WHITEPAPER

How Infineon ISO 26262 AURIX™ TC3xx microcontroller supports safety critical certification within aerospace industry

Date: 07/2024

www.infineon.com/aurix

Table of contents

Abstract

Aerospace industry is on the threshold of a new era in aviation aircrafts. Advanced Air Mobility (AAM) is emerging as a major force that promises to revolutionize the way we perceive and experience air travel. The seamless integration of cutting-edge technologies requires careful consideration of aerospace regulations which are commonplace in the aerospace industry and high-volume electronic components. Within this dynamic landscape, an exciting opportunity arises in the form of leveraging microcontrollers, specifically those conforming to highest Automotive Safety Integrity Level (ASIL-D), as defined within ISO 26262, for applications in aerospace.

TC3xx is Infineon's second generation of AURIX™ safety critical microcontrollers. Its innovative multicore architecture is based on up to six independent 32-bit TriCore CPUs, running at 300 MHz with four additional checker cores and delivering 4000 DMIPS. These microcontrollers are designed to meet the highest safety standards, while simultaneously increasing performance significantly. The TC3xx family is equipped with Flash memory up to 16 MB flash and up to 6.9 MB SRAM and powerful Generic Timer Modules (GTM). Further functional highlights are 1Gbit Ethernet, up to 12 CAN FD data frames. The AURIX™ TC3xx microcontrollers also stand out with high flexibility, best-in-class power consumption and significant cost savings.

This paper will discuss the synergy of ISO 26262 [1] safety evidence for aerospace relevant use cases on Infineon's AURIX™ TC3xx microcontroller family.

We will start with an abstract on ISO 26262 [1] development approach and compare it with EUROCAE ED-135 [5] / SAE ARP4761A [6] needs.

Then we set out the ways in which the AURIX™ TC3xx family aligns with the COTS (Commercial Off-The-Shelf) objectives defined in AMC20-152A [7] / AC20-152A [8], by illustrating the robust technical data supporting these objectives.

Also, we will highlight some internal AURIX™ TC3xx safety features which can support the aerospace engineers in developing improved and enhanced monitoring capabilities to simplify external monitoring functions by keeping the detection rate at the same or even higher level compared to classical aerospace monitoring concepts.

Lastly, we will present innovative thoughts on how the AURIX™ TC3xx functionality and information can play a decisive role in achieving multi-core certification objectives outlined in AMC20-193 [9] / AC20-193 [10].

Note: since EASA and FAA have own guideline and standard naming, even if the content is very similar, within the following paper the nomenclature is that both guidelines and standards are listed as following; <EASA-Standard> / <FAA-Standard>.

1 Infineon components within aerospace use case

1.1 Synergies from automotive standard ISO 26262 within aerospace development guidelines

Many Infineon products, like for example the AURIX™ TC3xx, are developed to satisfy the highest safety needs (ASIL-D) within automotive industry. The AURIX™ TC3xx is developed for the highest safety functions (ASIL-D) within automotive products, as the microcontroller has the capability to detect controller errors independently and react to detected failures, such as transferring into a fail-safe condition. To confirm the safety capabilities of the microcontroller within an electronic control unit, the AURIX™ TC3xx was developed in accordance with ISO 26262 regulations. To meet the highest safety requirements, it is important that the product is defined by a requirements-based development which is performed according to the V-model.

Infineon has developed the AURIX™ TC3xx according to the ISO26262 V-Cycle, which is similar to the one in EUROCAE ED-79B [11] / SAE ARP4754B [12] guideline. The mentioned development process is presented within Figure 1 below. Each development phase is supported by detailed safety analysis (within workflow covered by the verification activities) and documented in exhaustive safety reports [e.g., Fault Tree Analysis (FTA), Dependent Failure Analysis (DFA), Failure Mode Effect and Diagnostics Analysis (FMEDA)].

The safety activities capture the safety requirements applicable to the device in terms of reliability, failure rates, failure detection means and rates (or safety mechanisms and diagnostic coverage). As the AURIX™ TC3xx is developed as a Safety Element out of Context (SEooC), the captured requirements are assumed based on use-cases that are written in the safety manual. All potential failure modes of the device and the safety mechanisms to detect and control the failure modes and assess the effects of the failure modes within the device have been identified. The results are reported in the FMEDA. And finally, the safety requirements have been validated and verified, as documented within the Safety Case Report [32].

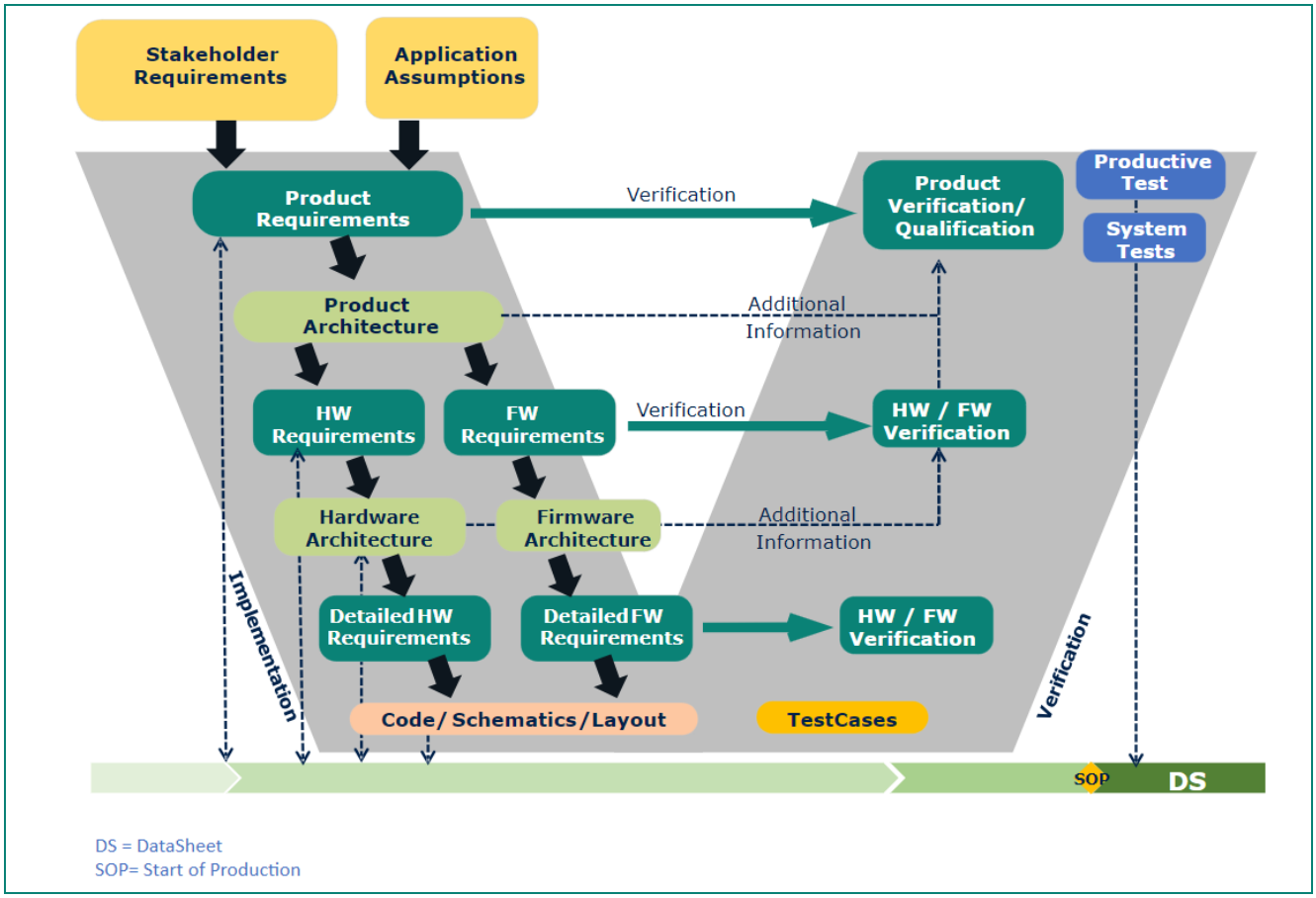

Figure 1 Requirements based development in accordance with ISO 26262 (source: Infineon)

The Top-Level Safety Requirements (TLSR) applicable to the device are identified in the Safety case report which is part of the safety package. These Top-Level Safety Requirements (TLSR) breakdown into the Technical Safety Requirements (TSR) and are allocated to the HW and SW design. The HW and SW mechanisms are developed respectively within the HW and SW detailed design and implementation phases. The safety case report describes then:

