Safety-Critical Systems Club

Seminar Information

Thursday 4th November 2021

Hotel TBC, London

Safe Use of Multi-Core and Manycore Processors

Safe Use of Multi-Core and Manycore Processors

Thursday 4th November 2021

0900 - 0925		**Registration and Coffee**

Main Programme (TBC)

0925 - 0930	Mike Parsons - SCSC	**Welcome and Introduction**
0930 - 1000	Louise Harney - Leonardo	**Safety Assessment of Multicore: The Challenge?**
1000 - 1045	Mark Hadley and Mike Standish - Dstl	**A Practical Assurance Approach for Multi-Cores (MCs) Within Safety-Critical Software Applications**
1045 - 1115		**Coffee**
1115 - 1200	Guillem Bernat - Rapita Systems	**Independently Verifying the effectiveness of RTOS Hypervisors at reducing Multicore Interference**
1200 - 1245	Olivier Charrier - Wind River	**Use of Multicore Processors in Certified Avionics: How Virtualization can help**
1245 - 1345		**Lunch**
1345 - 1430	Tim Loveless - Lynx Software Technologies	**Telemetry and Reactive Scheduling for Improved Multicore Partitioning**
1430 - 1515	Iain Bate - University of York	**Multi-core architectures and timing analysis: Their influence on the scheduling of certifiable real-time systems**
1515 - 1545		**Tea**
1545 - 1630	Sam Riley - MAA	**Certification Aspects of Multicore**

Extras

1630 - 1715	Catherine Menon - University of Hertfordshire	**Ask the Audience: Delegates give their views on Multicore challenges and solutions**
1715		**Tea and snacks with opportunities for networking**

Safety Assessment of Multicore: The Challenge?

Louise Harney
Lead Systems Engineer at Leonardo MW Ltd

ABSTRACT

The SCSC has recently stood up the Multi/Manycore Working Group (MCWG). Louise will provide an overview of the group's activities, focus and plans for the future. She will provide a brief introduction to multicore vs manycore implementations, completing the talk with some plans for a certification roadmap for these implementations, which will hopefully provoke valuable debate amongst attendees over coffee.

~

Louise Harney is a Lead Systems Engineer at Leonardo MW Ltd. She leads the System Safety team in Edinburgh to deliver design influence into the most complex radar and electro optic systems. Louise is also chair of the SCSC's Multi/Manycore Working Group (MCWG) and a member of the SCSC Steering Group.

Telemetry and Reactive Scheduling for Improved Multicore Partitioning

Tim Loveless
Lynx Software Technologies

ABSTRACT

Hardware interference makes multicore avionics systems notoriously difficult to build and expensive to safety certify. As per CAST-32A, hardware interference channels must be mitigated in order to bound an application's worst-case execution time (WCET). Such a platform is said to be robustly partitioned, the Holy Grail of multicore avionics platforms. Telemetry software placed between the hypervisor and virtual machines is ideally placed to monitor overall system performance independent of RTOS or application workloads. Using a simple 1-to-1 mapping of virtual machines to processor cores isolates workloads to cores. With this approach an existing RTOS-based avionics application can be benchmarked against adversarial software to measure its WCET and quantify interference. We show a customer use case using the Lynx environment where performance telemetry data is used to tune virtual machine scheduling to mitigate one source of interference.

~

Tim Loveless has 25 years' embedded industry experience in the fields of real-time operating systems, safety critical systems, JTAG tools, and embedded Linux. Before joining Lynx Software Technologies as Principal Solutions Architect, he worked for Intel's Internet of Things Group and as European Aerospace and Defence FAE Manager for Wind River. Tim's interests include computer security and macroeconomics. He enjoys running and cycling while skiing and paddle boarding are rare-treats.

Multi-core architectures and timing analysis: Their influence on the scheduling of certifiable real-time systems

Iain Bate
Department of Computer Science
University of York

ABSTRACT

Multi-core processors are both needed by industry due to enhanced functionality in systems but also being forced on them by the available supply chain. Regulatory authorities have provided some guidance on achieving certification when multi-cores are used. The current recommendations suggest simple devices with low numbers of cores. The guidance also suggests that interference channels are both understood and their potential effects mitigated. Our work has been driven by our usual mantra design-for-predictability and design-for-safety. In previous projects, we performed significant work on multi-core timing analysis and on scheduling approaches for mixed-criticality scheduling. This introduced us to the significant challenges of creating robust and justifiable analysis. The result was that systematic testing and careful statistical analysis is needed for the evidence gained to be useful. Important lessons include the way the software is written and the way the platform is configured is key to getting useful results. In this talk, I will briefly introduce the pillars of our work which are selection and configuration of platforms, multi-core timing analysis, and scheduling and timing analysis. I will then relate this to some of the requirements from CAST32A and then reflect on what work is currently being performed.

~

Dr Iain Bate is a Reader within the Real-Time Systems (RTS) Research Group at York. His main interests include scheduling and timing analysis, and design assurance to achieve dependable operation even when there are complex failures. His original doctoral work on scheduling and timing analysis was first patented and then adopted by Rolls-Royce for use on current aircraft projects. His work on timing analysis has been used on a large fast jet project. More recently he has worked on applying the principles of Dependable Real-Time Systems (DRTS) to more complex systems such as multi-core based systems, automotive systems and Wireless Sensor Networks (WSN) including for environmental monitoring. In particular he has concentrated on reducing the errors in systems through the building of systematic methods based around multivariate statistical models. Dr Bate has published over 200 papers and 30 industrial reports. He has recently secured nearly £2 million from Innovate UK, for HiClass, and Huawei (project MOCHA) to apply his current research to the next generation of systems. Dr Bate is heavily involved in the appropriate communities including being an Editor-in-Chief of leading international journals for more than 15 years, a member of all leading Program Committees in his research field, Program Chair of three leading international conferences, and a regular keynote speaker and guest researcher at other institutions. He has also been influential in both certification guidance and industrial practice. He is part of the SCSC multi-core working group.

Please note our upcoming events:

Safety-Critical Systems Symposium (SSS'22)

February, 2022 - Bristol, UK

Further details at: scsc.uk/events