Institution: The University of Essex

Unit of Assessment: 11 – Computer Science and Informatics

Title of case study: UltraSoC Technologies - On-chip debug, monitoring and analytics infrastructures to accelerate semiconductor product development and ensure trust

Period when the underpinning research was undertaken: 2005 – 2018

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Klaus McDonald-Maier	Professor	2005 – present
Andrew Hopkins	Senior Researcher, Visiting Research Fellow	2005 – March 2010, Apr 2010 - 2020

Period when the claimed impact occurred: 1st August 2013 – 31st December 2020

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact

Essex research has revolutionised on-chip debug, monitoring and analytics to deliver world leading on-chip diagnostic solutions via commercialisation by UltraSoC Technologies, a company whose creation and growth has been underpinned by Essex research. These solutions ensure correct functionality of complex microchips, substantially accelerate product development and ensure correct operation of the deployed systems in many, often safety critical, domains. Since August 2013, UltraSoC has attracted investment worth over USD 20 million and has licensed this technology to more than 20 leading edge start-ups and Tier 1 semiconductor companies including ARM, Huawei, Microsemi, Intel, Seagate and Western Digital. Employing this technology enables SoC design teams to double their profitability and reduce their design costs by 25%. UltraSoC's technology is also emerging as the de-facto standard debug support interface for RISC-V processor platform. UltraSoC so successfully enabled semiconductor industry customers to overcome manufacturing defects, software and hardware bugs, device early-failure and wear-out, as well as improve devices' functional safety and malicious attack protection, that it was acquired by Siemens in 2020 to help the global technology powerhouse provide comparable support.

2. Underpinning research

Since the early 2000s Multiprocessor Systems-on-a-Chip (MPSoC) have become extensively used in electronic systems. Such platforms are now commonplace in everyday life and underpin a vast array of consumer items including cars, smartphones and household appliances. The successful development of these products relies on, on-chip de-bugging and analysis in a short timeframe. However, the advancement of SoC technology, and particularly the move towards MPSoCs, rendered previous software debugging strategies obsolete, unreliable or insufficient. Traditionally these strategies were focused on providing debug support for chips comprising single processors, or multiple processors of a specific family of processor architectures.

Professor Klaus McDonald-Maier identified the need for support of software application development in SoC architectures, especially in cases where complex software is required to interact and execute on multiple processor cores. In cases where SoCs feature other highly interactive blocks (which may contribute to undesired behaviour of the system), this presented a significant technical challenge [R1, R2]. Beginning at the University of Essex in 2005, McDonald-Maier and Hopkins worked on EPSRC funded projects [G1 – G4] that developed initial concepts to

address this into practical implementations [R3]. McDonald-Maier's subsequent work [e.g. G5 and G6] expanded this technology [R4-6].

The research [R3] provided a highly modular debug support architecture, consisting of two important stages. Firstly, debug support adapters were provided in order to connect each processor core, peripheral or interconnect, to the debug infrastructure. The second stage then controlled these adapters, combining their debug data streams in order to preserve timing and compress resulting data to an absolute minimum. Critically, this compression meant that debug data could be straightforwardly sent from the SoC to an external development station or PC using a variety of limited bandwidth interfaces. This is an important characteristic because every product chip includes this additional debug infrastructure and therefore it is required in a high volume of devices.

The development of this process represented the first systems-centric debug support architecture for SoCs featuring multiple processor cores (i.e. cores from multiple IP provider such as ARM, MIPS etc. as well as other active peripherals). The architecture substantially outperformed the state of the art (i.e. by an order of magnitude) and, notably, achieved this in a significantly more compact implementation than existing architectures. The developed process provides debug support for two processor cores using less logic than that required for one processor core when using previous state of the art. Core contributions focus on ease of integration of processors and other components from different vendors and improved detection capability for unusual events and capability to provide this during the deployment stage of the respective SoC and for cybersecurity purposes.

