

Funktionale Sicherheit und PLT - Sicherheitseinrichtungen im Rahmen der Druckgeräterichtlinie 2014/68/EU

- Diese Richtlinie gilt für die Auslegung, Fertigung und Konformitätsbewertung von Druckgeräten und **Baugruppen** mit einem maximal zulässigen Druck (PS) von über 0,5 bar. Sie umfasst Behälter, Rohrleitungen, **Ausrüstungsteile mit Sicherheitsfunktion** und druckhaltende Ausrüstungsteile
- Ausrüstungsteile mit Sicherheitsfunktion sind Einrichtungen, die zum Schutz des Druckgerätes bei einem überschreiten der zulässigen Grenzen bestimmt sind.
- Die Überwachung von Druckgeräten im Betrieb wird nicht durch die EU-Richtlinie für Druckgeräte festgelegt; diese regelt maßgeblich das Inverkehrbringen. Für die Überwachung und die wiederkehrenden Prüfungen sind nationale Festlegungen zu beachten. In Deutschland ProdSG und BetrSichV

Lebenszyklus

- Die grundlegenden Anforderungen für Druckgeräte (siehe Anhang I der DGRL, wesentliche Sicherheitsanforderungen) gelten auch für Baugruppen. Der Hersteller ist verpflichtet, für Druckgeräte und Baugruppen eine Analyse der Gefahren und Risiken vorzunehmen, um die mit seinem Gerät verbundenen druckbedingten Gefahren und Risiken zu ermitteln; er muss das Gerät dann unter Berücksichtigung der Analyseergebnisse auslegen und bauen.
- **Und so rutschen wir in die Funktionale Sicherheit**

Begriffsbestimmung

- **Schaden**

Menschen entstehen physische Verletzungen oder Schädigungen ihrer Gesundheit, direkt oder indirekt als Ergebnis von Schäden an Gütern oder der Umwelt

- **Risiko**

Wahrscheinlichkeit das ein gefahrbringendes, schädigendes Ereignis auftritt und dessen Ausmaß

- **Tolerierbares Risiko**

Gemessen am aktuellen gesellschaftlichen Wertvorstellungen befindet sich das Risiko in einem tragbaren Bereich

- **Restrisiko**

Trotz Schutzmaßnahmen verbleibendes Risiko

- **Schutzmaßnahme**

Zum Erreichen einer Risikominderung vorgesehene Maßnahme

- **Sicherheitsfunktion**

Funktion, deren Ausfall zu einer unmittelbaren Erhöhung mindestens eines Risikos führt

