Sicherheitsgerichtete Anwendersoftware SRASW

Verifikation und Validierung nach DIN EN ISO 13849-1/2

Ihr Referent

Name:
Weidle-Safety - Stefan Weidle,
freier Technischer Redakteur
www.weidle-safety.de

Tätigkeiten im Laufe des Berufslebens:

- Inbetriebnehmer
- Leiter elektrische Instandhaltung
- Produktmanager Sicherheitssteuerungen
- Fachberater für Maschinensicherheit

Dienstleistungen:

- Begleitung bei Konformitätsbewertungsverfahren nach MRL 2006/42/EG
- Risikobeurteilungen, Gefährdungsbeurteilungen
- Nachweise funktionaler Sicherheit
- Betriebs-, Montage- und Einbauanleitungen
- Seminare, Vorträge und Workshops zu den Themen

Normativer Hintergrund

Anforderungen an sicherheitsbezogene Anwendersoftware (SRASW) nach DIN EN ISO 13849-1

4.6.1 Allgemeines

Alle Tätigkeiten im Lebenszyklus von sicherheitsbezogener Embedded- oder Anwendungs-software müssen hauptsächlich die Vermeidung von Fehlern berücksichtigen, die während des Softwarelebenszyklus eingebracht werden. Das Hauptziel der folgenden Anforderungen ist es, lesbare, verständliche, testbare und wartbare Software zu erhalten.

Maßgeblich ist Abschnitt 4.6.3 der DIN EN ISO 13849-1:

- Entwicklungslebenszyklus mit Verifikation und Validierung
- Spezifikation der Sicherheitsanforderungen
- Dokumentation von Spezifikation und Entwurf
- Modulare und strukturierte Programmierung
- Funktionale Tests
- Geeignete Entwicklungsaktivitäten nach Änderungen

Quelle: Beuth Verlag, DIN EN ISO 13849-1:2015(D), Abschnitt 4.6.1

Anforderungen an sicherheitsbezogene Anwendersoftware (SRASW), Aspekt der „steigenden Wirksamkeit“

DIN EN ISO 13849-1 [1] fordert in **Abschnitt 4.6.3** dazu:
„Bei SRASW für Bauteile mit einem PLr von a bis e müssen die folgenden Basismaßnahmen angewendet werden“ und im weiteren Text *„Für SRASW in Komponenten mit PLr von c bis e werden die folgenden zusätzlichen Maßnahmen mit steigender Wirksamkeit … erforderlich oder empfohlen.“*

