Technical White Paper

Benefits of Using Functional Safety in Space Applications

ABSTRACT

Originally published in the Journal of Space Safety Engineering (volume 12, issue 1)

According to IEC61508, functional safety is relevant whenever a product or system contains electrical, electronic or programmable electronic elements that perform safety-critical functions. It is used in many areas of technology such as, the process (for example, energy sector), automotive (transport sector), mechanical engineering and aviation industries. This article compares the approaches and concepts of functional safety based on IEC61508 and ISO26262 with the RAMS (reliability, availability, maintainability and safety) approaches of the space industry, in particular with the fault detection isolation and recovery (FDIR) approach.

The paper provides insights into the possibilities of minimizing risk at the component level, especially for complex integrated circuits (IC). Traditionally, the space industry has focused on qualifying the components used for the extreme environmental parameters and the typically very long duration of use in space. However, as ICs have become very complex, there is significantly increased risk of systematic failures that can occur during the development of the component itself and also by the designer using it for development of the actual circuit board assembly.

In addition, the cost of components is a major factor in the development of satellite constellations due to higher volumes, so a trade-off between qualification and affordability must be found.

This white paper discusses how systematic faults in other market sectors can be reduced and how “random faults” can be detected as quickly as possible and their effects ideally eliminated or at least minimized with the help of appropriate performance features of semiconductors, such as error correction code (ECC), lock-step, or built-in self-test (BIST).

This paper is intended as a suggestion on how to make the best use of existing features of semiconductors developed for functional safety in other market sectors for space applications.

Table of Contents

List of Figures

Trademarks

All trademarks are the property of their respective owners.

1 Introduction

Private investments into space flight kicked off the age of the so-called “New Space.” However, the term “New Space” goes well beyond the rise of private companies and their interest in an optimized return of investment; it represents a paradigm shift in how space products are developed. [1] This shift is driven not only by the private sector but also, to varying degrees, by national agencies, which are actively contributing to this transformation.

Designers and design managers are challenged to manage the risks of growing system level complexity. Accordingly, it is more important than ever to minimize faults by employing various methodologies, such as established verification and validation processes. This also requires minimizing faults from the very beginning of the project, with systems architects, systems engineers, software, hardware designers and product assurance engineers working hand in hand. Additionally, this involves avoiding faults in development tools, such as coding compilers, electronic design software, and RAMS tools.

Commercialization drives the space sector towards a balance between cost, performance, time, and risk. Together, these four factors will dominate the highly competitive industrial markets of the future, and no one can afford to focus on just one of them and still expect to be successful. These four factors must be monitored by a robust management system based on ISO 9001 or other relevant management standards. [2]

Top down it means on the engineering level an acceleration of development cycles in design, manufacturing, test and deployment. With a specified solution-oriented focus on the main aspects. Costly overengineering must be avoided to optimize the return of invest. This effect can be reached, for example by modular designs that reuse qualified parts and electronic components as much as possible. A lot of push for New Space comes from the communication industry, which demands volume production of satellites in support of super-constellations. [3]

As Starlink has already sent hundreds of satellites into space, the mass production of satellites represents one of the biggest shifts for the space industry, as most of the existing space-standards were designed for custom-made systems.

Because of that, it is worth looking at other industries that are oriented towards mass production and high reliability requirements, like automotive industries.

2 Space Benefits From Other Industry Segments and Overview

Space and automotive industries share similarities, but certain attributes differ completely from an established perspective. For example, space systems are characterized by the high complexity of their systems. This is due to the fact that products like satellites are physically inaccessible in space, requiring engineers to predict and mitigate risks posed by the extreme alien environment, such as vacuum, temperature cycles, microgravity, and long mission durations. This attribute, combined with the fact that a lot of space missions are driven by scientific questions, inherently leads to scientific progress and pushes the boundaries of technology. For most missions, a tailored ground-up design is necessary, which is robust and reliable. Product safety is crucial because there is no possibility for repair or maintenance of the hardware. This is especially important for crewed missions, making product safety a challenge for engineers.

In contrary to space, the innovation attributes beyond high reliability and safety that describe the automotive sector are high cost pressure and optimization for highly efficient mass production. With this background, engineers focus on re-use and modularity. Highly integrated semiconductor components enable significant cost advantages.

Product safety and high reliability is equally important to the space and the automotive industry. However, the reasoning behind is somewhat different to either one.

2.1 Product Safety Motivation Automotive

The primary motivation is, of course, the need for robust (reliable) technology for safety functions, similar to space, to protect people in hazardous situations in daily traffic, such as brakes or airbags, which can save lives in critical situations combined with the requirements of the public law. The second motivation is more of economic nature: Expensive product recalls pose a significant business risk for the automotive industry and can even lead to a shutdown of the company. The automotive industry addresses all aspects of functional safety with its dedicated standard ISO26262 based on the foundation standard IEC61508.

2.2 Product Safety Motivation Space

Given the high stakes involved in space missions, especially those with human crews, RAMS activities are essential to ensure the survival of astronauts. However, it is important to recognize that not all missions are crewed, yet the imperative for product safety—or more accurately, Product Assurance—remains paramount. This necessity stems from the fact that space exploration is a global endeavor, governed by international standards and requirements designed to prevent catastrophic failures that could have severe political repercussions.

