VORTEILE DES EINSATZES FUNKTIONALER SICHERHEIT IN KOMMERZIELLEN RAUMFAHRTANWENDUNGEN

Florian Lumpe DLR-NPQ, Normung, Produktsicherung, Qualifizierung

Michael Seidl, Texas Instruments Deutschland GmbH

DLR Bauteilekonferenz 2024 vom 14.-15. Mai 2024 in Kamp-Lintfort

TEXAS INSTRUMENTS

DLR

Vorteile des Einsatzes funktionaler Sicherheit in kommerziellen Raumfahrtanwendungen

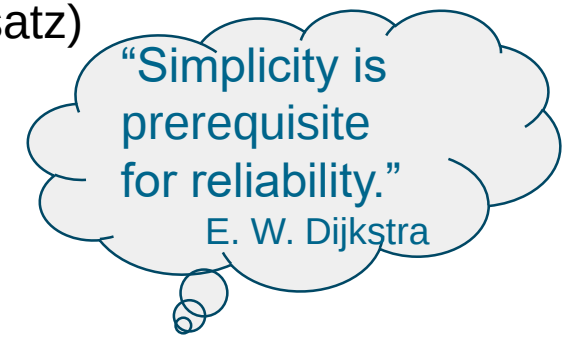
Agenda

- "NewSpace" erfordert einen neuen und umfassenden Blick auf die Resilienz auf der Systemebene
- RAMS vs. IEC61508 funktionale Sicherheit - Gemeinsamkeiten
- System-on-chip (SoC): Vorteile der funktionalen Sicherheit für die Raumfahrt

„New Space“ erfordert einen neuen und umfassenden Blick auf die Widerstandsfähigkeit der Systemebene

- Steigende Komplexität auf Systemebene erfordert methodische Validierung und Verifizierung
  - Minimierung von Fehlern, die von System-Architekten, Hardware- und Software-Designern verursacht werden
  - Minimierung von Fehlern, die durch die Design-Tools verursacht werden

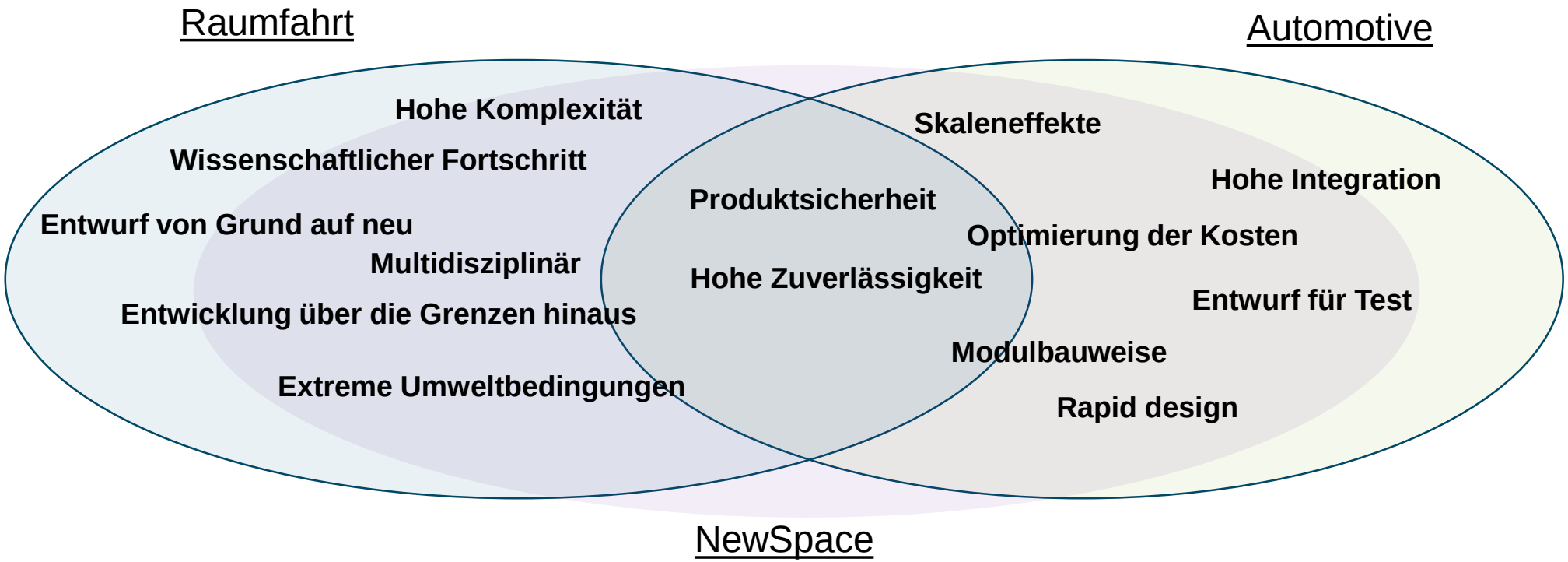
- Kommerzialisierung sorgt für ein Gleichgewicht zwischen Kosten, Leistung, Zeit und Risiko
  - Beschleunigung der Entwicklungszyklen (Entwurf, Herstellung, Test, Einsatz)
  - Vermeidung von kostspieligem Over-Engineering
  - Reproduzierbarkeit zur Erhöhung der Rentabilität der Investitionen
    - Wiederverwendbarkeit
    - Skaleneffekte (Massenproduktion)
  - ➢ Höhere Stückzahlen bei New Space ermöglichen eine neue Ausrichtung der Halbleiterindustrie auf den Raumfahrtsektor (Raumfahrt wird ökonomisch interessant)



