Impact Case Study: The world's smallest automotive real-time operating system

Robert I. Davis Real-Time Systems Research Group, Department of Computer Science, University of York, York, UK. rob.davis@york.ac.uk Nigel Tracey ETAS Ltd. York, UK nigel.tracey@etas.com

Impact Summary

Research from the Real-Time Systems Group at the University of York was exploited to design an exceptionally efficient Real-Time Operating System (RTOS), used in automotive Electronic Control Units (ECUs), and its



associated schedulability analysis tools. The RTOS has been deployed in over 1 billion ECUs. It has been standardised upon by many of the world's leading powertrain automotive systems and chassis electronics suppliers, and is used in cars produced by nearly all of the major car manufacturers world-wide.

Background

In real-time embedded systems, such as the ECUs used in vehicles, system functionality is decomposed into multiple software tasks running on a microprocessor. The system requirements place time constraints on these tasks. Hence a task may be required to execute every 10 milliseconds, read and process data from sensors, and output its results within a specific time constraint or deadline. When there are multiple tasks with different periods and deadlines running on the same microprocessor, an RTOS is needed to schedule when each task should execute. It is essential that all of the tasks are guaranteed to meet their deadlines during operation; otherwise the system may suffer from intermittent timing faults that compromise its functionality and reliability.

Given the complex behaviour of these systems, it is impossible to obtain a 100% guarantee that tasks will always meet their deadlines via testing. Instead, a rigorous scientific and systematic solution to this problem is schedulability analysis; a set of techniques used to determine off-line if each task can be guaranteed to meet its deadline under a specific scheduling policy. Schedulability analysis is used to compute the worst-case response time,

the longest time that can elapse from a task being released to it outputting its results and completing execution. If this is less than the deadline, then the task can be guaranteed to always meet its time constraints.

Research

In the 1990's seminal research into schedulability analysis [1], [2], [3], [4], and [5] for fixed priority pre-emptive scheduling, originally called *Deadline Monotonic Schedulability Analysis* but now widely referred to as *Response Time Analysis*, was introduced by the Real-Time Systems Research Group (RTSRG) at the University of York.

This analysis is applicable to fixed priority scheduling, and a task model that accurately accounts for the detailed timing behaviours of tasks in automotive systems. These timing behaviours include: tasks that are invoked sporadically (i.e. with minimum inter-arrival times, but not necessarily strictly periodically in time – for example tasks that are triggered off of a crank angle sensor measuring engine rotation); tasks with deadlines that are less than their periods and prior to completion [1], [2]- - accounting for tasks that need to make a response prior to their next invocation to avoid buffer overruns, and to carry out further computations after a response has been made, in preparation for the next cycle; tasks with offset release times [4] – used as a means of avoiding peak load in short time intervals; tasks with jittered released times [5] - that are triggered by the arrival of messages that can take a variable amount of time to be transmitted, and tasks that share resources [1], [2] - such as data structures and peripheral devices used for communication. The analysis also accounts for the overheads of a well-designed RTOS [3].

This research therefore introduced for the first time, schedulability analysis that could be applied in practice to commercial real-time systems, providing a rigorous approach to obtaining timing correctness. This was recognised in the EPSRC International Review of Computer Science undertaken in 2002:

The techniques developed built upon other important research contributions such as the Stack Resource Policy [11] for resource locking; however, without the work of the

researchers in the RTSRG, the impact would not have been possible due to the fact that the underlying models used by prior schedulability analyses were too limited to be used in practice.

Route to Impact

In 1997, Robert Davis and Ken Tindell (both previously members of the RTSRG) co-founded a company called Northern Real-Time Applications (NRTA) Ltd., with the aim of developing an RTOS and schedulability analysis tools specifically tailored to automotive applications that use low cost microcontrollers. In doing so, they utilised the research that they had been involved in and heavily exposed to while at the University of York

There were two fundamental design goals:

- The real-time behaviour of systems built using the RTOS must be fully analysable using schedulability analysis tools. In other words the behaviour of the RTOS must match the assumptions of the underpinning schedulability analysis techniques.
- The memory and execution time overheads of the RTOS must be significantly less than those of any other RTOS available for use in automotive applications.

Robert Davis led the team that developed the SSX5 RTOS and associated schedulability analysis tools (originally called the "Time Compiler", later "Real-Time Architect (RTA)"). The schedulability analysis tools implemented Response Time Analysis as introduced in [1], [2], [3], [4], and [5]. The SSX5 RTOS was developed precisely to meet the assumptions of this analysis. The execution time overheads were minimised and made constant, independent of the number of tasks, allowing them to be accurately measured and this data used in the schedulability analysis. The memory overheads of applications built on SSX5 were radically reduced by comparison with other automotive RTOS. This was achieved via the use of single-stack execution and compile time, i.e. off-line, configuration of the RTOS data structures to minimise RAM usage.