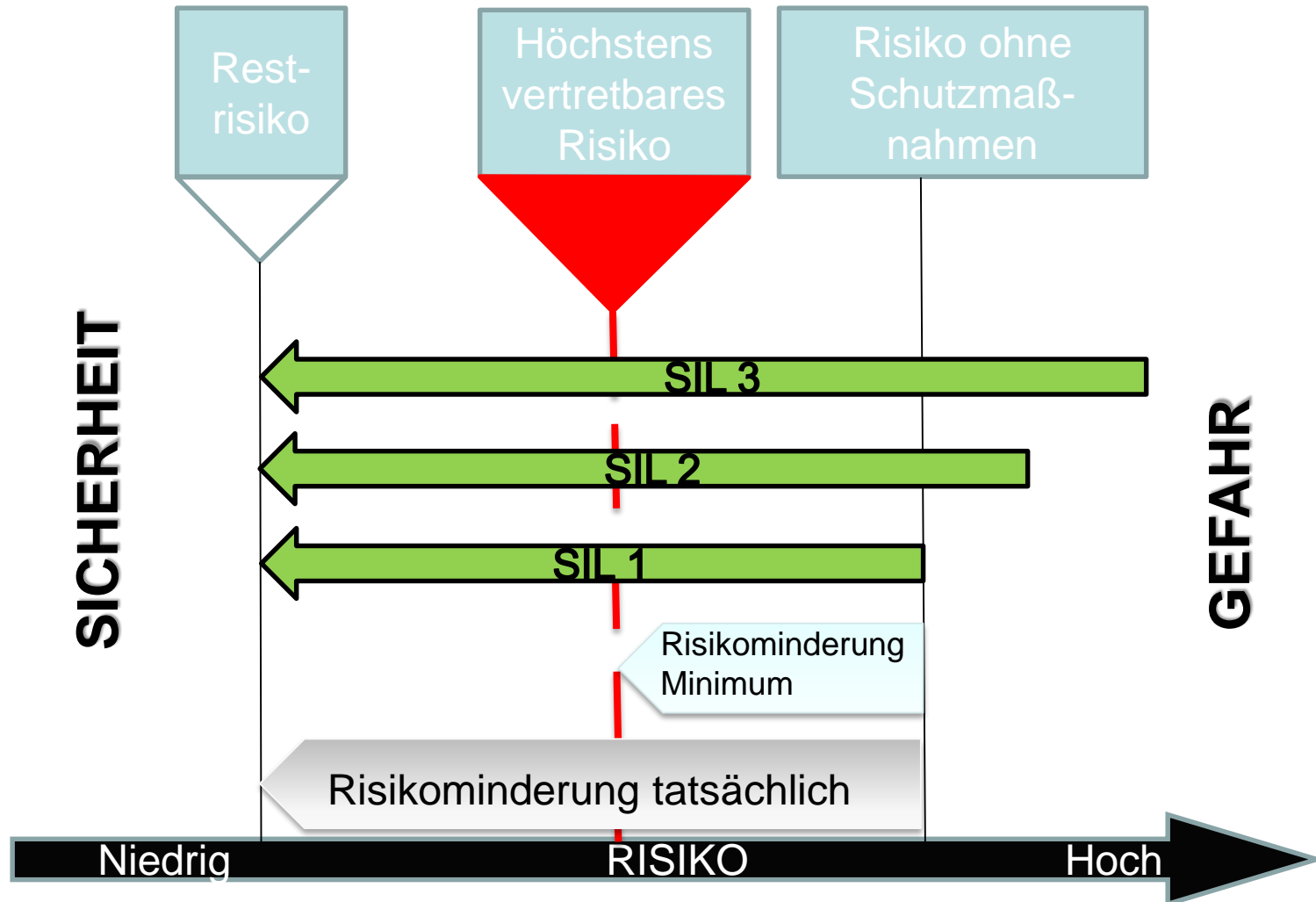
- **Aktive Fehler**

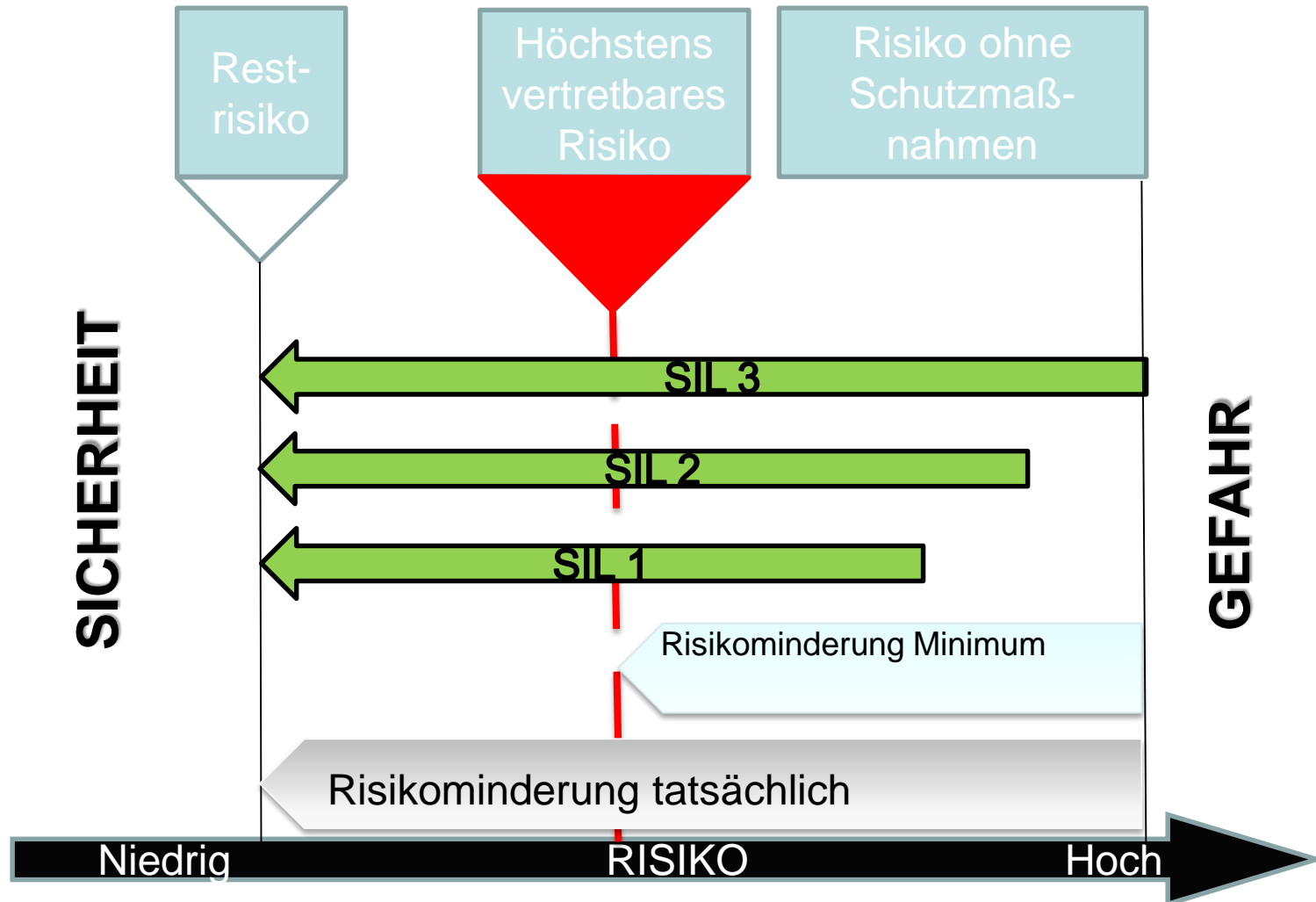
Führt immer zur Abschaltung (Drahtbruch) → Schutzfunktion bleibt erhalten

- **Passive Fehler**

Verhindert die Abschaltung (Relais fällt nicht ab) → Schutzziel bleibt unerreicht

Risiko





Funktionale Sicherheit ist...

Sicherheit

Das fernhalten von unvermeidbaren Risiken einhergehend mit physischen Verletzungen oder Schädigung der Gesundheit von Menschen, direkt oder indirekt entstanden als Ergebnis von Schäden an Gütern oder der Umwelt.

Funktionale Sicherheit

Ein Teil der Gesamtsicherheit. Sie ist davon abhängig, dass ein System oder ein Betriebsmittel korrekte Antworten auf Eingangszustände oder Signale liefert.

Korrekte Funktion des Sicherheitssystems inklusive der Sensoren und Aktoren.

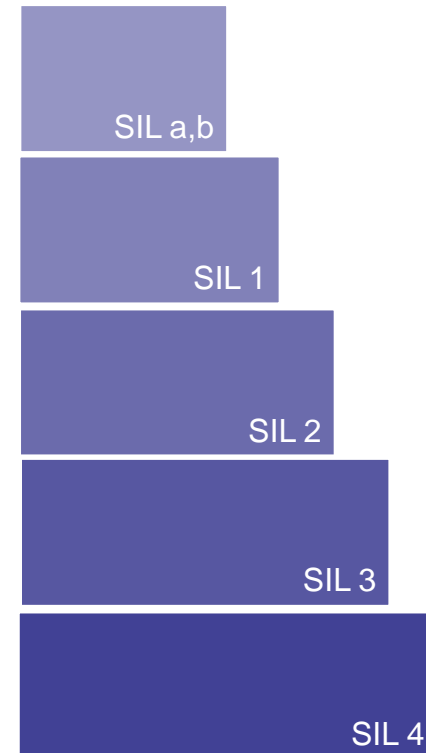
Regelung vs. Sicherheitssystem

- Regelung steht für optimale Führung von Prozessgrößen beim Anfahren und Laständerungen. Sie soll Prozessgrößen auf ihrem vorgegebenem Sollwert halten und damit Störungen vermeiden. Unzulässige Prozessbereiche sollen vermieden werden.
- Sicherheitssystem greift bei Störungen ein, die durch die Regelung prinzipiell, aufgrund der Intensität oder Dynamik nicht beherrscht werden können. Sie greift auch ein, wenn die Regelung ihre Funktion nicht aufnehmen kann.
- **Die Integrität (SIL) des Schutzsystems muss bestimmt werden.**

Der Sicherheits- Integritätslevel (SIL)

- Skala mit 4 Stufen (SIL 1 – SIL 4)
- SIL ist eine Maßeinheit für die Risikoreduzierung. SIL 1 niedrig; SIL 4 hoch
- Ermittlung mit anerkannten Methoden (Risikoanalyse)

- SIL – Klassifizierung ist Schritt im Sicherheitslebenszyklus des Systems

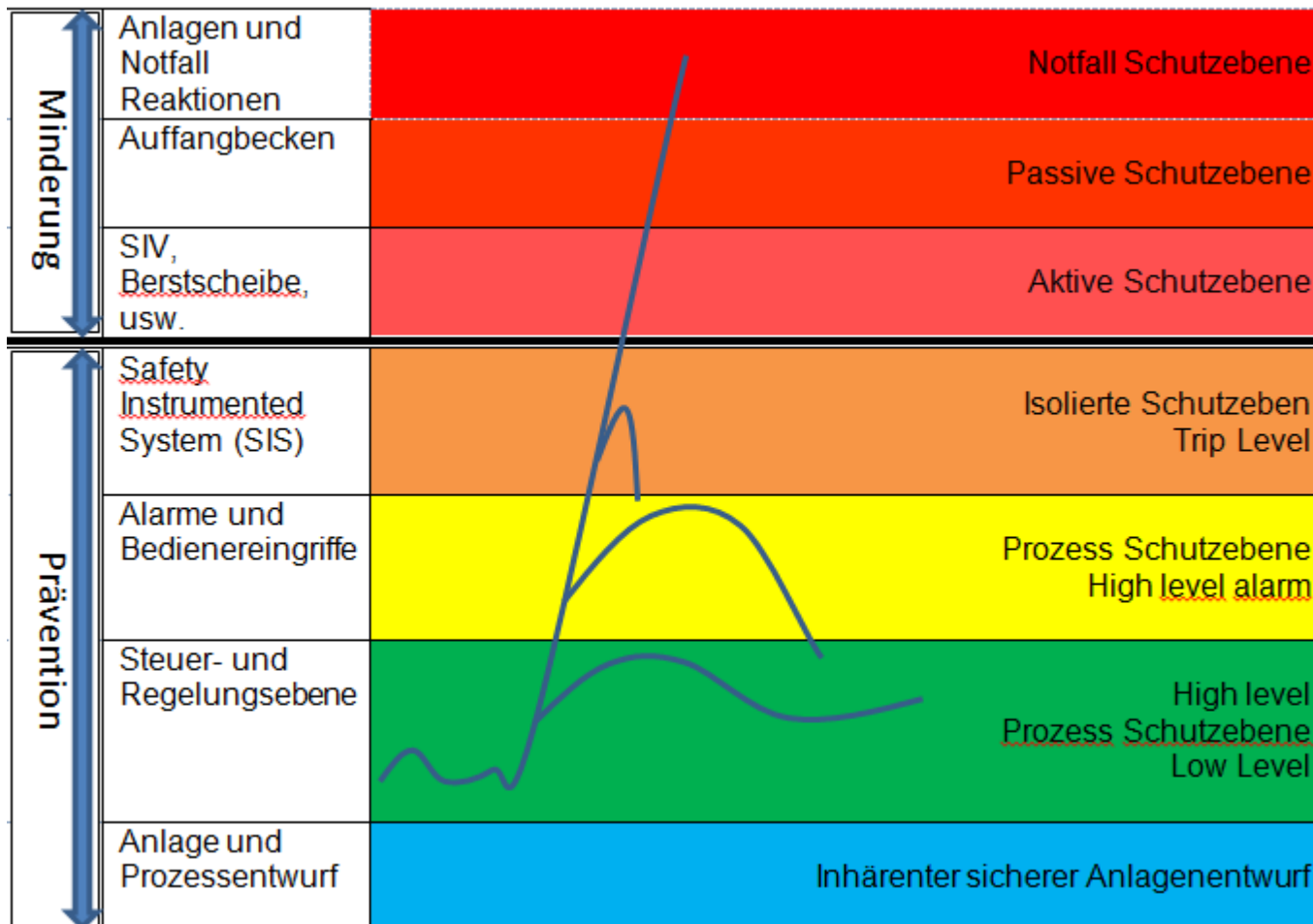


Was ist ein SIL?