Wie die Raumfahrt von anderen Industriesegmenten profitieren kann

z.B. automotive

Merkmale der Innovation



Vorteile des Einsatzes funktionaler Sicherheit in kommerziellen Raumfahrtanwendungen

Agenda

- "New Space" erfordert einen neuen und umfassenden Blick auf die Resilienz der Systemebene
- RAMS vs. IEC61508 funktionale Sicherheit - Gemeinsamkeiten
- System-on-chip (SoC): Vorteile der funktionalen Sicherheit für die Raumfahrt

Standardisierung

Basierend auf IEC 61508

Raumfahrt ECSS/ NASA

- **RAMS** Reliability, Availability, Maintainability, Safety (Dependency)
- **FDIR**- Fault Detection Isolation and Recovery
- Safety Level EEE
- Niedrige Stückzahlen

Luftfahrt DO-254

- Functional Safety
- DAL Design Assurance Level

Prozessindustrie 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
- Hohe Stückzahlen

Maschinenbau DIN EN 62061 DIN EN 13849

- SIL
- Kategorie B,1,2,3,4
- Industrie Engineering
- Lasersysteme auf der Erde

Raumfahrt und IEC61508 teilen den selben Ansatz und das selbe Ziel

RAMS

Reliability: Fähigkeit, eine bestimmte Funktion zu erfüllen, und kann als Entwurfszuverlässigkeit oder auch zur Zuverlässigkeit für den Betrieb angegeben werden

Availability: Fähigkeit, einen funktionierenden Zustand in der gegebenen Umgebung aufrechtzuerhalten

Maintainability: Fähigkeit zur rechtzeitigen und einfachen Wartung (einschließlich Wartung, Inspektion und Überprüfung, Reparatur und/oder Änderung)

Safety: Fähigkeit, während des gesamten Lebenszyklus weder Menschen noch die Umwelt oder andere Vermögenswerte zu schädigen.

IEC61508 Functional Safety

Funktionale Sicherheitsstandards für den Lebenszyklus elektrischer, elektronischer oder programmierbarer elektronischer (E/E/PE) Systeme und Produkte.

Beinhaltet auch RAMS Ansätze

Funktionale Sicherheit bezieht sich auf Sicherheitsfunktionen, kann aber auch auf Grundfunktionen ausgeweitet werden