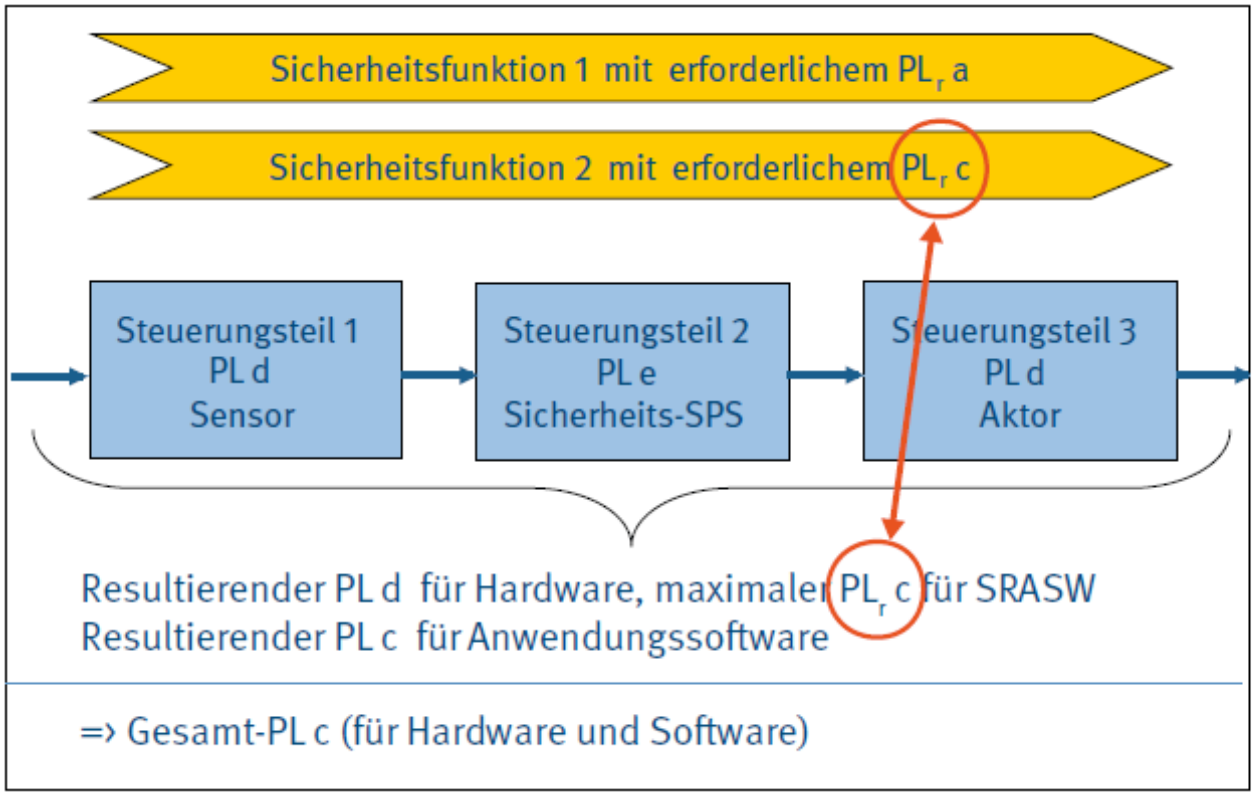
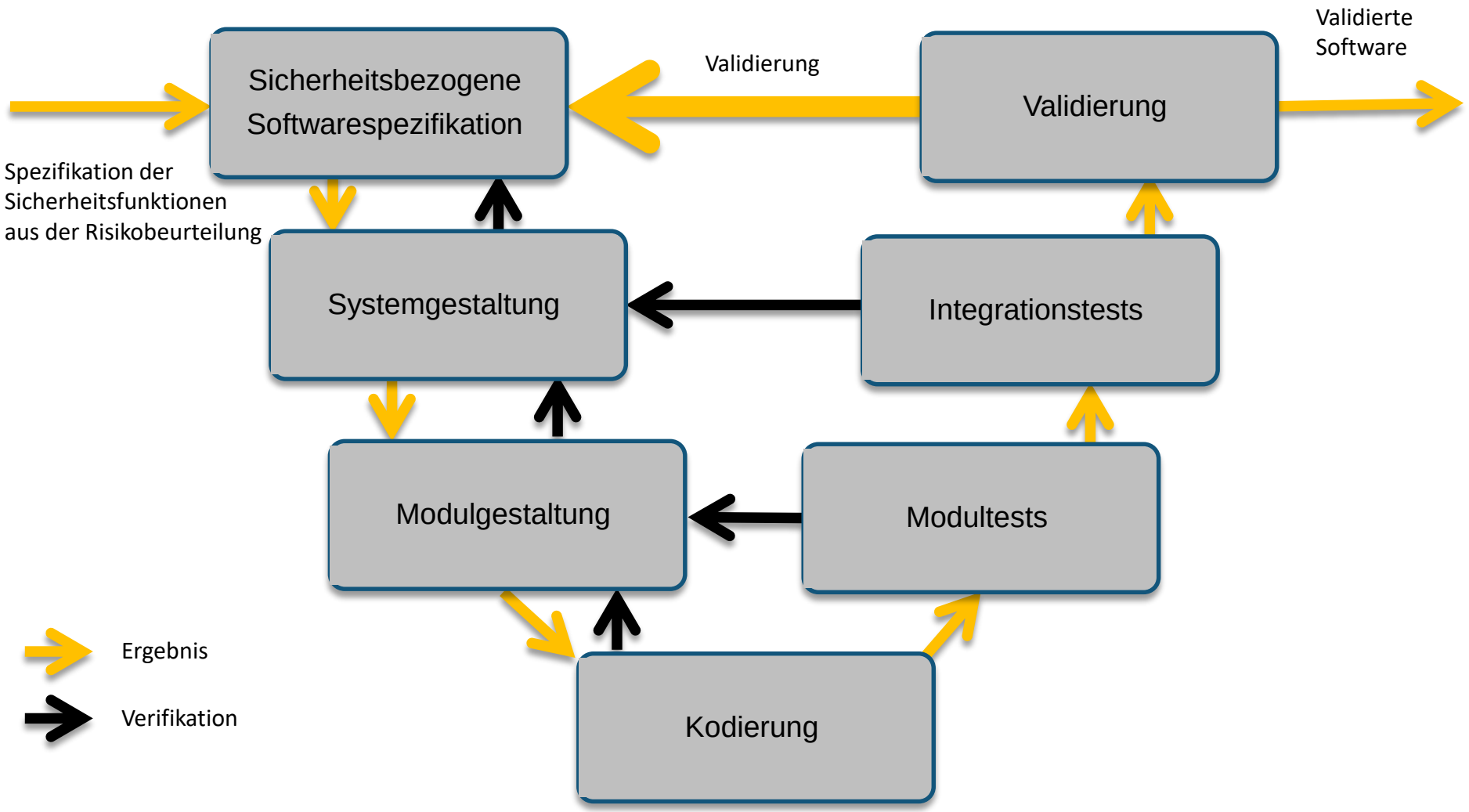


