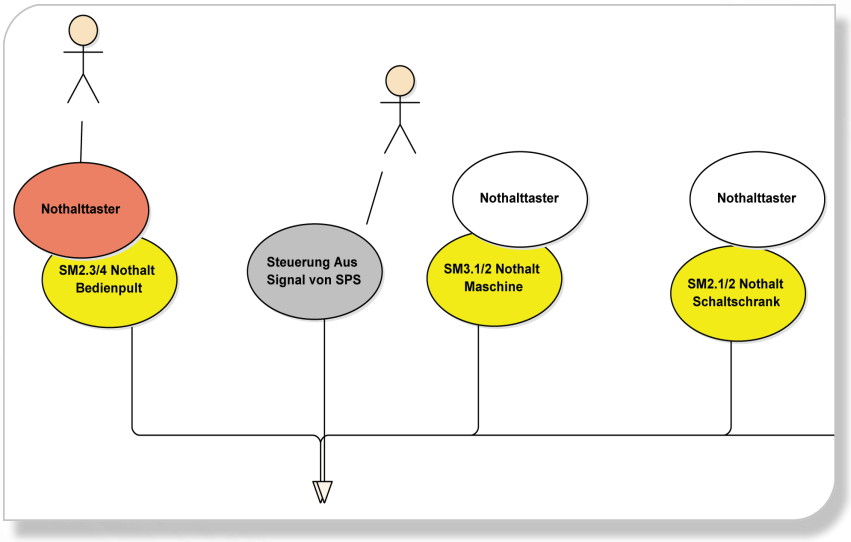
pantec automation



WIR REGELN DAS.

INSIGHTS

Nach dem Sicherheitskonzept in 3 Schritten zur sicheren Safety Software

Konzept wurde entworfen und getestet bei:

risomat

MIT UML-DESIGN

... in drei Schritten zur sicheren Safety Software

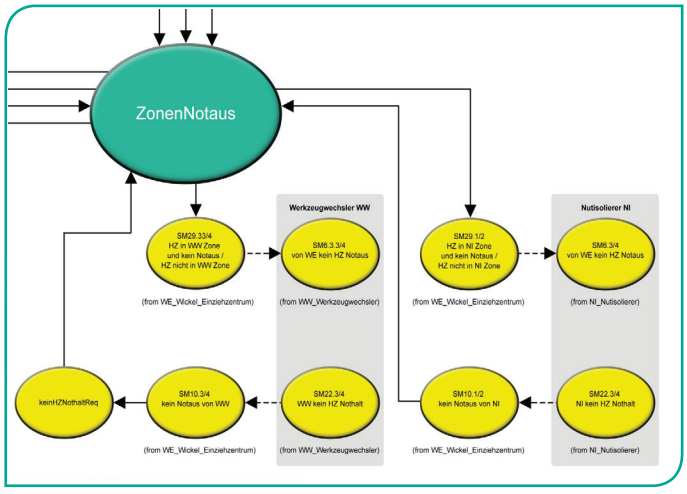
Im Maschinenbau sind die Informationen zur Risikoanalyse und -beurteilung – nicht zuletzt durch die Vorgaben der Maschinenrichtlinie – gut dokumentiert. Doch die Abbildung und Umsetzung der Sicherheitsfunktionen auf die Safety-SPS (SSPS) resultiert oft in einer intransparenten, meist nur rudimentär beschriebenen Black Box, welche es für Dritte schwierig macht, die Funktionalität nachzuvollziehen und unabhängige Testverfahren zur Abnahme zu entwickeln.

Dies bedeutet für Sicherheitsbeauftragte, Maschinen im guten Glauben bezüglich der SSPS-Funktionalität freizugeben. Auch Konstrukteure und Softwareingenieure, welche den operativen Betrieb der Maschine nicht unnötigerweise durch die Sicherheitsfunktionalität einschränken wollen, haben wegen der fehlenden Dokumentation grosse Abstimmungsschwierigkeiten.

Auch Pantec Automation war regelmässig mit dieser Problematik konfrontiert. Im Sommer 2015 übernahm das Entwicklungsteam ein Kundenprojekt im Bereich Safety-SPS, welches mit klassischer, textueller Beschreibung nicht mehr zu lösen war. Es ging dabei um ein Wickel- und Einziehzentrum für Elektromotoren der Risomat GmbH in Baienfurt, bei der sich die Sicherheitszonen – in Abhängigkeit der Position des Transportkrans – dynamisch veränderten. Die konventionellen Methoden waren zur Beschreibung dieser dynamischen Zustände nicht mehr ausreichend. Daher stellte sich den Pantec Ingenieuren die Frage, wie so eine Anlage in ihrer Komplexität transparent dargestellt werden kann.

Zugleich sollte geklärt werden, wie der Prozess der Safety-Softwareentwicklung ausschauen kann, damit die Sicherheitsfunktionalität optimal gestaltet werden und das Vorgehen bis zur Softwareabnahme umgesetzt werden kann.

Das Ergebnis wird in diesem Dokument aufgezeigt. Es wendet sich an Sicherheitsbeauftragte, Konstrukteure und Softwareingenieure, welche nach Möglichkeiten suchen, die Logik einer Safety-SPS Software transparent zu entwerfen, zu dokumentieren und über einen nachvollziehbaren Test sicherzustellen, dass die Funktion der Safety-SPS an der Maschine oder Anlage selbst umfassend und lückenlos geprüft wird.



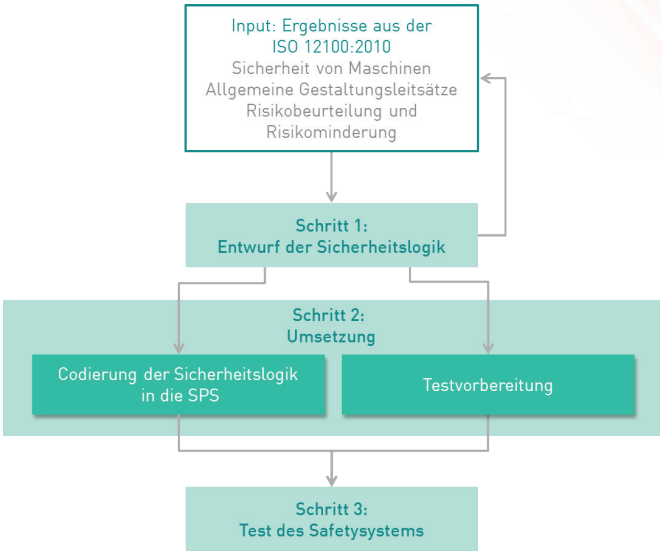
Die 3 Schritte zur sicheren Safety-SPS Software im Schnelldurchlauf

Die Entwicklung der Safety-SPS Software startet nach Abschluss des in der ISO-Norm 12100:2010 beschriebenen Prozesses der Risikoanalyse, Risikobewertung und Risikominderung (Sicherheitskonzept). Aus den Massnahmen der Risikominderung ergeben sich unter anderem jene elektrotechnischen Komponenten, welche über die Software der SSPS verarbeitet werden.

