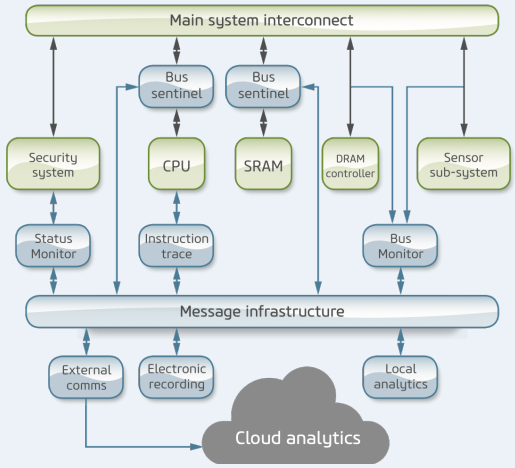
Product brief

UltraSoC Bus Sentinel

Hardware-based cybersecurity solution



FEATURES

- Cybersecurity implemented at hardware level
- Threat detection and response at clock speed
- Configurable: evolves with the threat
- Defense-in-depth: supplements software-based methods
- Fully protocol-aware: APB, AHB, AXI-4 and ACE
- Resists common threats
  - DoS, data theft, non-privileged access

The UltraSoC Bus Sentinel is a family of semiconductor IP modules that can be used as the core of a hardware-based on-chip security system.

The Bus Sentinel allows SoC designers to control access to sensitive areas of their devices, detect and block suspicious transactions at hardware speed, and build a long-term profile of system operation to secure against current and future cyber threats.

It sits on the internal bus of an SoC, identifying transactions of interest and making decisions on whether these should be allowed, blocked, modified or marked as “poison”.

Bus Sentinel is part of the UltraSoC range of cybersecurity, functional safety, monitoring and analytics IP, which allows designers to incorporate an independent internal monitoring system into their chips. This continuously checks that the device is operating as expected; provides rich data that helps build a profile of emerging threats; and can provide a forensic “black box” record of events on-chip

Overview

Cybersecurity is increasingly important in embedded systems. This is particularly true in industries such as automotive and aerospace, where security is inherently bound up with safe operation of the system: but is also true in a diverse range of sectors, from industrial robotics to consumer products. “Interconnectedness” (most commonly via the Internet) is a common point of vulnerability and attack – but by no means the only route for a system to be compromised.

The UltraSoC Bus Sentinel offers a number of benefits as part of the engineer’s cybersecurity toolbox. It contributes substantially to a defense-in-depth approach, being able to detect intrusions – including in some cases “zero-day attacks” – that may evade traditional software-based or root of trust approaches. Since it operates at the hardware level, it provides resistance to threats that evade perimeter defenses. And perhaps most importantly, it functions at hardware speed, detecting intrusions in microseconds rather than the milliseconds required by traditional techniques: important in safety-sensitive industries such as automotive, where elapsed time translates directly to distance traveled by the vehicle.

The Bus Sentinel integrates seamlessly into the broader UltraSoC on-chip monitoring and analytics infrastructure, enabling cross-triggering and capture and analysis of data across the entire SoC. This makes it possible to implement advanced cybersecurity functions such as forensic recording, threat analysis and profiling, allowing the defense system to adapt as the threat landscape evolves.

Functional description

The Bus Sentinel monitors and controls transactions on an on-chip interconnect that match a set of defined criteria. Conditions of interest are configurable at run-time via a set of counters and filters.

For matching transactions, one or more of the following actions can be taken:

- Allow the transaction to proceed unmodified
- Block the transaction from proceeding past the Bus Sentinel (using transaction gating)
- Modify the transaction before allowing it to leave the Bus Sentinel (ie change one or more of the transaction fields)
    - For example, mark the transaction with a “poison flag”
- Store state information to be used by filters in future transaction identification
- Gather statistics data (using counters)
- Issue a message via the on-chip UltraSoC architecture, triggering actions

Versions of the Bus Sentinel are available for APB, AHB, AXI-4 and ACE interconnects, each supporting a single interface. Other bus interface standards are under development.

Use cases

Example use cases for the Bus Sentinel include:

- Address-based transaction filtering
  Some addresses may be “locked” outside a specific time period. For example, control registers of a memory controller can be made inaccessible outside the boot phase.
- Privilege-based transaction filtering
  Access may be “locked” to transaction initiators that do not have sufficient privileges. For example, the control interfaces of some peripherals must only be accessed by a secure initiator running at a “hypervisor” privilege level
- Transaction redirection (IO remapping/virtualization)
- “Sticky” error detection (denial-of-service protection)
  When a problem (eg illegal access) has been detected, prevent all further accesses
- Denial of service / metered data service theft detection
  Block all traffic from a source if the amount of traffic from that source in a time interval exceeds a certain threshold

An integrated monitoring and analytics architecture

Bus Sentinel integrates with the UltraSoC on-chip monitoring and analytics system, a secure infrastructure that functions completely independently of the main system. It can be configured to act in co-ordination with other UltraSoC monitors, such as CPU instruction trace, our standard Bus Monitors and Status Monitors, communications and analytics modules. This allows engineers to create powerful systems for threat detection, understanding, recording and analysis.