White Paper

Intel Federal & Aerospace

Intel® Silicon Integrity Technology Tech Brief

Authors

Riccardo Locatelli, Intel

Elisa Spanò, Intel

Laura Spinella, Intel

Contents

1. Introduction

This document describes the benefits of using Intel® Silicon Integrity Technology to enable functional safety (FuSa) solutions. Intel® processors on the functional safety silicon roadmap work with Intel® Silicon Integrity Technology, a set of integrity-related features with related microcode/BIOS support. Specific FuSa technical collaterals are provided in documentation packages providing system-on-chip (SoC) information relevant to IEC 61508, ISO 13849 and RTCA DO-254/EUROCAE ED-80.

Key Takeaways:

- Intel® Silicon Integrity Technology is a set of SoC hardware/microcode-based integrity-related features that work in conjunction with the system BIOS to support FuSa solutions in multiple markets.
- Intel® Silicon Integrity Technology is available on select SKUs of Intel® processors as part of Intel's FuSa product roadmap.
- Intel® Silicon Integrity Technology includes features such as hardware lockstep, advanced in-field scan tests, and access to characterization data that helps facilitate system safety certification.

2. Intel® Silicon Integrity Technology Features

Intel® Silicon Integrity Technology comprises a set of SoC hardware and microcode capabilities plumbed into select Intel processors that works in conjunction with the system BIOS to support FuSa solutions in multiple application domains such as avionics, industrial, automotive, fixed robotics, and autonomous mobile robots. Table 1 provides a high-level description of the main feature categories.

Table 1. Integrity-Related Macro Feature Categories

Integrity-Related Macro Feature Categories
Core diagnostic and in-field test (Array/Logic Built-in Self-Tests (BIST), Core Lockstep)
Fabric Integrity (End-to-End (e2e) parity across fabrics)
Core, uncore, memory, array protection (ECC parity, CRC)
Off-line tests and flows (BIST, power-on set tests, Check-the-checker)
Error reporting and logging (aligned with Intel's Machine Check Architecture (MCA) Recovery)
Clock, voltage, power integrity (integrity monitors)

The features of this technology are functionally described in the documentation Intel creates for specific market segments.

Intel® Silicon Integrity Technology can assist in contributing to:

- Decreasing the residual failure rate of dangerous undetected faults;
- Efficiently detecting transient (soft errors) and permanent faults;
- Augmenting the integrity of on-chip shared and infrastructural resources, thus increasing the control of common cause failures;
- Offering an efficient error reporting and logging infrastructure;
- Enabling on-demand in-field diagnostic against latent fault accumulation; and
- Enhancing the on-chip anomaly detection capability for general silicon health diagnostics.

Intel® Silicon Integrity Technology features support two main categories, based on the execution phase (offline or runtime) during which the diagnostics are active.

- Offline diagnostic tests include features such as memory BIST and CtC (Check the Checker) executed during a dedicated on-demand offline diagnostic flow and further classified by:
  - Pre-BIOS diagnostics: run on-demand before the bootloader is executed and involves microcode of different IPs
  - BIOS diagnostics: run on-demand and implemented mainly via Firmware Support Package (FSP) or the bootloader.
- Runtime features include those that are always active (such as dual core lockstep, ECC/Parity, E2E Parity) and those that are periodically executed (periodic Mem/Scan BIST). Some of these require configuration by the BIOS or bootloader.

2.1 Intel® Silicon Integrity Technology Examples

Table 2 lists examples of integrity-related features organized according to IP and SoC logical function.

Table 2. Intel FuSa SKUs Integrity-Related Features

Detection	Runtime	Offline
Computing (E-Core, P-Core, GPU, NPU)	- Dual core lockstep - In-field diagnostic (Logic/Mem BIST) - ECC/Parity/CRC Array Protection	- In-field diagnostic (Logic/Mem BIST, ROM BIST) - Power-on self-test (and Check-the-checker)
Fabric and memory hierarchy	- ECC/Parity Array protection - End2End parity for on-chip fabric - IBECC for DRAM	- In-field diagnostic (Mem BIST)
Clock/ Voltage/Power Infrastructure	- ECC/Parity Power Manager Array protection - Clock/voltage monitors	- Power-on self-test
Reporting	Logging, aggregating, and reporting errors integrated with Intel MCA	

The Intel Performance-cores (or P-cores), Efficient-cores (or E-cores), the integrated GPU, and the other main SoC arrays have array protections, as well as offline diagnostics. On-chip communication fabric assists in protecting end-to-end communication, up to the external DRAM where the in-band ECC is supported. Clock, voltage and power distributions have monitoring capabilities.

Moreover, the E-cores offer state-of-the-art configurable and scalable dual core lockstep (DCLS) (see Section 2.12). E-cores also support a complete set of in-field diagnostic Memory BIST and scan BIST of the logics, which can be run at start-up/reset phase or periodically during runtime.

