KU LEUVEN

Trusted Computing Architectures for IoT Devices

Trusted IoT – March 21st, 2024

Project Partners

VUB VRIJE UNIVERSITEIT BRUSSEL

KU LEUVEN

TECHNISCHE UNIVERSITÄT DRESDEN

Universität Rostock Traditio et Innovatio

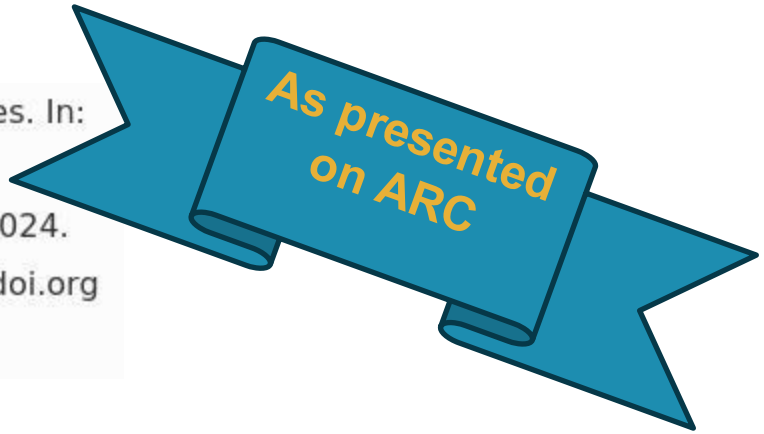
GFaI

Trusted Computing Architectures for IoT Devices

This work has been presented on March 21st, 2024; in Aveiro – Portugal

It was presented in the 20th International Symposium on Applied Reconfigurable Computing (ARC) 2024

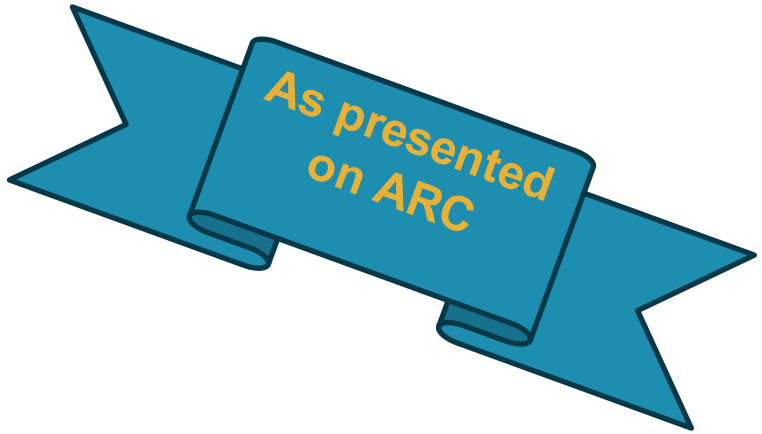
Braeken, A. *et al.* (2024). Trusted Computing Architectures for IoT Devices. In: Skliarova, I., Brox Jiménez, P., Véstias, M., Diniz, P.C. (eds) Applied Reconfigurable Computing. Architectures, Tools, and Applications. ARC 2024. Lecture Notes in Computer Science, vol 14553. Springer, Cham. https://doi.org/10.1007/978-3-031-55673-9_17



https://link.springer.com/chapter/10.1007/978-3-031-55673-9_17

Trusted Computing Architectures for IoT Devices

The contributions of the Belgian partners have been left out as these will be presented after this, in much further detail.



KU LEUVEN

Trusted Computing Architectures for IoT Devices

Trusted IoT – March 21st, 2024

Project Partners

VUB VRIJE UNIVERSITEIT BRUSSEL

KU LEUVEN

TECHNISCHE UNIVERSITÄT DRESDEN

Universität Rostock Traditio et Innovatio

GFaI

Internet of Things (IoT)

IoT is a network of interconnected physical objects interfaced to the Internet

Common scenarios:

- Smart-house: connected TVs, cameras, smartphones, computers and home appliances
- **Industrial IoT: connected sensors, instruments, and other devices to enhance industrial processes and applications**

Attractive target for malicious actors

- Need for efficient defense mechanisms

Trusted IoT

Evaluation of hardware-assisted security solutions for IoT devices
Development of new security solutions in different application domains

Five use cases driven by user group of SMEs:

Drones

Environmental monitoring

Mobile robots

Industrial IoT

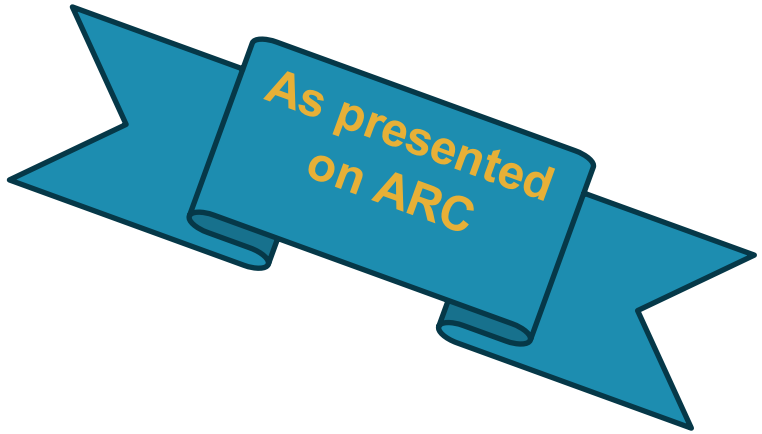
Cooperative robots

KU Leuven Use Case

Drones

Multi-Core RISC-V platforms

The contributions of the Belgian partners have been left out as these will be presented after this, in much further detail.

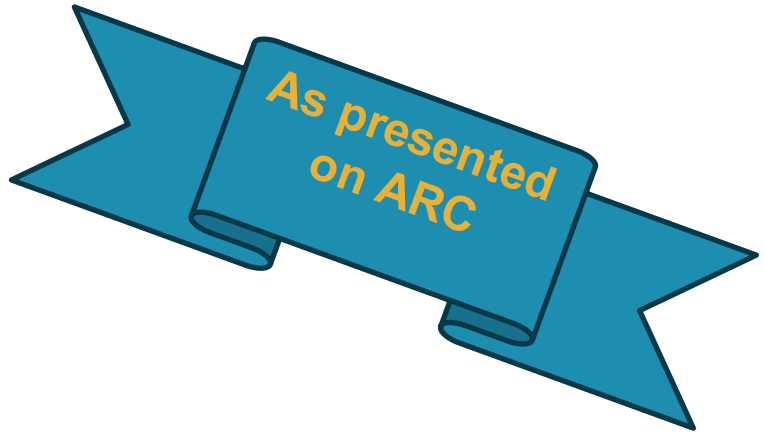


VUB Use Case

Environmental monitoring

Environmental monitoring

The contributions of the Belgian partners have been left out as these will be presented after this, in much further detail.