- SIL - Stufen sind festgelegt. Jede entspricht einem Bereich einer **Zielwahrscheinlichkeit** des gefahrbringenden Ausfalls einer **Sicherheitsfunktion**.
- **SIL ist eine Eigenschaft einer Sicherheitsfunktion**. SIL ist nur bedingt die Eigenschaft eines einzelnen Systems oder eines Teils des System.

Low Demand		High Demand
10E-02 ... 10E-01	SIL 1	10E-06 ... 10E-05
10E-03 ... 10E-02	SIL 2	10E-07 ... 10E-06
10E-04 ... 10E-03	SIL 3	10E-08 ... 10E-07
10E-05 ... 10E-04	SIL 4	10E-09 ... 10E-08

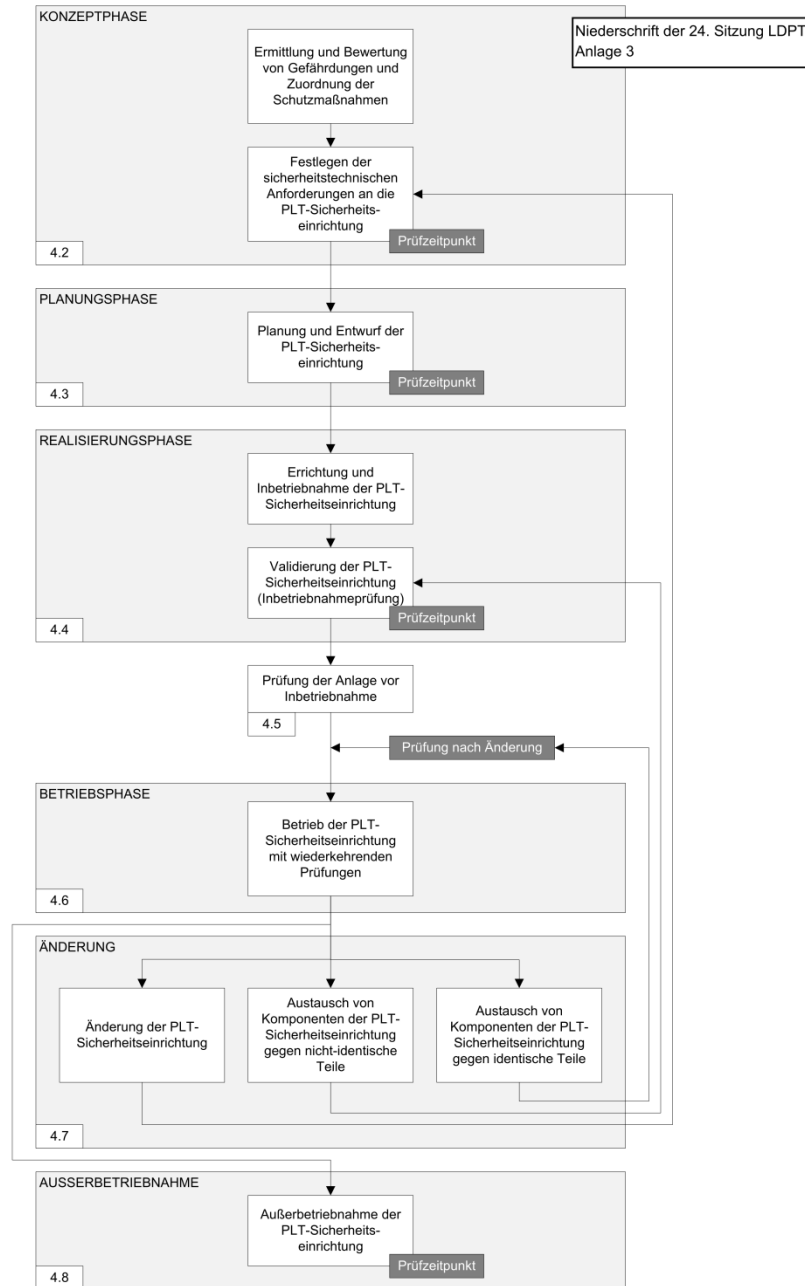
Präventive Maßnahmen zu Verhinderung eines Schadens



Einfache Methode zur ganzheitlichen Umsetzung der Funktionalen Sicherheit - Das Sicherheitshandbuch/ die Sicherheitsplanung



- Sicherheitslebenszyklus nach VD TÜV Merkblatt 372



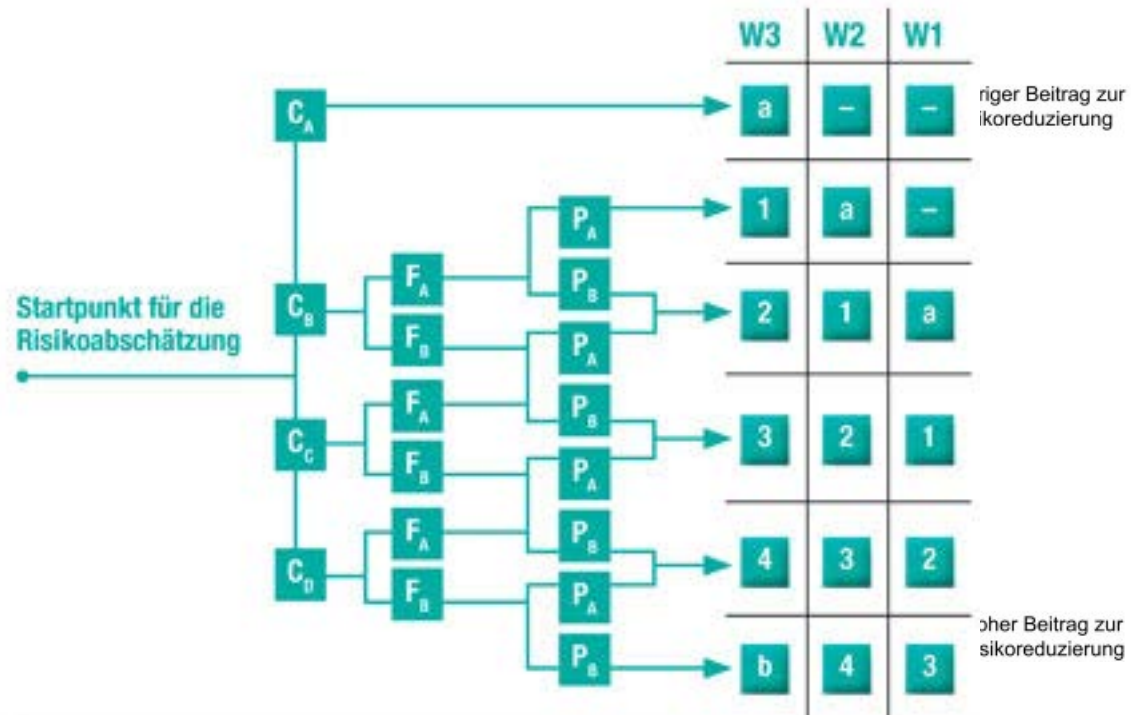
Konzeptphase

Die Risikobeurteilung

- Es ist in der Konzeptphase erforderlich, dass eine Gefahren- und Risikoanalyse für die gesamte Anlage durchgeführt wird und die anzuwendenden rechtlichen und normativen Anforderungen, die erforderliche Risikoreduzierung, die dazu erforderlichen PLT-Sicherheitseinrichtungen und weitere sicherheitstechnische Maßnahmen technischer und organisatorischer Art festgelegt werden.
- Welche Möglichkeiten für Risikobeurteilungen gibt es?

