

The background is a dark, textured surface with glowing orange and blue lines that resemble circuit traces and binary code. The text 'CSI' is centered in the middle of the image.

CSI

Cyber Security and IoT
Research Group



Staff

- Ivan Kotuliak
- Ladislav Hudec
- Pavol Helebrandt
- Xiaolu Hou
- Jan Laštinec
- Milan Pikula
- Alexander Valach
- Marek Zeman
- Ladislav Zemko

PhD. Students

- Jakub Dubec
- Máté Konkoly
- Ondrej Lesák
- Emma Macháčová
- Ján Mikulec
- Matúš Mikuláš
- Martin Pavelka
- Andrej Ralbovský
- Norbert Varga



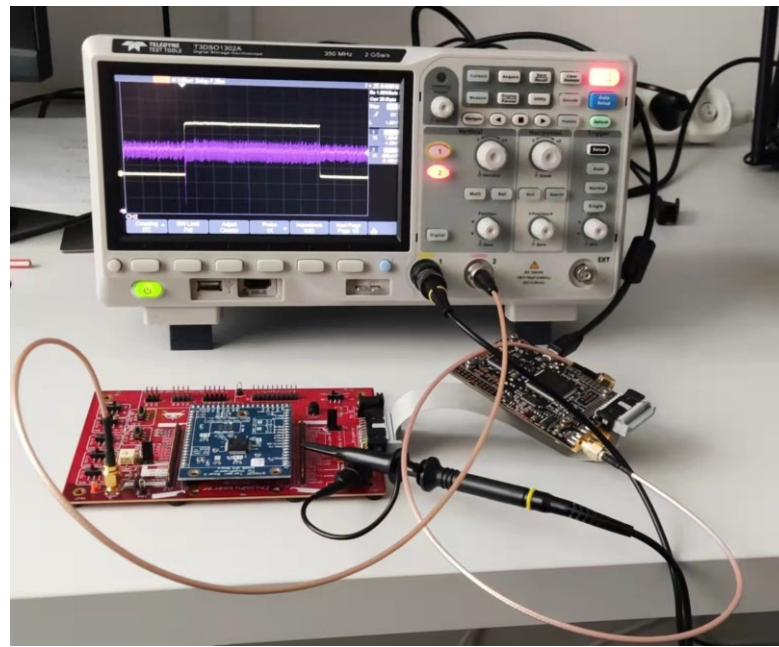


Areas of interest

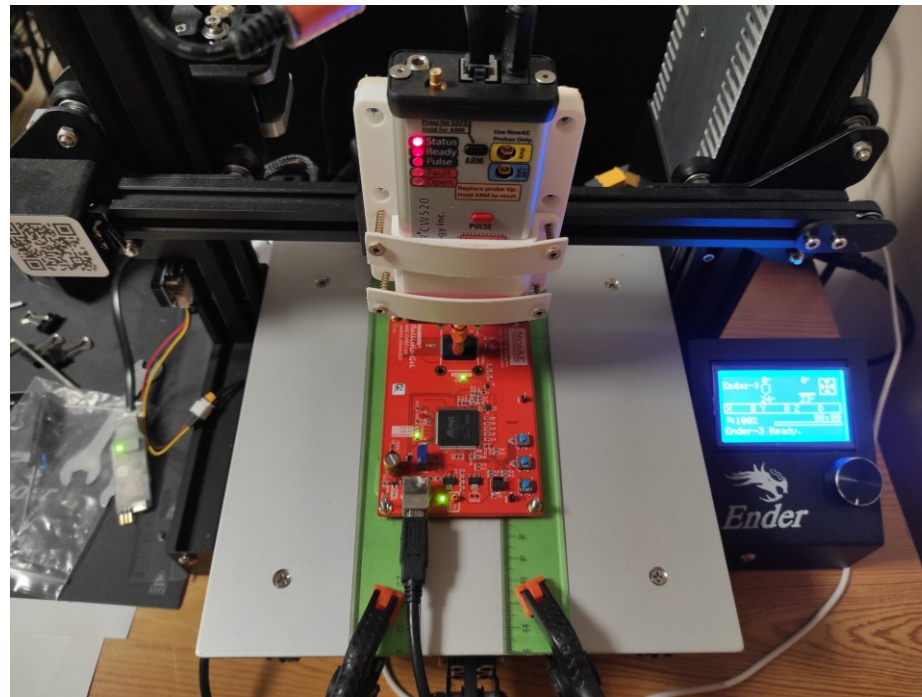
- Cybersecurity
 - Infrastructure
 - Monitoring
 - Threat detection
 - Side-channel attacks
 - AI/ML for security
 - AI/ML implementation security
- IoT and Networking
- Cyber Range
- Mobile 5G
- Intelligent systems

