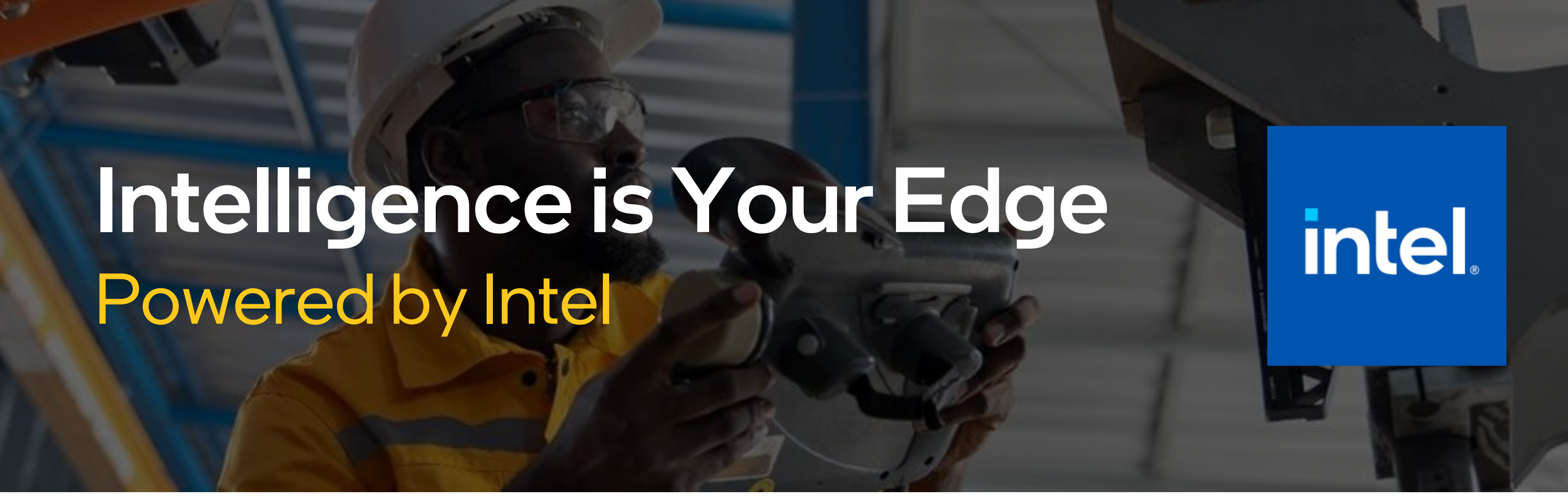


Intelligence is Your Edge

Powered by Intel

Functional Safety with Intel safety capable processors

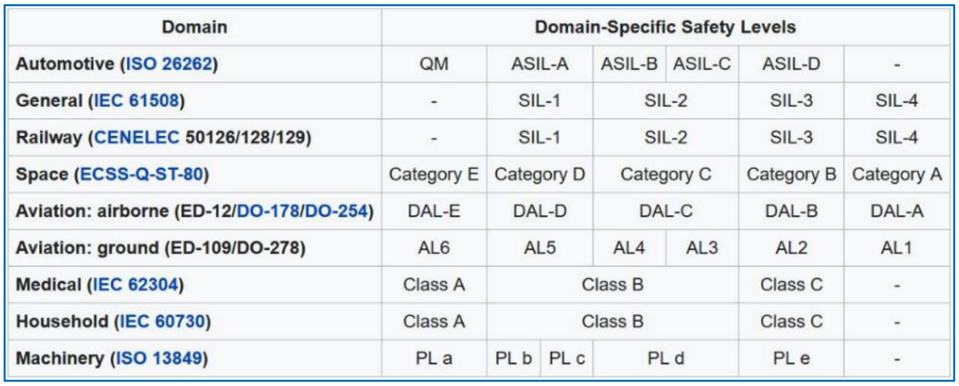
Written by Raj Darshan, Federal & Industrial Tech Platforms, Intel®

For Software-defined Workload consolidation and high-performance safety workloads

For software-defined workload consolidation and high-performance safety workloads, functional safety is, simply put, "protecting a user from technology." It also protects technology from users. More technically, however, the definition of functional safety is, "systems that lead to the freedom from unacceptable risk of injury or damage to the health of people by the proper implementation of one or more automatic protection functions (often called safety functions). A safety system consists of one or more safety functions."

