Impact Case Study: Guaranteeing the real-time performance of in-vehicle networks
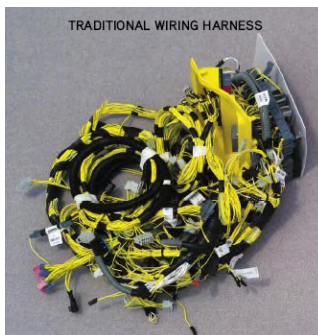
Robert I. Davis

Real-Time Systems Research Group,
Department of Computer Science,
University of York, York, UK.
rob.davis@york.ac.uk

Impact Summary

Controller Area Network (CAN) is a digital communications bus used by the automotive industry for in-vehicle networks. Research from the Real-Time Systems Group at the University of York introduced techniques that enable CAN to operate under high loads (approx. 80% utilisation) while ensuring that all messages meet their deadlines. The research led directly to the development of commercial products, now called Volcano Network Architect (VNA) and the Volcano Target Package (VTP). This Volcano technology (VNA and VTP) is now owned by Mentor Graphics. In recent years, VNA has been used to configure CAN communications for all Volvo production cars, with VTP used in the majority of Electronic Control Units (ECUs) in these vehicles, including the S40, S60, S80, V50, V70, XC60, XC70, XC90, C30, and C70; total production volume 330,000 to 450,000 vehicles per year. This Volcano technology is also used by Jaguar, LandRover, Aston Martin, Mazda, and the Chinese automotive company SAIC. It is used by the world's leading automotive suppliers, including Bosch and Visteon. It is also used by Airbus.
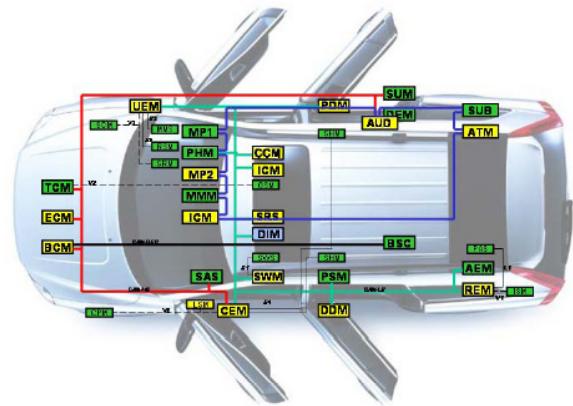
Background

Prior to the 1990s, cars used point-to-point wiring. This was expensive to manufacture, install and maintain. From 1991, the automotive industry began to use Controller Area Network (CAN) [1] to connect Electronic Control Units (ECUs) such as engine management and transmission control. Using this approach dramatically reduced the size, weight and complexity of the wiring harness, for example with CAN, a door system in a high-end car typically requires 4 wires, compared to 50+ with point-to-point wiring. The adoption of CAN led to significant cost savings and reliability improvements. It has supported a revolution in the complexity of automotive electronics, with the number of ECUs in a typical mainstream car increasing from 5-10 in the mid to late 1990's to 25-35 today.

CAN supports communications at typical bus speeds of 500Kbit/sec for powertrain applications and 125Kbits for body electronics. In a typical application, over 2000 individual signals (e.g. switch positions, wheel speeds, temperatures etc.) are sent in hundreds of CAN messages. There are deadlines on the maximum time that these messages can take to be transmitted on the bus. If a message fails to meet its deadline, then the reliability and functionality of the electronic systems can be compromised. This can lead to intermittent problems, and high warranty costs associated with 'no fault found' replacement of ECUs.

Messages queued by ECUs connected to a CAN bus compete to be sent on the bus according to their IDs, which represent their priority. Higher priority messages are sent in preference to those with lower priority. In the early 1990's, CAN messages were typically assigned IDs according to the data in the message and the supplier, with a range of message IDs assigned to each supplier. Further, extensive testing was the only way of trying to verify that the messages would meet their deadlines. This was effective up to bus utilisations of about 30%; however, higher bus loads would result in deadline failures and intermittent problems.

Research

In 1994, three members of the Real-Time Systems Research Group (RTSRG) in the Computer Science Department at the University of York; Ken Tindell, Alan Burns, and Andy Wellings, introduced schedulability analysis of messages on CAN. This research [17], [18], [19], and [20] computed the longest time that each message could take from being queued by an ECU to being successfully transmitted on the bus and therefore received by other ECUs, referred to as the worst-case response time. This analysis enabled system designers to determine offline if all of the messages on a CAN bus could be guaranteed to always meet their deadlines during operation. This systematic approach was a significant improvement over the methods previously used in the automotive industry, which involved extensive testing, followed by hoping that the worst-case response time of every message had been seen.