Vorgegebener Prozess, umfasst spezifische Maßnahmen und Methoden

Schutz vor unannehmbaren Risiken

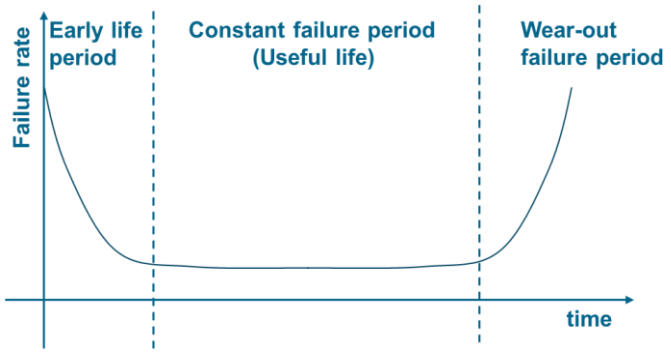
Risiko	=	Schwere des Schadens	x	Wahrscheinlichkeit des Auftretens dieses Schadens

Systematisches und zufälliges Fehler in der Funktionalen Sicherheit

Zufällige Fehler
HW: z. B. Widerstandskurzschluss, Funktionsausfall

... sind grundsätzlich unvermeidbar
... können nicht beseitigt werden, nachdem sie entdeckt wurden
... müssen kontrolliert werden, um ihre Auswirkungen abzuschwächen
... können mit guter Genauigkeit statistisch modeliert werden
... ʎ-Rate, FIT, PFH, PFD, MTTF, etc.

Quantitativer Ansatz
Maßnahmen: Selbstdiagnose, Redundanz, ...

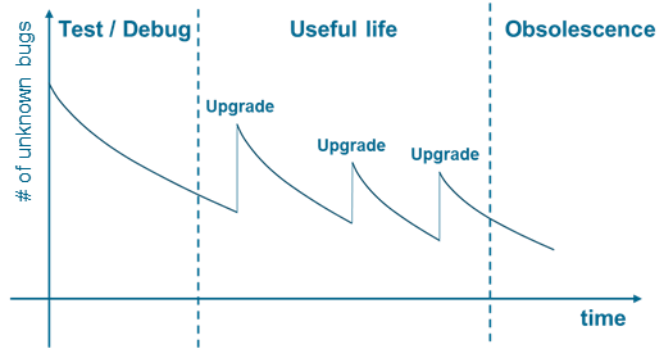


Z.B. Ausfallrate für eine einfache Komponente

Systematische Fehler
HW oder SW: z.B.: Spezifikationsfehler, Software-Bugs

... sind grundsätzlich vermeidbar
... sind im Wesentlichen auf Irrtümer zurückzuführen
... können nach Entdeckung der Ursache beseitigt werden
... können nicht statistisch modeliert werden
... Konzept der Systematischen Fähigkeit/ Anforderung (IEC61508: Skala von SC 1 bis SC 4 → SIL 1-4)
…. Safety Integrity Level (SIL) Sicherheits-Integritätslevel / Sicherheitsanforderungsstufe

Qualitativer Ansatz
Maßnahmen: kontrollierter Prozess, Analyse der installierten Systeme



Z.B. Qualitätslebenszyklus eines Softwareprodukts

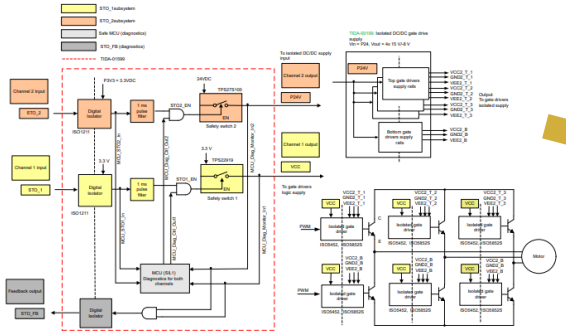
Vorteile des Einsatzes funktionaler Sicherheit in kommerziellen Raumfahrtanwendungen