NRTA attracted significant venture capital funding in 1998 (£1 million from 3i) and again in 2000 (£9.2 million from 3i and TecCapital). In 2001, the company changed its name to LiveDevices Ltd.

In March 2003 LiveDevices was sold to ETAS GmbH, a wholly owned subsidiary of Robert Bosch GmbH. The reason for the trade sale was that Robert Bosch had benchmarked RTA-OSEK and found it to be significantly more efficient than its subsidiary's Ercos RTOS. Rather than attempt to write a new OSEK RTOS from scratch and compete with LiveDevices, ETAS chose to buy the company, bringing the RTA-OSEK technology and the 20+LiveDevices engineering team in-house.

Standards

During the development of the SSX5 RTOS, the automotive industry was working on standards via the

OSEK organisation. As a Technical Committee Member of OSEK [7], NRTA influenced the OSEK OS standard [8] ensuring that the basic conformance classes (BCCx) could be achieved with a single-stack RTOS, leveraging the execution time and memory savings which that approach facilitates [12]. NRTA modified the SSX5 RTOS to comply with the OSEK standard, in the process renaming the product RTA-OSEK.

Subsequently, ETAS, as a premium partner [9] of the AUTOSAR (AUTomotive Open System ARchitecture)



partnership, have been involved heavily in specifying the **AUTOSAR** operating system standard [10], which extends the OSEK operating system standard. ETAS derived an AUTOSAR compliant RTOS called RTA-OS from RTA-OSEK [6]. (Note in [6] RTA-OSEK 'Planner' is the new for name the schedulability analysis tools, while 'Builder' is the name for the off-line configuration tool).

Impact

ETAS currently sell two versions of the RTOS, RTA-OSEK and RTA-OS compliant with the OSEK (Offene Systeme und deren Schnittstellen für die Elektronik in Kraftfahrzeugen; in English: "Open Systems and their Interfaces for the Electronics in Motor Vehicles") and AUTOSAR (AUTomotive Open System ARchitecture) operating system standards respectively.

The RTOS is currently available for more than 50 different ECU microcontrollers [6] including: Renesas: V850E, SH2, SH2A, H8S, H8SX, M16C; Xilinx Microblaze, PPC405 Core; Texas Instruments TMS470P, TMS570P; Infineon Tricore TC17x6, C166, XC2000; Freescale Star12, MPC555, MPC55xx, S12X, MPC56x, HC12X16, HC08, HCS12; Fujitsu 16LX; Analog Devices Blackfin, STMicroelectronics ST30, ST7, ST10.

ETAS customers for the RTOS cover a wide range of application areas within Automotive Electronics. It has been standardised upon (used by default in all ECUs) by many of the world's leading automotive powertrain systems and chassis electronics suppliers, and is used in cars produced by nearly all of the world's major car manufacturers. By 2015, the RTOS had been deployed in over 1 billion ECUs. This number is increasing at the quite astonishing rate of between 1 and 2 million new ECUs *per week*.

Beneficiaries

Use of the RTOS and its associated schedulability analysis tools has benefitted automotive manufacturers and their Tier 1 suppliers in the following ways: (i) A reduced memory footprint means that cheaper microcontroller variants with smaller on-chip RAM / Flash memory can be used. (The code size of RTA-OS is typically in the range 1 Kbytes to 1.5 Kbytes depending on the processor – making it the world's smallest AUTOSAR OS - so small that the hexadecimal machine code can be reproduced in the graphic below). This has reduced unit costs in production. (ii) The very low execution time overheads of the RTOS mean that more functionality can be included on a given low cost microprocessor reducing costs by avoiding the need for hardware upgrades to more capable but expensive devices. (iii) A reduction in the time spent debugging intermittent timing issues. Schedulability analysis and appropriate use of proven real-time mechanisms have enabled off-line analysis of task response times, reducing system integration time and testing effort, and improving reliability. For these reasons the world's major ECU suppliers and car manufacturers have adopted this technology. In a competitive market, some of these benefits will have been passed on to their customers in the form of cheaper, more reliable vehicles.