- How the MCU fulfils all the Top Level Safety Requirements (TLSR). The evidences are based in particular on the results of several activities such as the full verification of the Register Transfer Language (RTL) and post layout netlists, the full verification of the source code for Firmware (FW) and product verification of the HW-SW interface specification
- How the Random Hardware Faults (RHF) and safety related aspects of SW are covered. In particular:
    - how the MCU is able to detect/control all failure modes in the HW to avoid violation of any TLSR
    - how it is ensured that the TLSR and TSR are not violated by dependent faults in HW
    - how it is ensured that all the HW architectural metrics (SPFM, LFM, PMHF) which are defined in the TLSRs are met
    - how it is ensured that the developed SW is free from systematic fault
    - how it is ensured that all dependent failures have been analysed and considered in the developed SW.
- How the MCU is developed free from systematic faults, in particular via the implementation of development and production process, the verification of all HW and SW requirements and the qualification of the product

In addition to the available safety package´s evidences, the following safety analyses are performed (in accordance with ISO 26262 [1]) at the most stringent Safety Integrity Level (ASIL-D):

- Concept Level Fault Tree Analysis (CFTA) supporting the evaluation of random hardware faults and systematic faults versus the Technical Safety Requirement (TSR) applicable to the device
- Concept Failure mode and Effect Analysis (CFMEA) including the effect analysis of derived failure modes originated from random hardware failures occurring during the boot process which could affect the safety functionality within the chip
- Fault tree analysis (FTA) identifying the basic events potentially leading to a top hazard, the minimal cut sets and the associated independence requirements
- Dependent Failure Analysis (DFA) analysing how independence requirements could be defeated and showing evidence how mitigation measures can reduce the common cause failures (CCF) to an acceptable level. The DFA identifies and analyses the dependent failure initiators (DFIs), checks common causes, cascading failures or single events that could bypass or invalidate a required independence or freedom from interference between given elements. The results of the DFA are fed back in the FMEDA
- Design Failure Mode and Effects Analysis (DFMEA) increasing the maturity of the design, identifying and mitigating the systematic faults and especially treating the boot phase during which some safety mechanisms might not be available
- Hazard and Operability Analysis (HAZOP) analyses that the potential risk of a safety goal violation due to systematic software faults is sufficiently low by SW/FW. The basis for the safety analyses is the software architectural design describing the static aspects (e.g., expressed by a block diagram showing the functional elements and their interfaces/relationships) as well as the dynamic aspects (e.g., expressed by sequence, timing or scheduling diagrams or state charts)

  Note: random HW faults are expected to be covered by the safety analysis at the HW level.

Since the strong investment in safety functions of Infineon components could also be of interest for other safety relevant industries, like aerospace industry, Infineon analysed in cooperation with experienced aerospace development organizations how this existing safety evidence can bring added value for aerospace compliant products which needs to be developed in accordance to EUROCAE ED-79B [11] / SAE ARP4754B [12] and EUROCAE ED-135 [5] / SAE ARP4761A [6].

The safety package (upon request) can be used for aerospace products up to Design Assurance Level (DAL) A, like:

- hardware development for COTS analysis as defined within AMC 20-152A [7] / AC20-152A [8] (see §1.2)
- product/equipment development including safety analysis (see §0)
- software development even for multi core processor use cases as defined within AMC20-193/ AC20-193 (see §3)

Note: in front of the authority the organization which applies for equipment certification is mentioned as the applicant. Nevertheless, the item developer of an electronics device needs to respect the certification objectives, this is why within the paper item developer is used instead of applicant.

In conclusion, the AURIX™ TC3xx Microcontroller fulfils its top-level safety requirements. The safety case report provides arguments and evidence (e.g., based on internal assessments and audits) that the AURIX™ TC3xx Microcontroller conforms to the top-level safety requirements under the provided use-cases as stated in the Safety Manual. A list of known open problems / deviations and a declaration of conformance is also provided in the Safety case report.

1.2 Substantiation material to COTS objectives (AMC 20-152A/ AC20-152A)

Most of the Commercial-Off-The-Shelf (COTS) components are not developed according to aviation development assurance standards. Their development and production process undergo a semiconductor industry qualification based on other intended market (automotive, telecom…). COTS devices generally provide "off-the-self" already-developed functions, some of which are highly complex and configurable, and not always suitable for an airborne application.

The risks associated with the use of such COTS devices in an aircraft system or equipment is not zero (e.g., ambiguous detail within the documentation which is important for an airborne application, misalignment between the intended usage and the real usage of the device within airborne conditions, extension of the use of the device beyond the manufacturer's specifications, expertise deficiency in the integration of the device within the equipment). The corresponding risks need to be identified, assessed and if necessary mitigated. This is the purpose of the AMC 20-152A [7] / AC20-152A [8] released by the EASA/ FAA. This document provides the acceptable means of compliance for Airborne Electronic Hardware (AEH) contributing to Development Assurance Level (DAL) A, B or C functions. It describes objectives to support the demonstration of compliance with the applicable airworthiness regulations for the hardware aspects of airborne systems and equipment certification.

Infineon can provide devices contributing to up to Development Assurance Level (DAL) A function.

The first part of the AMC 20-152A [7] / AC20-152A [8] deals with custom design and COTS IP (Intellectual Property) (Soft IP, Firm IP or Hard IP) instantiated within FPGAs/PLDs/ASICs during the development of the custom device. Since the AURIX™ TC3xx is a Complex COTS device the first part of AMC-20 152A [7] is out of scope of this white paper.

The second part of the AMC 20-152A [7] / AC20-152A [8] deals with COTS electronic devices, such as semiconductor product fully encapsulated in a package, which is the concern of Infineon products.

The COTS objectives described in the AMC 20-152A [7] / AC20-152A [8] have to be fulfilled by the item developer of the COTS device. To support the item developer in showing compliance to the AMC 20-152A [7] / AC20-152A [8], Infineon can provide a set of data depending on the COTS objectives.

The following paragraphs are structured as follows:

> **Objective COTS-<COTS objective number> - <COTS objective title>**
>
> "<COTS objective summary>"
>
> Information regarding who is normally providing the evidence (Infineon, item developer) and what is provided by Infineon.

1.2.1 Objective COTS-1 complexity assessment

"The applicant should assess the complexity of the COTS devices […]".

The complexity assessment of the COTS device is performed by the item developer. Based on the number of functions and interfaces, the AURIX™ TC3xx can be classified as complex.

1.2.2 Objective COTS-2 Electronic Component Management Process (ECMP)

"The applicant should ensure that an electronic component management process (ECMP) exists to address the selection, qualification, and configuration management of COTS devices. The ECMP should also address the access to component data such as the user manual, the Datasheet, Errata, Installation manual, and access to information on changes made by the component manufacturer. As part of the ECMP, for devices contributing to hardware DAL A or B functions, the process for selecting a complex COTS device should consider the maturity of the COTS device and, where risks are identified, they should be appropriately mitigated."

To show evidence of a complete and correct:

- selection of the COTS device: Infineon provides the Datasheet of the device, which describe the intended usage of the device and its specification. Infineon can also provide evidence via quality records and audits reports that the process for the design and manufacturing of the device is also suitable to the aviation industry
- Qualification of the COTS device: Infineon provides the Qualification Test Report (QTR) showing the compliance statement of the device to the qualification tests
- Configuration management: Infineon works according to an internal Change and Configuration Plan (CCMP) as required by the ISO 26262 [1] §8-7 (and §8-8 regarding the product change notification PCN) and IATF 16949 [4]
- Maturity level: Infineon provides an estimated number of hours of device usage in the field [e.g., >10 million hours in-service-experience (ISE)] by application (e.g., 90% ASIL D automotive application and 10% industrial applications)

1.2.3 Objective COTS-3 Using a Device outside Ranges of Values Specified in its Datasheet

"When the complex COTS device is used outside the limits of the device manufacturer's specification (such as the recommended operating limits), the applicant should establish the reliability and the technical suitability of the device in the intended application."

If the COTS device is used outside of the specification limits, it is the responsibility of the item developer to establish the reliability and technical suitability of the device in the intended application.

1.2.4 Objective COTS-4 Considerations when the COTS Device has Embedded Microcode

"If the microcode is not qualified by the device manufacturer or if it is modified by the applicant, the applicant should ensure that a means of compliance for this microcode integrated within the COTS device is proposed by the appropriate process and is commensurate with the usage of the COTS device."

The AURIX™ TC3xx does not have any embedded microcode. The firmware, which is qualified within the device (see §1.1), ensures the initialization and hands over to the applicant start-up code.

1.2.5 Objective COTS-5 COTS Device Malfunctions - Errata

"The applicant should assess the Errata of the COTS device that are relevant to the use of the device in the intended application and identify and verify the means of mitigation for those Errata. If the mitigation means is not implemented in hardware, the mitigation means should be fed back to and verified by the appropriate process."