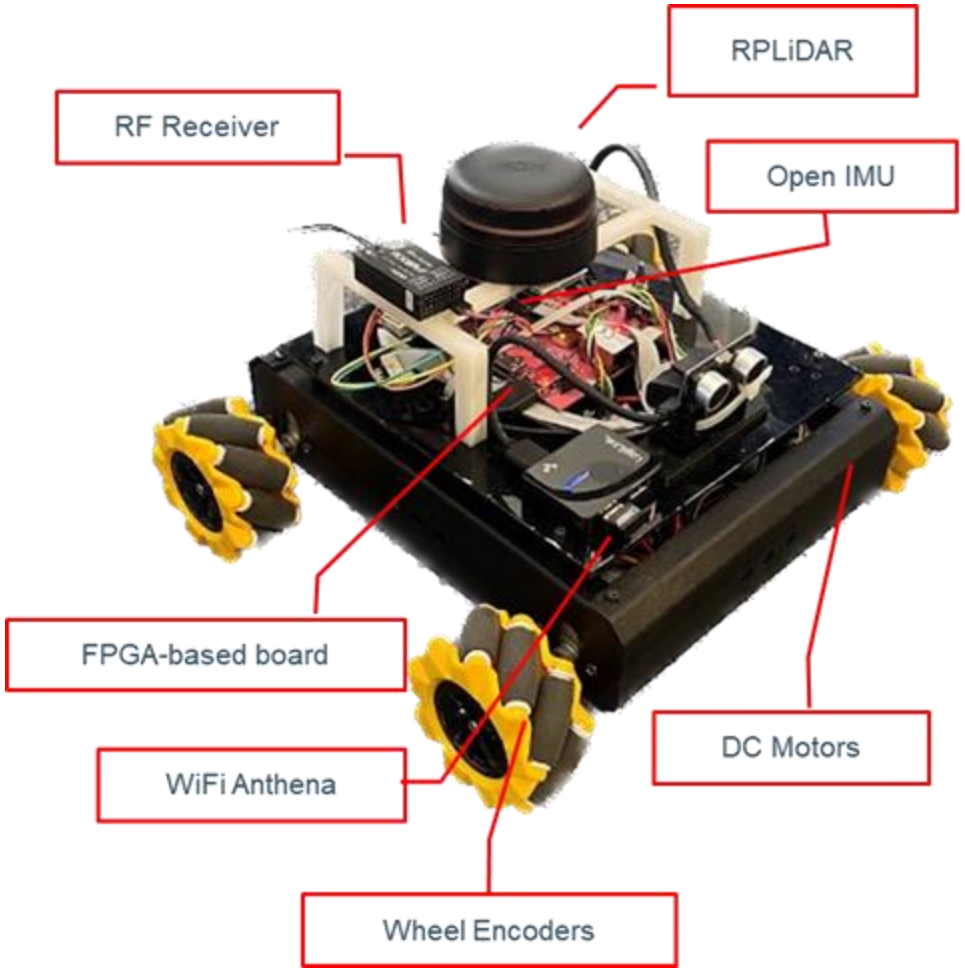


TU Dresden Use Case

Mobile Robots

Mobile Robots - Motivation

- FPGAs allow to accelerate functionality of mobile robots, e.g., for navigation.
- Prevention of illegal access to hardware accelerators



Mobile Robots - Adversary Model

- Malicious software tasks that invade the address space of a hardware accelerator assigned to a different task

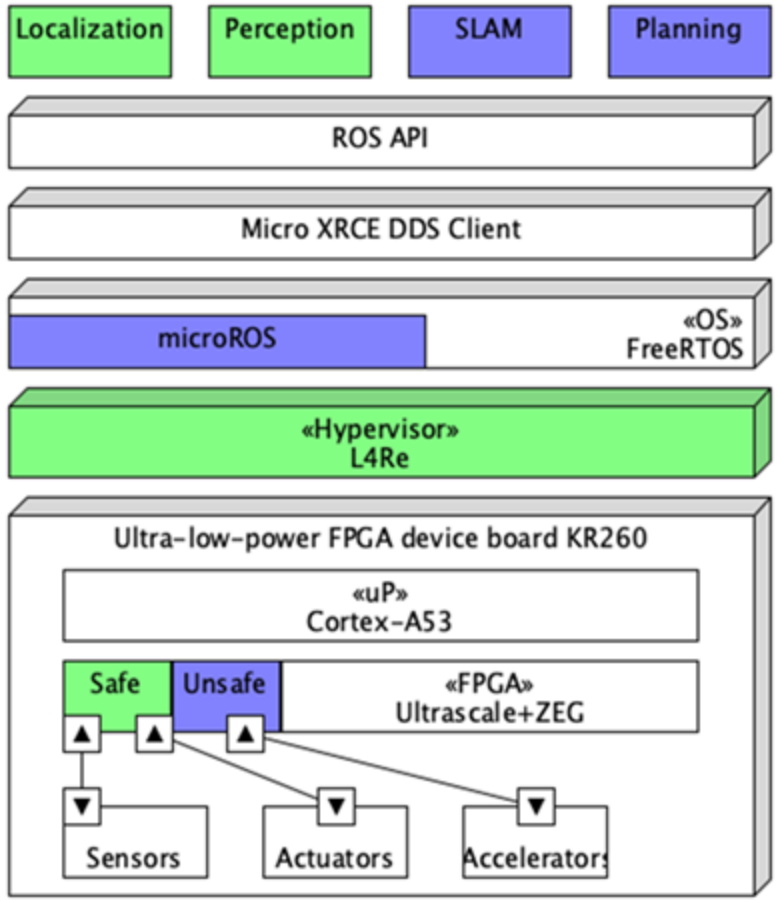
- Threat to the confidentiality, integrity, or availability of the associated data

