2 Umsetzung Schritt für Schritt

In diesem Kapitel werden die relevanten Schritte gemäß den Normen zur Funktionalen Sicherheit erläutert. Die beigefügte Software „FSP“ kann dabei unterstützen und als Arbeitshilfe dienen.

2.1 Projektinformationen

Wie in jedem Projekt wird ein Rahmen benötigt hinsichtlich der notwendigen Dokumentation und der betroffenen Personen bzw. Gruppen oder Abteilungen.

Typische Projektinformationen sind	
Projekt Daten:	Bezeichnung, interne Dokumentation, …
Projekt Verantwortliche und Funktionen (Rollen):	verantwortliche Gruppe sind die Kollegen: Projektleiter, Entwickler, Tester/QM, …
Projekt Konfigurations-management:	HW und SW werden durch den Kollegen Herr Konfigurator-QM geprüft.
Projekt Änderungs-management:	Jede Projektierungs-Änderung wird durch im Team freigegeben. Fehler beim Testen werden separat dokumentiert. Die Version der HW und SW wird eindeutig genannt.
Projekt Verifizierungsplan (Personen, Abteilungen, Gruppen, Einheiten):	Die Validierung jeder Sicherheitsfunktion basiert auf dem Verifizierungsplan; interne Dokumenten-Referenz ist VER *XYZ*.
Projekt Hardware:	interne Dokumenten-Referenz HW *XYZ* (Schaltpläne)
Projekt Software:	interne Dokumenten-Referenz SW *ABC* (Programm)

Bild 2.1 zeigt die typischen Projektinformationen. Diese Informationen können bereits in anderen Dokumenten vorliegen und müssen hier nicht mehr erfasst werden. „Wurde bereits durchgeführt, siehe Kommentare | Notizen“.

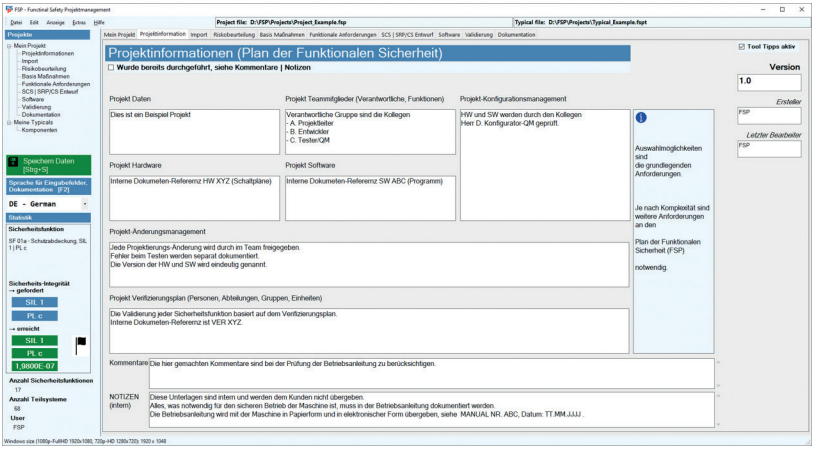

Bild 2.1 Projektinformationen (FSP)

Aktivitäten als „Plan der Funktionalen Sicherheit“ – Wer macht was?

Die DIN EN IEC 62061 (**VDE 0113-50**) beschreibt alle Aktivitäten im Rahmen der Funktionalen Sicherheit mit diesem Plan. **Bild 2.2** zeigt die relevanten Aktivitäten mit den Verantwortlichen.

Management für alle – kein Nachteil für den Einzelnen

In diesem Plan (en: safety plan) sollen alle notwendigen Aktivitäten erfasst und dokumentiert werden, damit die notwendige Funktionale Sicherheit des SCS also die entscheidenden Teile einer Sicherheitsfunktion, sichergestellt ist. Der Begriff „Managementaktivitäten“ in der Norm meint all die Aktivitäten, die diesbezüglich sowohl technisch als auch organisatorisch einzuhalten sind.