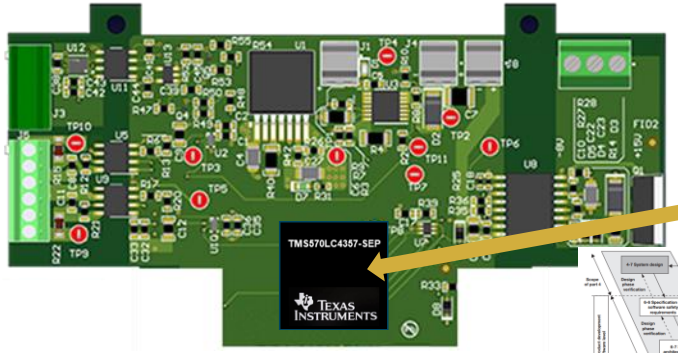
Agenda

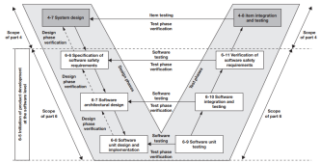
- "New Space" erfordert einen neuen und umfassenden Blick auf die Resilienz der Systemebene
- RAMS vs. IEC61508 funktionale Sicherheit - Gemeinsamkeiten
- System-on-chip (SoC): Vorteile der funktionalen Sicherheit für die Raumfahrt

Wachsende Komplexität auf Systemebene erfordert enge Zusammenarbeit mit der Halbleiterindustrie

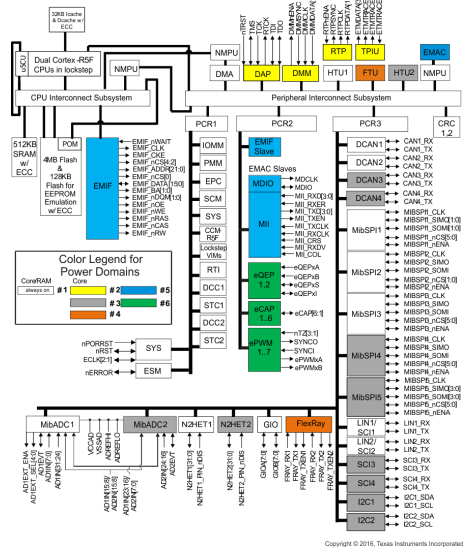
OEM-Verantwortung für hohe Zuverlässigkeit und Entwurf der Funktionalen Sicherheit







Sicherheitskonformes System-on-Chip



- System-on-Chip
  - Muss ausreichende Sicherheitskapazitäten bieten, um den Aufwand zur Risikominderung auf Systemebene zu minimieren
  - Die Grenze des erreichbaren Sicherheits-Integritätslevels des Systems ist vordefiniert

- Der Grad der Integration nimmt ständig zu:
  - Mehr als 100 Millionen Transistoren ermöglichen mehr als 1000 GOPS (Billionen von Operationen pro Sekunde)
  - Die Vermeidung von systematischen Fehlern wird stetig wichtiger

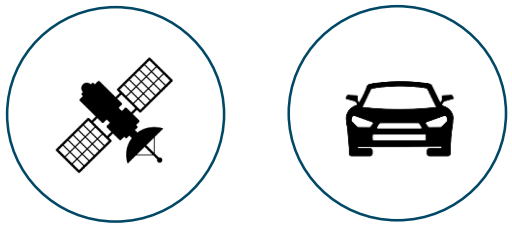
- Hohe Stückzahlen in der Automobilindustrie sind ein starker Antrieb für die Integration von Sicherheits-Funktionsmerkmalen (Selbsttest, Fehlerkorrektur, Taktüberwachung, ...)

Unterstützung der funktionalen Sicherheit durch Mikroelektronik

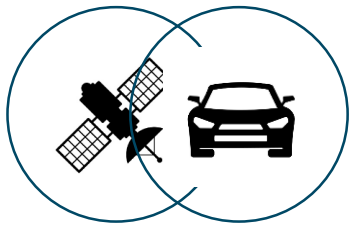
Robustheit	Selbstüberwachung	Validierung & Verifikation
Minimierung der Wahrscheinlichkeit von Ausfällen durch äußere Einflüsse	Vermeidung/Minimierung von Auswirkungen zufälliger Fehler	Vermeidung von systematischen Fehlern in der Hard- und Softwareentwicklung

Die Verwendung einer Komponente in der falschen Umgebung ist ein systematischer Fehler

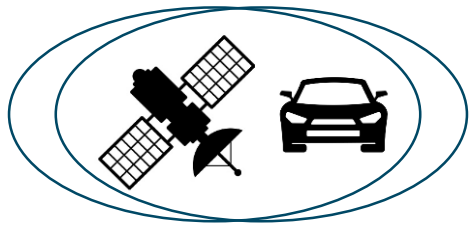
Qualifizierung mit 100%-iger funktionaler Testabdeckung:
- Strahlenbelastung (TID & SEE)
- Temperaturzyklen (Löten & im Orbit)
- Außendruck
- Betriebslebenszyklus
- Vibrationen



