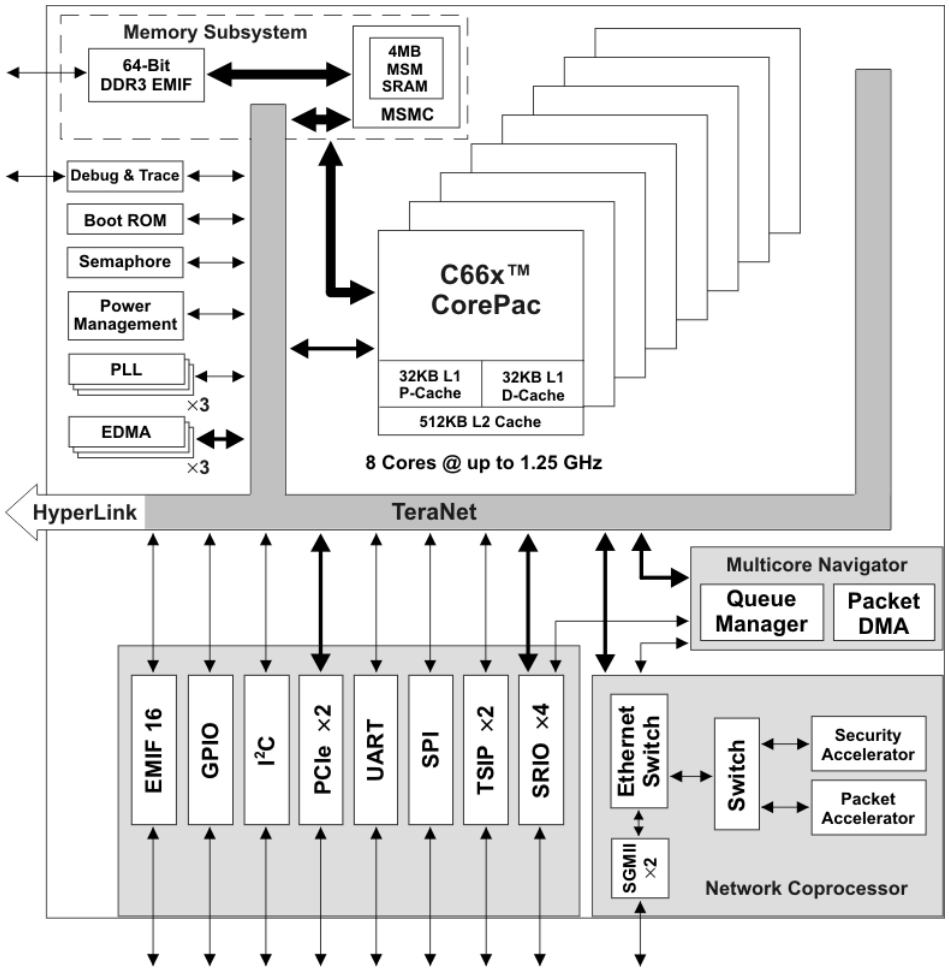
Protected mode RTOS: what does it mean?

Dr. Bernhard Sputh
bernhard.sputh@altreonic.com

Altreonic NV
Gemeentestraat 61 Bus 1
3210 Linden
Belgium

August 21, 2015

Current Trends in Embedded Systems
The RoC (Rack on a Chip)



Texas Instruments C6678

Assured Reliability Resiliance Level

Level	Definition	Measure
ARRL-0	The component might work ("use as is").	None
ARRL-1	The component works as tested.	Testing
ARRL-2	The component meets all its specifications, if no fault occurs.	+Formal proof.
ARRL-3	+ Guarante to reach a fail-safe or reduced operational mode upon a fault.	+Fault detection, containment, and preventing error propagation.

Altreonic

Why Protection is needed?

- Formal checking checks only models of the software, and is only sufficent for ARRL-2.
- The industry still develops applications using C/C++.
- Humans are imperfect!
- The environment may induce faults:
  - Bit-flips due to alpha particles.
  - Power glitch induced problems.
  - Faulty components.
  - ...
- For ARRL-3 fault detection and 'containment' are required, i.e. Protecting against unintended behaviour.

Altreonic

Current Approach Hypervisors

- Function:
  - Separate Applications in different Partitions.
  - Partitions cannot access the memory of other partitions.
  - Partitions get scheduled in time, i.e. time-sliced in the area of 1 – 100ms slices.
- Issues:
  - Time-slicing affects real-time behaviour.
  - Memory only protected at the partition level.

VirtuosoNext Approach

- Formally developed distributed RTOS for heterogeneous Systems;
- Virtual Single Processor (VSP) Programming Model;
- Programming with Interacting Entities, a Pragmatic Superset of CSP;
- Static allocation of Entities.
- Priority based Scheduling of Tasks.
- Tasks run separated in memory (memory protection). Currently supported on:
  - ARM-Cortex-M3 (MPU)
  - ARM-Cortex-A9 (MMU)
- Code is marked read only.
- Data is marked not-executable.