The enormous financial and temporal investments in space activities reinforce the importance of robust product assurance practices. Moreover, with the growing concern over space debris and the sustainability of space environments, the need for comprehensive safety measures is more pressing now than ever.

New Space increasingly adopts attributes from the automotive industry, such as mass production, cost optimization, and others that have already been discussed, summarized in Figure 2-1.

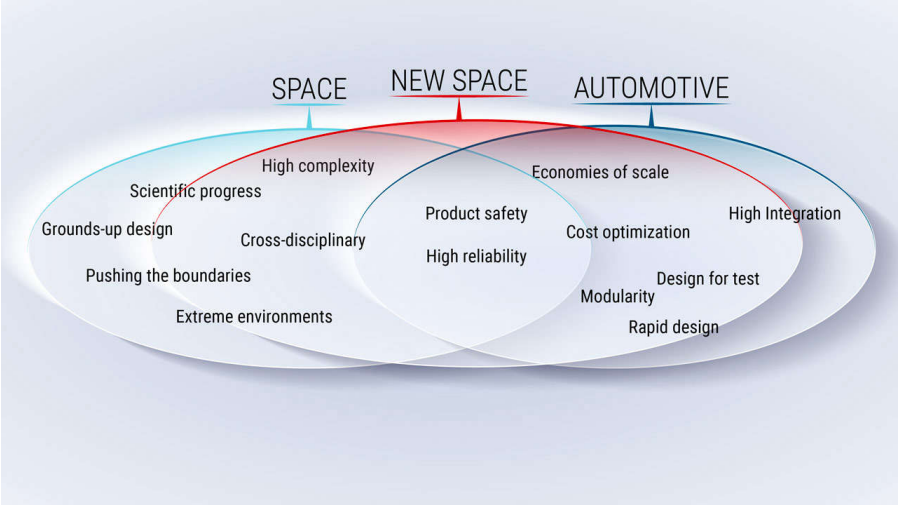

Figure 2-1. Attributes Space and Automotive

The foundational standard, IEC61508 [4], represents the base standard for most industry sectors. The space sector, however, does not follow the approach of IEC61508. This also implies that industries such as aviation, the process industry, automotive, and mechanical engineering follow the same methodology, as you can see in Figure 2-2. However, each industry also has its own specific sector standards in its respective language, along with detailed approaches and examples that are tailored to their particular needs. Space takes a rather universal approach and process for handling and managing functional safety for the systems.

The capability is characterized by the Safety Integrity Level (SIL) from 1 to 4 in ISO61508; in aviation, it is called the Design Assurance Level (DAL) and in the automotive industry it is called ASIL according to ISO26262 [5].

Figure 2-2. Different Sectors, Different Standards

In the space industry, which is not based on IEC61508, it is referred to as standards in the field of reliability, availability, maintainability, and safety (RAMS), a term that encompasses all these aspects and defining quality and reliability requirements [9]. A special roll leads the fault detection isolation and recovery (FDIR) [7], which is a concept, that can isolate and recover systems in case of detected anomalies. This concept goes beyond requirements of functional safety which only demands for reaching the safe state.

3 Commonalities of RAMS and IEC61508 Functional Safety

Functional safety and RAMS share the same objective of “freedom from unacceptable risk,” as shown in Figure 3-1, where both define risk as the product of severity of the damage times the probability of occurrence of this damage.

Figure 3-1. Freedom From Unacceptable Risk

The IEC61508 functional safety standard specifically addresses safety throughout the lifecycle of electrical, electronic, or programmable systems that are integrated into a safety instrumented system (SIS) in products to perform a safety function, which must be reliably defined and contains a sensor, Logic and actor and if it is necessary in a redundant architecture (channel).

The functional safety standard outlines a specific process and includes tools and methods for its implementation.

The acronym RAMS define all aspects about [8]:

- Reliability: Ability to perform a specific function; may be given as design reliability or operational reliability Availability: Ability to keep a functioning state in the given environment.
- Maintainability: Ability to be maintained (servicing, inspection and check, repair and/or modification) in an easy and timely manner.
- Safety: Ability to prevent harm to people, the environment and assets during a complete life cycle.

RAMS covers not only the electronic safety functions but also comprehensively addresses all quality requirements of the system, in contrast to functional safety. It also includes aspects of the material and mechanics, as well as how maintenance can be performed and how functions can be made available at specific times and intervals. All these capabilities contribute to a reliable, available, maintainable, and safe performance. While reliability, availability, and maintenance are not exclusively safety functions, they are crucial for operations.

Functional safety primarily refers to safety functions but the programmable electronic can also be applied to basic operational functions with RAMS- attributes.

Functional Safety and RAMS both have common, that they differ between:

- Random failures
- Systematic failures

3.1 Random Failures

Random failures occur in hardware components, such as resistor short circuits or transistor gate ruptures. These failures are essentially unavoidable and can occur unpredictably at any time, though their likelihood can be estimated using mathematical probability. Once detected, these failures cannot be reversed, as they result in total and irreversible damage to the affected components.

