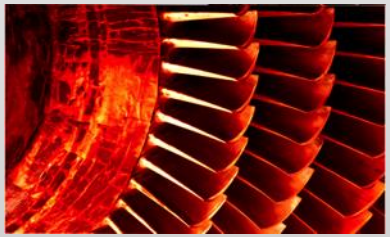
Autonomes Fahren

Nutzung der Luftfahrtindustrie-Erfahrung bezogen auf die Entwicklung von sicherheitsgerichteten Systemen.





Dipl.-Ing. Luft- und Raumfahrt J. Venrath | AvioniQ Engineering GmbH | Regattastraße 185 | 12527 Berlin

- In der Luftfahrt gibt es seit mehr als 50zig Jahren Erfahrung im Umgang mit sicherheitskritischen und komplexen Systemen.
- In der Luftfahrtindustrie wurden hierzu einschlägige Vorgehensweisen, Regelwerke, Zulassungsbedingungen etc. etabliert.
- Die Erfahrungen der Luftfahrt können auf den Bereich Autonomes Fahren übertragen und dort zielführend eingesetzt werden.

AvioniQ Engineering

- verfügt über langjährige umfangreiche Expertise im Bereich sicherheitskritische Systeme.
- verfügt über detaillierte Prozesskenntnisse bei Software und Hardware Entwicklung (SIL 4).
- unterstützt Automotive Kunden bei der Wegbereitung und Umsetzung Autonomes Fahren.
- unterstützt bei der Entwicklung und Umsetzung der Software-Entwicklungsstrategie (SIL 4).
- unterstützt bei der Entwicklung einer Verifikations- und Qualifikationsstrategie (SIL 4).
- unterstützt bei der Entwicklung und Umsetzung der Safety Assessment Strategie (SIL 4), als Grundlage für die sichere Nachweisführung und Risikobewertung.

Anforderungen Automotive autonomes Fahren

Technik	Echtzeit, Fail Safe, fehlertolerante Architekturen und Sensoren, Dissimilarität, Monitoring Konzepte, Redundanz, Reverse Engineering, Standards,....
Sicherheit	„Vollkommende funktionale Zuverlässig“, Reliability, Hazard Analysis, Common Mode Failure, Single Point Failure, EMI, Vernetzung (Datenquellen, Protection, Persönlichkeitsrechte), Catastrophic Events, ...
Recht	Wiener Straßenverkehrskonvention 1968 (WÜ), StVO, EU-Richtlinien (ECE), Produkthaftungsgesetz (ProdHaftG), Datenhoheit, Cracker.
Akzeptanz	Kosten, Vertrauen in die Technik, Marktpotential, Reduktion von Unfällen (menschliches Versagen), verfügbare Versicherungspolicen, ethische Grundsätze (KI), personenbezogene Daten.
Migration	Autonomes Fahren im allgemeinem Straßenverkehr (Kompatibilität zum menschlichen Verhalten), Schnittstellen (HMI), Entscheidungsmuster, ...
Ergonomie	Übernahme des Fahrzeugführers, Rating (e.g. Notbremsung), Entscheidungsfreiheiten.
Infrastruktur	Leitsysteme, Datenquellen und -server, gesonderte Fahrbahnen, Netzwerke, Informationssysteme, Prognostik,Traffic, Software (Updates, field loadable SW), Apps

Quellen: 1, 2, 3, 4

JAR25 §1309 (Die Mutter aller Safety Requirement)

- The equipment, systems, and installations whose functioning is required by the JAR and national operating regulations must be designed to ensure that they perform their intended functions under any foreseeable operating conditions. [….]

- The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that
  (1) The occurrence of any failure conditions which would prevent the continued safe flight and landing of the aeroplane is extremely improbable [….].

  (2) The occurrence of any other failure condition which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions is improbable [….].

  (3) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimise crew errors which could create additional hazards [….].

- Im Software Life Cycle wird die Kritikalität der Software-Funktion anhand der Effekte beim Ausfall eingestuft. Bei der Gefährdung von Menschenleben handelt es sich um ein sogenanntes „Catastrophic Event“ Design Assurance Level A (**DAL-A**). Der Safety Integrity (SIL) Level bestimmt dabei die Softwarearchitektur, Nachweisführung, Testaufwand, Quality Assurance Considerations und ebenso den begleitenden Certification Liaison Process.

- **Autonomes Fahren** kann im Fehlerfall Menschenleben gefährden.