Intel® Silicon Integrity Technology runtime features make use of Machine-Check Architecture Recovery (MCA Recovery) to log and signal the errors via dedicated pins. The offline diagnostics are orchestrated, and results reported via standard interfaces (GPIO, I2C, SPI).

2.1.1 In-Band Error Correction Code

The In-Band Error Correction Code (IBECC) module provides error-check-and-correct protection to all or specific regions of the physical memory space. ECC syndromes are stored in specially reserved ECC space in the memory to avoid needing distinct ECC memory.

IBECC converts a read/write transaction (cache line access) to a protected region of memory into separate memory requests (read/write), one to the actual data cache line and another to the cache line containing the ECC value.

IBECC data and syndromes are stored in different memory locations, thus intrinsically covering (see Figure 1).

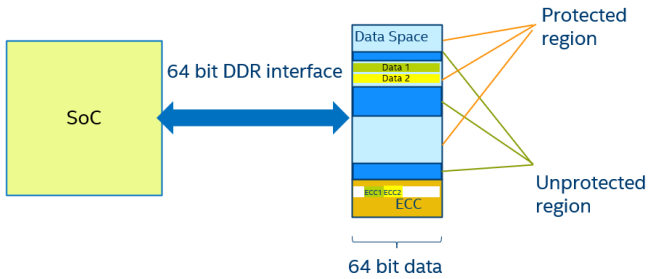

Figure 1: IBECC

2.1.2 E-Core Dual-Core Lockstep (DCLS)

To support high-integrity safety concepts, Intel® Silicon Integrity Technology provides DCLS by using two E-cores (a primary and a shadow E-core) coupled (same inputs) and compared cycle-by-cycle while being perceived by software as a single logical core. The primary core drives the outputs while the other shadows the primary core execution acting as replica for comparison purposes. A DCLS computation mismatch generates an MCA and a CATERR pin (the Intel SoC pin reporting non-recoverable internal errors detected by the integrity features) signaling.

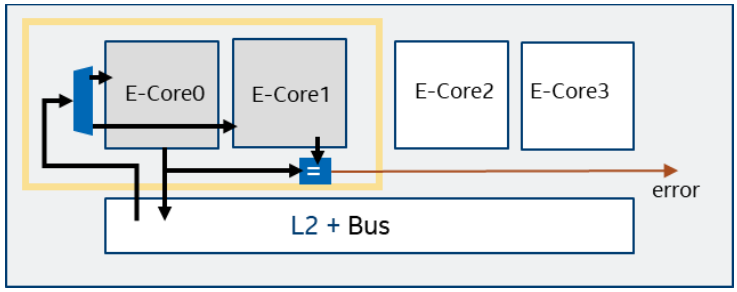

Figure 2 - E-Core Dual Core Lockstep Example

DCLS is configured by the system BIOS/bootloader that determines, via the dedicated model specific register (MSR), which processors enter in lockstep mode. After configuration, the logical processor pairs present as one core with the state of the primary core. The shadow core internally maintains the primary core architectural state and is in lockstep with it.

Each E-core module consists of four E-cores, which can be configured in couples to operate in lockstep. BIOS configuration enables maximum flexibility to configure the two E-core couples within a module to operate in lockstep or not. For each E-core module, the two E-core couples can be configured in the following combinations:

- No lockstep;
- Lockstep between E-core0 and E-core1; E-core2, E-core3 are not in lockstep;
- Lockstep between E-core2 and E-core3; E-core0, E-core1 are not in lockstep; or
- Lockstep between E-core0 and E-core1; lockstep between E-core2 and E-core3.

An example of possible E-core lockstep configurations for eight E-cores (two modules of 4 E-cores each) is provided in Figure 3.

