# BENEFITS OF USING FUNCTIONAL SAFETY IN COMMERCIAL SPACE APPLICATIONS

**TRISMAC, 24 – 26 June 2024 | ESA-ESRIN | Frascati (Rome), Italy**

**Florian Lumpe DLR-NPQ, Normung, Produktsicherung, Qualifizierung**

**Michael Seidl, Texas Instruments Deutschland GmbH**

TEXAS INSTRUMENTS

DLR

# Benefits of using functional safety in commercial space applications

## Agenda

- NewSpace forces a new and comprehensive look at system level resiliency
- Commonalities of RAMS and IEC61508 functional safety
- System-on-chip (SoC): functional safety benefits for space

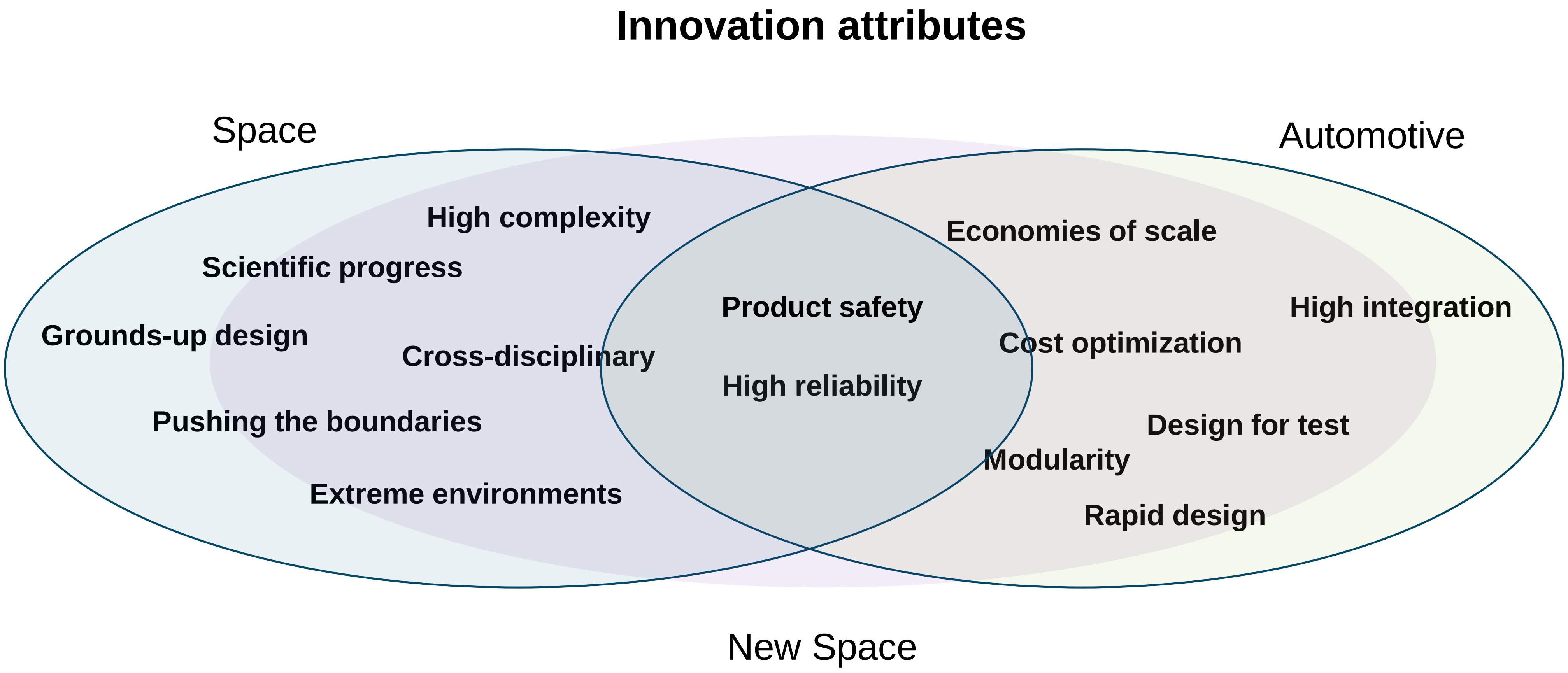
# New space forces a new and comprehensive look at system level resiliency

