A Safe and Secure ROS 2 Multi-Domain Architecture for AMD Embedded Heterogeneous Platforms

Alessandro Biondi, Accelerat SRL & Scuola Superiore Sant’Anna
Tomas Thoresen, AMD

© 2023 Accelerat Srl
Mixed-Criticality Software for Robotics

Multimedia

Third-Party Network

Perception

High-level Control

Low-level Control

Collision avoidance

Machine Learning

Planning

Field Network

Localization

© 2023 Accelerat Srl
Mixed-Criticality Software for Robotics

All in one platform to contain space, weight, wiring, power, and cost (SWaP-C)!

AMD Kria™ KR260 Robotics
Cyber-attacks starting from low-criticality software can compromise the mission of the system.
Safety issues that interest complex, mid-criticality software can propagate to safety-critical software.

AMD Kria™ KR260 Robotics
The temporal properties of safety-critical software can be disrupted by complex, mid-criticality software due to on-chip interference.
Multi-Domain Architecture

Criticality

Multimedia

Third-Party Network

Linux

Strong isolation boundary

Criticality

Perception

Planning

High-level Control

Localization

Machine Learning

Criticality

Low-level Control

Monitoring

Field Network

Collision avoidance

ROS

ROS 2

Strong isolation boundary
The CLARE Software Stack

Safe and secure islands on the same chip

Strong isolation between islands
(next-gen Hypervisor technology pioneered with research activities)

Automatic optimizations

Intelligent machine verification
(Design Rule Checking for avoiding mistakes in the configuration)

The expert is CLARE-Toolkit
(no need for experts in system-level software and hardware)

< 1 hour for the whole configuration

© 2023 Accelerat Srl
The CLARE Architecture

Configuration output
- User requirements
- Schedulers
- QoS regulators
- Resource partitioning
- Domains
- Middleware

CLARE-Toolkit

CLARE-Hypervisor
- Rich OS 0
- Rich OS 1
- RTOS
- Bare-metal runtime
- CLARE Basic Firmware

CLARE-Middleware (optional)

Domains
- Apps
- Resources
- User interaction
- Physical actuation
- Networking
- Remote updating
- QoS control mechanisms
- Safe fallbacks
- Monitoring
- Networking
- Machine learning
- Signal processing
- Control algorithms

Platform
- DSPs
- XMMU
- GPU
- Programmable logic
- Microcontroller-class Cores
- Application-class cores
- QoS control mechanisms
- Platform management cores

© 2023 Accelerat Srl
CLARE for Multi-Domain ROS

Mid-criticality domain
- Perception
- Planning
- Machine Learning

High-criticality domain
- Low-level Control
- Field Network
- Collision avoidance
- Monitoring

CLARE-Middleware (includes virtualized DDS)
- Real-time Linux
- FreeRTOS

CLARE-Hypervisor
- Programmable Logic
  - AI Accelerator(s)
  - Custom Peripherals

© 2023 Accelerat Srl
Main features relevant to Multi-Domain ROS2:

- Transparent, virtualized **publisher/subscriber** data distribution service
  - Uses CLARE’s built-in time-predictable, safe and robust **inter-domain communication**
- Signaling for **health and security monitoring**
CLARE-Hypervisor

**HARD REAL-TIME**
- Fixed-priority and EDF scheduling
- Bounded latency for event dispatching
- Super low-latency FastBoot
- Secure cache partitioning
- Bank-aware memory allocation
- Memory bandwidth reservation

**SECURITY**
- Address-Space Layout Randomization
- Control-Flow Integrity
- Secure boot for VMs
- TrustZone support
- Strong VM space separation
- Robust to denial-of-service and side-channel attacks

**SAFETY**
- Totally static
- MISRA compliancy
- Off-line auto-generated configuration
- Ongoing SIL4/ASIL-D certification
- ~ 8K LoC
- VM-level health-monitoring

© 2023 Accelerat Srl
**Strong Isolation**

CLARE-Hypervisor implements advanced mechanisms for **strong isolation**, which can be optimally and automatically configured from CLARE-Toolkit.

- **Secure cache partitioning**: Partitioning the shared levels of cache to control inter-core interference.
- **Bank-aware partitioning**: Allocating domains to different DRAM banks to control memory contention.
- **Memory bandwidth reservation**: Budgeting the number of transactions that can be issued by each core and each I/O peripheral over time.
- **Countermeasure for memory-related inter-domain DoS attacks**
- **Countermeasure for DRAM-related inter-domain side-channel attacks** (e.g., Row Hammer)
- **Countermeasure for cache-related inter-domain side-channel attacks**
Configuration of the entire CLARE Software Stack with availability of a rich template library

Automatic optimization of the deployment and configuration of complex mixed-criticality applications

Platform-awareness for low-level isolation mechanisms

Designed to be integrated with Chip Vendor Ecosystems

Options:
1. Browser-based on an Accelerat Cloud (SaaS)
2. On-premise

Chip Vendor Ecosystem

GUI Front-end
Stand-alone Back-end with support for scripting
High-level requirements:
- Criticalities and isolation capabilities
- Amounts of memory
- Desired bandwidths
- Security features
- Etc.

Performance estimations:
Bandwidth, Latencies, …

Low-level configuration:
- Spatial and temporal isolation settings
- Optimized distribution of the entire memory to comply with the requested configuration
- Etc.
Scalable AMD Kria™ Portfolio

Choose the **Starter Kit** ➔ Select the right **Production SOM** ➔ Develop your **Custom Carrier Card**

**KD240 DRIVES**
For Drives and Motor Control Systems

**KV260 VISION AI**
For Vision AI Cameras and Systems

**KR260 ROBOTICS**
For Robotics and Machine Vision Systems

**KRIA™ K24 SOM**
- Half the size of a credit card
- Power efficient
- ECC support

**KRIA™ K26 SOM**
- VCU and larger DPU
- 55% more I/Os
- Transceivers

© 2023 Accelerat Srl
Safety Certifications for AMD

> Functional Safety Certifications
  >> ISO 26262
  >> IEC 61508
  >> ISO 13849

> Certified
  >> Vitis/Vivado Developer Tools
  >> MicroBlaze compiler
  >> Zynq Ultrascale+ MPSoC
Target Applications for Embedded Developers

Robotics
- Joint Control
- Actuation
- Motion

Power Generation
- Pitch/Yaw Control
- Multi-level Inverter
- Communications

EV Charging
- Inverter Control
- V2G Communication

Medical Control
- Gantry and Bed
- Surgical Actuation
- Surgical Generator

Patient Care
- Sensor Fusion
- 3D Graphic Display
- Precision Calculations

Public Transportation
- Train Control / Mgmt.
- Comfort / Information
- Comms / Recorder
THANK YOU

See more at accelerat.eu and amd.com
All content and information on this presentation is for informational and educational purposes only. Although we strive to provide accurate general information, the information presented here is not a substitute for any kind of professional advice, and you should not rely solely on this information. Always consult a professional in the area for your particular needs and circumstances prior to making a professional, legal, instructional and financial decisions.