Integrated features and IP-blocks
- Diagnosedeckungsgrad
  e.g. loopback mode, Built-in self tests (BIST)
- Schnelle Fehlererkennung zur Minimierung der Fehlertoleranzzeit, e.g. CRC, lockstep
- Autokorrektur, e.g. ECC



Standardisierter Entwicklungsprozess für funktionale Sicherheit
- Schulung und Organisation des Entwicklungsteams
- Qualifizierung von Hardware- und Software-Entwicklungswerkzeugen
- Klar definierte Prüfpunkte für Validierung und Verifikation (V-Prozess)
- Dokumentation und QM

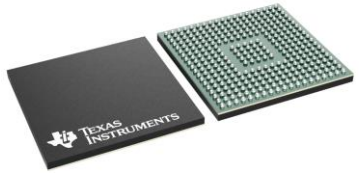


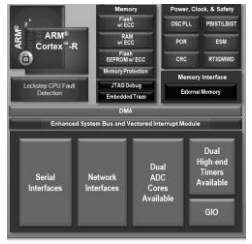
Functional Safety MCU TMS570LC4357-SEP

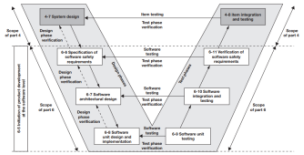
Vollqualifiziert für die Raumfahrt:
- Strahlung: 30 krad / 43 MeV-cm2/mg
- Temperatur Bereich : -55°C to +125°C
- Robuste Materialien
- Belastungsprüfungen, z.Bsp. HAST
- …

Integrierte Hardware-Diagnose:
- Dual-core lockstep CPUs
- ECC für Flash and RAM Speicher
- Built-In Self-Test (BIST)
- Spannungs- und Taktüberwachung
- …

Functional safety design:
- ISO 26262 mit ASIL-D Fähigkeit
- IEC 61508 mit SIL-3 Fähigkeit
- TÜV-zertifizierte Software- und Hardware-Entwicklungsprozesse
- …







Robustheit

Minimierung der Wahrscheinlichkeit von Ausfällen durch äußere Einflüsse

Selbstüberwachung

Vermeidung/Minimierung von Auswirkungen zufälliger Fehler

Validierung & Verifikation

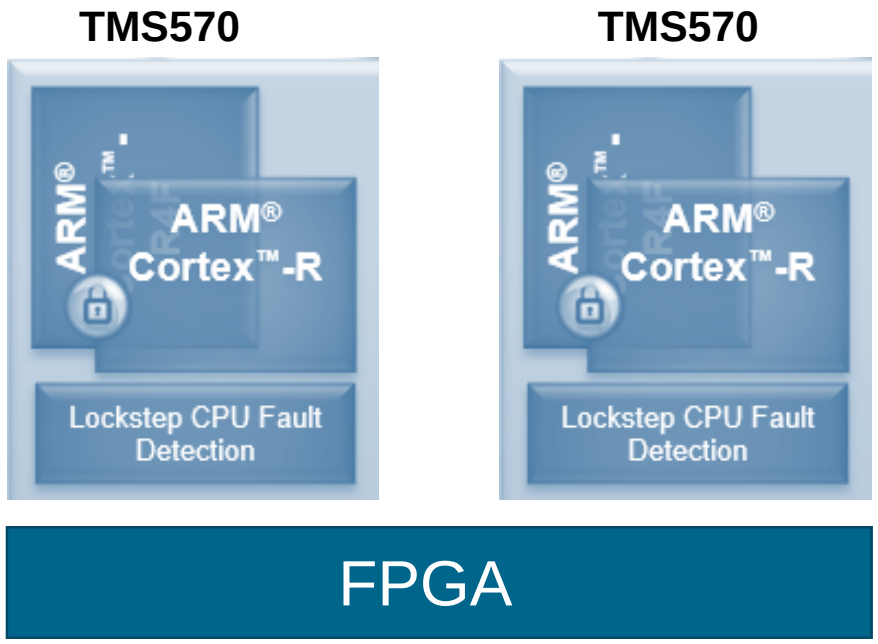
Vermeidung von systematischen Fehlern in der Hard- und Softwareentwicklung