Plan der Funktionalen Sicherheit

Die legitimen Fragen, die beantwortet werden müssen, damit eine gewisse Qualität im Konstruktionsprozess nachgewiesen werden kann, sind:

1. Welche Eingangsparameter gibt es, wer ist verantwortlich dafür?
2. Wie wird die Funktionale Sicherheit erreicht?
3. Wer macht was?
4. Wie können die Resultate verifiziert und überprüft werden?
5. Wie werden Änderungen (Modifikation) verfolgt?

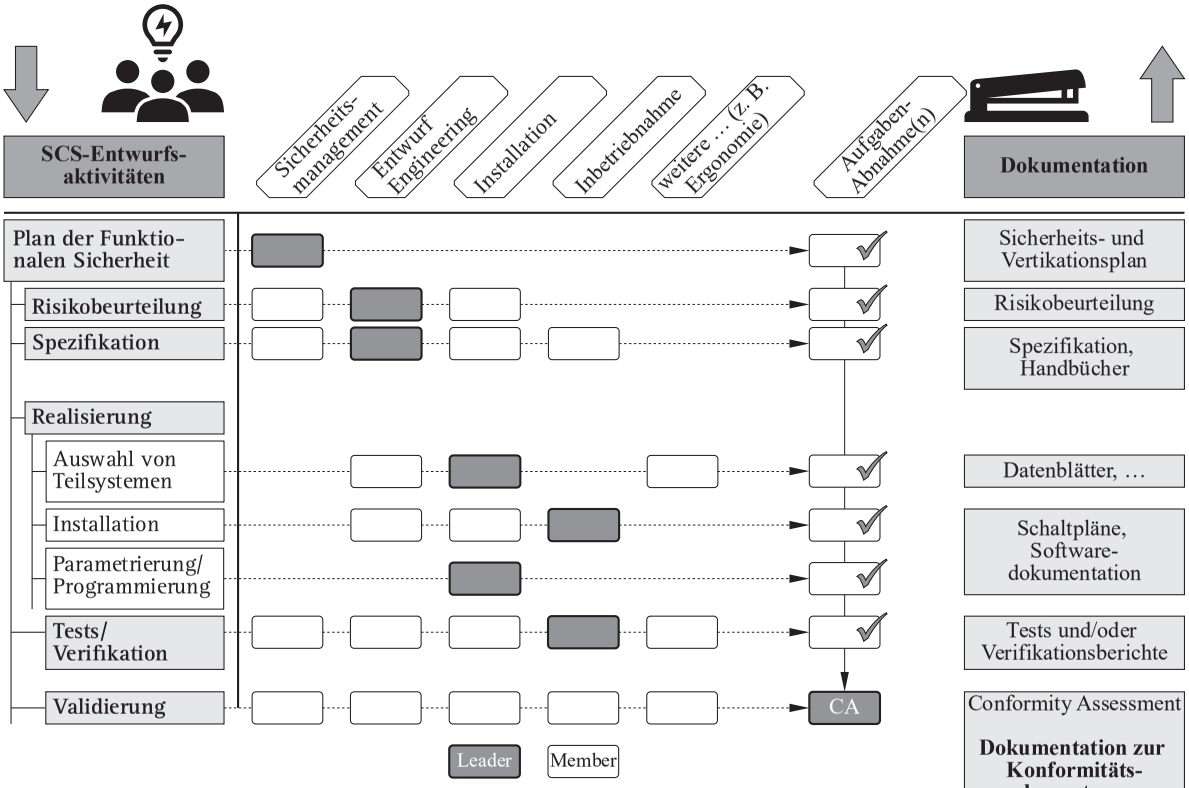

Bild 2.2 Plan der Funktionalen Sicherheit mit Aktivitäten und Verantwortlichen

All diese Informationen liegen bereits heute beim Hersteller von Maschinen vor (s. a. Bild 2.3).

Ein Bild sagt mehr als tausend Worte – Funktionale Sicherheit versteht sich als Projektmanagement, wie jedes andere auch.

Die Abschnitte 4 bis 10 der Normen finden sich im **Plan der Funktionalen Sicherheit** wieder.