RTA-OS: The smallest AUTOSAR OS in the world, so small it fits here:

501025a8	ffe2c04d	09820820	90000010	01370800	20bbffe2	c04d0000	0340000d	501025c8	04c0000d	Ofe2cfcd	0fa6f020	af8ff576
										0f7fe8f0		
50102608	00780£82	46800782	15824482	0a3c0065	a18ff576	0f37ffe2	c04d0148	006d4982	50102628	04c0000d	Ofe2cfcd	f781ffb7
8fa6f020	c04d4680	09820820	90009202	0f282f82	50102648	ffe2c04d	00000340	000d806a	0f37ffe2	cfcd0fa6	f020af8f	£5760£37
080020bb	50102668	0f190f28	f8d40fd9	13da04c0	000d0fe2	0f260004	4019e8f4	0f190008	f65fe8ec	50102688	0282f8d0	065912da
106ee8ec	Of190aee	00780f82	07825000	903b4482	90000f28	501026a8	af8ff576	0f37ffe2	c04d0100	006d4982	04c0000d	0fe2cfcd
f781ffb7	8fa6f020	501026c8	e8ec0919	e8f00819	90009202	0f2812da	000fe8f4	0019fb45	ff6d036e	e8ec0f19	501026e8	ff214013
0101f08b	f8a54f1b	0f8001b0	e8f00f59	f24c0000	e8ec0f99	e8ec0f59	50102708	Of99ffe2	c04d0000	0340000d	fb06ff6d	ffb70fa6
										00000000		
cfcd0fa6	f020af8f	f5760f37	080020bb	Of19e8ec	0f99fb05	ff6d04c0	000d0fe2	50102768	f8d00f19	e8f40f59	f0e00f0f	1048e8f4
0f590fa6	1048e8f4	0f19f8d0	0f990c6e	50102788	ffa7f83f	e8f40f19	f8d00f59	0f82e8f4	ff1d036e	e8ec0f19	e8ec0959	e8f00859
501027a8	0340000d	206a0f37	ffe2c04d	9000fab7	af8ff576	0£370800	20bbffe2	c04d0000	501027c8	03d92bda	04c0000d	Ofe2cfcd
0fa6f020	424c0004	2259086e	42d4424c	302cf8d4	501027e8	29f6216c	e8f00f19	0d3cf202	8010f27f	e8f00059	80040f7f	e8f00f19
00044019	50102808	e8ec0019	e8e80119	f2200f8b	e8e80f19	f5760f37	ffe2c04d	01681140	012b40cc	50102828	000d0fe2	cfcdf781
										0f280282		
										0f59e8f4		
e8f802d9	0252006d	39022802	9000fffc	2f240f82	f8cc0f59	395af8c8	501028a8	00000340	000d906a	0f37ffe2	c04d9000	f020af8f
f5760f37	080020bb	ffe2c04d	501028c8	0fd9f8d6	0cd904c0	000d0fe2	cfcd0fa6	e8d80fd9	1f828011	08df0428	c814f8d5	501028e8
0f59e8e0	0759e8dc	06590528	0058c02c	f5760f37	ffe2c04d	c834fe4a	ff6de8e4	50102908	000d0fe2	cfcdf781	ffb79fa6	f020af8f
										04c0000d		
50102948	043c0004	2819046e	42d4424c	c02cf8d4	00198916	0f6840cc	0f82e8f0	0f59214c	50102968	c04dfeaf	ff6d8004	0f7fe8f0
0f19e8f4	f781ffb7	8fa6f020	af8ff576	Of37ffe2	50102988	90000282	c02c4eda	04c0000d	0fe2cfcd	146e200c	302cb8b6	02d955da
										501029c8		
54da04c0	000d0fe2	20bbffe2	c04d0000	0340000d	0906a013	501029e8	Ofe2cfcd	0fa6f020	af8ff576	01370800	e8f00819	c02cf8d4
0cd957da	04c0000d	50102a08	0f37e8e8	Of99ffe2	c04d126e	e8e80f19	cfcdf781	ffb70fa6	1048f020	af8ff576	50102a28	f5760f37
ffe2c04d	2b3c04c0	000d0fe2	04c0000d	Ofe2cfcd	f781ffb7	f020af8f	50102a48	af8ff576	0f37ffe2	c04d0000	0340000d	e8ec0f99
										fe2aff6d		
										00000340		
cfcd0fa6	f020af8f	f5760f37	080020bb	50102ac8	11828616	0808b8b5	0fd904c0	000d0fe2	c04d0000	0340000d	0828f8ec	ff6d0f28
50102ae8	04c0000d	Ofe2cfcd	0fa6080f	f0bbffe2	63dafe3c	fd4bff6d	0f28b8b4	0fd90f82	50102b08	0080003b	ffe0404d	c02c4802
f8d40cd9	ffclff6d	7482043e	f020af8f	f5620f37	50102b28	0340000d	ffbbff6d	748294ae	ffe0404d	af8ff576	0f370800	20bbffe2
										50102b68		
										af8ff576		
										c04d106a		
										202c1fc2		
0£370310	f0372fc2	0082ffe3	50102c08	90001202	a1803000	f00bf020	cf8ff021	9000£4£c	0178f120	50102cf8	f06a0f37	ffe2c04d
										0fe2c0cd		
										4fcdf020		
										0f37e8e8		
										ffe2c04d		
										000dfc79		
									0428f8d5	0fd904c0	000d0fe2	cfcd0fa6
50102e18	f020af8f	f5760f37	ffe2c04d	fe47ff6d	900004c0	000d0fe2	cfcdf781	ffb78fa6				