Im **Schritt 1** werden die im Elektroschema eingearbeiteten Safetykomponenten zusammengefasst. Die Safetyeingangselemente werden als Use Cases in ein Use Diagramm übernommen, ebenso die Safetyausgänge.
Auf dieser Basis wird gemeinsam von Konstruktion und Softwareentwicklung - mit Hilfe von UML - die Sicherheitslogik ausgearbeitet und beschrieben. Abschliessend wird die definierte Sicherheitslogik durch eine Simulation der Maschinenbedienung mit den Maschinengegebenheiten abgestimmt. Diese Simulation zielt darauf ab, den Maschinenbetrieb so wenig als möglich durch die Sicherheitsmassnahmen der Maschinen einzuschränken und die Vollständigkeit der Sicherheitsmassnahmen nochmals zu prüfen.

Im **Schritt 2** wird die SSPS codiert, parallel dazu wird der Abnahmetest vorbereitet. Dieser umfasst neben einer logischen Prüfung der Funktionalität vorab ein strukturiertes Prüfen der gesamten Safety Hardware und deren Verdrahtung.

Zum Schluss erfolgt im **Schritt 3** der Abnahmetest des Safetysystems und abschliessend die Freigabe durch den Sicherheitsbeauftragten.



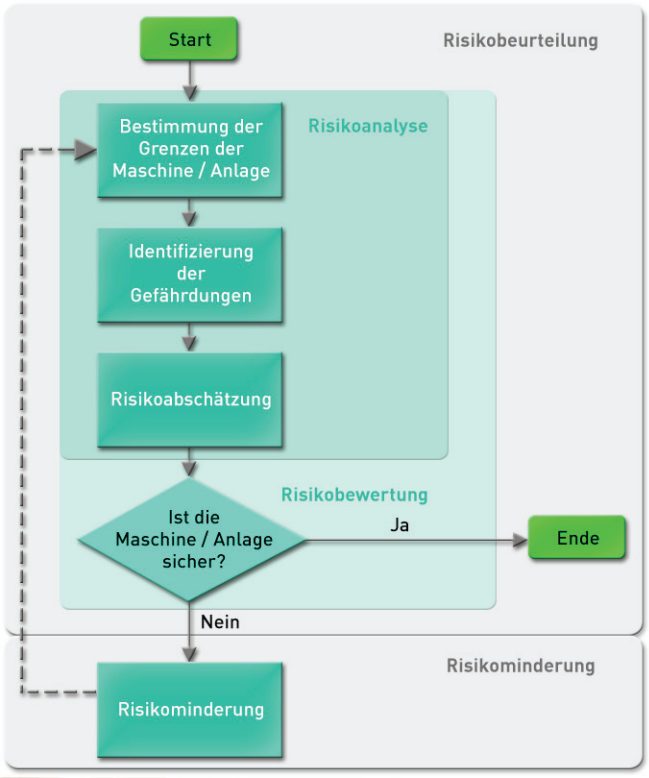
Die 3 Schritte zum nachvollziehbar geprüften Safetysystem im Überblick

Input: Ergebnisse aus der
ISO 12100:2010
Sicherheit von Maschinen
Allgemeine Gestaltungsleitsätze
Risikobeurteilung und
Risikominderung

Input für den Prozess zur sicheren SSPS Software:
Die Ergebnisse aus dem Sicherheitskonzept nach ISO-12100:2010

Die ISO-Norm 12100: 2010 „Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung“ ist in vielen Unterlagen dokumentiert und soll hier nur im Überblick tangiert werden. Der Ablauf der ISO 12100:2010 gliedert sich in folgende Schritte:

1. Bestimmung der Grenzen der Maschine / Anlage
2. Identifizierung der Gefährdungen / Risiken
3. Risikoabschätzung
4. Risikobewertung
5. Risikominderung



In der Phase der Risikominderung wird geprüft, mit welchen Massnahmen die determinierten Gefährdungen hinreichend gemindert werden können.
Nach EN ISO 12100 kommt ein 3-Stufen-Verfahren zum Einsatz, mittels dem eine erforderliche Minderung einer Gefahr erzielt werden kann.

3-Stufen-Verfahren zur Minderung von Gefahren laut ISO 12100:2010

1. Inhärent sichere Konstruktion

2. Technische Schutzmassnahmen und/oder ergänzende Schutzmassnahmen.

3. Aufzeigen möglicher Benutzerinformationen, welche dann erforderlich werden, wenn trotz inhärent sicherer Konstruktion und dem Einsatz technischer und ergänzender Schutzmassnahmen noch immer Risiken verbleiben. Die Benutzerinformation muss Personen entsprechend DIN EN ISO 12100 auf diese Restrisiken aufmerksam machen.

Hinweis:

Für den im Folgenden beschriebenen Prozess sind jene unter Schritt 2 definierten technischen Schutzmassnahmen relevant.

Die 3 Schritte zur sicheren SSPS Software am Beispiel eines Einziehzentrums für die Elektromotorenproduktion

Im Folgenden wird am Beispiel des Einziehzentrums der gesamte Prozess der 3 Schritte von der Zusammenstellung der relevanten Safetyelemente bis zur implementierten, getesteten Safetysoftware, beschrieben.
Die Risikoanalyse eines solchen Einziehzentrums zeigt, dass beim Nachlegen von Verbrauchsmaterial in die Maschine die Gefahr einer Quetschung vorliegt. Daher wird dieses Einziehzentrum durch einen Schutzzaun gesichert und der Zugangsbereich mit einer Schutztür über einen Schutzschalter abgesichert. Ein Öffnen der Türe löst einen Nothalt der Maschine aus. Um diese wieder zu starten, muss die Türe geschlossen, und die Nothaltmeldung (ausserhalb des Raumes) quittiert werden.
Dem Einziehzentrum übergeordnet ist ein Nothaltschalter, welcher auch auf das Einziehzentrum wirkt.

