SCSC

FOR EVERYONE WORKING IN SYSTEM SAFETY

Safety-Critical Systems Club

Seminar Information

Thursday 11th November 2021

Wellcome Collection, London and online

Safe Use of Multi-Core and Manycore Processors

Safe Use of Multi-Core and Manycore Processors

Thursday 11th November 2021

0900 - 0925		**Registration and Coffee**

Main Programme

0925 - 0930	Mike Parsons - SCSC	**Welcome and Introduction**
0930 - 1000	Lee Jacques Leonardo	**Multi- and Manycore Safety Working Group (MCWG)**
1000 - 1045	Mark Hadley - Atkins and Mike Standish - Dstl	**The Safety and Security Considerations for the Use of Multi-Core Processors**
1045 - 1115		**Coffee**
1115 - 1200	Guillem Bernat - Rapita Systems	**Incremental Assurance of Multicore Integrated Modular Avionics (IMA)**
1200 - 1245	Olivier Charrier - Wind River	**Multicore Processors usage in Certified Avionics: How Virtualization can help?**
1245 - 1345		**Lunch**
1345 - 1430	Tim Loveless - Lynx Software Technologies	**Telemetry and bare-metal Virtual Machines 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 – Frazer-Nash	**Certification Aspects of Multicore**

Extras

1630 - 1715		**Panel Discussion**
1715		**Tea and snacks with opportunities for networking**

Multi- and Manycore Safety Working Group (MCWG)

Lee Jacques
Leonardo MW Ltd

ABSTRACT

The SCSC has recently stood up the Multi/Manycore Working Group (MCWG). Lee will provide an overview of the group's activities, focus and plans for the future. He 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.

BIO

Lee is Head of Software for Electronic Warfare at Leonardo Electronics UK. Throughout his career he has been in and around Aerospace/Defence/High Integrity products delivering solutions for various armed forces and emergency services around the world. He has worked on Embedded Avionics, Command and Control systems, TETRA radios, Missile Systems and currently a variety of Electronic Warfare sensors, controller and effectors.

His role is multifaceted considering process, skills, recruitment, technology and governance. Multicore is an emerging challenge but also an opportunity to provide a step change in performance and capability.

His passion is software requirements and architecture and he initially got involved in this group to identify methods to ensure multicore is considered early in the process where the risk is at its lowest.

He enjoys Kayaking, Badminton and Tennis and is married with 3 children, 2 rabbits and 1 dog!

The Safety and Security Considerations for the Use of Multi-Core Processors

Mark Hadley
Atkins

Mike Standish
Dstl

ABSTRACT

Multi-Core Processors (MCPs) are pervasive within our current technology and our reliance on MCPs may increase more and more as we invest in expanding our technology. The process to gain safety assurance of MCPs has been a long journey but with these efforts come opportunities for MCPs to provide assurance solutions to safety and security challenges. This presentation will explore some of the MCP assurance challenges and solutions, and will look at some of the wider considerations when we build an MCP safety and security assurance approach.

BIOS

Mark has been involved in the safety critical software domain for almost 25 years with Atkins and the UK Defence Science and Technology Laboratory (Dstl) (and its predecessor organisations) working on a range of civil and UK Ministry of Defence (MOD) systems. Mark is a principal software safety consultant at Atkins and currently working in the energy sector. Mark was a senior principal consultant in software at Dstl and provided Independent Technical Evaluation (ITE) and Subject Matter Expert (SME) advice to a host of MOD Project Teams. He led research into a number of areas such as: multi-core processors, tool technology and the generation of diversity of evidence arguments to support the qualification of mission and safety critical systems. Mark completed his PhD in software testing at the University of York. He is a Chartered Engineer (CEng) gained via the Institution of Engineering and Technology (IET).

Mike is a senior scientist in systems at the UK Defence Science and Technology Laboratory (Dstl). Mike has experience of all aspects of software and systems lifecycles, which has been gained in over 15 years within the defence sector. Mike holds a BSc in Software Engineering and an MSc in Strategic Information Systems. Mike gained an Engineering Doctorate (EngD) in Systems from the University of Bristol with a focus on how to adopt wider diverse evidence to mitigate shortfalls in software process-based safety assurance evidence. He is a Chartered Engineer (CEng) gained via the British Computer Society (BCS).