- Die ISO 26262 deckt entsprechende Entwicklungsrichtlinien **nicht** ab, da es bis jetzt keine entsprechende Notwendigkeit gab (WÜ).

Approximate cross-domain mapping of ASIL

Domain	Domain Specific Safety Levels				
Automotive (ISO 26262)	QM	ASIL-A	ASIL-B/C	ASIL-D	-
General (IEC-61508)	(SIL-0)	SIL-1	SIL-2	SIL-3	SIL-4
Aviation (DO-178/254)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
Railway (CENELEC 50126/128/129)	(SIL-0)	SIL-1	SIL-2	SIL-3	SIL-4

Der vermehrte Einsatz von komplexen Systemen einschließlich Software darf nicht zu einer höheren Anzahl an Unfällen oder Todesfällen führen.

- Durch Adaption der Luftfahrtprozesse auf die Anforderung der Automotive Branche, entwickelt AvioniQ Vorgaben, um sicherheitskritische Softwareanwendungen gemäß ihres Kritikalitätslevel zu planen, zu entwickeln, zu implementieren und zu bewerten.

- Die eindeutige Definition von integralen Prozesse sichern die Kontrolle, den korrekten Ablauf und die Übereinstimmung der Software Life Cycle Aktivitäten mit den Vorgaben.

- Die Anzahl der Quality Objectives und deren Nachweise steigen mit der Kritikalität der SW-Funktion. Dazu werden Aktivitäten und Zielvorgaben der spezifizierten Abläufe vorgegeben und den Entwicklungsphasen sowie zuständigen Rollen zugeteilt (e.g. Requirement Validation, SW-Test Engineer).

- Review Gates mit definierten Transitionskriterien ermöglichen die qualitative Bewertung bezüglich Einhaltung von Entwicklungsstandards und Nachweisaktivitäten über die einzelnen Entwicklungsphasen.

- Die Ziele und Dokumente (e.g. Software Accomplishment Summary), die im Software Quality Assurance Prozess vorliegen müssen werden gemäß der Entwicklungsphasen definiert.

- Fehlerfreiheit in komplexen Systemen ist mit vertretbarem Aufwand nicht zu erreichen.
- Luftfahrt: der Verlust einer Funktion, eine Fehlfunktion, ein systematischer Ausfall o.ä., der im schlimmsten Fall zum Verlust von Menschenleben führen kann, ist in der Luftfahrt ein statistischer und in der Auswirkung bewerteter und akzeptierter Fakt.
- Um den §1309 zu erfüllen und die Safety Anforderung (DAL A) der Zulassungsvorgaben z.B. für Softwarefunktionen zu erreichen, sind technische, regulatorische und sicherheitsorientierte Richtlinien für die Entwicklung und Nachweisführung etabliert.
- Für die Zulassung, Auslegung und Entwicklung autonom fahrender Systeme kann die Erfahrungen der Luftfahrt zur Schaffung der rechtlichen Voraussetzungen als Basis dienen.
- Diskussion gesetzlicher Vorgaben kann durch qualitative und quantitative Assessments, Systemarchitekturen für sicherheitskritische Systeme, Verfügbarkeitszahlen für Funktionen, Fehlerklassifikationen, Monitorfunktionen sowie etablierte Autopilot-funktionen mit bestehendem Mensch-Maschine-Interface unterstützend begleitet werden.

*** Siehe Slide 4**

- Hoch-integrierte sicherheitskritisch Systeme werden komplexer, haben mehr Interaktionen mit externen Schnittstellen und teilen sich oft eine zentrale Datenbasis.
- Allein durch die größere Anzahl von Komponenten sinkt die System-Verfügbarkeit.
- Inverse Beziehung zwischen der Fehlerwahrscheinlichkeit (Ausfall einer Funktion) und dem Gefährdungsgrad für den Nutzer, erhöhen den Entwicklungsaufwand.
- Analysen zeigen: bezogen auf 100 Systeme alle 10E9 Flugstunden ein Totalverlust, bei dem ca. 10% der Unfälle auf Systemversagen oder Systemfehler beruhen.
- Damit tritt das „Catastrophic Event“ statistisch bei einer Milliarde Flugstunden auf.

Das wird von den Behörden akzeptiert!