Mobile Robots - Access Control

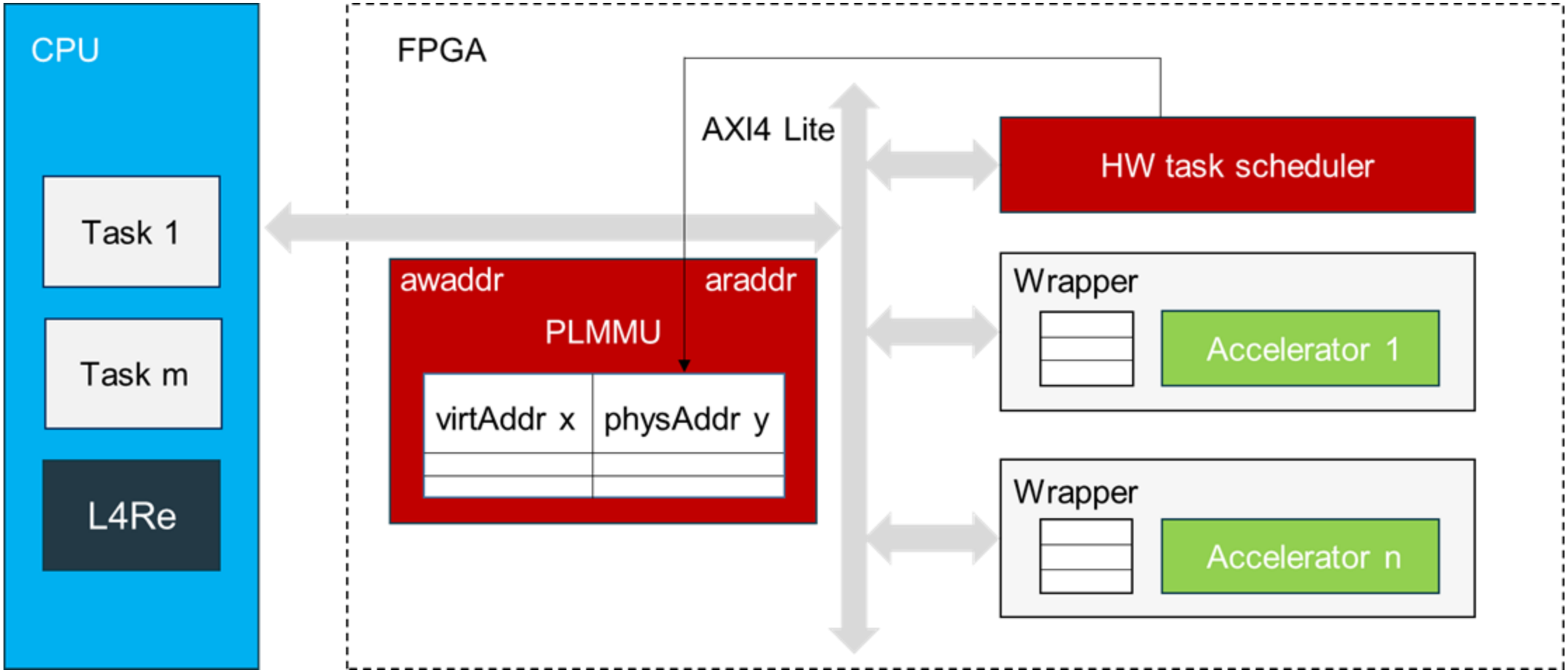
- Software side:
  Hypervisors isolate trusted from untrusted guest operating systems.

- Hardware side:
  Fine-grained isolation mechanism for shared usage of hardware accelerators is missing.

Focus on AXI memory-mapped interfaces

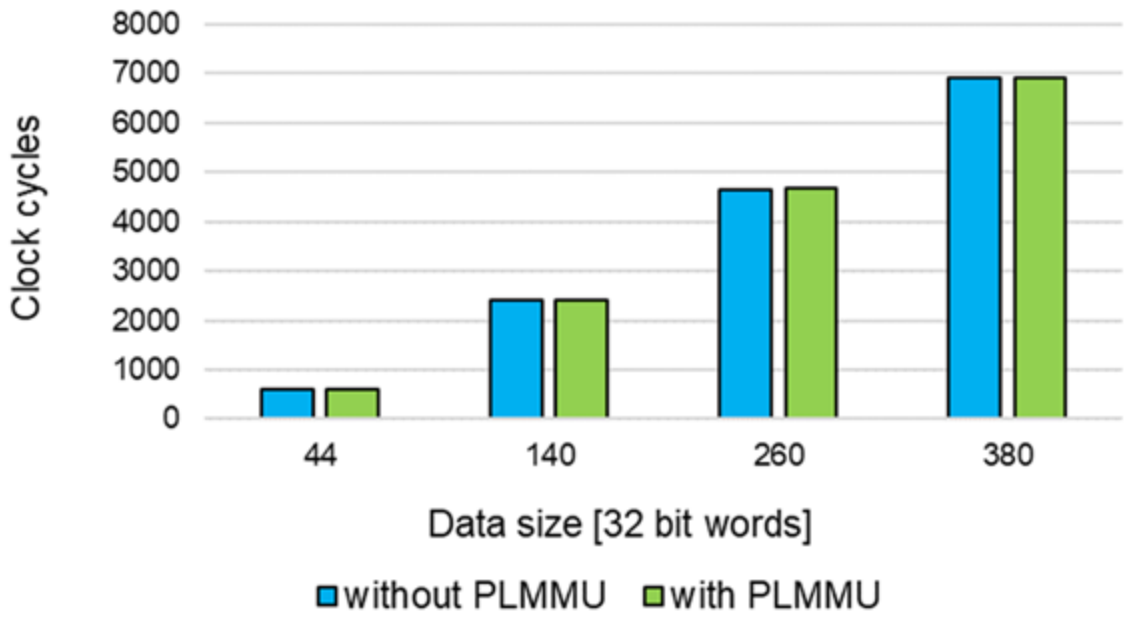


Mobile Robots - Access Control



Mobile Robots - Results

- Hardware accelerators: Encryption
- PLMMU adds negligible overhead to the communication between software task and hardware accelerator