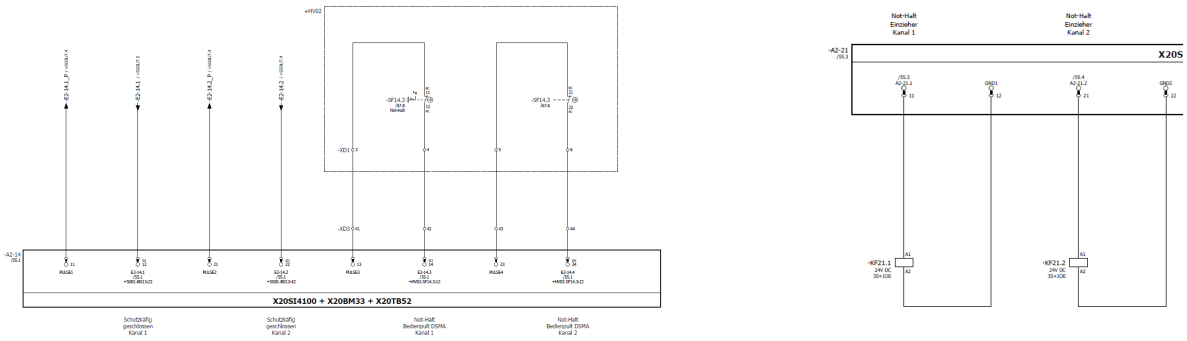
Ausgangssituation: Darstellung der Absicherungsmassnahmen eines Einziehzentrums für die Elektromotorenproduktion

Schritt 1: Entwurf der Sicherheitslogik

1.1. Safety-Elemente (Ein- und Ausgänge) für das Einziehzentrum eruieren

In einem ersten Schritt werden die als Ergebnis der Massnahmen zur Risikominderung im Elektroschema erfassten Sicherheitselemente (Safety-Elemente) als Grundlage für den Aufbau der Use Cases eruiert und am besten gleich in ein entsprechendes Tool übernommen (wie z.B. das für dieses Beispiel verwendete Enterprise Architects).

Wie vorab beschrieben, sind in unserem Beispiel - seitens der Konstruktion - zwei Notaus-Szenarien vorgesehen, welche im Elektroschema abgebildet sind. Zum Einen die Öffnung der Schutztür, zum Anderen der übergeordnete Nothalttaster.



Ausgangssituation: Schemaauszug Sicherheitsein- und ausgangselemente des Einziehzentrums

Der Schemaauszug links zeigt den Schutzschalter der Schutztüre sowie den übergeordneten Nothalttaster; beide in 2-kanaliger Ausführung.

Das rechte Bild zeigt die Freigabe des Antriebes für den Materialeinzug des Einziehzentrums; ebenfalls 2-kanalig.

Use Cases (Anwendungsfälle, Szenarien) sind Interaktionen zwischen Benutzer und Maschine. Use Cases sind im Fall der Safety-Funktionalität all jene Elemente an der Maschine, deren Betätigung/Auslösung zu einer Verarbeitung seitens der SSPS führen.

Use Case Legende:

Akteur

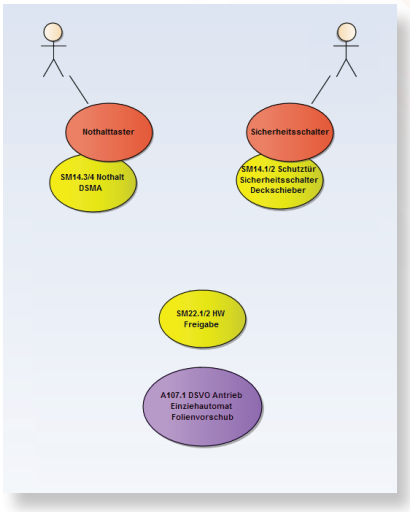
Anwendungsfall

Verlinkung auf SSPS

Zur grafischen Darstellung der Sicherheitslogik werden sogenannte Use Case Diagramme aus der UML-Modellierung verwendet

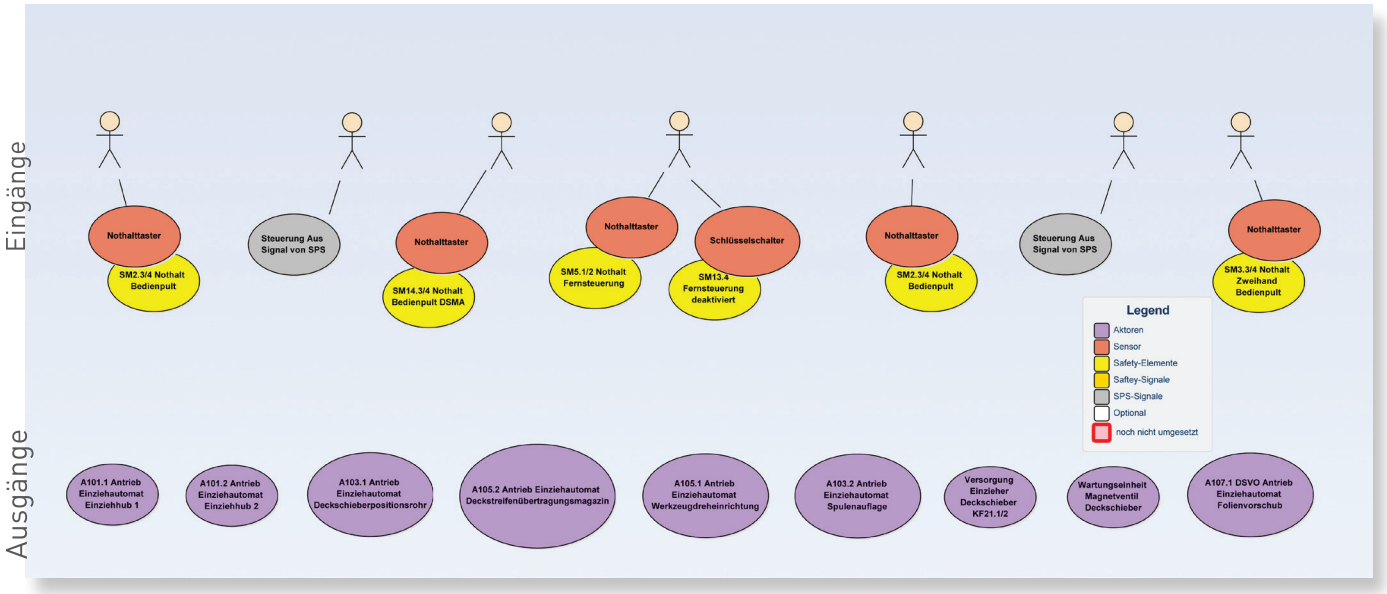
1.2. Safetyelemente ins UML übernehmen

Nun werden die im Schema dargestellten Safetyelemente ins UML übernommen. Im Beispiel des Einziehzentrums handelt es sich um den Use Case der Schutztüre sowie jenen des übergeordneten Nothalttasters, ausgangsseitig die zugehörige Freigabe des Antriebs für den Materialeinzug.