This work also showed how to obtain optimal priority assignments for CAN messages. The research in [17] provided the fundamental analysis of message response times. This was extended in [18] to account for errors on the network, and integrated in [19] with information about the timing behaviour of the sending and receiving software. The analysis provided in [17], [18], [19], does not apply to all CAN hardware, some specific CAN Controller designs were shown in [20] to have relatively poor real-time performance, while others matched the requirements of the theory well. The RTSRG has continued its work on CAN schedulability analysis. In 2007 research published by Robert Davis and Alan Burns [3] corrected some flaws in the original analysis of CAN message response times, and was used by Mentor Graphics to check their Volcano Network Architect implementation. More recent research by the RTSRG has addressed areas where the CAN controller hardware and the communications stack depart from the assumptions of the original research, such as non-abortable transmit buffers [6], and the use of FIFO [5] and other work-conserving [4] queuing policies, as well as systems where peak network load is reduced using offset message release times [7].

Route to Impact

The initial research on schedulability analysis for CAN [17] was disseminated at the 1st International CAN Conference. As a direct result of this Ken Tindell was approached by Antal Rajnak, then working for Volvo Car Corporation. In April 1995, Ken Tindell and Robert Davis founded a start-up company called Northern Real-Time Technologies Ltd. (NRTT) to exploit the research in [17], [18], [19], and [20]. This company was contracted by Volvo Car Corporation to develop a CAN software device driver library and associated configuration tools [12], now referred to as the Volcano Target Package. Over the next two years, NRTT developed the Volcano Target Package through 4 major versions, and ported it to more than 10 different microprocessors used in the Volvo S80 and other

automotive applications. At the same time, the message priority assignment policies and schedulability analysis techniques first introduced in [17], [18], [19], [20] were implemented in a CAN message configuration and analysis toolkit called Volcano Network Architect (VNA). The initial versions of VNA were developed by Kimble AB (a Swedish company founded by Antal Rajnak), working in conjunction with NRTT. Rights to the initial versions of the Volcano Target Package were transferred to Volcano Communications Technologies AB (a Swedish company founded by Antal Rajnak) which subsequently developed fully commercial versions of the Volcano technology (VNA and VTP), before being acquired by Mentor Graphics in 2005 [6].

From 1997 onwards the Volcano technology was used in the Volvo XC90, S80, S/V/XC70, S60, S40, and V50 cars. When Volvo was bought by Ford in 1999, this technology was adopted by Ford Premier Automotive Group, including Jaguar, Land Rover, and Aston Martin.

As part of its work on the Volcano technology, NRTT consulted with Motorola, strongly influencing the hardware design used in the on-chip peripheral MSCAN controller [12], [13] (section 4.2). This design used a 3 transmit buffer solution to ensure that the MSCAN controller can send out a stream of high priority CAN messages without releasing the bus − essential in achieving high bus utilisation without deadline failures. The 3 transmit buffer solution reduced the silicon area, and hence the unit cost of the hardware, compared to a 'full' CAN controller with 15 or 16 transmit buffers. This gave Motorola a competitive advantage, and reduced unit production costs for Volvo. Since 1997, microprocessors using MSCAN have been used in the door modules and other ECUs in a wide range of Volvo cars.

In 2007, [5] was used by Mentor Graphics to verify that the analysis provided by VNA [14] was correct. Further details of the Volcano Target Package and Volcano Network Architect can be found on Mentor Graphics' website [15], [16] with a detailed description given in [8].

Impact

The initial research [17], [18], [19], and [20] was exploited in the design of CAN network layer software, called the Volcano Target Package (VTP), and network schedulability analysis tools, called Volcano Network Architect (VNA). The Volcano Target Package is deployed in ECUs, while Volcano Network Architect is used to

configure networks and to ensure that the configurations obtained result in all messages meeting their time constraints. The research was initially exploited by a start-up company called Northern Real-Time Technologies Ltd. (NRTT) that developed the first versions of the Volcano Target Package for Volvo Car Corporation (VCC) and worked in conjunction with Kimble AB to develop the first versions of Volcano Network Architect. Fully commercial versions of the Volcano technology (VNA and VTP) were later produced by Volcano Communications Technologies AB, which was sold to Mentor Graphics in 2005 [8].