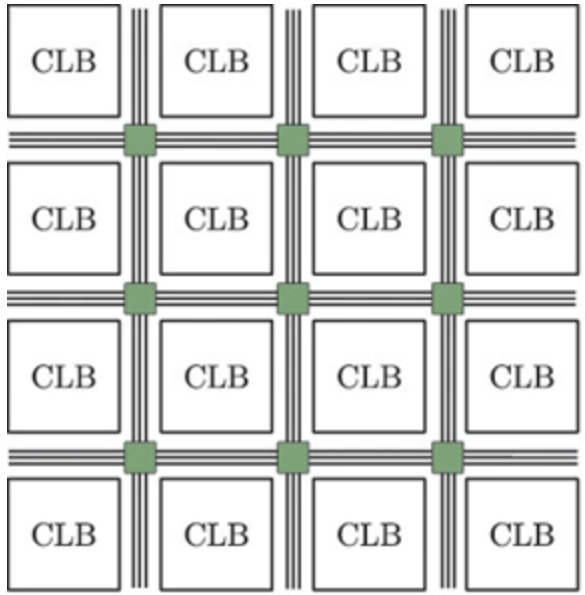


Universität Rostock Use Case

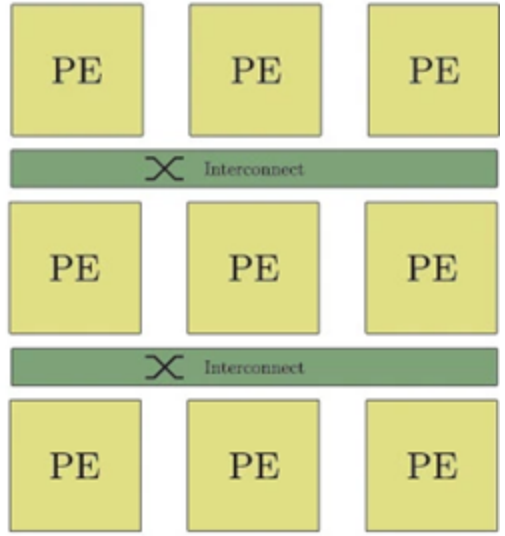
Industrial IoT

HERA on CGRAs – CGRAs

- CGRAs (Coarse-Grained Reconfigurable Arrays) are adaptable computing architectures
- Consist of programmable computation blocks and interconnects
- Offer flexibility and high performance for specific tasks



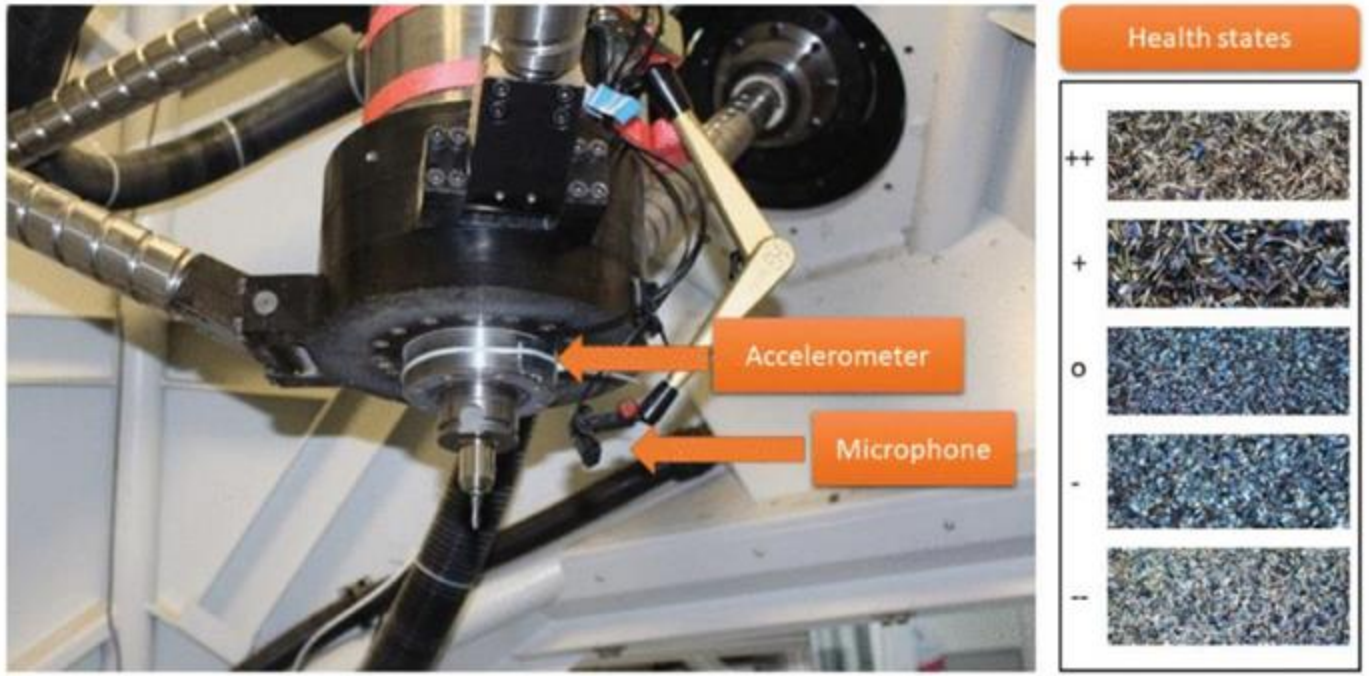
a) FPGA (simplified)



b) CGRA (simplified)

CGRAs in Industry 4.0

- Industry 4.0 demands adaptable, high-performance computing
- CGRAs support real-time data analytics and machine learning
- Essential for smart manufacturing and IoT integration



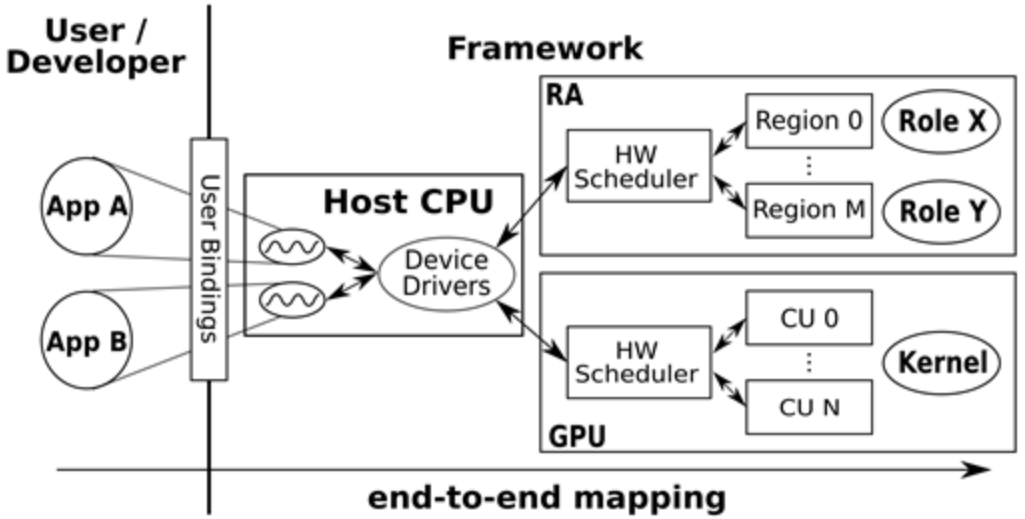
From: P. F. Suawa, A. Halbinger, M. Jongmanns and M. Reichenbach, "Noise-Robust Machine Learning Models for Predictive Maintenance Applications," in IEEE Sensors Journal, vol. 23, no. 13, pp. 15081-15092, 1 July, 2023, doi: 10.1109/JSEN.2023.3273458 (used with permission)

