Der Unterschied zwischen IEC 61508 und ISO 26262

- **Die IEC 61508-Reihe ist die Sicherheitsgrundnorm für funktionale Sicherheit und die ISO 26262 die sektorspezifische Ausprägung für die Automobilindustrie.**
- **Bei der Erstellung der ISO 26262 wurden die Grundsätze der IEC 61508 übernommen, an einigen Stellen gibt es jedoch wesentliche Abweichungen.**
- **Wir haben sie zusammengestellt in einer studentischen Arbeit an der Hochschule Darmstadt.**

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbeit
FACHBEREICH ELEKTROTECHNIK
UND INFORMATIONSTECHNIK

Normenvergleich zwischen DIN EN 61508:2011 und ISO 26262:2018

Teamprojekt im Modul M8 im Studiengang Zuverlässigkeitsingenieurwesen
Wintersemester 2019/2020

Projektteam

- Thomas Becker Matr.-Nr.: 763586
- Fabian Dorn Matr.-Nr.: 759816
- Johannes Schmidt Matr.-Nr.: 759780
- Andreas Weber Matr.-Nr.: 759818

Betreuung: Ingo Rolle, Lehrbeauftragter im Fachbereich EIT

Projektbericht vom 29. Februar 2020

Ingo Rolle, im September 2021

Der Unterschied zwischen IEC 61508 und ISO 26262

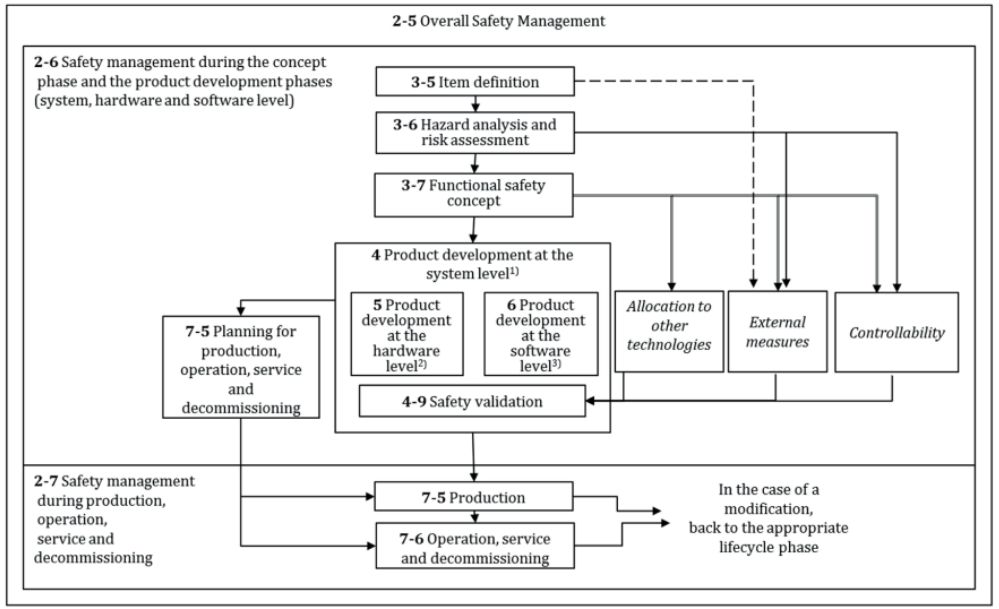
Das sind z.B.