Today, the Volcano Target Package is available for more than 30 different ECU microcontrollers [9], including: Fujitsu 16LX, FR Series; Hitachi H8S, SH7055, SH7058; Infineon C16x, TC179x, TC176x, XC800, XC2000; Renesas M16C, R32C/M32C; Freescale HC08, HC12, MC683xx, MPC5xx, MAC71xx; S12, S12X, MPC55xx, MPC 56xx; Mitsubishi M32R, MC32C; PowerPC; National CR16; NEC V85x, 78K0; ST Microelectronics ST9, ST10; Texas Instruments TMS470; Toshiba TMP92/TMP94.

Since the introduction of the Volvo S80 in 1998, Volcano Network Architect has been used to configure CAN communications in all new Volvo production cars, with the Volcano Target Package used in the majority of Electronic Control Units (ECUs) in these vehicles. During the period 2008 – 2012, this includes the S40, S60, S80, V50, V70, XC60, XC70, XC90, C30, and C70; total production volume 330,000 to 450,000 vehicles per year. A rough estimate of the number of Volvo cars in use during the period 2008-2013 which use this technology can be obtained from the production figures for the decade 2001 to 2011 which are approx. 4.5 million [21] (Note we cannot say how many of these vehicles remain on the road).

The Volcano technology (VNA and VTP) is also used by Jaguar, LandRover and Aston Martin. Since 2007, this technology has been used in own branded vehicles by the Chinese automotive giant SAIC [10]. In 2012, Mazda announced that they would be using Volcano technology in order to make more efficient and reliable use of CAN in vehicles featuring their "Skyactiv Technology" [11]. The Volcano Target Package is also used by the world's leading automotive suppliers, including Bosch and Visteon.

Beneficiaries

Volcano Network Architect, and the Volcano Target Package software that conforms to its assumptions, enable system architects at automotive manufacturers to configure in-car networks using CAN such that all of the messages are guaranteed to meet their deadlines at bus loads (utilisations) of up to approx. 80%. This compares with a maximum of approx. 30% using the approach otherwise prevalent in industry, where message IDs (priorities) are assigned in groups according to ECU supplier, and extensive testing and a large engineering margin for error is used to gain some confidence that message deadlines will be met. Achieving higher bus utilisation enables far more functionality to be supported using the same bus speed and communications hardware, providing those automotive manufacturers that adopt this technology with a key competitive advantage. With higher bus utilisations, more ECUs can be connected to the same network, and the network can support a larger number of signals and messages. Wiring complexity can be reduced, with fewer connectors, increased reliability, and improved brand image. Further, there is enhanced support for the addition of lucrative 'software-only' options.

These benefits are summarised in the Volvo Technology Report [2]:

"*The advantages to Volvo of the development and application of Volcano include: Production cost benefits due to high bus efficiency (four times as many signals can be transmitted at half the baud rate). Development cost benefits (in the form of a single, proven implementation which is much cheaper than multiple implementations by suppliers and conformance testing by Volvo). Improved network reliability, resulting in higher product quality. Reduction in Volvo´s test load. Reduction in supplier´s test load. High degree of flexibility (useful in many situations). Recognition of the real-time problem (Volvo developed solutions before the problem had been recognised generally)*".

Although [2] was written in 1998, the benefits of using this technology remain the same today. They are highlighted in [10] (2006) in relation to the Chinese automotive giant SAIC:

"*By using Volcano, network design is made easy and predictable, guaranteeing data communication, which reduces the verification effort to almost zero and eliminates warranty and change costs caused by networking issues.*"

Similarly, in [11], (2012):

"*Mazda's use of VNA has enabled significant improvements in network efficiency and reliability*"…" continues, "*This procedure increased the network utilization and significantly reduced the testing requirements and time*".

The research on CAN undertaken in the Real-Time Systems Group at the University of York also led directly to the design by Motorola (now Freescale) of a low-cost on-chip CAN peripheral MSCAN [2], [15] that requires less silicon area than a 'full' CAN controller, and so reduces unit costs in production.

In summary, car manufacturers and their sub-suppliers have benefited from the research in terms of reductions in development, production, and warranty costs. Development costs have been reduced via improvements in the time taken to verify network timing behaviour, reducing the cost of testing, and time-to-market. Production costs have been reduced via the ability to run in-vehicle networks at high loads while ensuring that all message deadlines are met. This has enabled increasing amounts of functionality to be accommodated using the same low cost CAN hardware. Improvements in network reliability, via off-line guarantees that messages will always meet their deadlines, have

reduced warranty costs, in particular, costly 'no fault found' ECU replacement. In a competitive marketplace, benefits to the car manufacturers have been passed on to the consumer, in terms of less expensive vehicles, with more functionality, and better reliability.