Security Aspects for CGRAs

- Security challenges of CGRAs similar to those faced by FPGAs
- Importance of module separation from different vendors
- Focus on robust security design in interconnected systems

- In Industrial application: Security affects Safety, so hardening is necessary

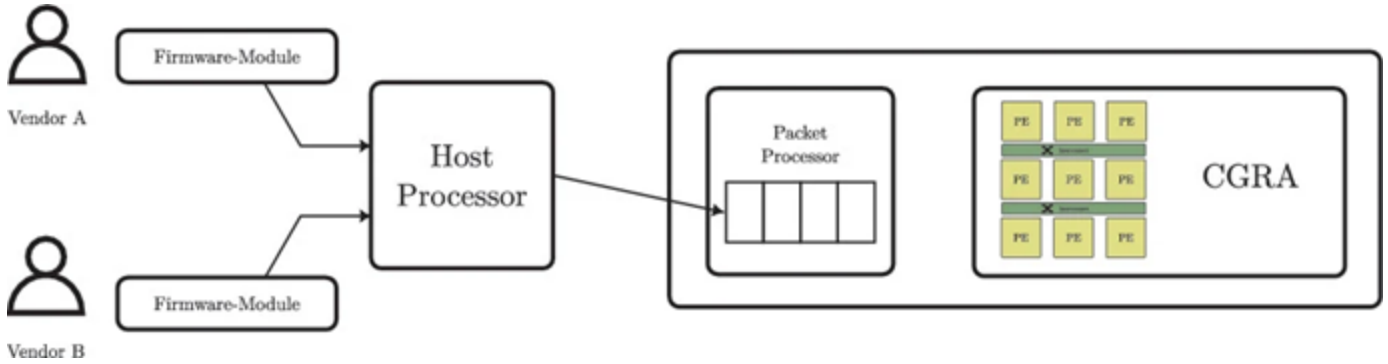
HERA Methodology

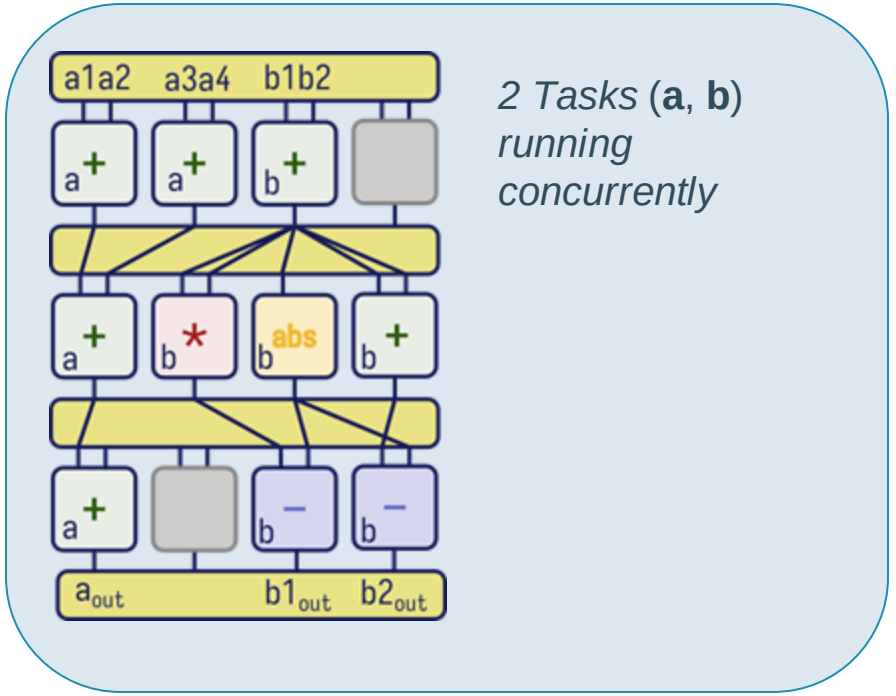


From: P. Holzinger and M. Reichenbach, "The HERA Methodology: Reconfigurable Logic in General-Purpose Computing," in IEEE Access, vol. 9, pp. 147212-147236, 2021, doi: 10.1109/ACCESS.2021.3123874 (Used with permission)

- HERA: Heterogeneous Reconfigurable Architectures
- Focuses on multi-user capabilities and accessibility
- Enhances security and efficiency in reconfigurable computing

