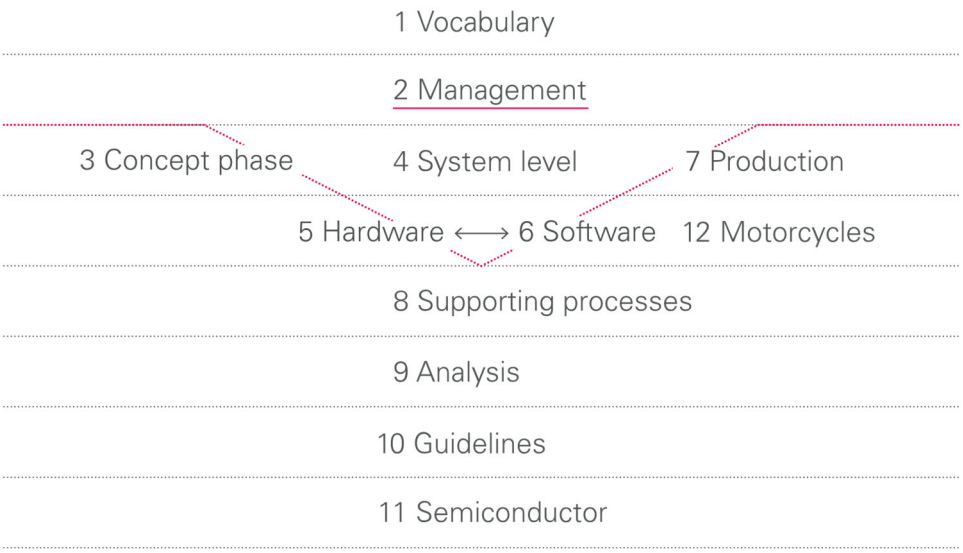
KUGLER MAAG CIE

Management der Funktionalen Sicherheit

nach ISO 26262:2018; eine Einführung

Dr. Erwin Petry



Lernen Sie funktionale Sicherheit mit Kugler Maag Cie GmbH

1. Version – August 2020

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Über dieses Whitepaper

Dieses Whitepaper enthält dieselben Inhalte, die ich in meinem Anfängervideo zur funktionalen Sicherheit auf YouTube behandelt habe.

https://youtu.be/BF8DAvAuYNM

Sowohl das YouTube-Tutorial als auch dieses Dokument behandeln die Kernkonzepte und sind in keiner Weise vollständig. Diese Veröffentlichung wurde nur zur grundlegenden Orientierung erstellt. Bitte handeln Sie nicht nach den Angaben in diesem Dokument, ohne eine weiterhergehende professionelle Beratung zu erhalten. Der Herausgeber, die KUGLER MAAG CIE GmbH, haftet nicht für Schäden, die durch die Verwendung der in diesem Bericht enthaltenen Informationen entstehen.

Wenn Sie mehr über funktionale Sicherheit lernen möchten und ein Experte zum Thema werden möchten, besuchen Sie eines unserer Trainings:

https://www.kuglermaag.de/trainings/funktionale-sicherheit/

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Über den Autor

Erwin Petry gehört zu den Gründungsmitgliedern von Kugler Maag Cie. Er ist Partner und Principal. Seine Kunden hat er im Automotive-Bereich, in der Industrie und in der Finanzbranche. Er ist SCAMPI Lead Appraiser für CMMI. Er ist Functional Safety Expert (TÜV Rheinland) und hat die Entwicklung der ISO 26262 zur funktionalen Sicherheit von Straßenfahrzeugen seit fast 20 Jahren vom ersten Tag an miterlebt. Er bildet Functional Safety Manager und Engineers aus, berät in Projekten, assessiert Produktentwicklungen und publiziert zur funktionalen Sicherheit.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Motivation

Es ist eine weit verbreitete Meinung, dass die funktionale Sicherheit nur eines von vielen Themen ist, die der Projektleiter bei der Entwicklung von Elektronik für Fahrzeuge koordinieren muss.