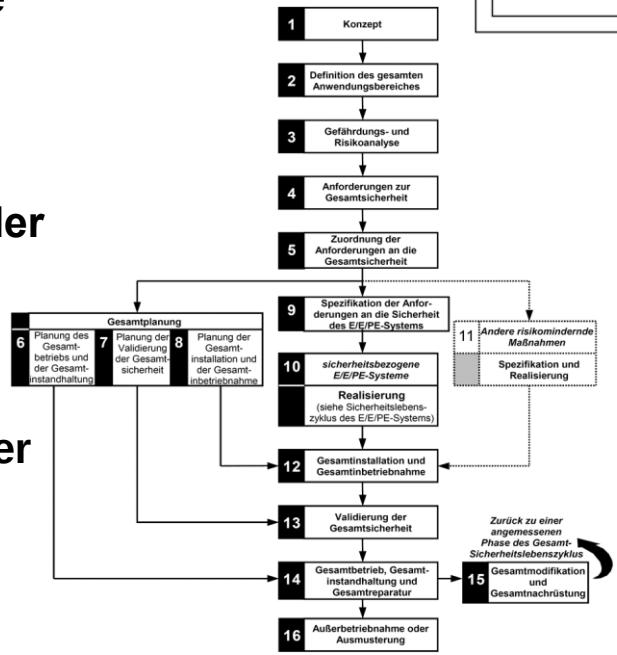
- **Die unterschiedlichen Metriken ASIL und SIL**
- **andere Lebenszyklen**
- **andere Ausfallmodelle**
- **andere Kennziffern zur Begrenzung zufälliger Bauteilausfälle**
- **andere Kennziffern zur Herleitung der Architekturbeschränkungen (Redundanzgrad)**

Einige Unterschiede erklären sich vor dem Hintergrund des Automobilgeschäftes, denn die IEC 61508 wurde vor dem Hintergrund von Einzelanlagen geschrieben.

Eine Tendenz zum „Weichspülen“ in die eine oder andere Richtung haben wir nicht feststellen können.

Der gravierendste Unterschied liegt jedoch in der Wahl des Betrachtungsgegenstandes.





Ingo Rolle, im September 2021

Der Unterschied zwischen IEC 61508 und ISO 26262

Nach IEC 61508 muss eine Anlage gesamthaft untersucht werden.

7.3.2.1 Die Grenze der EUC und des EUC-Leit- oder Steuerungssystems muss definiert werden, um alle Einrichtungen und Systeme zu berücksichtigen (einschließlich Menschen, wo dazugehörig), die mit den relevanten Gefährdungen und Gefährdungssituationen in Verbindung stehen.

Z. B. kann eine HAZOP-Analyse entlang des Materialflusses gemacht werden, um alle Gefährdungen aufzufinden.

EUC = Equipment under Control

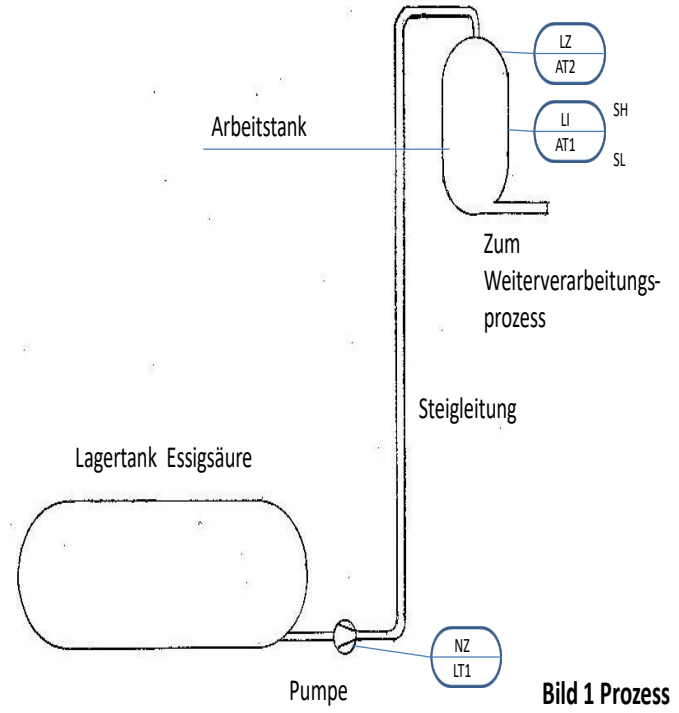


Bild 1 Prozess

Gefährdung (EUC-Risiko)	Ablauf	Ursache
Trockenlauf Pumpe NZLT1	Lagertank wird leer	
Überlauf Lagertank	Überfüllung durch anliefernden LKW	Füllstandsanzeige Lagertank fehlerhaft
Überlauf Lagertank	Flüssigkeitssäule drückt in den Tank zurück	Rückschlagventil festgeklemmt
Überfüllung Arbeitstank	Versagen Steuerung	Programmfehler, Kabelfehler, SPS defekt

Ingo Rolle, im September 2021

Der Unterschied zwischen IEC 61508 und ISO 26262

Statt EUC finden wir in der ISO 26262 den Begriff des Items. Für die Wahl der Betrachtungsgrenze gibt es keine konkreten Bedingungen. Es scheint nicht üblich zu sein, das ganze Automobil als Item zu definieren und auch nicht das System Automobil + Straße.

