Journal of Space Safety Engineering xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of Space Safety Engineering

journal homepage: www.elsevier.com/locate/jsse

Benefits of using functional safety in commercial space applications

F. Lumpe[a,*], M. Seidl[b]

[a] German Center of Aerospace: Linder Höhe, Cologne 51147, Germany
[b] Texas Instruments Deutschland GmbH, Haggertystr, Freising 185356, Germany

ARTICLE INFO

Article history:
Received 5 November 2024
Accepted 6 November 2024
Available online xxx

Keywords:
Functional safety
Programmable electronic elements
Safety-critical functions
RAMS approaches
Flight detection isolation and recovery
FDIR
Risk minimization
Component level
Complex
System on the chip
Soc
Integrated circuits
Extreme environmental parameters
Systematic faults
Chip development
Hardware Development
Built-in Self Test
Self-Diagnostic

ABSTRACT

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, process industry (e.g., energy sector), automotive (transport sector), mechanical engineering, or aviation. This article will compare 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 will provide an insight into the possibilities of minimizing risk at the component level, especially for complex integrated circuits. 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 (Integrated Circuit) 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 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.

The presentation will show how systematic faults in other market sectors can be avoided as far as possible and how so-called 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 the semiconductor products, such as ECC (Error Correction Code), lock-step, or BIST (Built-in Self Test).

The successful mission of the Mars Rotorcraft Ingenuity from JPL (NASA) provides an insight into the practical application of a functional safety concept in a space application.

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

1. Introduction: new space forces a new and comprehensive look at system level resiliency

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 (ROI) or ROI in short; 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. In this context, it is challenging to manage increasingly complex spacecrafts, whose system-level complexity continues to grow. At the same time, 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].

[*] Corresponding author.
E-mail addresses: florian.lumpe@dlr.de (F. Lumpe), m-seidl@ti.com (M. Seidl).

https://doi.org/10.1016/j.jsse.2024.11.002
2468-8967/© 2024 International Association for the Advancement of Space Safety. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

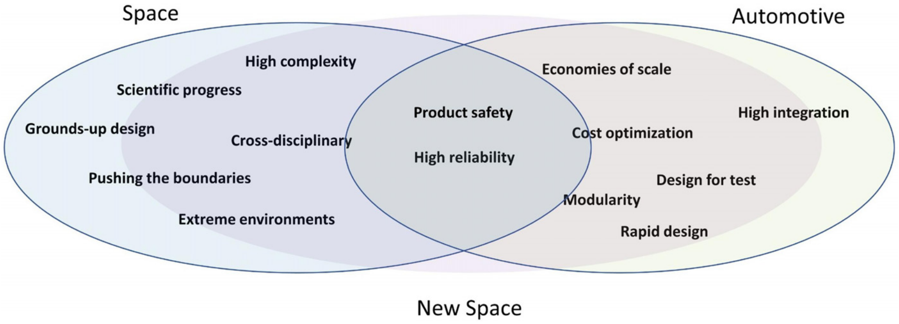


Fig. 1. Attributes space and automotive.

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’s 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 industry share some similarities, but certain attributes differ completely from an established perspective. Space systems, for instance, 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 al lot of space missions are driven by scientific questions, inherently leads to scientific progress and pushes the boundaries of technology. For most of the missions, a tailored ground-up design is necessary, which is robust and reliable. Product safety must be guaranteed because there is no possibility for repair or maintenance of the hardware, but especially for crewed based mission product safety is the most important issue and 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.

The primary motivation of the automotive industry regarding Product safety 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.

The product Safety motivation for space is driven by the high stakes involved in space missions, especially those with human crews, RAMS activities are essential to ensure the survival of astronauts. However, it’s 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.