Risikograph

- Schadensausmaß **C**
- Aufenthaltsdauer **F**
- Gefahrenabwendung **P**
- Eintrittswahrscheinlichkeit des unerwünschten Ereignisses **W**
- SIL = Safety Integrity Level



a... keine Nachweißführung

b... eine PLT – Schutzeinrichtung nicht ausreichend

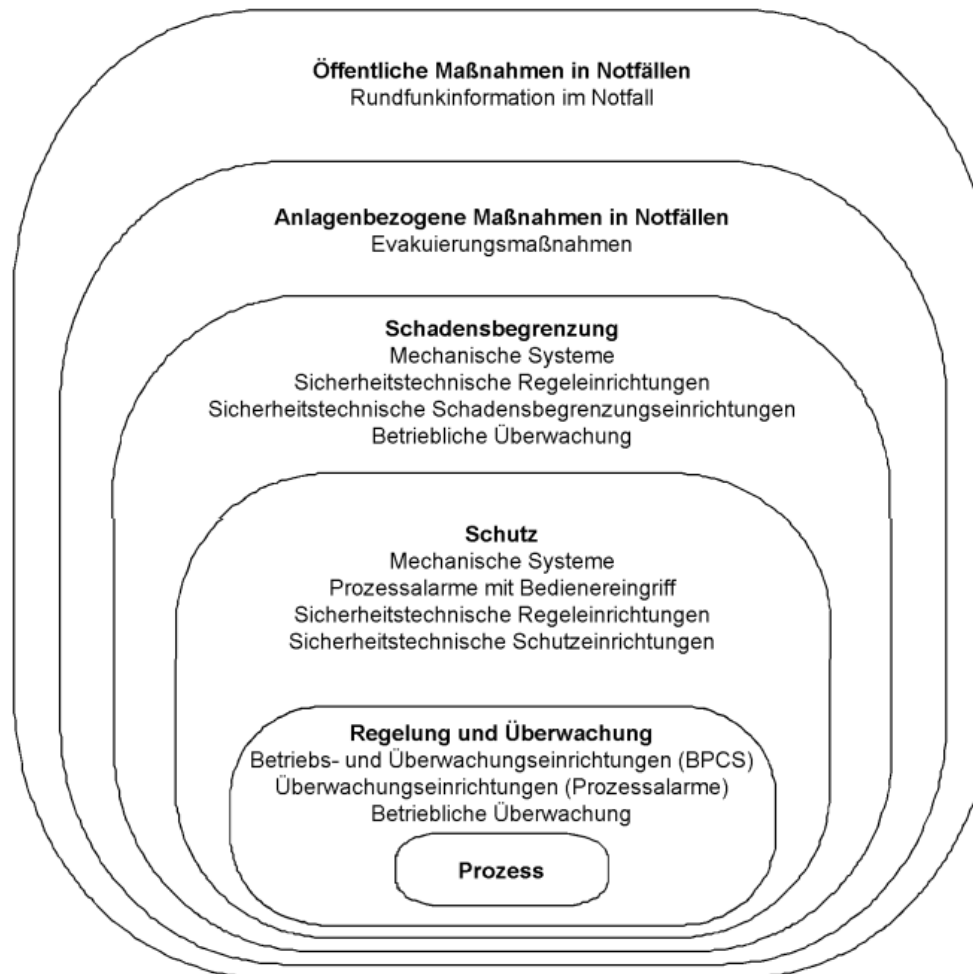
Risikomatrix

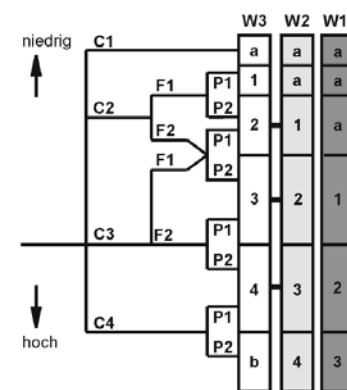
- Klasse I:
 - Nicht tolerierbares Risiko
- Klasse II:
 - Unerwünschtes Risiko
- Klasse III:
 - Vernachlässigbares Risiko

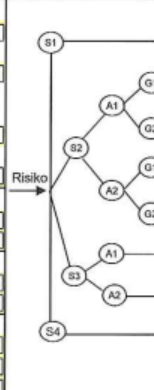
	Auswirkung			
Wahrscheinlichkeit	katastrophal	kritisch	gering	vernachlässigbar
Häufig	I	I	I	II
Wahrscheinlich	I	I	II	II
Gelegentlich	I	II	II	II
Gering	II	II	II	III
Unwahrscheinlich	II	III	III	III
Nicht glaubhaft	II	III	III	III