Abbildung 3:
Beispiel für Herleitung der Anforderungen an SRASW

Quelle:
IFA Fachbericht 2/2016

Vereinfachtes V-Modell des Softwarelebenszyklus nach DIN EN ISO 13849-1



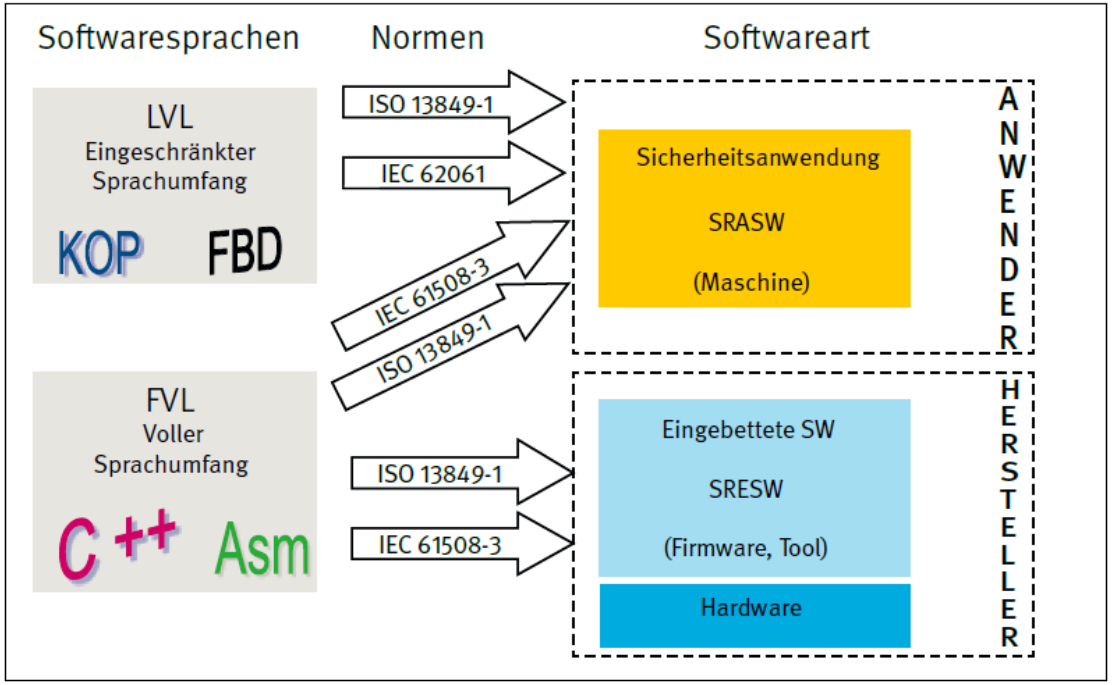
Quelle: Beuth Verlag, DIN EN ISO 13849-1:2015(D), Abschnitt 4.6.1, Bild 6

Sprachtypen sicherheitsgerichteter Software
SRESW, SRASW, FVL, LVL

FVL:
Programmiersprache mit nicht eingeschränktem Sprachumfang (englisch: Full Variability Language), siehe DIN EN ISO 13849-1 [1], Abschnitt 3.1.35, (bspw. C++ / Assembler)

LVL:
Programmiersprache mit eingeschränktem Sprachumfang (englisch: Limited Variability Language), siehe DIN EN ISO 13849-1 [1], Abschnitt 3.1.34, (bspw. FUP / KOP)

Abbildung 1:
Zusammenhang zwischen Softwaresprachen, Softwarearten und anzuwendenden Normen, Asm = Assembler



Quelle:
IFA Fachbericht 2/2016

SRASW und nicht-SRASW in einer Komponente kombiniert

DIN EN ISO 13849-1 [1] *verweist in* ***Abschnitt 4.6.3 d)*** *auf folgende zusätzliche fehlervermeidende Maßnahme:*

„d) Wo SRASW und nicht-SRASW in einer Komponente kombiniert werden:

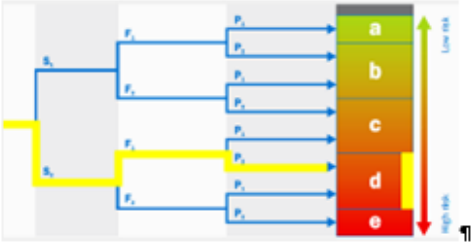
1) SRASW und nicht-SRASW müssen in unterschiedlichen Funktionsblöcken codiert werden, mit sorgfältig definierten Datenschnittstellen.