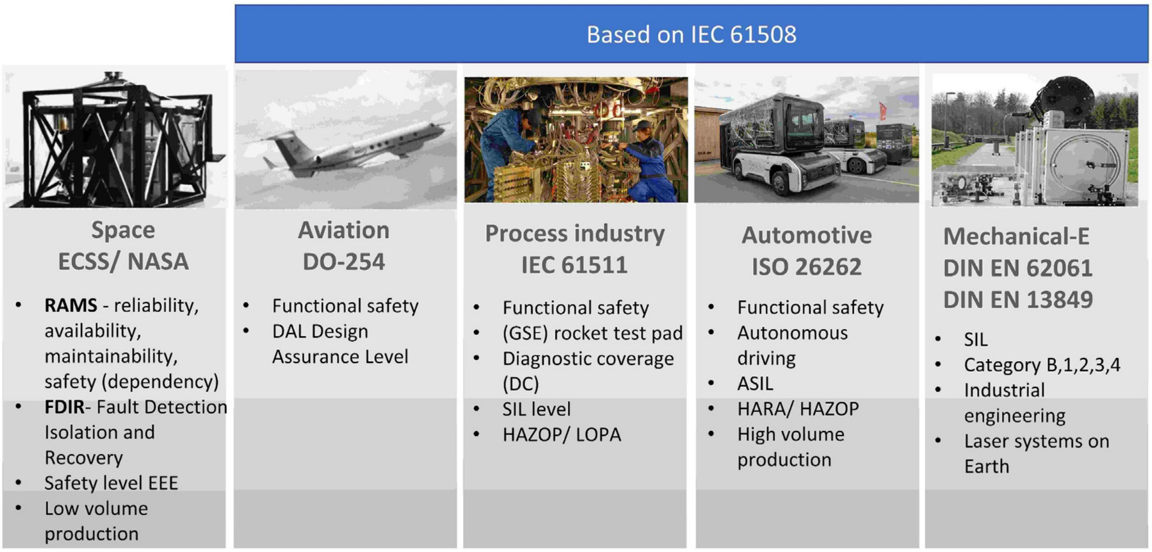
Many space missions are driven by military objectives, further underscoring the need to rigorously manage and mitigate risks. The enormous financial and temporal investments in space activities also reinforce the importance of robust Product Assurance practices. Moreover, with the growing concern over space debris and the sustainability of space environments, the need for comprehensive safety measures is more pressing than ever.

New Space will increasingly adopt attributes from the automotive industry, such as mass production, cost optimization, and others that have already been discussed, see Fig. 1.

The foundational standard, IEC61508 [4], represents the base standard for the most industry sectors. The space sector, however, does not follow the approach of IEC61508. Space takes a rather universal approach and process for handling and managing functional safety for the systems. This also implies that industries such as aviation, the process industry, automotive, and mechanical engineering follow the same methodology, as you can see in Fig. 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.

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 automotive industry it‘s called ASIL according to ISO26262 [5].

On the other side space industry is not based on IEC61508, and here it is referred to Standards in the field of Reliability, Availability, Maintainability, and Safety (RAMS), a term that encompasses all these aspects and defining the 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 based in case of detected anomalies. This concept goes beyond requirements of functional safety which only demands for reaching the safe state.



Based on IEC 61508

Space
ECSS/ NASA

- **RAMS** - reliability, availability, maintainability, safety (dependency)
- **FDIR**- Fault Detection Isolation and Recovery
- Safety level EEE
- Low volume production

Aviation
DO-254

- Functional safety
- DAL Design Assurance Level

Process industry
IEC 61511

- Functional safety
- (GSE) rocket test pad
- Diagnostic coverage (DC)
- SIL level
- HAZOP/ LOPA

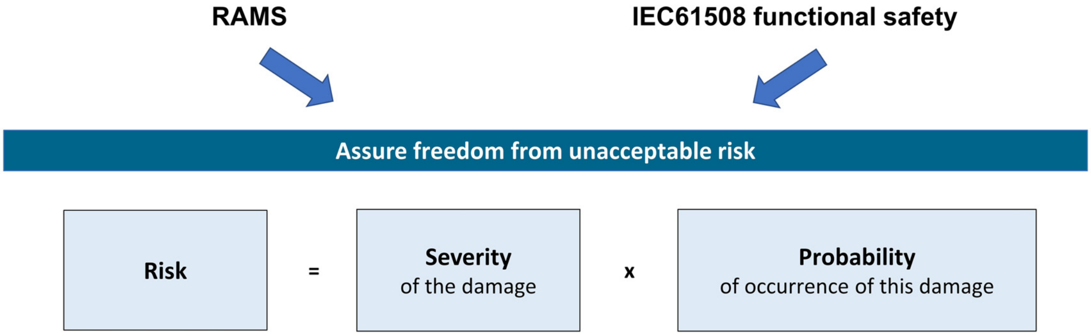
Automotive
ISO 26262

- Functional safety
- Autonomous driving
- ASIL
- HARA/ HAZOP
- High volume production

Mechanical-E
DIN EN 62061
DIN EN 13849

- SIL
- Category B,1,2,3,4
- Industrial engineering
- Laser systems on Earth

Fig. 2. Different sectors, different standards [6].



