CHERITech'26
CONFERENCE

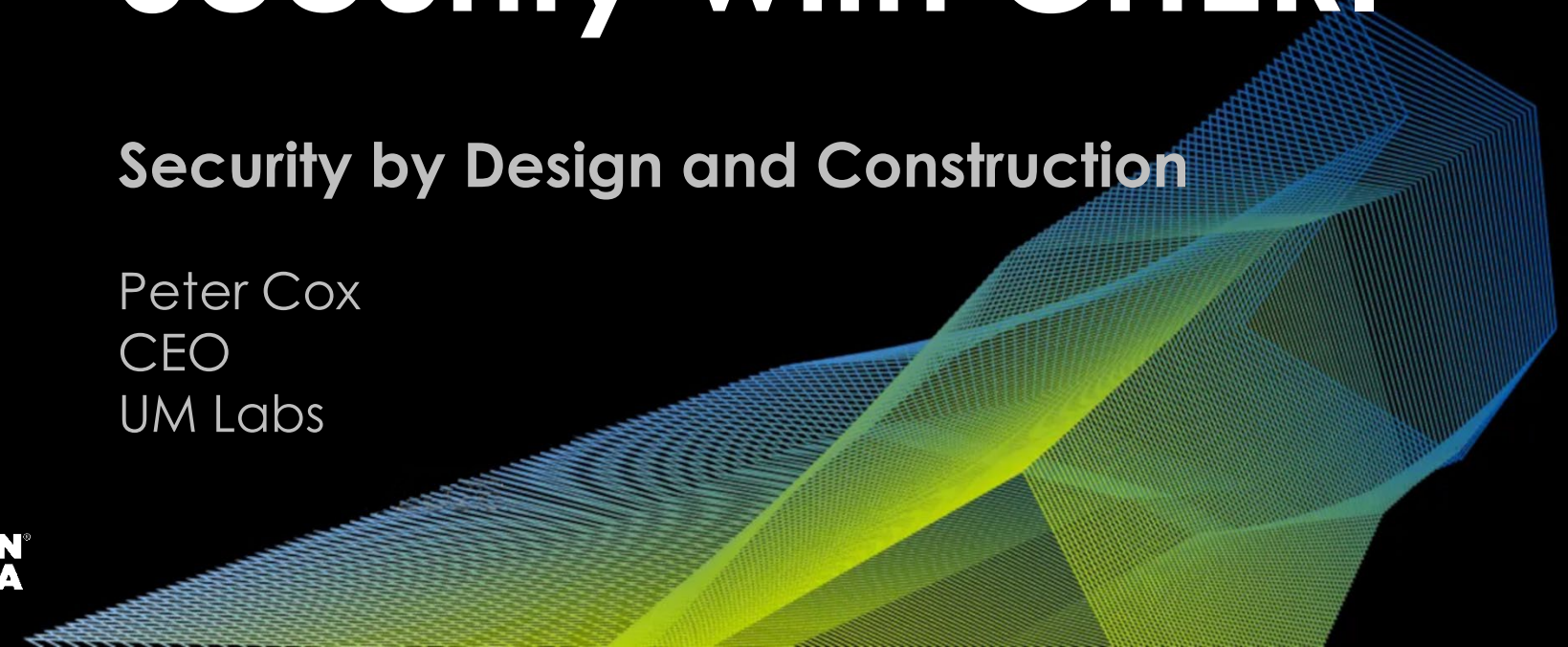
CHERI

12-13 Nov 2026
Munich, DE

Core to Edge IoT Security with CHERI

Security by Design and Construction

Peter Cox
CEO
UM Labs



Located at semi | SEMICON EUROPA

Agenda

- About UM Labs
- Securing the Edge
- Connection to the Core
- Common Edge/Core Design
- CHERI: Secure by construction
- Future Plans

About UM Labs

- UK Based Cybersecurity R&D Company
- Specialising in securing standards based real-time communication applications on IP networks
- Member of CHERI Alliance
- Customer base includes:
  - Government, Defence
  - National Telcos
  - System Integrators
- Protected protocols and applications include:

SIP – Unicus RTC

- Voice and video calls
- Global phone network interconnects

RTSP – Unicus SVSS/CXR

- Streaming video
- Extended Reality

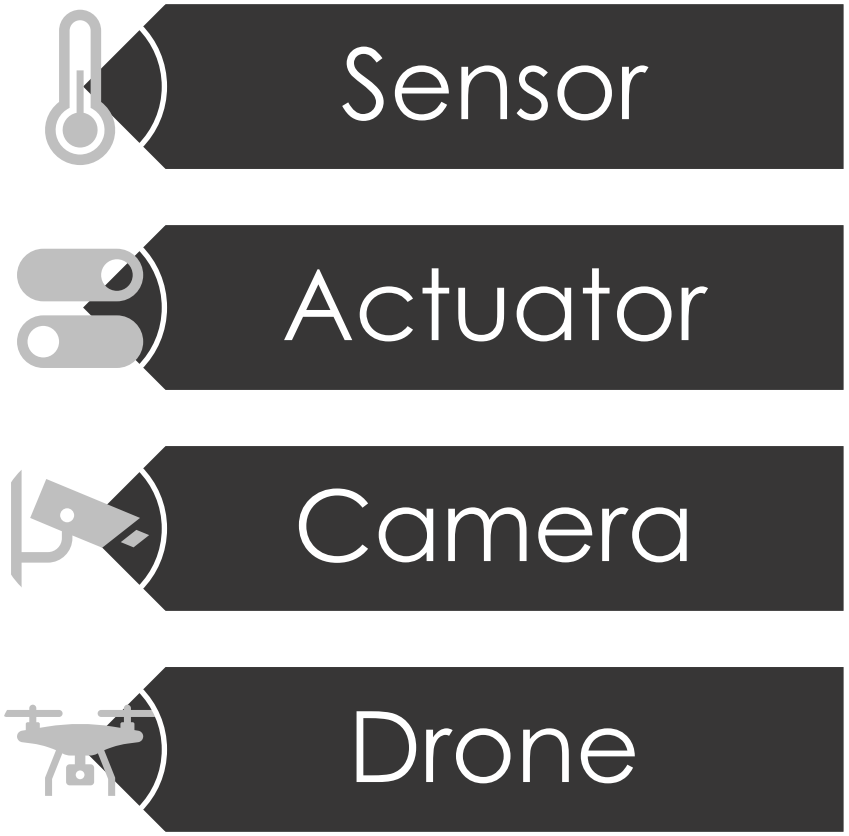
MQTT, etc. – Unicus IoT

- IoT

Securing The Edge

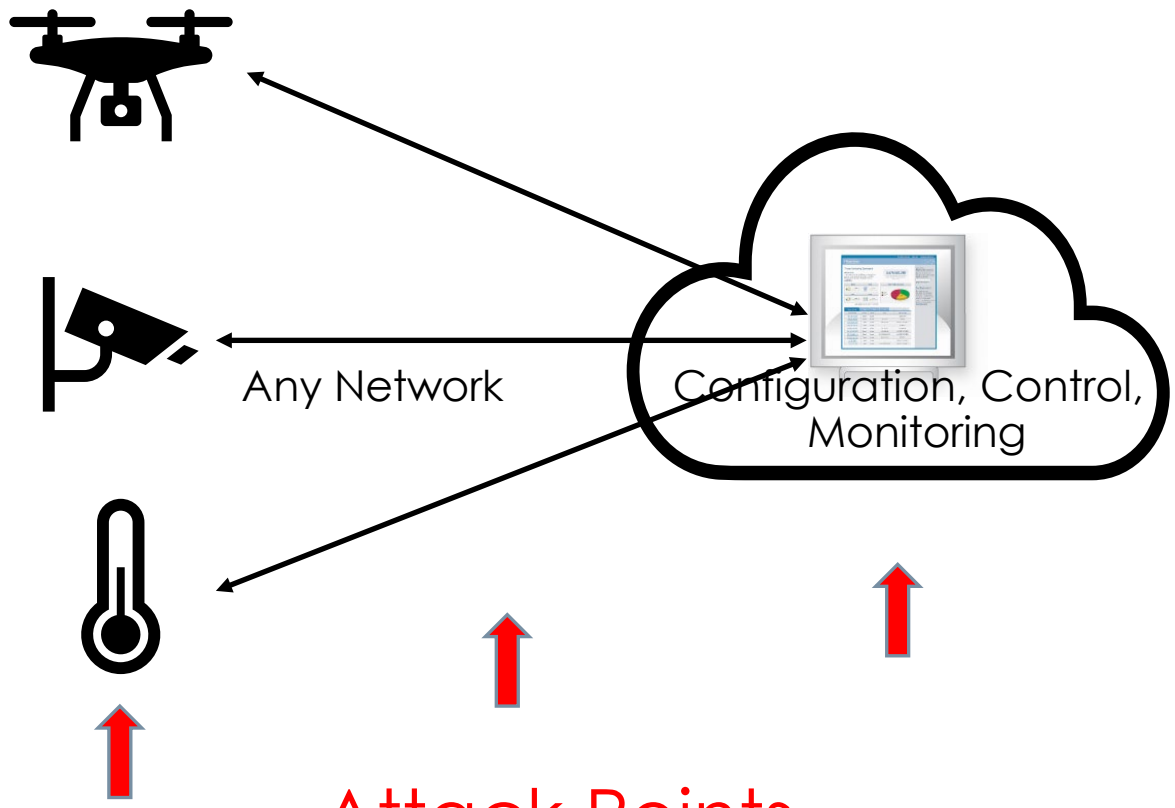


- Security limited on many Edge devices
- Open to attack