LOPA, Analyse der Schutzebenen

Layer of Protection Analysis

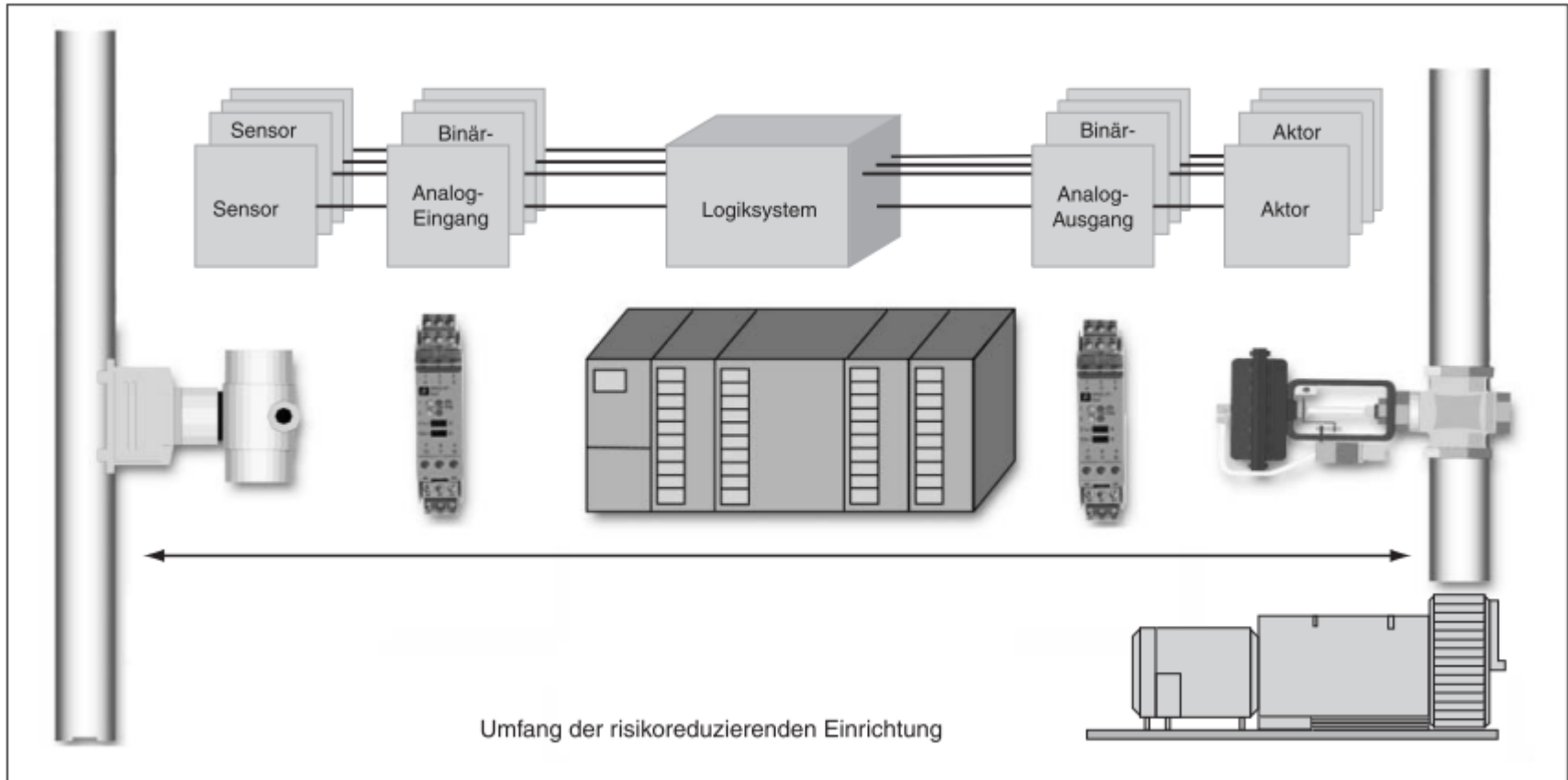


Festlegung der Schutzanforderungen an Schutzsysteme nach DIN EN 50156-1:2015					
Pos. in der Gefahrenanalyse 2.1.2	Anlage: Thermische Verwertungsanlage Schwarzta				
KKS-Nr. HAD10CL001 - 004	Bezeichnung im Klartext: Niveau Dampftrommel			PID-Nr. / Rev.: 211001-01 / 12	
Abzudeckendes Risiko / Schutzziel: Wasserstand Trommel tief → Strukturversagen Verdampfer durch Überhitzung					
Schadensausmaß C1 leichte Verletzungen einer Person oder kleinere schädliche Umwelteinflüsse, die z. B. nicht unter die Störfallverordnung fallen <input type="checkbox"/> C2 schwere, irreversible Verletzungen einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung <input type="checkbox"/> C3 Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung <input checked="" type="checkbox"/> C4 katastrophale Auswirkungen, sehr viele Tote <input type="checkbox"/>		 <p style="text-align: right;">EN 50156-1:2015</p>			
Häufigkeit und Dauer des Aufenthalts im Gefahrenbereich F1 selten bis öfter <input type="checkbox"/> F2 häufig bis dauernd <input checked="" type="checkbox"/>					
Gefahrenabwendung P1 möglich unter bestimmten Bedingungen <input type="checkbox"/> P2 kaum möglich/beinahe unmöglich <input checked="" type="checkbox"/>					
Eintrittswahrscheinlichkeit W1 sehr gering (< 1 in 10 Jahren) <input checked="" type="checkbox"/> W2 gering (< 1 mal pro Jahr) <input type="checkbox"/> W3 relativ hoch (1 bis 10 mal pro Jahr) <input type="checkbox"/>					
Kurzbegründung für die Wahl der Risikoparameter					
Schadensausmaß: C1 - C4	Aufreißen des Kessels durch Überhitzung infolge von Wassermangel möglich. Ggf. halten sich mehrere Personen im Gefahrenbereich auf (z.B. bei Wartungsarbeiten)				
Aufenthaltsdauer: F1 - F2	Im Normalbetrieb sind Rundengänger und Wartungspersonal im Gefahrenbereich. Bei Wartungsarbeiten im Gefahrenbereich kann die Aufenthaltsdauer mehrere Stunden betragen.				
Gefahrenabwendung: P1 - P2	Die Gefahrensituation ist für Personal, das im Gefahrenbereich tätig ist, nicht erkennbar.				
Eintrittswahrscheinlichkeit: W1 - W3	Sehr geringe Eintrittswahrscheinlichkeit, da vorgelagerte Trommelniveauregelung und mehrstufige Alarmpalette über PLS.				
Ergebnis der Einstufung	SIL 2				
Die PLT-Schutzeinrichtung unterliegt folgenden Gesetzen / Verordnungen / Richtlinien:					
BetrSichV	X	DIN EN 12952	X	DIN EN 50156	X
DGRL		DIN EN 12953			
		DIN EN 746			
Sonstige					
Unterschriften					
Vertreter	Name	Unterschrift			Datum
Planer	---				
Hersteller	---				
Betreiber					
Sachverständiger					