Infineon provides the Errata sheet as part of the safety package documentation so that the item developer can assess the Errata of the COTS device. The Errata sheet [26] describes the identified functional or parametric deviations, their impact and their recommended work around. The Errata sheet is also representative of the in-service deviations reported from the field.

1.2.6 Objective COTS-6 COTS Device Malfunctions – failure modes

"The applicant should identify the failure modes of the used functions of the device and the possible associated common modes, and feed both of these back to the system safety assessment process."

For the identification of the failure modes of the used function of the device, and the possible associated common modes, Infineon can provide:

- The safety manual [31] describing in particular the assumptions to be validated at integration level, the management of faults, the available safety mechanisms to detect and react to failures, the recommended safety mechanisms to be implemented external to the device
- The FMEDA [29] including the failure mode description (hard and soft errors) and their effects, the associated failures rates, the associated detection means and detection rate (see details in §1.2.6.1)

- The conclusions of the Dependent Failure Analysis (DFA) treating the potential common cause failures (CCF). Dependent Failure Analysis (DFA) analysing how independence requirements could be defeated and showing evidence how mitigation measures can reduce the common cause failures (CCF) to an acceptable level. The DFA identifies and analyses the dependent failure initiators (DFIs), checks common causes, cascading failures or single events that could bypass or invalidate a required independence or freedom from interference between given elements. The results of the DFA are fed back in the FMEDA
- The application notes (e.g., Guidance against common cause failures in packages [27] or Hints related to safety mechanisms [28]) containing some recommendations how to integrate the device and for example, how pins should be connected to avoid common cause failures (CCF) within the package
- The safety case report [32] describing the safety requirements of the device, the safety process overview, the open problems reports and the arguments for their acceptance, and the declaration of conformance of the device and process with respect to ISO 26262 ASIL-D
- The Safety Analysis Summary Report [30] describing the performed safety analysis and the corresponding safety analysis results

1.2.6.1 More details on the AURIX™ TC3xx FMEDA

One of the main safety documents provided by Infineon is the FMEDA [29]. This document provides an exhaustive overview of the failure modes of the device and the safety mechanisms to detect and react to failures.

The FMEDA is provided as a highly configurable excel document:

- The package type can be selected to obtain the number of pins. The base failure rate for the package is distributed evenly among the number of pins in the FMEDA [29]
- In the component FMEDA [29] sheet, it can be stated which feature, function or module of the device are used and which are unused, which percentage of memory is used for the safety related program code or data, and which pin or port is used for the safety related peripherals. The results of the FMEDA [29] (failures rates and metrics) depends on these parameters
- In the Safety Mechanism sheet, it can be stated which safety mechanism is used / unused. These parameters impact the failure detection rate / diagnostic coverage and the metrics related to the detected and latent faults

Based on these input parameters, the FMEDA [29] provides as output the result overview in terms of failure rate for hard errors and soft errors, for single and dual faults, for detected and latent faults. It also provides the corresponding failure rate metrics: Probabilistic Metric for random Hardware Failure (PMHF), Single Point Fault Metric (SPFM) and Latent Fault Metric (LFM).

The failure rates are computed based on:

- a temperature and mission profile which is described in the FMEDA [29]
- the IEC TR 62380 [2] or SN29500 [3] reliability standards
- the applicable flux factor for the neutron and alpha particles

The figure below provides an overview of the FMEDA result sheet.

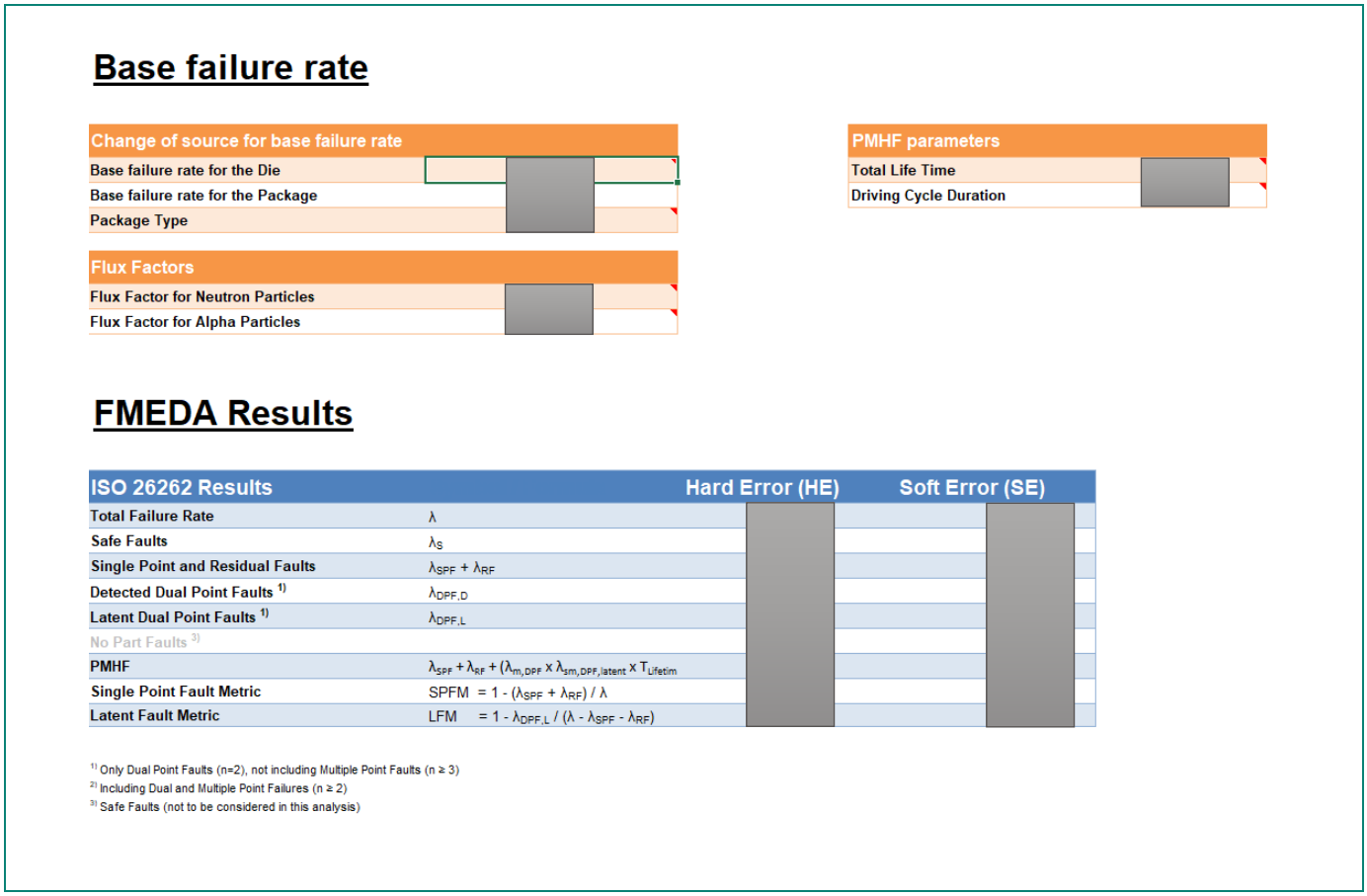

Figure 2 Example of AURIX™ TC3xx FMEDA results overview sheet

The soft error (SE) rates are computed based on the neutron and alpha particles flux according to the JEDEC standard JESD89B [19]. The flux of natural cosmic radiation depends on the location and altitude of operation. The soft error rate is extrapolated based on the flux factor corresponding at the expected conditions of operation (e.g. altitude, latitude). More details on soft errors are provided in §1.3.

In the end, this FMEDA helps the item developer to analyze the failures modes of the device and can provide accurate failure rates to be integrated at item level.

1.2.6.2 Link between the AURIX™ TC3xx FMEDA and potential FTA

According to the AMC 20-152A [7]/ AC20-152A [8] COTS-6 Objective, the failures modes of the device have to be fed back at the integration/item level into the system safety assessment process.