Mit anderen Worten: Wer das Projektmanagement beherrscht, kann auch das Management der funktionalen Sicherheit übernehmen. Seien Sie vorsichtig: Die Erfahrung zeigt, dass dieser Glaube gegen Ende des Projekts zu massiven Problemen führt, weil die Sicherheit des Produkts nicht nachgewiesen werden kann. Ein Sicherheitsnachweis ist nur möglich, wenn die Organisation Vorkehrungen getroffen hat, und eine Reihe von Dingen während der Entwicklungszeit berücksichtigt werden. Es gibt keine funktionale Sicherheit, wenn man die funktionale Sicherheit nicht managt.

Werfen wir einen Blick auf die ISO 26262: Teil 2 ist speziell dem Management-Aspekt des gesamten Sicherheitslebenszyklus gewidmet. Teil 2 zeigt insbesondere wie das Thema der funktionalen Sicherheit gehandhabt werden soll.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

INTERNATIONAL STANDARD

ISO 26262-2

Second edition
2018-12

Road vehicles — Functional safety —

Part 2:
Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —
Partie 2: Gestion de la sécurité fonctionnelle

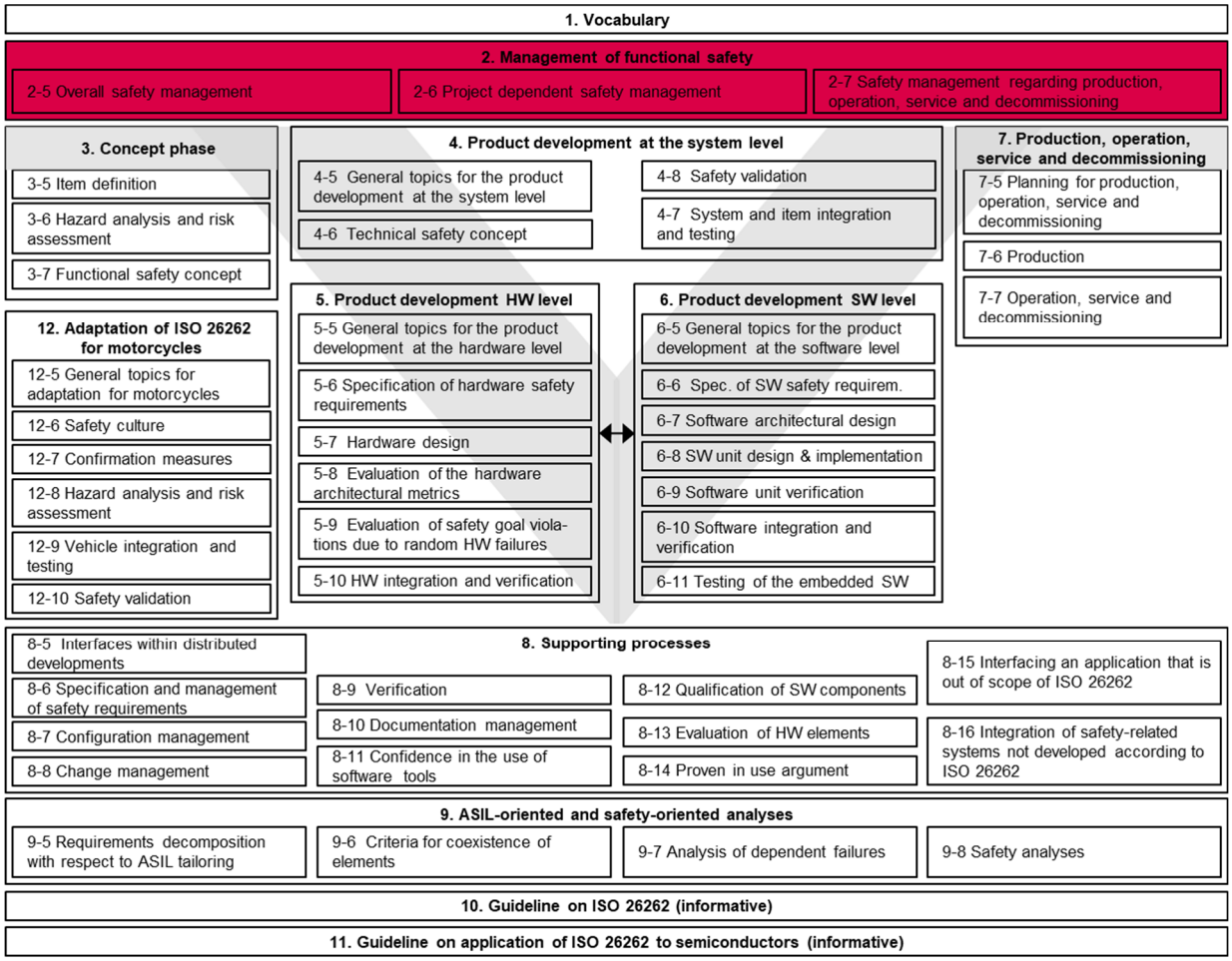
Deckblatt des 2. Teils der ISO 26262:2018