Therefore, it is crucial to manage these risks proactively, often by employing redundancy to mitigate their impact. The applicable hardware reliability can be predicted by statistically modeling it with reasonable accuracy:

- ʎ-rate [9]: Failure Rate is the limit, if it is existing of the conditional probability that the failure occurs within time interval (t, t+δt)], to δt when δtà0, when, given that the item was new at t=0 and did not fail in the interval (0,t]
- FIT [9]: failures in time or failure per 10^9 h. The FIT-rate is very commonly used by the semiconductor industry
- PFH [10]: Average probability of a dangerous failure per hour
- PFD [10]: Average probability of a dangerous failure on demand
- MTTF [9]: MTTF= $(t_1+….+t_n)/n)$ where $t_1…t_n$ are failure free times of statistically identical item

In summary, random failures refer to a quantitative approach and are exclusively related to hardware components—software cannot show random failures. The principle bath tube curve in shows the three phases [9]:

- Phase 1, early failures: for example, weaknesses in the materials, components, or production process.
- Phase 2, failures with constant (or nearly constant) failure rate: Failures in this period are Poisson-distributed and often occur suddenly.
- Phase 3, wear-out failure rates: Failures in this phase are attributable to aging, wear-out, fatigue, and so forth.

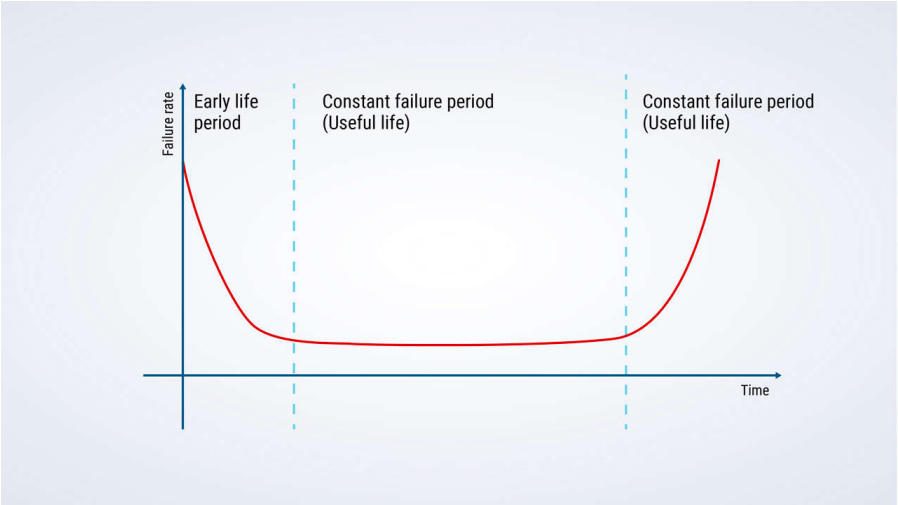

Figure 3-2. Random Failure Rate for a Simple Device-Bathtub Curve

Reliability engineering focuses on the middle part of the curve, also called useful life. Methods are applied to avoid the early life period, for example, burn in; the wear-out period is avoided by limiting the time the system is used.

3.2 Systematic Failures

Systematic failures can occur in both hardware and software items. These failures consistently [9] occur under particular conditions of handling, storage, and use. Systematic failures are in essence caused by human mistakes. They are basically avoidable and must be minimized through various steps during development. By addressing these conditions and taking preventive measures, it is possible to minimize systematic failures, which otherwise can impact the entire product life cycle. These issues can have their root cause in various factors, such as incorrect specifications, process flaws, design mistakes, manufacturing errors, or software bugs. While software bugs can often be eliminated through testing or debugging processes, addressing a wrong specification can require more comprehensive changes to the system design.

However, these kinds of failures may not be present at t=0 due to the item's complexity and can appear as if they were distributed over time. [9] That's why, according to the IEC61508 standard, statistic models are generally not applicable to quantify systematic failures. They are typically addressed through a qualitative approach, involving systematic analysis and managed processes for identifying and avoiding this type of failures. In Figure 3-3, you can see a conceptual view of the quality life cycle of a software product, although this concept can also be applied to hardware products.