The following figure shows how the failure modes of the device or basic events of the FMEDA (single points and residual faults, detected multiple point faults, latent multiple point faults) might integrate into a typical fault tree established at item/system level. Two top events are chosen:

- an unavailability hazard: loss of the function or detected malfunction
- an un-integrity hazard: undetected malfunction

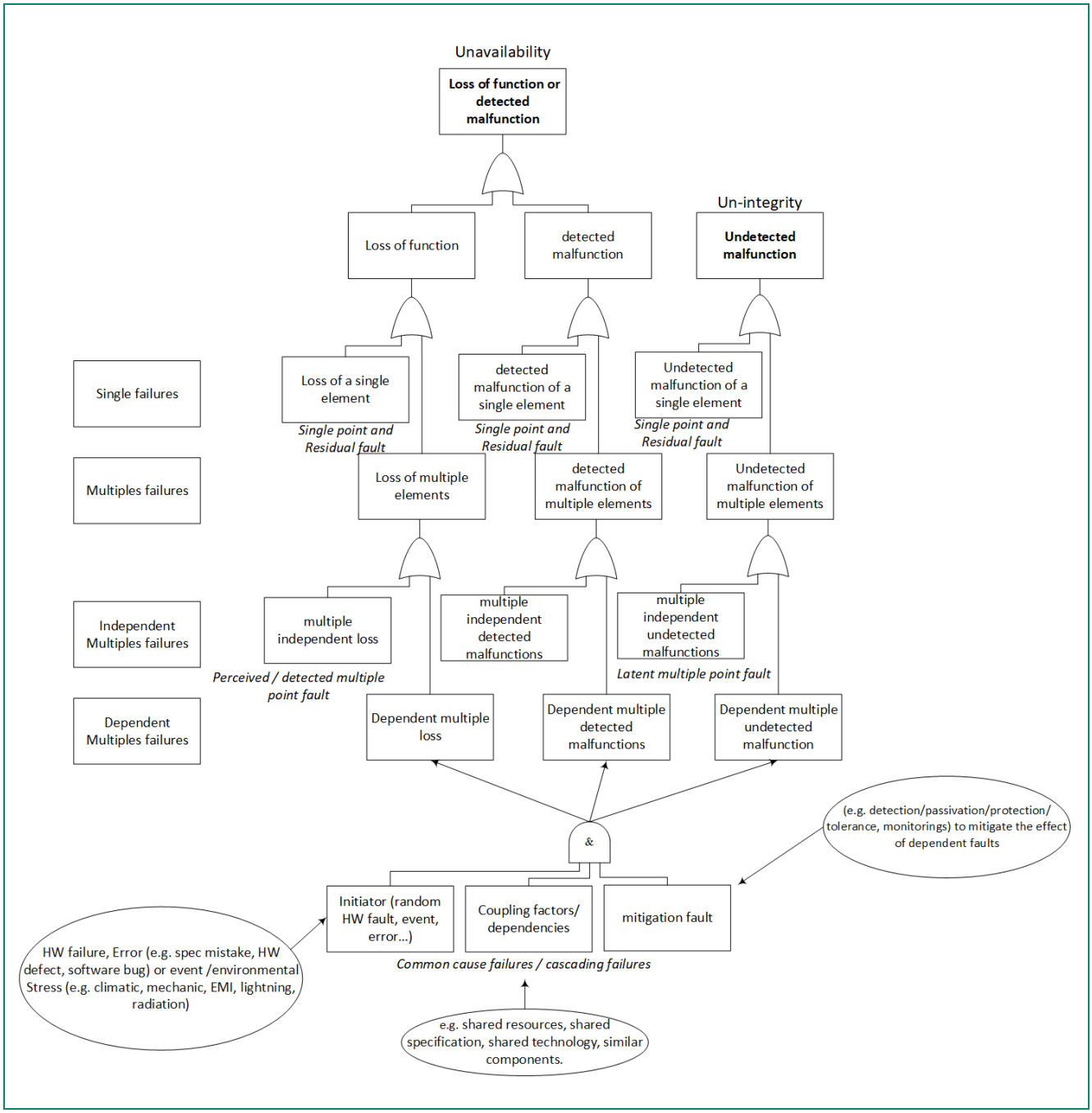

Figure 3 Illustration how basic events described in the FMEDA can be integrated within a fault tree

The figure above shows also how the common cause failures (CCF) or cascading failures belonging to the dependent multiple failures of the device (as described in the FMEDA) might also contribute to some basic events in the fault tree.

In the end, Infineon provides detailed data to support accurate analysis at item/functional level as expressed in the AMC 20-152 [7]/AC20-152A [8] objective COTS-6.

1.2.7 Objective COTS-7 Usage of COTS Devices

"The applicant should ensure that the usage of the COTS device has been defined and verified according to the intended function of the hardware. This also includes the hardware–software interface and the hardware to (other) hardware interface. When a COTS device is used in a hardware DAL A or B function, the applicant should show that unused functions of the COTS device do not compromise the integrity and availability of the COTS device's used functions."

Even if Infineon can provide the information about the usage of the COTS device (data sheet, user manual, safety manual), it is the mandatory that the item developer ensures verification of the intended functions on the target hardware (item).

In addition, Infineon can support with the evidence that the deactivation of functions in the COTS device does not compromise the integrity and availability of other used functions (see FMEDA and DFA) as it is mandatory for highly critical application (DAL-A or DAL-B).

1.2.8 Objective COTS-8 Inadvertent alteration of critical configuration settings

"If the complex COTS device contributes to DAL A or B functions, the applicant should develop and verify a means that ensures an appropriate mitigation is specified in the event of any inadvertent alteration of the 'critical configuration settings' of the COTS device."

Infineon can support with the evidence that the critical configuration settings of the COTS device (e.g. configuration of the boot code) is checked via a proper safety mechanism (e.g. CRC automatically monitored by the Firmware).

1.2.9 Conclusion

This white paper shows evidence that Infineon provides supporting evidence to the fulfilment of the objectives set by the AMC 20-152A [7]/ AC20-152A [8] related to COTS device. AURIX™ TC3 data is complete to allow the usage of AURIX™ TC3 as complex COTS device according to AMC 20-152A [7]/ AC20-152A [8].

1.3 Substantiation material to SEE analysis (EASA CM-AS-004)

The EASA CM-AS-004 [17] Issue 01 released by the EASA in 2018 deals with the certification considerations and analysis method to demonstrate the acceptability of Single Event Effect (SEE) caused by atmospheric radiation on aircraft and equipment. This Certification Memorandum (CM) does not introduce new certification requirements but provides guidance for compliance demonstration with current standard considering the impact of SEE on systems and equipment.

Note: no applicable Certification Memorandum for SEE at FAA available, but the following technical report should be taken into account at FAA; DOT/FAA/TC-15/62 “Single Event Effects Mitigation Techniques Report”

Single Event Effects (SEE) occur when atmospheric radiation, comprising high energy particles, collide with specific locations on semiconductor devices contained in aircraft systems. SEE can also occur when low energy neutrons interact with boron 10 isotope, which can also be present in semiconductors devices. Memory devices, microprocessors and FPGAs are most susceptible to SEE. High voltage (power) transistors and diodes may also be affected by SEE.

Some examples of these types of effects are Single Event Upset (SEU), Multiple Bit Upset (MBU), Single Event Latch-up (SEL), Single Event Functional Interrupt (SEFI), Single Event Gate Rupture (SEGR) and Single Event Burnout (SEB). SEU and MBU are two of the most frequent examples of SEE which affect aircraft systems.

The SEE rate is likely to be greater for aircraft system flying at hight altitude and high geographic latitudes (North and South).

The AURIX™ TC3xx device is, as other microcontrollers, susceptible to SEE (e.g., logic device, memory or other semiconductor devices). To support the SEE analysis performed by the item developer, Infineon can provide substantiation materials:

- The safety manual [31] describes the safety mechanisms which can mitigate the SEE (e.g., ECC/EDC functions, CRC engine, lockstep to detect transient faults inside a CPU core, logic and memory built-In Self Tests…)
- The FMEDA [29] provides the soft error rates of the device (see §1.2.6.1) depending on the relative neutron flux applicable to the aircraft and on the enabled safety mechanisms mitigating the SEE. The base soft error rate is determined by the evaluation of each memory technology when exposed to alpha and neutron particles according to the JEDEC standard JESD89B [19]

Thus, Infineon can provide substantiation material for the assessment of hardware susceptibility to SEE according to EASA CM-AS-004 [17].

2 Principle Safe Architecture for a DAL-A Computing Platform

2.1 General features of AURIX™ and PMIC

With its up to hexa-core high-performance architecture and its advanced features for connectivity, security and functional safety, the AURIX™ microcontroller TC3xx family is ideally suited for a wide field of industrial applications, e.g., for the aviation industry. The combination of performance and powerful safety architecture makes the microcontrollers ideal fit for domain control and data fusion applications. Infineon's OPTIREG PMIC products are the perfect companions for AURIX™ microcontrollers. The PMIC chipset has efficient, reliable, and safe voltage regulation, including pre- and post-regulator architectures, and DCDC-, linear, and tracking regulators. Besides power supply, additional monitoring and supervision functions enable reliable and easy design of the safety concept for electronic control units.

