Leitfaden Functional Safety Management

Safety Integrated

https://siemens.com/machine-safety

Siemens Industry Online Support

Rechtliche Hinweise

Nutzung der Anwendungsbeispiele

In den Anwendungsbeispielen wird die Lösung von Automatisierungsaufgaben im Zusammenspiel mehrerer Komponenten in Form von Text, Grafiken und/oder Software-Bausteinen beispielhaft dargestellt. Die Anwendungsbeispiele sind ein kostenloser Service der Siemens AG und/oder einer Tochtergesellschaft der Siemens AG („Siemens“). Sie sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit und Funktionsfähigkeit hinsichtlich Konfiguration und Ausstattung. Die Anwendungsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern bieten lediglich Hilfestellung bei typischen Aufgabenstellungen. Sie sind selbst für den sachgemäßen und sicheren Betrieb der Produkte innerhalb der geltenden Vorschriften verantwortlich und müssen dazu die Funktion des jeweiligen Anwendungsbeispiels überprüfen und auf Ihre Anlage individuell anpassen.
Sie erhalten von Siemens das nicht ausschließliche, nicht unterlizenzierbare und nicht übertragbare Recht, die Anwendungsbeispiele durch fachlich geschultes Personal zu nutzen. Jede Änderung an den Anwendungsbeispielen erfolgt auf Ihre Verantwortung. Die Weitergabe an Dritte oder Vervielfältigung der Anwendungsbeispiele oder von Auszügen daraus ist nur in Kombination mit Ihren eigenen Produkten gestattet. Die Anwendungsbeispiele unterliegen nicht zwingend den üblichen Tests und Qualitätsprüfungen eines kostenpflichtigen Produkts, können Funktions- und Leistungsmängel enthalten und mit Fehlern behaftet sein. Sie sind verpflichtet, die Nutzung so zu gestalten, dass eventuelle Fehlfunktionen nicht zu Sachschäden oder der Verletzung von Personen führen.

Haftungsausschluss

Siemens schließt seine Haftung, gleich aus welchem Rechtsgrund, insbesondere für die Verwendbarkeit, Verfügbarkeit, Vollständigkeit und Mangelfreiheit der Anwendungsbeispiele, sowie dazugehöriger Hinweise, Projektierungs- und Leistungsdaten und dadurch verursachte Schäden aus. Dies gilt nicht, soweit Siemens zwingend haftet, z.B. nach dem Produkthaftungsgesetz, in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit, bei Nichteinhaltung einer übernommenen Garantie, wegen des arglistigen Verschweigens eines Mangels oder wegen der schuldhaften Verletzung wesentlicher Vertragspflichten. Der Schadensersatzanspruch für die Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegen oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit gehaftet wird. Eine Änderung der Beweislast zu Ihrem Nachteil ist mit den vorstehenden Regelungen nicht verbunden. Von in diesem Zusammenhang bestehenden oder entstehenden Ansprüchen Dritter stellen Sie Siemens frei, soweit Siemens nicht gesetzlich zwingend haftet.
Durch Nutzung der Anwendungsbeispiele erkennen Sie an, dass Siemens über die beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden kann.

Weitere Hinweise

Siemens behält sich das Recht vor, Änderungen an den Anwendungsbeispielen jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in den Anwendungsbeispielen und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.
Ergänzend gelten die Siemens Nutzungsbedingungen (https://support.industry.siemens.com).

Securityhinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.
Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.
Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.
Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter: https://www.siemens.com/industrialsecurity.
Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.
Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter: https://www.siemens.com/industrialsecurity.

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Vor dem Inverkehrbringen von Waren in den europäischen Markt, muss der Hersteller oder Inverkehrbringer die Anforderungen des Bestimmungslandes erfüllen. Für den Europäischen Wirtschaftsraum wurden einheitliche Anforderungen definiert. Der Hersteller muss alle anwendbaren Richtlinien umsetzen und deren Erfüllung durch die CE-Kennzeichnung erklären. Dazu gehört im Wesentlichen auch die Dokumentation des Entwicklungsprozesses.

Der gesamte CE-Prozess einer Maschine berücksichtigt die Erfüllung der grundlegenden Gesundheits- und Schutzanforderungen für die Konstruktion und den Bau von Maschinen.

Aus diesen geht die Ausarbeitung und Durchführung einer Risikobeurteilung hervor. Die Bewertungsergebnisse müssen für die Konstruktion und den Bau der Maschine beachtet werden. Dazu wird empfohlen, dass harmonisierte Normen, die zur Erfüllung der grundlegenden Anforderungen der Richtlinien konzipiert wurden, verwendet werden.

Um dem Prozess der CE-Kennzeichnung vollständig zu entsprechen, muss jede geeignete Richtlinie berücksichtigt werden. Die Einhaltung der Maschinenrichtlinie 2006/42/EG ist nur eine Voraussetzung für die CE-Kennzeichnung.

