NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Selected NORCICS Results

NTNU CCIS and SFI NORCICS Joint Conference 2025 November 18-19 2025

Stephen Wolthusen (stephen.wolthusen@ntnu.no)

NTNU | Norwegian University of Science and Technology

Research Results and Applications

NORCICS is now in its second half-period and has produced a number of interesting results as well as successful Ph.D. graduates (or those about to finish)

The collaborations with partners allowed graduates to combine academic insights with domain knowledge, helping to bridge an important gap

Research has resulted in publications and academic recognition, but this is not the main focus of the examples presented here

Research is led by academic colleagues but we highlight the contributions of several (but not all) Ph.D. candidates and postdoctoral researchers

Knowledge Transfer

Smaller entities such as SMEs and public sector bodies like municipal governments are just as likely to be direct victim of attacks or vulnerable through dependencies and supply chains

As part of T4.3, **Arnstein Vestad** analysed incidents and capabilities, developing a framework for understanding actual capabilities and challenges

- Legal and regulatory requirements by themselves are insufficient with limited practices and competence network particularly where rapid developments occur
- Public Ph.D. Viva Voce 20/11/2025 at NTNU (G144) and online

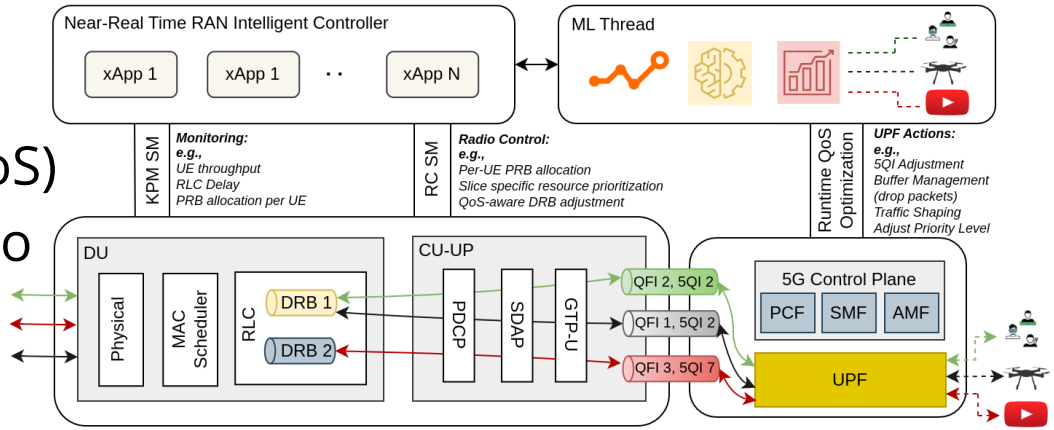
Enabling Critical Infrastructure Applications (1)

Applications in industry and critical sectors such as drones and UAV/UGV or industrial control benefit from low-latency networks

In 5G/6G networks, traffic with different priority levels are not always possible or practical to subject to hard prioritization schemes

Work by **Suneet Singh** shows that it is possible to use AI/ML techniques to classify traffic and assign quality of service (QoS)

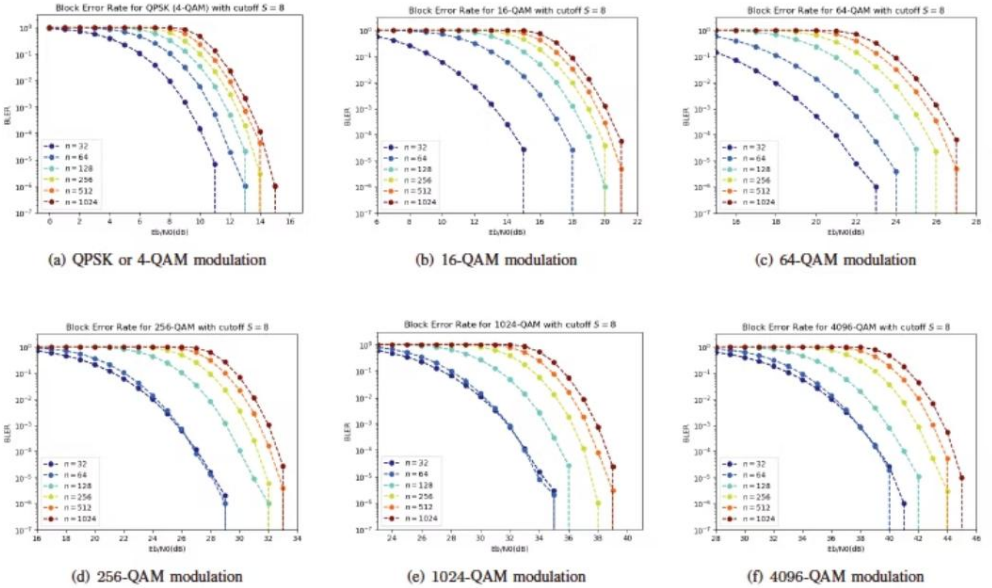
- This information can be used to inform behaviour of the radio access network