2.2 AURIX™'s safety mechanisms

The AURIX™ microcontroller provides many functions and safety mechanisms, which can improve the diagnostics of the computing platform and can be an advantage compared to classic designs/implementations (like a MCU with a FPGA). Following aspects can be considered regarding this advantage:

- Some of the AURIX™ safety mechanisms support the architecture definition of the equipment (e.g., lockstep core or diverse redundancy on ADC acquisitions)
- Some of the AURIX™ functions or safety mechanisms can replace specific item developer's implementations of a function in HW or SW (e.g., usage of AURIX™'s Flexible CRC Engine vs dedicated CRC functionality implemented in SW)
- If the safety mechanisms replace specific item developer's SW implementations, the CPU load is reduced during SW execution

The following is a list of the most interesting AURIX™'s functions and safety mechanisms for aerospace applications, which contribute to improve the failure detection capabilities:

- **Internal Built-In Self Tests:** these have to be enabled as a pre-requisite to use and rely on the other safety mechanisms:
  - Power BIST
  - Logic BIST
  - Memory BIST
  - Monitor BIST
- **Safe computation** (see sections 4.3.1 and 4.3.2.1 of safety manual [31]**):**
  - Lockstep (covered later in section 2.2.1)
  - HW means for protection on memory and resource accesses; see some examples below:
    - ECC/EDC functions
    - NVM integrity checks
    - Flexible CRC Engine
    - Signal Processing Unit which performs FFTs safely with its safety mechanisms (e.g., a second SPU instance can be configured for full redundancy to compare control and data outputs)
- **Analog acquisitions** (see sections 4.3.1 and 4.3.2.4 of safety manual [31], see also tutorial for analog acquisition[23]:
  - Diverse redundancy on ADC acquisitions (AURIX™ provides independent redundant modules with two diverse measuring principles: Delta-Sigma conversion and Successive Approximation Register)

- **Digital acquisitions** (see sections 4.3.1 and 4.3.2.6 of safety manual [31] , see also tutorial for digital acquisition [22]):
    - independent and diverse modules that can be used to check the acquired digital input signals within the Generic Timer Module (GTM)
        - Timer Input Module (TIM)
        - Capture/Compare Unit 6 (CCU6)
        - General Purpose Timer Unit (GPT12)
- **Digital actuation** (see sections 4.3.1 and 4.3.2.7 of safety manual [31], see also tutorial for digital actuation [21]):
    - independent and diverse modules that can be used to check the digital output command signals (via loopback lines to the microcontroller) within the Generic Timer Module (GTM)
        - Timer Output Module (TOM) and Timer Input Module (TIM)
        - Capture/Compare Unit 6 (CCU6), which supports the generation of three-phase PWM with six outputs
        - General Purpose Timer Unit (GPT12)
- **Avoidance/detection of common cause failures** (see sections 4.3.1 and 4.3.3.1 of safety manual [31]**):**
    - Internal voltage monitoring performed by the AURIX™ Power Management System (PMS) (can be used also in combination with an external and independent voltage monitoring provided by the OPTIREG PMIC)
    - Internal Watchdog (used in combination with an external and independent Watchdog, e.g., provided by the OPTIREG PMIC)
    - Loopback function for General Purpose I/O ports and Peripheral I/O Lines
- **Safety Management Unit** (see section 4.2.12.1 of safety manual [31] **):** SMU is used to configure the reaction upon detection of internal failure and reports this information to an external device (e.g., OPTIREG PMIC) to trigger the reaction at equipment level

2.2.1 TriCore Lockstep in AURIX™ TC3xx

Lockstep is a HW redundancy method that mitigates the impact of Single Event Effect (SEE) by detecting errors caused by radiation-induced bit flips. This method works as follows: two independent and identical CPUs, one called Master CPU Core and another one called CPU Checker CORE, are operated in a lockstep manner. The primary inputs and inputs coming from the CPU memories, connected to the Master CPU CORE, are delayed by two clock cycles and connected to the CPU Checker CORE. The Outputs of the Master CPU CORE are then delayed by 2 clock cycles before being compared in hardware with the outputs of the CPU Checker CORE. The comparison is done on a cycle-by-cycle basis. Upon detecting a comparison failure, an alarm (sx_alarm_*) is sent to the SMU [Safety and Security Management Unit] (see figure below).

Additional measures, like layout separation, are implemented to mitigate common cause failures (e.g., any transient faults, due to an alpha particle hitting any of the cores for example, would not affect the other core). In addition, the layout creates a diverse implementation by inverting the Flip-Flop logic. Furthermore, a self-checking error injection mechanism is implemented in hardware to cover failures in the lockstep comparator.

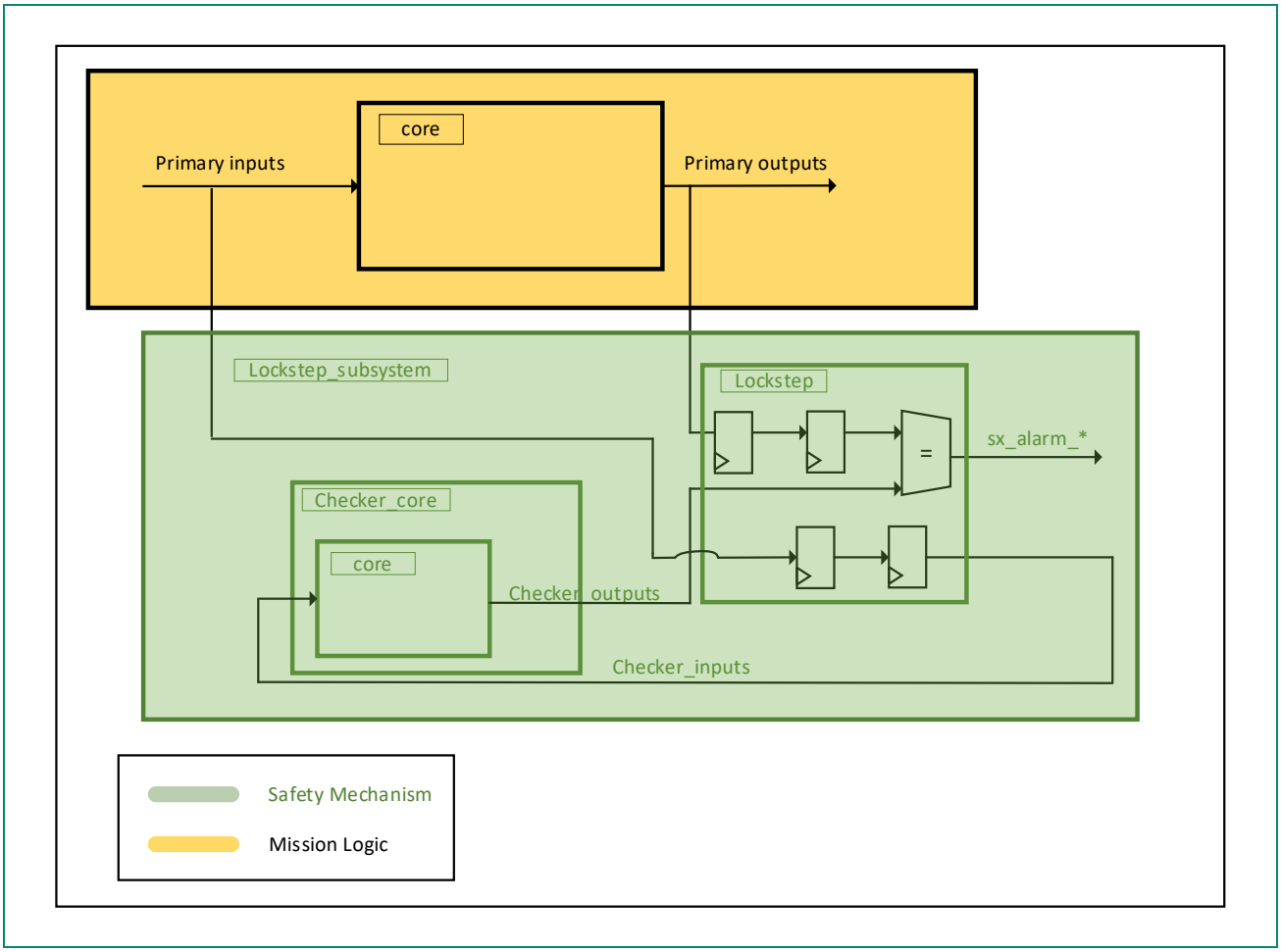

Figure 4 HW redundancy is provided to detect faults inside TriCore CPU (source: Infineon)

In conclusion, the redundancy along with a diverse implementation (with a temporal and physical separation) of the lockstep as safety mechanism, contribute further to improve the failure diagnostic coverage of the microcontroller.

