Solution Brief
Flight Safety Certification
Aerospace Industry

Airworthiness Enablement of Systems Using Intel® Multi-Core Processors

Intel licenses Flight Safety Evidence Packages to help aerospace suppliers achieve flight safety certification.

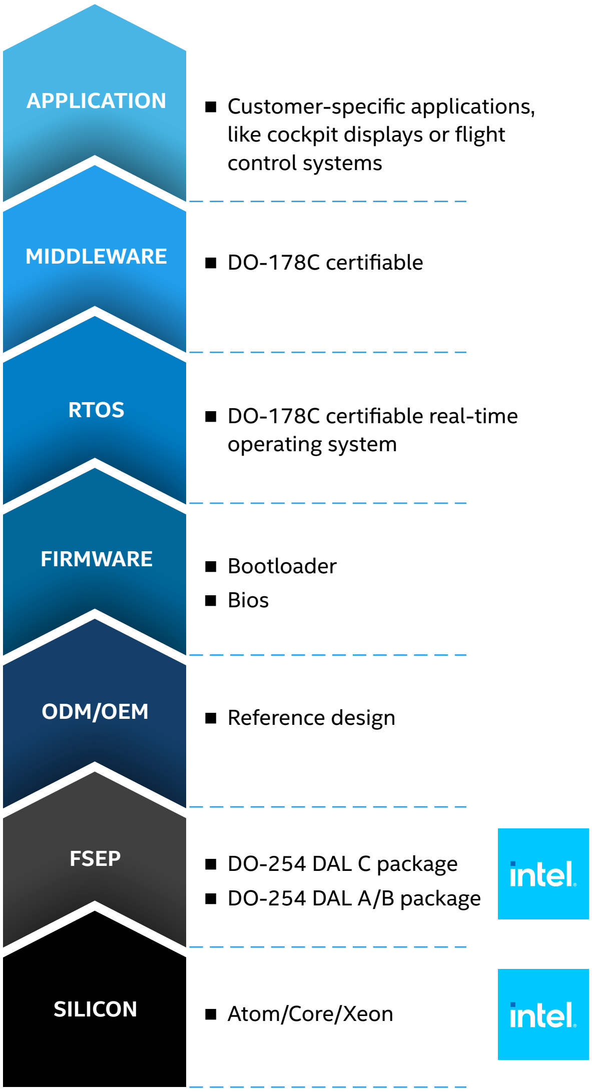
Executive Summary

To help aerospace suppliers in their efforts to achieve certification, Intel is licensing a Flight Safety Evidence Package (FSEP) for the Intel Atom® C3708 processor. This FSEP was developed to support Lockheed Martin's certification for its F-35 fighter aircraft by providing the evidence needed for DO-254 certification. The Intel Atom® C3708 processor is also backed by an ecosystem of hardware and software suppliers, including real-time operating systems and middleware certifiable to DO-178C. Intel's avionics roadmap includes processors that offer a range of performance and size, weight, and power (SWaP) options.

Intel Addresses Multi-Core Processor Certification Challenges

The avionics industry has begun to transition safety critical electronic systems from single-core to multi-core processors to improve performance and SWaP compared to traditional single-core processors.

Multi-core processors are more challenging to certify than single-core processors because of potential performance degradation due to unintended interactions between applications, such as contention for system memory, I/O, and other shared platform resources. Interference between applications, including time delays, could cause non-deterministic



APPLICATION	Customer-specific applications, like cockpit displays or flight control systems
MIDDLEWARE	DO-178C certifiable
RTOS	DO-178C certifiable real-time operating system
FIRMWARE	Bootloader Bios
ODM/OEM	Reference design
FSEP	DO-254 DAL C package DO-254 DAL A/B package
SILICON	Atom/Core/Xeon

and unsafe behavior. The CAST-32A—the position paper published by an international group of certification and regulatory authority representatives called the Certification Authorities Software Team (CAST)—provides guidance for identifying and mitigating potential failure conditions due to interference.

As the avionics industry moves to commercial-off-the-shelf (COTS) multi-core processors, Intel can help aerospace suppliers in their efforts to achieve certifications for flight safety by providing documentation on how the silicon performs under various conditions.

With significant experience in functional safety, Intel has introduced a "Flight Safety Evidence Package" for the Intel Atom® processor C3708 series that provides aircraft embedded manufacturers with processor artifacts to support DO-254 certification up to design assurance level (DAL) A. Intel licenses this data package to help aerospace customers achieve airworthiness certification with less development effort and risk than if customers attempted to generate processor artifacts on their own.

