Safety with Embedded Multicores
Glenn Farrall: Microcontrollers Infineon UK
2014-09-23
Agenda

- Automotive ECUs
- Automotive Trends
- AURIX™ MultiCore
Automobiles are no longer a composition of mechanical systems.

- In 2008: 10,000,000 lines of code in the average in premium vehicles.
- Software is responsible for up to 80% of the innovation in premium vehicles.
- 30% to 40% of the added value in the automotive industry is based on software.
- The software runs on variously sized ‘Electronic Control Units’– mixture of 8-bit (still!) 16-bit and 32-bit ECUs
Increasing electronic functionality => increasing number of ECUs

“There simply is no more room or mass allowance to package additional ECUs; up-integration is a must.”

Robert Rimkus, General Motors, 2013 AUTOSAR Conference
Agenda

- Automotive ECUs

- Automotive Trends
  - MultiCore
  - AUTOSAR
  - ISO26262

- AURIX MultiCore
MultiCore for Automotive Performance

- Clearly a need for more performance in automotive

- Why multicore and not higher performance uniprocessors
  - 300MHz -> 600MHz?

- Power limitations and memory issues similar to other industries, just occurring at a lower performance level
  - Passive cooling for reliability + cost;
  - Higher leakage issue (under bonnet 150°C or higher);
  - Avoiding expensive packaging (ceramic, heat spreaders, etc.)

- eFLASH – capacity scaling with technology nodes, but not latency
  - Complicated memory hierarchies are anathema to Hard Real Time multiprocessors with 2-3 cores at 200 and 300MHz now common offerings.
Agenda

- Automotive ECUs

- Automotive Trends
  - MultiCore
  - AUTOSAR
  - ISO26262

- AURIX MultiCore
AUTOSAR

- **AUTomotive Open System Architecture**: goals include
  - Definition of a modular software architecture for automotive ECU
  - Consideration of HW dependent and HW independent SW modules
  - Integration of SW modules provided by different suppliers to increase the functional reuse

- To aid in legacy porting, AUTOSAR does not mandate a protected operating system – instead scalability classes
  - SC1: deterministic RTOS baseline
  - SC2: protected timing
  - SC3: protected memory (MMU/MPU)
  - SC4: protected timing and memory
AUTOSAR Releases

AUTOSAR worldwide: Exploitation

Volume of ECUs with AUTOSAR

© 2013 AUTOSAR
Agenda

- Automotive ECUs

- Automotive Trends
  - MultiCore
  - AUTOSAR
  - ISO26262

- AURIX MultiCore
ISO 26262
Automotive Functional Safety Standard

- Adapted from generic IEC 61508 for Electrical/Electronic safety systems
- Published in 2011
- Takes into account
  - automotive life cycle
  - automotive environment, driver controllability, etc.
- Specifies Automotive Safety Integrity Levels
  - low ASIL-A to high ASIL-D
  - & QM; no safety required

Passive Safety
- Airbag
- Restraint
- Driver Assistant

Active Safety
- Power Steering
- Central Chassis
- Suspension
- Braking
ISO 26262
System Development

- Development rigour for both SW and HW is specified
  - Assumption that SW developed to the required level is then ‘fault free’
  - Running ASIL code of different levels (+QM) on the same ECU is possible provided it can be shown there is ‘freedom from interference’
  - Hardware will have fault rates, that must be managed to a lower failure rate

“**A quantitative analysis** of the hardware architecture with respect to the single-point, residual and dual-point faults shall provide evidence that target values ... have been achieved”

<table>
<thead>
<tr>
<th>ASIL</th>
<th>Random hardware failure target values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>&lt;10⁻⁸ h⁻¹</td>
</tr>
<tr>
<td>C</td>
<td>&lt;10⁻⁷ h⁻¹</td>
</tr>
<tr>
<td>B</td>
<td>&lt;10⁻⁷ h⁻¹</td>
</tr>
</tbody>
</table>

i.e. for ASILD: show that with technology fault rate system does not result in failure rate >10⁻⁸ per hour.
Agenda

- Automotive ECUs
- Automotive Trends
- AURIX MultiCore
  - Introduction
  - ISO26262 support
  - Customer experience
TriCore Introduction

- Most widely distributed microcontroller you’ve probably never heard of
  - In approximately 50% of all automobiles produced this year
- 32-bit architecture with a focus on hard real time
  - Combines RISC and DSP support for C and DSP native data types.
- Application areas
  - Automotive powertrain
  - Stability control systems
  - EVehicle: charging, BMS etc.
  - Industrial control
Embedded Flash for code and EEPROM emulation. No external memory required.