RAMS

IEC61508 functional safety

Assure freedom from unacceptable risk

Risk = **Severity** of the damage x **Probability** of occurrence of this damage

Fig. 3. Freedom from unacceptable risk.

3. Commonalities of RAMS and IEC61508 functional safety

Functional Safety and RAMS in the Space Industry share the same objective of “freedom from unacceptable risk”, see Fig. 3, where both define risk as the product of severity of the damage times the probability of occurrence of this damage.

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

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’s 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:

- ƛ-rate [9]: Failure Rate is the limit, if it is existing of the conditional probability that the failure occurs within time interval (t, $t+\delta_t$)], to δ_t when $\delta_t \to 0$, when, given that the item was new at t = 0 and did not fail in the interval (0,t].

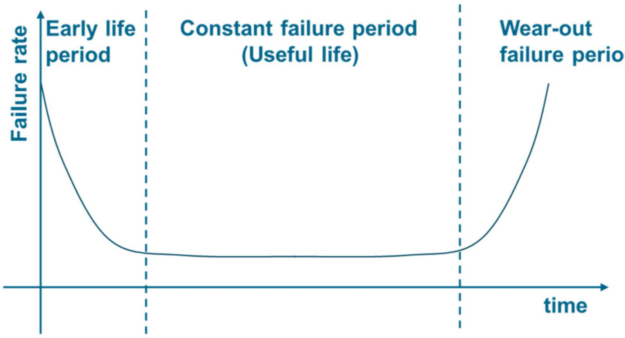


Fig. 4. E.g., random failure rate for a simple device -bathtub curve.

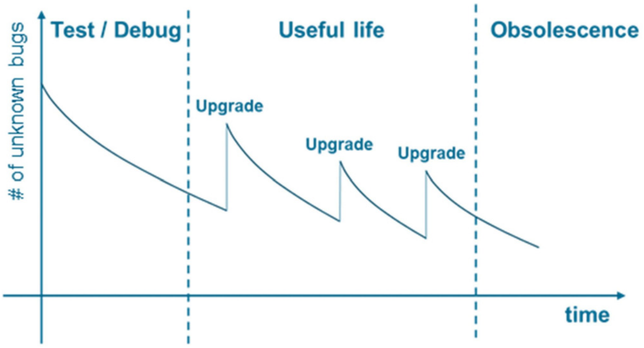


Fig. 5. E.g., Quality life-cycle of a software product.

- FIT [9]: failures in time or failure per 109 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= (t1 + ... + tn)/n) where t1…tn are failure free times of statistically identical item.
- Etc.

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 Fig. 4 shows the three phases [9]:

- Phase 1, early failures: e.g., 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, etc.

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

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 might 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 Fig. 5, 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. At the beginning of the product life cycle, there are many 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 System-on-Chip (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 therefore 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 100 s 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 Fig. 6.

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

5. Growing system level complexity requires strong collaboration with semiconductor industry

The key driver for the semiconductor vendors to develop SoCs with strong functional safety or high reliability capabilities is the automotive sector with its high need for safety and high sales volumes at the same time.

As explained in chapter 3, the overall standardization between space and other industries that need high reliability or 'freedom from unacceptable risk' as ISO26262 spells out its objective apply very different approaches. It is very difficult to assess the value of a functional safety compliant SoC developed in accordance to an IEC61508-based standard towards the requirements defined in RAMS.

We decided to divide the overall contribution of a component to the risk mitigation from hardware and software failures into three categories, see Fig. 7:

- Hardness assurance.
- Self-monitoring capabilities.
- Validation and verification.