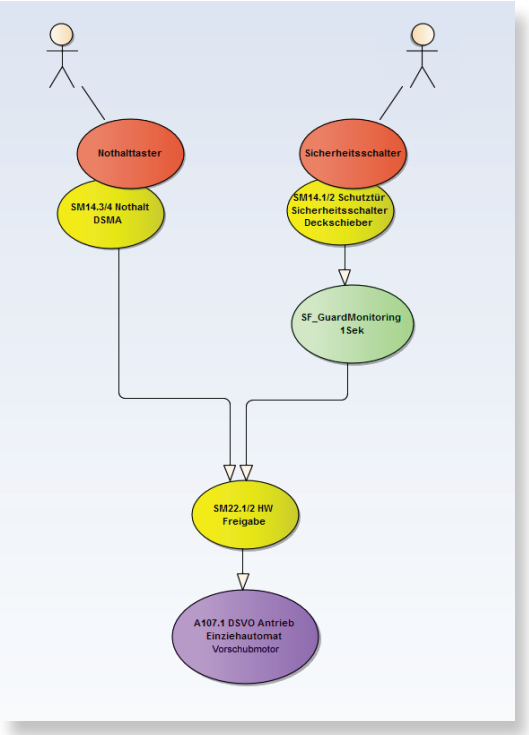
Sicherheitselemente für Ein- und Ausgang des Einziehzentrums

Dieses Prozedere wird nun schrittweise für alle im Schema angeführten Sicherheitselemente durchgeführt, sodass dann alle SSPS-Ein- und Ausgangselemente in der UML Darstellung visualisiert werden.
Hier zeigt sich nun ein erster wesentlicher Vorteil der UML-Beschreibung: es sind alle Safetyelemente, sowohl aktiv als auch passiv visualisiert. So hat man beim folgenden Entwurf der Sicherheitslogik alle Elemente vor sich, vergisst nichts und kann einfach weitere Elemente in die Logik mit aufnehmen oder weitere Verknüpfungen herstellen.