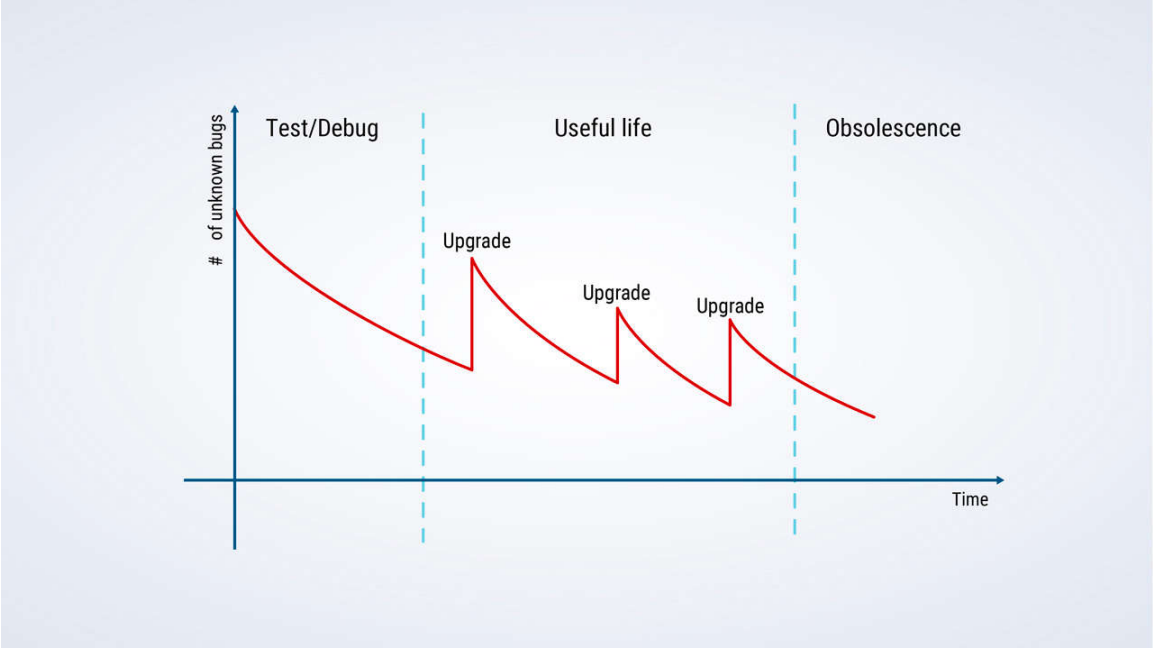

Figure 3-3. Quality Life-Cycle of a Software Product

At the beginning of the product life cycle, there are often unknown software bugs that are discovered through debugging and testing. Over time, the number of bugs decreases, and reliability increases. The same cycle repeats when there is an upgrade to the software. This phenomenon, caused by systematic failures and the elimination of errors, is known as the learning curve or reliability growth. [9]

4 System-on-chip (SoC): Functional Safety Benefits for Space

The high integration level of SoC devices enable designers to generate highly sophisticated and complex functions on a single circuit board assembly (CBA).

The complexity of the used SoCs is nowadays typically even significantly higher than the circuitry around it to build the actual CBA.

It is essential that any systematic faults have been avoided as much as possible already during the design phase of the SoC by the vendor.

Designers of high-reliability systems depend on the solidity of the SoC itself and all the development tools that come with it. In other words, the SoC must have been developed according to a managed process to enable proper assessment of the level of risk that the SoC contributes to the CBA.

The more complex a circuit is the higher the efforts to monitor its proper operation and detect any faults. With current integration levels of 100s of millions of gates it is next to impossible to test and monitor the proper operation of such SoC exclusively with external circuitry. It is mandatory that the SoC vendor has built in self-test and monitoring capabilities in hardware to enable a satisfying level of diagnostic coverage and effective control of faults, see Figure 4-1.

According to IEC61508 the used SoC pre-defines the limit of the reachable systematic capability of the full design [11].

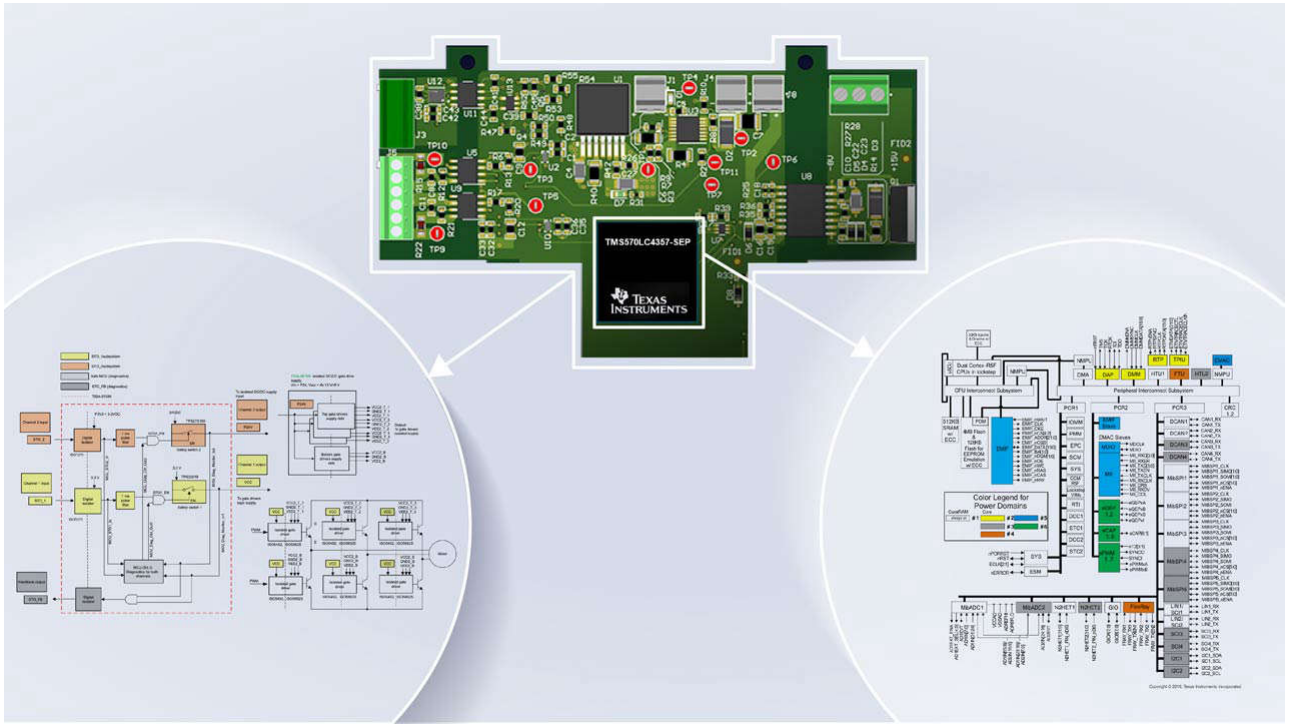

Figure 4-1. Complexity of SoC Being Much Higher Than the Circuitry Around it is not Uncommon