2) Es darf keine logische Verknüpfung von nicht sicherheitsbezogenen und sicherheitsbezogenen Daten geben, die zur Herabstufung der Integrität der sicherheitsbezogenen Signale führen könnten, z. B. Verknüpfen eines sicherheitsbezogenen und eines nicht sicherheitsbezogenen Signals durch ein logisches **„ODER“**, dessen Ausgang sicherheitsbezogene Signale steuert.“

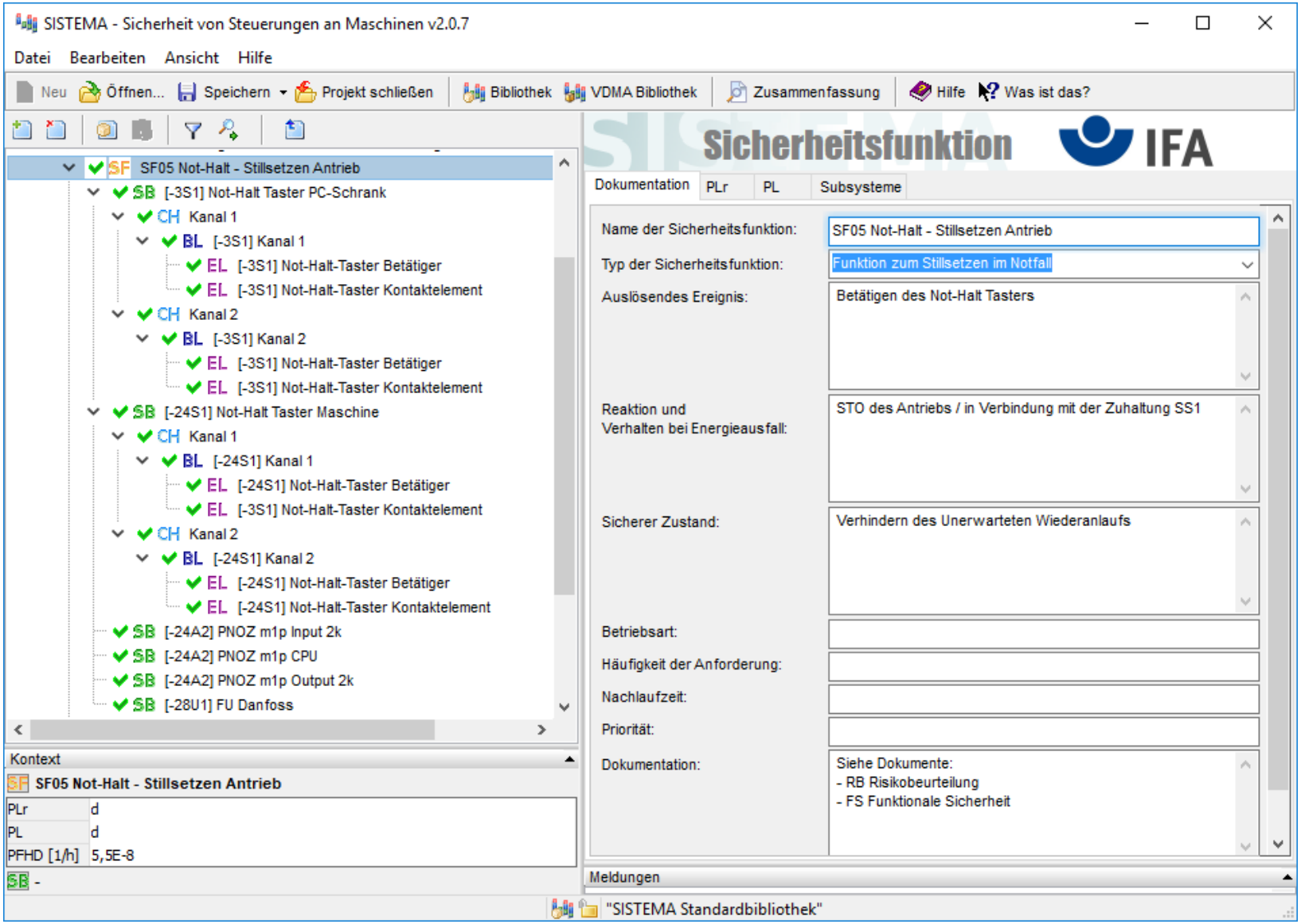
Quelle:
IFA Fachbericht 2/2016

Sicherheitsfunktion SRASW

Definition der Sicherheitsfunktion
In der Risikobeurteilung

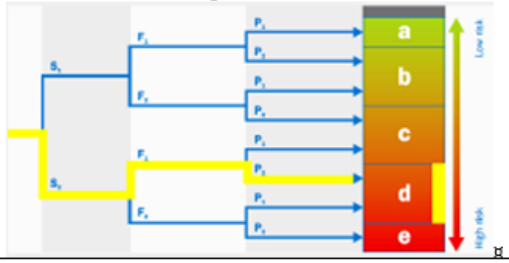
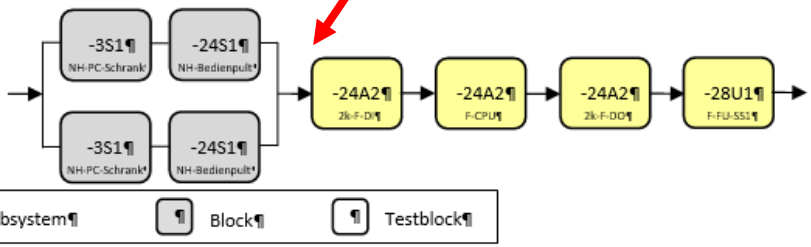
Feststehende trennende Schutzeinrichtungen	Anwendung der DIN EN ISO 13857, DIN EN SO 14120 Der Bereich wird mit feststehenden trennenden Schutzeinrichtungen umschlossen. Die beweglichen trennenden Schutzeinrichtungen werden als verriegelte ausgeführt. Wenn vorhersehbar ist das feststehende trennende Schutzeinrichtungen entfernt werden, müssen die Befestigungsmittel mit den feststehenden trennenden Schutzeinrichtungen verbunden bleiben. Der hintere Bereich des Antriebsmotors wird mit Blechen verkleidet.
Handlung im Notfall	Sicherheitsgerichtetes Anhalten des Antriebs SS1
Verriegelte trennende Schutzeinrichtung	Alle Türen werden mit Verriegelungseinrichtungen ausgerüstet die dann bei Öffnen ein sofortiges sicherheitsgerichtetes Anhalten des Antriebs einleiten SS1.
Manipulationsanreiz	Siehe: Abschnitt 8
Zuhaltung	Da es einen Nachlauf an der Maschine gibt ist eine Zuhaltung an der Schutzumhausung anzubringen.
Energieausfall Verhindern des unerwarteten Wiederanlaufens	Ein Energieausfall muss zu einem Anhalten des Antriebes führen. Nach einem Energieausfall darf der Motor nicht wieder anlaufen, es muss erst eine Rückstellfunktion ausgelöst werden. Danach kann die Maschine wieder eingeschaltet werden. DIN EN 60204-1. DIN EN 1037
Sicherheitsfunktion	