Labs





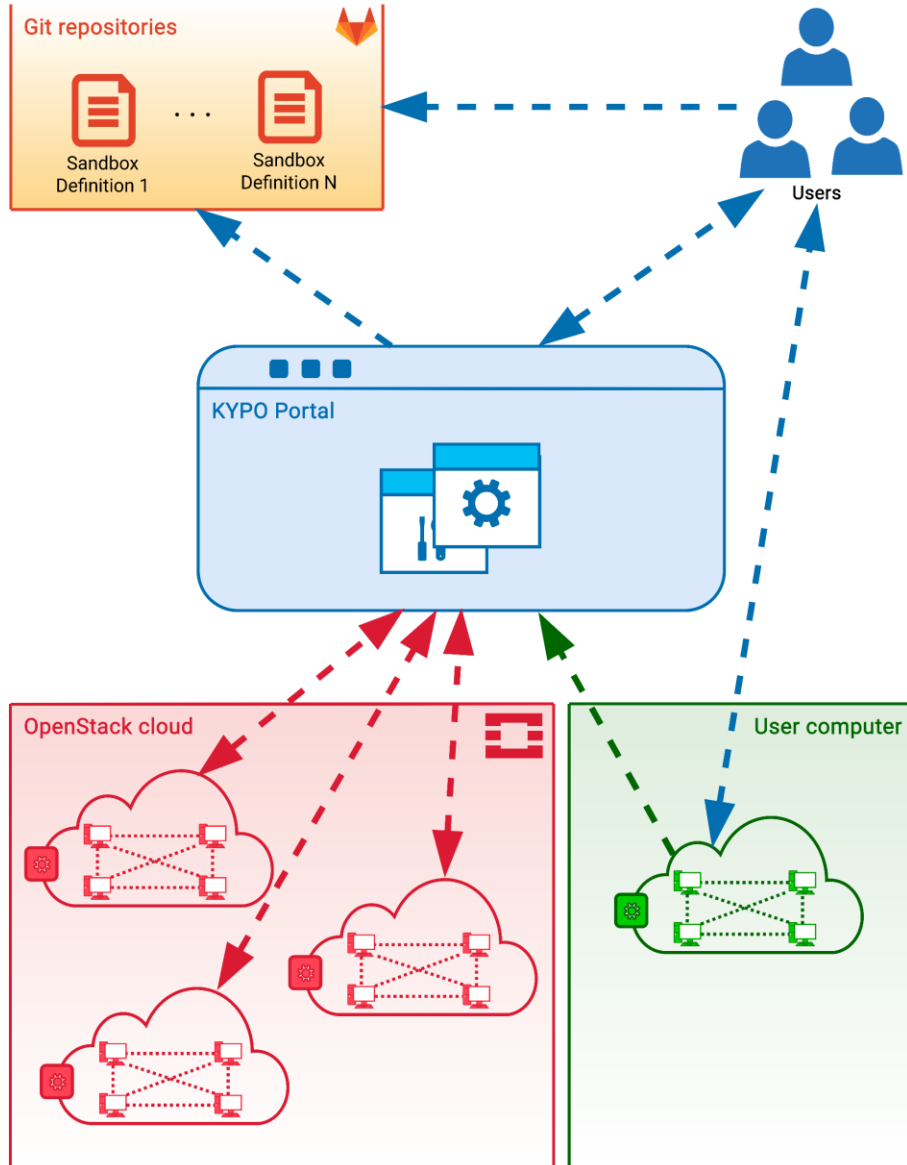
Labs



Security of neural networks against hardware attacks

- Fault attacks perturbs the neural network computations to cause misclassification
- Side-channel attacks steal secret parameters of neural network assuming a black box attacker model
- The projects aim to study neural network security w.r.t. one of the two attacks





