AUTOSAR Compatible Hypervisors for Supporting Cross-Company Workflows and Enhanced Safety and Security Requirements

Stuart Mitchell
Contents

AUTOSAR and the ECU workflow
• Integration – An AUTOSAR Success Story

Hypervisor Introduction
• What is it? Why is it necessary?

Hypervisors for Integration
• Intra- and Inter-company,
• Safety and Security
Current System – Function per ECU

- Current model places one functional sub-system per ECU
- Expensive due to many ECUs
- Good for safety and security
Integration – Multiple Functions per ECU

- Larger ECUs reduce complexity of vehicle and hence cost
- Multiple functional sub-systems per ECU
- Reduced safety and security
Functional Integration

- Reduce complexity of vehicle topology
  - Reduce ECU count
  - Need more powerful ECUs
    - Multicore

- Functional integration is an AUTOSAR success story
  - Aggregate SWCs on ECU
  - Reconfigure and regenerate MCAL / BSW / RTE

- AUTOSAR provides mechanisms to protect against **unsafe** and **insecure** systems
But there can be problems
- Integrating ASW from multiple vendors
  - No single team: Who is responsible?
- SW Sharing
  - Who is liable when ECU fails?
  - How to retain security barriers of a multiple ECU system?
  - How do multiple vendors protect IP?
- Debugging
  - Who performs root cause analysis?
    - what? why? who?
  - Long round trip time to get fix
  - Can different RTE/BSW configurations trigger/mask bugs in ASW?
System integration using Hypervisors

- Hypervisors
  - Different software providers (e.g. OEM and Tier 1) to develop SW stacks separately
  - Integrate with low effort.
- Each VM becomes a virtual ECU
  - No need to share IP on the same virtual ECU
  - Temporal and Spatial separation for safety and security
- Integration and validation of each virtual ECU can be performed without the need to coordinate with other software providers
  - If a virtual ECU fails it’s clear which one failed and, therefore which supplier is responsible.
Hypervisor based Cross-Company Workflow

Integrator

Hypervisor

Supplier 1

Hypervisor

Supplier 2

Hypervisor

ECU

Integrator

AUTOSAR Hypervisors for Safety and Security

Hypervisor for Workflow
Abstract Architecture

AUTOSAR Hypervisors for Safety and Security

What is a Hypervisor?

Virtual Machine

Virtual Machine

Hypervisor

MPU abstraction
Exceptions
Services

VM-VM Comms VDE
Shared IO VDE

Own IO
Own IO
CPU 
MPU

Shared IO
CPU 
MPU
Own IO
Own IO

ECU “image”.

Safe, secure inter-VM comms

Virtual Device Emulator (VDE) for HW Arbitration

IO via HV ➔ Slow

Direct IO ➔ Fast

Safe, secure inter-VM comms

Virtual Device Emulator (VDE) for HW Arbitration

IO via HV ➔ Slow

Direct IO ➔ Fast
Automotive Domain-specific Requirements

- Contradictory requirements
  - Resolve via configuration

- Configuration allows some requirements to be removed.
  - E.g. Diagnostics might be configurable.

- How many of these requirements are supported by current commercial hypervisors?
  - Very few.

Small Systems
- Low interrupt latency
- Small footprint
- Hard Real-Time
- MPU
- Static config.
- Debug support

Large Systems
- Peripheral support
- Feature download
- Soft Real-Time
- MMU
- Dynamic config

All Systems
- Certification
- Boot loader
- Safety
- Security
- Portability
- Multicore

Contradictory requirements
- Resolve via configuration
- Configuration allows some requirements to be removed.
- E.g. Diagnostics might be configurable.
- How many of these requirements are supported by current commercial hypervisors?
- Very few.
Architecture of a Real-Time, Safety-Critical Automotive Hypervisor

- RTA-HVR – A Real-Time Automotive Hypervisor
  - "Bare Metal" Hypervisor: Runs directly on underlying hardware
  - Para-virtualisation: Guest OS and MCALs make system calls via the hypervisor
  - Safety and Security: Makes use of the native MMU/MPU and supports resource sharing between virtual machines (VM)
  - Static build-time configuration: Maps VMs to cores for real-time
Advantages of a Hypervisor Approach

- Configuration using ARXML
  - Familiar tools
  - Proven robust cooperation model
  - Same code generators

- Support Integration of SW from multiple vendors
  - Single team responsible for each stage
  - Liability clear
  - Hypervisor ensures safety and security
  - IP protection
  - Freedom from interference – e.g. temporal properties of other VECUs

- Debugging
  - Isolated and Simplified (quicker) round trip for fix
Virtualized software

- Para-virtualized OS within VM
- SW Stacks can be individually developed, configured and updated

Security Domain

- Provides dedicated security services
- Crypto services
- Secure Boot
- Access to HSM
- Communication Stack with Firewalling

Hypervisor

- Compatible to Automotive microcontrollers
- Enables privileged security domain
- Offers virtual machines behaving like a full computing system

Automotive ECU Hardware

- Standard ECU HW
- Support of Automotive HSMs (Bosch HSM)
AUTOSAR Hypervisors for Safety and Security
RTA-HVR

- **RTA-OS**
  - Separation at application SW level
  - IP sharing
  - High integration
  - AR safety & security
  - Automotive µCs
  - Multi-core

- **RTA-HVR v1.0**
  - Full separation of SW stacks
  - SW Stacks can be independently integrated/tested
  - Full safety & security separation between SW stacks
  - Automotive µCs
  - Static configuration of one partition/core

- **RTA-HVR v2.0**
  - Integration of dedicated security functionality
  - Support more automotive µCs
  - Static configuration of multiple partitions per processing core

- **RTA-HVR v3.0**
  - Support integration RT safety critical vehicle functions with intensive processing
  - Support for µPs with many processing cores
  - Static and dynamic configuration of >1 partitions per core

Now 2016 2017 2018+
Summary

- AUTOSAR has achieved its aim
  - Abstraction to control complexity
  - Support functional integration on ECUs

- But it’s perhaps been too successful!
  - Applied to many use cases not originally foreseen

- Virtualization means we can support integration
  - Keep what’s good
  - But prevent new failure modes

- Automotive domain specific requirements
  - ETAS has developed Type-1 Hypervisor to meet the needs of AUTOSAR