Determinism for Real-Time Workloads

COTS processors are popular with aerospace suppliers because they offer low-cost alternatives to full mil-spec parts, and reduce time to market and production costs.[1] However, demonstrating design assurance of COTS processors can pose serious difficulties since their inner workings are considered proprietary and best known by the silicon vendor.

A common design assurance challenge is to establish an application's worst-case performance and deterministic response. To address this challenge, information about the processor architecture is required which designers are typically unable to access (Table 1). Without understanding the behavior of multi-core processors, systems developers can struggle to

SHARED RESOURCE	MECHANISM
System Bus	Contention by multiple cores Contention by other devices: I/O, DMA, etc. Contention by coherency mechanism traffic
Shared Cache	Cache line eviction Contention due to concurrent access Coherency: Read delay due to invalidated entry Coherency: Contention by coherency mechanism
Local Cache	Coherency: Read delay due to invalidated entry Coherency: Contention by coherency mechanism read
Translation Lookaside Buffers (TLBs)	Coherency overhead
Pipeline Stages	Contention by parallel threads

Table 1. Undesired Processor Mechanisms Affecting Temporal Determinism[2]

induce and guarantee mitigation of all potential failure conditions. For example, processor manufacturers may typically withhold details about how a multi-core processor's shared cache works (e.g., when cache lines are evicted), although cache operation has a significant impact on application performance. Consequently, it is a significant advantage for aerospace suppliers to closely cooperate with COTS silicon manufacturers to rigorously characterize application performance and behavior.

Applying Functional Safety Expertise to Flight Safety

An essential requirement of safety-critical systems is the ability to gracefully handle the unexpected, whether it is caused by operator error, hardware failure, environmental change, or other factors. Functional safety (FuSa) is defined as the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electronic systems. FuSa is governed by International Standards that describe the requirements and the "state-of-the-art" techniques and methodologies to fulfill them. These systems must correctly respond to many inputs, remaining in a predictable state to avoid harming humans or damaging critical infrastructure. To create solutions to help its customers with their flight safety certifications, Intel has built upon its foundational expertise in functional safety.

Functional safety is critical in a wide range of applications that use Intel® processors, including smart grids, connected vehicles, healthcare, robotics, industrial control systems, and oil and gas extraction. For years, Intel technology has helped industrial and automotive system manufacturers attain certifications to the IEC 61508 and ISO 26262 standards for industrial and automotive safety critical systems.

Intel consulted with a FAA Designated Engineering Representative (DER) to perform a gap analysis between the avionics DO-254 standard (including EASA Certification Memorandum EASA CM – SWCEH – 001) and the ISO 26262 standard used in automotive applications. The DER determined that the safety approaches of the two standards are generally equivalent and many of the major objectives, requirements, methods, and activities can be mapped. However, there are some differences in the required level of artifact details needed by avionics system developers to demonstrate airworthiness of an avionics system.

Intel's component level Flight Safety Evidence Package provides a significant advantage to the system developer in addressing the gaps between ISO26262 and DO-254 and helps identify the additional work needed to achieve a DO-254 certifiable system.

Reduce Time to Market with Unparalleled Access to Flight Safety Evidence

Intel is now applying its expertise in multi-core processor technologies for functional safety to support avionics applications. One example is the Flight Safety Evidence Package developed for the Intel Atom® processor C3708, which is well suited for applications such as flight control, engine control, and flight mission computers.

Originally developed in partnership with Lockheed Martin for use on their F-35 platform, the FSEP provides the evidence needed by system integrators to independently achieve DO-254 certification up to DAL A. Additionally, the FSEP contains artifacts addressing more than 200 items in the form of answered questions and information; some of these items are discussed in more detail in the following:

Failure Modes, Effects, and Diagnostic Analysis (FMEDA)

This report identifies potential processor failure modes, failure rates, and their impact on processor and system operation. This information can be used to determine the severity of a failure mechanism and develop recovery strategies.

Reliability Data

Component reliability modeling and qualification data (e.g., failures in time (FIT) and defects per million (DPM)) enables system integrators to design off-chip mitigations to comply with platform reliability targets needed to achieve safety certification.

Single Event Effects Analysis

Single event effects (SEE) testing, characterization, and modeling was performed under terrestrial environments at 900 meters using beam testing to measure susceptibility (e.g., bit flips) via FIT rate calculations across the design hierarchy. This granular SEE data enables the development of targeted mitigations, as needed.