Incremental Assurance of Multicore Integrated Modular Avionics (IMA)

Guillem Bernat
Rapita Systems

ABSTRACT

DO-297/ED-124 defines incremental acceptance as a "process for obtaining credit toward approval and certification by accepting or finding that an IMA module, application, and/or off-aircraft IMA system complies with specific requirements." However, the standard was written before the introduction of multicore processors into avionics systems. In this paper, we will examine incremental acceptance of multicore-based IMA systems, discussing how the IMA platform and each hosted partition application can be independently verified to accumulate evidence to form the overall certification package. The paper starts with an overview of IMA, partitioning, and multicore avionics. It then proposes an approach to incremental acceptance of a multicore IMA system, organized around the six tasks identified in DO-297/ED-124 for incremental acceptance. The proposed approach is based on robust partitioning mechanisms verified using multicore interference generators. The paper concludes with some additional considerations regarding scheduling, shared memory, safety nets, and commercial aspects.

BIO

Dr Guillem Bernat is the CEO of Rapita Systems, which he co-founded in 2004 with Dr Ian Broster and Dr Antoine Colin as a spin-out from the Real-Time Systems Group of the University of York. Under his leadership both as CEO and Head of Sales, Rapita Systems has grown to become the leader in software analysis and verification, serving customers in major companies across the world. Dr. Bernat has more than 70 published papers in international conferences and Journals, has lectured extensively in real-time systems and is a frequent speaker at international conferences, he is the co-founder of the international workshop on worst-case execution time analysis. Dr. Bernat is acknowledged as one of the world's leading experts on worst-case execution time analysis. He can be contacted at bernat@rapitasystems.com

Multicore Processors usage in Certified Avionics: How Virtualization can help?

Olivier CHARRIER
Wind River

ABSTRACT

Single-core processors with effective computing power are being replaced by multi-core System-on-Chip devices, which have the potential to cause interference between these multiple cores.

Multi-core interference can have a significant impact on functional safety. The avionics sector has been the first to address multi-core interference with the definition of additional objectives to be addressed for Safety Certification in position papers like CAST-32A to be superseded by the upcoming FAA AC / EASA AMC 20-193.

However, multi-core processors are appealing due to the increase in the available computing power. This provides the possibility to consolidate different applications from multiple sub-systems, extending the reduction of space, weight, power and cabling (SWaP-C), much further than with a single-core processor. Consolidation requires the management of execution of applications carrying different Design Assurance Levels on the same processor, and consideration of multi-core interference with its impact on Safety Certification.

In this presentation, we will review the benefits of the usage of multi-core processors to run multiple types of applications, in the scope of Safety Certification, reviewing the explicit objectives defined for this purpose by the avionics industry and identify the areas where the usage of virtualization can provide benefits.

BIO

Olivier CHARRIER is a Functional Safety Specialist at Wind River. He has a master's degree in software engineering (DESS). In June 2001 he joined Wind River as Senior Field Application Engineer dedicated to the Aerospace & Defence Market. In January 2007, he became an EMEA Aerospace & Defence Principal Engineer also starting to participate to the SAE/ARINC APEX Software Subcommittee (on ARINC 653). In January 2017, his role became Functional Safety Specialist, for avionics, Railway, Nuclear, Medical and Automotive, also adding APAC to EMEA geo.

He can be contacted at olivier.charrier@windriver.com

Telemetry and bare-metal Virtual Machines 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 and AMC 20-193, 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. This session explores how and why bare-metal virtual machines are used by three safety-critical multicore research projects to investigate multicore interference. A simple 1-to-1 mapping of virtual machines to processor cores isolates workloads to cores. With this approach existing RTOS-based safety applications are benchmarked against adversarial software to measure WCET and quantify interference.

BIO

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
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.

BIO

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.

Certification Aspects of Multicore

Sam Riley
Frazer Nash

ABSTRACT

In his talk, Sam will consider some of the certification issues for Multicore from a military aviation perspective.

BIO

Sam Riley trained and worked in SCS through DE&S UAS team through to working at the MAA within their Programmable Elements team, before recently transitioning to working for Frazer-Nash as a consultant in their Digital Assurance team.’.

Please note our upcoming events:

Safety Futures Initiative "Get To Know You" event x2

Wednesday 24 November, 2021 – Zoom

Safety-Critical Systems Symposium (SSS'22)

February 8-10th, 2022 - Bristol, UK

Seminar: Managing ‘Black Swans’: Handling Rare and Severe Events Now and in the Future

April 8, 2022 - London, UK and blended online

Further details at: scsc.uk/events