2.3 Additional monitoring means with OPTIREG PMIC

Besides the usage of the AURIX™ internal safety mechanisms, as stated before, there are additional advantages if AURIX™ is used together with OPTIREG PMIC:

- Independent external Watchdog
- Independent external monitoring of AURIX™ supply voltages to provide overvoltage/undervoltage protection (instead of an implementation of this function with additional HW circuitry)
- Independent external reset function for the AURIX™

OPTIREG PMIC has, additionally, the following advantages:

- It avoids single point fault propagation to its output pins connected to the AURIX™
- It provides independent voltage outputs for different devices (not only for the AURIX™)
- It gets the information from the AURIX™'s Safety Management Unit and can configure the reactions at equipment level
- It offers self-test functions which can be initiated by application software

The following figure shows as an example how AURIX™ can be connected to the PMIC:

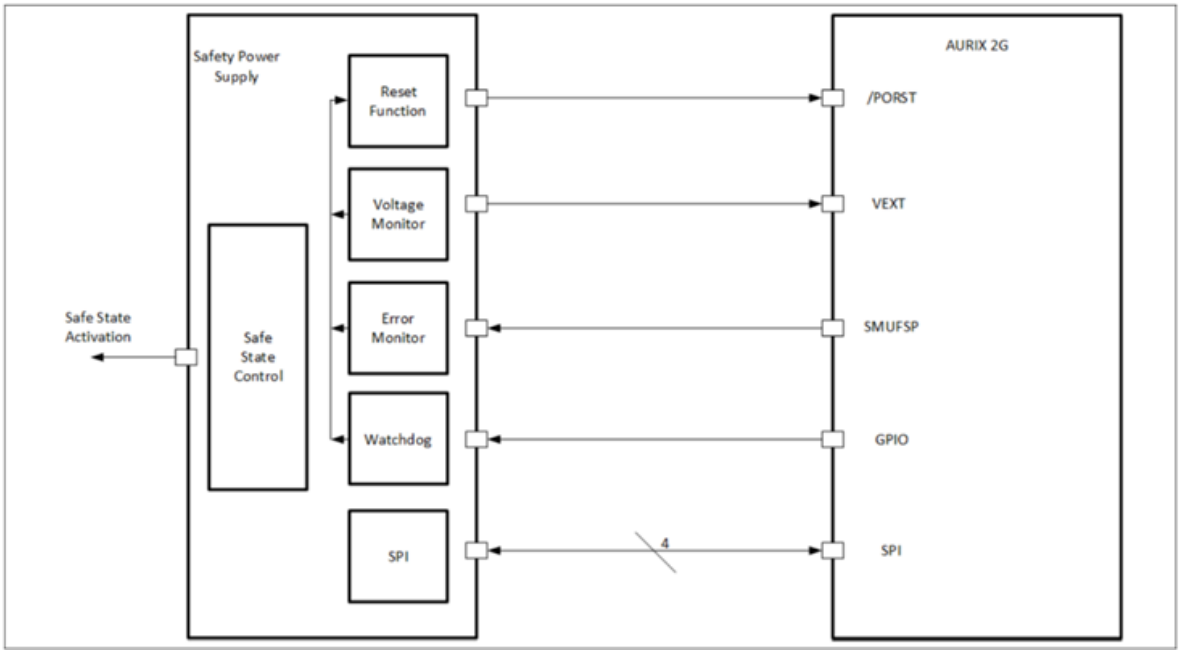

Figure 5 Signals used to connect the MCU with an external IC (source: Infineon)

2.4 Conclusion

AURIX™ provides several monitoring means and safety mechanisms which contribute to:

- increase the failure diagnostic coverage of the microcontroller and
- limit additional item developer's proprietary solutions

Furthermore, if AURIX™ is used together with OPTIREG PMIC, this unit can provide functional independent monitoring means (e.g., external Watchdog, voltage monitoring, etc.) which:

- simplifies the architecture of the electronic equipment and
- contributes to avoid common cause failures when only the microcontroller is used

3 AURIX™ in Multicore Application

3.1 Using the Multi-Core Features of AURIX™ within Aerospace

This section shows a sample architecture how the multi-core features of the AURIX™ TC39x family can be used in the Aerospace context. The example demonstrates a typical use case that two software items are hosted on the same microcontroller to reduce costs and weight:

- A control software, developed according EUROCAE ED-12C [13] / RTCA DO178C [14] DAL A
- A related health monitoring software, developed according EUROCAE ED-12C [13] / RTCA DO178C [14] DAL C

AURIX™ provides several features to minimize interference.

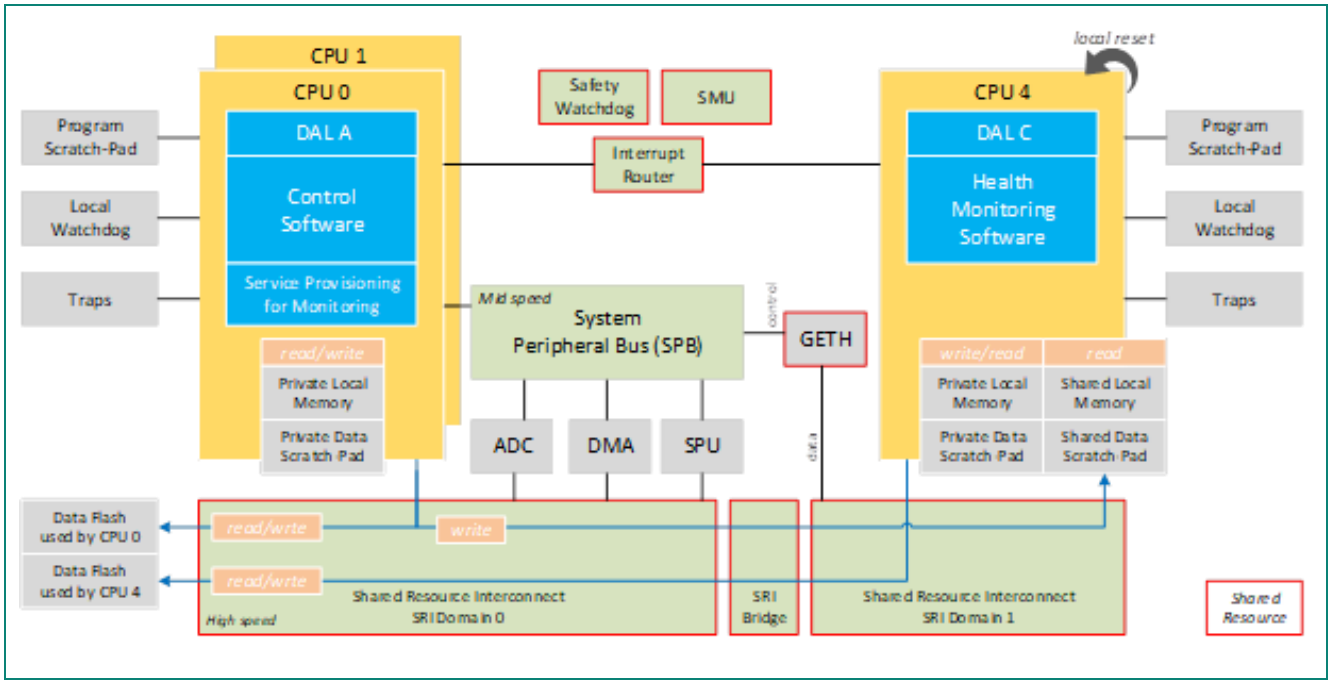

Figure 6 Example architecture based on AURIX™ TC39x

The following architectural decisions have been made for the example architecture:

- The multi-core architecture is used to separate the two software items: the control software is allocated to CPUs 0 and 1, the health monitoring software to CPU 4
- The AURIX™ features of splitting the high-speed bus traffic into two domains (SRI domain 0 and domain 1) are used
- The peripherals are controlled by CPU 0, supported by a service provisioning software component that provides peripheral data to the health monitoring software through shared memory
- The CPUs can exchange data through three types of shared memory: local memory, data scratch-pad and NVM. The data is restricted to flow only from the DAL A item towards the DAL C item to prevent that the health monitoring software can negatively impact the operation of the control software
- The Ethernet data traffic is only exposed to the CPU 4
- The CPU 4 can perform a local reset in case of a severe error within the health monitoring software without impacting the operation of the control software. The opposite direction is not foreseen, as a failure of CPUs 0/1 impact the service provisioning software, which is required for the normal operation of the health monitoring

3.2 Compliance to AMC20-193/ AC20-193

The EASA document AMC20-193 [9]/ AC20-193 [10] “Use of multi-core processors” lists objectives to support the demonstration of compliance with the applicable airworthiness regulations in case of using multi-core processors.

Some of these objectives need to be answered in combination with the selected operating system. The following objectives typically can be answered by relying on the AURIX™ safety manual and the AURIX™ user manual – based on the project-specific usage of the multi-core processor: MCP_Planning_2.1, MCP_Planning_2.2, MCP_Resource_Usage_1, MCP_Resource_Usage_3, MC_Resource_Usage_4, MCP_Planning_2.4, MCP_Error_Handling_1.

The following sections show how the AURIX™ TC39x device supports the coverage of these objectives regarding the guideline document AMC20-193 [9]/ AC20-193 [10].