MCUs für funktionale Sicherheit auf dem Mars

Redundante Flugsteuerung mit zwei TMS570 Hercules MCUs

Lock-Step MCU ermöglicht nahezu sofortige Fehlererkennung

- FPGA schaltet auf redundante MCU um



> "Simplicity is prerequisite for reliability."
>
> E. W. Dijkstra

Die Zukunft der Raumfahrt erfordert neues strategisches Denken

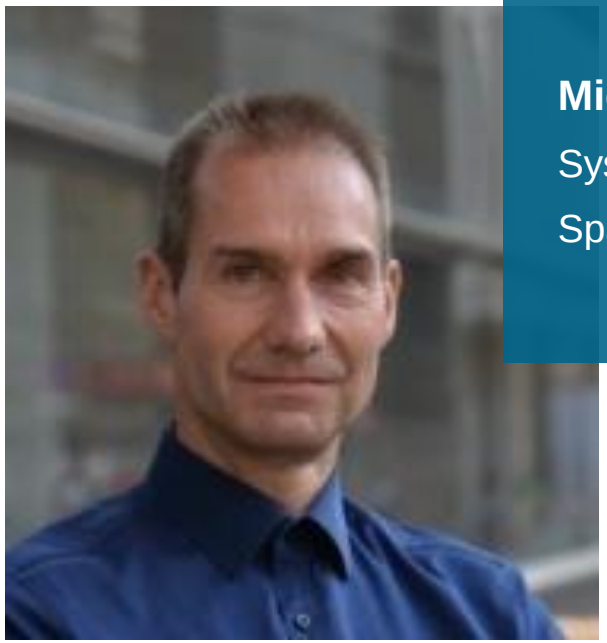
Source: NASA's New Project Looks Beyond Solar System to Look for Earth-like Planets - News18

Ein neuer Ansatz für schnellere Entwicklungszyklen, mehr Kosteneffizienz, mehr Möglichkeiten und dennoch hohe Zuverlässigkeit:

- EEE-Technologien aus anderen Branchen nutzen, z. B. hat die Automobilindustrie große Erfahrung mit:
  - starkem Wettbewerb
  - Massenproduktion
  - Null- Fehlerstrategie (Rückrufe sind fatal)
  - Funktionaler Sicherheit

- Nutzung des Konzepts der funktionalen Sicherheit (IEC61508) für die Verwendung in Raumfahrtprojekten

Der heutige Referent: Michael Seidl Texas Instruments



Michael Seidl
Systems Engineer,
Space and Avionics

Michael hat an der Hochschule München, einen Abschluss als Diplom-Ingenieur für Nachrichtentechnik erworben. Michael hat 28 Jahre Erfahrung in der Halbleiterindustrie gesammelt und war in den Bereichen DSP-Softwaredesign, Applikation, Produktmarketing, Geschäftsentwicklung und Systemtechnik tätig.

Micheal ist Systemingenieur für Luft- und Raumfahrtanwendungen bei Texas Instruments. Er unterstützt Kunden bei ihrer Entscheidungsfindung mit fundierten Systemkenntnissen, kombiniert mit Fachwissen über die Produktangebote von TI.

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

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

Der heutige Referent: Florian Lumpe DLR R&D

Florian Lumpe, DLR
Coordinator Strategic Product Assurance

Florian Lumpe begann seine Karriere in der Luft- und Raumfahrtindustrie mit einem akademischen Abschluss in Maschinenbau und General Management. In seiner derzeitigen Funktion als Koordinator Strategische Produktsicherung am Deutschen Zentrum für Luft- und Raumfahrt in Köln koordiniert er die Integration der Produktsicherung in Projekte.

Zu Florians Aufgaben gehören das Management von technischen Schnittstellen und die Anpassung von gesetzlichen Anforderungen sowie die Konzeption und Durchführung von Schulungen. Als Auditor trägt er dazu bei, die Leistungsfähigkeit des Unternehmens zu optimieren.

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)