5 Growing System Level Complexity Requires Strong Collaboration With Semiconductor Industry

Hardness assurance characterizes a component to have a low enough failure rate that meets the reliability requirement needed to meet the CBA's reliability target. Hardness assurance is always specific to the environment the component is exposed to. The space industry has developed a very high grade of expertise and understanding of the harsh and very complex environment of space and has developed corresponding test methods to qualify electronic components according to mission needs.

It is possible to statistically model random hardware failures and conclude on reliability figures of merit such as average probability of failure on demand (PFDavg), the average frequency of a dangerous failure per hour (PFH), or meant time to failure (MTTF).

It is important to understand that any such reliability figures are specific to environmental conditions.

Pure mathematical extrapolation of the FIT-rate of a Commercial-off-the-shelf (COTS) or an Automotive (Q100) device to the space environment is not possible. There is certainly the path to apply correction factors to adopt from one environment to another [12]. However, space adds radiation as a harsh environmental condition. Since radiation tests are not part of the characterization of a COTS or automotive semiconductor device there is no starting value to extrapolate from or apply any correction factor to it. Characterization for radiation hardness must always be added separately. Operating a product outside of its specified environmental parameter range is considered a systematic fault. [9]

5.1 Validation and Verification – Avoidance of systematic Faults

Hardware and software development processes must follow a rigorous process, including all development tools used to avoid systematic faults as much as possible. Complex SoCs must be validated and verified throughout their development phases. It is impossible for a user to verify and validate all functions of an SoC with reasonable efforts retrospectively.

Systematic faults are in essence due to human mistakes.

5.2 Self-Monitoring Capabilities

Despite all efforts to minimize the probability of a random hardware fault or the inclusion of a systematic fault, there is a residual probability of faults to happen. It is important to detect such faults rapidly and control the impact. The more complex a component is, the higher is the importance of having such fault detection and control capabilities integrated.

Strong self-monitoring capabilities can allow for small compromises on the target failure rate but only within very narrow limits. If random failures occur too often, the system needs to handle more than one fault concurrently or it can end up in permanent re-boot, causing an availability issue. Typically, the systems can only handle a single fault at a time. The probability of a fault must stay at a very low level to meet the overall reliability target.

Self-monitoring and fault management capabilities do only partially overlap between industries.

For example, automotive and space do share the concern of single and multiple bit upsets from cosmic radiation. However, if such fault is detected an automotive system seeks the safe state typically by commanding an immediate stop followed by an immediate inspection, which can include the call of a tow truck. A satellite system must go beyond such safe state and must seek full recovery of the system autonomously while staying in orbit without any physical hands-on interaction.

Fast and reliable fault detection is a common concern across industries. Figure 5-1 shows the links of risk mitigation.