Stattdessen werden einzelne Funktionsbereiche betrachtet, wie z.B. Fensterheber oder Bremssystem.

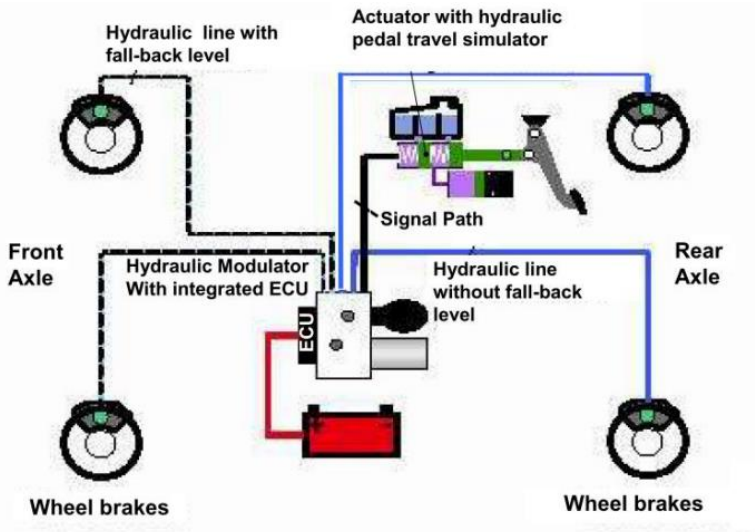
Auszug aus ISO 26262-3:2018

NOTE 2 Hazards resulting only from the item behaviour, in the absence of any item failure, are outside the scope of this document.

6.4.2.2 The hazards shall be determined systematically based on the possible malfunctioning behaviour of the item.

Es geht also nur um mögliche Ausfälle des Items (Bremse, Fensterheber), nicht um eine gesamthafte Betrachtung des Automobils.

Beispiele für Items nach ISO 26262



Bilder von Dr. Rudolph/Continental AG

Der Unterschied zwischen IEC 61508 und ISO 26262

Doch halt, sagen wir als 65108/61511-Anwender, ist das zu schmalspurig gedacht?

Machen wir einmal ein Gedankenexperiment, betrachten wir das Gesamtsystem Fahrzeug-Straße, machen eine HAZOP-Analyse entlang des Fahrweges, sagen wir auf der Fahrt zwischen Mannheim und Darmstadt. Berücksichtigen wir alle möglichen Gefährdungen.

kein
mehr
weniger
zusätzlich
Teil von
rückwärts
etwas anderes

Doch wenn es zu den risikomindernden Maßnahmen kommt, ist das Ergebnis stets das gleiche:

Gefährdung (EUC-Risiko)	Ablauf	Risikomindernde Maßnahme
Keine Haftreibung mehr zwischen Rad und Straße	Regen, Aquaplaning	Fahrer muss aufpassen und Fahrweise anpassen
Keine Haftreibung mehr zwischen Rad und Straße	Glatteis	Fahrer muss aufpassen und Fahrweise anpassen

Bilder von Pixabay

Der Unterschied zwischen IEC 61508 und ISO 26262

Was war der Fehler?

IEC 61508 (und auch IEC 61511) betrachten hauptsächlich autonome Schutzsysteme (wenn auch, verglichen mit einem autonomen Fahrzeug, mit geringem Funktionsumfang.

Die Systeme im Automobil heute (Stand ISO 26262, 2. Ausgabe) sind überwiegend Assistenzsystem. Die Betrachtung des Automobils insgesamt ist nicht der Job der funktionalen Sicherheit, das wurde bereits vorher von anderen gemacht (Ergonomie).

Die Anwendung der gesamthaften Risikoanalyse nach dem Muster für autonome Systeme auf ein Assistenzsystem bringt wenig. Ein Ansatz mit Ergonomie und unter Berücksichtigung des Menschen als Akteur ist stattdessen notwendig.