Es gibt immer einen **Verantwortlichen** für eine Tätigkeit. Diese Person muss nicht zwangsläufig diese Tätigkeit bis ins letzte Detail ausführen. Sie muss aber dafür Sorge tragen, dass alle Unterlagen und Ergebnisse vorhanden und auch nachvollziehbar sind.

Das Ziel ist eine nachvollziehbare und verständliche Dokumentation.

Diese ist Teil der Maschinendokumentation und wird in der Praxis in den Standard-Konstruktionsprozess eingebaut werden.

Die **Betriebsanleitung** der Maschine zeigt dem Nutzer der Maschine, was zu beachten ist, damit die Maschine ordnungsgemäß und sicher (für den Bediener) betrieben werden kann (Stichworte: Arbeitssicherheit und Gewährleistung).

Sie ist die sichtbare Schnittstelle zwischen Betreiber und Hersteller der Maschine.

Hier werden die Sicherheitsfunktionen aus Sicht des Bedieners und der möglichen Wartung, als auch der Störungshandhabung genannt, ohne dass der Begriff Sicherheitsfunktion in der Regel verwendet wird:

Der Bediener muss z. B. die technische Umsetzung für eine Schutztürüberwachung und das Warum nicht kennen. Aber sehr wohl wann diese zu quittieren ist und wann die Maschine erst erneut gestartet werden darf.

Die technische Dokumentation (z. B. Risikobeurteilung, Sicherheitsfunktionen, …) sind Betriebsgeheimnisse die nicht weitergegeben werden müssen – sie dienen der CE-Konformitätsbewertung und helfen im Schadensfall den Nachweis zu erbringen, nicht grob fahrlässig gearbeitet zu haben.

Einfache und klare Ziele – Prüfen was vielleicht schlief

Aufgabenstellung (Was)	*Nachweis und Aktivitäten (Wie)*
Überprüfen der *SRS auf Konsistenz und Zielerreichung:* *Entspricht die SRS wirklich den Sicherheitsanforderungen?*	*Festgelegte Aktivitäten im Plan der Funktionalen Sicherheit müssen überprüft werden.* Nachweis, dass die Konstruktion vollständig im Einklang mit dem Plan der Funktionalen Sicherheit ist, mittels ✓ Inspektion (auch Analyse) und ✓ Prüfung der SRS hinsichtlich der Sicherheitsanforderungen. Wichtige Ergebnisse der Prüfung SRS sind durch die Überprüfung der ✓ Funktionalen Anforderungen und ✓ Anforderungen an den spezifizierten SIL zu erbringen.
	Wer? „Unabhängige" Personen (nicht am Entwurf und der Realisierung beteiligt).
	Womit? Der Validierungsprozess besteht aus ✓ der Analyse und ✓ erforderlichen Funktionstests.
	Bei komplexen Steuerungssystemen kann eine *getrennte Validierung der Teilsysteme* vor der Integration vorgenommen werden.

2.2 Risikobeurteilung und SRS

Aus der Risikobeurteilung ergeben sich risikomindernde Schutzmaßnahmen, dabei gehen die technische immer vor organisatorischen Maßnahmen.

Diese technischen Schutzmaßnahmen können mit Sicherheitsfunktionen beschrieben werden. Wenn eine Sicherheitsfunktion mittels einer „Steuerung" integriert oder realisiert wird, wird ein SCS oder SRP/CS entworfen.

Dabei ist entscheidend, welche Vorgaben aus der Risikobeurteilung an diesen SCS oder SRP/CS Entwurf gemacht werden.