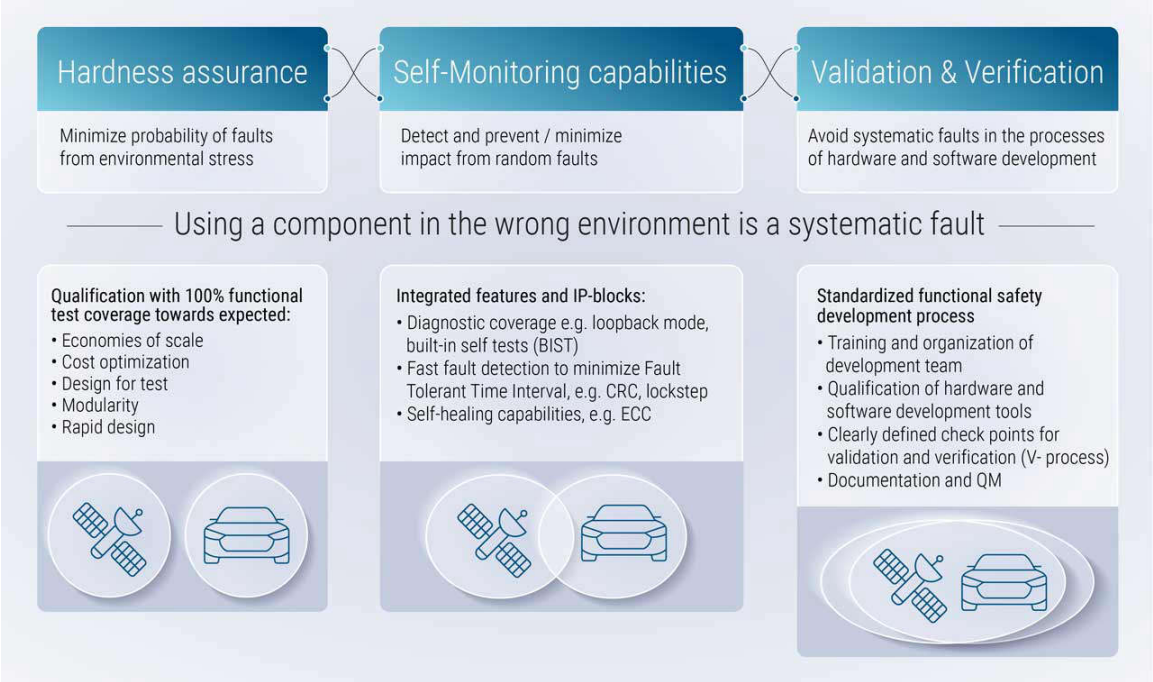

Figure 5-1. Three Chain Links of Risk Mitigation to Accomplish "Freedom From Unacceptable Risk"

6 Example of a Functional Safety SoC in Space

The following provides a closer look at TMS570LC4357-SEP as an example on how an existing SoC with strong functional safety capabilities originally developed for IEC63508 SIL-3 / ISO26262 ASIL-D applications has been extended in its characterization to be applicable for space flight, see Figure 6-1.

6.1 Hardness Assurance

The biggest concern for space applications is the harsh environment the electronic components are exposed to. Radiation hardness must be assessed in terms of total ionizing dose but also for single event effects. For digital or mixed signal devices build in a CMOS process single event latch-up (SEL) is the most common cause for the destruction of a device from heavy ions.

The TMS570LC4357-SEP was characterized to be immune to TID of 30krad and SEL of up-to 43MeVcm2/mg.

The MCU can operate at extreme temperatures from -55°C up to 125°C and against the very fast cycling between the temperature extremes that satellites are exposed in the Low Earth Orbit (LEO). All materials used in the MCU are in accordance with the needs for space, including the avoidance of pure tin to avoid tin whisker and special mold compound to keep outgassing well below typical requirements.

The TMS570LC4357-SEP follows the TI standard of Space Enhanced Products (SEP). This includes requirements such as controlled baseline: single fabrication site, single assembly/test site and single material set; extended product life cycle, extended product-change notification, product traceability in support of long-term product safety.

6.2 Validation and Verification – Avoidance of systematic Faults

The development of the TMS570LC4357 product family was developed for applications with safety critical requirements up-to ASIL D for automotive or SIL 3 for industrial machinery. The development of the design and associated tools followed the IEC61508:2010 and ISO26262:2011 process. TI's hardware and software development processes have been audited and certified by TÜV Süd (Hardware) [13] and TÜV Nord (Software) [14].

The software offer includes HALCoGen (Hardware Abstraction Layer Code Generator), a GUI-based initialization, configuration and driver code generator for TMS570 MCU and the corresponding HALCoGen compliance support package (CSP) to assist customers using HALCoGen generated software to comply with functional safety standards such as IEC61508 and ISO26262. Further, the HALCoGen Test Automation Unit (HALCoGen TAU) helps users generate a Dynamic Coverage Analysis Report and Regression Report for HALCoGen generated drivers to support ISO26262 and IEC61508 assessments. [15]

The TMS570LC4357-SEP hardware and software offer provides users a great starting point for their own high-reliability design.

6.3 Self-Monitoring Capabilities

The safety architecture of the TMS570LC4357-SEP includes several on-chip diagnostic features for high diagnostic coverage and near-instant fault detection.

A very important feature to mention is the lockstep safety mechanism of the CPU system.

The lockstep CPU scheme adds a second, so-called “checker CPU”, which executes the very same code as the main CPU. The so-called fail-safe unit compares the results of the two cores and can detect almost instantly in case a random fault has caused a difference in their results.

To verify that common cause failures cannot escape, the two cores execute the code 1.5-2 cycles apart and they are also implemented rotated and flipped to each other to give temporal and physical diversity.

Further, the clock and voltage are permanently monitored and all memories are ECC protected to maintain dependable results from software execution.

Hardware diagnostics include self-test (BIST) logic for CPU, the N2HET coprocessors, and for on-chip static random access memory and loopback capability on peripheral I/Os. [16]