3.2.1 Minimizing Interference

Interference in the context of multi-core processing is regarded as an impact on the behaviour of a core triggered by actions of other components (another core or HW units like DMA with their own processing capabilities). AURIX™ provides features to reduce interference and to mitigate the impact of a potential interference.

The following channels can be subject to interference:

- **Memory**: Each CPU has its own local program memory, data memory. Accessing shared memory is controlled by partitioning the memory into areas via the memory protection unit MPU such that each area has exactly one CPU as a unique owner (write access)
- **Cached memory**: By the AURIX™ HW design, the cache is local to each CPU. It is recommended to configure the MPU such that the other CPUs can't write the underlying memory areas (in other words: in case a CPU writes the memory of another CPU, this other CPU should read this data without using its locally cached data)
- **SRI Domains**: An interference can occur within one of the SRI domains. AURIX™ provides on HW level the separation into multiple SRI domains and various arbitration mechanisms. The communication paths and communication patterns between SRI masters and SRI slaves are configurable
- **Serial Peripheral Bus (SPB/FPI) and shared peripherals**: Interference could occur on the SPB bus or when using a shared peripheral attached to the SPB. A typical approach is to nominate (and configure) one CPU as the only owner of the SPB bus (in the example architecture done for GETH). Alternatively, the arbitration mechanisms of AURIX™ provided for SPB can be used (e.g., priorities between SPB masters, round robin groups, starvation prevention)
- **Clock:** The clock is typically configured only once during start-up and then locked to prevent that a CPU impacts the timing behaviour of other CPUs by reprogramming the clock
- **DMA:** In case parallel DMA activities are required, AURIX™ supports an arbitration within the DMA and parallel operation of move engines
- **Interrupts/traps/watchdog:** Each CPU has its own interrupt control unit, trap system and CPU watchdog. The interrupts and traps should be configured such that an interrupt/trap caused by CPU is processed by the same CPU

3.2.2 Monitoring and Debug Capabilities

As part of covering the objectives of AMC 20-193 [9]/ AC20-193 [10] it is necessary to demonstrate that failures occurring within the processor are properly detected and handled in a fail-safe manner as described in section §1.2.6.

A detected error or suspect behaviour can be configured to be reported to the Safety Management Unit (SMU), which itself can create interrupts.

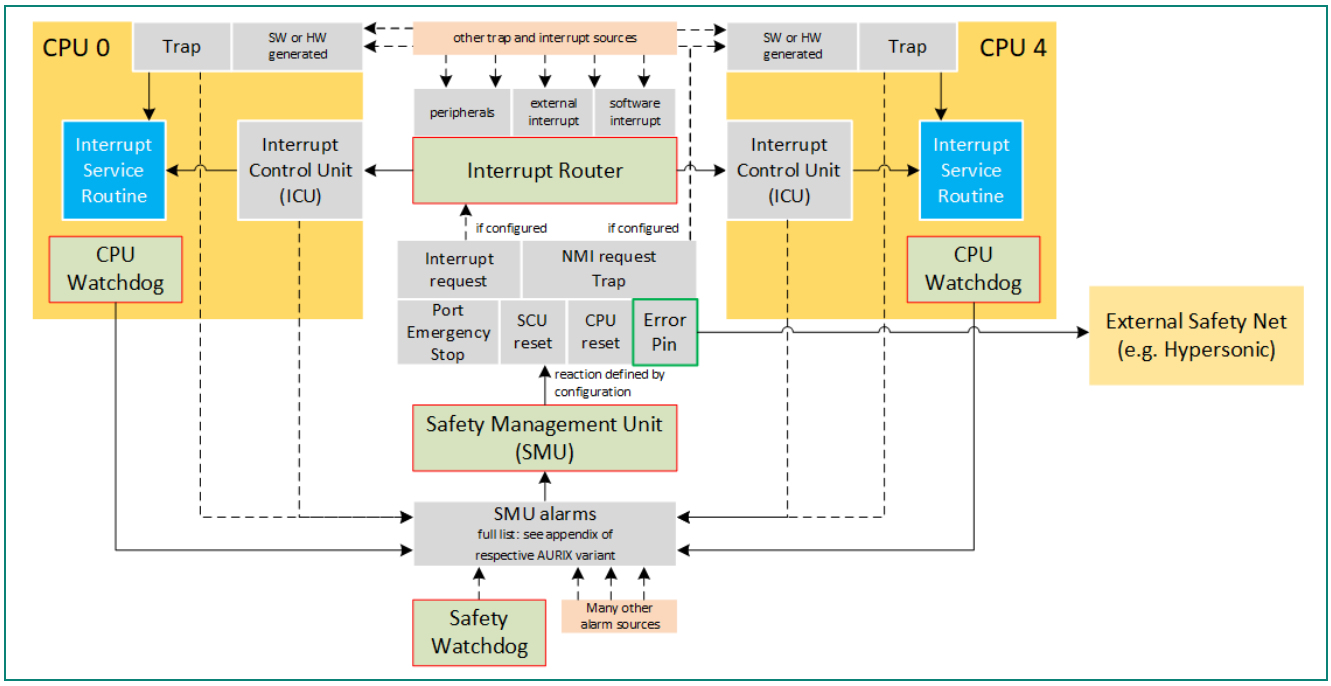

Figure 7 Error propagation

The AURIX™ architecture decouples the operation of the SMU from the operation of the CPUs in case of a proper configuration, e. g., following the pattern that a SMU alarm caused by a CPU leads to a SMU action only impacting the same CPU.

A complete failure (impacting all CPUs) should be propagated through the Error Pin to the surrounding safety net.

Additionally, the AURIX™ debug interface allows to monitor the traffic on the SRI and SPB busses during development time, e. g., to provide evidence that the master/client communication is restricted by hardware means as intended.

The AURIX™ processor family allows to use a multi-core architecture in the Aerospace context. The Infineon documentation provides the respective inputs to demonstrate that the objectives of AMC20-193 [9] can be covered after applying a proper configuration of the AURIX™ and integrating it with an embedded operating system.

4 Conclusion

Within the paper it is demonstrated that Infineon AURIX™ TC3xx microcontroller, which is developed for ASIL-D safety needs according to the ISO 26262 [1], also fits to aerospace certification requirements.

The paper shows that the implemented design standard at Infineon brings added value to aerospace product developer and safety teams since detailed design and analysis documentation is available which allows the aerospace developing team to optimize the own product designs.

Compliance was demonstrated to all relevant AMC20-152A [7]/ AC20-152 COTS [8] objectives where certification statements from product owner rely on component manufacturer. It is concluded that Infineon offers all mandatory data which is requested for complex COTS components in aerospace.

Since the AURIX™ TC3xx microcontroller needs to set automotive controllers in case of internal failures into a fail-safe condition, this offers additional opportunities for aerospace use cases. The increased amount of microcontroller safety features provides a higher microcontroller failure detection rate, which improves the safety figures for aerospace applications. In addition, the proposal to use the AURIX™ TC3xx in combination with an external device like an Infineon PMIC offers a smart and effective solution to mitigate microcontroller dormant failures and helps to achieve external monitoring functions to allow a deactivation of the current lane in control as a use case for fail safe condition.

Finally, an outlook on the AMC20-193 [9]/ AC20-193 [10] (usage of Microcontrollers in multi core conditions) objectives was given, which can be supported by dedicated Infineon inputs in case a multi core certification is planned.

As discussed within this paper, ISO 26262 [1] components offer all relevant information which is also needed in aerospace industry to certify safety critical products including complex COTS components. Infineon offers the necessary set of data which is expected from a component manufacturer and provides further documentation to support effective and optimized safety features for all necessary Design Assurance Levels in aerospace products.