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

ISO 26262:2018 Teil 2 – Management der Funktionalen Sicherheit

In Teil 2 finden Sie drei Klauseln mit Anforderungen. Der erste davon bezieht sich auf die Entwicklungsorganisation. Der zweite ist für jedes Entwicklungsprojekt relevant und der dritte bezieht sich auf die Phase nach der Entwicklung.

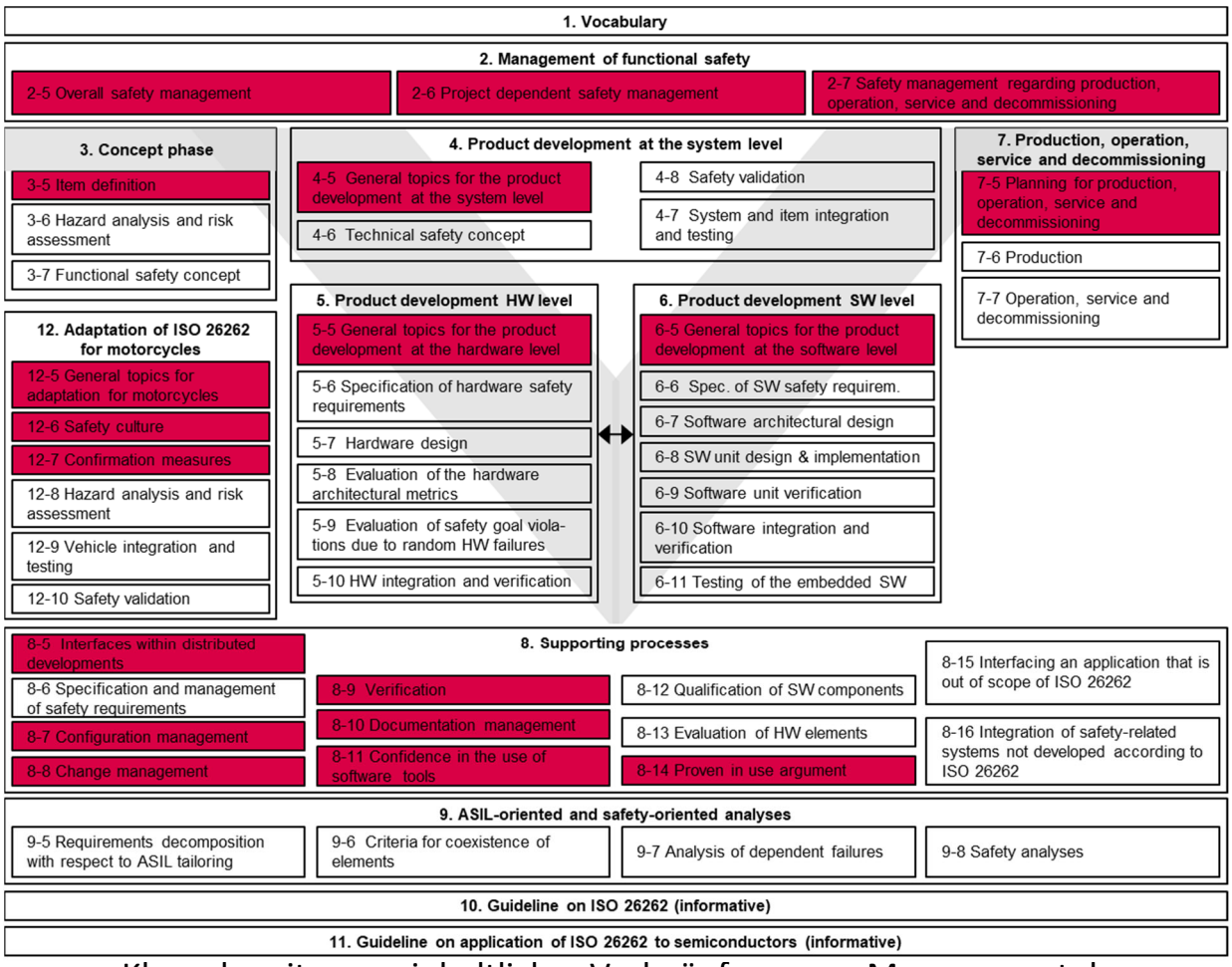


Teil 2 im Überblick der ISO 26262:2018

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

In einer Reihe weiterer Abschnitte der ISO 26262 gibt es weitere Anforderungen, die in engem Zusammenhang mit dem Management der funktionalen Sicherheit stehen. Zum Beispiel gibt es in den entsprechenden Teilen der ISO 26262 bestimmte Lebenszyklen für die