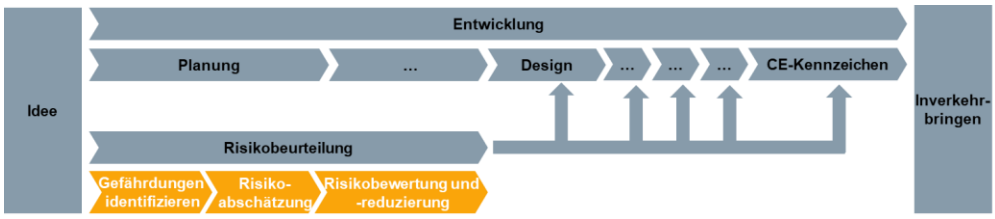
Dieses Anwendungsbeispiel konzentriert sich, ausgehend von der Maschinensicherheit, auf die Erfüllung der Anforderungen an steuerungstechnische Maßnahmen. Dazu werden in diesem Dokument die notwendigen Mindestanforderungen an ein Functional Safety Management (FSM) und die Vorteile dieses zusätzlichen Aufwands zur leichteren Erfüllung der Anforderungen aufgezeigt.

1.2 Risikobeurteilung

Der Risikobeurteilungsprozess in diesem Anwendungsbeispiel basiert auf der Norm DIN EN ISO 12100. Die Durchführung der Risikobeurteilung umfasst verschiedene Schritte, die für die Erfüllung des vorgegebenen Prozesses notwendig sind.

- Gefährdungen identifizieren
- Risiko abschätzen
- Risiko bewerten und reduzieren

Abbildung 1-1: Einordnung der Risikobeurteilung in den Entwicklungsprozess von der Idee zum Inverkehrbringen einer Maschine



Identifizierung von Gefährdungen

Nachdem die Grenzen der Maschine festgelegt wurden, werden darauf basierend, für jede Lebensphase und jeder Betriebsart, potenzielle Gefahren analysiert.

Risikoabschätzung

Aus den ermittelten Gefährdungen müssen die davon ausgehenden Risiken betrachtet werden. Das Risiko ist eine Kombination aus

- Schadensausmaß und
- der Wahrscheinlichkeit des Schadenseintritts.

Risikobewertung und -reduzierung

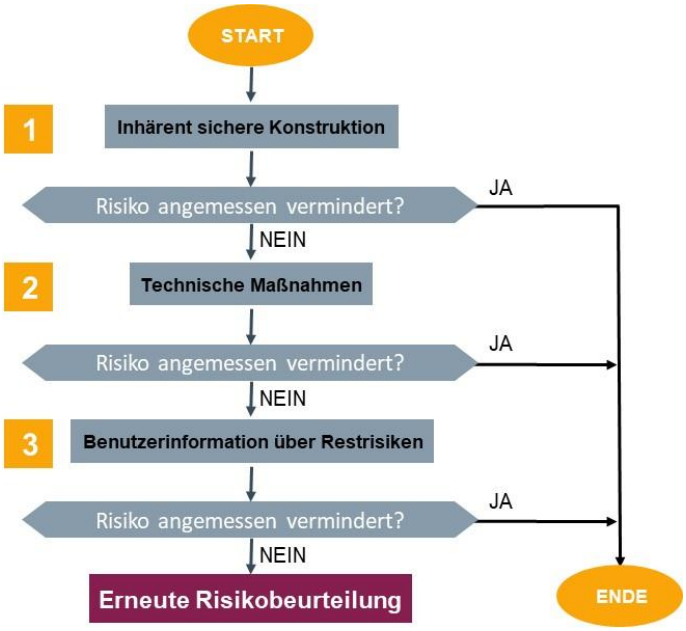
Nach Abschluss der Risikoabschätzung findet eine Bewertung der ermittelten Risiken statt, damit festgestellt werden kann, ob eine Reduzierung erforderlich ist.

Aus der Norm DIN EN ISO 12100 können nachstehende Maßnahmen festgelegt und angewandt werden:

1. Inhärent sichere Konstruktion (Beseitigung der Gefahr durch Konstruktionsänderung)
2. Technische Maßnahmen (Anwendung von Sicherheitsbauteilen oder Schutzvorrichtungen)
3. Benutzerinformationen über Restrisiken

Nach der Verwendung einer jeden Risiko mindernden Maßnahmen, muss eine weitere Risikobewertung durchgeführt werden, um zu überprüfen, ob das Risiko auf ein akzeptables Maß reduziert wurde. Wenn das nicht der Fall ist, so müssen weitere Maßnahmen zur Risikominderung definiert werden.

Abbildung 1-2: Drei-Stufen-Verfahren



Details zu technischen Maßnahmen

Technische Maßnahmen mit Überwachung (≙Sicherheitsfunktionen bzw. steuerungstechnische Maßnahmen) werden mit geeigneten Geräten, wie z.B. Sicherheitsrelais oder fehlersicheren Steuerungen realisiert. Bei Verletzung der überwachten Grenzen bzw. Grenzwerten wird die Maschine automatisch in einen sicheren Zustand überführt, ebenso wie bei Fehlfunktion der Schutzeinrichtungen.

Um geeignete sicherheitsrelevante Einrichtungen auszuwählen, muss ein quantitatives Maß für die sicherheitsrelevante Leistung ermittelt werden. Hierfür können die nachstehenden Level Verwendung finden.

- Safety Integrity Level (SIL) gemäß EN 62061
- Performance Level (PL) gemäß EN ISO 13849

Das Ergebnis dieser Auswertung bildet die Grundlage für die Definition und Realisierung der Sicherheitsfunktionen.