- Growing system level complexity requires methodical validation and verification
  - Minimize faults caused by system architects, hardware and software designers
  - Minimize faults caused by the design tools

- Commercialization drives for a balance between cost, performance, time & risk
  - Acceleration of development cycles (design, manufacturing, test, deployment)
  - Avoidance of costly over-engineering
  - Repeatability to maximize the return of investment
    - Re-use
    - Economies of scale (volume production)
  - ➢ Accountability (& measurability) for cost, performance, time & risk
- Higher volumes from new space enable new focus from semiconductor industry on space segment

# How space could benefit from other industry segments

## E.g. automotive



# Benefits of adopting functional safety in commercial space applications

## Agenda

- NewSpace forces a new and comprehensive look at system level resiliency
- Commonalities of RAMS and IEC61508 functional safety
- System-on-chip (SoC): functional safety benefits for space

# Standardization Overview

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

Source: DLR (CC BY-NC-ND 3.0)

# Space and IEC61508 share same approach and objective

## RAMS

**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.

## IEC61508 functional safety

Functional safety standards for the lifecycle of electrical, electronic, or programmable electronic (E/E/PE) systems and products.

Also includes RAMS approaches

Functional safety refers to safety functions, but can also be applied to basic functions

Specified process, includes specific tools and methods

**Assure freedom from unacceptable risk**

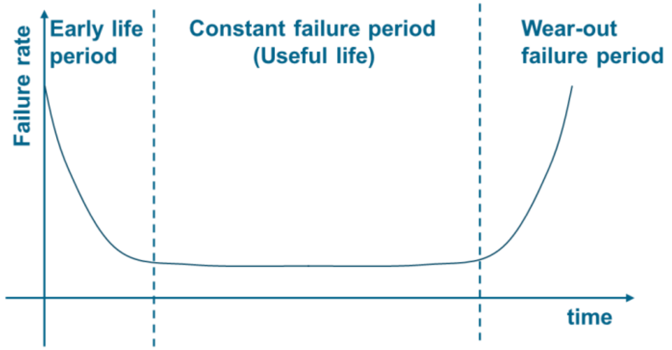
**Risk** = **Severity** of the damage x **Probability** of occurrence of this damage

# Systematic and random failure in functional safety

## Random failures
HW: e.g. resistor shortcut, transistor gate rupture

… are basically unavoidable
… can not be eliminated after being detected
… must be controlled to mitigate their impact
… can be statistically modeled with reasonable accuracy
… ʎ-rate, FIT, PFH, PFD, MTTF, etc.

## Quantitative approach
Measures: self-diagnostic, redundancy, …

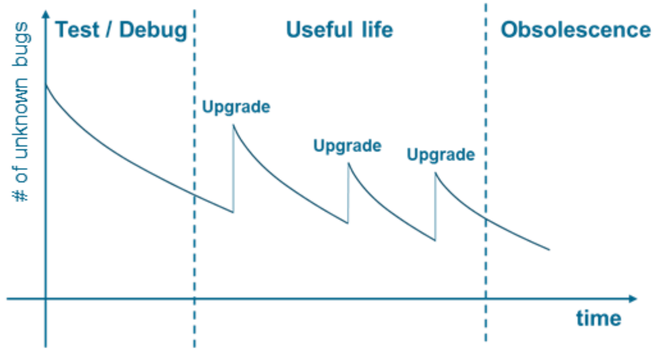



E.g. random failure rate for a simple device

## Systematic failures
HW or SW: e.g. specification faults, software bugs

… are basically avoidable
… are in essence due to mistakes
… can be eliminated after being detected
… cannot be statistically modeled
… concept of **Systematic Capability**
(IEC61508: scale of SC 1 to SC 4 → SIL 1-4)

## Qualitative approach
Measures: managed process, installed base analysis




E.g. Quality life-cycle of a software product

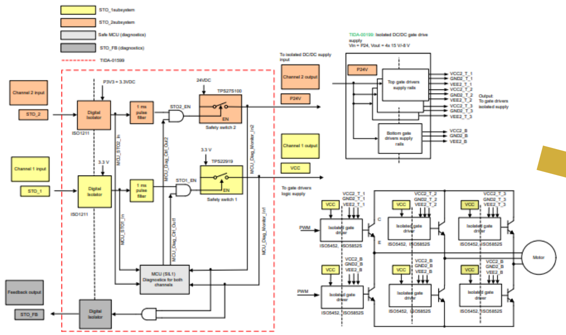
# Benefits of adopting functional safety in commercial space applications