Auszug der SSPS Ein- und Ausgänge im UML dargestellt

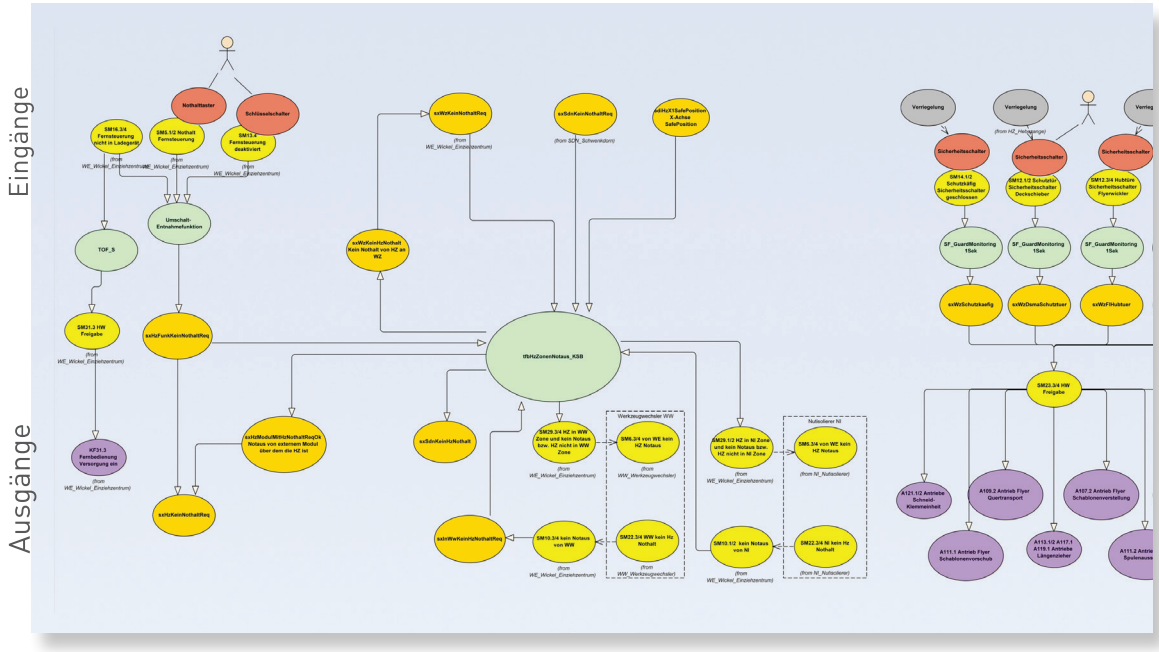
1.3. Beschreiben der Sicherheitslogik

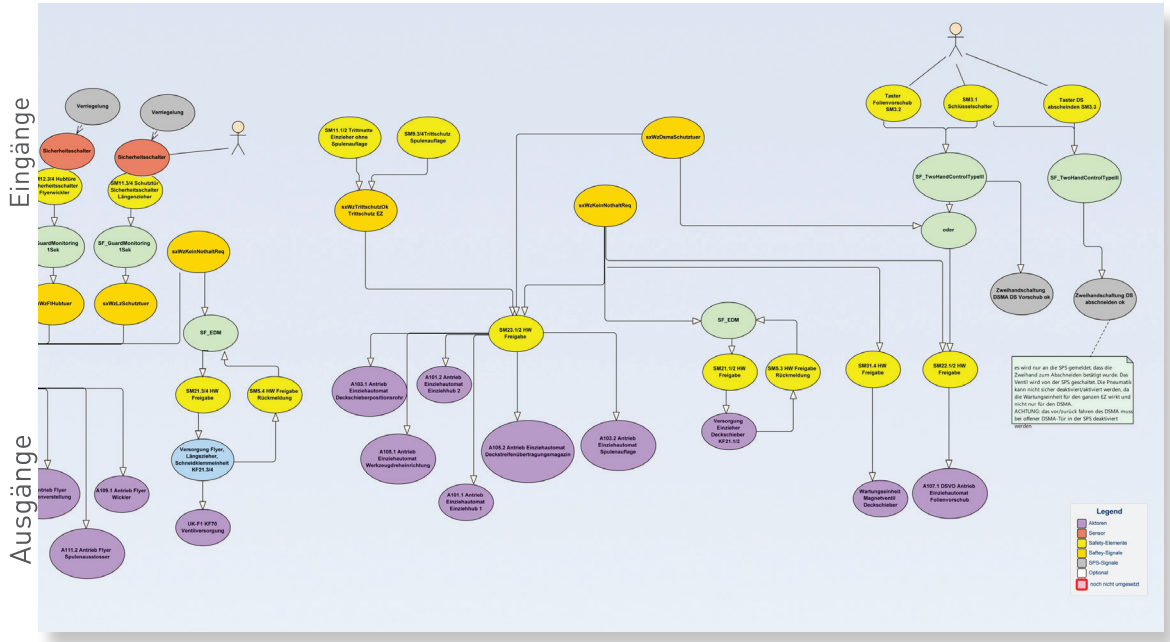


Verknüpfung der SSPS Elemente des Einziehzentrums

Mit Vorliegen der Benutzerszenarien bildet der Softwareentwickler nun gemeinsam mit dem Konstrukteur bzw. dem Sicherheitsverantwortlichen für die Maschine die Sicherheitslogik der Maschine ab, d.h. man definiert, welche Szenarien zu welchen Sicherheitsstati an der Maschine führen.
Am einfachen Beispiel des Vorschubmotors für das Verbrauchsmaterial ist die Voraussetzung für die Freigabe des Antriebs, dass die Anlage seitens des übergeordneten Nothalttasters freigegeben, und der Sicherheitsschalter der Schutztüre geschlossen ist. Im Use Case Diagramm wird dies wie im nebenstehenden Bild visualisiert.

Nun wird die Sicherheitslogik für alle Anwendungsfälle definiert und im UML visualisiert.

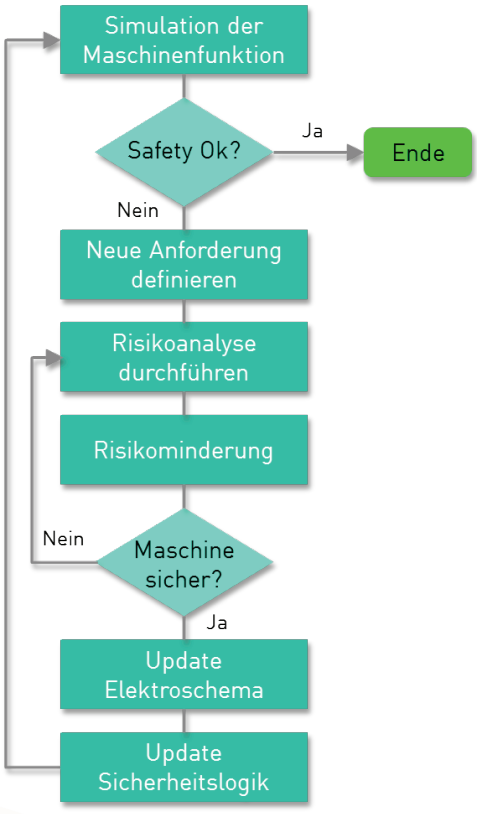




Die Darstellung von Safety-Elementen und deren Verknüpfungen auf einen Blick hilft Klarheit zu schaffen und den Überblick zu bewahren.

1.4. Validierung der Sicherheitslogik

Sobald die gesamte Sicherheitslogik beschrieben ist, wird deren Funktionalität nun in Abstimmung mit der Maschinenfunktionalität durch eine virtuelle Simulation auf Vollständigkeit und Praktikabilität geprüft. Durch die einfache Sprache des UML und die intuitive Darstellung der Sicherheitslogik wird dieser Schritt signifikant vereinfacht.

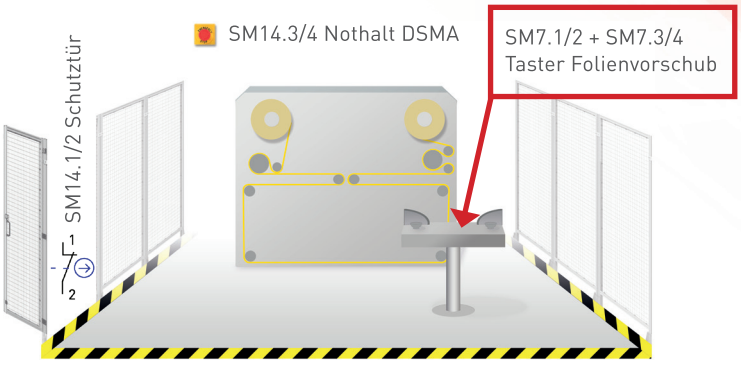


Simulation der Maschinenfunktion

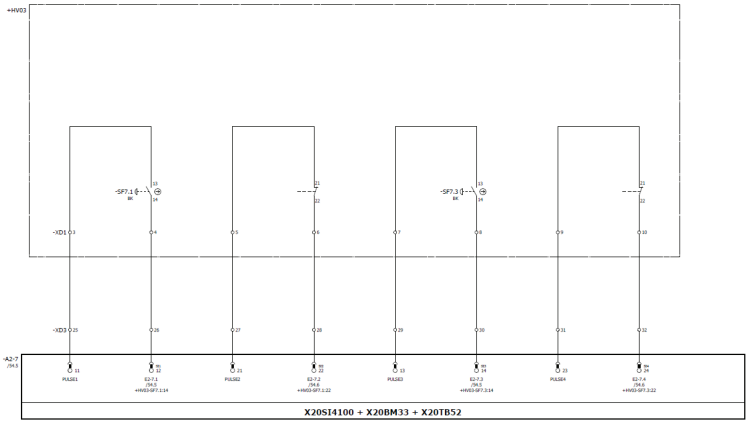
Es empfiehlt sich bei der Validierung der Sicherheitslogik konkret die Bedienung der Maschine zu simulieren, d.h. die verschiedensten Bedienungssituation und Operatoreingriffe durch zu spielen und zu prüfen, ob die definierten Sicherheitsmassnahmen ausreichend und passend sind.