- Einschätzung des Betriebsrisikos für Behörden: Vorlage umfangreicher statistischer Analysen (Safety Assessments), in denen den operativen Betriebszuständen mit Funktionsverlust der Gefährdungsgrad entgegengestellt wird (inklusive Autopilot).
- Das Ergebnis gibt dem Entwickler eine statistische Größe, für welche Funktion er eine wie hohe Verfügbarkeit gewährleisten muss.

- Sicherheits- und Zuverlässigkeitsanforderungen bestimmen maßgeblich die Entwicklung und Auslegung von sicherheitskritischen Systemen.

- Definition des Safety Management Prozess zur Messung der Safety Performance im Produkt Autonomes Fahren, um daraus Risikokontrollstrategien abzuleiten.

- Definition der Sicherheitsanalyse Methoden zum Nachweis des Risikopotentials bei Verlust von Funktionen und Erfüllung der Zulassungsforderungen für Autonomes Fahren.

- Definition von Sicherheitsstandards, um zu gewährleisten, dass die Software- und Systemarchitektur die Sicherheitsstandards erfüllt und dadurch kostspielige Designänderungen vermieden werden.
  - Gefahrenanalyse im Rahmen des Functional Hazard Assessment (FHA)
  - Failure Modes and Effects Analysis (FMEA)
  - Common Cause Analyses (CCA)

- Für die Qualitätsüberprüfung von komplexen Systemen existieren zahlreiche Validierungs- und Verifikationsmethoden, die bezogen auf das Ausfallrisiko eine ausreichende Test Coverage und Traceability Aussage erzeugen müssen.

- Definition der Verifikation und Validation Strategie im sicherheitsgerichteten Softwareprozess.

- Erstellen notwendiger Richtlinien, Review- und Quality Gates, für die Validation, Verifikation und Annahme sicherheitsgerichteten System- und Softwarelösungen.

- Qualitätssicherung im Entwicklungs- und Verifikationsprozess durch Einsatz von Fehlerpotential und Regressionsmethoden

- Definition von Test- und Verifikationsklassen (e.g. ist die mathematische Verifikation, Objektvarianten, etc.).

- Akzeptiertes „Catastrophic Event“ bei TBD Stunden.
- Functional Hazard Analysen mit Bewertung der Ausfallwahrscheinlichkeit und des Gefährdungsgrad bei Funktionsverlust für alle Betriebszustände „autonomes Fahren“.
- Eindeutige Definition der Zulassungsvoraussetzungen „autonomes Fahren“.
- Mensch Maschine Interface
  - Echtzeitdarstellung des Betriebszustands (Fahrerinformation)
  - Datenechtheit der Informationen Anzeigeelemente (LCD Cluster Panel).
  - Monitorfunktionen („predictable Events“)
  - „A Priori“ Eingriffsmöglichkeit des Fahrzeugführers in autonome Funktionen
- Fail Safe Verhalten im autonomen Betrieb.
- Standardisierung als Schlüsselfaktor für kooperierende Systeme.

- Standardisierte Means of Compliance (Gleichgewicht zwischen Durchführungsbestimmungen, Zulassungsspezifikationen und annehmbaren Nachweisverfahren)

- Zulassungsrelevante Standards SW Coding und Test, HW Entwicklung e.g. FPGA.