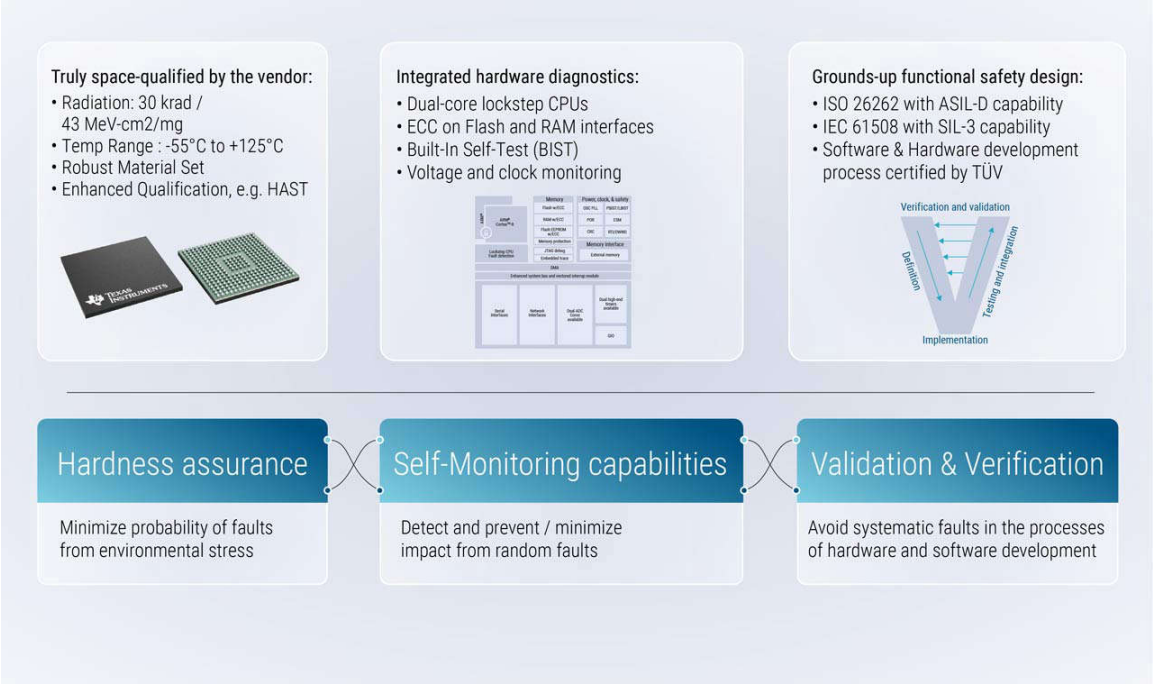

Figure 6-1. Functional Safety MCU TMS570LC4357-SEP: Applied Risk Mitigation to Accomplish “Freedom From Unacceptable Risk”

6.4 Near-Instant Fault Detection and Recovery

Figure 6-2 shows how two TMS570 MCUs can be used to form a redundant system. A random fault detected on the primary MCU device “informs” the FPGA about the unsafe situation to switch over to the redundant MCU. Thanks to the near-instant detection of any faults, the system can meet very tight real-time requirements as needed in time and mission critical sub-systems such as flight controller, thrusters, collision avoidance or docking systems. This example shows how the well-thought through architecture and strict development according to functional safety standards of a complex SoC enable high reliability even for a highly sophisticated and time critical function.

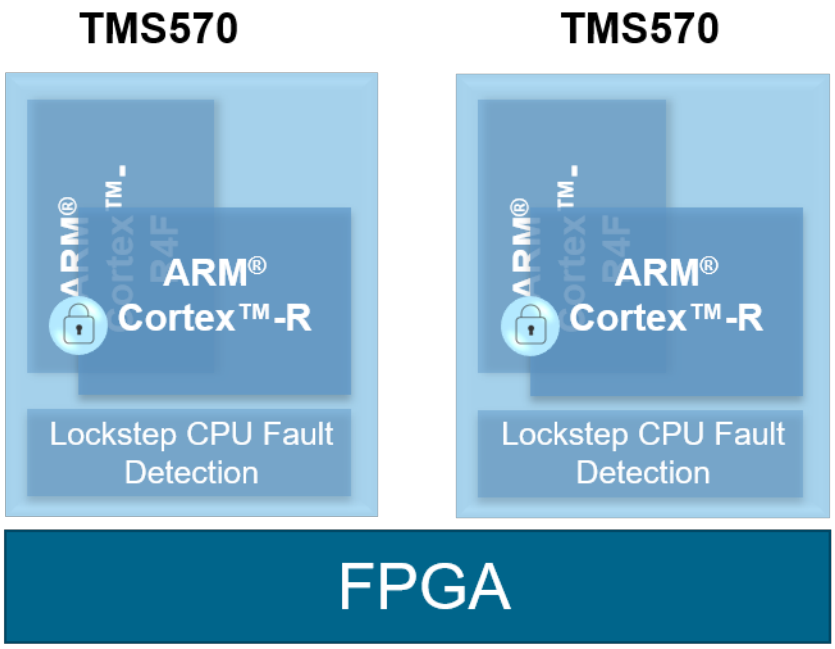

Figure 6-2. Two TMS570 MCUs Form Highly Resilient Real-Time System

7 The Future in Space Needs New Strategic Thinking

To serve the increased needs for cost reduction and acceleration of development cycles of electronic designs for the space industry mass production-oriented industries like automotive can serve in some aspects as a blueprint. E. W. Dijkstra stated “Simplicity is prerequisite for reliability.” While this is very true modern electronic designs are extremely complex and far from being simple. However, if one looks at a functional safety compliant SoC as a RAMS-compliant sub-system it simplifies the overall RAMS process significantly. It can be worthwhile to see how the RAMS standards can add guidance on how to deal with functional safety compliant electronic designs to benefit from the use of functional safety compliant SoCs in space designs even further.

8 Summary

The age of New Space continues to challenge space electronics designers more and more by having to deal with an increase in complexity of the functions they are asked to integrate onto a single circuit board assembly and speeding up their development cycles while at the same time keeping cost under control and must not allow for any compromise on reliability. One can actually observe a trend of the space industry’s needs towards the needs of the automotive industry, which does traditionally also share the need for high reliability and product safety but has to deal with cost pressure for much longer time already.