SF **Not-Halt – Stillsetzen Antrieb**	**Not-Halt – Stillsetzen Antrieb** Wenn einer der Not-Halt Taster betätigt wird dann muss der Antrieb sicherheitsgerichtet angehalten werden SS1. PLr=d S2: irreversible Verletzungen möglich. F1: Eingriff weniger als einmal pro Stunde P2: Ausweichen nicht möglich. Unerwarteter Anlauf.  Solange eine verriegelte Not-Halt Taster ausgelöst ist muss ein wieder anlaufen sicher verhindert werden. Nach der Einleitung eines Stoppbefehls durch eine Schutzeinrichtung muss der Stoppzustand aufrechterhalten bleiben, bis eine manuelle Rückstelleinrichtung betätigt wird und der sichere Zustand für einen Wiederanlauf gegeben ist.

Definition der Sicherheitsfunktion
Im Sistema Tool



Definition der Sicherheitsfunktion
Im Nachweis der funktionalen Sicherheit

4.5 SF05, Not-Halt – Stillsetzen Antrieb

Nachweis Sicherheitsfunktion nach DIN EN ISO 13849-1 und -2	Beschreibungen
SF-Nr.:	5
Abschnitt Risikobeurteilung	6.2.13
Identifizieren der SF	**Not-Halt – Stillsetzen Antrieb** - → Wenn einer der Not-Halt Taster betätigt wird dann muss der Antrieb sicherheitsgerichtet angehalten werden SS1. - → Solange eine verriegelte Not-Halt Taster ausgelöst ist muss ein wieder anlaufen sicher verhindert werden. - → Nach der Einleitung eines Stoppbefehls durch eine Schutzeinrichtung muss der Stoppzustand aufrechterhalten bleiben, bis eine manuelle Rückstelleinrichtung betätigt wird und der sichere Zustand für einen Wiederanlauf gegeben ist.
Eigenschaften festlegen	- → Alle Betriebsarten - → SS1 Antrieb
Erforderlicher Performancelevel	PLr=d S2: irreversible Verletzungen möglich. F1: Eingriff weniger als einmal pro Stunde. P2: Ausweichen nicht möglich. Unerwarteter Anlauf. 
Festlegen der Kategorie	3
Gestaltung und technische Realisierung der Sicherheitsfunktionen: Identifizieren der sicherheitsbezogenen Teile, die die Sicherheits-funktion ausführen	- → Sensor: → Not-Halt Taster - → Eingänge: → PNOZmulti zweikanalig - → CPU: → PNOZmulti - → Ausgänge: → PNOZmulti Relaisausgang zweikanalig - → Aktoren: → FU STO 

Sicherheitsfunktion SRASW

Validierung der SRASW
Softwarespezifikation, was der Programmierer wissen muss

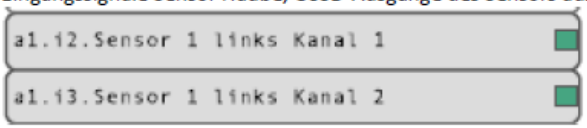
6.5 SF05, Not-Halt – Stillsetzen Antrieb