Dabei kann es zur Aufdeckung von Unstimmigkeiten kommen, die bis dato noch nicht berücksichtigt wurden bzw. kann festgestellt werden, dass die Sicherheitsmassnahmen den Betrieb der Maschine einschränken. Werden dann neue Bedien- oder Sicherheitsfunktionen festgelegt, werden diese wieder nach dem Ablauf der ISO 12100:2010 analysiert, bewertet und entsprechende Risikominderungsmassnahmen durchgeführt, bis die Maschine wieder als sicher deklariert werden kann. Der jeweilige Durchlauf wird mit dem Update des Elektroschemas und der Aktualisierung der Sicherheitslogik abgeschlossen. Die Validierung der Sicherheitslogik ist fertig, wenn keine neuen Anforderungen mehr definiert werden und die Risikoanalyse keine mehr zu mindernden Risiken aufzeigt.

Bei unserem Beispiel des Einziehzentrums ergab eine Simulation der Bediensituation, dass dem Konstrukteur bewusst wurde, dass es umständlich ist, wenn man nach dem Zuführen des neuen Verbrauchsmaterials die Schutzzone verlassen und die Schutztüre schliessen musste, um die Maschine wieder freizugeben. Daraus ergab sich die neue Anforderung, den Einziehmotor auch bei offener Schutztüre zu betreiben. Die Risikoanalyse ergab, dass mit dieser gewünschten Funktion das mit der Schutztür reduzierte Risiko - die Finger zwischen den Einzugswalzen einzuklemmen - wieder gegeben war. Als Möglichkeit zur Risikominderung entschied sich der Konstrukteur dafür, beim Materialeinzug einen Zweihandtaster einzusetzen, welche eine Maschinenfreigabe ermöglicht und sicherstellt, dass beide Hände des Maschinenbedieners an den Tastern sind und somit nicht beim Materialeinzug sein können. Diese Risikominderung wurde als ausreichend erachtet. Entsprechend wurde danach das Elektroschema um die Sicherheitstaster ergänzt und die Sicherheitslogik entsprechend erweitert.

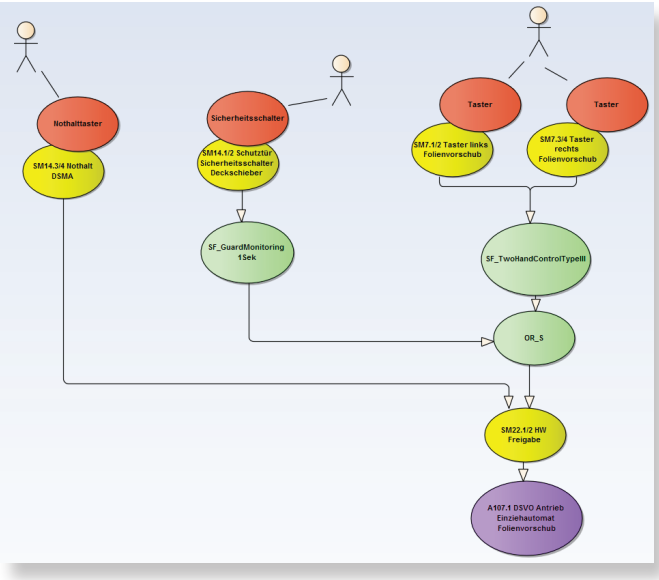


Sicherheitsfunktionen des Einziehzentrums
um einen Zweihand-Taster ergänzt



Schema Update: Zusätzlich zum Schutzschalter der Türe wurde nachträglich ein Zweihandtaster implementiert,
um die Bedienung des Einziehzentrums zu vereinfachen

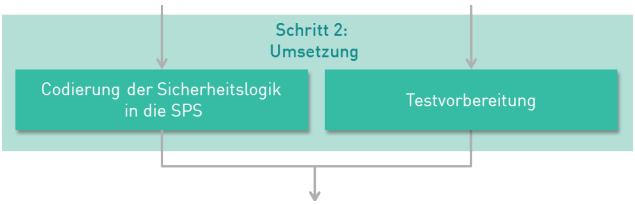
1.5. Update der Sicherheitslogik im UML



Mit der Erweiterung um das neue Sicherheitselement „Zweihandtaster“ wird nun das UML-Diagramm entsprechend erweitert. Zuerst erfolgt die Erweiterung um den Use Case für die Zweihandtaster, danach werden die logischen Verknüpfungen adaptiert. In diesem Fall ist der Vorschubmotor freigegeben, solange der zentrale Notaus nicht aktiviert ist und entweder die Schutztüre geschlossen ist, oder die Zweihandtaster aktiviert sind.

Adaption der Sicherheitslogik und Freigabe

Mit den Review-Feedbacks vom vorigen Punkt „Validierung der Sicherheitslogik“ wird die Sicherheitslogik im UML überarbeitet und dann zur Umsetzung freigegeben.



Schritt 2: Umsetzung - Codierung und Testvorbereitung

Mit der freigegebenen Sicherheitslogik kann nun die Codierung der Safety SPS durchgeführt werden. Gleich parallel dazu werden für die Abnahme der SSPS die Testszenarien bzw. die Testprotokolle vorbereitet.

2.1. Codierung

Mit den Use Cases und der Darstellung der Sicherheitslogik im UML liegen für die Softwareentwicklung die Grundlagen für die Codierung vor.

2.2. Testvorbereitung

Mit der Dokumentation der Use Cases bzw. der UML-Visualisierung ergibt sich nun auch der Vorteil, dass die Codierung und die Testvorbereitung völlig getrennt ablaufen können. D.h. die Tests der Software werden in diesem Fall nicht – wie oft üblich – aus den Softwarealgorithmen abgeleitet, sondern direkt aus den Use Cases bzw. der Sicherheitslogik. So wird nicht getestet was programmiert ist, sondern das, was definiert ist!

Der Testablauf besteht im Wesentlichen aus 2 Schritten:

A) Funktionstest der Safety-Elemente und

B) Logiktest der Safetyfunktionalität.

A) FUNKTIONSTEST DER SAFETY-ELEMENTE

Im ersten Schritt wird die Hardwareprüfung der Erfasser-Komponenten vorbereitet. Dabei wird jeweils zuerst die Tasterfunktion geprüft und danach die Schalterkontakte getestet.