Functional Safety techniques are implemented as a "separate" entity that monitors sensors and actuators, which can put the system in a known good state in case of a failure. Separation between control function and safety function grows with increasing Safety Level. In the case of a Real Time system, an application missing a cycle can result in a CNC machine that creates an out-of-spec wonky part or a weld that fails quality check. This can be quite expensive due to wasted raw materials, workforce, energy consumption in addition to delays, penalties, and loss of revenue.

When human lives are at stake in activities that interact with such systems the precautions taken need to be much more ordered, deliberate, and systematic to bring down the chances of a mishap.



Domain	Domain-Specific Safety Levels						
Automotive (ISO 26262)	QM	ASIL-A		ASIL-B	ASIL-C	ASIL-D	-
General (IEC 61508)	-	SIL-1		SIL-2		SIL-3	SIL-4
Railway (CENELEC 50126/128/129)	-	SIL-1		SIL-2		SIL-3	SIL-4
Space (ECSS-Q-ST-80)	Category E	Category D		Category C		Category B	Category A
Aviation: airborne (ED-12/DO-178/DO-254)	DAL-E	DAL-D		DAL-C		DAL-B	DAL-A
Aviation: ground (ED-109/DO-278)	AL6	AL5		AL4	AL3	AL2	AL1
Medical (IEC 62304)	Class A	Class B				Class C	-
Household (IEC 60730)	Class A	Class B				Class C	-
Machinery (ISO 13849)	PL a	PL b	PL c	PL d		PL e	-

Fig 1. Different Functional Safety Standards and their application/domain (Ref)

Functional safety inherently relies on a real-time system (often in the 1 to 100 millisecond time range) that is now used in environments where control operations can adversely impact humans if the system misbehaves. This can range from a lost fingernail, lost finger, severe damage to body parts that can hamper the livelihood of the impacted individual(s), to death or deaths. To address each level of severity, there are various levels of safety in each safety standard. As a simplified example, considering the IEC 61508 safety standard, an Agri-Tech robot in the field is SIL1, Autonomous Mobile Robots (AMR) on a factory floor are SIL2, a safety PLC measuring the pressure/temperature of a tank in an industrial-scale hydrochloric acid plant is SIL3, and a train carrying hundreds of passengers has its brake system designed to a safety target of SIL4.