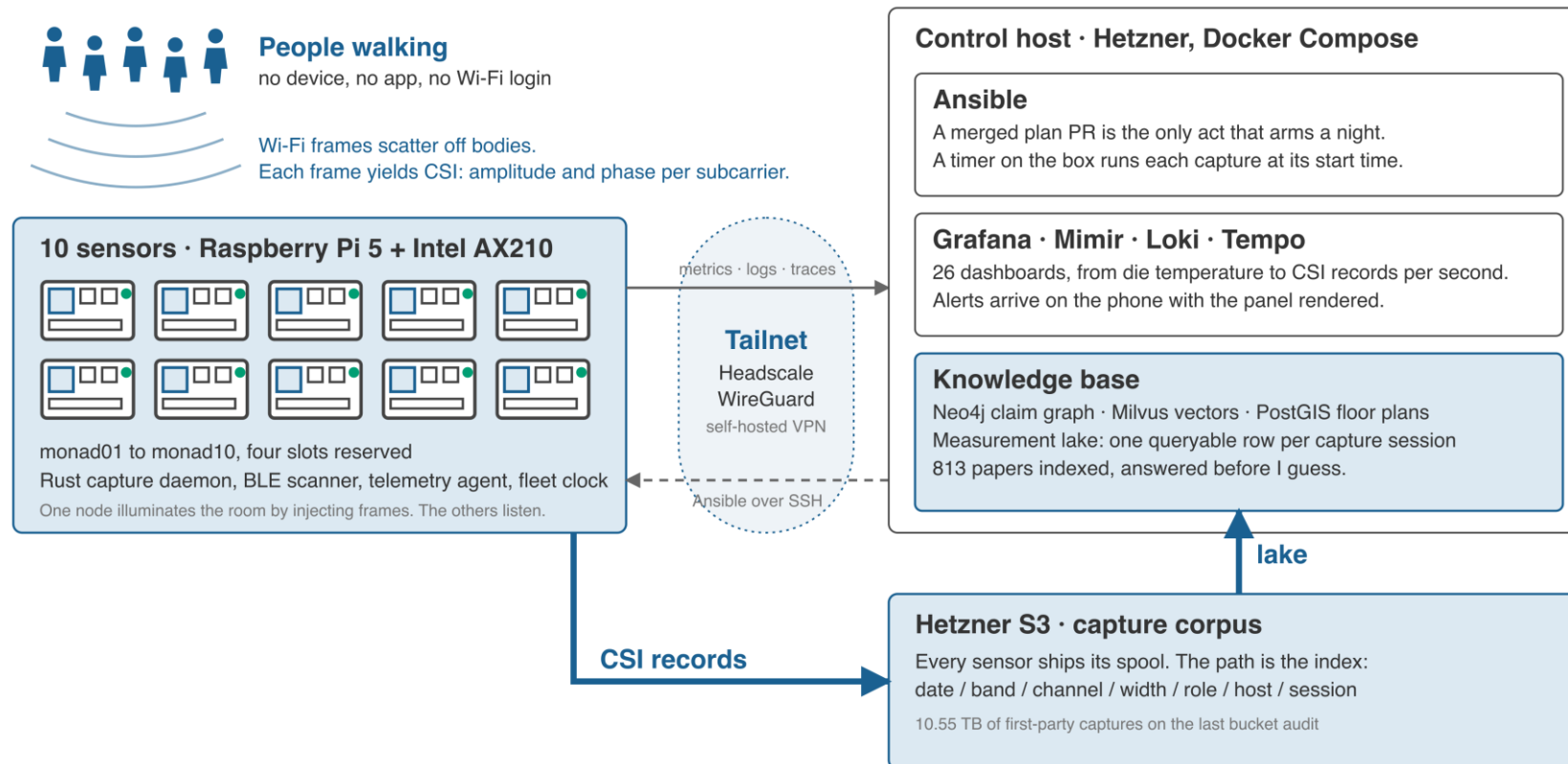
Cyber Range

- KYPO CRP
- Training
- Research
- CTF & CDX
- Red vs Blue Team

IoT

Ten sensors, one private network, one control host

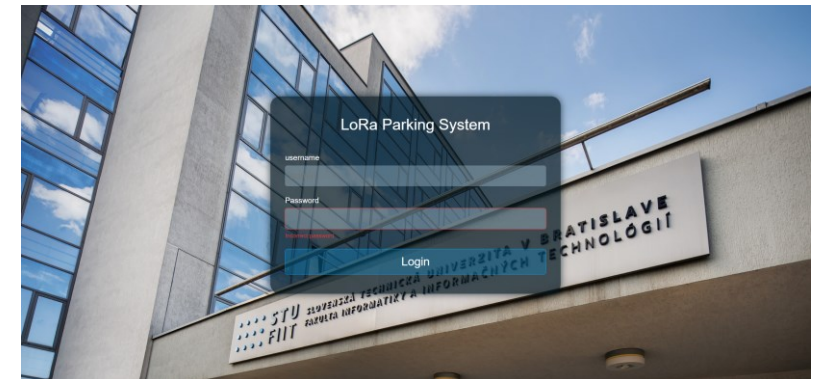
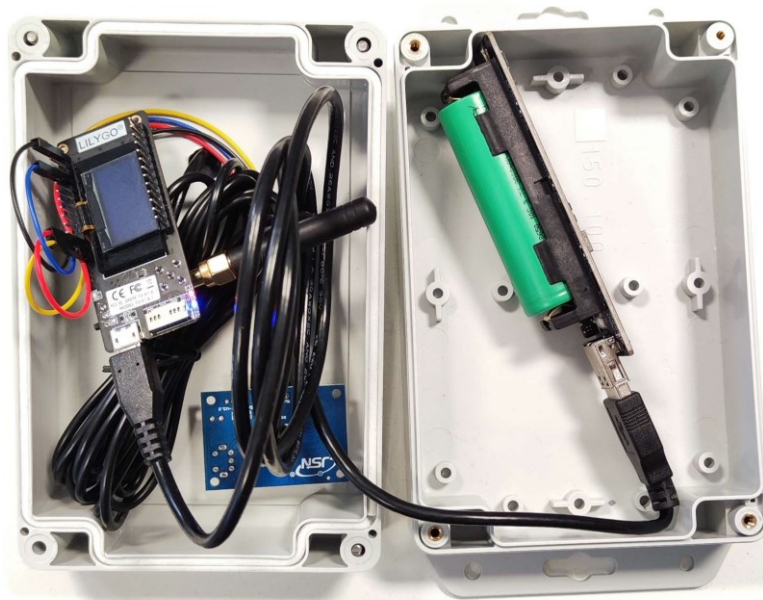
Blue is the measurement path. Grey is management and telemetry.