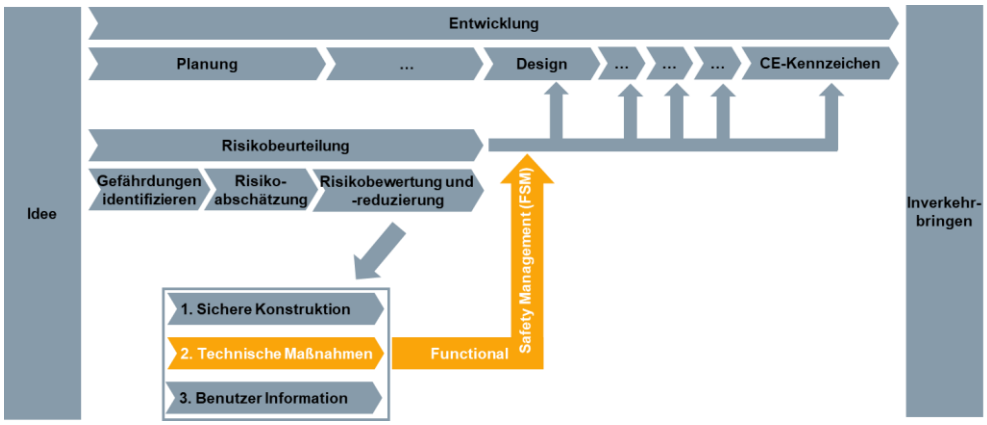
Um eine hohe Qualität während der Implementierungs- und Designphase zu gewährleisten, muss ein geeigneter Prozess etabliert werden. Zur Beschreibung sind mehrere Schritte notwendig, um die Anforderungen zu erfüllen. Mit diesen Schritten können die Phasen Spezifikation, Realisierung, Verifikation und Validierung erfüllt werden. Der gesamte Prozess wird als Functional Safety Management (FSM) bezeichnet.

2 Functional Safety Management

Gemäß den Anforderungen der Maschinenrichtlinie ist es notwendig, eine hohe Güte jeder einzelnen Maschinenkomponente zu gewährleisten. In Bezug auf den Teil der funktionalen Sicherheit, der zur Gewährleistung des sicheren Betriebs der Maschine eingesetzt wird, sollten die folgenden zwei Punkte für die Erreichung eines akzeptablen Niveaus bedacht werden.

- Verwendung zuverlässiger Hardware
- Gewährleistung einer verlässlichen und korrekten Umsetzung

Abbildung 2-1: Einordnung des Functional Safety Managements im Prozess



Aus der Risikobewertung heraus müssen die Maßnahmen zur Risikominderung in Form von technischen, speziell steuerungstechnischen Maßnahmen durch das Rahmenwerk für das Management der funktionalen Sicherheit definiert werden. Der Functional Safety Management Prozess definiert unter anderem folgende Schritte und deren Ausführung.

- Auflistung einer Safety Requirement Specification (SRS) mit allen relevanten Sicherheitsinformationen
- Entwurf und Auswahl der erforderlichen Hardware und Software
- Überprüfung der Einhaltung aller erforderlichen Sicherheitswerte
- Erstellung eines geeigneten Programms
- Test von Hardware und Software

Der FSM-Prozess gewährleistet die notwendige Unabhängigkeit zwischen allen am Prozess beteiligten Personen. Der Abschluss des Prozesses zeigt, dass alle Sicherheitsanforderungen umgesetzt wurden und einwandfrei funktionieren.

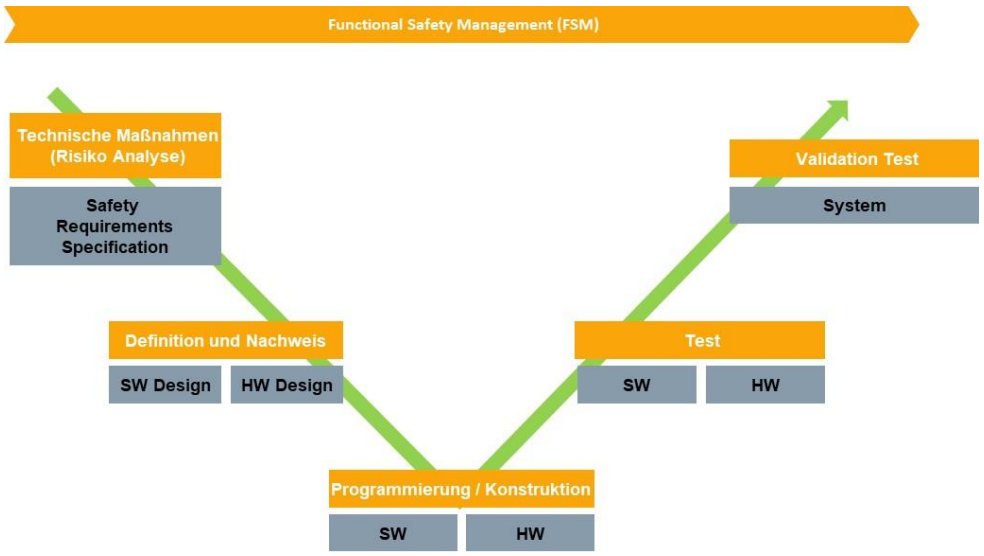
Durch die Verwendung von grundlegenden Dokumenten können diese Anforderungen des FSM-Prozesses dokumentiert sowie stets nachvollzogen werden.

2.1 Functional Safety Management-Plan

Der FSM-Plan steht im Mittelpunkt des Functional Safety Management Prozesses und stellt somit eine Prozessbeschreibung für die strukturierte Umsetzung aller Sicherheitsanforderungen dar.