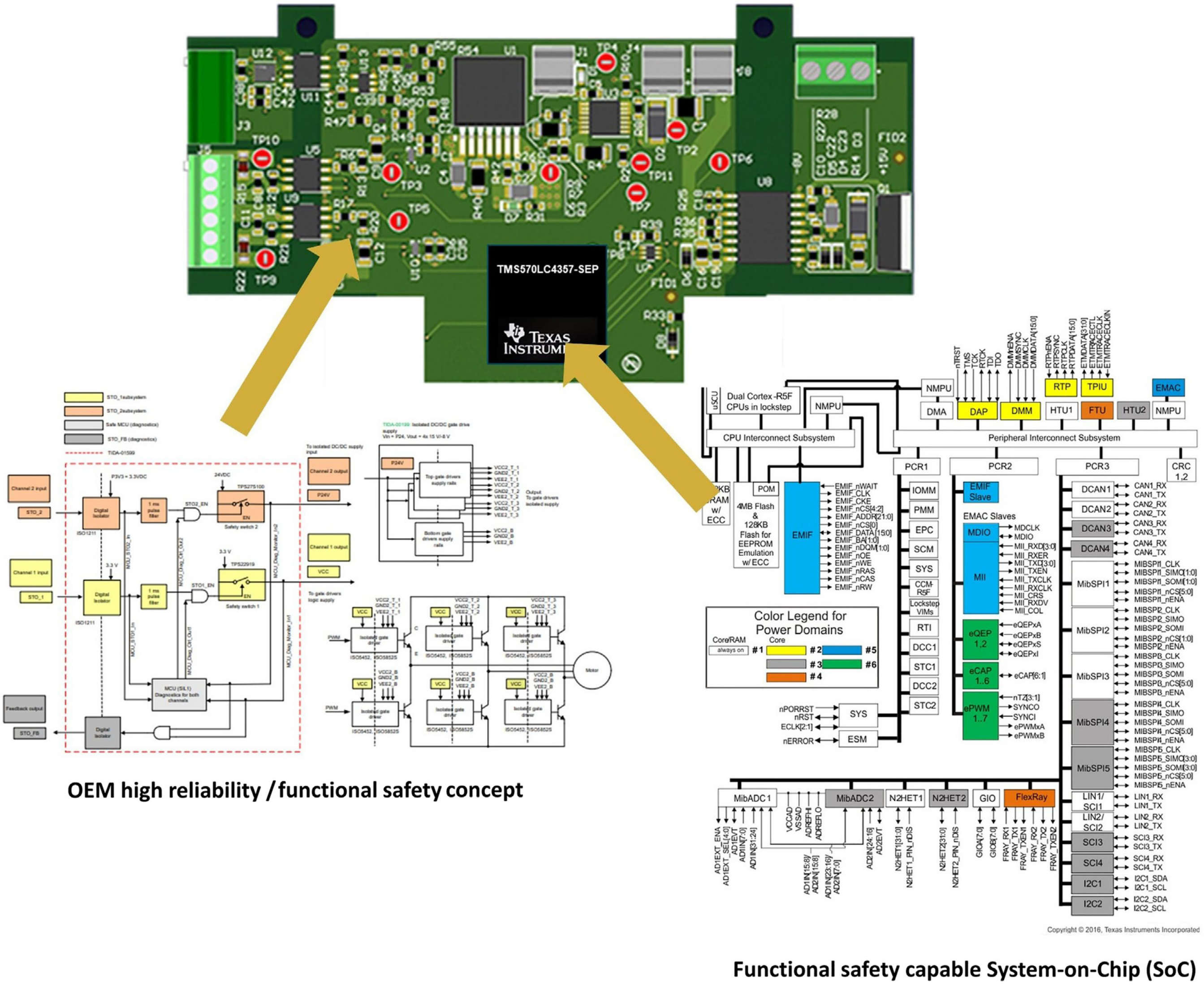
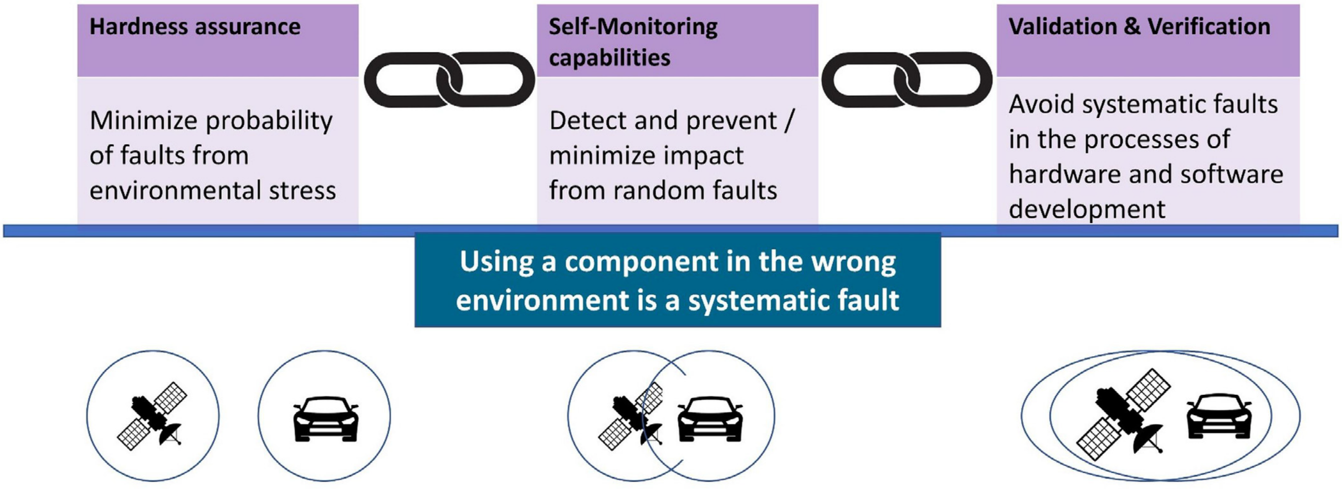

