ComputerScience

Boston University

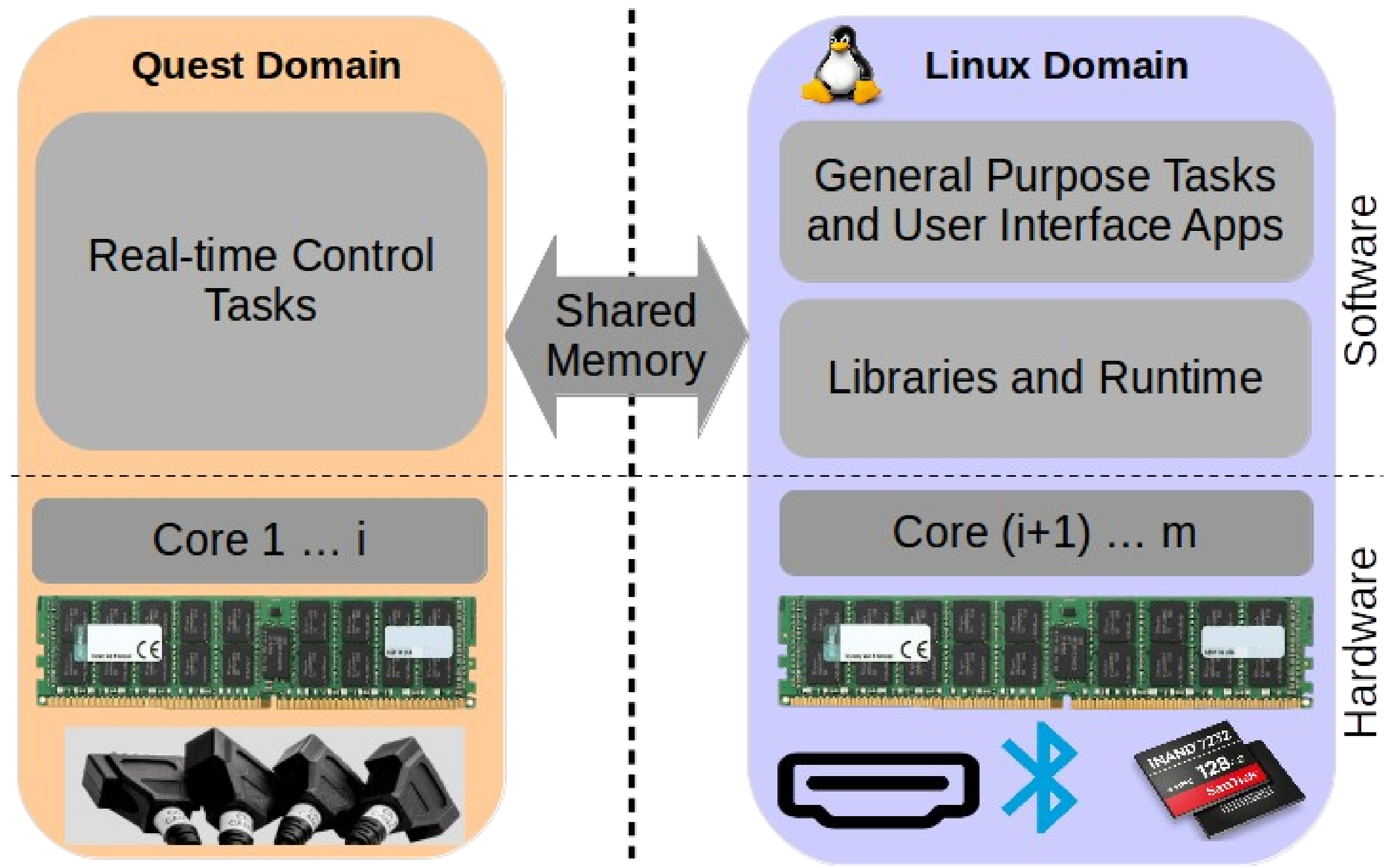
ModelMap: A Model-based Multi-domain Application Framework for Centralized Automotive Systems

Soham Sinha*, Anam Farrukh, and Richard West
Department of Computer Science
Boston University, USA (*presently at Nvidia)