Highly integrated SoCs are available that enable the increase of functionality needed. At the same time such complex SoCs are a major contributor to the overall reliability level of the actual CBA they are designed in. Typically, such SoCs are driven by the automotive industry, accordingly the functional safety standards applicable to automotive designs IE C61508/ ISO26262 provide strong guidance to the semiconductor industry to enable strong functional safety support.

This paper compares the IEC61508/ ISO26262 based functional safety approach with the space industry's RAMS approach with special focus on their main commonalities:

They share the same objective of "freedom from unacceptable risk" where both approaches define risk as the product of severity of the damage times the probability of the occurrence of that damage.

Further, both industries divide failures into random and systematic failures to develop the methods needed to minimize their occurrence and control the impact in case they still happen to reduce the overall risk.

With that understanding we have split up our analysis of the reliability contribution of a complex SoC and its supporting tools into the three areas of hardware assurance to quantify the probability of random failures, validation and verification to minimize the probability of systematic failures and self-monitoring capabilities to eliminate or at least mitigate the impact from any failures.

Functional safety according to IEC61508 and ISO26262 offers a compact and well-structured approach with a defined process for designing electronic designs with functional safety requirements. Systematic capability is rated using Safety Integrity Levels (SIL), enabling the evaluation of software and hardware. This approach represents the state of the art for electronic designs across various sectors, including automotive, avionics and industrial machinery. Specifically, systematic failures from hardware and software are avoided due to the defined processes and specified methods outlined in IEC61508. Especially very complex designs with strong software involvement, either as development tools or as part of the actual product, benefit from this approach of dealing with all reliability and safety related aspects of the electronic design based on a single standard saves efforts, iterations and time.

A good example is the functional safety MCU TMS570LC4357-SEP and its software components, which have been certified by a notified body like TÜV to be safety compliant. The result is a reduction in the complexity of the verification process of the design based on such functional safety SoC.

9 References

1. K. Bousedra (2023). Downstream Space Activities in the New Space Era: Paradigm Shift and Evaluation Challenges. Space Policy. BETA CNRS 7522, University of Strasbourg, France. Space Policy 64 (2023) 101553.
2. ISO 9001:2015 (2015), Quality management systems – Requirements Chapter 9- Performance Evaluation (ISO 9001:2015).
3. VDE (2023) Verband der Elektrotechnik Elektronik Informationstechnik e.V.Informationstechnische Gesellschaft im VDE (VDE ITG) : VDE Positionspapier NeSC – NewSpace Communications NeSC – NewSpace Communications (Germany Frankfurt).
4. IEC 61508-1:2010 (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements. International Electrotechnical Commission.
5. ISO 26262 (2018). Road vehicles - Functional safety. Part 1: Vocabulary. International Organization for Standardization.
6. German Center of Aerospace DLR (2024), Picture source: DLR (CC BY-NC-ND 3.0).
7. NASA DFE 7 (1996) Fault-Detection, Fault-Isolation, and Recovery (FDIR) Techniques, Page 1 of 6 NASA. (1996). Design for Environment (DFE-7): Preferred Reliability Practices. Kennedy Space Center. National Aeronautics and Space Administration: https://extapps.ksc.nasa.gov/Reliability/Documents/Preferred_Practices/dfe7.pdf.
8. ECSS-S-ST-00-01C (2023) – Glossary of terms, RAMS page 50, reliability- chapter 2.3.189 page 39, availability -chapter 2.3.21 page 16, maintainability- chapter 2.3.149 page 32, safety- chapter 2.3.199 page 40.
9. A. Birolini (2017) 8th edition- Reliability Engineering- Theorie and Practice, λ-Rate p. 390, FIT p. 36, MTTF p. 393 RAMS p. 407, bath tube- curve p. 6-7, environment p. 82, Springer-Verlag GmbH Deutschland.
10. DIN EN 61508-4 (VDE 0803-4) based on IEC 61508-4:2010 (2010), Part 4: Definitions and abbreviations, p. 5.
11. Gerry Creech (2014) IEC 61508 Systematic Capability (sagepub.com), Measurement and Control 2014, Vol. 47(4) 125–128 © The Institute of Measurement and Control 2014 Reprints and permissions: sagepub.co.uk/journalsPermissions.nav DOI: 10.1177/0020294014528895 mac.sagepub.com.
12. MIL-HDBK-217 MIL Handbook

13. P.Weiß, A. Köhnen, Matthias Ramold, Report of the Functional Safety Audit, 2013, TÜV SÜD Rail GmbH, Generic Safety Systems, Barthstraße 16, D-80339 München Functional Safety Audit: SafeTI Functional Safety Hardware Development (Rev. A).
14. Bianca Pfuff, Certificate QRAS AP00213 – SafeTI – Functional Safety Software Development Process, 2015, TÜV NORD Systems GmbH & Co. KG, Große Bahnstarße 31, 22525 Hamburg, Germany SEBS_A.165253_14_Cert_Process_TI_EN_V0_1.
15. Texas Instruments: *HALCoGen-CSP User's Guide*
16. Texas Instruments: *Hercules™ Microcontrollers: Real-time MCUs for safety-critical products*.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265