Entwicklung von Hardware und Software. Und es wird zum Beispiel gefordert, dass bestimmte Kodierungsrichtlinien definiert und angewendet werden müssen.



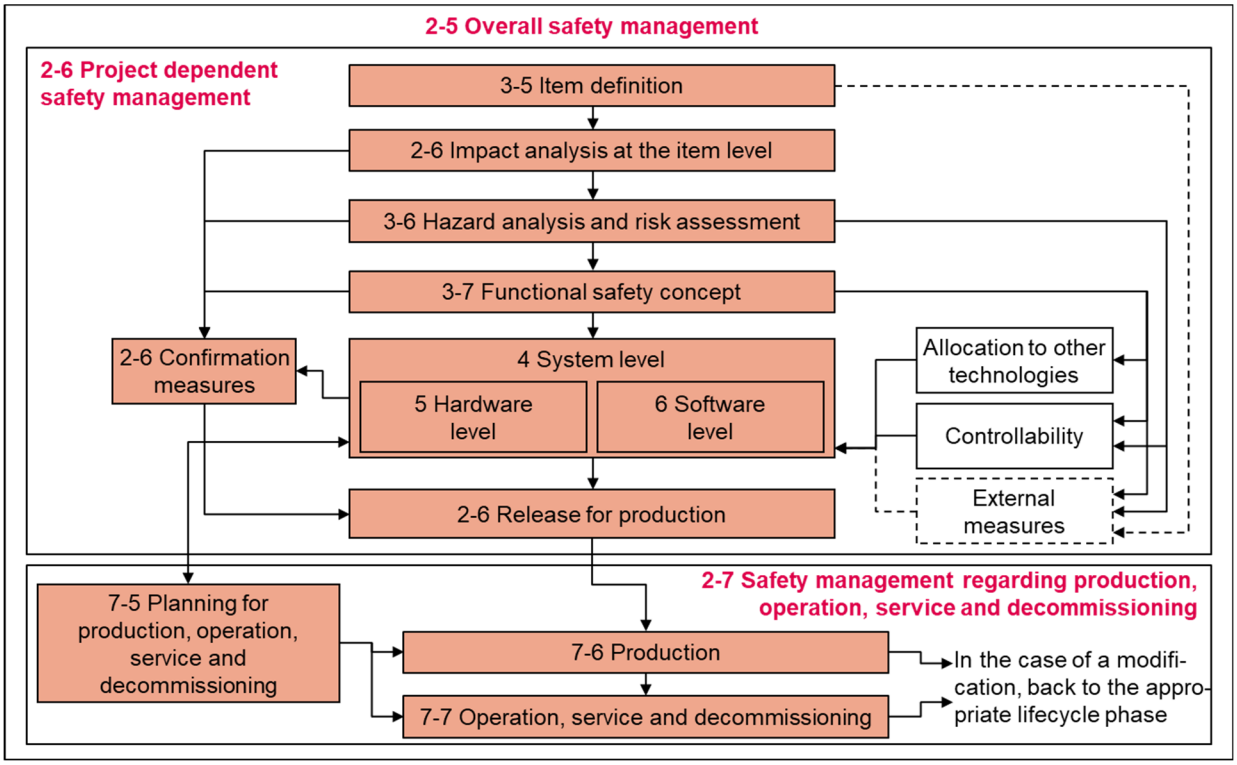
Klauseln mit enger inhaltlicher Verknüpfung zum Management der funktionalen Sicherheit

In diesem Paper werde ich die wichtigsten Punkte erläutern und Sie werden die wichtigsten Lektionen mitnehmen können, um Probleme frühzeitig zu vermeiden.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Beginnen wir mit **Punkt Nummer 1**. Für die funktionale Sicherheit im Automobilbereich wurde ein sogenannter Sicherheitslebenszyklus definiert, den Sie der folgenden Abbildung sehen. Das Lifecycle-Management wird in drei Bereiche unterteilt dargestellt.