BU Operating Systems and Services

Centralized Automotive Systems

- Consolidate timing-, safety- & security-critical vehicle functions with low-criticality services on the same multicore machine
- Mixed-criticality systems:
  - High-criticality RTOS domain: HVAC, BMS, VCU
  - Low-criticality legacy domain: IC, IVI, GPU-based ADAS services
  - Example centralized systems:
    - MB.OS (Mercedes), AreneOS (Toyota), Ultifi (GM), DriveOS (Drako Motors)
- DriveOS: Based on the Quest-V separation kernel [1], hosting a Quest RTOS [2] and a paravirtualized Yocto Linux



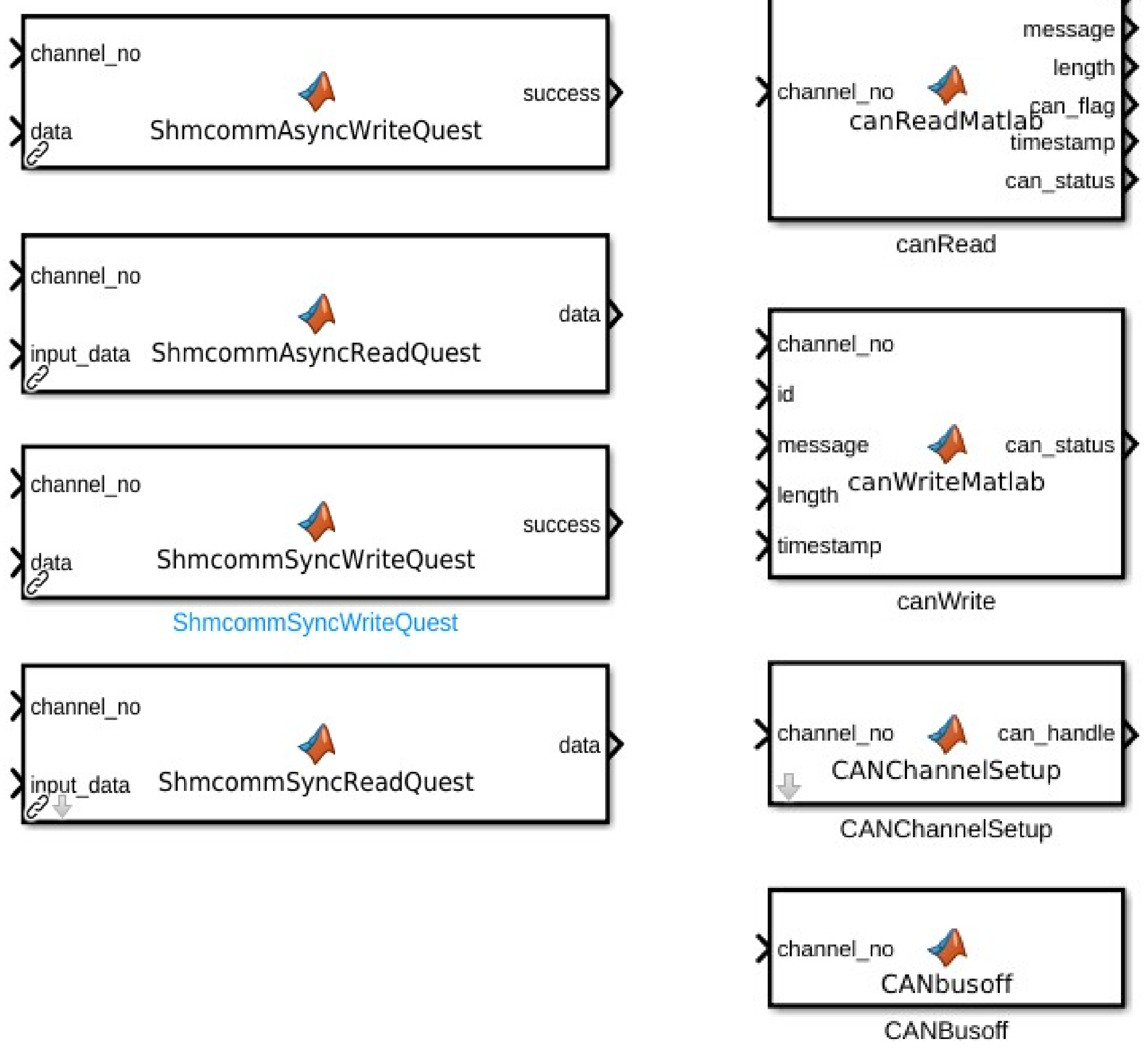
ModelMap Application Framework

- Model-based Multi-domain application framework for DriveOS using Simulink
- Generates *nested binaries* encapsulating executable code for multiple OS domains
- Executables are deployed using a nested binary loader
- Simulink blocks for inter-task & cross-domain communication, CAN I/O & real-time threads

