*Arm TechCon*
*October 8 – 10, San Jose Convention Center, CA*

# UltraSoC announces next-generation hardware-based cybersecurity products

## *Embedded monitors detect, block and record attacks, prevent propagation*

**CAMBRIDGE, UK and SAN JOSE, CA – 8 October 2019**

UltraSoC today announced next-generation hardware-based cybersecurity products that can be used to detect, block and record cyber-attacks in a broad range of applications – from vehicles and factory robots to consumer devices.

These new offerings embed advanced real-time cybersecurity features in the systems-on-chip (SoCs) that power and control every modern product. The first product in the range, the UltraSoC Bus Sentinel, allows SoC designers to control access to sensitive areas of their devices, instantaneously detect and block suspicious transactions, and build a long-term profile of system operation to secure against current and future cyber threats.

UltraSoC's security solutions allow designers to incorporate an independent internal monitoring system into their chips. This continuously checks that the device is operating as expected, detecting anomalous behavior that might indicate a security breach. Because it is embedded in the hardware, it can respond in real time (in microseconds rather than the milliseconds required by traditional threat mitigation measures), is very hard to subvert or circumvent, and can even block "zero-day" type attacks that the chip's designers have not anticipated. In addition to detecting and blocking cyber threats, it can be used to trigger actions that prevent propagation, and to provide a forensic "black box" record of events.

UltraSoC Chairman Alberto Sangiovanni-Vincentelli, commented: "In an age of autonomous vehicles, ubiquitous connectivity and increasing dependence on technology, cybersecurity is one of the top challenges for technologists. We feel that we have a truly unique solution to these problems: which is why more and more customers are turning to UltraSoC to ensure that their products function safely, securely, and exactly as they were designed to do."

The new Bus Sentinel module monitors and controls the internal bus of an SoC, observing how the chip's interconnected sub-blocks are interacting. It can be configured at run time to detect specific transaction types; for example, if a process tries to access the control registers of the memory controller at any time other than a system re-boot; or if a process with insufficient privileges attempts to access a protected area of memory. The detection process itself is performed via a range of configurable filters which can be cascaded to implement complex conditions and detect even very subtle nuances of system behavior.

In addition to its detection functions, the Bus Sentinel can be configured to respond to threats in a variety of ways, also in real time: it can allow the transaction to proceed unmodified; it may block the transaction from proceeding beyond the monitor using a transaction gating technique; it can modify the transaction in some way – for example by marking it with a flag; and it can generate a response on the bus. It can also issue a trigger event across the dedicated UltraSoC communications fabric, allowing an immediate response to be generated by other system blocks, or by external threat mitigation systems.

David Rogers MBE, CEO of cybersecurity specialists Copper Horse, commented: "As the threat landscape evolves and the consequences of attacks become more concerning, implementing security features in hardware has many advantages. By putting security at the heart of an SoC, UltraSoC's technology helps by monitoring, detecting and addressing security concerns at the most fundamental level possible today."

The Bus Sentinel's system of filters, counters and timers allows it to be configured to detect common known security threats. These powerful capabilities give the system designer a wide variety of approaches to any given threat vector. Suspicious transactions can be detected and flagged, and subsequent transactions monitored without the attacker's knowledge, to profile the threat. Transactions can be blocked, with the option to respond to the initiator and gather further information. Or the Bus Sentinel can trigger a response anywhere else within the on-chip system, communicating via the dedicated UltraSoC communications fabric.

Just as importantly, the Bus Sentinel is equipped with storage units that can record data for use by the filters in future transaction identification. It can also be used in concert with the overall UltraSoC infrastructure to gather rich statistical data. This can be used by an on-chip analytics engine, or passed to an external cloud-based analytics system, to profile the system and produce a "signature" of normal behavior based on many deployed instances of the device. This in turn allows the threat mitigation system to adapt to the rapidly evolving threat landscape.

The UltraSoC Bus Sentinel will be generally available in Q1 2020. Its modular design allows it to support any bus protocol, with immediate support for commonly-used on-chip buses including Arm APB, AHB, AXI-4 and ACE.

**About UltraSoC**

UltraSoC is a pioneering developer of analytics and monitoring technology at the heart of the systems-on-chip (SoCs) that power today's electronic products. The company's embedded analytics technology allows product designers to add advanced cybersecurity, functional safety and performance tuning features; and it helps resolve critical issues such as increasing system complexity and ever-decreasing time-to-market. UltraSoC's technology is delivered as semiconductor IP and software to customers in the consumer electronics, computing and communications industries. For more information visit **www.ultrasoc.com**

**Contacts**


Andy Gothard andy.gothard@ultrasoc.com
+44 7768 082 044

David Marsden david.marsden@ultrasoc.com
+44 7968 407 739

Twitter: @ultrasoc