Altreonic

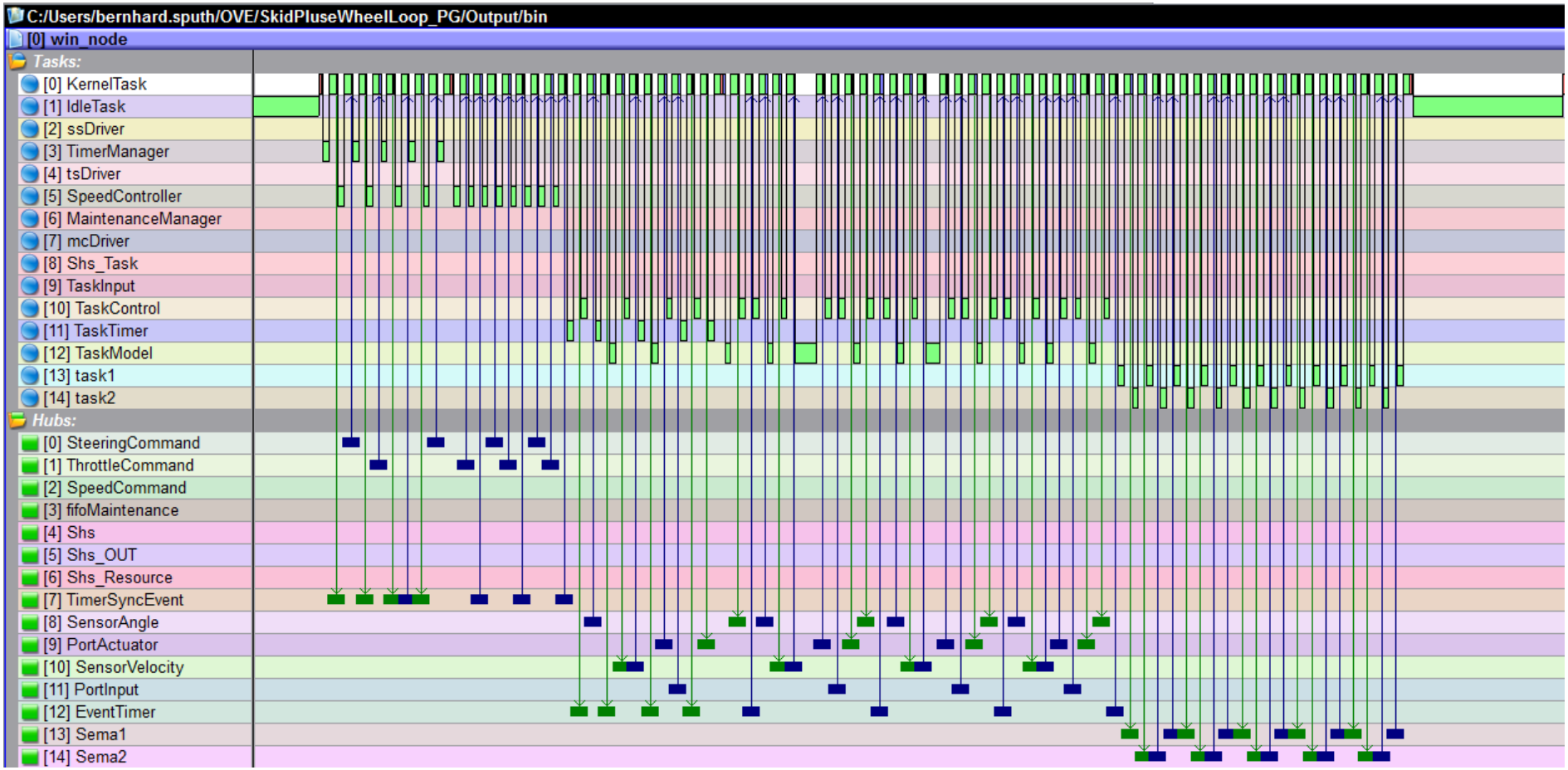
ARM-Cortex-M3 MPU Protected Mode

- Variable region size (32B, 64B, 128B, – 4GiB).
- Region alignment depends on region size.
- 8 regions in parallel.
- Context Switch had to be rewritten to reconfigure the MPU.
- The build process now performs memory mapping of Entities.

