

CHERITech'25 CONFERENCE

Manchester, UK

2025

14th November

cheri-alliance.org



Flight To CHERI-UAV

Compartmentalizing PX4 modules on NuttX
using CHERI Capabilities

Donato Ferraro

PhD Student – Minerva Systems, University of
Modena and Reggio Emilia

○ Why protect drones?

Security, memory, and real-time challenges in PX4/NuttX

Applications

Civilian and Military domain

Operations

Data collection
Real-Time processing
RC or Autonomous

Software Challenges

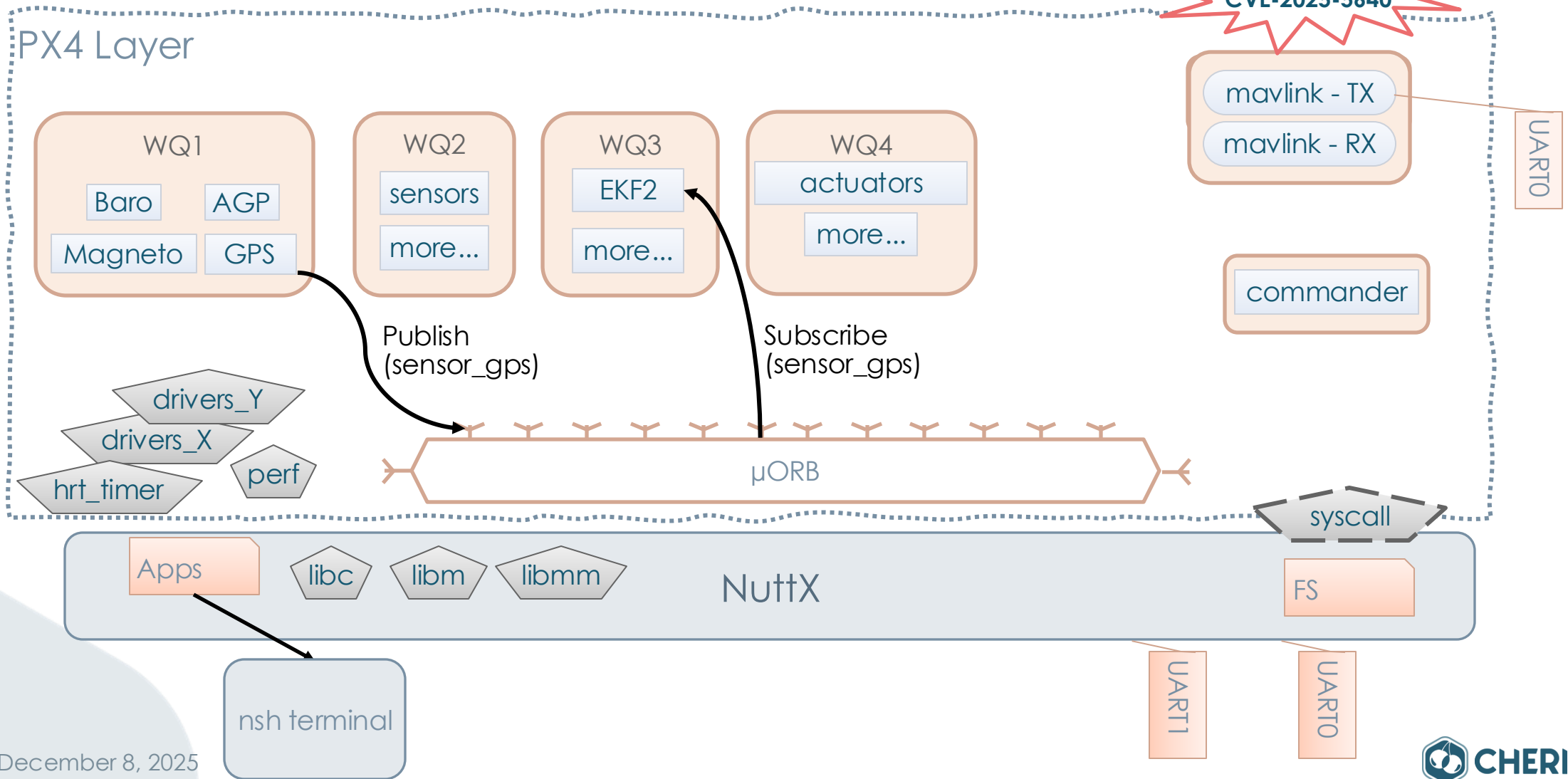
Flat memory space
Real-Time Constraints



PX4/NuttX architecture



Simulation-In-Hardware Setup



○ Why use CHERI capabilities?