Lebenszyklus der funktionalen Sicherheit

Wir sehen

- allgemeines Sicherheitsmanagement (overall safety management),
- projektspezifisches Sicherheitsmanagment (project-dependent safety management) und
- Sicherheitsmanagement für die Zeit nach jeder Release (“post-release” safety management).

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you’ll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Lassen Sie mich dies leicht umformulieren und als erste wichtige Lektion im Gedächtnis verankern.

Das Management der funktionalen Sicherheit muss behandelt werden

- auf Organisationsebene,
- auf einer projektbezogenen Ebene und
- für die Zeit nach der Freigabe zur Produktion.

Kommen wir zu unserem **zweiten Punkt**. Dieser Punkt ergibt sich aus dem Sicherheitsmanagement auf organisatorischer Ebene, das wir jetzt betrachten. Ein umfassendes Sicherheitsmanagement setzt voraus, dass Ihr Unternehmen Verfahren für die Elektronikentwicklung definiert hat und anwendet.

Dazu gehören zum Beispiel Verfahren

- einen unternehmensspezifischen Lebenszyklus zu definieren,
- festzulegen, welche Tools verwendet werden sollen,
- wie man das Konfigurationsmanagement organisiert und
- welche Arten von Sicherheitsanalysen durchzuführen sind.

Ein Qualitätsmanagementsystem muss eingerichtet werden. Dieser Aspekt wird vom Automotive SPICE-Standard stark unterstützt. Automotive SPICE unterstützt die Umsetzung von ISO 26262. Lassen Sie mich für weitergehende Informationen auf unsere Automotive SPICE Tutorials verweisen.

https://www.youtube.com/watch?v=crz9WmoUoKc&t=392s

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

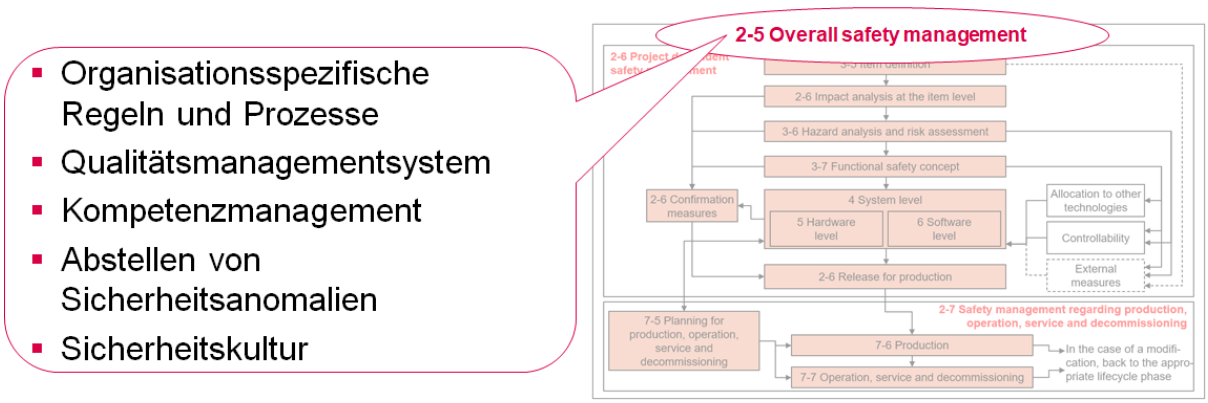
Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Des Weiteren erwartet ISO 26262, dass Sie für die Ihnen zugewiesene Arbeit qualifiziert sind. Das bedeutet, dass es in Ihrer Organisation ein aktives Kompetenzmanagement geben muss.

Funktionale Sicherheit erfordert, dass Sie über einen Prozess verfügen, der sicherstellt, dass Sicherheitsanomalien identifiziert, kommuniziert und gelöst werden.