Functional Safety with Workload consolidation

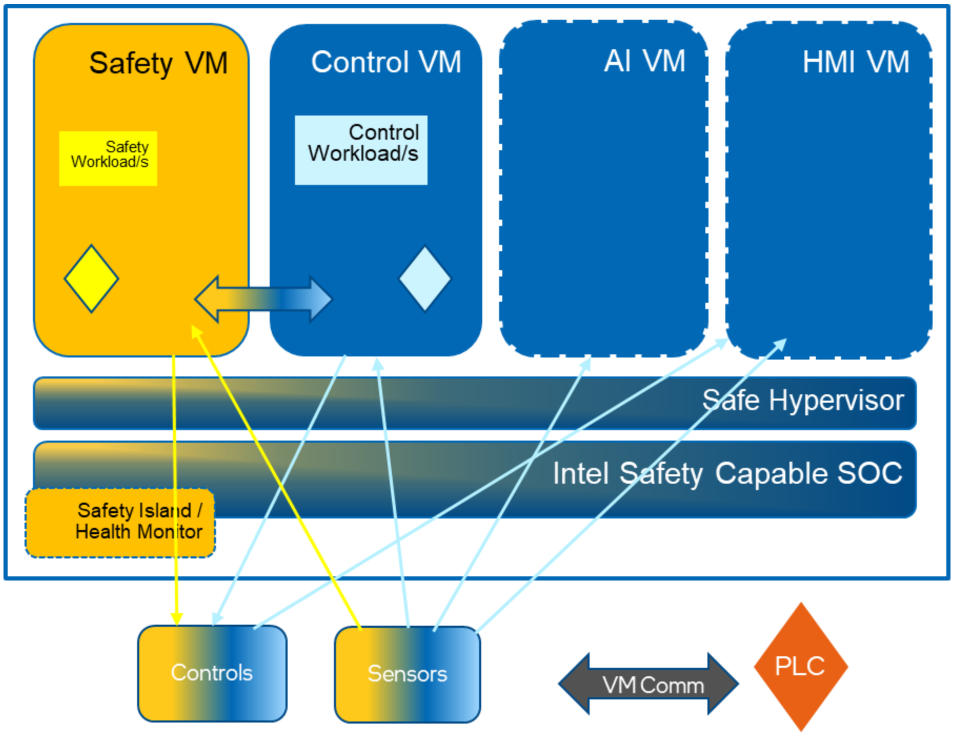


Fig 2. SW defined workload consolidation (WLC) with Functional Safety workloads

Industrial workloads that run on fixed-function microcontrollers (uC) are indeed "fixed" to a single/select purpose. Any change in purpose or application requires manual updates (HW and/or SW) and re-provisioning. This increases operation costs and reduces flexibility in the long run. Industrial applications are evolving using cloud technologies at the edge, becoming compute-intensive, and using new sensors, communication buses/protocols to address enhanced automation requirements. It is hard to impossible to run these on low-performance microcontrollers.

How is the problem addressed with Intel® SoCs?

1. Transition applications on fixed-function microcontrollers to general-purpose software workloads and applications runnable on Intel® SoCs – a Software (SW) Defined Workload. It is comparable to apps on a smartphone – be it a keyboard or a paintbrush, phone, or messaging, they are all applications.

2. Leverage multiple cores and AI processors on a single Intel® chip to consolidate multiple such SW workloads – Real-Time (RT), Artificial Intelligence (AI), and Functional Safety (FuSa) Work-Load-Consolidation (WLC).

3. Leverage cloud-based technologies - containerization, orchestration to enable manageability and provisioning to purpose, provide scale, availability, and recoverability.

Intel® Offerings for Functional Safety

1. Intel® Processor SKUs that are functional safety capable due to specially integrated features and IPs.

2. Documentation addressing random HW failures (IP level, SoC level), safety analysis, systematic capability, and Silicon Integrity Technology:

    - Functional Safety Essential Design Package (FSEDP).

3. SIL3 Safety Pre-OS Checker (Safety HV/RTOS can also address it).

4. SlimBootLoader (SBL) – for reference only (Independent BIOS Vendor (IBV) to supply for commercial use).

5. Collaboration with popular safety software vendors and board manufacturers to design and develop a safety-certified platform.

Functional Safety on Intel® for a Future of Fully Autonomous Systems

- Intel® functional safety-capable processors, along with providing industrial use conditions, extended temperature ranges, and long life, offer value for:

    - Truly software-defined workload consolidation (WLC) – Real-Time, AI, Functional Safety

  - Bill of Materials (BOM) simplicity

- Manageability, provisioning, availability, recoverability/healing

- Adaptable/Flexible functional safety goals and signatures on the same hardware by changing safety software.

- Use of new sensors, multi-modal inputs, complex safety workloads/decisions, high compute.