Klassifizierung der PLT-Schutzeinrichtung in		Funktion																																																																									
PLT-Schutzeinrichtung, ereignisverhindernd		A Z																																																																									
Risikoeinschätzung für die PLT-Schutzeinrichtung																																																																											
Abzudeckendes Risiko/ Schutzziel	Absicherung gegen Druckhoch 371.P.017 und angeschlossenen Systeme (641.W.1025): Überschreitung der Auslegungsgrenzen P.017/641.W.1025, Freisetzung von Kohlerwasserstoffen Bildung gefährlicher explosionsfähiger Atmosphäre, Brand- und Explosionsgefahr, cancerogene Gefährdung des Personals. Ursache: Rückströmen von Produkt aus der Leitung 371.P.015 zur Leitung 371.P.017																																																																										
Schadensausmaß (zutreffendes bitte ankreuzen) <table border="1"> <tr> <td>S1</td> <td>leichte Verletzungen einer Person oder kleinere schädliche Umwelteinflüsse, die z. B. nicht unter die Störfallverordnung fallen</td> <td><input type="checkbox"/></td> </tr> <tr> <td>S2</td> <td>schwere, irreversible Verletzungen einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>S3</td> <td>Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung</td> <td><input type="checkbox"/></td> </tr> <tr> <td>S4</td> <td>katastrophale Auswirkungen, sehr viele Tote</td> <td><input type="checkbox"/></td> </tr> </table>	S1	leichte Verletzungen einer Person oder kleinere schädliche Umwelteinflüsse, die z. B. nicht unter die Störfallverordnung fallen	<input type="checkbox"/>	S2	schwere, irreversible Verletzungen einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung	<input checked="" type="checkbox"/>	S3	Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung	<input type="checkbox"/>	S4	katastrophale Auswirkungen, sehr viele Tote	<input type="checkbox"/>		<table border="1"> <thead> <tr> <th></th> <th>W 3</th> <th>W 2</th> <th>W 1</th> </tr> </thead> <tbody> <tr> <td>AK1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>SIL 1</td> <td></td> <td>SIL 1</td> <td></td> </tr> <tr> <td>AK2</td> <td></td> <td>AK1</td> <td></td> </tr> <tr> <td>SIL 2</td> <td></td> <td>SIL 1</td> <td>SIL 1</td> </tr> <tr> <td>AK3</td> <td></td> <td>AK2</td> <td>AK1</td> </tr> <tr> <td>SIL 2</td> <td></td> <td>SIL 2</td> <td>SIL 1</td> </tr> <tr> <td>AK4</td> <td></td> <td>AK3</td> <td>AK2</td> </tr> <tr> <td>SIL 3</td> <td></td> <td>SIL 2</td> <td>SIL 2</td> </tr> <tr> <td>AK5</td> <td></td> <td>AK4</td> <td>AK3</td> </tr> <tr> <td>SIL 3</td> <td></td> <td>SIL 3</td> <td>SIL 2</td> </tr> <tr> <td>AK6</td> <td></td> <td>AK5</td> <td>AK4</td> </tr> <tr> <td>SIL 4*</td> <td></td> <td>SIL 3</td> <td>SIL 3</td> </tr> <tr> <td>AK7</td> <td></td> <td>AK6</td> <td>AK5</td> </tr> <tr> <td>AK8</td> <td></td> <td>SIL 4*</td> <td>SIL 3</td> </tr> </tbody> </table>		W 3	W 2	W 1	AK1				SIL 1		SIL 1		AK2		AK1		SIL 2		SIL 1	SIL 1	AK3		AK2	AK1	SIL 2		SIL 2	SIL 1	AK4		AK3	AK2	SIL 3		SIL 2	SIL 2	AK5		AK4	AK3	SIL 3		SIL 3	SIL 2	AK6		AK5	AK4	SIL 4*		SIL 3	SIL 3	AK7		AK6	AK5	AK8		SIL 4*	SIL 3	Bemerkungen keine PLT-Schutzeinrichtung (z.B. technische Arbeitsschutzmaßnahmen) PLT-Schutzeinrichtung nicht ausreichend
S1	leichte Verletzungen einer Person oder kleinere schädliche Umwelteinflüsse, die z. B. nicht unter die Störfallverordnung fallen	<input type="checkbox"/>																																																																									
S2	schwere, irreversible Verletzungen einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung	<input checked="" type="checkbox"/>																																																																									
S3	Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung	<input type="checkbox"/>																																																																									
S4	katastrophale Auswirkungen, sehr viele Tote	<input type="checkbox"/>																																																																									
	W 3	W 2	W 1																																																																								
AK1																																																																											
SIL 1		SIL 1																																																																									
AK2		AK1																																																																									
SIL 2		SIL 1	SIL 1																																																																								
AK3		AK2	AK1																																																																								
SIL 2		SIL 2	SIL 1																																																																								
AK4		AK3	AK2																																																																								
SIL 3		SIL 2	SIL 2																																																																								
AK5		AK4	AK3																																																																								
SIL 3		SIL 3	SIL 2																																																																								
AK6		AK5	AK4																																																																								
SIL 4*		SIL 3	SIL 3																																																																								
AK7		AK6	AK5																																																																								
AK8		SIL 4*	SIL 3																																																																								
Aufenthaltsdauer A1 selten bis öfter A2 häufig bis dauernd	<input checked="" type="checkbox"/> <input type="checkbox"/>																																																																										
Gefahrenabwendung G1 möglich unter bestimmten Bedingungen G2 kaum möglich/beinahe unmöglich	<input type="checkbox"/> <input checked="" type="checkbox"/>																																																																										
Eintrittswahrscheinlichkeit W1 sehr gering (< 0,1 mal pro Jahr) W2 gering (< 1 mal pro Jahr) W3 relativ hoch (1 bis 10 mal pro Jahr)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>																																																																										
AK1 bis AK8 stellen den Bezug zur zurückgezogenen Norm DIN V 19250 dar. *) SIL 4 ist wegen des erforderlichen überproportionalen Aufwands zu vermeiden!																																																																											
Kurzbeurteilung für die Wahl der Risikoparameter																																																																											
Schadensausmaß: S1 - S4	Potentieller Austritt von Naphtha, Bildung einer explosionsfähigen Atmosphäre. Produktleitung verläuft teilweise über und parallel zur grünen Straße (2). Die Flansche, als wahrscheinlichste Austrittsstelle befinden sich mehrheitlich in Anlagen- oder Tanknähe. Statistisch gesehen: Größtes Schadensausmaß entfernt von der grünen Straße. 641W1025 befindet sich in der Anlage.																																																																										
Aufenthaltsdauer: A1 - A2	Frei zugängliche, grüne Straße (2). Der einzelne Geschädigte befindet sich nicht "häufig bis dauernd" im Schadensbereich. Siehe statistische Erhebung von R-SA bzgl. Personen auf grüner Straße																																																																										
Gefahrenabwendung: G1 - G2	Nicht möglich.																																																																										
Eintrittswahrscheinlichkeit: W1 - W3	Eingangsschieber der Tanks schließen durch Ansprechen der Überfüllsicherung.																																																																										
Die Schutzeinrichtung ist eingestuft mit		SIL 1	zur Einstufung siehe Bemerkung im Blatt SIS-Definition																																																																								

- Prüfgegenstand sind die Unterlagen des Lastenheftes unter Berücksichtigung der Ergebnisse der Gefahren- und Risikoanalyse und der sich aus dieser ergebenden Schlussfolgerungen für notwendige PLT-Sicherheitseinrichtungen und deren erforderliche Qualität.
- Für jede PLT-Sicherheitseinrichtung ist auf Grundlage der Gefahren- und Risikoanalyse im Einzelnen zu prüfen:
die vorgesehene Funktion, die Anforderungen an die Reaktionszeit, die konzeptionelle Ausführung, der Verifizierungsplan, sofern zutreffend die Festlegungen zu Änderungen, die Festlegung der anzuwendenden rechtlichen und normativen Anforderungen.
- Eine Plausibilitätsprüfung der Unterlagen unter Einschluss einer Ordnungsprüfung ist durchzuführen.

Planungsphase

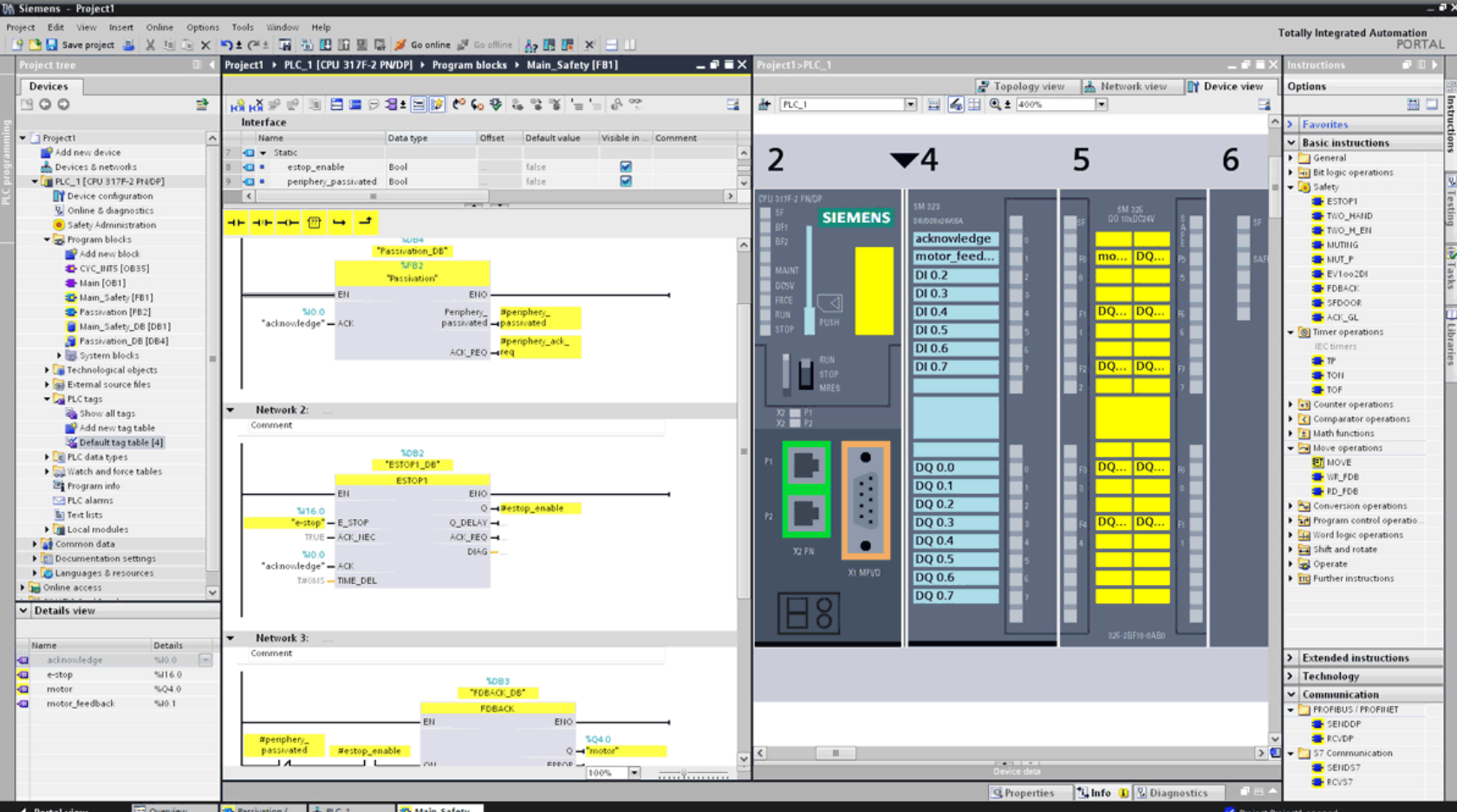


Prüfumfang an Hand der Unterlagen aus dem Sicherheitshandbuch (Planungsphase)