SF Nr.	5
Abschnitt Risikobeurteilung	6.2.13
Softwarespezifikation	Identifizierung der Sicherheitsfunktion: Not-Halt – Stillsetzen Antrieb - Wenn einer der Not-Halt Taster betätigt wird dann muss der Antrieb sicherheitsgerichtet angehalten werden SS1. - Solange eine verriegelte Not-Halt Taster ausgelöst ist muss ein wieder anlaufen sicher verhindert werden. - Nach der Einleitung eines Stoppbefehls durch eine Schutzeinrichtung muss der Stoppzustand aufrechterhalten bleiben, bis eine manuelle Rückstelleinrichtung betätigt wird und der sichere Zustand für einen Wiederanlauf gegeben ist. Sicherheitsfunktionen mit erforderlichem PL und zugehörigen Betriebsarten: - Performance Level d / Kategorie 3 - Alle Betriebsarten Leistungskriterien, z. B. Reaktionszeiten: - SS1 Zeit = 2000ms Verbale Beschreibung: Wir einer der Not-Halt Taster in Schaltschrank oder Bedienpult betätigt, dann muss der Frequenzumrichter des Antriebes sicherheitsgerichtet stillgesetzt werden. Der Frequenzumrichter wird mittels Bremsrampe innerhalb 2 Sekunden heruntergebremst, danach mit in STO sicher stillgesetzt. Hardwarearchitektur mit externen Signalschnittstellen und Erkennung und Beherrschung externer Ausfälle: - Sensor: Not-Halt Taster - Eingänge: PNOZmulti zweikanalig, Taktsignale, Plausibilitätsprüfung - CPU: PNOZmulti, zertifizierte Bausteine des Softwareherstellers - Ausgänge: PNOZmulti Relaisausgang zweikanalig, Plausibilitätsprüfung - Aktoren: FU STO

Validierung der SRASW
Softwareentwurf, wie es der Programmierer umsetzen muss

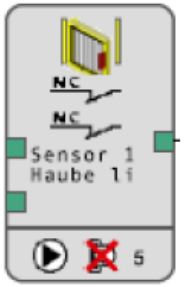
Softwareentwurf:

- Eingangssignale Sensor Haube, OSSD-Ausgänge des Sensors auswerten



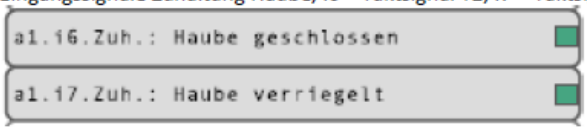
Eingänge

- I2/I3 mittels Schutztür Baustein auswerten, Querschlusserkennung und Plausibilitätsabfrage



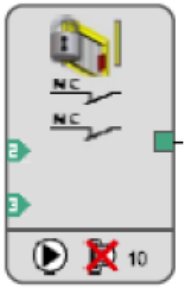
Funktionsbaustein

- Eingangssignale Zuhaltung Haube, I6 = Taktsignal T2, I7 = Taktsignal T3



Eingänge

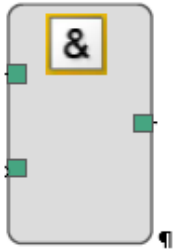
- I6/I7 mittels Schutztür Baustein auswerten, Querschlusserkennung und Plausibilitätsabfrage



Funktionsbaustein

Validierung der SRASW
Softwareentwurf, wie es der Programmierer umsetzen muss

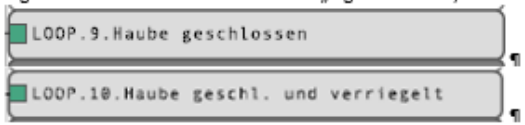
- Auswertung der Ergebnisse von Zuhaltung und Haube, mit UND verknüpfen



Verknüpfung

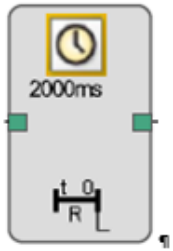
- I12 Reset Taster Signal auswerten, Rücksetzen darf erst möglich sein, wenn die Haube geschlossen und verriegelt ist

- Ergebnis der Schutztür Bausteine muss „high aktiv" sein, für die weitere Verarbeitung auf einen Merker legen