Shared Resource Management

CAST-32A was used to characterize the processor's determinism, ensuring calculations are highly repeatable, execute within a bounded time frame, and meet worst-case execution-time-targets. Intel® Resource Director Technology enables tracking and control of shared resources. This technology provides visibility and control over Last Level Cache and memory bandwidth used by applications, containers, or virtual machines (VMs) running concurrently on the platform. Cache and memory monitoring and allocation capabilities enable safety-critical Software Applications to behave more deterministically. Furthermore, Intel® Time Coordinated Computing Technology supports clock synchronization inside applicable SoCs across data networks, thus reducing the risk of interference adversely affecting applications hosted on multiple systems.

Product Service Experience

Intel provides an estimate of the service experience of its products operating in certain environments, including commercial electronics, automotive, commercial aerospace, and medical. Where there is low product service experience, Intel provides additional artifacts that support applicable design assurance activities for highly complex COTS microprocessors.

Intel Introduces DO-254 Flight Safety Evidence for the Atom® Processor C3708

Developed for SWaP-constrained applications, the 1.7 GHz Intel Atom® processor C3708 series delivers exceptional performance-per-watt with a low thermal design power of 17W. As a system-on-a-chip (SoC), it enables compact designs without sacrificing I/O flexibility or computing performance. The processor is on Intel's long-life roadmap and has an extended operating temperature range of -40°C to +85°C.

A flexible array of on-chip I/O includes 20 lanes of configurable high-speed input/output (HSIO), 16 lanes of PCIe Gen 3, x16 SATA* 3.0, and four USB 3.0 ports. A fixed embedded MultiMediaCard (eMMC) enables customization, including dedicated functional safety channels and support for next-generation storage expandability.

The Intel Atom® processor, detailed in Figure 2, has several features that contribute to higher flight safety, such as:

High Level of Determinism

The processor has eight powerful 64-bit processor cores, each with dedicated 2 MB L2 cache. Since each processor core has its own large cache, it can run quickly and without delays caused by sharing cache with other processor cores. Software-guided redistribution of cache capacity is enabled by Cache Allocation Technology, allowing critical applications to benefit from improved cache capacity and reduced cache contention.

Soft Error Rate Protection

Error-correcting code (ECC) memory support helps safeguard data stored in memory by automatically detecting two-bit errors and correcting single-bit errors every 64-bits.