Der jeweilige Ablauf kann zum Beispiel mit einem V-Modell abgebildet werden und zeigt die zeitliche Abfolge der Entwicklungsschritte.

Abbildung 2-2: Vereinfachter FSM-Plan anhand eines V-Modells



Je nach Größe und Komplexität des zu entwickelnden Systems kann der Detaillierungsgrad des FSM-Plans variieren, folgt aber immer dem gleichen Prinzip.

Die wichtigsten zu definierenden Inhalte sowie eine beispielhafte Realisierung derer sind im Folgenden dargestellt.

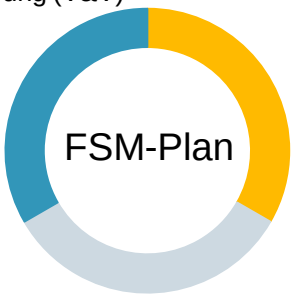
Abbildung 2-3: Bestandteile des FSM-Plans

Dokumentation

- Beschreibung des Prozesses
- Spezifikation der Sicherheits-anforderungen (SRS)
- Funktionale Design-Spezifikation (FDS)
- Validierung/Verifizierung (V&V)

Rollen der Personen

- Personen und ihre Qualifikation
- Aktivitäten jeder Rolle (Aufgaben, Verantwortung)
- Definition einer Rollenaufteilung (z.B. Designer, Tester, Manager)



Entwicklungsprozess

- Abfolge der Aktivitäten (V-Modell)
- Anforderungen der Aktivitäten
- Verifizierungs- und Validierungsverfahren
- Konfigurationsmanagement

Abbildung 2-4: Beispielhafte Dokumentation FSM-Plan

FSM-Plan

Projekt: Name des Projekts
Version: XY vom xx.yy.zz

Verfasser: NAME (Functional Safety Manager)

1. Beschreibung des Projekts

Kurze Beschreibung zum Ziel des Projekts

2. Personen und ihre Qualifikationen

In diesem Kapitel können die Definierten Rollen definiert und beschrieben werden.

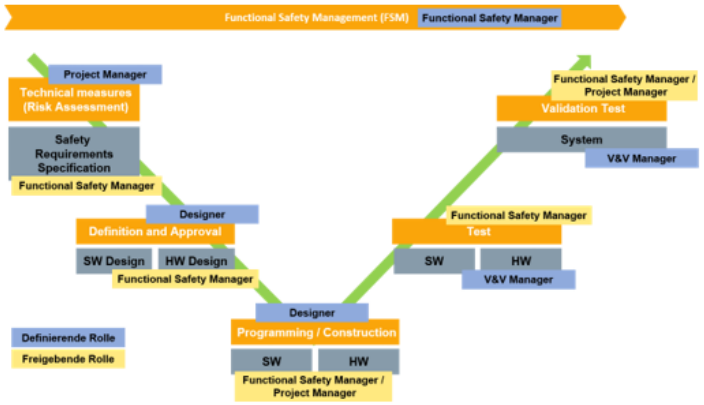
Tabelle 0-1: Definition und Beschreibung der Rollen

Rolle	Name	Qualifikation
Project Manager		- Mehrjährige Erfahrung in Projekten bzgl. funktionaler Sicherheit - Weiterbildung xY
Funktional Safety Manager		
Designer		
V&V Manager		
.....		

3. Verantwortungsbereich der Rollen

Diese Kapitel beschreibt die Tätigkeiten der Rollen und deren Verantwortungsbereiche.

Abbildung 0-1: Beispielhafte Darstellung des Prozesses und die Rollen



4. ...

2.2 Safety Requirement Specification

Nach einer Risikobewertung und der Definition von Maßnahmen, muss die Spezifikation jeder einzelnen Sicherheitsfunktion festgelegt werden. Sie umfasst den Teil der risikoreduzierenden Maßnahmen aus dieser Risikobewertung, die durch den Einsatz von Sicherheitstechnik (steuerungstechnische Maßnahmen) umgesetzt werden müssen.

Die Gestaltung der Hard- und Software von steuerungstechnischen Maßnahmen, kann mit folgenden Parametern beschrieben werden.

Abbildung 2-5: Übersicht Definition von steuerungstechnischen Maßnahmen

Basierend auf einer detaillierten Beschreibung, kann die Hard- und Software im Nachgang beschrieben und definiert werden.

Abbildung 2-6: Beispielhafte Dokumentation SRS

Safety Requirement Specifikation

Projekt: Name des Projekts
Version: XY vom xx.yy.zz

Verfasser: NAME (Project Manager)
Freigebender: NAME (Functional Safety Manager)