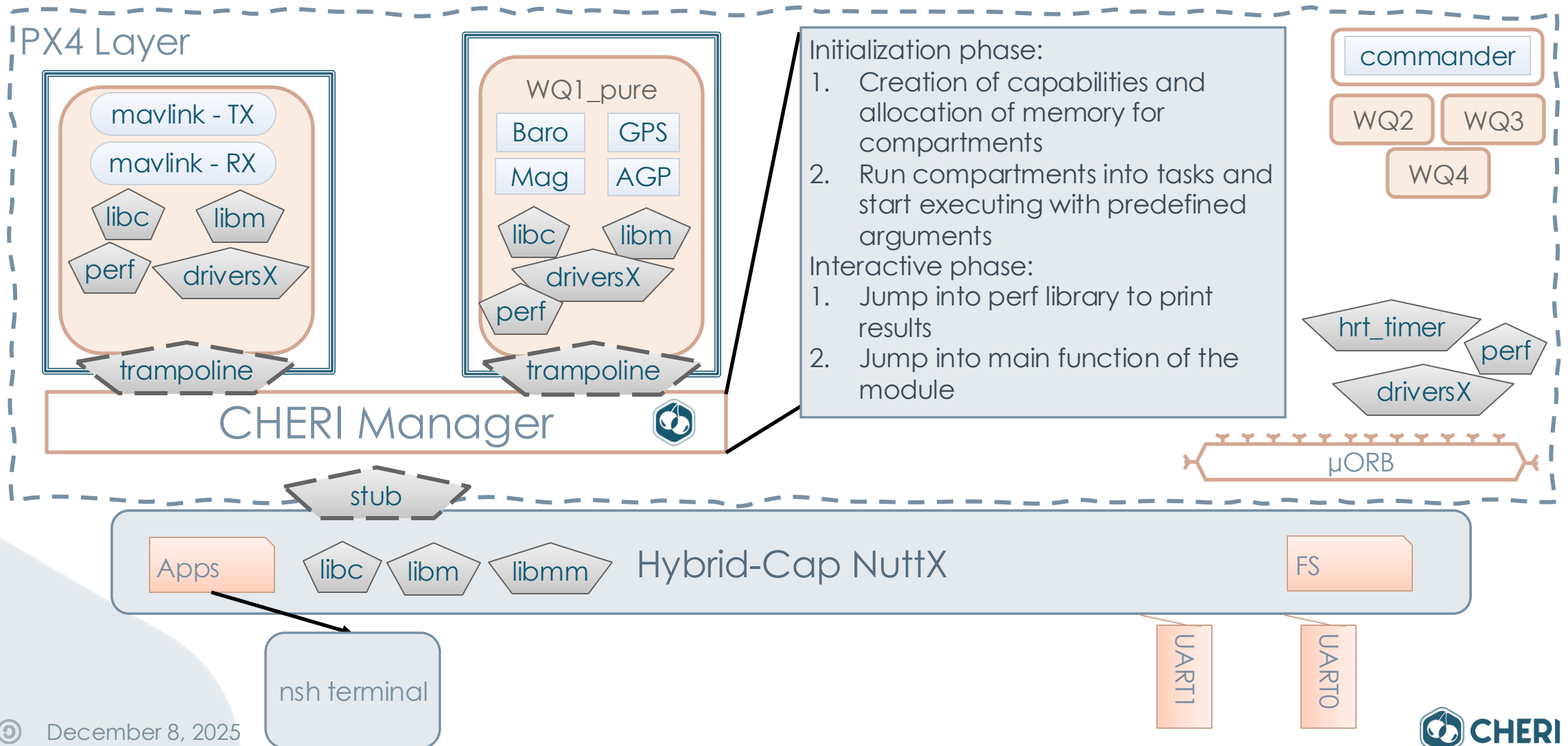
- Research and industry examples demonstrate that capability-based approaches can effectively protect real-world systems
 - *seL4 protected DARPA drone from DEFCON hackers[1]*
- CHERI brings capability directly to hardware
 - Fine-grained memory protection
 - Flexible protection
- Let's protect PX4/NuttX!
 - Running on CVA6-CHERI ISA v9 on FPGA