- Ausführung der PLT-Sicherheitseinrichtung hinsichtlich Anforderungen aus der Spezifikation (Pflichtenheft)
- konstruktive Auslegung der Komponenten
- verfahrenstechnische Eignung von Sensorik und Aktorik
- Festlegung der Messbereiche
- Umgebungseinflüsse auf die Komponenten (siehe hierzu 4.2.1 Abs. 2)
- Eignungsnachweise der eingesetzten PLT-Komponenten und -Systeme
- Einhaltung der in Sicherheitshandbuch, Betriebsanleitung oder Baumusterprüfung der PLT-Sicherheitseinrichtung enthaltenen Bedingungen
- Umsetzung der Funktion der Schutz Aufgabe in die Logik- oder Funktionspläne sowie die Anwendungssoftware
- Signalaustausch zwischen PLT-Komponenten oder PLT-Sicherheitseinrichtungen und anderen PLT Einrichtungen hinsichtlich
 - Rückwirkungsfreiheit
 - sicherheitsgerichteter Ausführung
 - Kennzeichnung der sicherheitsrelevanten übertragenen Signale in der Dokumentation
- Sicherheitsrelevante Parameter wie Zeiten, Zähler und Grenzwerte der Prozessgrößen sowie die Berechnung der sicherheitsrelevanten Parameter
- Verfügbarkeit und Qualität der Hilfsenergieversorgung
- Einbau- und Verlegebedingungen, elektrotechnische Eignung
- Eignung weiterer organisatorischer Maßnahmen
- Eignung der für die Durchführung der wiederkehrenden Prüfungen der PLT-Sicherheitseinrichtung erforderlichen Maßnahmen
- FuSi-Eignung der PLT-Komponenten und -Systeme

Realisierungsphase

- Prüfunterlagen sind zum Beispiel die Unterlagen aus der Planungsphase. Zusätzlich Parameterlisten, Installationsunterlagen der PLT, Installationsnachweise, alte Prüfberichte
- Gegenstand ist die Funktion und Einbindung der PLT - Sicherheitseinrichtung in die Anlage.
 - Korrekt erfolgte Einstellung von Parametern
 - Installierte Anwendersoftware = geprüfte Anwendersoftware?
 - FuP korrekt umgesetzt?



Siemens - Project1

Project Edit View Insert Online Options Tools Window Help

Project1 > PLC_1 [CPU 317F-2 PN/DP] > Program blocks > Main_Safety [FB1]

Project tree: PLC_1 [CPU 317F-2 PN/DP] > Program blocks > Main_Safety [FB1]

Interface

Name	Data type	Offset	Default value	Visible in	Comment
7	Static				
8	estop_enable	Bool	false		
9	penphery_passivated	Bool	false		

Network 1:

```

%I0.0 "acknowledge" --ACK--> SFB2 "Passivation"
SFB2 --EHO--> #penphery_passivated
SFB2 --EHO--> #penphery_ack_
SFB2 --EHO--> AOI_REQ --req--
  
```

Network 2:

```

%I16.0 "e-stop" --E_STOP--> SFB2 "ESTOP1"
SFB2 --EHO--> #estop_enable
SFB2 --EHO--> AOI_REQ --req--
SFB2 --EHO--> DIAG --diag--
  
```

Network 3:

```

#penphery_passivated --AND-- #estop_enable --AND--> SFB3 "FOBACK_FB"
SFB3 --EHO--> %Q4.0 "motor"
  
```

Hardware Rack:

- SIEMENS CPU 317F-2 PN/DP
- SM 322 DI 0.2-0.7
- SM 325 DI 0.2-0.7
- DI 0.2
- DI 0.3
- DI 0.4
- DI 0.5
- DI 0.6
- DI 0.7
- DQ 0.0
- DQ 0.1
- DQ 0.2
- DQ 0.3
- DQ 0.4
- DQ 0.5
- DQ 0.6
- DQ 0.7

Right Sidebar (Instructions):

- Basic instructions
 - General
 - Bit logic operations
 - Safety
 - ESTOP1
 - TWO_HAND
 - TWO_H_EN
 - MUTHING
 - MUT_P
 - EVI00204
 - FDBACK
 - SFD008
 - ACT_GL
 - Timer operations
 - IOC timers
 - TP
 - TOH
 - TOF
 - Counter operations
 - Comparator operations
 - Math functions
 - Move operations
 - MOVE
 - WR_FDB
 - PD_FDB
 - Conversion operations
 - Program control operation
 - Word logic operations
 - Shift and rotate
 - Operate
 - Further instructions
- Extended instructions
 - Technology
 - Communication
 - PROFIBUS / PROFINET
 - SEIDDP
 - FCVDP
 - S7 Communication
 - SEID57
 - FCV57

Unit	Unit 641
FSC-Steuerung	U641
Verify-Datum	24.04.2017
Verify-Zeit	09:51 Uhr
alte Revisionsnummer	104
alter CP1-CRC-Code	\$01D63FD4 (R710.7)
alter CP2-CRC-Code	\$03AF97C6 (R710.7)
neue Revisionsnummer	106
neuer CP1-CRC-Code	\$0177D193 (R710.7)
neuer CP2-CRC-Code	\$030E7981 (R710.7)

- 1) Logik zum BHC-Projekt geändert
- 2) Logik zum Projekt „Mittelnaphta“
- 3) Kommunikationssignale aus Projekt „Dampfejektoren im 641C2001“

Seitenänderungen:

Konfi, 140, 142, 144, 174, 244, 246, 248, 250, 252, 254, 256, 258, 270, 272, 2074, 276, 278, 280, 282, 284, 286, 288, 290, 292, 500, 502, 506, 510, 512, 514, 520, 522, 524, 538, 580, 588, 590, 596, 610, 700, 702, 750, 752, 754, 756, 758, 760, 762, 764, 770, 772, 774, 776, 778, 800, 802, 804, 806, 808, 810, 1622, 1680, 1682, 1726, 1728, 1730, 1750, 1827, 1883, 1885, 1997, 2000, 2001

Datei : VERIFY_U641_104_106.docx
erstellt am : 14.06.2016 10:01:00

Seite : 1 / 48

Start FSC-Datenbankvergleich: Datum: 24.4.2017 Zeit: 11:04

HINWEIS: Für jedes Zentralteil müssen insgesamt 5 Unterschiede mit Bezug auf die Variable VRF.TEST.RECORD gemeldet werden. Diese Unterschiede müssen für den Integritätsnachweis der Entwicklungssystem-Hardware während des Vergleichs der Datenbank aufgeführt werden.