Further work from 2014 focused on increasing ease of integration and flexibility with a message-based infrastructure and focus on detection capability for systems security and analytics [R4-5]. The Essex research group continued to contribute to the development of this technology in UltraSoC, the University of Essex spinout established for its commercialisation on it, and Siemens, who acquired it. For instance, as part of EPSRC funded research projects SPIRIT [G5] and the EPSRC National Centre for Nuclear Robotics [G6], there was extensive direct collaboration, focusing on methods for on-line detection of faults introduced through exposure to extreme environments such as radiation [R6].

3. References to the research [can be supplied by HEI on request]

[R1] Hopkins, A.B.T. and K.D. McDonald-Maier (2006) Debug support for complex Systems on-Chip: A review, IEE Proceedings on Computers and Digital Techniques, 153(4), 197-207. (212 citations – July 2019) DOI:10.1049/ip-cdt:20050194
[R2] Mayer, A., H. Siebert and K.D. McDonald-Maier (2007) Boosting Debug Support for Complex Systems-on-Chip, IEEE Computer, 40(4), 76-81. (44 citations – July 2019) DOI:10.1109/MC.2007.118
[R3] Hopkins, A.B.T. and K.D. McDonald-Maier (2006) Debug Support Strategy for Systems-on-Chips with Multiple Processor Cores, IEEE Transactions on Computers, 55(2), 174-184. (100 citations – July 2019) DOI:10.1109/TC.2006.22
[R4] Zhai, X., K. Appiah, S. Ehsan, G. Howells, H. Hu, D. Gu, K. McDonald-Maier (2015) A Method for Detecting Abnormal Program Behaviour on Embedded Devices, IEEE Transactions on Information Forensics and Security, 10(8), 1692-1704, DOI 10.1109/tifs.2015.2422674
[R5] Alheeti KMA, Al-ani, MS, McDonald-Maier K (2018) A hierarchical detection method in external communication for self-driving vehicles based on TDMA. PLoS ONE 13(1): e0188760.

https://doi.org/10.1371/journal.pone.0188760
[R6] Saha, S., Ehsan, S., Stoica, A., Stolkin, R. and K. McDonald-Maier (2018) Real-Time Application Processing for FPGA-Based Resilient Embedded Systems in Harsh Environments, 2018 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), Edinburgh, 2018, 299-304. doi: 10.1109/AHS.2018.8541449

Research funding:
[G1] McDonald-Maier, Debug support strategy for systems-on-chips with multiple processor cores, (EPSRC), Aug '05 – May '06, £39,218
[G2] McDonald-Maier, ReSIP – Reconfigurable system-on-chip based networks of integrated and distributed sensor platform nodes for environmental diagnostic and sensing, (EPSRC), Oct '05 – Sep '08, £265,844
[G3] McDonald-Maier, Networking of distributed sensors for proactive condition monitoring of wind, (EPSRC), Oct '05 – Jan '09, £213,374
[G4] McDonald-Maier, ESPACENET – Evolvable networks of intelligent and secure integrated and distributed reconfigurable system-on-chip sensor nodes for aerospace based monitoring and diagnostics, (EPSRC), Oct '05 – Nov '08, £268,856
[G5] McDonald-Maier, SPIRIT, (EPSRC), Jan '17 – Dec '19, £236,494;
[G6] McDonald-Maier, National Centre for Nuclear Robotics (NCNR), (EPSRC), Oct '17 – Mar '21, £11,588,431, of which £1,386,737.010 was for Essex

4. Details of the impact

UltraSoC was spun out to commercialise the debug and on-chip analytics technology invented as part of EPSRC funded research [G1-G4]. The company has subsequently been built around research undertaken by McDonald-Maier and his Embedded and Intelligent Systems (EIS) laboratory at the University of Essex [S1]. The research group at Essex recognised that the outputs of their work [R1-R3] held broad applicability for providing debug support to MPSoCs in a vast array of global scenarios that rely on embedded systems. In a marketplace where nearly half the cost of chip development was spent on de-bugging activities, the novel architecture resulting from the research conducted at Essex enables development of more reliable software, having significant economic and safety implications in consumer electronics and safety-critical applications [S1] (self-driving vehicle electronics exemplify this). Essex researchers sought to share the capabilities and associated benefits of this technology with a wide audience and developed a robust strategy in order to transform research insight into practical benefit. This centred on a broad range of dissemination activities that *targeted investment* from a variety of sources, in order to help commercialise the technology via its spin-out UltraSoC Technologies.