1. System und Funktionsbeschreibung

Allgemeine Beschreibung und Definition der Sicherheitsziele

2. Spezifische Beschreibung der Sicherheitsfunktionen

Nummer: *Lfd. Nr.*	**Risk ID:**	**Name:** *Name der Sicherheitsfunktion*
1. Beschreibung		
Beschreibung der Sicherheitsfunktion		
2. Gefordertes Performance Level		
Beschreibung, auf welcher Grundlage das geforderte PL definiert wurde.		
3. Sicherer Zustand		
Beschreibung, wie der sichere Zustand definiert und eingenommen wird		
4. Maßnahmen beim Auftreten eines Fehlers		
Beschreibung der Maßnahmen bei auftretenden Fehlern		
5. Grenzwerte und Auslösekriterien der Sicherheitsfunktion		
Definition der Grenzwerte und ihre zugehörige Maschinenreaktion		
6. Quittierung und Wiederanlauf nach Fehler		
Beschreibung der Bedingungen, welche zum Wiederanlauf und der Erteilung der Betriebsfreigabe erfüllt werden müssen.		
7. Möglichkeiten zum Umgehen der Sicherheitsfunktion		
Beschreibung evtl. Bedingungen, welche ein Umgehen der Sicherheitsfunktion ermöglichen		
8. Anforderungsrate		
Definition der Anforderungsrate		
9. Beteiligte Sensoren		
Beschreibung der benötigten Sensorik		
10. Beteiligte Aktoren		
Beschreibung der definierten Aktorik		
11. Reaktionszeiten		
Definition der max. tolerierbaren Reaktionszeit		
12. Eingriff Bedienpersonal		
Definition und Beschreibung eines evtl. notwendigen Eingreifens des Bedienpersonals		
13. Gegenseitige Beeinflussung der Sicherheitsfunktionen		
Beschreibung einer evtl. gegenseitigen Beeinflussung		
14. Schnittstelle zu nicht-sicheren Funktionen		
Evtl. Beschreibung		

3. …

2.3 Functional Design Specification

Die Functional Design Specification (FDS) beschreibt den kompletten Funktionsumfang des zu erstellenden Gesamtsystems und enthält eine Aufteilung der Funktionalitäten auf Teilsysteme/Teilprojekte. Um diese zu realisieren, ist ein Hard- sowie Software Designprozess notwendig. Der Detaillierungsgrad der FDS hängt von der jeweiligen Projektkomplexität ab und ergibt sich maßgeblich aus dem Liefer- und Leistungsumfang.
Bei komplexeren Projekten bietet es sich an eine weitere Aufteilung vorzunehmen. So kann in der FDS eine elementare Beschreibung einer Funktion definiert sein. Die Beschreibung mit einem tieferen detailierungsgrad kann dann in einer jeweiligen Detailed Design Spezifikation (DDS) vorgenommen werden.

Hinweis Wichtig ist, dass bei Spezifikationspunkten mit Bezug zu steuerungstechnischen Maßnahmen Referenzen auf die Safety Requirements Specification vorgesehen werden, um Nachvollziehbarkeit zu gewährleisten.

Hardware Design

Die Auslegung und Wahl der Hardware spielt eine wesentliche Rolle bei der Realisierung einer Sicherheitsfunktion. Hier müssen die, aus der Risikobeurteilung, erarbeiteten Ergebnisse beachtet und angewandt werden. Wenn eine Kombination von sicherheitsrelevanten Teilen erforderlich ist, müssen dafür geeignete qualifizierte Komponenten ausgewählt werden. Dazu gehören unter anderem

- zertifizierte,
- nicht-zertifizierte oder
- kombinierte

Hardware.

Der Konstrukteur muss sich verschiedene Fragen stellen, um zum einen das geforderte Sicherheitsniveau zu erreichen und zum anderen geeignete Hardware auszuwählen.

- Erfüllt die Hardware die Sicherheitsanforderungen?
- Kann mit der Hardware der Funktionsumfang abgedeckt werden?
- Kann jedes Teilsystem mit Hardware realisiert werden?
- Welche Architektur ist geeignet?
- Wie zuverlässig muss die Sicherheitsfunktion sein?
- Welche Diagnose wird gefordert?
- Resistenz gegen äußere Einflüsse?
- Geeigneter Prozess vorhanden?
- Werden weitere Maßnahmen benötigt?
  - Diagnosen?
  - Einstellungen?

Hinweis Fehlersichere Baugruppen bieten auf Grund von integrierten Strukturen und Diagnosemaßnahmen die notwendige Güte und sind für den Einsatz zur Realisierung von Sicherheitsfunktionen entsprechend zertifiziert. Beachten Sie bei der Verwendung von nicht-zertifizierter Hardware, dass Zusatzmaßnahmen erforderlich sein können, um diese für den Einsatz zu qualifizieren.

Nach Auswahl der sicherheitsrelevanten Komponenten kann die Verifikation dieser mittels TIA Selection Tool Safety Evaluation gemäß der Normen EN 62061 und EN ISO 13849-1 erfolgen. Unter Berücksichtigung dieser kann ein Konstrukteur die Sicherheitsfunktionen der Maschine schnell und einfach beurteilen.

Durch die frühzeitige Verifizierung der erreichbaren Sicherheitslevel mit den gewählten Komponenten, kann der Konstrukteur die Auswahl und Bestellung von Hardware, welche nicht für die Sicherheitsanforderungen geeignet ist, vermeiden.

