

Embedded World 2008

Bart van Kuik



Netherlands Institute for Space Research

Timing verification

- Problem: testing doesn't show all timing problems
- Typical testing: start all tasks at the same time
- BMW active steering (extra comfort)
- Gathered data with trace tool
- SymTA/S tool asks how long the interrupts and events *could take*.



Software in automotive

Challenges:

- testable code
- maintainable code
- modular (new car models)
- Dependencies explicit
- C++ templates: compile-time checks
- Configuration: static instantiation
- Lifecycle manager
- Continuous integration

Generate code from time constraints

- TDL: timing definition language
- Focus on declaring time that tasks take

```
mode main [period=10ms] {  
    . . .  
    . . .  
}
```



Custom hardware acceleration

- Tools like Catapult C
- Subset of C is synthesized in HDL
- Careful with doubles and pointers
- Functions become HW blocks
- Experience necessary



Embedded Filesystems

- Wikipedia: > 100 FS
- FAT ubiquitous
- JFFS is journalling
- Trade-off
- NAND is cheap
- NOR allows random access and can run code in place



Embedded systems power management



- BIOS -> APM/ACPI -> Application
- Enables fast booting
- Turn EVERYTHING off except put RAM in selfrefresh
- When warm booting, just reinitialize peripherals

Energy Monitoring in homes

- Small power monitoring device
- System: client/server
- Sensor: Open Source Gateway Initiative multi-bus controller
- Autodiscovery of new devices
- Control via browser

Home Appliance Safety

- Cut off heaters, close washing machine door
- Class B: HW as well as SW protection
- Class C: only SW
- Periodic selftests
- Too much interrupts
- Clock CPU still OK
- RAM checks
- Flash CRC test

Integrated Modular Avionics

- Move towards putting tasks together on one board
- Put tasks in virtual machines
- Main contractor has control
- Configuration data very large (50k lines)
- In XML
- Direct move from XML to binary form
- Special compiler

Monitoring body temperature

- Microcontroller is stuck on a glove with sensors
- Quantify emotions
- Data is validated using SEVA
- Standard method Oxford University
- No old data
- No double data
- Detect missing data
- Et cetera

Software Certification in safety critical applications

- Specifications not met
- Timing errors
- Run-time errors
- 30 to 40 pct. is a run-time error
- Testing is more suited for functional testing
- IEC61508 is mother of all safety standards
- DO178B avionics
- The standards ask to quantify the remaining risk
- PolySpace, for Matlab

Time Partitioning

- Typical: threads
- Priorities aren't enough
- Partitioning: groups processes
- Prioritize among threads now safe



Time sync in hardware

- IEEE 1588: protocol syncs clocks across buses
- Large variation: time difference
- Freescale does this in a custom ethernet interface
- In-band
- Out-of-band



Timing Analysis and Optimization

- Large loops that don't fit in CPU cache
- Domino effect: cache miss gets repeated
- Future: extract timing model from HDL