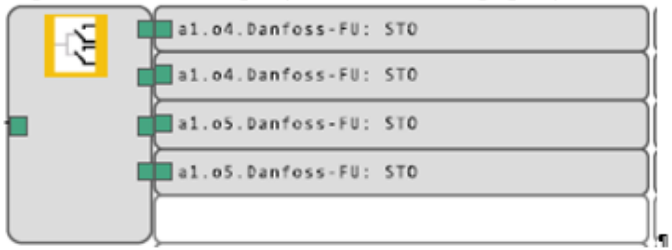
Merker/Ergebnis

- Verzögerungszeit SS1, 2000ms



Verzögerungszeit

- Ausgabebaustein Ansteuerung Frequenzumrichter und Ausgänge O4/O5



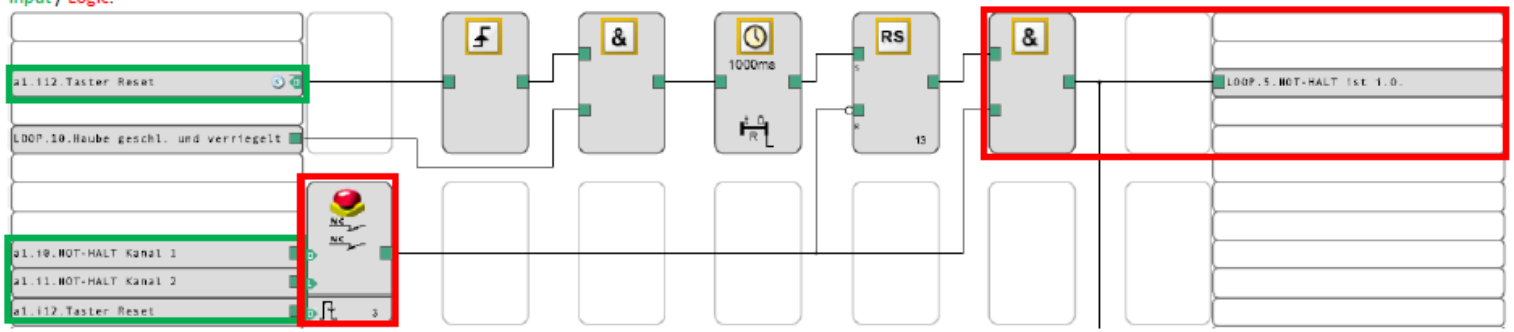
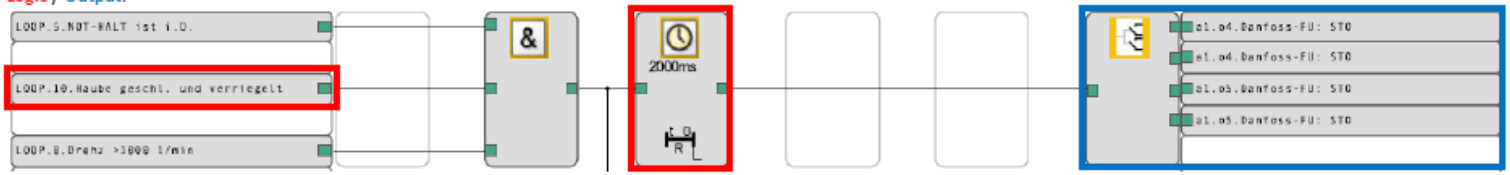
Funktionsbaustein
Ausgänge

Validierung der SRASW
System- und Modulgestaltung, Datenflussanalyse

Während die Systemgestaltung durch die Angaben im Abschnitt Softwarespezifikation abgedeckt wird, kann bei der Überprüfung der Modulgestaltung und der Modultests, auf die im Projekt konsequent angewendeten und bereits vom Hersteller verifizierten und validierten Funktionsbausteine verwiesen werden.

Bei der Prüfung der Kodierung mittels Datenflussanalyse wird der Nachweis des korrekten Signalflusses entsprechend der Spezifikation nachgewiesen.

Der eigentliche Integrationstest muss mittels Grey- und Black-Box-Test an der Maschine erfolgen.

Systemgestaltung	Siehe Spezifikation
Modulgestaltung	Es werden nur von dem Hersteller der PNOZ Multi geprüfte Funktionsbausteine eingesetzt
Kodierung / Datenflussanalyse	Input / Logic:  Logic / Output: 
Modultest	Es werden nur von dem Hersteller der PNOZ Multi geprüfte Funktionsbausteine eingesetzt
Integrationstest	Von Fa. ??? zu erbringen
Validierung	Dieses Dokument

Validierung der SRASW
Funktionaler und erweiterter Test, Testabdeckung

Die Anforderungen der DIN EN ISO 13849 Teil 1 und 2 zu SRASW unterscheiden beim Aspekt der Validierung zwischen Funktionalen Tests (als Basismaßnahme) und erweitertem Funktionstest (als zusätzliche Maßnahme).

- Bei einem funktionalen Test werden die Sicherheitsfunktionen, wie spezifiziert, überprüft. Erforderlich für PL a bis b, ausreichend für PL a und b.
- Beim erweiterten Funktionstest werden typischerweise Fehler in den Peripheriegeräten der Steuerung oder der Steuerung selbst eingebaut bzw. simuliert. Erforderlich ab PL c.