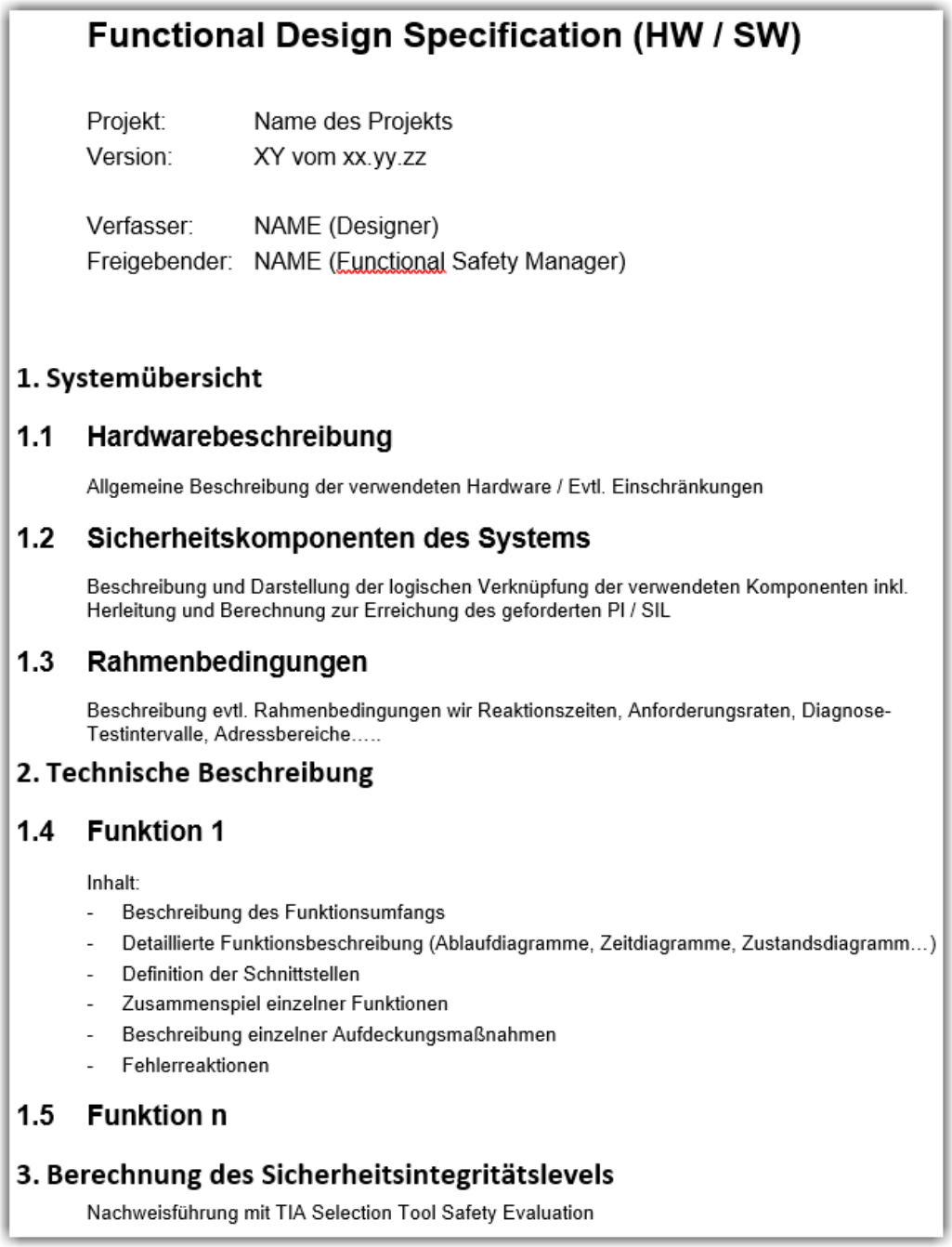
Software Design

Basierend auf der SRS und der gewählten Hardware kann es nötig sein, eine geeignete Anwendersoftware zu entwerfen. Für das Softwareprogramm ist eine detaillierte Planung dessen Designs hilfreich. Um dies zu realisieren, muss ein Designer eine Spezifikation des Programms ausarbeiten. Hierfür können die nachstehenden Punkte helfen.

- Beschreibung der Funktion
- Semiformale Darstellung des Programmablaufs
  - Ursache-Wirkungs-Diagramm
  - Detaillierter Zustandsautomat
  - Signalflussdiagramm
  - Programmablaufpläne für Zustandsübergänge
- Allgemeine textliche Beschreibung
- Beschreibung der Schnittstelle
- Adressbereiche

Diese Punkte können den Software-Programmierer unterstützen, das Programm für die Sicherheitsfunktionen zu realisieren. Mit steigender Qualität der Design Planung, z.B. durch detaillierte Zustandsdiagramme, steigt analog die Qualität der im Anschluss erstellten Software und deren Nachvollziehbarkeit.

Abbildung 2-7: Beispielhafte FDS



Functional Design Specification (HW / SW)

Projekt: Name des Projekts
Version: XY vom xx.yy.zz

Verfasser: NAME (Designer)
Freigebender: NAME (Functional Safety Manager)

1. Systemübersicht

1.1 Hardwarebeschreibung

Allgemeine Beschreibung der verwendeten Hardware / Evtl. Einschränkungen

1.2 Sicherheitskomponenten des Systems

Beschreibung und Darstellung der logischen Verknüpfung der verwendeten Komponenten inkl. Herleitung und Berechnung zur Erreichung des geforderten PI / SIL

1.3 Rahmenbedingungen

Beschreibung evtl. Rahmenbedingungen wir Reaktionszeiten, Anforderungsraten, Diagnose-Testintervalle, Adressbereiche.....

2. Technische Beschreibung

1.4 Funktion 1

Inhalt:
- Beschreibung des Funktionsumfangs
- Detaillierte Funktionsbeschreibung (Ablaufdiagramme, Zeitdiagramme, Zustandsdiagramm…)
- Definition der Schnittstellen
- Zusammenspiel einzelner Funktionen
- Beschreibung einzelner Aufdeckungsmaßnahmen
- Fehlerreaktionen

1.5 Funktion n

3. Berechnung des Sicherheitsintegritätslevels

Nachweisführung mit TIA Selection Tool Safety Evaluation

2.4 V&V Spezifikation

Mit der V&V-Spezifikation wird der Prozess hinsichtlich der Validierung und Verifizierung definiert. Es wird spezifiziert, wie diese Maßnahmen durchgeführt werden müssen und welche Dokumente dabei entstehen können. Eine hohe Qualität bei der Dokumentenerstellung helfen dabei die Nachweispflicht einzuhalten.