Informationen aus der Risikobeurteilung (DIN EN ISO 12100):
siehe 1.1 Gefahr, Risiko und Schaden 1.3 Beziehung zwischen DIN EN ISO 12100 und DIN EN IEC 62061 (**VDE 0113-50**), DIN EN ISO 13849-1
Die Liste der Sicherheitsfunktionen wurde aufgrund der Risikobeurteilung, Warnhinweise oder sonstige Informationen, die in die Betriebsanleitung übernommen werden müssen, sind in den Kommentaren hervorgehoben. Herr *C.* Tester/QM ist verantwortlich für die Überprüfung der Informationen (Vollständigkeit), die in die Betriebsanleitung übernommen werden müssen.
Allgemeine Beschreibung der Sicherheitsfunktion (SF):
z. B. Die Maschinenbeschreibung ist im Dokument MACHINE NR. ABC, Datum: TT.MM.JJJJ hinterlegt. Die Betriebsanleitung ist das Dokument MANUAL NR. ABC, Datum: TT.MM.JJJJ Die Abstimmung erfolgte mit der Konstruktion (Mechanik), die federführend die Risikobeurteilung geleitet hat. Die Risikobeurteilung ist in dem Dokument RISK NR. ABC, Datum: TT.MM.JJJJ hinterlegt.

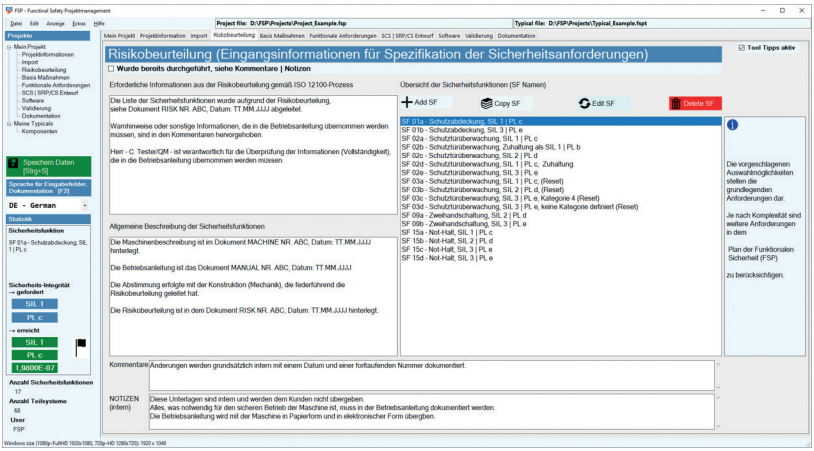

Bild 2.3 Risikobeurteilung und Spezifikation der Sicherheitsanforderungen (FSP)

Die geforderte Sicherheitsintegrität (Güte) der Sicherheitsfunktion kann mit DIN EN IEC 62061 (**VDE 0113-50**) oder aber auch DIN EN ISO 13849-1 ermittelt werden (siehe **Bild 2.4** und **Bild 2.5**).

SIL-Zuweisung (Anhang A der DIN EN IEC 62061 (VDE 0113-50))

Folgen	Schwere *Se*	Klasse *Kl* = *Fr* + *Pr* + *Av*												
		3	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
Tod, Verlust eines Auges oder Arms	*4*	**SIL 1**		**SIL 2**			**SIL 2**			**SIL 3**			**SIL 3**	
		PL_r b	PL_r c	PL_r d			PL_r d			PL_r e			PL_r e	
dauerhafte Verletzung, Finger verlieren	*3*			**AM**			**SIL 1**			**SIL 2**			**SIL 3**	
				PL_r a			PL_r b		PL_r c	PL_r d			PL_r e	
reversible Verletzung, medizinische Versorgung	*2*	kein SIL (oder PL) erforderlich					**AM**			**SIL 1**			**SIL 2**	
							PL_r a			PL_r b		PL_r c	PL_r d	
reversible Verletzung, Erste Hilfe	*1*									**AM**			**SIL 1**	
										PL_r a			PL_r b	
AM: andere Maßnahmen (z. B. grundlegende Sicherheitsprinzipien)														

Folgen	Schadensausmaß *Se*
irreversible: Tod, Verlust eines Auges oder Arms	4
irreversible: gebrochene Extremität(en), Verlust eines Fingers (von Fingern)	3
reversibel: erfordert Versorgung durch einen Arzt	2
reversibel: benötigt Erste Hilfe	1

