SYNOPSYS®

SUCCESS STORY

Synopsys and Arm

Enabling SoC Visibility for Future Secure Hardware Architectures with In-Chip Environmental Monitoring

arm

Challenges

Billions of people around the world are now online and generating vast amounts of data every day. This data revolution, which is largely driven by user performance requirements, is a double—edged sword. On one hand it is enabling huge technology advancements, revolutionizing the way we connect with each other and the world around us, but on the other hand it is exposing major vulnerabilities in the security of semiconductor devices.

Project Overview

To help overcome these challenges Arm is leading a research program called Morello, which could radically change the way we design and program processors in the future, to enable better built—in security. This is funded by the UK government's Industrial Strategy Challenge Fund (ISCF) Digital Security by Design (DSbD) program. The main output of DSbD will be a technology platform prototype called the Morello evaluation board. (UKRI refer to this as The DSbD Technology Platform Prototype.)

Figure 1: The Arm Morello SoC on TSMC 7FF process technology on the Morello prototype board

The prototype architecture developed by Arm extends the Armv8.2a 64—bit architecture with new architectural features to enhance support. Having identified the new semiconductor IP requirements and features needed to support the Morello architecture, it was necessary to specify a Morello SoC which would form the heart of the technology demonstrator platform. In addition to an extensive list of Arm IPs, a range of third—party IPs were sourced. These included PCIe and CCIX controllers and physical interfaces, along with the DDR DRAM physical interface and a subsystem of Synopsys process, voltage, and temperature (PVT) monitors. These embedded environmental monitors also form the foundation of the Synopsys Silicon Lifecycle Management family for improving operational metrics at every phase of the device lifecycle.

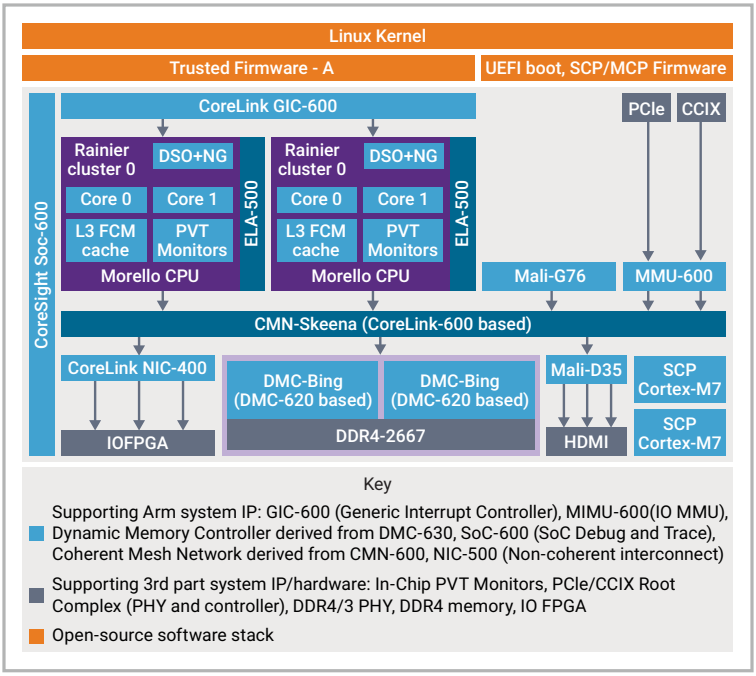

Figure 2: Arm Morello architecture, including Synopsys In—Chip PVT Monitors within the CPU

Synopsys Solution

Synopsys has been collaborating with Arm on the Morello project since its launch in October 2019 and has provided its well—established 7nm in—chip environmental monitoring subsystem to enable greater measurement and control of the real time dynamic conditions on the Morello SoC.

With guidance from Synopsys, Arm instantiated 3 temperature sensors, 4 voltage monitors, and a process detector into the Morello SoC. The application software was then enabled to use the temperature sensors to measure the temperature of the CPUs. If the temperature goes beyond a configurable warning threshold, the software issues a warning and if the temperature goes beyond a configurable critical threshold, the software initiates a shutdown for the device. The temperature sensors are used in uncalibrated mode allowing an accuracy of +/- 4 °C. If calibrated during test the temperature sensors are capable of providing an increased accuracy of +/- 1.2 °C.

Figure 3: Placement of Synopsys temperature sensor, voltage monitor, and process detector IP within the Morello CPU architecture

IP access to the monitor IP

The end user can access the Synopsys temperature sensors by configuring the temperature level in Arm's Cortex MCore software, where they can configure the alarm and shutdown thresholds.

The Synopsys temperature sensors are being used by the Cortex M Class software, and they are monitoring the temperature on the Cortex A Class processors. The voltage sensors are also exercised from the Cortex M Class Software. The ATE test program uses the Synopsys process monitors to judge the process skew of each device relative to the population. A built in PVT controller then monitors and manages the subsystem of monitors, relieving the system control processor of many associated tasks.

SoC safety and security are now key considerations at every phase of the silicon lifecycle. Aging effects in the silicon structures change the performance characteristics of the device over time. The system operating environment can also contribute to changes in chip performance. These effects include environmental variations in temperature, voltage, and silicon speed. Security breaches or changes in workload and electrical operating parameters can also impact chip performance. Because of this, it is vitally important to be able to monitor and understand the dynamic environmental on—chip conditions, as sudden changes in temperature or voltage can sometimes be indicative of an attack or security breach.

Based on the collaborative work on the Morello project, Synopsys looks forward to providing environmental in—chip monitoring solutions for customers working on future security applications helping the continued secure growth of the global datasphere.

Key Benefits of In—Chip Monitors for Future Secure Hardware Architectures

- Improved accuracy of thermal monitoring with embedded temperature sensors closer to hotspots
- Lifetime thermal stress analysis, supporting increased chip reliability
- Real—time, multi sense point embedded supply monitoring, supporting supply voltage optimization at critical circuits
- Measurement of process variability at multiple points across the die, allowing global variation assessment
- In—test and in—field production variability analysis of delay chain circuits, providing circuit delay assessment for power/speed optimization
- PVT controller monitors and manages the subsystem of monitors, relieving the system control processor of many tasks associated with monitoring and managing the subsystem

Expertise and Technical Support

Arm engaged with Synopsys to help bridge their resource gaps in embedded IP integration. The Synopsys IP in—chip sensing and monitoring team did an excellent job all around. They understood the product and leveraged Synopsys' internal expertise to accelerate the development of future secure hardware architectures.

Based on the collaborative work on the Morello project, Synopsys looks forward to providing environmental in—chip monitoring solutions for customers working on future security applications helping the continued secure growth of the global datasphere.

Want to know more about the Morello project? Visit the website. For more information on PVT monitors, visit the Synopsys website.