5 Glossary

Abbreviation	Meaning
AEH	Airborne Electronic Hardware
AMC	Acceptable Means of Compliance
ARP	Aerospace Recommended Practice
ASIC	Application Specific Integrated Circuit
ASIL	Automotive Safety Integrity Level
AURIX™	Automotive Realtime Integrated Next Generation Architecture
COTS	Commercial-Off-The-Shelf
CBIT	Continuous Build-in Test
CCF	Common Cause Failure
CCMP	Change and Configuration Plan
CFMEA	Concept Failure mode and Effect Analysis
CFTA	Concept Failure mode and Effect Analysis
CM	Certification Memoranda
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSCI	Computer Software Configuration Item
DAL	Development Assurance Level
DFA	Dependent Failure Analysis
DFMEA	Design Failure Mode and Effects Analysis
EASA	European Union Aviation Safety Agency
ECC	Error Correction Code
ECMP	Electronic Component Management Process
EDC	Error Detection Code
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEDA	Failure Mode Effect and Diagnostic Analysis
FMEA	Failure Mode Effect Analysis

FPGA	Field Programmable Gate Array
FPI	Flexible Peripheral Interconnect
FTA	Fault Tree Analysis
FW	FirmWare
GETH	Gigabit Ethernet
HW	HardWare
IATF	International Automotive Task Force
IEC	International Electrotechnical Commission
IP	Intellectual Property
ISE	In-Service-Experience
ISO	International Organization for Standardization
JEDEC	Joint Electron Device Engineering Council
JESD	JEDEC Standard
LFM	Latent Faults Metric
MBU	Multiple Bit Upset
MCP	Multi-Core Processor
MCU	MicroController Unit
NSER	Neutron Soft Error Rates
NVM	Non-Volatile Memory
PBIT	Power-up Build-in Test
PCN	Product Change Notification
PLD	Programmable Logic Device
PMHF	Probabilistic Metric for random Hardware Failure
PMIC	Power Management Integrated Circuit
PSSA	Preliminary System Safety Assessment
QTR	Qualification Test Report
RHF	Random Hardware Faults
RTL	Register Transfer Language
SAE	Society of Automotive Engineers
SEB	Single Event Burnout

SEE	Single Event Effect
SEFI	Single Event Functional Interrupt
SEGR	Single Event Gate Rupture
SEL	Single Event Latch-up
SEooC	Safety Element out of Context
SEU	Single Event Upset
SMU	Safety Management Unit
SPB	System Peripheral Bus
SPFM	Single Point Faults Metric
SRAM	Static Random Access Memory
SRI	Shared Resource Interconnect
SSA	System Safety Assessment
SSPC	Solid-State Power Controller
SW	SoftWare
TLSR	Top Level Safety Requirement
TSR	Technical Safety Requirement

6 Guidelines for Access to “MyICP”

What is MyICP?

MyICP or **My Infineon Collaboration Platform** is a portal through which you can access all the documentation related to Infineon microcontrollers.

While you may find plenty of details about Infineon microcontrollers on our official website, there are some **confidential** documents that require a Non-Disclosure Agreement (NDA). These can be accessed through MyICP. The access link is:

https://www.infineon.com/cms/en/product/promopages/MyICP-platform-for-Microcontroller

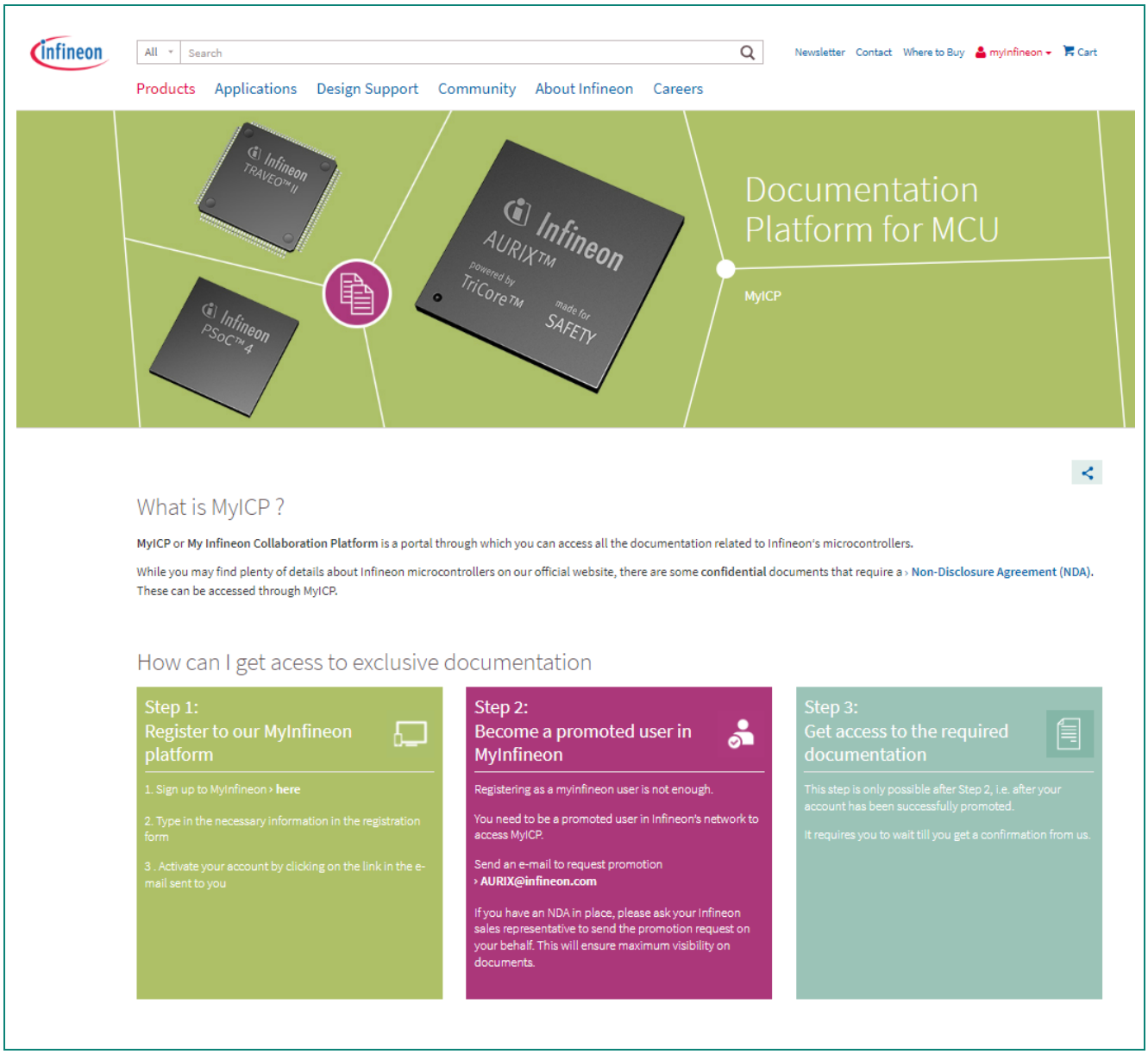

Figure 8 Overview of MyICP platform

References

[1] ISO 26262:2018 Road vehicles — Functional safety
[2] IEC TR 62380 Reliability data handbook
[3] Reliability Prediction Standards - SN29500
[4] IATF 16949 Automotive Quality Management System
[5] EUROCAE ED-135 Safety assessment process – EASA
[6] SAE ARP4761A Safety assessment process - FAA
[7] AMC20-152A Development Assurance for Airborne Electronic Hardware (AEH) – EASA
[8] AC20-152A Development Assurance for Airborne Electronic Hardware (AEH) – FAA
[9] AMC20-193 Use of multi-core processor – EASA
[10] AC20-193 Use of multi-core processor –FAA
[11] EUROCAE ED-79B Guidelines for Development of Civil Aircraft and Systems – EASA
[12] SAE ARP4754B Guidelines for Development of Civil Aircraft and Systems – FAA
[13] EUROCAE ED-12C Software development – EASA
[14] RTCA DO178C Software development – FAA
[15] EUROCAE ED-80 Electronic hardware development – EASA
[16] RTCA DO254 Electronic hardware development – FAA
[17] EASA CM-AS-004 Issue 01 “Single Event Effects (SEE) Caused by Atmospheric Radiation”- EASA
[18] DOT/FAA/TC-15/62 “Single Event Effects Mitigation Techniques Report” – FAA
[19] JEDEC JESD89B Measurement and reporting of alpha particle and terrestrial cosmic ray induced soft errors in semiconductor devices
[20] Tutorial sensor acquisition (application note: AP32517)
[21] Tutorial digital actuation (application note: AP32515)
[22] Tutorial digital acquisition (application note: AP32514)
[23] Tutorial analog acquisition (application note: AP32512)

Note: [20] to [23] are IFX documents, available under “myicp” (see chapter 6)

Safety package documentation

The safety package is specific for each AURIX™ TC3xx variant and it is composed of the same type of documents, as listed below for AURIX™ TC39x:

[24] AURIX™ TC3xx IFX User manual
[25] AURIX™ TC39x Data sheet
[26] AURIX™ TC39x Errata sheet
[27] Guidance against common cause failures in packages (application note: AP32405)
[28] Hints related to safety mechanisms (application note: AP32535)
[29] AURIX™ TC39x FMEDA
[30] AURIX™ TC3xx Safety analysis summary report
[31] AURIX™ TC3xx Safety manual
[32] AURIX™ TC39x Safety case report

Note_1: this paper is based on Safety package version 1.6.

Note_2: the safety package is only available for customers under NDA.

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

© 2024 Infineon Technologies AG.
All rights reserved.

Public

Version: V1.0_EN
Date: 07/2024

Stay connected!

Scan QR code and explore offering
www.infineon.com/aurix

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com/aurix).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.