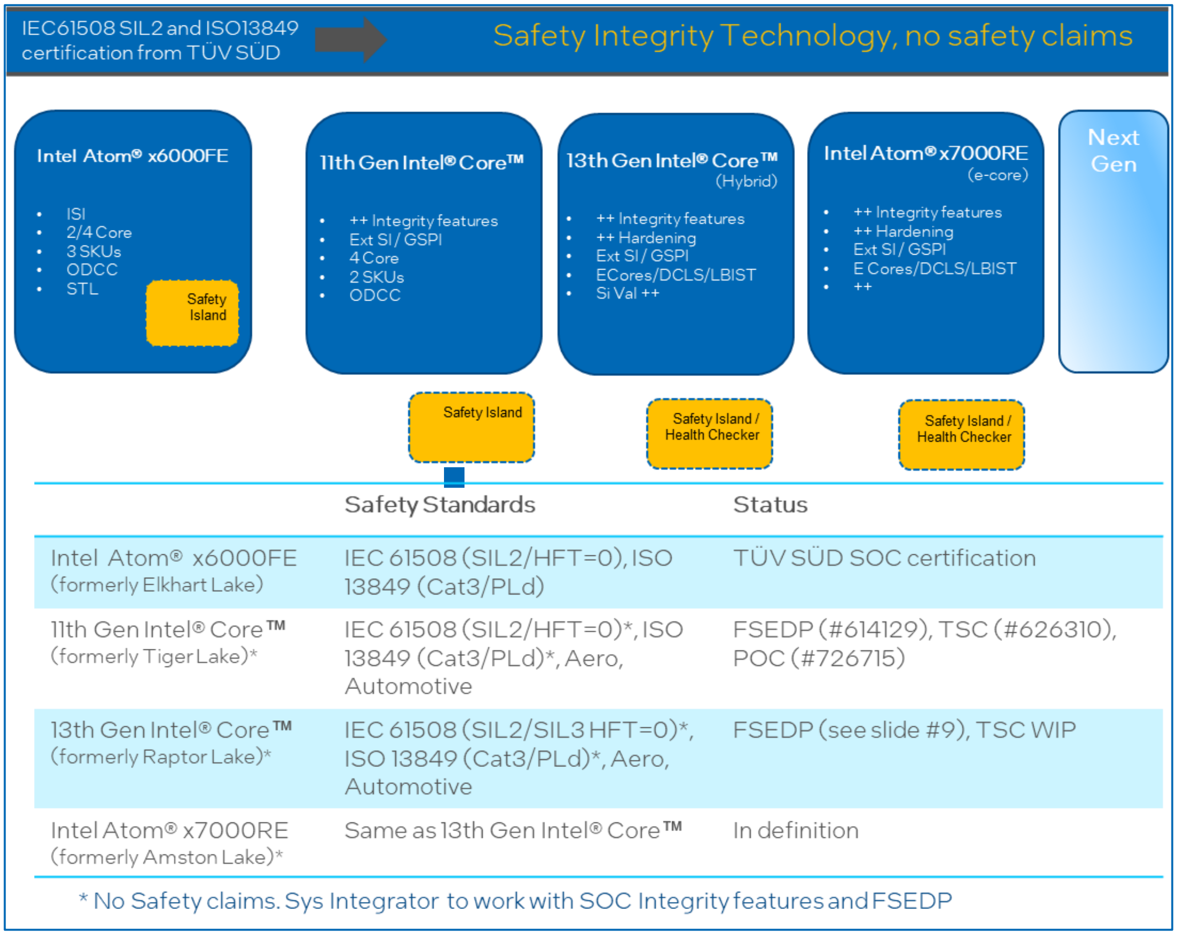
- Achieving more than red-orange-green safety output.

- Preventive, predictive safety analysis and decisions.

- Intel® generation-on-generation compatibility – reuse, scale, core count, performance.

Intel's Functional Safety-Capable Processor Journey

Intel's functional safety journey started with the Intel Atom® x6000FE (formerly Elkhart Lake) family of processors. Since then, improvements have been made generation-on-generation to serve a wider variety of safety applications by developing safety-capable processors.