Tabelle 3:
Empfehlungen für Testabdeckung

Testabdeckung in Anlehnung an IEC 61508-3	PL_r SIL	Umfang der Testfälle im Black-Box-Testen der SRASW
100 % der Eingänge	a, b und c SIL1	Mindestens alle sicherheitsrelevanten Eingänge, d. h. alle Schutzeinrichtungen und damit die Funktionsbausteine der Vorverarbeitungsebene einmal anfordern und den Wiederanlauf testen. Ziel: Stellt sicher, dass jedes Unterprogramm der SRASW, auch die Funktionsbausteine der Ansteuerlogik und Ansteuerungsebene, mindestens einmal aufgerufen worden ist. Empfohlen wird aber auch für diese PL_r der Testumfang wie in der nächsten Zeile für PL_r d.
100 % der Programmanweisungen	d SIL2	Alle Sicherheitsfunktionen in allen Betriebsarten anfordern und den Wiederanlauf testen. Ziel: Stellt sicher, dass alle Anweisungen in der Ansteuerlogik der SRASW (Abbildung 7) mindestens einmal ausgeführt worden sind. Enthält PL_r a, b, c.
100 % der Programmverzweigungen	e SIL3	Alle Sicherheitsfunktionen in allen Betriebsarten anfordern, den Wiederanlauf testen und alle Diagnosefunktionen durch Fehlersimulation testen. Ziel: Beide Möglichkeiten jeder Verzweigung in der Ansteuerlogik der SRASW sollten getestet werden. Enthält PL_r a, b, c, d.

Quelle:
IFA Fachbericht 2/2016

Validierung der SRASW
Gefährdungen durch Modifikation

*Auch bereits getestete **SRASW** wird während Implementierung und Inbetriebnahme häufig angepasst und dabei geändert.*
*Auf diesem Wege können Fehler in den bereits geprüften **Code** eingebracht werden, oder neue Wechselbeziehungen zu bisher unbekanntem Fehlern führen.*

Nach **Modifikationen** muss stets wieder an dem Punkt in den Software Entwicklungsprozess im V-Modell eingestiegen werden, an welchem die Veränderung erfolgte:

- Bei geänderter Codierung sind evtl. das **Codereview**, der **Integrationstest** sowie die Validierung erneut durchzuführen.
- Wurde sogar die **Spezifikation** geändert werden, ist diese ebenfalls erneut zu verifizieren, z. B. durch **Review (Gegenlesen)** einer **anderen Person**, damit sich keine Fehler an anderer Stelle der Spezifikation einschleichen. Dementsprechend müssen alle Entwicklungs- und Verifikations-maßnahmen sowie die Validierung der betroffenen Sicherheitsfunktionen wiederholt werden.
- Je nach PLr für die SRASW-Entwicklung von einer:
  - Anderen Person,
  - unabhängigen Person,
  - unabhängigen Abteilung,
  - unabhängigen Organisation

Quelle: IFA Fachbericht 2/2016

Validierung der SRASW
Test, Überprüfung und Unabhängigkeitsgrade

Tabelle 4:
Definition der Unabhängigkeitsgrade für SRASW (angelehnt an DIN EN 61508-4:2011)

	Definition (Beispiel) als Empfehlung des IFA
Andere Person	Person, die nicht die zu überprüfende Tätigkeiten selbst durchgeführt hat, aber in das Projekt eingebunden sein kann oder Verantwortung trägt (ja: Projektleitung, Vorgesetzte, Beteiligte an der betrachteten Tätigkeit)
Unabhängige Person	Person, die nicht eingebunden ist in die zu überprüfende Tätigkeiten und die keine direkte Verantwortung für diese Tätigkeiten trägt (nein: Projektleitung, Vorgesetzte, Beteiligte an der betrachteten Tätigkeit; ja: Hardwareprojektierende für SRASW-Entwicklung, Inbetriebnehmende für Projektierungstätigkeit)
Unabhängige Abteilung	Abteilung, die nicht in Verbindung mit den Projekt-/Entwicklungsabteilungen steht, die verantwortlich für die SRASW-Tätigkeiten sind (Person aus der Qualitätsabteilung/der CE-Abteilung/dem Schaltanlagenbau usw.)
Unabhängige Organisation	Organisation, die aufgrund ihres Managements und ihrer anderen Mittel nicht in Verbindung mit den Entwicklungsorganisationen steht (anderer Geschäftsbereich, anderes Unternehmen, Prüfstelle)

Tabelle 5:
Grad der Unabhängigkeit für Verifikation und Validierung (SRASW)

Minimaler Unabhängigkeitsgrad für Verifikation und Validierung bei SRASW * als Empfehlung des IFA	Maßgeblicher PL_r für SRASW-Entwicklung *			
	a und b	c	d	e
Andere Person**	Für alle SRASW empfohlen	Für alle SRASW	Standard-SRASW	Nicht ausreichend
Unabhängige Person	Möglich, aber nicht notwendig	Möglich, aber nicht notwendig	Komplex oder neue SRASW	Standard-SRASW
Unabhängige Abteilung	Möglich, aber nicht notwendig	Möglich, aber nicht notwendig	Möglich, aber nicht notwendig	Komplex oder neue SRASW
Unabhängige Organisation***	Möglich, aber nicht notwendig	Möglich, aber nicht notwendig	Möglich, aber nicht notwendig	Möglich, aber nicht notwendig

Quelle:
IFA Fachbericht 2/2016

Weidle-Safety - Stefan Weidle, freier technischer Redakteur

Mobil: 0151 21553726
www.weidle-safety.de

Herrenzimmerner Strasse 11
78667 Villingendorf