Needs*** |
| 14:10 - 14:30 | Summary in plenary by selected groups |
| 14:30 - 14:50 | Coffee break |
| 14:50 - 15:10 | **Keynote:** ***Can we trust AI?***<br>Nikolaos Pitropakis, Associate Professor of Cyber Security Edinburgh Napier University |
| 15:10 - 15:30 | **Group work:** ***Trustworthy AI: Balancing Benefits and Risks in Critical Sectors*** |
| 15:30 - 15:50 | Summary in plenary by selected groups |
| 15:50 - 16:00 | Closing remarks |

NTNU Center for Cyber and Information Security

NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU CCIS and SFI NORCICS Joint Conference 2024

November 21st 2024, Clarion Hotel The Hub Oslo

## Presentation of keynotes

**Keynote: *A unified approach to cyber-physical testing***

**Jon Leistad**
*Senior Project Manager/Coordinator EDF project FACT, Kongsberg Defence & Aerospace*

**Abstract:**
As cyberattacks grow more sophisticated, both traditional IT systems and operational technology (OT) are increasingly targeted. Cyber-physical systems (CPS), which integrate computational and physical processes, enhance efficiency and safety in sectors like industrial automation, transportation, energy, healthcare, and defense.
CPS use sensors, software, and actuators to monitor and control the physical world via continuous feedback. However, they face unique cybersecurity risks, with breaches potentially causing significant real-world damage. Cyber-physical testing is crucial for identifying vulnerabilities and ensuring CPS reliability and resilience against cyber threats, vital for public safety and national security.
This presentation advocates for a unified approach to cyber-physical testing across industries. The Federated Advanced Cyber Physical Test range (FACT) project, funded by the European Defence Fund, aims to bolster Europe's ability to assess cyber vulnerabilities in defense equipment. FACT seeks to develop a shared testing "toolbox" with a common architecture and federated environment for critical sectors, enhancing cyber resilience and national security.

**Bio:**
Jon Leistad is a seasoned professional with over 30 years of experience in the military, holding various positions from troop level to enterprise management in the Norwegian Defense Staff. In previous positions, Jon has contributed to developing Defence IT strategy, governance, and operational models. Jon has held several senior staff officer positions, leading analysis work and (IT) strategy implementation processes.
Currently, Jon serves as a Senior Project Manager at Kongsberg Defence and Aerospace (KDA), where he started in November 2023. His primary responsibility is coordinating the EDF project FACT. Jon's educational background includes a Master's level education from the Swedish Defense University, NATO Defense College, and various other military courses.

**Keynote:** ***How may cybersecurity risks impact the design of safety instrumented systems?***

**Mary Ann Lundteigen**
*Professor Engineering Cybernetics, NTNU*

**Abstract:**
Safety-instrumented systems (SIS) are vital for preventing major accidents at process facilities. Their primary function is to detect and respond to hazardous events and ensure the plant enters a safe state. Also, the SIS systems must be independent so that they are not adversely affected by other systems. Ensuring the latter capability can be more challenging with the increased OT and IT integration. Lack of independence can be a vulnerability that an attacker may exploit.

This talk provides more insight into SIS systems' role, requirements, design, and operational principles. It discusses the relationship between cybersecurity attacks and their potential to violate safety, supported by some practical examples. The aim is knowledge exchange and to stimulate discussion on how we best can maintain vital functionalities of SIS systems in case of cyber-attacks, considering also engineering measures.

**Bio:**
Mary Ann Lundteigen is a professor in instrumentation systems and functional safety at the Department of Engineering Cybernetics at the Norwegian University of Science and Technology (NTNU). Her background combines 15+ years of industrial experience with academic activities in safety instrumented systems, safety and reliability analysis, cybersecurity from the safety perspective, and adopting industry 4.0 solutions. Two examples of research activities are within the APOS project on automated follow-up of safety systems and the cyberbarrier management project (CBM) project. She has an MSc in Engineering Cybernetics from the Norwegian Institute of Technology (NTH) (1993) and received her Ph.D. in Reliability, Availability, Maintainability, and Safety at NTNU (2009). She is involved in standardization work related to IEC 61511 (on functional safety for the process industry), NEK AG1 (on cybersecurity), and ISA 84 WG10 (on digitalization of functional safety). In Norway, she is part of the organizing committee of the PDS forum, CDS forum, and the AAS forum.

**Keynote:** ***Is evaluating emerging threats in an objective way possible? Practical lessons from the world of critical infrastructure***

**Izabela Hawrylko**
*Head of Customer Success, Omny Security*

**Abstract**:
For decades researchers and practitioners within the field of risk analysis have been on a dangerous journey in search of their Holy Grail - the one and only, accurate and objective way of assessing risks that organizations and their crown jewels are exposed to. Many years and methodologies later, the industrial world is still relying on a 5x5 matrix with risks assigned green, yellow and red depending on the daily form of the members of the risk committee.
Why are we still doing risk analysis the way “we have always done it”? And most importantly, what can we do about it to help improve the risk posture of our organizations? The reflections and ideas you will hear are not from a perspective of a risk SME. They are a condensed version of insight coming from many discussions with industrial organizations as well as own experience.

**Bio**:
Izabela Hawrylko is a Head of Customer Success and Delivery at Omny, an industrial security technology company founded by Aker, Telenor and Cognite. Hawrylko has been part of the company since its early days and responsible for its partnership and ecosystem strategy as well as business development.Prior to joining Omny back in 2022, Hawrylko worked at Cognite as a Director for Partner Development and Microsoft, where she supported Norwegian enterprises in adopting data platform and analytics technologies.Hawrylko brings into the discussion the voice of industrial organisations that have to adopt new technologies to defend themselves from threats amplified by the same technologies. Her perspective is anchored in an understanding of the American tech world combined with an over 10 years of experience from working in and with innovation and startup ecosystems across Norway, Germany and Poland.

**Keynote: *Can we trust AI?***

**Nikolaos Pitropakis**
*Head Of Cybersecurity and Systems Engineering Subject Group*
*Associate Professor of Cyber Security*
*Edinburgh Napier University*

**Abstract:**
Our modern lives are filled with devices and services that utilize Artificial Intelligence (AI) and Machine Learning (ML) to enhance performance and meet our needs. However, this widespread adoption has made ML-based systems vulnerable to attacks, where malicious actors manipulate training or test data to degrade system performance. This talk outlines the threat landscape of such adversarial attacks and uses different case studies to illustrate how these attacks manifest and their potential impact on ML systems.

**Bio:**
Dr. Nikolaos Pitropakis is an Associate Professor of Cybersecurity at Edinburgh Napier University and Head of the Cybersecurity and Systems Engineering Subject Group. He is a Fellow of the Higher Education Academy and a core member of the Blockpass Identity Lab. His research focuses on adversarial machine learning, trust and privacy using distributed ledger technologies, cyberattack attribution, and IoT security. He leads the BSc Cyber Security apprenticeship programme, the first in the UK to receive full NCSC accreditation, and serves as an external examiner for cybersecurity programmes at institutions like the American College of Greece and Northumbria University. His recent work has included £310,843 for the EU TRUSTEE project and over £500,000 through Edinburgh Napier's latest spinout TRUEDEPLOY. He collaborates with leading global institutions, including NTNU, and has published over 80 scholarly articles. A frequent speaker at conferences, he has received multiple awards for his research and supervises PhD students, with several achieving significant success in the cybersecurity industry.