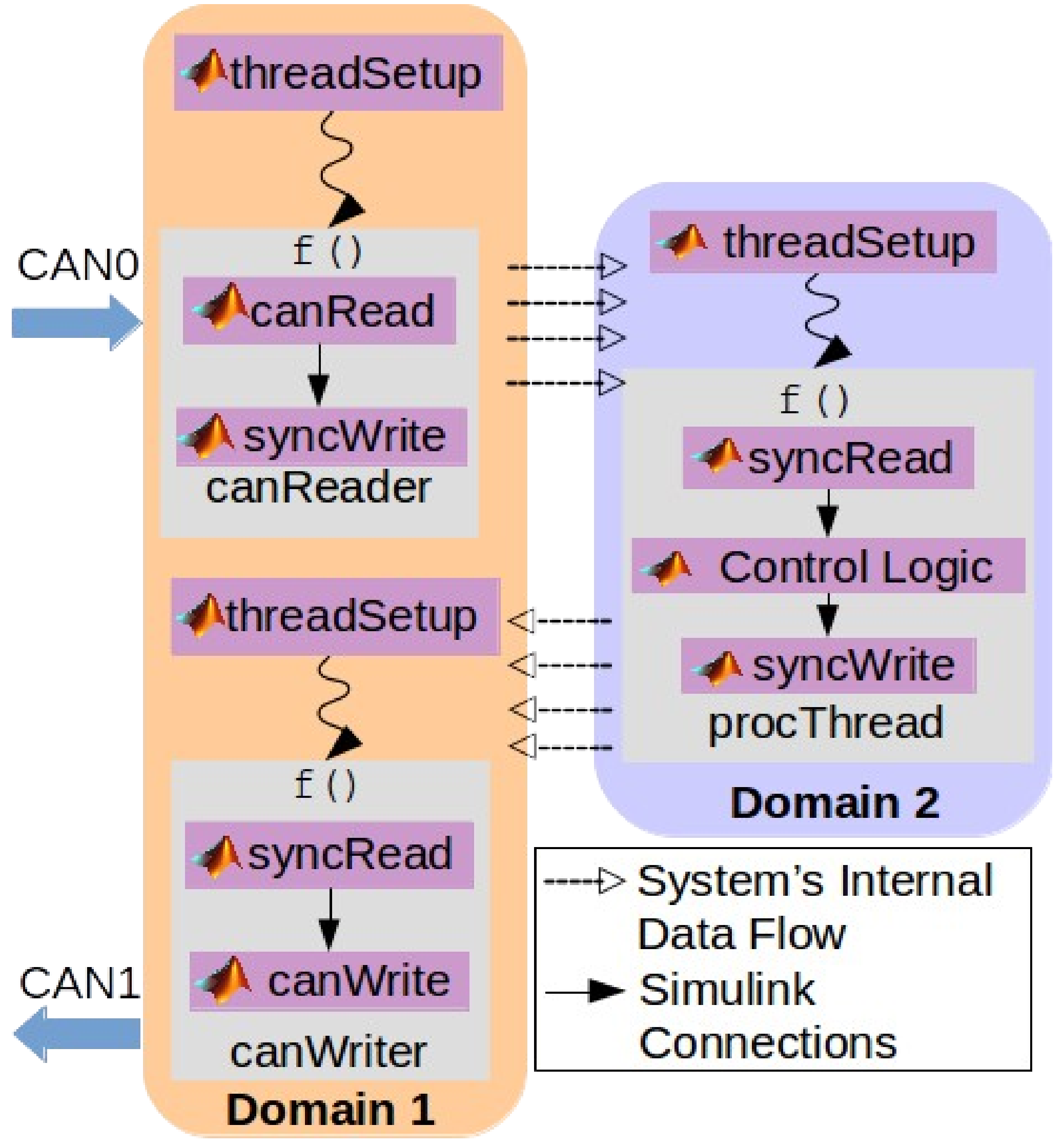
Example ModelMap Functional Blocks

(A)synchronous & cross-domain message passing

Real-time CAN I/O

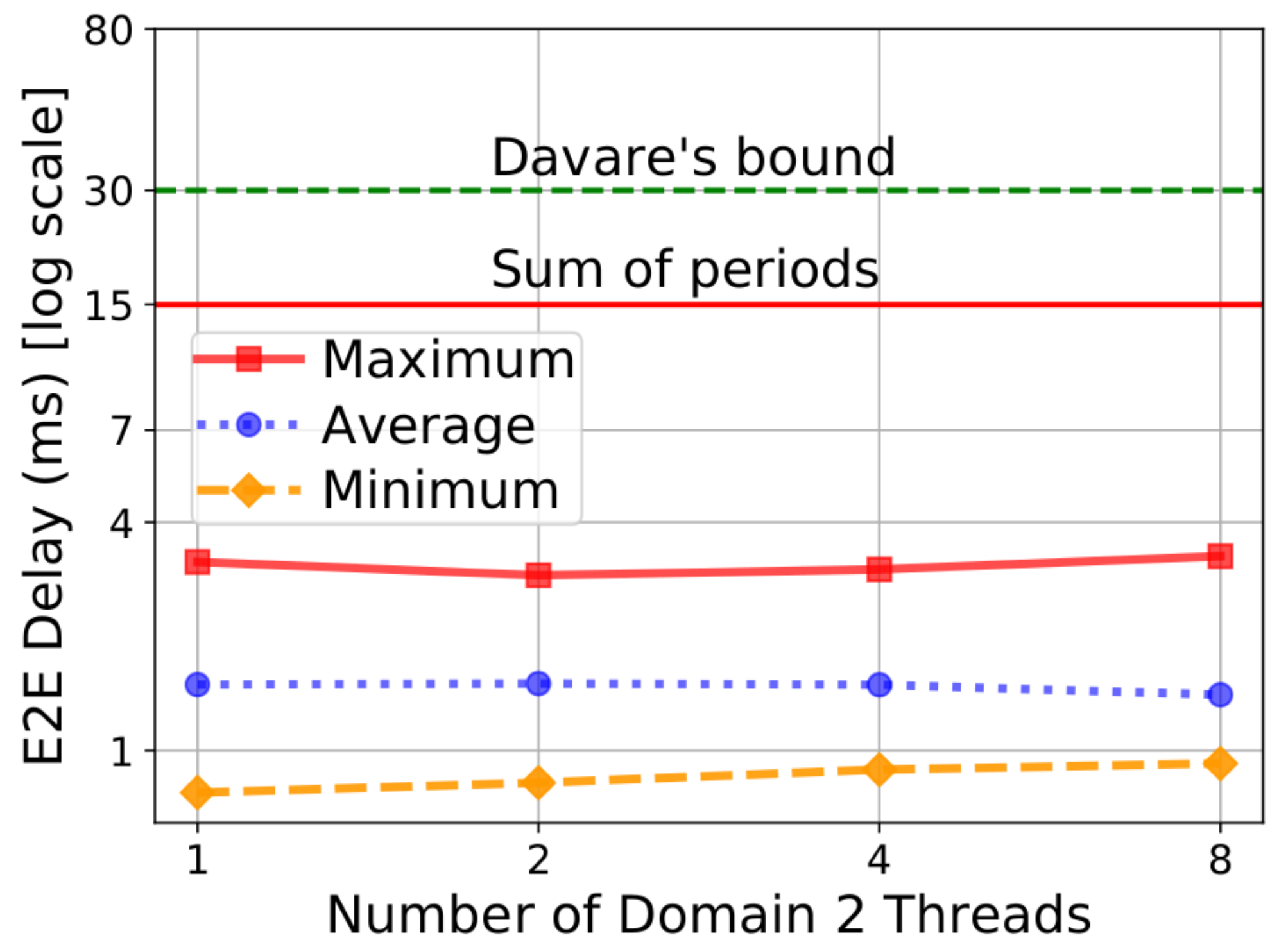


Mixed-criticality Simulink Model



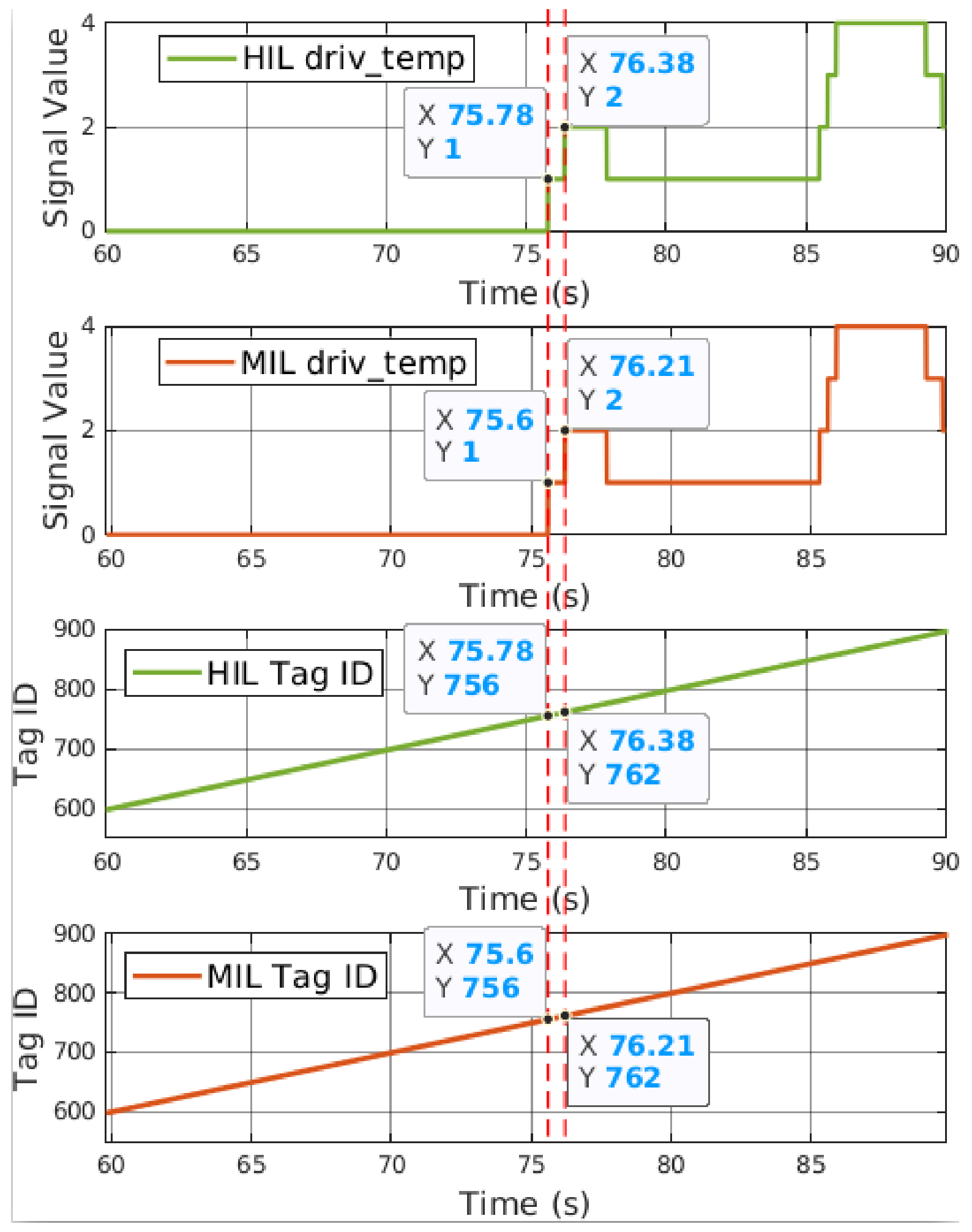
Case Study 1: Scalable CAN Gateway

- Real-time I/O in Quest RTOS to up to 8 Linux threads
- Predictable end-to-end latency within bounds



Case Study 2: EV HVAC

- Drako Motors' EV HVAC model ported from MotoHawk ECU to DriveOS using ModelMap
- Outputs of model-in-the-loop and hardware-in-the-loop simulation are matched to verify correctness



References

- [1] R. West, Y. Li, E. Missimer & M. Danish, "A Virtualized Separation Kernel for Mixed Criticality Systems", in ACM TOCS, Vol 34, Issue 3, Article 8, June 2016
- [2] www.questos.org

ICCAD 2022