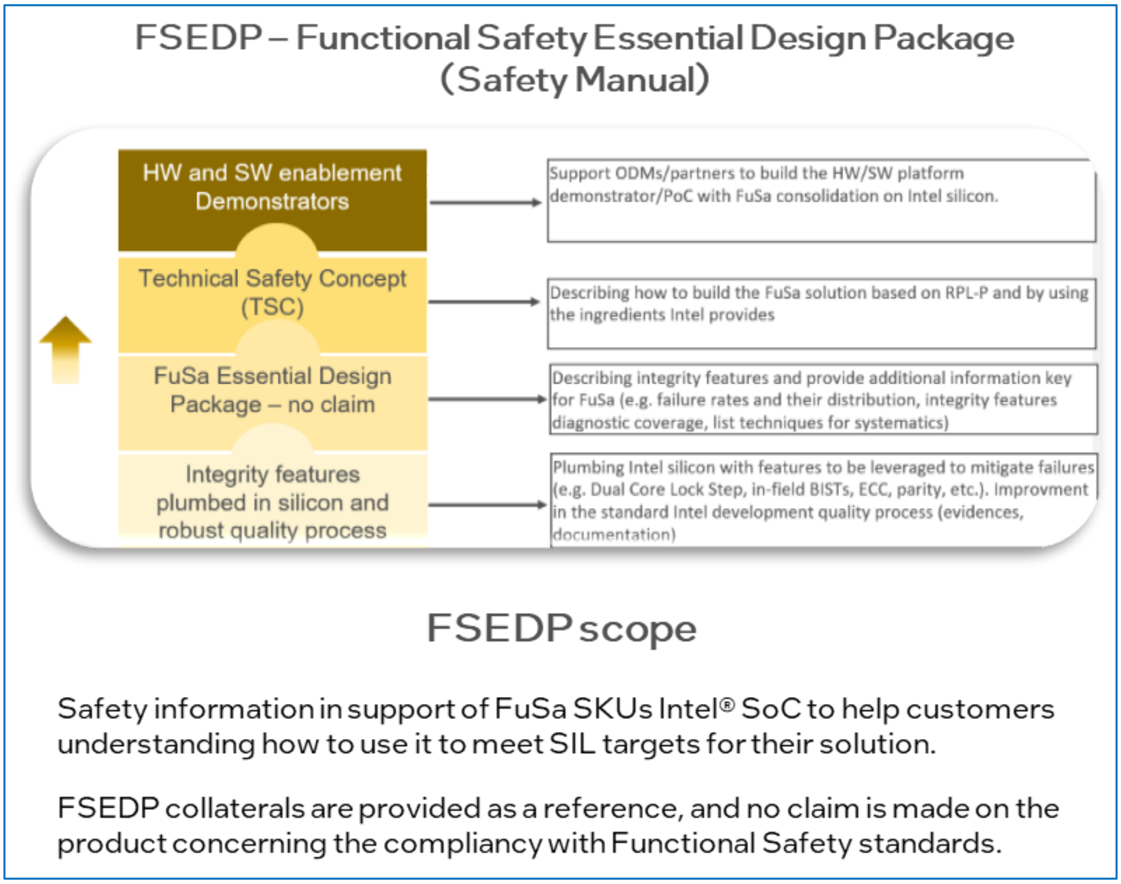


	Safety Standards	Status
Intel Atom® x6000FE (formerly Elkhart Lake)	IEC 61508 (SIL2/HFT=0), ISO 13849 (Cat3/PLd)	TÜV SÜD SOC certification
11th Gen Intel® Core™ (formerly Tiger Lake)*	IEC 61508 (SIL2/HFT=0)*, ISO 13849 (Cat3/PLd)*, Aero, Automotive	FSEDP (#614129), TSC (#626310), POC (#726715)
13th Gen Intel® Core™ (formerly Raptor Lake)*	IEC 61508 (SIL2/SIL3 HFT=0)*, ISO 13849 (Cat3/PLd)*, Aero, Automotive	FSEDP (see slide #9), TSC WIP
Intel Atom® x7000RE (formerly Amston Lake)*	Same as 13th Gen Intel® Core™	In definition

* No Safety claims. Sys Integrator to work with SOC Integrity features and FSEDP

Fig 3. Intel Functional Safety capable processors, gen-on-gen

Intel® functional safety-capable processors provide building blocks in terms of documentation, Pre-OS Checker (POSC), and preliminary safety concepts to software and hardware vendors, enabling them to leverage these features further in their designs.