Insgesamt spricht man hier von einer "Sicherheitskultur" - die jedes Unternehmen haben sollte. Dazu gehört z.B. auch, dass die für die funktionale Sicherheit erforderlichen Ressourcen vom Management auch tatsächlich zur Verfügung gestellt werden.

Lassen Sie mich die oben genannten Punkte als zweite wichtige Lektion zusammenfassen: Eine Organisation, die elektronische Produkte für Autos entwickelt, muss eine Sicherheitskultur und Prozesse für die funktionale Sicherheit haben.



Hauptaspekte der Klausel 2-5

Wir kommen zu **Punkt Nummer 3**, der Frage, was das Management der funktionalen Sicherheit auf Projektebene umfasst.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Die verschiedenen Aktivitäten müssen von Menschen ausgeführt werden. Dazu müssen Rollen definiert und Personen zugewiesen werden. Insbesondere muss klar sein, wer für die funktionale Sicherheit des Produkts verantwortlich ist.

Eine Auswirkungsanalyse („impact analysis“) zeigt auf, was im Laufe der Produktentwicklung alles getan werden muss. Denn nur in den seltensten Fällen beginnt ein Unternehmen eine Entwicklung von Grund auf neu. In der Regel gibt es eine Vorgängerversion des Produkts. Das Ergebnis dieser Auswirkungsanalyse wird verwendet

- zur Anpassung des Lebenszyklus und
- um die notwendigen Sicherheitsaktivitäten zu planen.

Logischerweise umfasst das Management der funktionalen Sicherheit auch die kontinuierliche Überwachung der Fortschritte gegenüber dem Plan und, falls erforderlich, die Überarbeitung des Plans. All dies sind die Aufgaben eines so genannten Sicherheitsmanagers („safety manager“).

Wir können dies als wichtige Lektion Nummer 3 zusammenfassen: Jedes sicherheitsrelevante Elektronikprojekt hat einen für diesen Bereich verantwortlichen Sicherheitsmanager und eine maßgeschneiderte („tailored“) Sicherheitsplanung.

In **Punkt Nummer 4** geht es um die Dokumentation von Sicherheitsnachweisen. Eines der wichtigsten Arbeitsprodukte, die Sie entwickeln müssen, ist eine fundierte Argumentation dafür, dass das Produkt sicher ist. Dies nennt man den Sicherheitsnachweis („safety case“). Er beinhaltet eine geeignete Strategie, um funktionale Sicherheit zu erreichen. Er beinhaltet den Nachweis, dass diese

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Strategie tatsächlich befolgt wurde. Und er umfasst Evidenzen, nämlich die während der Entwicklung entstandenen Arbeitsprodukte.

Lektion Nummer 4: Ein zentrales Ergebnis jedes Projekts ist ein Sicherheitsnachweis: Er enthält die Argumentation dafür, dass das Produkt sicher ist.

Im nächsten **Punkt Nummer 5** geht es darum, Vertrauen aufzubauen. Funktionale Sicherheit bedeutet auch zu verhindern, dass ein Projekt die ISO 26262 falsch interpretiert und/oder „betrügt“. Dies soll durch Bestätigungsmaßnahmen („confirmation measures“) gewährleistet werden, die von unabhängigen Parteien durchgeführt werden.

Es gibt drei Arten von Bestätigungsmaßnahmen.

- Bestätigungsreviews („confirmation reviews“) für wichtige Arbeitsprodukte, wie den Sicherheitsplan oder Sicherheitskonzepte. Diese brauchen eine Bestätigung durch eine unabhängige Person.
- Bei einem Audit der funktionalen Sicherheit („functional safety audit“) muss geprüft werden, ob das Projekt tatsächlich die notwendigen und definierten Verfahren und Prozesse anwendet und umsetzt. Das Audit bezieht sich also auf die Einhaltung der Prozesse.
- Für eine Produktionsfreigabe („release for production“) ist es notwendig, von einer unabhängigen Person eine Bestätigung der erreichten funktionalen Sicherheit zu erhalten. Dies wird als Assessment der funktionalen Sicherheit („functional safety assessment“) bezeichnet. Sie ist für Produkte erforderlich, die eine hohe Sicherheitsintegrität erfordern, wie zum Beispiel ein adaptiver Tempomat.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