Häufigkeit und Dauer der Exposition (*Fr*)			Wahrscheinlichkeit des Eintritts	Wahrscheinlichkeit *Pr*	Möglichkeit zur Vermeidung oder Begrenzung eines Schadens *Av*	
Häufigkeit der Exposition	Häufigkeit, *Fr*					
	Dauer der Exposition ≥10 min	Dauer der Exposition <10 min				
≥1 pro Stunde	5	5	sehr hoch	5	unmöglich	5
<1 pro Stunde bis ≥1 pro Tag	5	4	wahrscheinlich	4		
<1 pro Tag bis ≥1 pro 2 Wochen	4	3	möglich	3	selten	3
<1 pro 2 Wochen bis ≥1 pro Jahr	3	2	selten	2		
<1 pro Jahr	2	1	vernachlässigbar	1	wahrscheinlich	1

Bild 2.4 SIL-Zuweisung

PL-Ermittlung (Anhang A der DIN EN ISO 13849-1)

Riskoelemente:

S Schwere der Verletzung
S1 leichte (üblicherweise reversible Verletzung)
S2 ernste (üblicherweise irreversible Verletzung einschließlich Tod)

F Häufigkeit und/oder Dauer der Gefährdungsexposition
F1 selten bis weniger häufig und/oder die Zeit der Gefährungsexposition ist kurz
F2 häufig bis dauernd und/oder die Zeit der Gefährungsexposition ist lang

P Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
P1 möglich unter bestimmten Bedingungen
P2 kaum möglich

O Eintrittswahrscheinlichkeit
O1 gering
O2 hoch

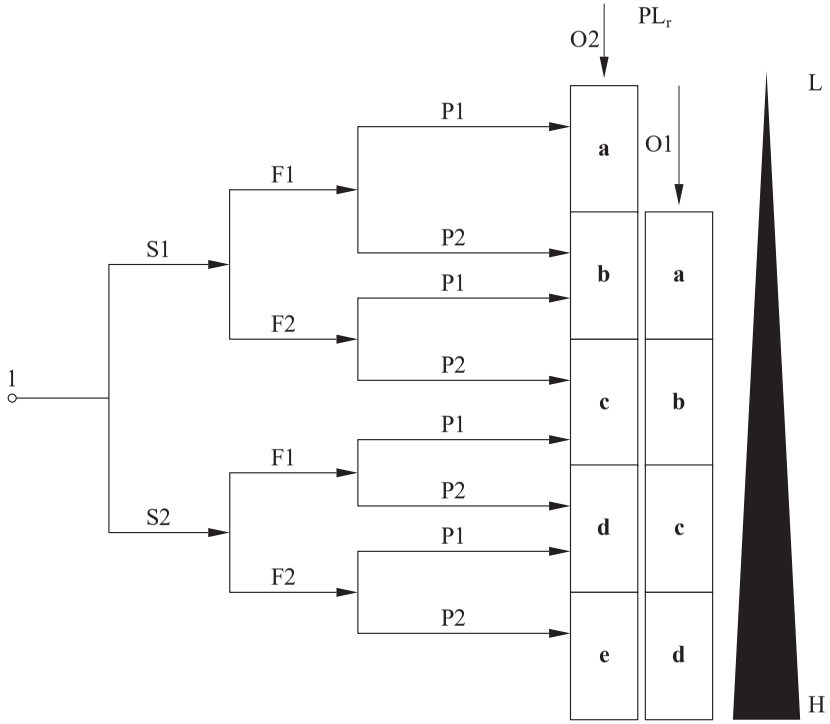

Bild 2.5 Risikograph

Angabe, die nicht selten unterschlagen wird

Neben einem geforderten SIL oder PL ist der *Typ der Sicherheitsfunktion* eine sehr prägnante Information.

Man kann grundsätzlich zwischen drei Arten oder Gruppen von Sicherheitsfunktionen unterscheiden:

- ✓ **Sicherheitsfunktionen zum Schutz von Personen**
- ✓ **Andere Sicherheitsfunktionen**
- ✓ **Sicherheitsfunktionen zum Schutz der Maschine**

Im Kapitel 3 wird auf diese Unterteilung genauer eingegangen.