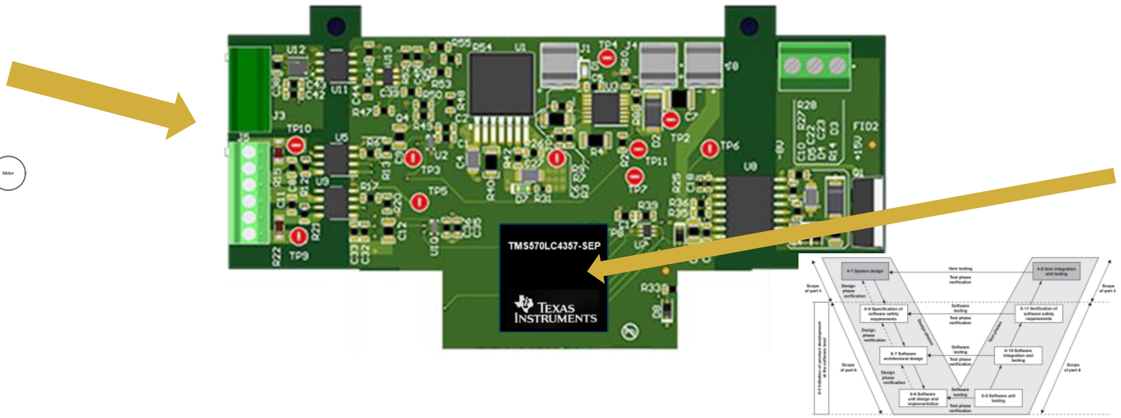
## Agenda

- NewSpace forces a new and comprehensive look at system level resiliency
- Commonalities of RAMS and IEC61508 functional safety
- System-on-chip (SoC): functional safety benefits for space

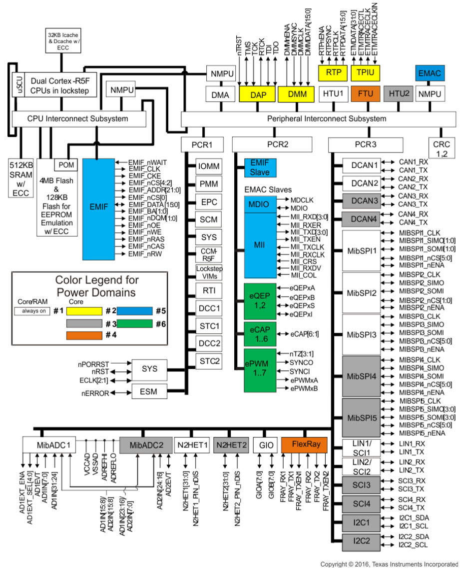
# Growing system level complexity requires strong collaboration with semiconductor industry

**OEM high reliability / functional safety concept**






**Functional safety capable System-on-Chip**




- System-on-Chip
  - Must provide sufficient safety capability to minimize risk mitigation efforts at system level
  - Pre-defines the limit of reachable reliability level of the system

- Level of integration keeps growing:
  - 100’s of millions+ of transistors enabling 1000’s of GOPS+ (trillion operations per second)
  - Greater importance in avoiding systematic failure

- High volumes of automotive are a strong driver for ‘integration of safety’ (Self-test, error correction, clock monitor, …)

# Microelectronic functional safety support

## Three chain links of risk mitigation to accomplish “freedom from unacceptable risk”

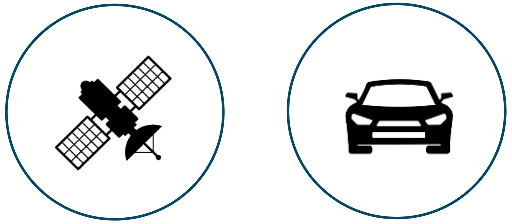
| Hardness assurance | Self-Monitoring capabilities | Validation & Verification |
| --- | --- | --- |
| Minimize probability of faults from environmental stress | Detect and prevent / minimize impact from random faults | Avoid systematic faults in the processes of hardware and software development |