Thema		Testpunkt	Testbeschreibung	Ausgangslage
Safety-Erfasser-Komponenten				
1	**Nothalttaster DSMA**			
1	Funktion Notaustaster	Funktion	Überprüfen der Tasterfunktion	Steuerung ein
2	Abschaltung Kanal 1	Schalterkontakt 11/12 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberw achung der Klemme SM14. 3/4	Steuerung ein
3	Abschaltung Kanal 2	Schalterkontakt 21/22 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberw achung der Klemme SM14. 3/4	Steuerung ein
2	**Schutztür DSMA**			
1	Funktion Taster 1/2	Schutztür entriegeln Schutztür öffnen Schutztür verriegeln	überprüfen SM14. 1/2 abgeschaltet	Steuerung ein
2	Funktion Taster 2/2	Schutztür schliessen	überprüfen SM14. 1/2 eingeschaltet	Steuerung ein
3	Abschaltung Kanal 1	Schalterkontakt 21/22 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberw achung der Klemme SM14. 1/2	Steuerung ein
4	Abschaltung Kanal 2	Schalterkontakt 41/42 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberw achung der Klemme SM14. 1/2	Steuerung ein

Testprozesse Safety-Erfasser-Komponenten

B) LOGIKTEST DER SAFETYFUNKTIONALITÄT

Im zweiten Schritt wird die Prüfung der Sicherheitslogik vorbereitet, d.h. ob die Verknüpfung der Safetyelemente - wie im UML konzipiert - in der SSPS umgesetzt wurde.

Thema		Testpunkt	Testbeschreibung	Ausgangslage	Testresultat	Test	Tester	Wertung	Prüfer	Datum	Memo
Safety Aktoren											
1	Achsfreigabe DSVO										
1	Achse freigegeben	SM22.1\2 eingeschaltet folgende Regler sind RDY: -A107.1 DSVO Antrieb	Kontrolle: Achsen sollte das RDY durchgehend leuchten	Steuerung ein Schutztüre DSMA geschlossen							
2	Verdrahtungsprüfung	obige Achsen nicht RDY	SM22.1 und SM22.2 separat öffnen und RDY kontrollieren	Steuerung ein Schutztüre geschlossen SM22.1\2 eingeschaltet							
3	Achse sperren Schutztüre	obige Achsen nicht RDY	Schutztüre öffnen	Steuerung ein SM22.1\2 eingeschaltet							
4	Achsen freigegeben Zweihandbedienung ok	SM22.1\2 eingeschaltet folgende Regler sind RDY: -A107.1 DSVO Antrieb	Kontrolle: Achsen sollte das RDY durchgehend leuchten Gültige Zweihandbedienung	Steuerung ein Schutztüre DSMA offen							
5	Achsen gesperrt keine Zweihandbedienung	SM22.1\2 schalten ab obiger Regler nicht RDY	Zweihandbedienung abbrechen	--"--							
6	Achsen sperren keine gültige Zweihandbedienung	SM22.1\2 schalten nicht ein obiger Regler nicht RDY	Ungültige Zweihandkombinationen testen	--"--							
7	Achse gesperrt Notaus	SM22.1\2 schalten ab obiger Regler nicht RDY	Notaus drücken	--"-- Achsen RDY mit gültiger Zweihandbedienung							

Thema		Testpunkt	Testbeschreibung	Ausgangslage
Safety Aktoren				
1	Achsfreigabe DSVO			
1	Achse freigegeben	SM22.1\2 eingeschaltet folgende Regler sind RDY: -A107.1 DSVO Antrieb	Kontrolle: Achsen sollte das RDY durchgehend leuchten	Steuerung ein Schutztüre DSMA geschlossen
2	Verdrahtungsprüfung	obige Achsen nicht RDY	SM22.1 und SM22.2 separat öffnen und RDY kontrollieren	Steuerung ein Schutztüre geschlossen SM22.1\2 eingeschaltet
3	Achse sperren Schutztüre	obige Achsen nicht RDY	Schutztüre öffnen	Steuerung ein SM22.1\2 eingeschaltet
4	Achsen freigegeben Zweihandbedienung ok	SM22.1\2 eingeschaltet folgende Regler sind RDY: -A107.1 DSVO Antrieb	Kontrolle: Achsen sollte das RDY durchgehend leuchten Gültige Zweihandbedienung	Steuerung ein Schutztüre DSMA offen
5	Achsen gesperrt keine Zweihandbedienung	SM22.1\2 schalten ab obiger Regler nicht RDY	Zweihandbedienung abbrechen	--"--
6	Achsen sperren keine gültige Zweihandbedienung	SM22.1\2 schalten nicht ein obiger Regler nicht RDY	Ungültige Zweihandkombinationen testen	--"--
7	Achse gesperrt Notaus	SM22.1\2 schalten ab obiger Regler nicht RDY	Notaus drücken	--"-- Achsen RDY mit gültiger Zweihandbedienung

Testprozess Safety Aktoren-Komponenten

Schritt 3: Test des Safetysystems

Mit dem Vorliegen des Testprotokolls und der fertig implementierten Safety-Software wird zum Abschluss ein umfassender Abnahmetest der SSPS an der Maschine durchgeführt.
Dabei empfiehlt es sich protokollarisch jeden Abnahmeschritt wie folgt zu dokumentieren: Testresultat des jeweiligen Schrittes mit Datum und Test sowie einem Status. Daneben bestätigt der Sicherheitsbeauftragte der Maschine die Abnahme mit Unterschrift und Datum.