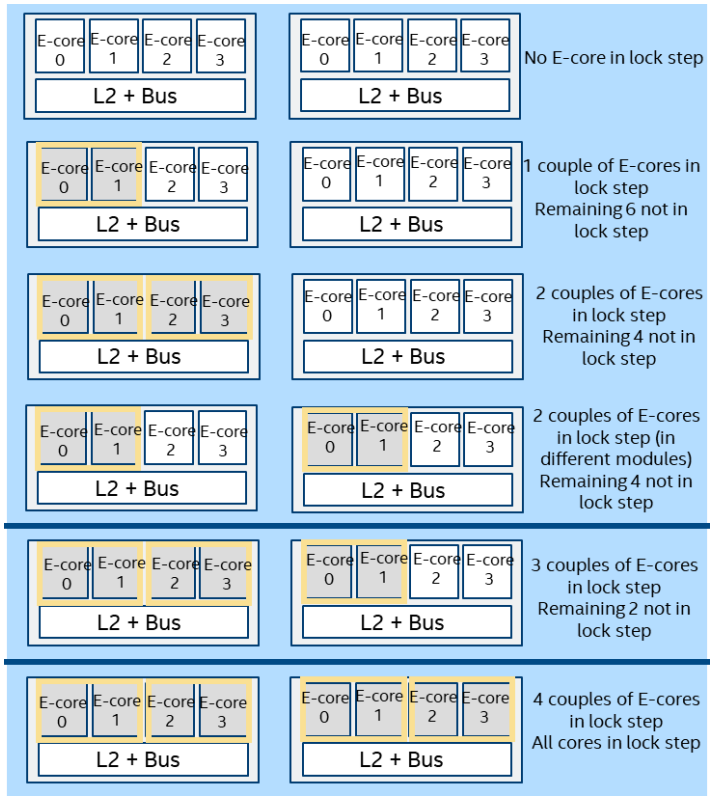

Figure 3- E-Core DCLS Scalability: Configuration Examples

2.1.3 In-Field Scan Logic Test of E-Cores

The E-cores provide a capability to run in-field scan-BIST that can perform diagnostic tests on the E-core and module logic.

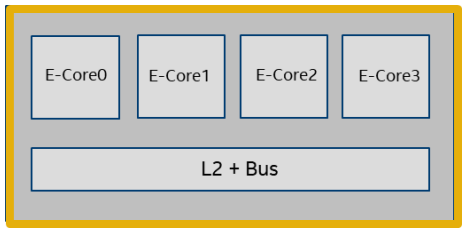

Figure 4 - Module Level Startup In-Field Logic Test

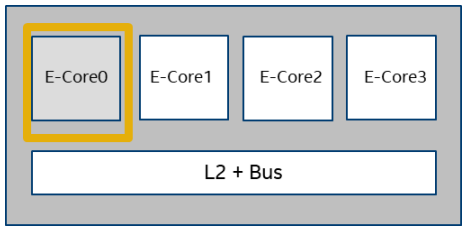

Figure 5 - E-Core Level Periodic In-Field Logic Test

Software can trigger the in-field test leveraging a simple MSR-based interface; the test is automatically run by the E-core hardware itself. To run the test, the E-cores must be in a diagnostic mode; entering/exiting the diagnostic mode is fully managed by the E-core hardware which is transparent to the software. The E-Core hardware ensures

the functional states before and after running the in-field test are identical.

3. BIOS and Intel® Slim Bootloader Support

The Intel® Silicon Integrity Technology leverages the integrated firmware image (IFWI), which comprehends microcode and ingredients required to make the platform operational. This includes the Intel® Firmware Support Package (Intel® FSP) which implements logic to configure and manage integrity features. The Intel® Silicon Integrity Technology leverages the Intel® Slim Bootloader (SBL) as refence platform bootloader.

Intel is also developing a certifiable avionics pre-OS-checker (APOSC) to address bootloader failure modes by verifying that safety related aspects of system are configured as expected before handing over control to the OS/Hypervisor.

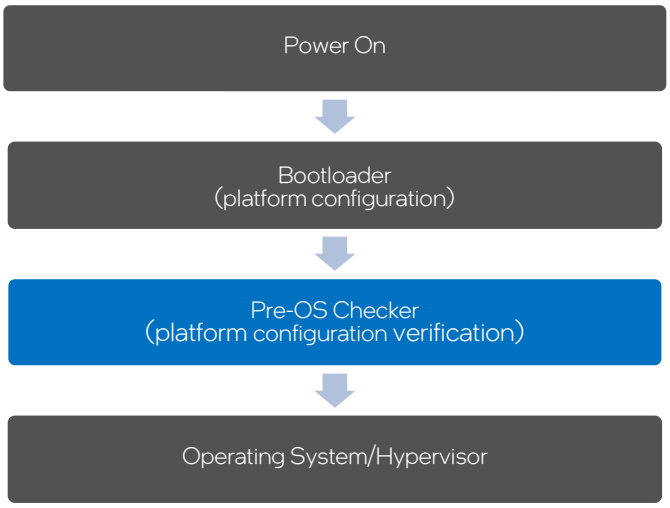

Figure 6 – Boot Flow

4. FuSa Technical Collaterals

In addition to the integrity-related features described in this paper, to help aerospace suppliers in their efforts to achieve certification, Intel licenses the Intel® Airworthiness Evidence Package (Intel® AEP) for select Intel® Core™ processors SKUs. The Intel® AEP is a collection of documents for DO-254 and ED-80 that aids in meeting the design assurance requirements of safety critical systems including flight control, cockpit display and flight monitoring systems which can help reduce time to market and help deliver certifiable high-performance components.

Conclusion

Intel® Silicon Integrity Technology is enabled on selected Intel® Processors to support a variety of safety-critical market solutions by integrating SoC hardware and microcode-based integrity-related features with related BIOS and bootloader support.

Intel further facilitates time-to-market for certifiable solutions by providing market-specific evidence packages, such as the Intel® Functional Safety Essential Design Package for industrial IEC-61508 applications and the Intel® Airworthiness Evidence Package for avionics DO-254/ED-80 applications.

If you are interested in learning more about Intel® Silicon Integrity Technology and functional safety-related features in Intel processors, please contact your Intel Sales Representative.