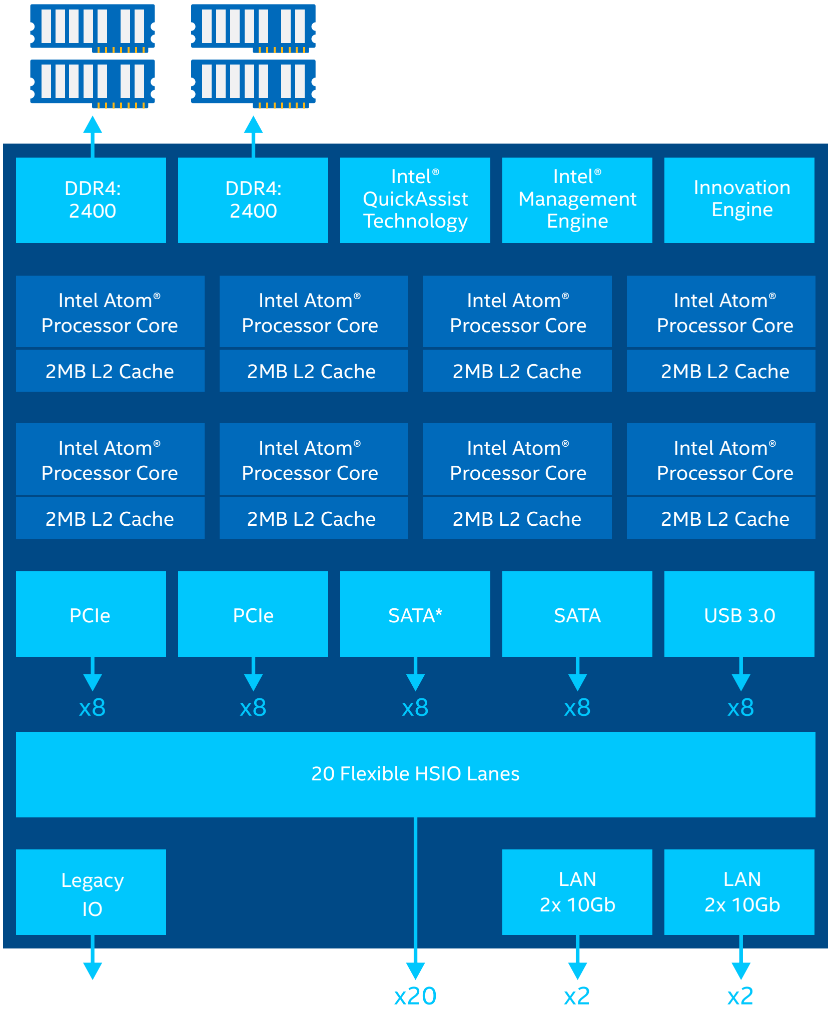


Figure 2. Intel Atom® Processor C3708 Block Diagram

Cybersecurity Acceleration

Intel® QuickAssist Technology provides accelerated security and networking capabilities, including up to 20 Gbps cryptography and up to 20 Gbps compression. This technology allows avionics systems to encrypt and decrypt communications over wireless networks without burdening the processor. Features include symmetric encryption and authentication, asymmetric encryption, digital signatures, RSA, DH, and ECC, and lossless data compression.

Error Reporting

The processor detects and reports processor and I/O errors:

- Machine Check Architecture (MCA) for core and uncore modules
- Advanced Error Reporting (AER) for PCI Express* devices and integrated I/O modules

DO-254/ED-80 Certification Evidence

Aerospace suppliers may be able to accelerate their development of safety-certified avionics systems by using COTS Intel® silicon and Flight Safety Evidence documentation from Intel.

Manageability and Security Feature Inclusion

Intel's Integrated Innovation Engine enables developers to create custom firmware that adds manageability and security features to solutions without the cost, space, or power required for baseboard management controllers (BMC). In addition, Intel's ecosystem of ODM and ISV partners offers Innovation Engine applications that allow avionics developers to integrate additional hardware-based features without the need to create custom firmware themselves

Going to Market with Intel®-Based Solutions

Aerospace suppliers can more easily and efficiently build airworthy, application-ready platforms using Intel hardware and other hardware and software solutions offered by Intel's large network of ecosystem partners. These solutions include Intel processor-based boards, firmware, real-time operating systems (RTOS), and middleware certifiable to DO-254 DAL A/B/C and DO-178 A/B/C. In the avionics industry, Intel has strong ties with many well-known ODMs and ISVs that can help aerospace suppliers lower their development cost and reduce risk.

As an essential part of any flight safety certifiable system, real-time operating systems (RTOS) provides the foundation for software developers to build their applications. Lynx Software Technologies is example of a key ecosystem partner with a deployed RTOS solution for Intel's multi-core processors.

Lynx Delivers Flight-Certifiable Solution for the Atom® Processor C3708

Lynx Software Technologies (Lynx) offers the LYNX MOSA.ic™ for avionic platforms that meet the exacting standards of DO-178B, software considerations in airborne systems and equipment certification. These considerations include:

- FAA AC 20-148 Reusable Software Component (RSC) certified RTOS
- Intel-specific DO-178C DAL A RTOS and network stack quality artifacts
- Intel-specific CAST-32A multi-core certification support

The Lynx solution supports open standards and APIs (FACE, POSIX), an IPv6 network stack, and file system with support for Intel virtualization, multi-core, cache partitioning, and SR-IOV.

To learn more about how Intel and Lynx products provide complementary technologies to address Avionics DO-178 visit https://www.lynx.com/products.

Avionics Safety with Intel

In the future Intel, Lynx, and other ecosystem partners will be delivering flight safety evidence and full avionics solution stacks for a variety of Intel Processors.

More Information

For more information about the Flight Safety Evidence Package discussed in this paper, please email us at: **IOTG-PublicSector@intel.com**

Notices & Disclaimers

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors.

Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For complete information visit www.intel.com/benchmarks.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Customer is responsible for the overall system and system level safety where Intel Products are used, including compliance to any applicable regulatory standards or safety-related requirements. Intel bears no responsibility, liability, or fault for any integration or system level issues associated with the inclusion of the Intel Products into a system, including where the failure of the system could result in personal injury. It is Customer's responsibility to design, manage, and assure safeguards to anticipate, monitor, and control component, system, quality, and or safety failures.

No product or component can be absolutely secure. Intel is not responsible for the design and assurance of system-level safeguards to anticipate, monitor, and control system failures required for end products used in safety-critical applications designed to comply with functional safety standards or requirements.

Your costs and results may vary.

Intel technologies may require enabled hardware, software, or service activation.

[1] Jonathan Wilkins for the Aerospace Manufacturing publication, "Using COTS: is it worth the risk?" March 19, 2019, https://www.aero-mag.com/using-cots-is-it-worth-the-risk

[2] Ondrej Kotaba et al, "Multicore in Real-Time Systems – Temporal Isolation Challenges Due to Shared Resources," http://www.cister-labs.pt/docs/multicore_in_real_time_systems_-_temporal_isolation_challenges_due_to_shared_resources/1044/view.pdf