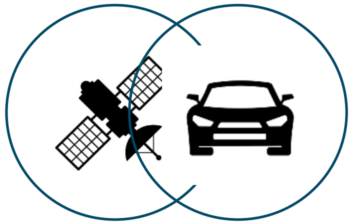
**Using a component in the wrong environment is a systematic fault**

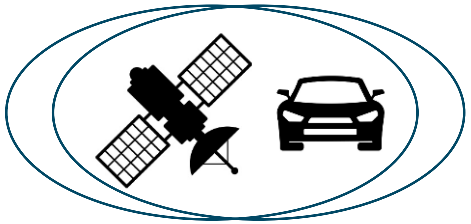
**Qualification with 100% functional test coverage** towards expected:
- Radiation levels (TID & SEE)
- Temp cycles (soldering & in-orbit)
- Air pressure
- Operation life cycle
- Vibration

**Integrated features and IP-blocks**
- Diagnostic coverage
  e.g. loopback mode, built-in self tests (BIST)
- Fast fault detection to minimize Fault Tolerant Time Interval, e.g. CRC, lockstep
- Self-healing capabilities, e.g. ECC

**Standardized functional safety development process**
- Training and organization of development team
- Qualification of hardware and software development tools
- Clearly defined check points for validation and verification (V- process)
- Documentation and QM



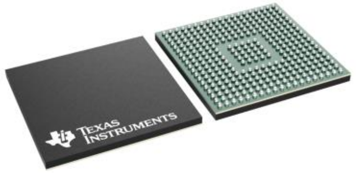




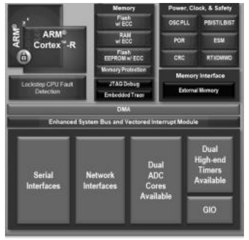
# Functional safety MCU TMS570LC4357-SEP

## Applied risk mitigation to accomplish “freedom from unacceptable risk”

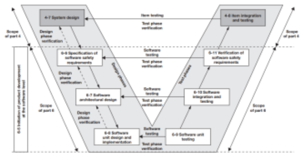
**Truly space-qualified by the vendor:**
- Radiation: 30 krad / 43 MeV-cm2/mg
- Temp Range : -55°C to +125°C
- Robust Material Set
- Enhanced Qualification, e.g. HAST
- …




**Integrated hardware diagnostics:**
- Dual-core lockstep CPUs
- ECC on Flash and RAM interfaces
- Built-In Self-Test (BIST)
- Voltage and clock monitoring
- …




**Grounds-up functional safety design:**
- ISO 26262 with ASIL-D capability
- IEC 61508 with SIL-3 capability
- Software & Hardware development process 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 processes of hardware and software development

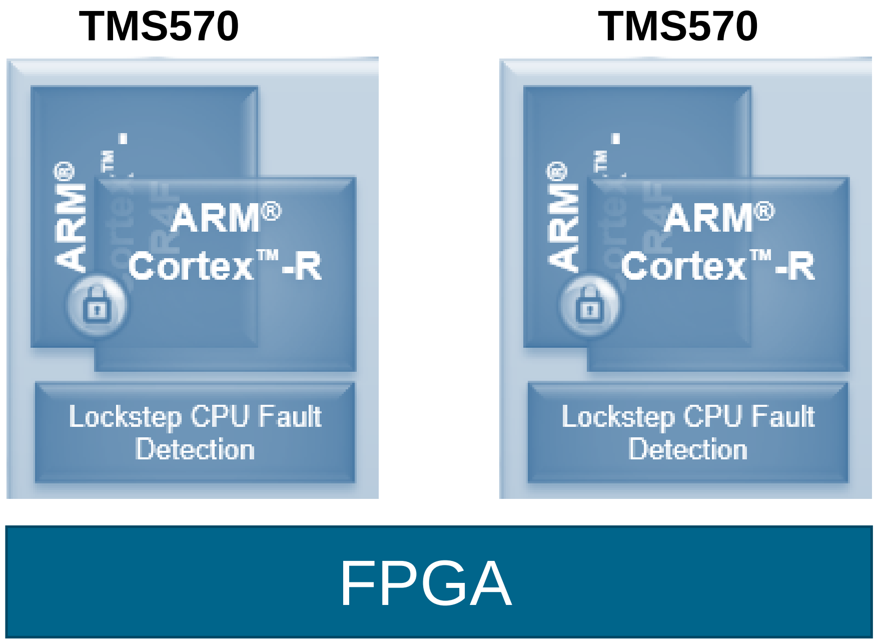
# Functional safety MCU on Mars
## Two TMS570 Hercules MCUs form highly resilient flight controller