HERA on CGRAs – Packet Processor

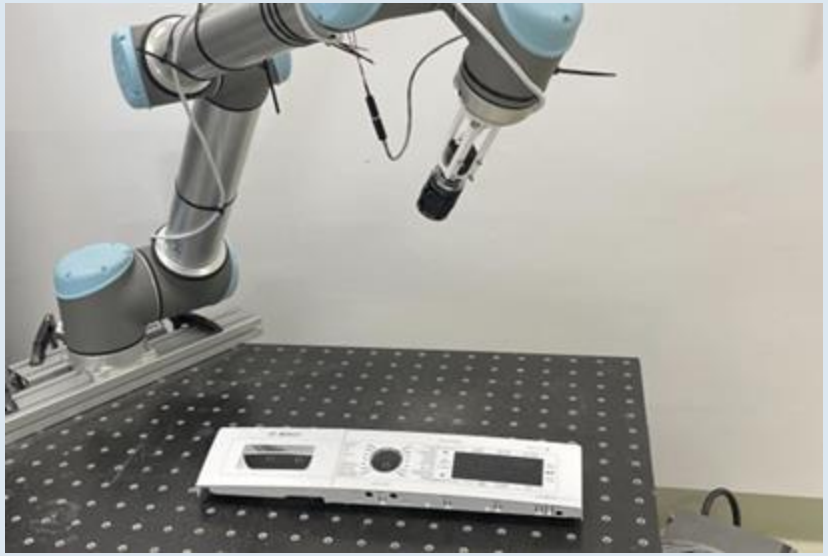


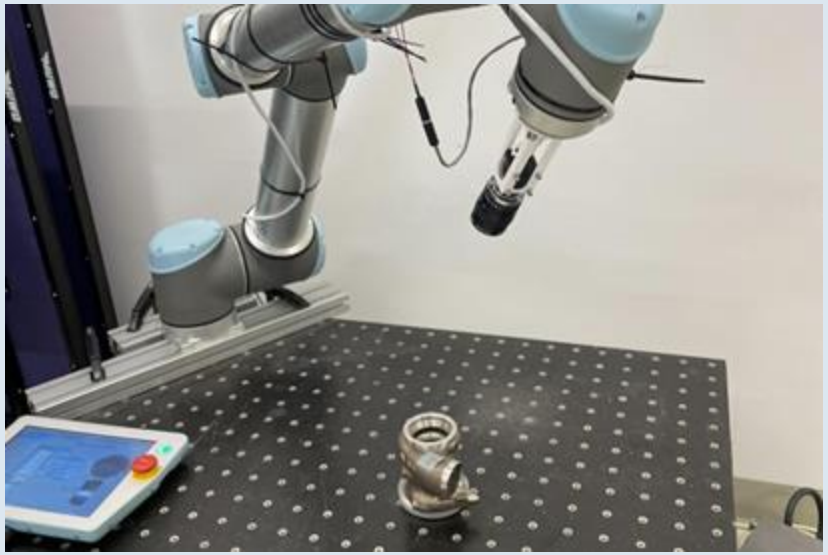


- Responsible for task scheduling and dispatching
- Optimizes resource allocation and workload management
- Key component in managing CGRA's dynamic adaptability