- Access to or Modification of reported data
- Denial of service
- Provisioning and life-cycle challenges
- Limited access to smaller devices



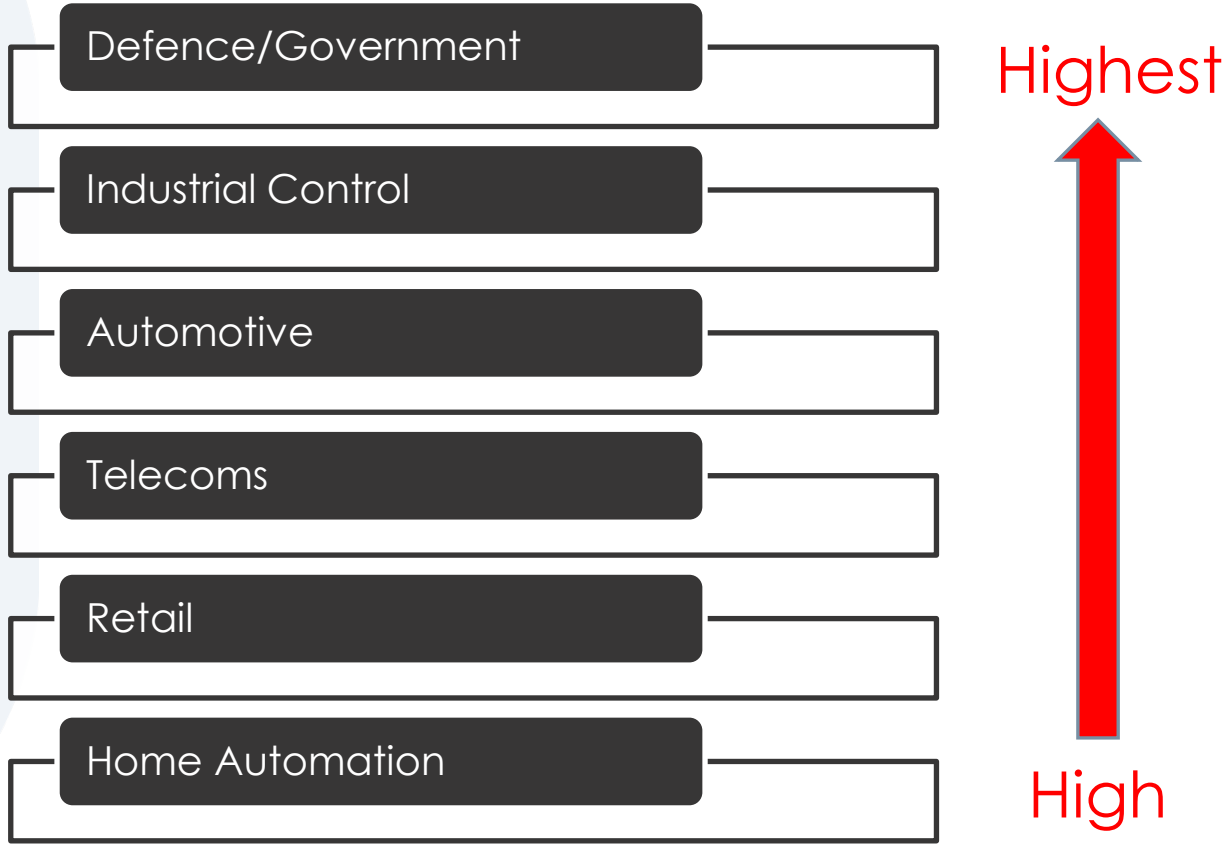
Connection to the Core

- Core systems provide configuration, control and monitoring
- Untrusted networks
- Geographical separation