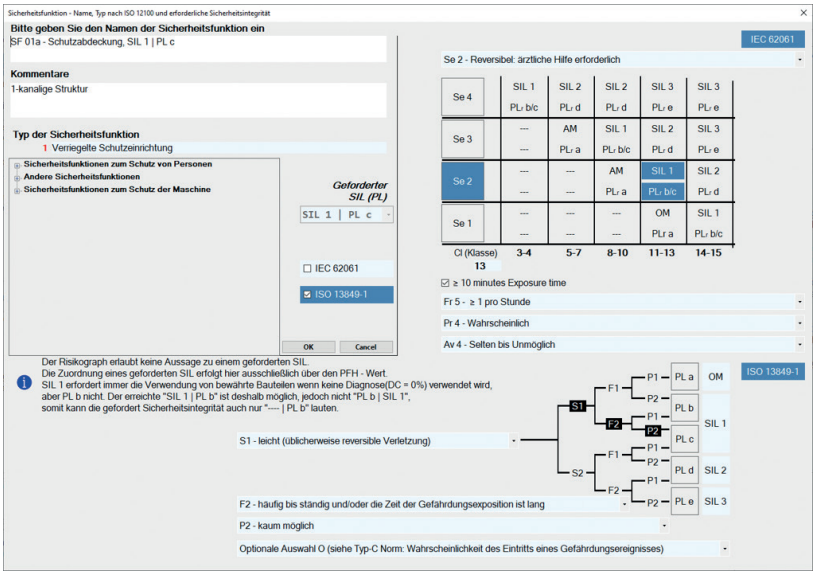

Bild 2.6 Risikoeinschätzung (FSP)

***SIL 1* | *PL b* (mit DIN EN IEC 62061 (VDE 0113-50)) und ---- | *PL b* (mit DIN EN ISO 13849-1) ergibt sich aufgrund der Definition von SIL und PL.**

Der Risikograph erlaubt keine Aussage zu einem geforderten SIL.

Die Zuordnung eines geforderten SIL erfolgt hier ausschließlich über den *PFH*-Wert.

SIL 1 erfordert immer die Verwendung von bewährten Bauteilen, wenn keine Diagnose (*DC* = 0 %) verwendet wird, aber PL b nicht. Der erreichte „*SIL 1* | *PL b*“ ist deshalb möglich, jedoch nicht „*PL b* | *SIL 1*“, somit kann auch nur die gefordert Sicherheitsintegrität „---- | *PL b*“ lauten.

2.3 Sicherheitsfunktionen und funktionale Anforderungen

Die nachfolgenden Tabellen zeigen die typischen Merkmale, die beschrieben werden sollten, damit die Sicherheitsfunktion funktional (als Zielsetzung oder Schutzziel) verstanden wird, bevor die Suche nach einer technischen Lösung beginnt.

Typische Merkmale sind zum Beispiel

Spezifikation der funktionalen Anforderungen an die Sicherheitsfunktion	
Beschreibung	Wenn … dann … (Ursache-Wirkung)
Bedingung(en)	Betriebsarten
Neustart/Zurücksetzen	manuelle menschliche Eingriffe sind erforderlich, wenn …
Priorität	hohe Priorität im Vergleich zu anderen Sicherheitsfunktionen; die Not-Halt-Funktion wird die höchste Priorität haben
Häufigkeit des Betriebs	*X* mal pro Stunde; *Y* Stunden pro Tag; *Z* Tage pro Jahr
Reaktionszeit	max. 500 ms vom Auslöseereignis (Öffnen der Schutztür) bis zur elektrischen Reaktion …
Schnittstelle(n) zu anderen Maschinenfunktionen	… Informationen zur Verwendung des Komponentenherstellers sind zu referenzieren
Fehler-Reaktionsfunktion	sofortiger Stopp oder Erkennung beim erneuten Start zumindest durch Verhinderung des Wiederanlaufs.
Manipulation/Umgehung	Entwurf der Schutztür und Einbau von Verriegelungseinrichtungen nach DIN EN ISO 14119
Umgebung	Temperatur, Staub, Vibrationen, …
Spezifikation der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktion	
geforderter SIL oder PL_r	SIL 2 mit zugehörigem Zielwert *PFH*
Architektur Einschränkungen	Verwendung von … Schutzverriegelungen (Positionsschalter) wegen Vibrationen keine Typ-C-Normanforderungen (z. B. geforderte *HFT*)

Tabelle 2.1 Funktionale Beschreibung

Die funktionale Beschreibung ist neben der geforderten Sicherheitsintegrität Teil der Spezifikation der Anforderungen der Sicherheitsfunktion (SRS, en: safety requirements specification).