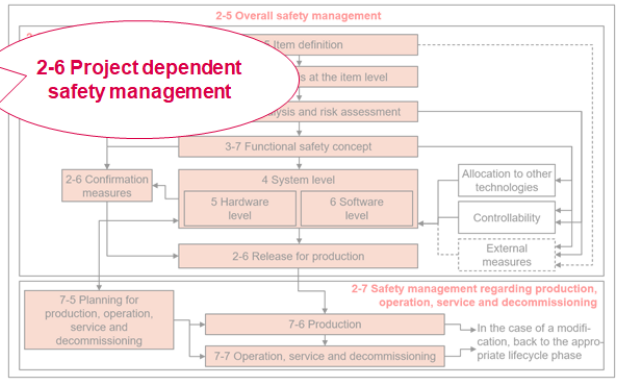
Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Nicht zuletzt darf ein Entwicklungsergebnis nur dann für die Produktion freigegeben werden.

- wenn es einen Sicherheitsnachweis gibt,
- wenn die funktionale Sicherheit unabhängig bestätigt wurde, und
- wenn das Entwicklungsergebnis als Baseline unter Konfigurationskontrolle steht.

Warum? Ich möchte es als zentrale Lektion Nummer 5 formulieren: Unabhängige Bestätigungsmaßnahmen sollen verhindern, dass die Entwicklungsteams ISO 26262 falsch interpretieren und/oder betrügen.

- Rollen und Verantwortlichkeiten
- Auswirkungsanalyse
- Maßschneidern der Sicherheitsaktivitäten
- Planung der Sicherheitsaktivitäten
- Überwachung des Fortschritts
- Sicherheitsnachweis
- Bestätigungsmaßnahmen
  - Bestätigungsreviews
  - Audit der funktionalen Sicherheit
  - Assessment der funktionalen Sicherheit
- Freigabe zur Produktion



Hauptaspekte von Klausel 2-6

Der **sechste und letzte Punkt** bezieht sich auf die Phase, nachdem Sie die Entwicklung abgeschlossen haben. Wenn Ihr Entwicklungsergebnis durch die konsequente Anwendung des Managements der funktionalen Sicherheit sicher

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

entwickelt wurde, müssen Sie dafür sorgen, dass das Produkt auch korrekt produziert wird und über die Lebensdauer der Fahrzeuge sicher bleibt.

Die ISO 26262 verlangt, dass die beteiligten Unternehmen Personen benennen, die für die Produktion und die Feldüberwachung verantwortlich sind, und dass die notwendigen Aktivitäten für die funktionale Sicherheit geplant und eingeleitet werden.

Auch hierfür müssen geeignete Verfahren vorhanden sein. Dies sind z.B. bestimmte Kontrollschritte in der Produktion, wie das Auslesen der installierten Software, um sicherzustellen, dass keine Bitfehler in den Steuergeräten auftreten.

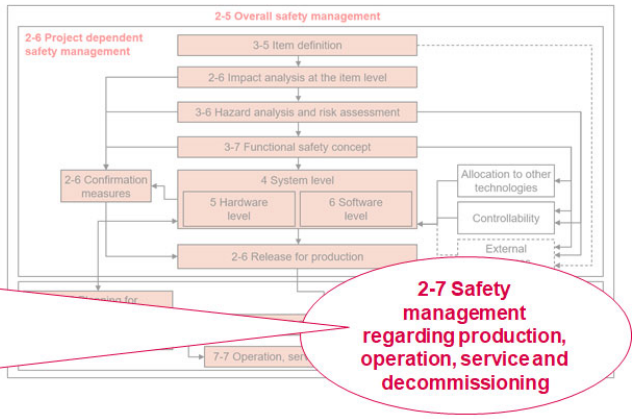
Der Prozess der Feldbeobachtung muss sicherstellen, dass Feldrückläufer auf Verletzungen der Sicherheitsziele untersucht werden. Schließlich erfordert die funktionale Sicherheit, dass Software oder Hardware in den Fahrzeugen bei Bedarf über einen formalisierten Änderungsprozess ausgetauscht wird.