Thema		Testpunkt	Testbeschreibung	Ausgangslage	Testresultat	Test	Tester	Wertung	Prüfer	Datum	Memo
Safety-Erfasser-Komponenten											
1 Nothalttaster DSMA											
	1 Funktion Notaustaster	Funktion	Überprüfen der Tasterfunktion	Steuerung ein	Meldung 1337 WZ geht in Nothalt	10.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	2 Abschaltung Kanal 1	Schalterkontakt 11/12 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberwachung der Klemme SM14.3/4	Steuerung ein	SM14.3 Klemmenredundanzfehler Meldung 1337 nicht quittierbar Nothalttaster muss einmal funktionierend schalten um Fehler zu quittieren	10.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	3 Abschaltung Kanal 2	Schalterkontakt 21/22 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberwachung der Klemme SM14.3/4	Steuerung ein	SM14.4 Klemmenredundanzfehler Meldung 1337 nicht quittierbar Nothalttaster muss einmal funktionierend	10.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
2 Schutztür DSMA											
	1 Funktion Taster 1/2	Schutztür entriegeln Schutztür öffnen Schutztür verriegeln	überprüfen SM14.1/2 abgeschaltet	Steuerung ein	Funktion ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	2 Funktion Taster 2/2	Schutztür schliessen	überprüfen SM14.1/2 eingeschaltet	Steuerung ein	Funktion ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	3 Abschaltung Kanal 1	Schalterkontakt 21/22 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberwachung der Klemme SM14.1/2	Steuerung ein	Baustein SF_GuardMonitoring in Safety schaltet ab muss mit korrekten Flanken an beiden Eingängen quittiert werden	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	4 Abschaltung Kanal 2	Schalterkontakt 41/42 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberwachung der Klemme SM14.1/2	Steuerung ein	Baustein SF_GuardMonitoring in Safety schaltet ab muss mit korrekten Flanken an beiden Eingängen quittiert werden	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
3 Bedienpult DSMA Zweihandtaster links											
	1 Funktion Notaustaster	Funktion	Überprüfen der Tasterfunktion SM7.1 Schliesser SM7.2 Öffner	Steuerung ein	ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	2 Abschaltung Kanal 1	Schalterkontakt 13/14	einkanaliges Einschalten; Kontrolle Redunazüberwachung der Klemme SM7.1/2	Steuerung ein Schaltkontakt 13 abklemmen	Klemmenredundanz ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	3 Abschaltung Kanal 2	Schalterkontakt 21/22	einkanaliges Abschalten; Kontrolle Redunazüberwachung der Klemme SM7.1/2	Steuerung ein Schaltkontakt 21 abklemmen	Klemmenredundanz ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
4 Bedienpult DSMA Zweihandtaster rechts											
	1 Funktion Notaustaster	Funktion	Überprüfen der Tasterfunktion SM7.3 Schliesser SM7.4 Öffner	Steuerung ein	ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	2 Abschaltung Kanal 1	Schalterkontakt 13/14 schliessen	einkanaliges Einschalten; Kontrolle Redunazüberwachung der Klemme SM7.3/4	Steuerung ein Schaltkontakt 13 abklemmen	Klemmenredundanz ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
	3 Abschaltung Kanal 2	Schalterkontakt 21/22 öffnen	einkanaliges Abschalten; Kontrolle Redunazüberwachung der Klemme SM7.3/4	Steuerung ein Schaltkontakt 21 abklemmen	Klemmenredundanz ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	

Dokumentation der Abnahme im Überblick

Testresultat	Test	Tester	Wertung	Prüfer	Datum	Memo
Meldung 1337 WZ geht in Nothalt	10.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
SM14.3 Klemmenredundanzfehler Meldung 1337 nicht quittierbar Nothalttaster muss einmal funktionierend schalten um Fehler zu quittieren	10.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
SM14.4 Klemmenredundanzfehler Meldung 1337 nicht quittierbar Nothalttaster muss einmal funktionierend	10.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
Funktion ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	
Funktion ok	11.08.2015	HartOli SonnRen	OK	HustMan	12.08.2015	

Testresultate und Infos zu Test und Abnahme

ZUSAMMENFASSUNG

Die Vorteile mit der erläuterten Methodik

In der Konzeption

Einfache, selbsterklärende Beschreibung ermöglicht klare Kommunikation zwischen Softwareentwicklung und Maschinenbau, vereinfacht Ergänzungen und schafft einen guten Überblick.

In der Testvorbereitung

Mit der UML-Visualisierung lassen sich die Testfälle umfassend und einfach planen.

Bei der SSPS-Abnahme

- Test der effektiven Safetyfunktionalität an der Maschine
- Vollständige und umfassende Abnahmedokumentation
- Verkürzte Testzeit durch strukturierten Ablauf

Beim Maschinenbetrieb

Die einfache Visualisierung im UML erleichtert es dem Maschinenbediener und dem Servicetechniker bei Problemen mit der Safety, schnell einen Überblick der Zusammenhänge und Funktionen der SSPS zu bekommen.

Über den Verfasser

René Sonnweber
ist erfahrener Applikations-Ingenieur bei
Pantec Engineering AG.

Sein konzeptionelles Know-How und seine Erfahrung mit unterschiedlichsten Entwicklungsumgebungen und Programmiersprachen hat vielen Maschinen schon zum Erfolg verholfen.

„Das Use Case orientierte Design der Sicherheitslogik ist ein Meilenstein im Thema Maschinensicherheit. Früher war die Sicherheitsfunktionalität meist nur spärlich dokumentiert, und wenn, dann in komplizierten Tabellen. Mit den grafischen Use Cases liegt nun ein Instrument vor, das die Verständigung zwischen Maschinenbauer und Softwareentwickler vereinfacht, Implementierung und Test beschleunigt und dem Servicetechniker eine einfach verständliche Darstellung der Sicherheitslogik bietet."

pantec automation

Pantec Automation ist eine Business Unit der Pantec Engineering AG, und ist ein führendes Systemhaus für Steuerungslösungen im Maschinen- und Anlagenbau. Breite technische Kompetenz, Konzentration auf Schlüsseltechnologien und hohe praktische und methodische Expertise in der Projektabwicklung machen Pantec Automation zum ausgewählten Partner für Just-in-Time Engineering in höchster Qualität.

Die **Pantec Engineering AG** ist ein weltweit operierender Technologieausrüster für Maschinenbau und Medizintechnik und bietet Dienstleistungen und Komplettlösungen in den Bereichen Automatisierung und mechatronische Systeme. Durch die Umsetzung konsequenter Nischenstrategien besetzt das Unternehmen Top-Positionen in seinen Zielmärkten – nicht zuletzt durch eine hohe Serviceorientierung.

Headquarter International
Pantec Engineering AG
Industriering 21
9491 Ruggell
Liechtenstein
T: +423 377 13 33

Schweiz
Pantec GS Systems AG
Heldswilerstrasse 13
9214 Kradolf
Schweiz
T: +41 71 644 98 98

Deutschland
Pantec GmbH
Am Kerbersgraben 2
63825 Schöllkrippen
Deutschland
T: +49 6024 634 13 11

China
Pantec (Shanghai) Co., Ltd.
128 Shenfu Road
Xinzhuang, Industry Park
201108 Shanghai, China
T: +86 21 517 60 282

KONTAKT

info.automation@pantec.com
www.pantec-automation.com