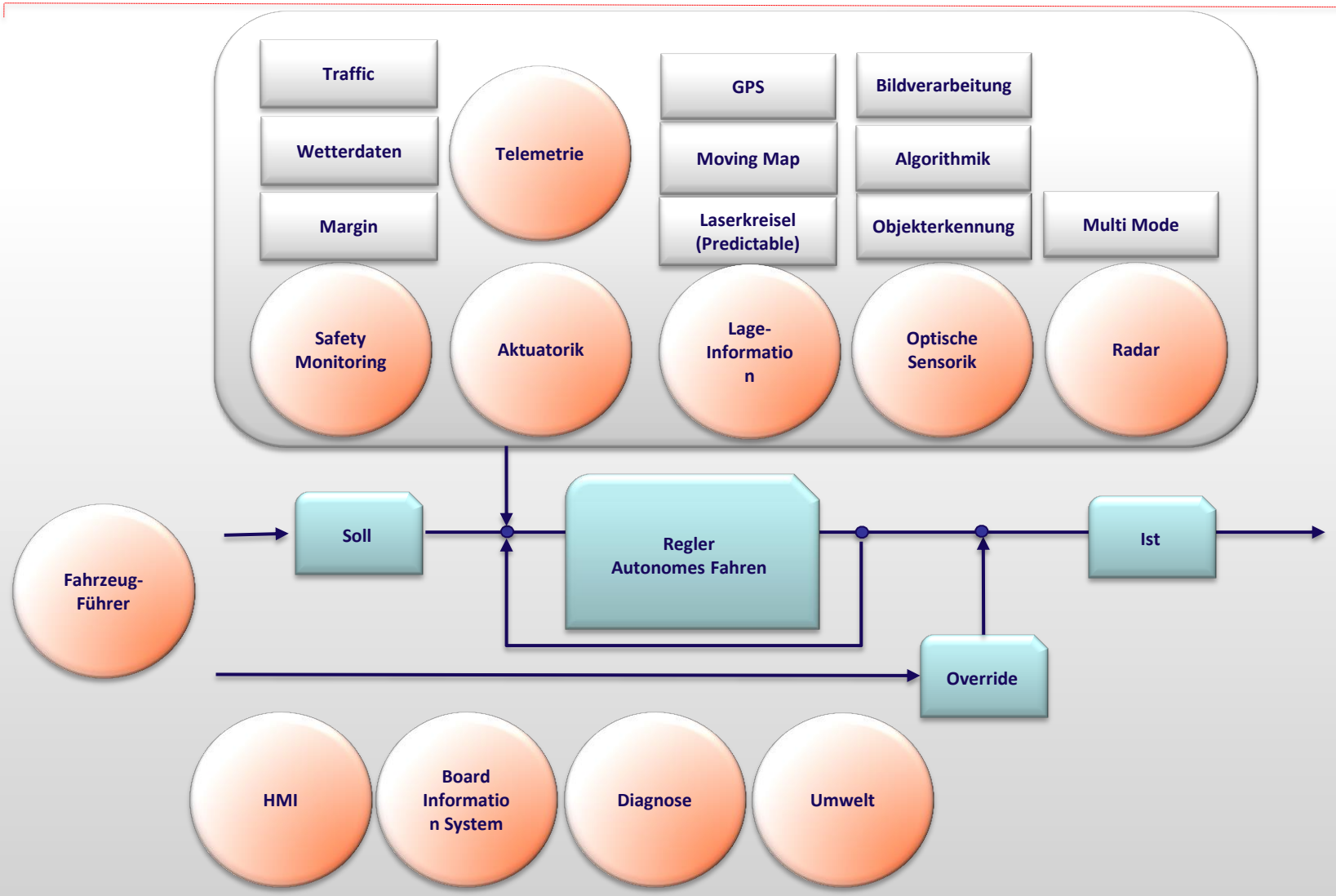
- Zulassungsrelevante Testrichtlinien
  - Environment (e.g. Power Interrupt, EMV, Alterung FPGA, ...).
  - Test Coverage in Abhängigkeit der Verfügbarkeitsanforderung.
  - Regressionsanalysen um Systemschwächen aufzudecken.

- Life Cycle Prozesse
  - Change Management (e.g. SW Issue/Fahrzeugtyp).
  - Maintenance (Kompatibilität SW und HW über das Fahrzeugleben).
  - Obsoleszenzmanagement (Zulassungsrelevant).

- Designvorgaben e.g. Fehlertoleranz, Safety Margins, Fehlerpfade, ...

- Standardisierte, hoch-integrierte Modulare Steuereinheiten.
- Redundanz, Back-up Systeme, Funktionsseparierung, Dissimilarität.
- Konzepte für die Erkennung von Latenten Fehlern (e.g. Redundanter Pfad).
- Fehlerwarnungen und Anzeigen für den Abbruch „autonomes Fahren“.
- Standardisierte und eindeutige Sequenz bei Abbruch des autonomen Fahrens durch eine Fehlerwarnung für den Fahrzeugführer (Aural Warning, Indications e.g. green, yellow, amber).
- Konzept für die gesicherte Verfügbarkeit von Lagedaten, GPS, Maps, Traffic (Datenbank?)
- Upload und Zugriff auf die Steuerungssoftware (Upload field loadable Software).