TMS570LC4357-SEP
Texas Instruments
OEM high reliability / functional safety concept
Functional safety capable System-on-Chip (SoC)
Dual Cortex-R5F CPUs in lockstep
CPU Interconnect Subsystem
Peripheral Interconnect Subsystem
4MB Flash & 128KB Flash for EEPROM Emulation w/ECC
EMIF
Color Legend for Power Domains
MCU (SIL1) Diagnostics for both channels
Safety switch 1
Safety switch 2
Motor
Copyright © 2016, Texas Instruments Incorporated

Fig. 6. Complexity of SoC being much higher than the circuitry around it is not uncommon.



Hardness assurance

Minimize probability of faults from environmental stress

Self-Monitoring capabilities

Detect and prevent / minimize impact from random faults

Validation & Verification

Avoid systematic faults in the processes of hardware and software development

Using a component in the wrong environment is a systematic fault

Fig. 7. Three chain links of risk mitigation to accomplish “freedom from unacceptable risk”.

Hardness assurance characterizes a component to have a low enough failure rate that meets the reliability requirement needed to meet the CBS's reliability target. Hardness assurance is always specific to the environment the component will be 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.

The nice thing about random hardware failures is that it is possible to statistically model them 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 a given of environmental conditions.

Pure mathematical extrapolation of the FIT-rate of a COTS (Commercial-off-the-shelf) or 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 the guaranteed environmental parameters is considered a systematic fault [9].

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. Provided that engineers from any industry are humens with very similar DNA, any methods to avoid such human mistakes shall be applicable across industries.

Despite all efforts to minimize the probability of a random hardware fault or the inclusion of a systematic fault there will be a residual probability of faults to happen. Therefore, self-monitoring capabilities of the system are necessary. 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 may allow for small compromises on the target failure rate but only within very narrow limits. If random failures occur too often, the system may have to handle more than one fault concurrently or it may 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 therefore stay at 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 may 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.

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 Fig. 8.

The biggest concern for space applications lays in the harsh environment the electronic components will be exposed. 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 SEL (single event latch-up) is the most common cause for the destruction of a device from heavy ions.

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

Proper operation at extreme temperatures from −55 °C up to 125 °C have been assured and also robustness against the very fast cycling between the temperature extremes that satellites are exposed in the Low Earth Orbit (LEO) has been verified. All materials used 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) which includes requirements such as controlled baseline: single fabrication site, single assembly/test site & single material set; extended product life cycle, extended product-change notification, product tracability in support of long term product safety.

