



Funktionale Sicherheit - ISO 26262/IEC 61508 - Einsatz und Nutzen

Auf Nummer sicher kann man nicht nur gehen, sondern eben auch fahren. Das beweist die Tatsache, dass elektronische Sicherheits- und Assistenzsysteme einen Großteil der Innovationen in der Fahrzeugindustrie ausmachen. Die Weiterentwicklung und Verbesserung der Systeme hat gerade in den vergangenen Jahren ein großes Plus bei der Verkehrssicherheit gebracht.

Dabei ist es von enormer Wichtigkeit, dass diese Sicherheits- und Assistenzsysteme nicht nur Schritt halten mit der Entwicklung der stetig wachsenden Komplexität elektronischer Komponenten in Fahrzeugen, sondern einen Schritt voraus sind, was das Erkennen, Einschätzen und Abstellen möglicher Fehlfunktionen angeht.

Ist eine sicherheitsrelevante Komponente von einer solchen Fehlfunktion betroffen, können im schlimmsten Fall Menschen zu Schaden kommen. Würde z.B. ein ESP-Steuergerät in einem Kraftfahrzeug bei zügiger Fahrt unberechtigt eine Vollbremsung auslösen, könnte dies zu einer Massenkarambolage führen.

Um das Risiko von Gefahr bringenden Fehlfunktionen von sicherheitsrelevanten Elektronik-Systemen zu minimieren, sollten diese unter Berücksichtigung einschlägiger Normen entwickelt werden. In der Vergangenheit galt die Empfehlung, elektrische/elektronische Systeme, die eine sicherheitsrelevante Funktion in Automobilen ausführen und deren Ausfall ein maßgebliches Risiko für Mensch oder Umwelt bedeutet, auf Basis der **IEC 61508** zu entwickeln.

Diese Norm ist generisch auf sicherheitsrelevante Produkte, wie ein Sicherheitsschaltrelais für eine Notstromabschaltung, anwendbar. Da dieser Standard für moderne Automotive-Anwendungen nicht ausreichend bzw. nicht spezifisch genug ist, wurde eine neue Norm erstellt.

Zu den Anwendern dieses Standards gehören Automobilhersteller, Automobilzulieferer und Prüfinstitute. Möchte beispielsweise ein **Automobilhersteller oder -zulieferer** ein sicherheitsrelevantes System bzw. eine Komponente entwickeln, muss dies anhand einer **Sicherheitsnorm wie der ISO 26262** erfolgen.

Um die funktionale Sicherheit des Produkts zu gewährleisten, wird von der ISO 26262 ab einem entsprechenden Sicherheitslevel gefordert, dass eine von der Entwicklung organisatorisch unabhängige Stelle (z. B. ein externes Prüfinstitut, u. U. aber auch eine interne QM-Stelle) hinzugezogen wird. Eine Prüfung durch eine für ISO 26262 gemäß EN ISO/IEC 17025 akkreditierte Prüfstelle kann dann neben dem Sicherheitsnachweis auch dem Reduzieren der Risiken im Bereich der Produkthaftung im juristischen Sinn dienen.

Die ISO 26262 ist nach einhelligem Verständnis der deutschen Experten zur funktionalen Sicherheit als Beitrag zum Stand der Wissenschaft und Technik in Bezug auf die funktionale Sicherheit von Straßenfahrzeugen anzusehen (Konsens bei der letzten Fachtagung zur funktionalen Sicherheit).

Die ISO 26262 wird aus zehn Teilen bestehen, die folgende Inhalte abdecken:

1. Vokabular
2. Management der funktionalen Sicherheit
3. Konzeptphase
4. Produktentwicklung: Systemebene
5. Produktentwicklung: Hardwareebene
6. Produktentwicklung: Softwareebene
7. Produktion, Betrieb und Außerbetriebnahme
8. Unterstützende Prozesse
9. **ASIL- und sicherheitsorientierte Analysen**
10. Guideline (nur informativ)

Wir leisten Trainings, Schulungen, Projektbegleitung und beraten der Auswahl und Einführung von Software-Systemen.

- ✓ Einführung von Methodik und Prozessen der funktionalen Sicherheit aufbauend auf **Standards wie IEC 61508, ISO 26262**
- ✓ Safety-Analysen mit Methoden u. a. **FMEA, FTA, FMEDA**
- ✓ Review von Sicherheitskonzepten und Überprüfung sicherheitskritischer Systeme und Komponenten
- ✓ Einführung und Durchführung von Safety-Prozessen
- ✓ Sicherheitsanforderungen entwickeln, spezifizieren und prüfen
- ✓ Einführung von Strategien und Vorgehensweisen zur Gewährleistung von Informationssicherheit in technischen Systemen, denn funktionale Sicherheit verlangt durchgängige Informationssicherheit
- ✓ Schulung und Coaching von **Safety-Managern und -Ingenieuren**

Rechtliche Einordnung der ISO 26262

Aus der vorherrschenden Gesetzeslage ergibt sich für den Hersteller von Verbraucherprodukten (hier Straßenfahrzeuge) eine Verkehrssicherungspflicht, nach der Produkte nur dann in Verkehr gebracht werden dürfen, wenn sie die Sicherheitserwartungen erfüllen, die der Verbraucher nach dem Stand von Wissenschaft und Technik zum Zeitpunkt des In-Verkehr-Bringens berechtigterweise erwarten darf. Eine Norm trägt zu ihrem Veröffentlichungszeitpunkt zum vorhandenen Stand von Wissenschaft und Technik bei.

Wir sollten reden...

... und zwar, wenn Sie Fragen zu unserem Einsatz als **Trainer und Berater für FMEA haben, wenn Sie Informationen zu den Themen Risikomanagement oder APQP wünschen.**

Oder wenn Sie unschlüssig sind. Nehmen Sie einfach Kontakt zu uns auf.

Wo erhalte ich weitere Informationen rund um die Themen FMEA, Risikomanagement, Qualität und APQP?

Informationen zum Thema FMEA und Risikomanagement im Pharma und Medizintechnik Umfeld erhalten Sie hier: <https://www.fda-kontor.de/>

Weitere Informationen zu den Themen Reklamationsmanagement und Qualität erhalten Sie hier: <https://www.qm-kontor.de/>

Weitere Informationen zu den Themen APQP, Projektmanagement und Qualitätsvorausplanung erhalten Sie hier: <https://www.apqp-kontor.de/>

Wo erhalte ich weitere Informationen rund um die Themen von Seminar-Terminen, Inhalten und Veranstaltungsorten?

Alle Informationen zu unseren Trainings und Seminaren erhalten Sie auf unserem [Seminar- und Trainings-Portal Seminar Plenum](#)

Wo erhalte ich Antworten auf häufig gestellte Fragen?

Alle Fragen und Antworten zu häufig gestellten Fragen erhalten Sie hier in [Glossar und „FAQ“ FAQ-Datenbank](#). Sie haben Fragen oder Anregungen? Wir freuen uns auf Ihr Feedback und die Gespräche mit Ihnen. Gerne nehmen wir Ihre Anregungen und Fragen mit in die Datenbank auf.