GFaI Use Case

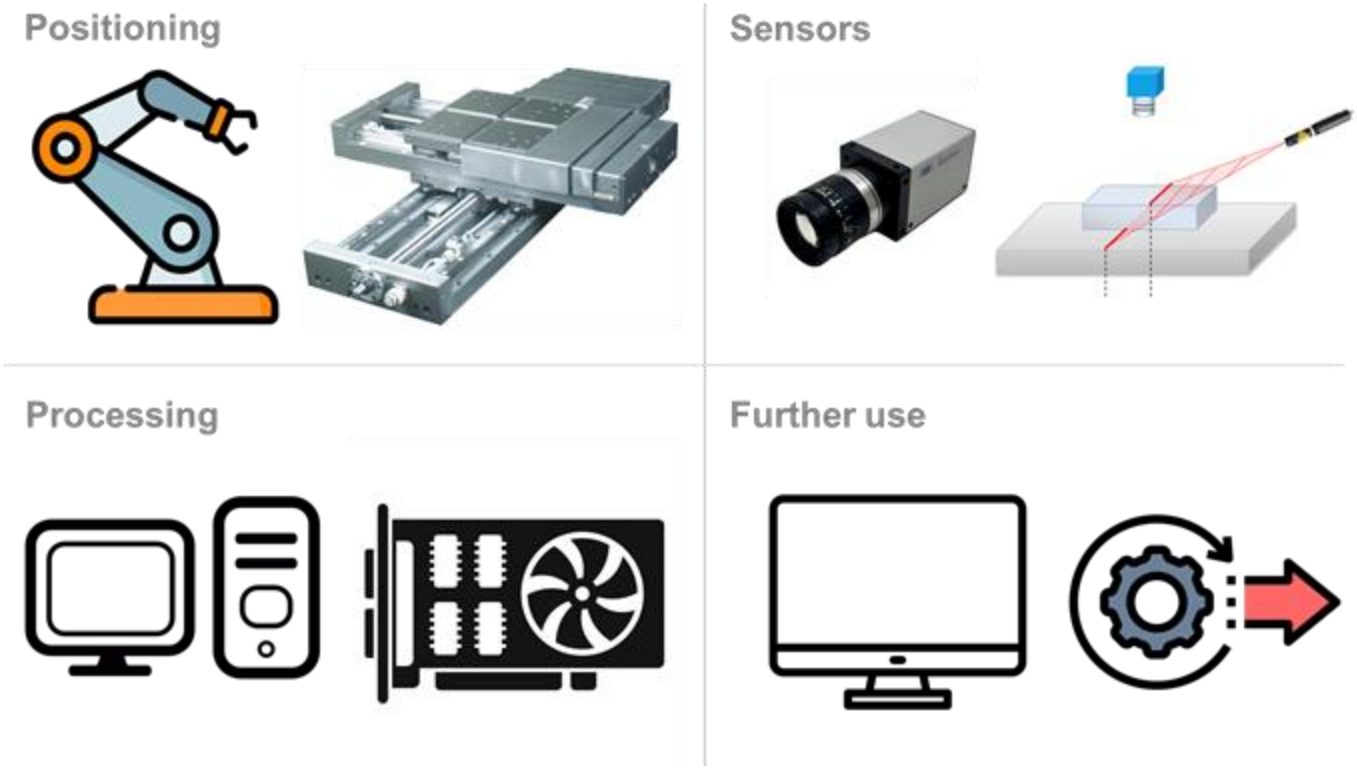
Cooperative robots





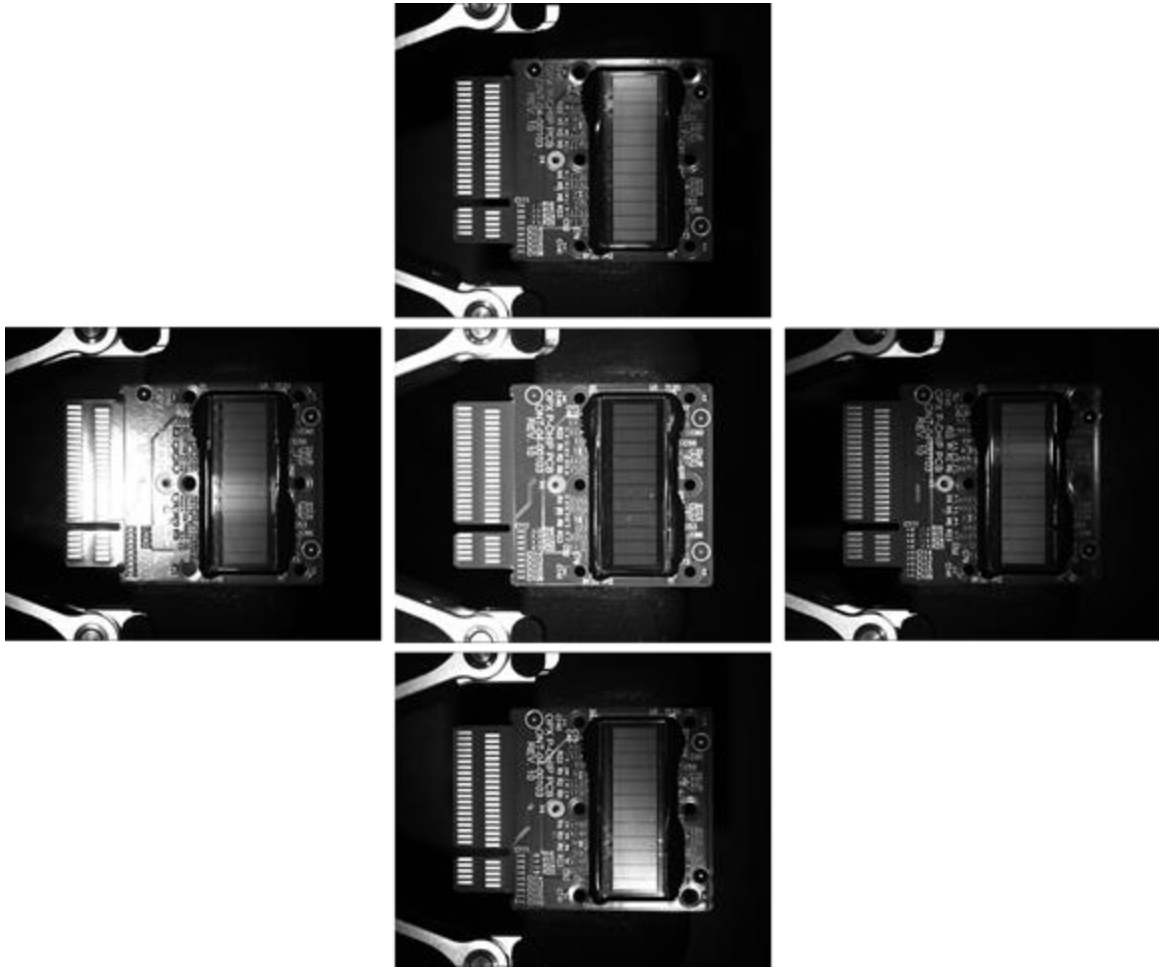
Secured quality assurance of workpieces

- Automated positioning
- Image capture with different light settings
- Anomaly detection
- e.g. sorting out defective components