Dies ist der letzte wichtige Punkt: Um die funktionale Sicherheit nicht nur während der Komponenten- und Fahrzeugproduktion, sondern auch über die gesamte Fahrzeuglebensdauer zu gewährleisten, ist eine geeignete Planung erforderlich, die einen Feldbeobachtungsprozess und ein Änderungsmanagement einschließt.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

- Benennung verantwortlicher Personen
- Planung der Aktivitäten um funktionale Sicherheit dauerhaft zu gewährleisten
- Prozesse der funktionalen Sicherheit nach Freigabe zur Produktion
  - Feldbeobachtungsprozess
  - Änderungsmanagement



Hauptaspekte von Klausel 2-7

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Zusammenfassung:

Der vorangegangene Abschnitt war ein Überblick über das Management der funktionalen Sicherheit im Automobil nach ISO 26262. Welche Lektionen haben wir gelernt? Hier ist meine Zusammenfassung dessen, was Sie sich merken sollten:

1. Das Management der funktionalen Sicherheit muss auf Organisationsebene, auf der Ebene der einzelnen Projekte und für die Zeit nach der Freigabe für die Produktion addressiert werden.
2. Ihre Entwicklungsorganisation über eine Kultur und Prozesse verfügen, die die funktionale Sicherheit unterstützen.
3. Jedes sicherheitsrelevante Elektronikprojekt hat einen für dieses Thema verantwortlichen Sicherheitsmanager und eine maßgeschneiderte Sicherheitsplanung. Wenn wir die anderen Teile der ISO 26262 durchgehen, werden Sie feststellen, dass es viele Themen gibt, die über das übliche Projektmanagement hinausgehen und spezifisches Know-how zur funktionalen Sicherheit erfordern.
4. Ein Schlüsselergebnis jedes Projekts ist ein Sicherheitsnachweis, der die Argumentation für die Sicherheit des Produkts enthält.
5. Drei Arten unabhängiger Bestätigungsmaßnahmen sollen verhindern, dass Entwicklungsteams die ISO 26262 falsch interpretieren und/oder betrügen:
    - Bestätigungsreviews wichtiger Arbeitsprodukte, wie zum Beispiel des Sicherheitskonzepts und des Sicherheitsnachweises

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

- Mindestens ein Audit der funktionalen Sicherheit, um sicherzustellen, dass die notwendigen Prozessschritte befolgt werden
- Ein Assessment der funktionalen Sicherheit zur Beurteilung und Bestätigung der Erreichung der funktionalen Sicherheit durch eine unabhängige Person

6. Sechstens: Um sicherzustellen, dass die funktionale Sicherheit während der Komponenten- und Fahrzeugproduktion, sowie während der gesamten Fahrzeuglebensdauer gegeben ist, ist eine geeignete Planung erforderlich. Dazu gehören ein Feldbeobachtungsprozess (der Verletzungen von Sicherheitszielen aufdeckt) und ein Änderungsmanagement.

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com

Sie wollen mehr über funktionale Sicherheit lernen?

Wie Sie gesehen haben, gab es eine Menge verschiedener Aspekte, auf die ich in diesem Paper nur kurz eingehen konnte. Sie fragen sich wahrscheinlich, wie Sie diese Themen in der Praxis angehen können. Dazu haben wir eine ganze Reihe von kostenlosen Expertenvideos erstellt. Zum Beispiel darüber, wie die funktionale Sicherheit in einen bestehenden Entwicklungsprozess eingebettet werden kann. Oder über die Rolle des Sicherheitsmanagers.

Wenn Sie sich auf ein externes Assessment vorbereiten müssen, kann unser Video und Paper zum Assessment der funktionalen Sicherheit nützlich sein.

Ich hoffe dieses Paper hat Ihnen gefallen. Empfehlen Sie es gern Ihren Kollegen.

Falls Sie mehr über funktionale Sicherheit erfahren wollen, empfehle ich Ihnen an einem unserer Trainings teilzunehmen.

Besuchen Sie dazu folgende Seite:

https://www.kuglermaag.de/trainings/funktionale-sicherheit/

Competence from A to Z: Training courses and workshops
Whether you need training to gain a certificate or an individual workshop, we can set up and provide the training you need, anything from courses for experts to exclusively in-house training at your place of business.
Workshops or training courses? With us, you'll find it a lot easier!

Who to contact?
Smilja Mateja
Training Coordination
+49 7154 1796 229
info@kuglermaag.com