NuttX RTOS

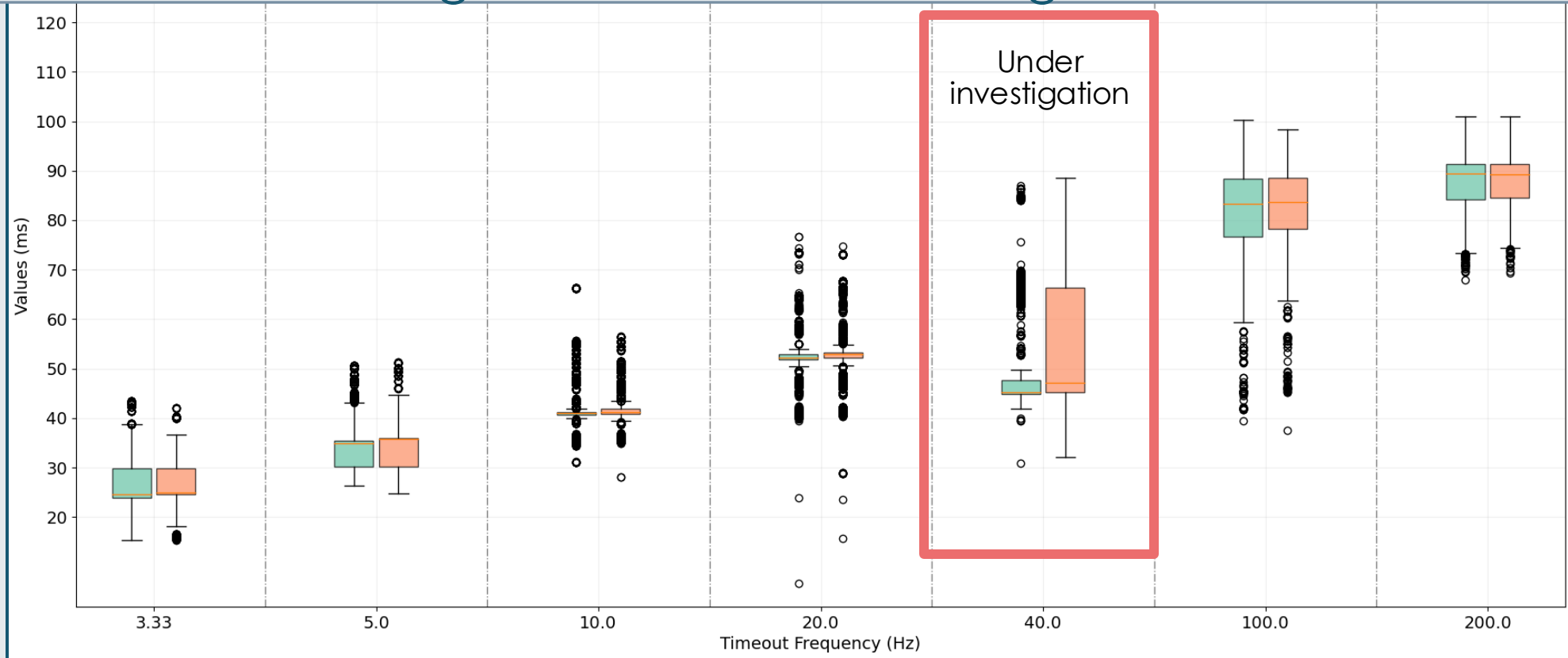
○ PX4/NuttX CHERI-enabled architecture

Simulation-In-Hardware Setup



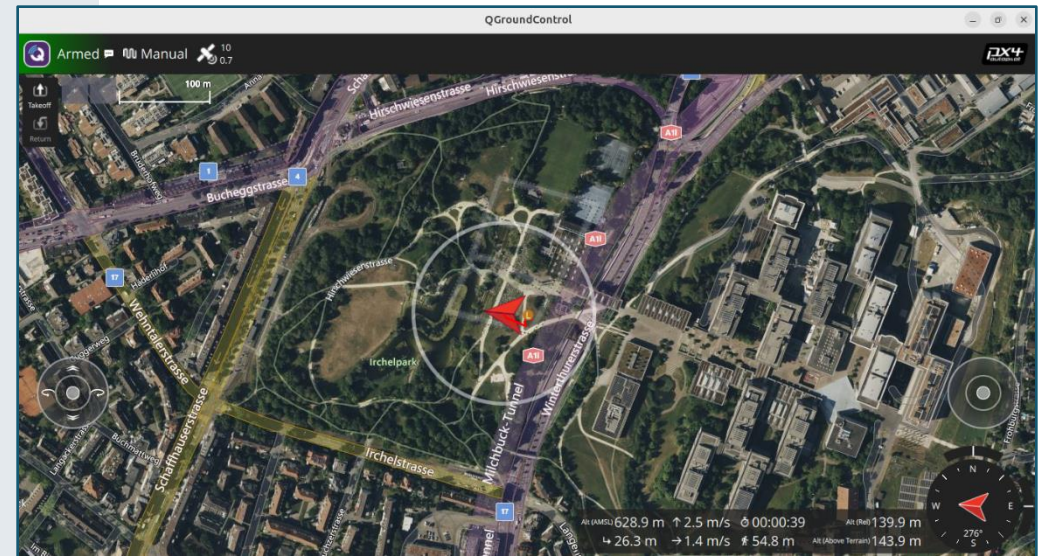
○ Preliminary evaluation

Average overhead: $< 1\%$
Average overhead considering 40Hz: $< 3\%$



○ Future Directions

- ◆ Comparison with MMU-based PX4/NuttX
- ◆ CVEs and CWEs analysis on PX4/NuttX (and similar)
- ◆ Real hardware tests are planned...when available.



CHERITech'25 CONFERENCE

Manchester, UK



2025

14th November

cheri-alliance.org

Thank you!

Contact donato.ferraro@minervasys.tech

Web www.minervasys.tech