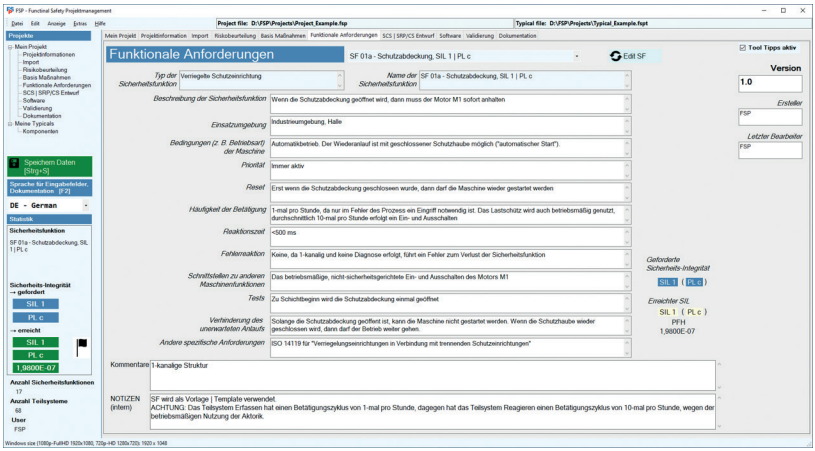

Bild 2.7 Funktionale Anforderungen (FSP)

Die funktionale Beschreibung erlaubt die Aufteilung der Sicherheitsfunktion in Teilfunktionen, die wiederum dann Teilsystemen zugeordnet werden können.

Sicherheitsfunktion = ∑ von Teilfunktionen
Teilfunktionen → Teilsysteme
SCS = ∑ der Teilsysteme

2.4 SCS- und SRP/CS-Methodik

Der Sicherheitsintegritätslevel SIL eines SCS gemäß DIN EN IEC 62061 (**VDE 0113-50**) oder der Performance Level PL eines SRP/CS gemäß DIN EN ISO 13849-1 muss spätestens bei der Validierung und Verifikation immer drei Anforderungen genügen bzw. entsprechen:

- die strukturellen Einschränkungen der Teilsysteme und des Systems
- die Sicherheitsintegrität der Hardware
- die systematische Sicherheitsintegrität der Teilsysteme und des Systems

Daraus ergibt sich:

$$PL_{System} \leq \left(PL_{Teilsystem}\right)_{niedrigste}$$

$$SIL_{System} \leq \left(SIL_{Teilsystem}\right)_{niedrigste}$$

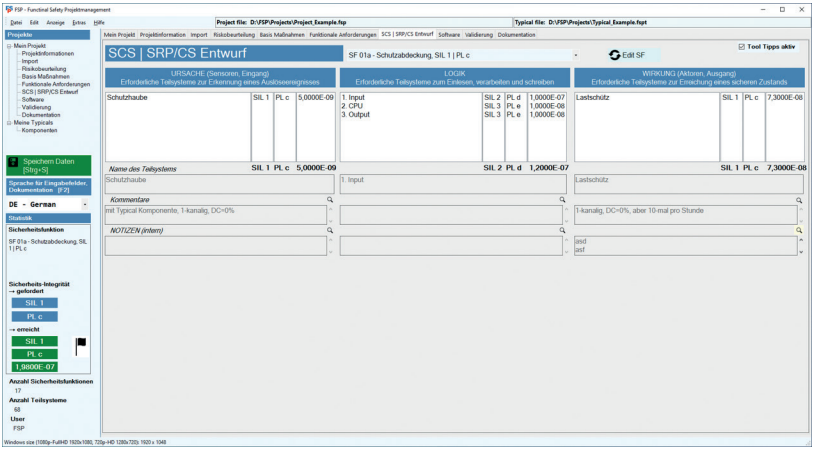

Bild 2.8 SCS oder SRP/CS Entwurf (FSP)