The development of the TMS570LC4357 product family has been developed for applications with safety critical requirements up-to ASIL D for automotive or SIL 3 for industrial machinery.This means that for the chip, a validation and verification process has already been carried out to avoid systematic faults. The development of the design and associated tools followed the process of IEC61508:2010 and ISO26262:2011. 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].

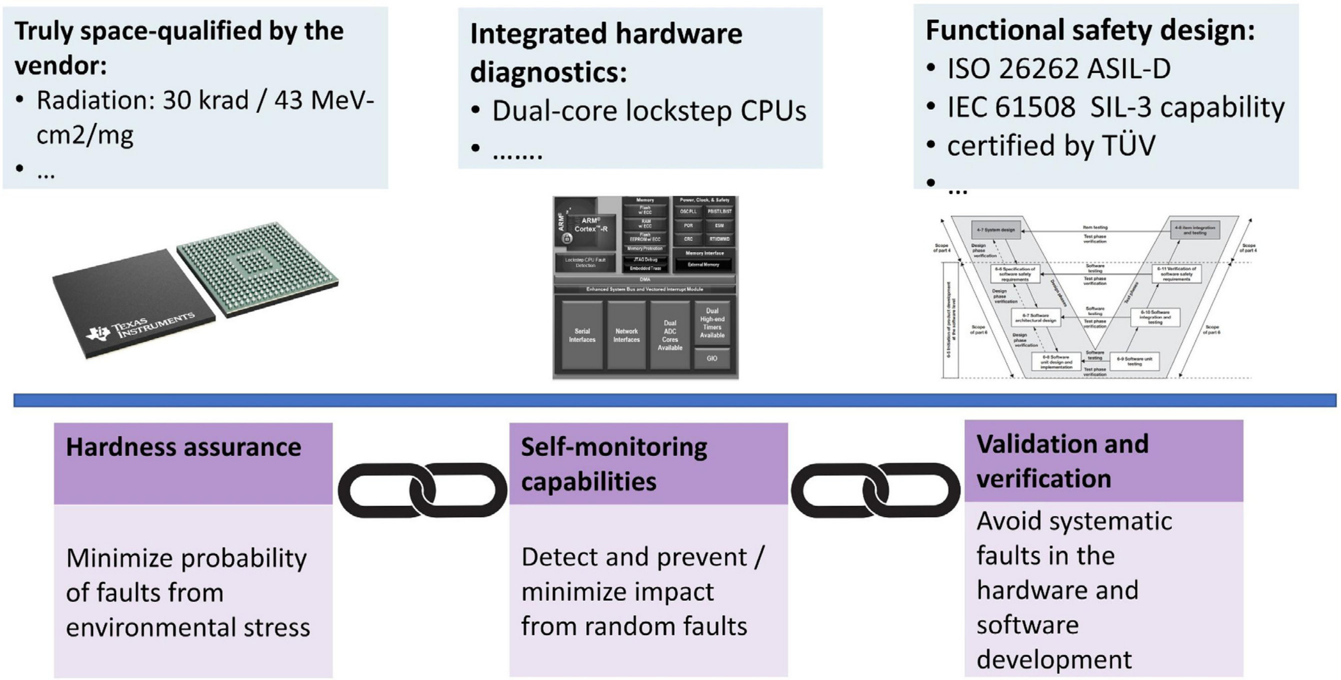
The TMS570LC4357-SEP hardware and software offer provides users a very solid starting point for their own high reliability design.

The safety architecture of the TMS570LC4357-SEP includes several on-chip diagnostic features for high diagnostic coverage and near-instant fault detection. This means that self-monitoring capabilities are already integrated into this chip.

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 will detect almost instantly in case a random fault would have caused a difference in their results.

To assure 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.



Truly space-qualified by the vendor:
- Radiation: 30 krad / 43 MeV-cm2/mg
- …

Integrated hardware diagnostics:
- Dual-core lockstep CPUs
- …….