Future Challenges

The future challenges in this area arise from the use of multiple networks, often of different types, with signals and messages transferred between them. Here the inflexibility of some legacy applications gives rise to a number of interesting issues, which are still being researched today. A new CAN standard has also been proposed allowing flexible high speed data rates. This brings a whole new set of research problems. The Real-Time Systems Group at York remain at the forefront of research into real-time communications and continue to produce world-class research in this area.

References

[1] Bosch. "CAN Specification version 2.0". Robert Bosch GmbH, Postfach 30 02 40, D-70442 Stuttgart, 1991.

[2] L. Casparsson, A. Rajnak, K. Tindell, and P. Malmberg. "Volcano - a revolution in on-board communications". Volvo Technology Report, 1998/1.

[3] R.I. Davis, A. Burns, R.J. Bril, and J.J. Lukkien. "Controller Area Network (CAN) Schedulability Analysis: Refuted, Revisited and Revised". Real-Time Systems, Volume 35, Number 3, pages 239-272, April 2007.

[4] R.I. Davis, N. Navet "Controller Area Network (CAN) Schedulability Analysis for Messages with Arbitrary Deadlines in FIFO and Work-Conserving Queues" . In proceedings 9th Workshop on Factory Communication Systems (WFCS 2012) pages 33-42, 21st - 24th May, 2012.

[5] R.I. Davis, S. Kollmann, V. Pollex, F. Slomka, "Schedulability Analysis for Controller Area Network (CAN) with FIFO Queues Priority Queues and Gateways. ". Real-Time Systems, Volume 49, Issue 1, Pages 73-116, Jan 2013.

[6] D.A. Khan, R.I. Davis, N. Navet "Schedulability Analysis of CAN with Non-abortable Transmission Requests". In proceedings 16th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'11) , Sept 5-9th, 2011.

[7] P. M. Yomsi, D. Bertrand, N. Navet, R.I.Davis "Controller Area Network (CAN): Response Time Analysis with Offsets" In proceedings 9th Workshop on Factory Communication Systems (WFCS 2012) pages 43- 52, 21st - 24th May, 2012.

[8] http://www.mentor.com/company/news/volcano_acquisition

[9] Mentor Graphics, "Volcano Target Package Datasheet",http://www.mentor.com/products/vnd/in-vehicle_software/volcano_target_package/upload/vtp-ds.pdf

[10] http://www.mentor.com/products/vnd/news/saic_sdopts_volcano

[11] http://www.mentor.com/products/vnd/news/mentor-vnd-mazda

[12] Mentor Graphics, "Volcano Network Architect Datasheet", http://www.mentor.com/products/vnd/communication-management/vna/upload/VNA_Datasheet.pdf

[13] http://www.mentor.com/products/vnd/in-vehicle_software/

[14] http://www.mentor.com/products/vnd/communication-management/vna/

[15] Motorola, "MSCAN Block Guide", Document No. S12MSCANV2/D. Available from http://application-notes.digchip.com/314/314-67565.pdf

[16] A. Rajnak, "Volcano Technology: Enabling Correctness by Design" in Embedded Systems Handbook, Edited by Richard Zurawski, CRC Press, July 2009. ISBN 9781439807613.

[17] K.W. Tindell, A. Burns, "Guaranteeing message latencies on Controller Area Network (CAN)". In Proceedings of 1st international CAN conference, pp 1–11, 1994.

[18] K.W. Tindell, A. Burns, A.J. Wellings, "Calculating Controller Area Network (CAN) Message Response Times", Control Engineering Practice, Vol 3, No 8, pp1163-1169, 1995. DOI:10.1016/0967-0661(95)00112-8.

[19] K.W. Tindell, A. Burns, A.J. Wellings, "Analysis of Hard Real-Time Communications", Real-Time Systems, Vol 9, No 2, pp147-171, 1995. DOI: 10.1007/BF01088855

[20] K.W. Tindell, H. Hansson, A.J. Wellings. "Analysing real-time communications: Controller Area Network (CAN)". In Proceedings 15th Real-Time Systems Symposium (RTSS'94), pp. 259-263. IEEE Computer Society Press, 1994. DOI: 10.1109/REAL.1994.342710.

[21] http://www.volvocars.com/intl/top/about_volvo/corporate/volvo-sustainability/Documents/Facts_and_Figures_2011-12.pdf (page 13).