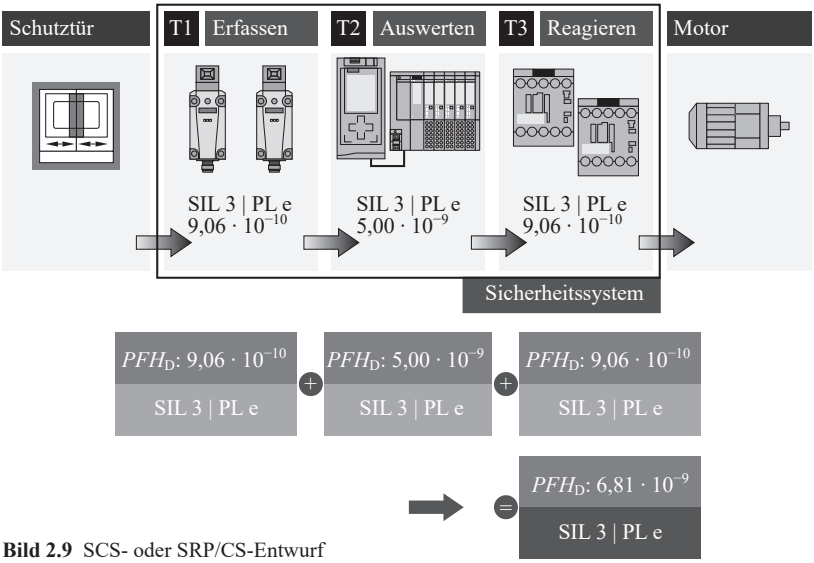

Bild 2.9 SCS- oder SRP/CS-Entwurf

(Sicherheits-)Teilfunktionen → Teilsysteme

Die Sicherheitsfunktion wurde in Teilfunktionen zerlegt.

Das führt dazu, dass jedes Teilsystem hinsichtlich Teilsystem-Elemente weiter betrachtet wird: Zum Beispiel eine Schutztürüberwachung für SIL 1 bedarf nur eines einzelnen Positionsschalters. Dagegen ist für SIL 2 oder SIL 3 eine Zweikanaligkeit gefordert.

Wenn ein Teilsystem mehreren Sicherheitsfunktionen dient

In der Praxis entsteht diese Situation z. B. durch die Notwendigkeit, dass jede Maschine mindestens eine Not-Halt-Funktion haben muss. Diese übergeordnete Funktion wird andere Sicherheitsfunktionen beeinflussen, in dem Sinne, dass die Ausgangskreise durch die Not-Halt-Funktion mit abgeschaltet werden.

2.5 Kategorien und Architekturen

2.5.1 Geräte-Typen

Bevor die Architekturen beschrieben und bestimmt werden, sollte kurz aus Sicht der verwendeten Komponenten ein Blick auf die Eigenschaften dieser Komponenten geworfen werden.

Geräte-Typ 1 oder „pre-designed" Teilsystem

„Bereits entwickeltes und geprüftes" Teilsystem –
kennt jeder unter falschem Namen.

Diese sperrige deutsche Formulierung (en: pre-designed subsystems) wurde bewusst so gewählt, da es zwei Möglichkeiten gibt, sog. Teilsysteme zu entwerfen oder zu nutzen:

1. Ein Komponentenhersteller stellt Teilsysteme bereit (also verkauft dies frei auf dem Markt, im Jargon der Maschinenrichtlinie „bringt diese in Verkehr"), die anschließend mit ihren mitgebrachten Eigenschaften verwendet werden können: Die Begrifflichkeit „zertifiziert" darf nicht verwendet werden, weil das bedeuten würde, dass die Norm eine Zertifizierung durch eine Drittstelle verlangen würde – was de facto nicht erlaubt ist, erst recht nicht im Kontext der Maschinenrichtlinie;
   Beispiele: Laserscanner von Fa. Sick oder Simatic S7 von Siemens, …