FSEDP – Functional Safety Essential Design Package (Safety Manual)

HW and SW enablement Demonstrators → Support ODMs/partners to build the HW/SW platform demonstrator/PoC with FuSa consolidation on Intel silicon.

Technical Safety Concept (TSC) → Describing how to build the FuSa solution based on RPL-P and by using the ingredients Intel provides

FuSa Essential Design Package – no claim → Describing integrity features and provide additional information key for FuSa (e.g. failure rates and their distribution, integrity features diagnostic coverage, list techniques for systematics)

Integrity features plumbed in silicon and robust quality process → Plumbing Intel silicon with features to be leveraged to mitigate failures (e.g. Dual Core Lock Step, in-field BISTs, ECC, parity, etc.). Improvment in the standard Intel development quality process (evidences, documentation)

FSEDP scope

Safety information in support of FuSa SKUs Intel® SoC to help customers understanding how to use it to meet SIL targets for their solution.

FSEDP collaterals are provided as a reference, and no claim is made on the product concerning the compliancy with Functional Safety standards.

Fig 4. Intel FSEDP for Functional Safety capable SKUs

Once Intel® functional safety SKUs provide their feature set, board vendors, BIOS vendors, safety software hypervisor/RTOS providers, and safety software middleware and applications come together to create a safety system addressing end-user and application requirements.

OEMs often cover the applications as each addresses a unique problem. Middleware and communication protocols to talk to sensors and actuators are common and need to run on a safety-certified RTOS (QNX and Sysgo on Intel® today; less safety-critical Cat2-PLb, SIL1 systems can use Linux though). ODMs, OEMs, and software vendors with a template/blueprint for functional safety-compliant offerings can design once, copy, and repeat for generation-on-generation Intel® SoCs with a one-time and recurring minimal NRE investment. All these activities are often done in alignment/consultation with a safety body/expert at each stage.

Intel® functional safety-capable processors provide building blocks in terms of documentation, Pre-OS Checker (POSC), and preliminary safety concepts to software and hardware vendors, enabling them to leverage these features further in their designs.

Conclusion

Intel's functional safety-capable processors are designed to meet the rigorous demands of fully autonomous systems that often interact with multi-modal inputs requiring high performance. These processors not only offer industrial use conditions, extended temperature ranges, and long life, but they also provide value in terms of software-defined workload consolidation, high performance, real-time processing, artificial intelligence (AI), and functional safety. It is an exciting phase in automation that requires zero-touch onboarding, provisioning, availability, and recoverability/healing capabilities for achieving fully autonomous systems, whether in manufacturing or multi-functional robotics systems usable in commissioning to a production line.

References and Links

Intel® Silicon Integrity Technology for Industrial - Tech Brief	https://www.intel.com/content/www/us/en/content-details/829836/content-details.html
Functional Safety with Intel® – presentation deck	https://www.intel.com/content/www/us/en/secure/content-details/834013/content-details.html
Sysgo PikeOS with Intel®	https://www.sysgo.com/blog/article/intel-sysgo-building-a-functional-safety-compliant-industry-solution-for-iec-61508 https://www.sysgo.com/technology-alliances/nexcobot
QNX with Intel®	https://www.blackberry.com/us/en/company/newsroom/press-releases/2024/blackberry-qnx-introduces-software-defined-functional-safety-platform-in-collaboration-with-intel-for-industrial-automation
Nexcobot SCB100 with Intel Atom® x6427FE Processor - IEC 61508 and ISO 13849-1 certified platform	https://www.nexcobot.com/en/product/robot-system/robot-safety/scb100
TÜV SÜD	https://www.tuvsud.com/en-us/services/functional-safety/about

Partner Name

Intel Corporation

Booth Info

Hall 5
Booth #5-353

embeddedworld
Exhibition&Conference