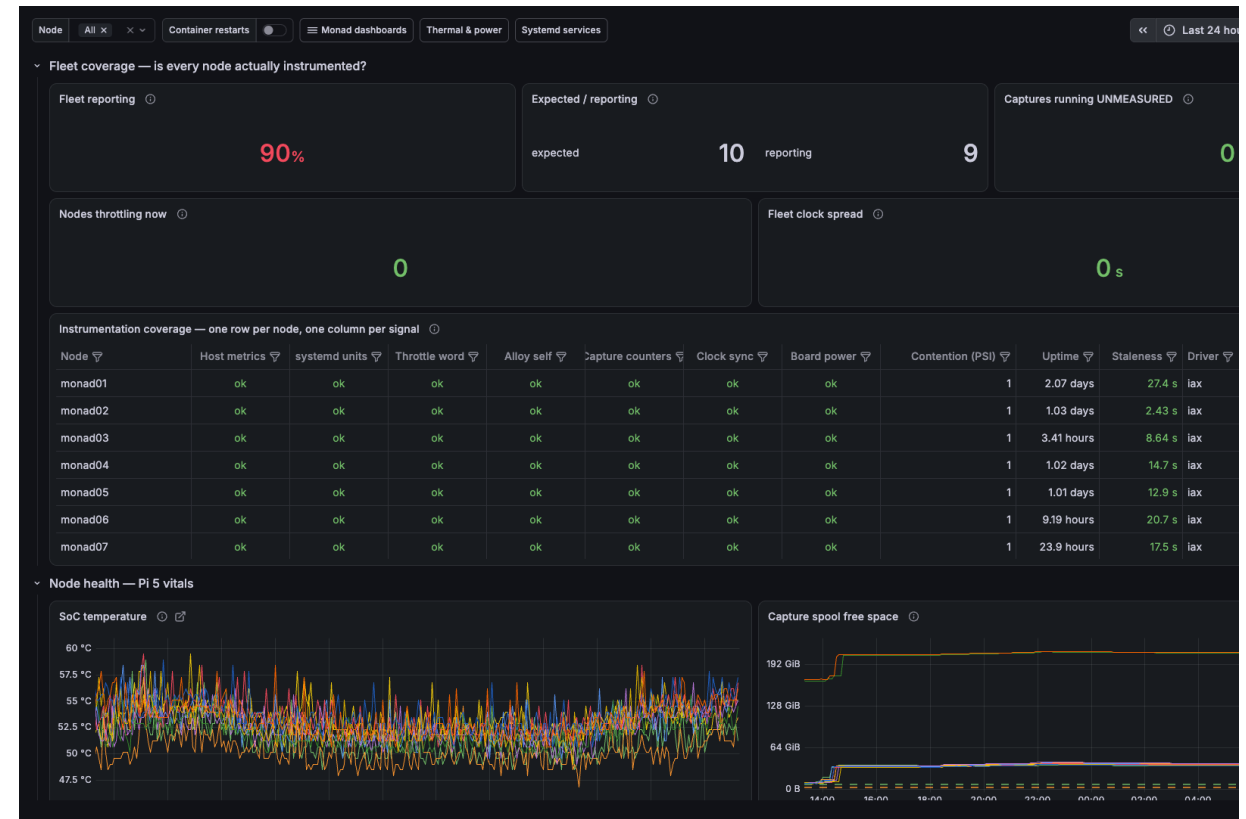
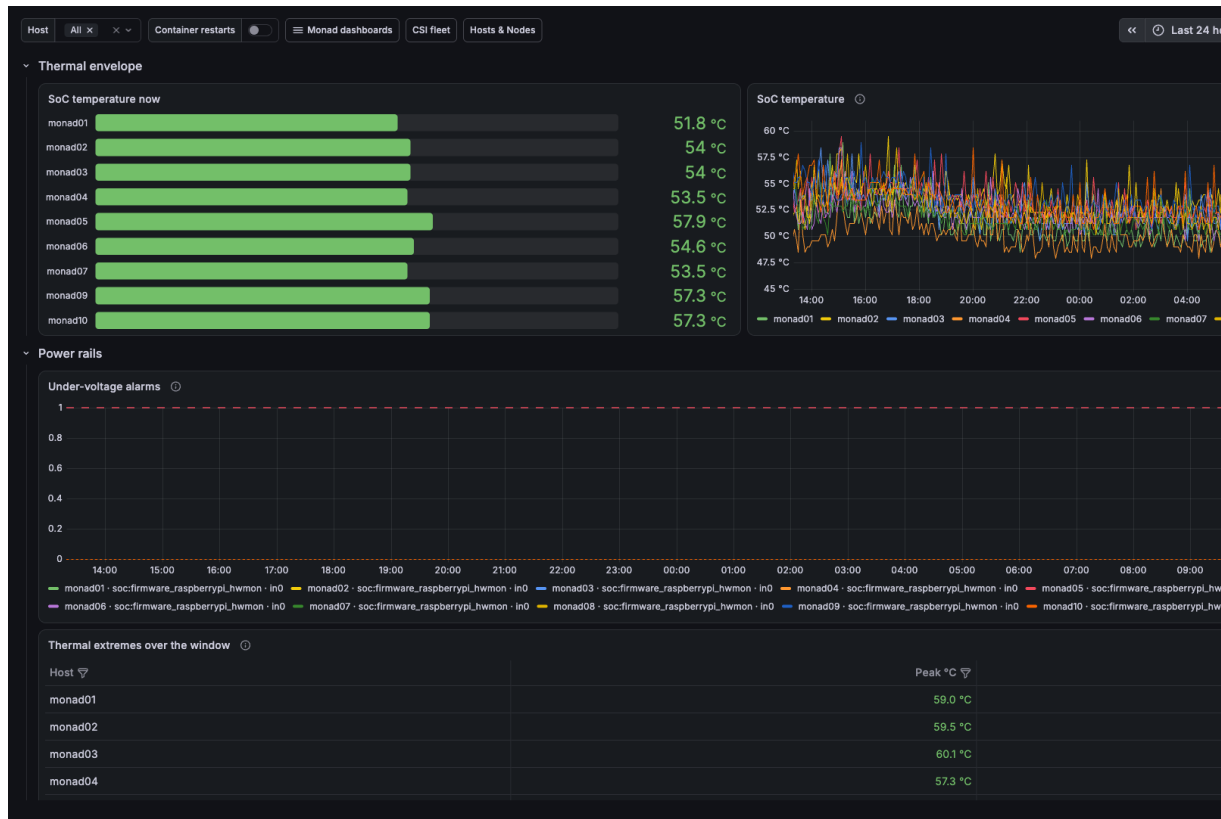
IoT Devices / Networks



Smart Parking



IoT Monitoring / Management



Thank you

Questions?