Security Requirement

- IoT and other real-time communications applications need security able to counter the risk
- Dependent on location of Edge devices and Core control/management



IoT Vulnerabilities



CVE Vulnerability Reports

Protocol	# Reports	Latest Report
MQTT	318	2026-09-23
Zigbee	49	2026-09-29

Buffer Overflow Vulnerability (HackerOne)

```
# Craft CONNECT packet with password length = 65535 (0xFFFF)
printf '\x10\x1a\x00\x04MQTT\x04\xc2\x00\x3c\x00\x04test\x00\x04user\xff\xff' | nc localhost 1883
```

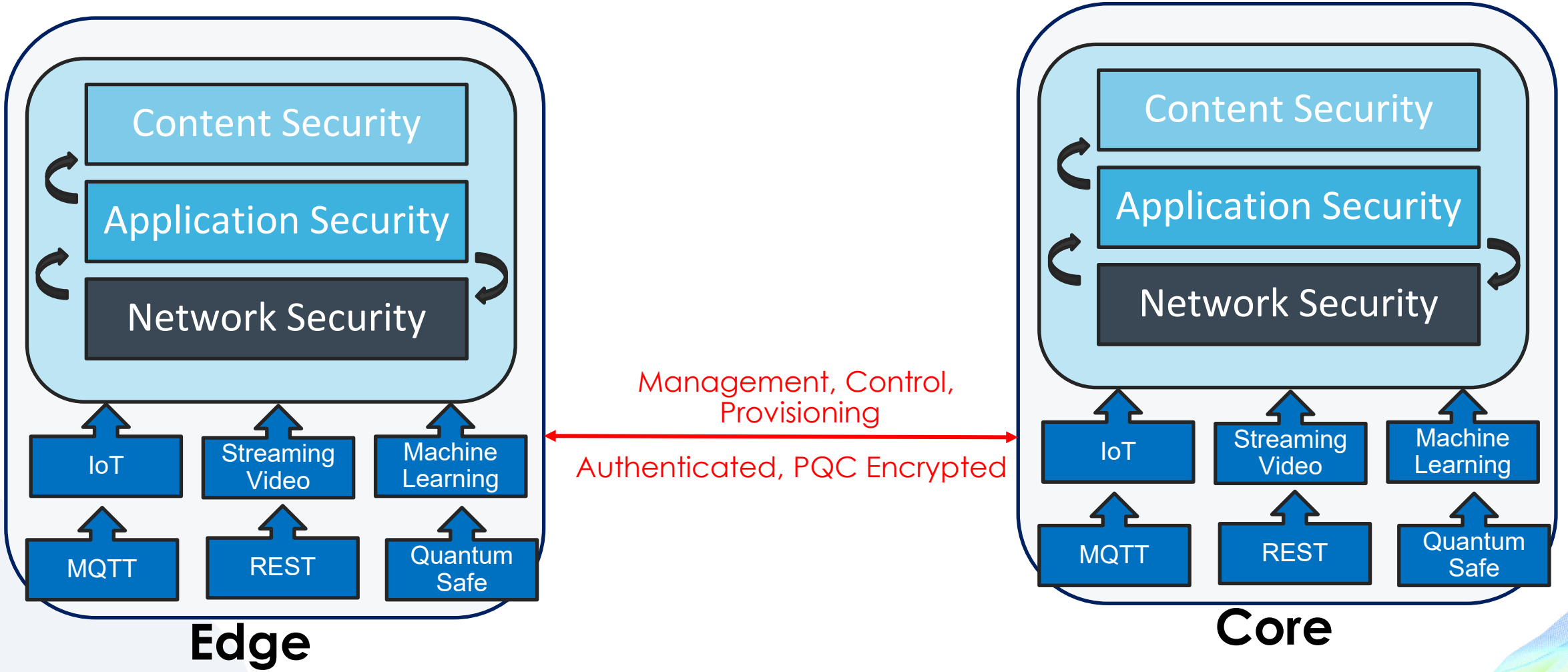


The attack triggered the defrost cycle on all our refrigerated display cases
temperature raised to 50 degree Celsius - 122 degrees Fahrenheit. 300 stores hit, loss tens of millions of Euros – October 2026

https://www.databreachtoday.com/hackers-attack-french-supermarket-freezers-causing-food-loss-a-33084