Doch beim Übergang der Automobiltechnik zu autonomen Systemen gibt es nun eine Lücke: jetzt muss der Betrachtungsumfang erweitert werden und wirklich alle möglichen Einflüsse im Rahmen der funktionalen Sicherheit betrachtet werden.

Die Kollegen aus der Automobiltechnik fragen sich, ob die Sicherheitsfunktionen richtig definiert sind:

Safety of intended functionality = SOTIF

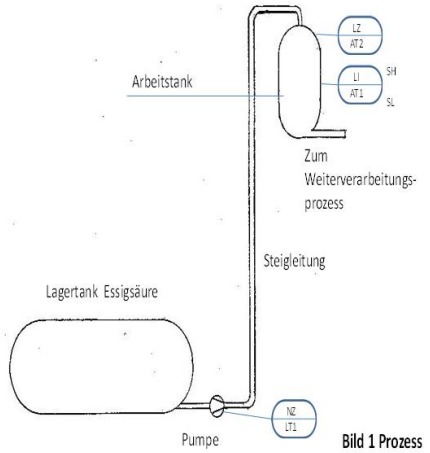


Bild 1 Prozess

Ingo Rolle, im September 2021

Bild von Pixabay

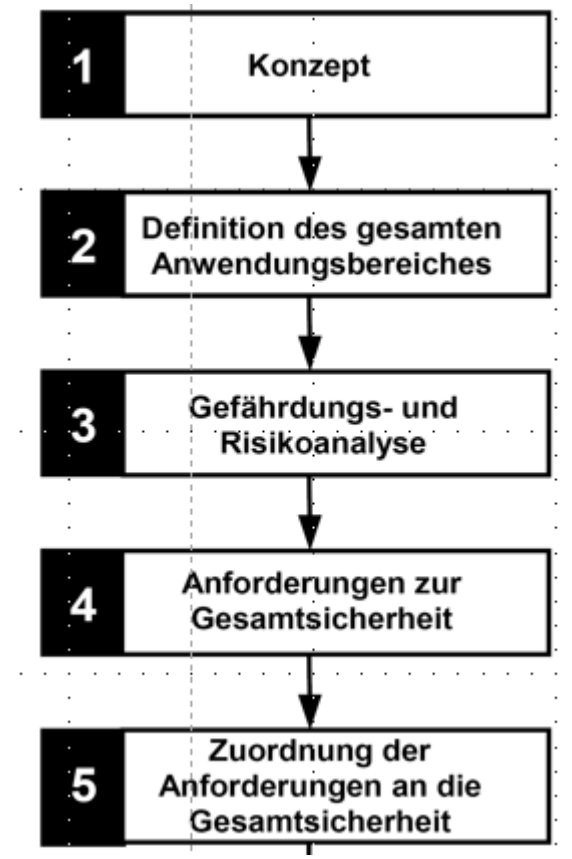
Der Unterschied zwischen IEC 61508 und ISO 26262

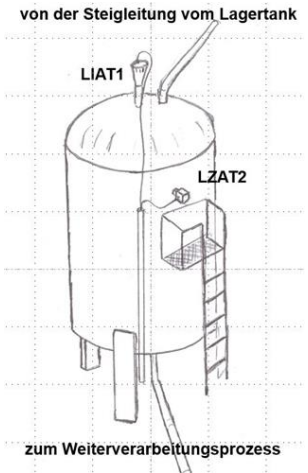
Ich vertraue schon darauf, dass die Kollegen aus der Automobiltechnik den richtigen Weg einschlagen werden. Allerdings frage ich mich, ob die Definition wirklich so kompliziert sein muss:

The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF). (aus ISO/PAS 21448:2019, Road vehicles — Safety of the intended functionality)

In einem Mittelpunkt der SOTIF steht die unbestimmte Frage, wie eine Sollfunktion zu spezifizieren, zu entwickeln, zu verifizieren und zu validieren ist, sodass sie als ausreichend sicher angesehen werden kann. (aus Wikipedia).

Vielleicht könnte eine passende Terminologie auch einfach aus dem oberen Teil des Sicherheits-Lebenszyklus nach IEC 61508-1 und den zugehörigen Anforderungen gewonnen werden?





Ingo Rolle, im September 2021

Bild von Pixabay