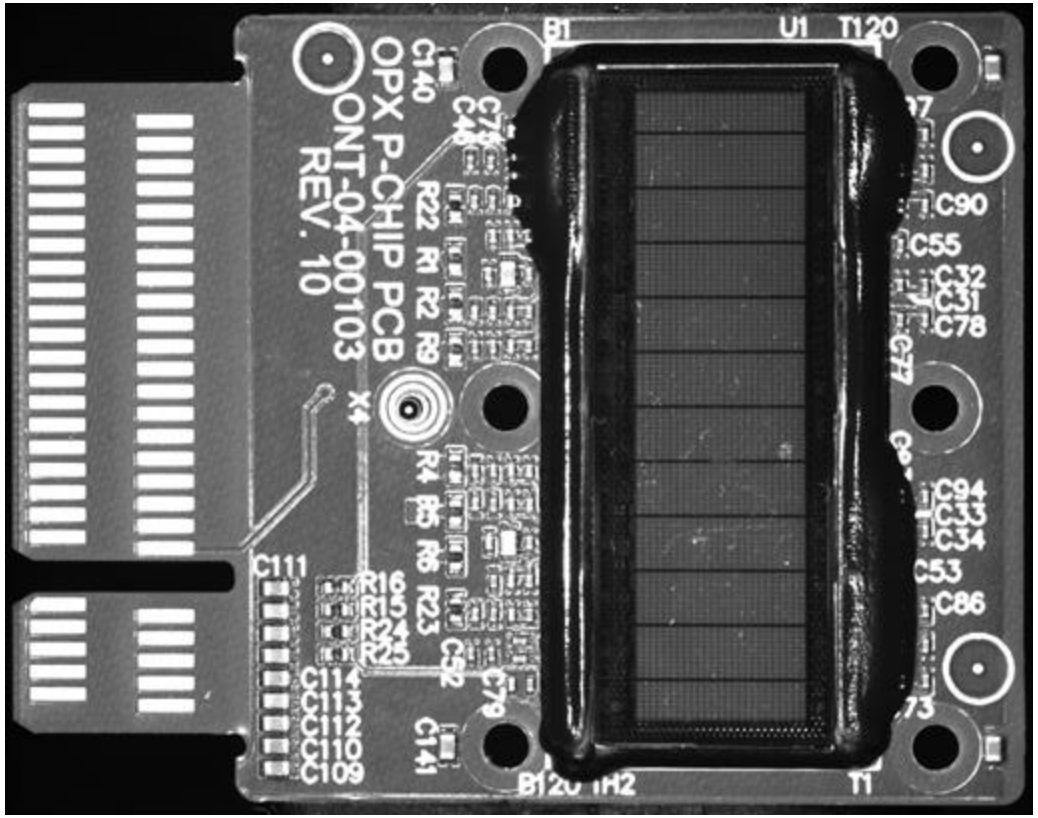


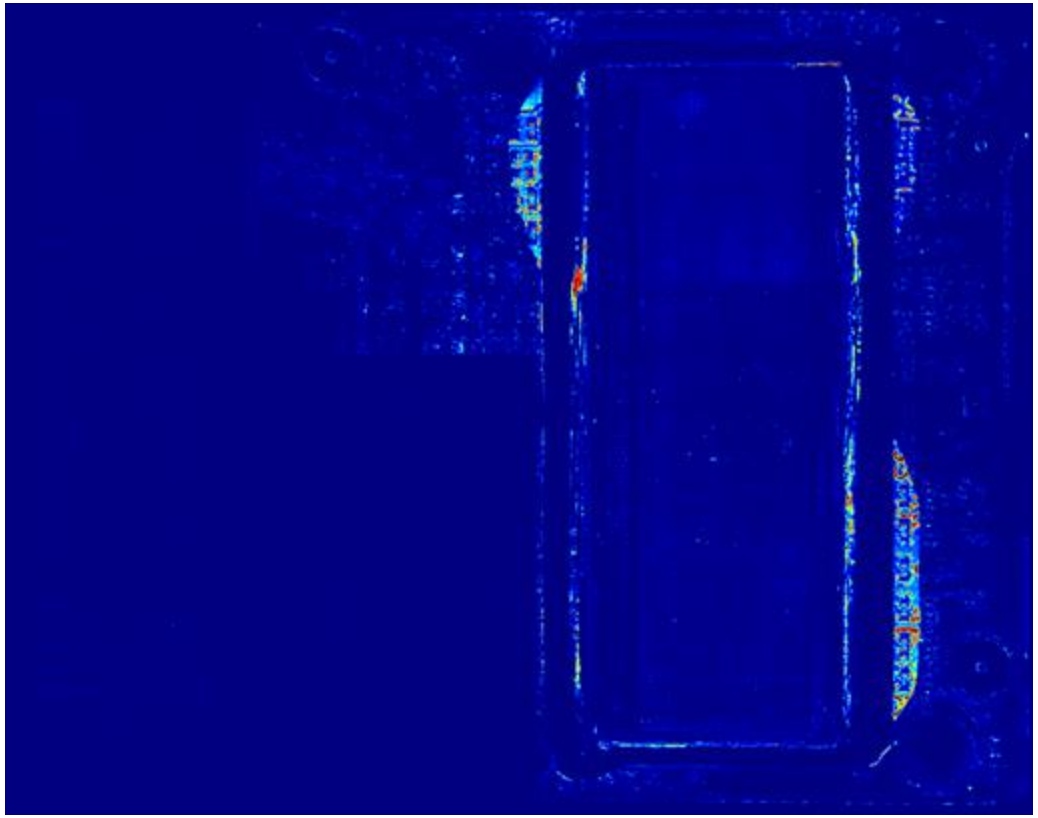
Images with different lighting

- Simple reference image comparison not possible due to tolerances in production
- Images from several lighting directions combined to visualise as many defects as possible
- Partitioning into image sections, one anomaly detector per section and illumination

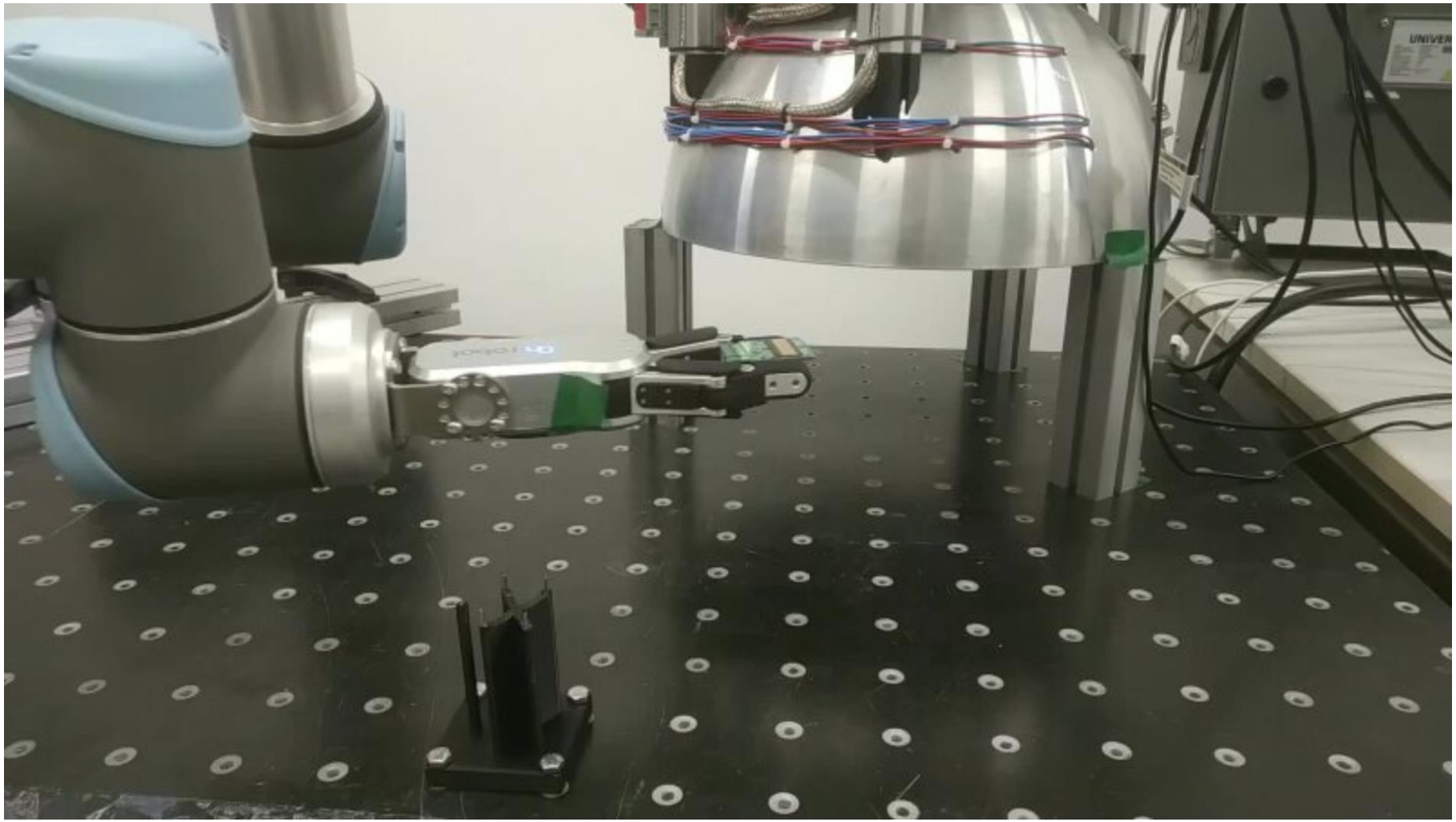


Anomaly map





Trusted IoT – Demonstration video



Questions?