UltraSoC has developed significantly since August 2013 with Venture capital funding raised from the original series A investors Octopus and new investors led by electronic design legend and Chairman of UltraSoC, Prof Alberto Sangiovanni-Vincentelli (UBerkeley and co-founder of Cadence and Synopsis, Atlante Ventures) and expansion to new design centres in Bristol and Poland, increasing the number of employees from 12 in July 2013 to over 40 in 2020 (FTEs: 40) [S1]. UltraSoC raised significant rounds, with GBP 5M led by Atlante for the continued expansion of the UltraSoC team and its product portfolio to support all mainstream embedded processor platforms in 2017 (see C21 of [S2]) and UltraSoC secured new investment of GBP 5 M (see C21 of [S2]) and in 2019 an additional GBP 5M to focus on hardware security (see C9 of [S2]). Recently, UltraSoC has revisited the work on analytics, originally undertaken in the RESIP [G2] and Espacenet [G4] grants, where this was employed for design space optimisation and security applications and expanded this towards applications in AI and Machine Learning [R4]. In June

2020, UltraSoC was acquired by Siemens [S6] to enable semiconductor industry customers overcome key pain points including manufacturing defects, software and hardware bugs, device early-failure and wear-out, functional safety, and malicious attacks [S1] and [S3]. [S1] confirms:

'The research undertaken by you and your EIS laboratory at the University Essex has provided the technological foundations of the UltraSoC product portfolio and enabled us to build practical debug and analytic solutions which proved to be of such immense commercial and technological value they established UltraSoC as the world leading provider in the debug analytics and cybersecurity technology market. Consequently, UltraSoC was the company Siemens chose to acquire to achieve a step change in its activities in this market.' [S1]

UltraSoC's embedded analytics IP and debugging tools are used to monitor and boost the performance, reliability and safety of consumer electronics, safety-critical vehicle electronics, AI chips, servers and high performance computing platforms. Early customer PMC-Sierra, the fabless semiconductor company (acquired by Microsemi in 2016), used analytics and other monitoring tools within its disk drive controllers, which power a significant proportion of server chipsets globally. The monitors were used to collect detailed data on chip behaviour, while also shedding light on the performance of server infrastructure those SoCs support. "The hardware-based approach can detect hard-to-identify issues [making] it substantially easier to home in on non-fatal bugs." (see C23 of [S2]).

Extensive licensing activity followed this breakthrough with PMC-Sierra, with UltraSoC's technology increasingly seen as the world leading on-chip analytics capability to enable companies to bring their products to market rapidly, resulting in a series of technology licenses to global companies like ARM (2016 see C20 of [S2]), HiSilicon (Huawei, 2016), Esperanto (2017, see C18 of [S2]), Mircosemi (2017), Movidius (Intel, 2016), Alibaba (2018, see C17 of [S2]), Kraftway (2018, see C15 of [S2]), Seagate (2019, see C9 of [S2]) and Western Digital (2019 see C9 of [S2]). UltraSoC achieved 100% client retention; all licensees continued their engagement with UltraSoC, renewing and expanding their licenses. This was facilitated by its universal monitoring and analytic system to support rapid 'plug and play' integration of semiconductor IP blocks from different vendors (e.g. processors from ARM, MIPS, RISC-V etc.), enabling to effectively support mixed IP SoCs with a minimum of engineering effort (see C29 of [S2]) and fully support this via respective tools integration through its partners Andes, Arm, Cadence/Tensilica, Imperas, Lauterbach, Mentor, Percepio, Segger, SiFive, and Sondrel [S1].

