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.)

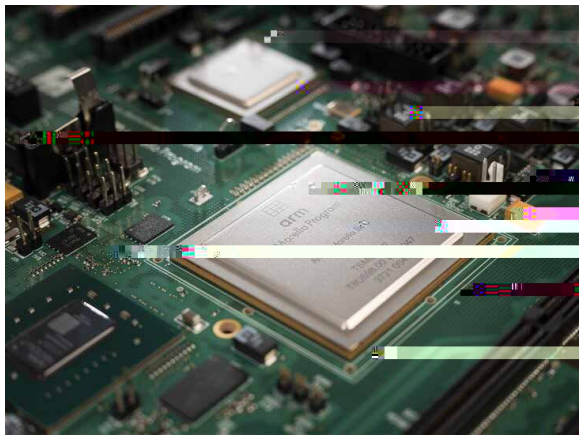
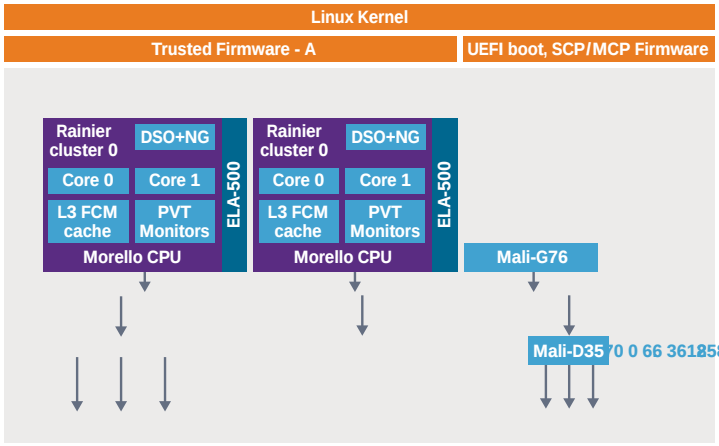


Figure 1: The Arm Morello SoC on TSMC 7FF process technology on the Morello prototype board

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.


Linux Kernel
Trusted Firmware - A
UEFI boot, SCP/MCP Firmware
Rainier cluster 0
DSO+NG
Core 0
Core 1
L3 FCM cache
PVT Monitors
Morello CPU
ELA-500
Rainier cluster 0
DSO+NG
Core 0
Core 1
L3 FCM cache
PVT Monitors
Morello CPU
ELA-500
Mali-G76
Mali-D35

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