The Automotive Electronics market is both huge and highly competitive, with electronics now contributing 15-30% of overall vehicle production costs. For the reasons given above, the world's leading Automotive OEMs and Tier-1 suppliers have adopted the RTA-OSEK and RTA-OS operating systems. They have done so for the substantial benefits it brings to them and to their customers.

The technology has led directly to the creation and sustaining, over a period of more than 15 years of a large number of high technology jobs in York. The fact that ETAS has offices in York is a direct consequence of the research conducted at the University of York. (ETAS is head-quartered in Germany and has offices in 12 other countries).

Future Challenges

Automotive systems are now moving implementations on multicore hardware. The availability of such high performance multiprocessors means that it is now cost effective to integrate different applications that would otherwise have run on independent ECUs onto the same hardware platform. These different applications have different criticality levels which leads to a host of interesting problems. Mixed Criticality Systems [13] are currently a hot topic in real-time systems research. The Real-Time Systems Research Group is a world leader in this area with a number of projects funded by both the UK EPSRC and the EU. The group continues to have close ties with ETAS who act as industrial advisors on these projects as well as sponsoring research students.

References

- [1] N.C. Audsley, A. Burns, M. Richardson, K.W. Tindell, A.J. Wellings, "Applying New Scheduling Theory to Static Priority Preemptive Scheduling". Software Engineering Journal, Volume 8, Issue 5, pages 284-292, 1993. ISSN: 0268-6961
- [2] N.C. Audsley, A. Burns, A.J. Wellings, "Deadline Monotonic Scheduling: Theory and Application". Control Engineering Practice, Volume 1, No. 1, pages 71-78, 1993. DOI:10.1016/0967-0661(93)92105-D.
- [3] A. Burns, A. J. Wellings, "Engineering a Hard Real-Time System: From Theory to Practice" Software Practice and Experience, Volume 25, Issue 7, pages 705-726, July 1995. DOI: 10.1002/spe.4380250702.
- [4] N.C. Audsley, K.W. Tindell, A. Burns, "The End Of The Line For Static Cyclic Scheduling?" In proceedings, 5th Euromicro Workshop on Real-Time Systems, pages 36-41, June 1993. DOI: 10.1109/EMWRT.1993.639042
- [5] K.W. Tindell, A. Burns, A.J. Wellings, "An extendible approach for analyzing fixed priority hard real-time tasks". Real-Time Systems, Volume 6, Issue 2, pages 133-151, 1994. DOI: 10.1007/BF01088593.
- [6] http://www.etas.com/en/products/rta_software_products.php, http://www.etas.com/en/products/rta_osek.php, http://www.etas.com/en/products/rta_os.php
- [7] http://portal.osekvdx.org/index.php?option=com_content&task=view&id=8&Itemid=1 1
- [8] http://portal.osek-vdx.org/files/pdf/specs/os223.pdf
- [9] http://www.autosar.org/index.php?p=2&up=1&uup=2&uuup=0
- [10] http://www.autosar.org/download/R4.1/AUTOSAR SWS OS.pdf
- [11] T.P. Baker, "Stack-based Scheduling of Real-Time Processes." Real-Time Systems Journal (3)1, pp. 67-100. 1991.
- [12] R.I. Davis, N. Merriam, N.J. Tracey, "How Embedded Applications Using an RTOS can stay within On-chip Memory Limits". In proceedings of the Work in Progress and Industrial Experience Sessions, 12th EuroMicro Conference on Real-Time Systems. Stockholm, Sweden. June 2000.
- [13] A. Burns, R.I.Davis, "Mixed Criticality Systems: A Review", 2014 available from http://www-users.cs.york.ac.uk/~burns/review.pdf