Common Edge/Core Design

Secure by Design



CHERI

Secure by Construction







Unicus Edge (CHERI-Risc-V Linux)

Mutually authenticated, PQC encrypted link (X25519 + ML-KEM-768)

Unicus Core (Arm Morello, CheriBSD, purecap)



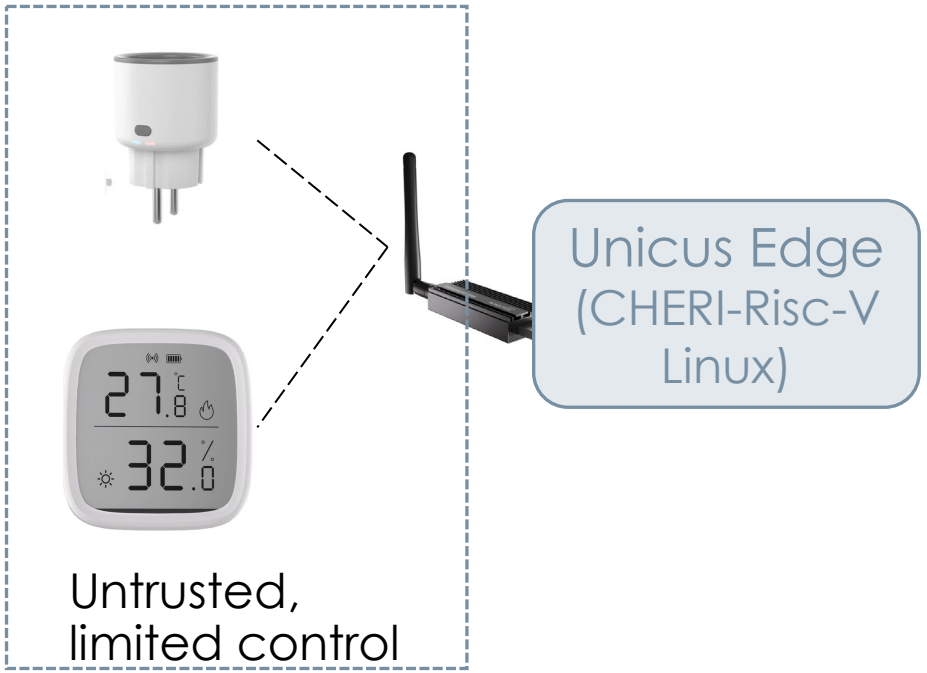
Configuration, Control, Monitoring

- Codasip Prime or QEMU
- Purecap Unicus Edge
- Purecap Zigbee Coordinator (new)
- Purecap MQTT
- Purecap telemetry and command relay

- Purecap Unicus Core
- **Purecap telemetry and command relay**
- Provisioning Server

CHERI -- Edge

Secure by Construction



- Codasip Prime and CHERI Risc-V QEMU
- ~~Zigbee2MQTT/Node.js stack~~
- Purecap MQTT broker
- Purecap Zigbee Coordinator (new)
- Two radio families: TI Z-Stack and Silicon Labs EZSP

Unicus: CHERI status



Unicus Platform	Application	Protocols	Core Status	Edge Status
Unicus RTC	VoIP Services	SIP, SDP, RTP	Ported and tested	N/A
Unicus SVSS	Streaming Video	RTSP, SDP, RTP	Ported and tested	Ported and tested
Unicus CXR	(Cloud) eXtended Reality	RTSP, RTP, others	Ported and tested	Ported and tested
Unicus IoT	IoT	Zigbee, MQTT, Matter, others	Ported and Tested (Morrello)	Ported and Tested (Codasip)

Future Plans



- CHERI an integral part of our design/development/test cycle
  - All new releases built on CHERI Hardware/QEMU
  - Testing on CHERI Hardware/QEMU
- Future Deployment on CHERI dependent on hardware availability and cost



THANK YOU

https://www.um-labs.com

info@um-labs.com

Located at semi | SEMICON EUROPA

CHERI™ and the CHERI logo are protected trademarks. Use of these marks is subject to the CHERI Alliance Trademark Policy – https://cheri-alliance.org/legal-and-policies/trademark/

This work © 2026 by CHERI Alliance is licensed under CC BY-SA 4.0 (Creative Commons Attribution-ShareAlike 4.0 International) – https://creativecommons.org/licenses/by-sa/4.0/