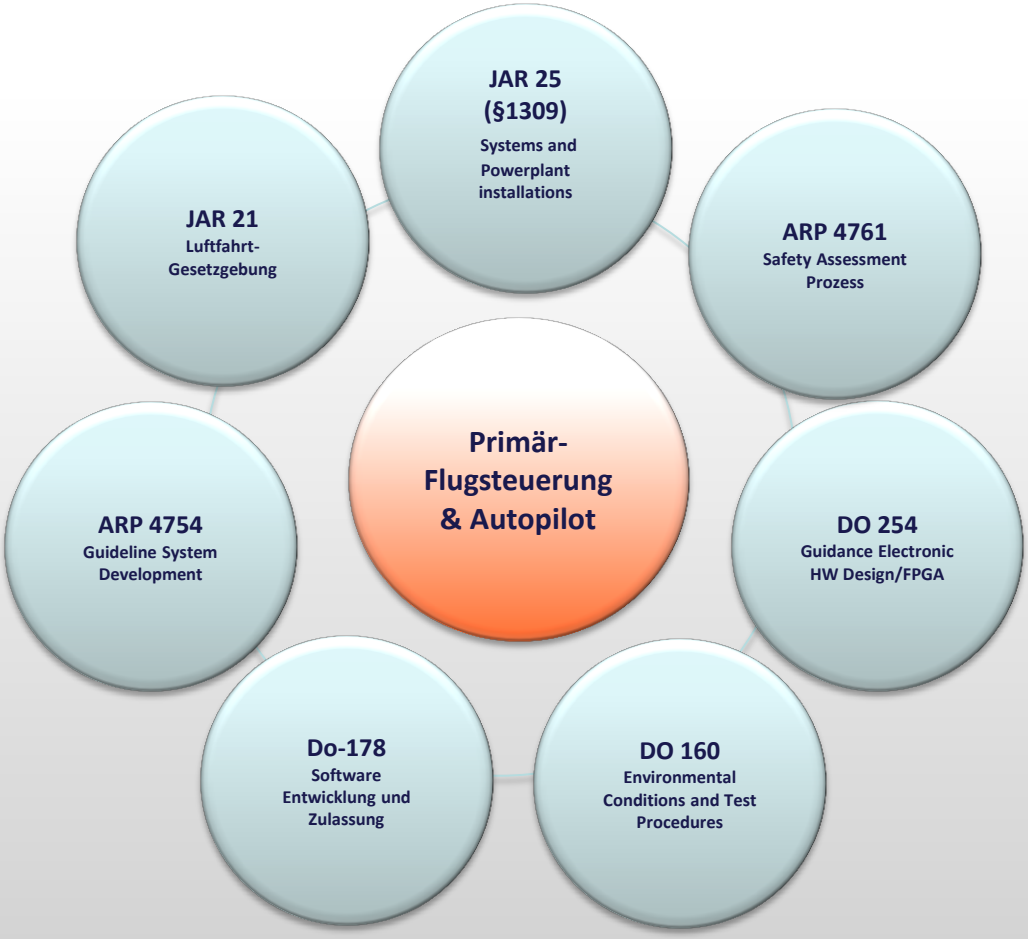
Sicherheitsrelevante Software-Funktionen



Standards Safety-related Design Luftfahrt

EASA *

Musterzulassung und Lufttüchtigkeitsanforderungen von Luftfahrtzeugen



* EASA is the European Union Authority in aviation safety. The main activities of the organisation include the strategy and safety management, the certification of aviation products and the oversight of approved organisations and EU Member States.

Möglicher „Way Ahead“

- Gemeinsamer Work Shop
  - Diskussion der Anforderungen Automotive vs. Luftfahrt.
  - Architekturen und Sicherheitskonzepte.
  - Zulassungsvorschriften, Nachweise, Rechtslage und deren Einhaltung.
  - Identifikation von Synergien aus Luftfahrtlösungen.
  - Mögliche Adaption für Automotive.
  - Weitere Vorgehensweise.
- Integriertes Team
  - Strategiepapier
  - Erste Konzepte

Kontaktinformationen

Sie haben in Ihrem Unternehmen einen möglichen Einsatzbereich für ein Interim Management Mandat Autonomes Fahren identifiziert? Dann lassen Sie mich Sie in einem persönlichen Gespräch davon überzeugen, meine fachlichen und menschlichen Erfahrung in Ihr Mandat einzubringen.

AvioniQ Engineering GmbH
CEO Dipl.-Ing. Luft- und Raumfahrt
Hans Joachim Venrath
Regattastraße 185
D-12527 Berlin Germany

phone: +49 (0) 30 516 44 185
fax: +49 (0) 30 516 44 186
cell phone: +49(0)1708509825
mail: info@avioniQ.de
Web: AvioniQ Interim Management