UltraSoC's technology has had a distinct impact on the economics of the semiconductor industry, where its "intelligent analytics' closed the productivity gap created by the failure of traditional SoC development methodologies to keep pace with escalating systemic complexity. Providing engineering teams actionable insights that shorten the total development cycle time, accelerate debug, and reduce risk and cost to ensure timely market entry. Analysis from SemiCo research demonstrates the bottom-line value of this approach – SoC design teams can double their profitability and reduce their development costs by a quarter by using UltraSoC [S1]. Thus, UltraSoC's in chip monitoring is increasingly seen as an essential part of coping with "rising complexity and a spectrum of possible interactions" (see C23 of [S2]) which is particularly vital for the monitoring and analytics for automotive and safety-critical systems, increasingly important for self-driving and autonomous systems (see C13 of [S2]), where it is necessary to "adopt a new approach of looking inside the electronics." With "On-chip monitoring … allowing continuous measurement of previously-inaccessible information … so that users can actually take corrective action at every stage." (see C25 of [S2]). These on-chip monitoring mechanism also provide key capabilities for systems level cybersecurity through its Lockstep Monitor (See C22 of [S2]) and its

Sentinel technology [S5 and S6], this is also evidenced by UltraSoCs selection into the major DARPA Automatic Implementation of Secure Silicon programme to enable "scalable defence mechanisms into chip designs" (see C30 of [S2]).

Additionally, UltraSoC provides the only commercial grade debug solution for emerging ARM alternative Open Source processor core platform RISC-V (see C1 and C2 of [S2]) with its "standards-compliant RISC-V trace solution is a major contribution … to create a comprehensive ecosystem that delivers robust, commercial grade open-source platforms" (C1 of [S2]).

UltraSoC's development of novel chip design technology which addresses the big problem of complex Integrated circuit design was recognised at the 2015 Elektra Awards. At the European 'Oscars' of the electronic Industry, UltraSoC was named Best New Company. The judges were impressed by its partnerships with leading firms for its patented IC debug tools, which are already making an impact in global semiconductor markets. [S4] Its cybersecurity focused version of the technology was recognised with selection as finalist for the Embedded Solution Product of the Year in the 2020 Electronic Industry Awards [S5] and with the Best in Show Security Award at the globally leading Embedded World 2020 trade show [S6].

Finally, the General Manager, Siemens Digital Industries Software and Tessent Vice President confirms: "*Siemens' acquisition of UltraSoC means that for the first time our customers can access not just design-for-test, but a comprehensive 'Design for Lifecycle Management' solution for system-on-chips, including functional safety, security and optimization*," Adding: "*By utilizing design augmentation to detect, mitigate and eliminate risks throughout the SoC lifecycle, customers can radically improve time-to-revenue, product quality & safety, and profitability. UltraSoC has a fast-growing business and impressive customer list and, as part of Siemens, can complement Tessent to create a truly unique offering in the market*." [S3]. Siemens also confirms that "*UltraSoC is a pioneer of embedding monitoring hardware into complex SoCs to enable "fab-to-field" analytics capabilities designed to accelerate silicon bring-up, optimize product performance, and confirm that devices are operating "as designed" for functional safety and cybersecurity purposes*." [S3]. All this from the company with a product portfolio founded on, and practical debug and analytic solutions enabled by research led by McDonald-Maier at the University Essex [S1].

5. Sources to corroborate the impact

[S1] Former Chief Strategy Officer, UltraSoC Technologies now Senior Director Portfolio Strategy at Mentor, a Siemens Business
[S2] Compilation of links from open access press and media publications evidencing company developments and significance
[S3] Compilation of links covering UltraSoC acquisition by Siemens (e.g. 'Siemens acquires UltraSoC to drive design for silicon lifecycle management')
[S4] 2015 Elektra Awards: UltraSoC named Best New Company: https://www.electronicsweekly.com/news/elektra-awards-2015-the-winners-2015-11/
[S5] Finalist for the Embedded Solution Product of the Year in the 2020 Electronic Industry Awards https://electronicsindustryawards.co.uk/finalists/
[S6] UltraSoC wins Security Award https://www.realwire.com/releases/UltraSoC-wins-Security-Award-for-Bus-Sentinel-hardware-cybersecurity-IP