ARM-Cortex-A9 Memory Management Unit (MMU) Protected Mode

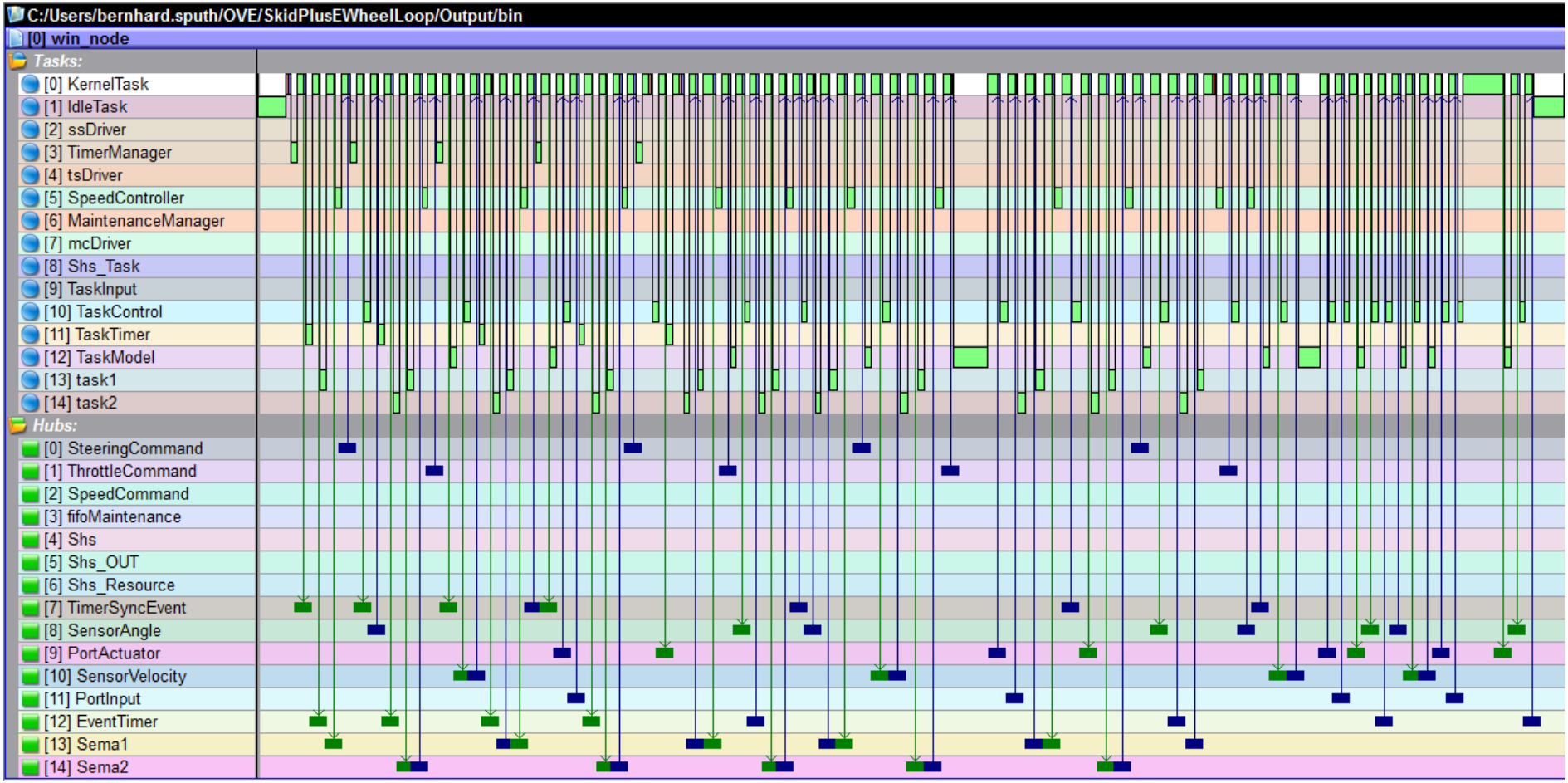
- Memory regions composed from 4kiB pages.
- Initialisation of the MMU is complex.
- Context Switch must reconfigure the MMU, impact on run-time;

Impact of Task Priorities in VirtuosoNext 1/2



Three applications at different Priorities.

Impact of Task Priorities in VirtuosoNext 2/2



Three applications at the same Priority.

Code size differences between OpenComRTOS-1.6 and VirtuosoNext

	OCR	VN	Difference
ARM-Cortex-M3	18800 B	19060 B	+360 B
ARM-Cortex-A9	20232 B	26932 B	+6700 B

Adding memory protection has a limit impact on the code size.

Runtime Impact of Memory Protection

1. Semaphore-Loop runtime differences

	OCR	VN	Difference
ARM-Cortex-M3 (50MHz)	54.6μs	58.9μs	+4.3μs
ARM-Cortex-A9 (700MHz)	11.59μs	14.89μs	+3.3μs

2. Interrupt to ISR Latency

	OCR	VN	Difference
ARM-Cortex-M3 (50MHz)	780ns	780ns	$\pm$0ns
ARM-Cortex-A9 (700MHz)	100ns	138ns	+38ns

3. Interrupt to Task Latency

	OCR	VN	Difference
ARM-Cortex-M3 (50MHz)	16μs	17μs	1μs
ARM-Cortex-A9 (700MHz)	994ns	1726ns	+732ns

Adding memory protection has a limit impact on the run-time

Conclusions

Comparing VirtuosoNext to a typical Hypervisor:

- Space partitioning does not require a lot of additional code.
- Lower memory consumption due to fine grain protection scheme.
- Tasks of each Application are still scheduled in order of Priority. Thus real-time behaviour is not affected by the protection.
- Hypervisors are suitable for soft-realtime applications, not for hard-realtime.

Questions?

Thank You
for Your attention

http://www.altreonic.com