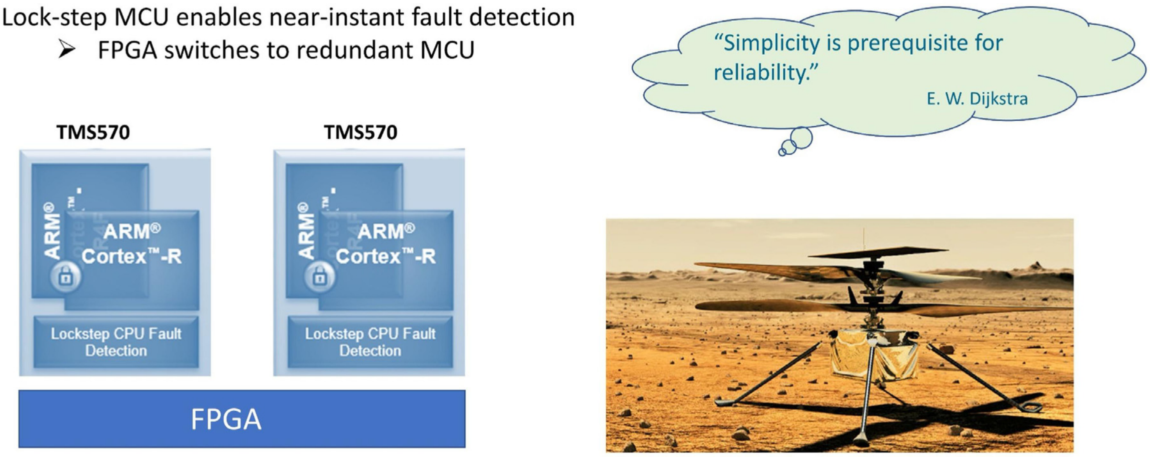
Functional safety design:
- ISO 26262 ASIL-D
- IEC 61508 SIL-3 capability
- certified by TÜV
- …

Hardness assurance
Minimize probability of faults from environmental stress

Self-monitoring capabilities
Detect and prevent / minimize impact from random faults

Validation and verification
Avoid systematic faults in the hardware and software development

Fig. 8. Functional safety MCU TMS570LC4357-SEP: Applied risk mitigation to accomplish “freedom from unacceptable risk”.



Lock-step MCU enables near-instant fault detection
➢ FPGA switches to redundant MCU

“Simplicity is prerequisite for reliability.”
E. W. Dijkstra

Fig. 9. Functional safety MCU on Mars: Two TMS570 Hercules MCUs form highly resilient flight controller.

Further, the clock and voltage are permanently monitored and all memories are ECC protected to assure “trustworthy” results from software execution.

Hardware diagnostics include Self-Test (BIST) logic for CPU (central processing unit), the N2HET coprocessors, and for on-chip SRAMs (Static Random Access Memory) and loopback capability on peripheral I/Os [16].

7. The application on Mars

NASA made successfully use of the TMS570LC4357’s lockstep architecture in their flight controller for the Ingenuity helicopter as part of their Mars mission, see Fig. 9 [17].

Two components of the TMS570 devices 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 the tight real-time requirements of the flight controller.

The 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 such as a flight controller.

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.

The semiconductor industry provides highly integrated SoCs to 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.

In order to show the value that such functional safety compliant SoCs can bring to the space industry this paper compared 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 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. 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." [18]. 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 should be worthwhile to see how the RAMS standards could even 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.

Declaration of competing interest

The author declares that there is no conflict of interest.

CRediT authorship contribution statement

F. Lumpe: Conceptualization, Investigation, Methodology, Validation, Visualization, Writing – original draft, Writing – review & editing, Data curation, Formal analysis, Funding acquisition, Project administration, Resources, Supervision. **M. Seidl:** Conceptualization, Data curation, Investigation, Validation, Visualization, Writing – original draft, Writing – review & editing, Formal analysis, Funding acquisition, Methodology, Project administration, Resources, Supervision.

References

[1] K. Bousedra, Downstream Space Activities in the New Space Era: paradigm Shift and Evaluation Challenges, Space Policy 64 (2023) 101553 BETA CNRS 7522, University of Strasbourg, France. Space Policy2023.
[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 (2020), HALCoGen-CSP User's Guide (Rev. C) (ti.com)
[16] Karl Greb, Dev Pradhan, Hercules^{TM} Microcontrollers: real-time MCUs for safety-critical products, 2011, Literature #: SPRY178, Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
[17] NASA/JPL-Caltech (2020), Picture source: artist's Concept: mars Helicopter – NASA Mars Exploration
[18] E.W. Dijkstra (2024), Wikipedia: https://en.wikipedia.org/wiki/Edsger_W._Dijkstra