>>> ZENTRALTEIL 1 <<<

FEHLER: Ungleiches Feld in regenerierter Applikationsdatenbank:

Typ	FUP	Feld	Datenbank	FSC-System
Prg.-Block	244	Blocktyp	Programmblock	Undefiniert
Prg.-Block	244	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	246	Blocktyp	Programmblock	Undefiniert
Prg.-Block	246	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	248	Blocktyp	Programmblock	Undefiniert
Prg.-Block	248	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	250	Blocktyp	Programmblock	Undefiniert
Prg.-Block	250	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	252	Blocktyp	Programmblock	Undefiniert
Prg.-Block	252	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	254	Blocktyp	Programmblock	Undefiniert
Prg.-Block	254	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	256	Blocktyp	Programmblock	Undefiniert
Prg.-Block	256	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	258	Blocktyp	Programmblock	Undefiniert
Prg.-Block	258	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	270	Blocktyp	Programmblock	Undefiniert
Prg.-Block	270	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	272	Blocktyp	Programmblock	Undefiniert
Prg.-Block	272	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	274	Blocktyp	Programmblock	Undefiniert
Prg.-Block	274	Blockstatus	Compiliert	Leerer FUP
Prg.-Block	276	Blocktyp	Programmblock	Undefiniert
Prg.-Block	276	Blockstatus	Compiliert	Leerer FUP

Prüfung vor Inbetriebnahme

- Bei der Pvl handelt es sich um die Prüfung der Anlage gemäß den gültigen Vorschriften, Regelwerken und Vereinbarungen.
- Die Prüfung der PLT-Sicherheitseinrichtung hat bereits vor Inbetriebnahme der Anlage stattgefunden.
- Wird die PLT -SiE während der Pvl geändert, so muss in den jeweiligen Schritt des Lebenszykluses zurückgesprungen werden.
 - Die Ergebnisse der Realisierungsphase sind zu berücksichtigen
 - Maßnahmen der Pvl der Anlage dürfen die PLT nicht beeinflussen
 - Prüfung der PLT ist immer eigenständig erforderlich, auch wenn die Prüfung der Anlage schon vor der Pvl stattfindet

Betriebsphase

- Die PLT-Sicherheitseinrichtungen sind auf Einhaltung der Spezifikationen in regelmäßige, festgelegten Abständen zu überprüfen.
- Änderungen am entwickelten und umgesetzten Konzept der funktionalen Sicherheit sind generell unzulässig.

Beispiel

Bemerkungen:

Der Niveaubegrenzer GESTRA NRS 1-50 wird mit 2 Wasserstandelektroden Typ GESTRA NRG 16-50 beschalten. Nach Herstellerunterlagen ist dies zulässig. Der GESTRA NRS 1-50 besitzt intern zwei getrennte Eingänge für die Wasserstandelektroden. Der erreichte SIL 3 wird nur unter Einhaltung der Auflagen in der GESTRA Betriebsanleitung Nr.: 808805-06 wirksam.

2.3.1 Scharfe Prüfung der Schutzeinrichtung und des Sicherheitsloop:

Messbereich:

Grenzwert: Wasserstand Min

Prüfintervall: 8760h

Lebensdauer erreicht: Ja Nein, verbleibend Jahre

Bauteil wie bei Ja Nein, neu am:

Inbetriebnahme: Hersteller:

Typ:

SIL-fähig:

Dokumente/ Zertifikate vorhanden:

Neuvalidierung erfolgt am/ Nummer:

Voralarm/Regelaus: %

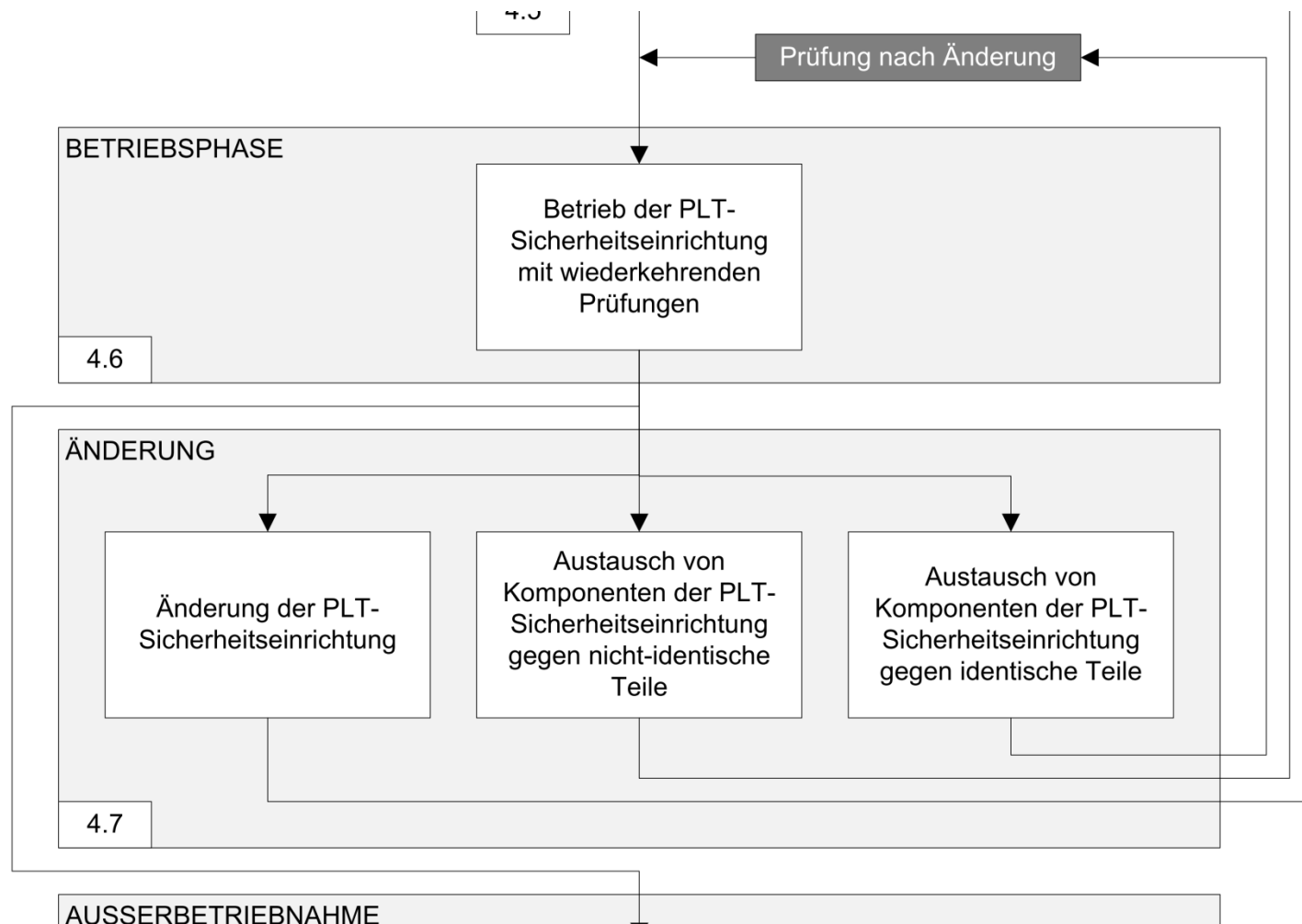
Abschaltung: %

Brenner verriegelt: Ja Nein

Wenn „NEIN“, Anlage stillsetzen und Fehler finden. Evtl. Neuvalidierung erforderlich.

Handeingriff: deaktiviert. Bestätigung durch Name ,Datum und Unterschrift

Änderung der PLT Sicherheitseinrichtung



Außerbetriebnahme

- Wenn eine PLT-Sicherheitseinrichtung einer weiterhin Betrieb befindlichen Anlage ganz oder teilweise außer Betrieb genommen werden soll, sind vor der geplanten Außerbetriebnahme der PLT-Sicherheitseinrichtung die sicherheitstechnischen Konsequenzen der Außerbetriebnahme für die Anlage zu bewerten, ggf. ist eine Risikobeurteilung durchzuführen.

Zusammenfassung

- Schreiben Sie alle Phasen des Lebenszykluses der PLT - Sicherheitseinrichtung schon mit Beginn der Konzeptphase fest und dokumentieren Sie dies.
- Planen Sie so genau wie möglich und schreiben Sie Grenzen fest.
- Dokumentieren Sie jede Abweichung.
- Schalten Sie Experten und Prüforganisationen so früh wie möglich ein um Folgekosten zu vermeiden.

VIELEN DANK FÜR DIE AUFMERKSAMKEIT

M.Eng. (FH) Sascha Pospischil

Funktionale Sicherheit

Telefon: 03628/598-473

Mobil: 0151/20331726

E-Mail: sascha.pospischil@tuev-thueringen.de