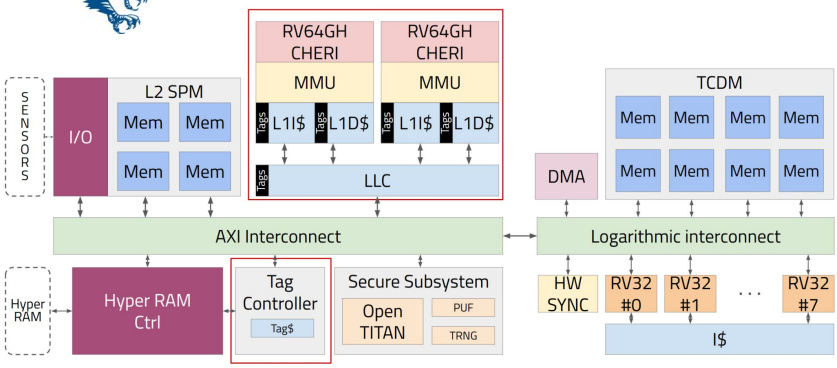
Security, Safety, and Predictability of CHERI RISC-V for Drone Systems

Scope of the Work

- There are several use cases in which drones can be deployed, such as autonomous systems, robotics, and real-time operations
- Current architectures: e.g., PX4/NuttX: for small embedded systems, security and safety isolation capabilities are not available
- CHERI has the potential of being a game changer in this field
- Investigate the potential impact of *CHERI RISC-V* in terms of autonomy, communication, and data processing in drone systems
- Evaluation of predictability, security, safety aspects, and real-time guarantees
- *Arm Morello* as alternative platform for comparisons

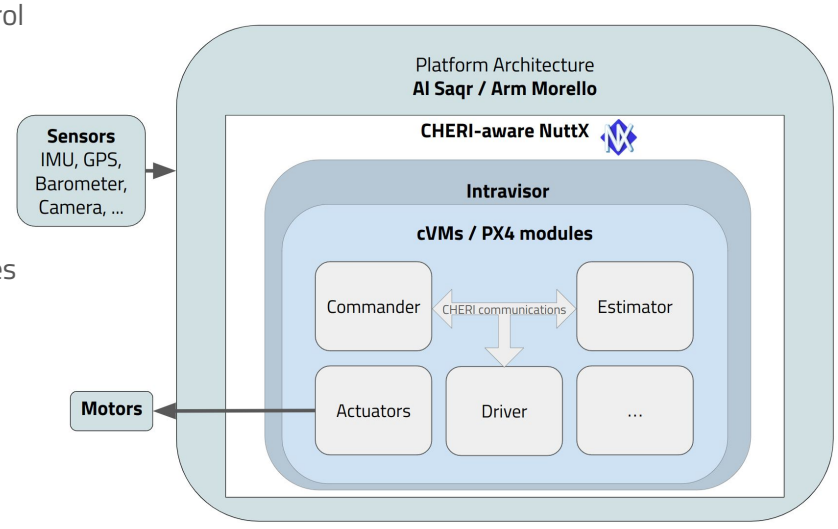
AI Saqr platform with **CHERI RISC-V**



- 2x RISC-V 64-bit cores (CVA6) with **Hypervisor extension** supporting **CHERI ISAv8**
- 8x RISC-V 32-bit accelerators (a.k.a. PULP Cluster)
- Tag Controller
- HyperRAM
- OpenTITAN Secure Subsystem
- Multiple I/O:
  - UART
  - SPI
  - Ethernet...

WiP: CHERI-UAV Software Architecture

- *PX4* is designed as a modular and flexible flight control system and is built upon *NuttX RTOS*.
  - Each module implements specific functionalities
- CHERI enables compartmentalization and secure communications between modules
- Investigation Direction:
  - **CHERI-aware Hybrid NuttX** with ***Intravisor*** [1] component and PX4 as cVMs
- UAVs HiL evaluation and assessment:
  - Measure end-to-end latencies, real-time properties (e.g., deadlines), etc.
- Current and next steps:
  - Implement ***CHERI-aware NuttX/PX4***
  - Evaluation of real-time and isolation capabilities
  - Comparison with Arm Morello
    - Isolation and real-time features
    - QoS
  - Combine HW-virtualization and CHERI
    - ***CHERI-aware Bao hypervisor***



[1]: CAP-VMs: Capability-Based isolation and sharing in the cloud. Vasily A. Sartakov, Lluís Vilanova, David Eyers, Takahiro Shinagawa, and Peter Pietzuch. OSDI 22, Carlsbad, CA, July 2022