Enabling Critical Infrastructure Applications (2)

Critical services running over 5G/6G networks will inevitably need cryptographic protection, but with **low latency**

Work by **Sahana Sridhar**, Daniel Gligoroski and Katina Kralevska reduces the error pattern space of a decoding function and parallelism to minimise latency - allowing decoding in constant (wall) time, which also reduces susceptibility to *side channel attacks*



(a) QPSK or 4-QAM modulation (b) 16-QAM modulation (c) 64-QAM modulation

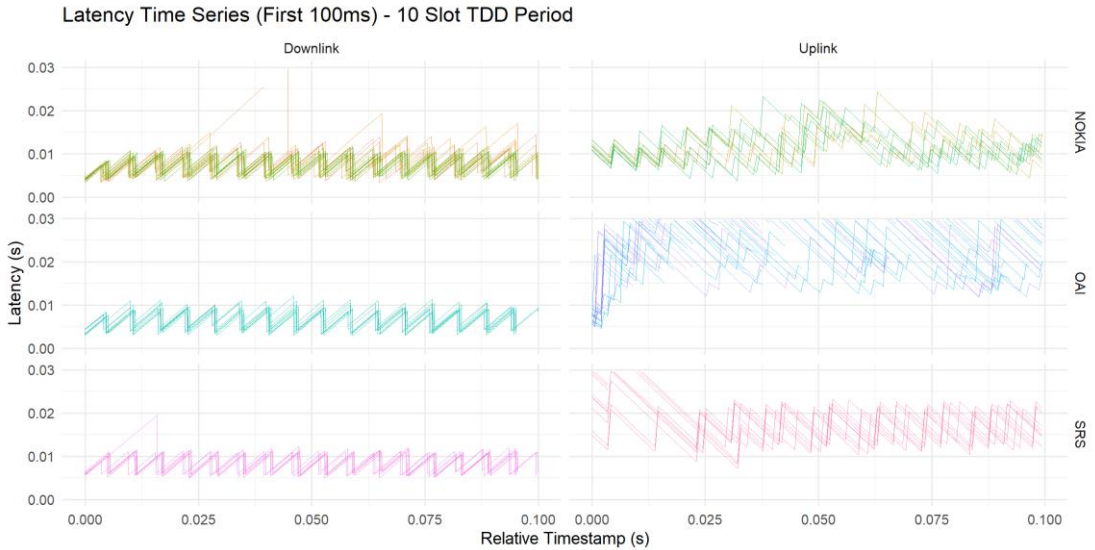
(d) 256-QAM modulation (e) 1024-QAM modulation (f) 4096-QAM modulation

From Laboratories to Insights (1)

5G/6G networks can use both public but also private networks (such as in industrial settings) - Work by **Sebastian Grøsvik** investigates how the choice of gNB (radio interface base stations) and their configuration parameters affect performance characteristics critical for e.g. industrial settings

This included both commercial and open source base stations and core networks – showing significant differences

The 5G and Beyond Lab allows precise investigations into this type of behaviour and for given application environments in a controlled environment



From Laboratories to Insights (2)

NORCICS supports the development of the Norwegian Cyber Physical Range - working in conjunction with the Norwegian Cyber Range (NCR) including work by **Vyron Kampourakis**

Work by **Michail Takaronis** extends the features of the CPR to a more service-oriented architecture allowing simulation where direct use of equipment or emulation is not necessary enabling

- Attack scenarios and simulations including with re-usable building blocks
- Construction of training scenarios (separate or joint with NCR)

Understanding Attacks and their Aftermath (1)

Digital Twins are a well-established way to model and understand *cyber-physical systems* (CPS) in particular

Work by **Gizem Erceylan** uses digital twins for enhanced threat modelling – recognising that threats to CPS arise particularly from interactions or in different modes of operation, requiring multiple iterations and combinations

Work by **Jule Langedahl Leirmo** studies how organisations cope with and learn from attacks: Problem-focused as well as emotional coping responses result in different learning outcomes

Work by **Vahiny Gnanasekaran** studies organisational roles at the intersection of safety and security incidents

Understanding Attacks and their Aftermath (2)

In addition to modelling threats for incident prevention, digital twins are also highly useful for enhancing incident detection and response in cyber-physical systems

Work by **Konstantinos Kampourakis** studied their use in energy, health care, and smart cities in particular and is developing a framework for their development and deployment including validation using benchmark data sets and in use cases

In this context work by **Jessica Heluany** focused on vulnerability management in OT (SCADA) environments, eliciting surprising findings e.g. on prioritisation from asset owners

Work by **Ming-Chan Lee** studies how light-weight anomaly detection can operate in real time based on existing instrumentation data in CPS

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU | Norwegian University of Science and Technology