Hinweis Auch die zu definierenden V&V Schritte werden zu einem Großteil aus dem Liefer- und Leistungsumfang abgeleitet. Wichtig ist aber auch hier, analog zur FDS, dass zum Nachweis der Vollständigkeit, V&V Schritte mit Bezug zu steuerungstechnischen Maßnahmen mittels Referenzen auf die SRS gekennzeichnet werden müssen

Validierung

Ziel der Validierung ist es zu prüfen, ob die implementierten Sicherheitsfunktionen den erforderlichen Beitrag zur Risikominderung leisten. Bei Abweichungen von den erwarteten Ergebnissen müssen Korrekturen an der technischen Realisierung vorgenommen und eine entsprechende Wiederholungsprüfung durchgeführt werden.

Der Validierungsprozess kann in folgende Phasen gegliedert werden:

Spezifikation der Sicherheitsanforderungen (SRS), abgeleitet von der Risikobewertung

Nach der Definition und Ausarbeitung der SRS wird geprüft, ob alle in der Risikobeurteilung festgestellten Risiken durch die Spezifikation erfüllt sind. Darüber hinaus wird neben der inhaltlichen Überprüfung auch deren Vollständigkeit, Widersprüche und Richtigkeit betrachtet.

Hardware- und Software-Spezifikation, abgeleitet von der SRS

Im Rahmen der Hard- und Softwarevalidierung wird geprüft, ob alle im SRS festgelegten Anforderungen abgedeckt wurden. Dazu gehört beispielsweise das Gegenüberstellen der implementierten Software und deren Beschreibung zur eingesetzten Hardware. Es muss nachgewiesen werden, dass diese den geforderten Maßnahmen genügen, um die Risikominderung ausführen zu können.

Verifikation

Bei der Verifikation muss überprüft werden, ob die jeweils verwendete Hard- oder Software den jeweiligen Vorgaben erfüllen. Mittels Analysen, Reviews oder anhand verschiedener Testszenarien kann dieser Nachweis erbracht werden.

Für die Sicherheitsfunktionen muss entsprechend gezeigt werden, dass die Anforderungen aus der SRS, ggf. mittels FDS gegenüber der Hard- und Software-Implementierung eingehalten werden. Dies kann in zwei Teststufen erfolgen. Zwingend zu empfehlen ist die Durchführung eines Funktionstest. Hier wird die gesamte Funktion gegen die Spezifikation getestet.

Bei Funktionsmodulen, welche wiederkehrend in definierten Funktionen verwendet werden, kann die Durchführung eines Modultests sinnvoll sein.

Modultest

Dieser Test beinhaltet die Analyse der Anwendersoftware mit dazugehöriger Hardwarekonfiguration. Dazu werden die Grundfunktionen der Module, i. d. R. Funktionsbausteine getestet. Dies kann mit Hilfe von z.B. Parameterüberprüfungen, Black/White-Box-Tests etc. durchgeführt werden. Darüber hinaus sind auch allgemeine Tests, wie im Folgenden gelistet, denkbar.

- Hardware-Aufbautest im Schaltschrank
- Analyse der Adressbereiche zwischen den Modulen
- Grenzwertanalyse (Speichertest usw.)
- Einhaltung von Richtlinien für die Programmierung

Funktionstest

Der Funktionstest betrachtet die Programmfunktionalität im Detail. Dazu sind verschiedene Tests denkbar, wie z.B. Prozesssimulationen, Parameterüberprüfungen und Grenzwerttests. Um die Funktionalität der Software zu untersuchen, gibt es unter anderem verschiedene Tests und Analysen.

- IO-Test
- Abnahmeprüfung
- Funktionstest
- Reaktionszeit-Test
- Signalweg-Test

Factory Acceptence Test

Abgeschlossen wird die Abnahme einer Sicherheitsfunktion auf der Anlage im Rahmen eines Factory Acceptance Tests (FAT). Hierfür gibt es im Industry Online Support unter der Beitrags-ID 109758262 eine Beispieldokumentation.

Abbildung 2-8: Beispielhafte V&V Specifikation

V&V Specification

Projekt: Name des Projekts
Version: XY vom xx.yy.zz

Verfasser: NAME (V&V Manager)
Freigebender: NAME (Functional Safety Manager)

1. Modultest

Dieses Kapitel beschreibt die Testdurchführung für das Testen der einzelnen Module.

1.1 Testdurchführung

Hardware

Beschreibung der verwendeten Hardware zur Durchführung des Modultests.

Software

Beschreibung der verwendeten Software zur Durchführung des Modultests.

Vorgehen

Beschreibung der Durchführung der Tests

Aufbau der Tests

Beschreibung, wie die Testfälle definiert werden (Flussdiagramme, Zustandsgraphen…)

1.2 Übersicht der Projektparameter

Vor dem Test werden folgende Parameter dokumentiert:

- Dateiname des Testprojekts
- Symbolischer Bausteinname
- Objektnummer
- Bausteinsignatur
- Passwort

1.3 Modul Test Checkliste

Hier werden die Testfälle mit den zu erwartenden Ergebnissen dargestellt

1.4 Testfall 1

Lfd. Nr.	IN1	IN2	IN3	IN4	Q		Test i.O.
					Erwartet	Real	
1.							
2.							
3.							
4.							