Cores and Memory on full frequency 64-bit crossbar

Automotive specialised peripherals (CAN, FlexRAY, LIN, SENT, PSI, etc.) on low speed 32-bit bus
Agenda

- Automotive ECUs
- Automotive Trends
- AURIX MultiCore
  - Introduction
  - ISO26262 support
  - Customer experience
AURIX Family
Safety Features

A

Lockstep core(s)
Soft Errors and ISO26262

- Alpha and other particles will induce soft-errors in most Si based processes.
- SER (Soft Error Rate) is high enough to violate ASIL-D failure rate without mitigation.
- Multiple Approaches possible

**Time Separation**
- ~ double execution time
- Safety on demand

**Spatial Separation**
- some execution time increase

**LockStep’d Logic**
- No execution increase

**Simplest quantitative safety argument**

Alpha and other particles will induce soft-errors in most Si based processes. SER (Soft Error Rate) is high enough to violate ASIL-D failure rate without mitigation. Multiple Approaches possible.

- Time Separation
  - ~ double execution time
  - Safety on demand

- Spatial Separation
  - some execution time increase

- LockStep’d Logic
  - No execution increase
  - Simplest quantitative safety argument
AURIX Family
Safety Features

- **A**: Lockstep core(s)
- **B**: SRAM ECC (w. SECDED+)
- **C**: Flash ECC (w. DECTED +)
- **D**: SRI Transport Checked
- **E**: Safe DMA
AURIX Family Safety Features

- Lockstep core(s) (A)
- SRAM ECC (w. SECDED+) (B)
- Flash ECC (w. DECTED +) (C)
- SRI Transport Checked (D)
- Safe DMA (E)
- Redundant, spatially separated peripherals (F)
- Bus Protection for Memory (G)
- Bus Protection for Peripherals (H)
- Safe Interrupt Processing (I)
- Clock Monitoring (J)
AUTOSAR + Safety Critical Challenges

- AUTOSAR scalability classes provided through
  - Core MPU
  - Temporal protection system (cannot be turned off like interrupts).

- ISO26262 Freedom from interference (spatial) is provided through bus protection mechanisms which can be viewed as a system MPU

  - Distinct from Core MPU – which could always be incorrectly setup by QM software

  - System MPU can be setup once then locked down by highest ASIL software developed for ECU.
Temporal isolation is more difficult with implicit sharing of a resource

- i.e. multiple cores accessing an interconnect, a memory or a memory controller

- AURIX design (crossbar for compute cluster) allows for allocation of cores to memories without sharing
  - Requires judicious placement and non shared libraries

- Only resource not timing isolated is the peripheral bus
  - Strict priority arbitration is possible to bound access for safety critical code;
  - Allows only a small timing interference effect
Agenda

- Automotive ECUs
- Automotive Trends
- AURIX MultiCore
  - Introduction
  - ISO26262 support
  - Customer experience
Customer migration experience

- Continental Engine System Software ported to AURIX multicore (see references) with AUTOSAR like RTOS
  - around 700,000 of lines of code and 20,000 variables.
  - training of ~1000 programmers to be multicore aware (this is not only development but maintenance etc.)
  - an exhaustive identification of the use cases of shared variables (around 150,000 data access points);
    e.g. RPM used in more than 300 different modules
  - creation of own tooling to automate buffering of shared variables depending on code allocation to same or different cores
  - use of commercial tooling to optimise placement vs performance vs data footprint
May 2013: SWC Based distribution

Today: Runnable based distribution
Thank you for your attention
Innovative semiconductor solutions for energy efficiency, mobility and security.
References

- **Managed and Continuous Evolution of Dependable Automotive Software Systems;** A. Rausch et al., in 2014 Symposium of Automotive Powertrain Control Systems

- **Introducing Multi-Core at Automotive Engine Systems;** D. Claraz, F. Grimal, T. Leydier, R. Mader, G. Wirrer, in ERTS 2014

- **EMS3 PowerSAR® Platform - A Multi Core Software Implementation for Powertrain Applications based on AUTOSAR;** R. Mader, in 2014 Symposium of Automotive Powertrain Control Systems

- **INTERNATIONAL STANDARD ISO26262 Road vehicles — Functional safety**