Lock-step MCU enables near-instant fault detection

- FPGA switches to redundant MCU

"Simplicity is prerequisite for reliability."

E. W. Dijkstra




TEXAS INSTRUMENTS

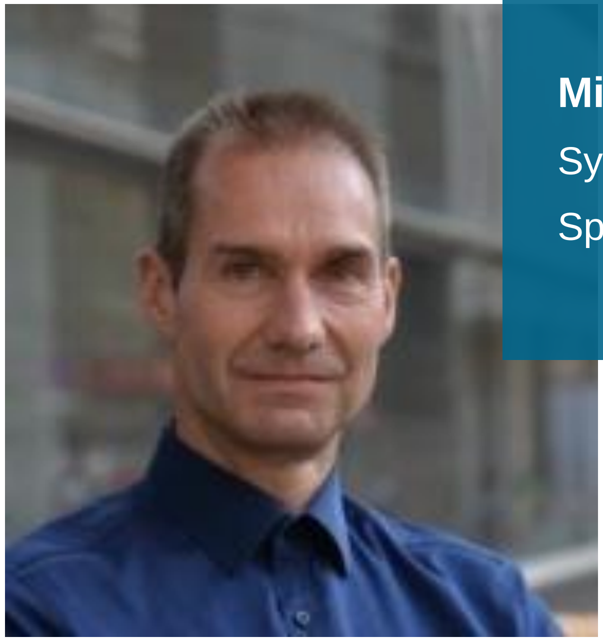
# The future in Space needs new strategic thinking

New approach for faster development cycles, more cost effectiveness, increased capabilities, yet highly reliable:

- EEE cross pollination from other industries,
  e.g. the automotive industry has strong experience in
  - High competition
  - Mass production
  - No failure strategy (recalls are fatal)
  - Functional safety

- Adopt functional safety (IEC61508) thinking to enable its use in space projects

# Today's speakers Michael Seidl Texas Instruments



**Michael Seidl**
Systems Engineer,
Space and Avionics

Michael received his Dipl. Ing. (FH) degree in communication technologies from Fachhochschule Munich in Germany.
Michael has 28 years of experience in semiconductors and held positions in DSP software design, applications, product marketing, business development and system engineering.

Michael is a Systems Engineer for Aerospace Applications at Texas Instruments. He supports customers in their decision making with in-depth system knowledge, combined with expertise on TI's product offerings.


**Michael Seidl**
m-seidl@ti.com / +49 163 80 62 575

**Texas Instruments Deutschland GmbH**
Haggertystr. 1
85356 Freising
www.ti.com/space

# Today’s speakers Florian Lumpe DLR R&D

**Florian Lumpe, DLR**

Coordinator Strategic Product Assurance

Florian Lumpe began his career in the aerospace industry a academic degree in mechanical engineering and general management. In his current role as Coordinator Strategic Product Assurance at the German Aerospace Centre in Cologne, he coordinates the integration of Product assurance into projects.

Florian is Coordinator Strategic Product Assurance for R&D at the DLR. His tasks include the management of technical interfaces and the adaptation of legal requirements, as well as the design and implementation of training courses. As an auditor, he contributes to optimizing the company’s performance.

**Deutsches Zentrum für Luft- und Raumfahrt** (DLR)
Qualitäts- und Produktsicherung | Normung, Produktsicherung & Qualifizierung | Linder Höhe | 51147 Köln

Dipl.-Ing. **Florian Lumpe** M.Sc. | Koordinator Strategische Produktsicherung
Telefon +49 2203 601-3694 | Telefax +49 2203 601-3235 | florian.lumpe@dlr.de

Funktionale Sicherheit in der Luft- und Raumfahrt (dke.de)