1.5 Testfall n

2. Funktionstest

Dieses Kapitel beschreibt die Testdurchführung des gesamten Systems im Zusammenspiel der einzelnen Module.

2.1. Testdurchführung

Hardware

Beschreibung der verwendeten Hardware zur Durchführung des Modultests.

Software

Beschreibung der verwendeten Software zur Durchführung des Modultests.

Vorgehen

Beschreibung der Durchführung der Tests

Hardware Parameter

Vorgaben zur Parametrierung der Hardware

Aufbau der Tests

Beschreibung, wie die Testfälle definiert werden (Flussdiagramme, Zustandsgraphen…)

Verknüpfung der Bausteine

Beschreibt das Zusammenspiel und die Signalverläufe zwischen den einzelnen Bausteinen

2.2. Übersicht der Projektparameter

Vor dem Test werden folgende Parameter dokumentiert:

- Dateiname des Testprojekts
- Symbolische Bausteinnamen
- Objektnummern
- Bausteinsignaturen
- Projektsignaturen
- Passwörter

2.3. Beschreibung der Testdokumentation

Lfd. Nr.	FDS Funktion, Schritt	Testfall	Testvoraussetzungen	Testbeschreibung/Durchführung	Erwartetes Ergebnis	Testergebnis / Tester / Datum
1.						
2.						
3.						
4.						
5.						
6.						

3. Zusammenfassendes Testergebnis

Zusammenfassung des Testergebnis bzw. Aufzählung abzustellender Mängel

3 Zusammenfassung und Fazit

Jeder Maschinenhersteller muss einen Nachweis erbringen, dass die von ihm auf den Markt gebrachten Produkte allen gesetzlichen Anforderungen gerecht werden. Mit dem Functional Safety Management Prozess wird dafür eine Möglichkeit an die Hand gegeben.

Mit dem aufgezeigten Prozess können alle notwendigen Aufgaben Schritt für Schritt, durch eine definierte Organisationsstruktur, durchgeführt werden. Dabei werden verschiedene Phasen wie die Spezifikation, Realisierung, Verifikation bis hin zur Validierung durchlaufen und ausgearbeitet. Darüber hinaus werden dadurch Verantwortlichkeiten für Aktivitäten, Dokumente und Meilensteine festgelegt.

Dies hilft, systematische Fehler zu vermeiden, die Qualität der Produkte zu erhöhen sowie eine strukturierte Arbeitsweise in den Arbeitsablauf zu integrieren.

Der jeweilige Detaillierungsgrad sowie der Umfang dieses aufgezeigten Prozesses obliegt dem Anwender selbst. Hier ist stets darauf zu achten, dass für den jeweiligen Projektumfang ein geeignetes Maß gefunden wird.

4 Anhang

4.1 Service und Support

Industry Online Support

Sie haben Fragen oder brauchen Unterstützung?

Über den Industry Online Support greifen Sie rund um die Uhr auf das gesamte Service und Support Know-how sowie auf unsere Dienstleistungen zu.

Der Industry Online Support ist die zentrale Adresse für Informationen zu unseren Produkten, Lösungen und Services.

Produktinformationen, Handbücher, Downloads, FAQs und Anwendungsbeispiele – alle Informationen sind mit wenigen Mausklicks erreichbar:
support.industry.siemens.com

Technical Support

Der Technical Support von Siemens Industry unterstützt Sie schnell und kompetent bei allen technischen Anfragen mit einer Vielzahl maßgeschneiderter Angebote – von der Basisunterstützung bis hin zu individuellen Supportverträgen.

Anfragen an den Technical Support stellen Sie per Web-Formular:
www.siemens.de/industry/supportrequest

SITRAIN – Training for Industry

Mit unseren weltweit verfügbaren Trainings für unsere Produkte und Lösungen unterstützen wir Sie praxisnah, mit innovativen Lernmethoden und mit einem kundenspezifisch abgestimmten Konzept.

Mehr zu den angebotenen Trainings und Kursen sowie deren Standorte und Termine erfahren Sie unter:
www.siemens.de/sitrain

Serviceangebot

Unser Serviceangebot umfasst folgendes:

- Plant Data Services
- Ersatzteilservices
- Reparaturservices
- Vor-Ort und Instandhaltungsservices
- Retrofit- und Modernisierungsservices
- Serviceprogramme und Verträge

Ausführliche Informationen zu unserem Serviceangebot finden Sie im Servicekatalog:
support.industry.siemens.com/cs/sc

Industry Online Support App

Mit der App "Siemens Industry Online Support" erhalten Sie auch unterwegs die optimale Unterstützung. Die App ist für Apple iOS, Android und Windows Phone verfügbar:
support.industry.siemens.com/cs/ww/de/sc/2067

4.2 Links und Literatur

Tabelle 4-1

Nr.	Thema
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link auf die Beitragsseite des Anwendungsbeispiels https://support.industry.siemens.com/cs/ww/de/view/
\3\	

4.3 Änderungsdokumentation

Tabelle 4-2

Version	Datum	Änderung
V1.0	08/2020	Erste Ausgabe