Nachweis des Safety Integrity Levels (SIL) für PLT-Schutzeinrichtungen aus elektronischen Komponenten

Vortragender: Daniel Düpont

Kaiserslautern, 07.07.2006

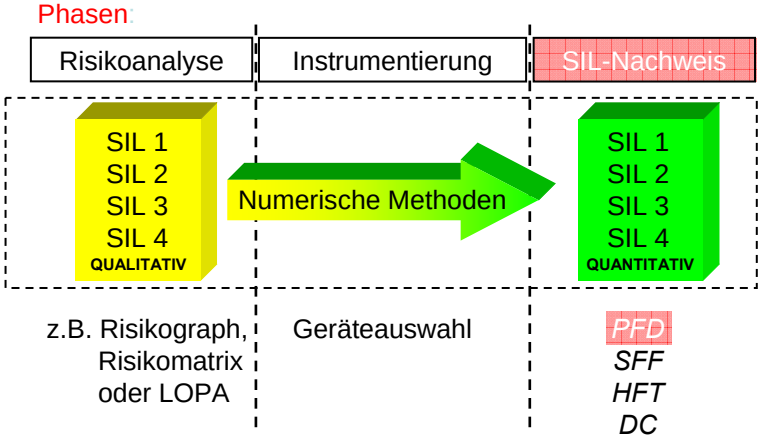
Inhalte

- Information
- Analytischer Bottom-Up-Ansatz
- Praxisorientierter Top-Down-Ansatz
- Analyse und Zusammenfassung
- Ausblick

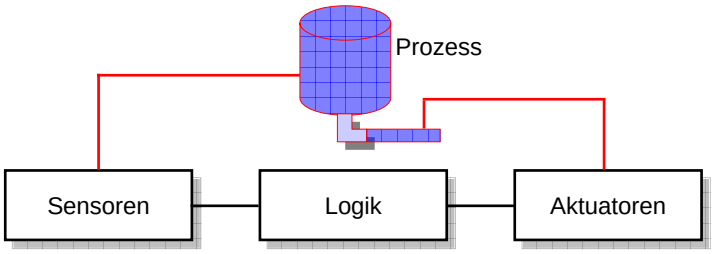
SIL-Assessment

Forderung nach IEC 61511:
ganzheitliches *SIL*-Assessment

Phasen:

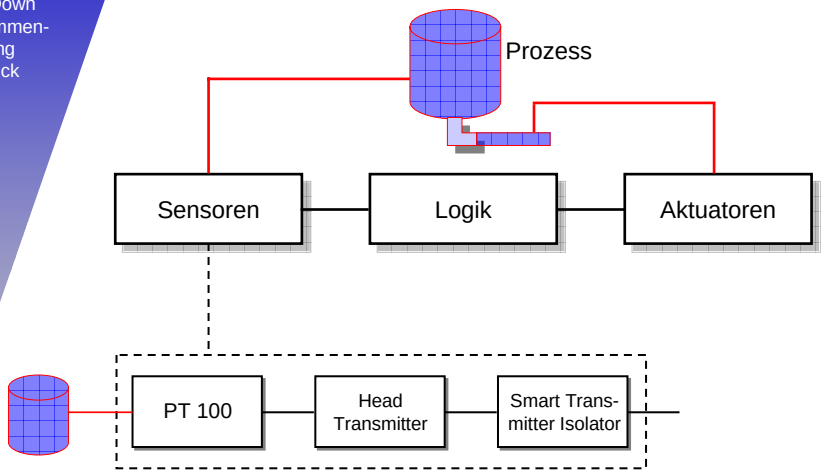


Struktur des verteilten Systems



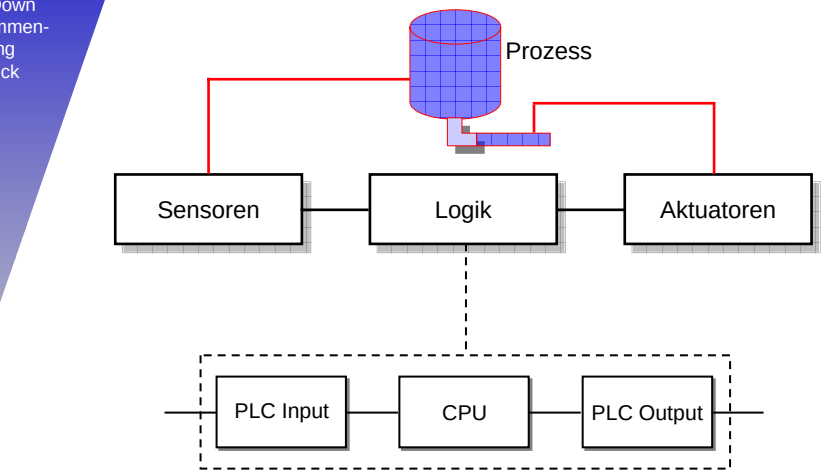
Struktur des verteilten Systems

1. Information
2. Bottom-Up
3. Top-Down
4. Zusammen-fassung
5. Ausblick

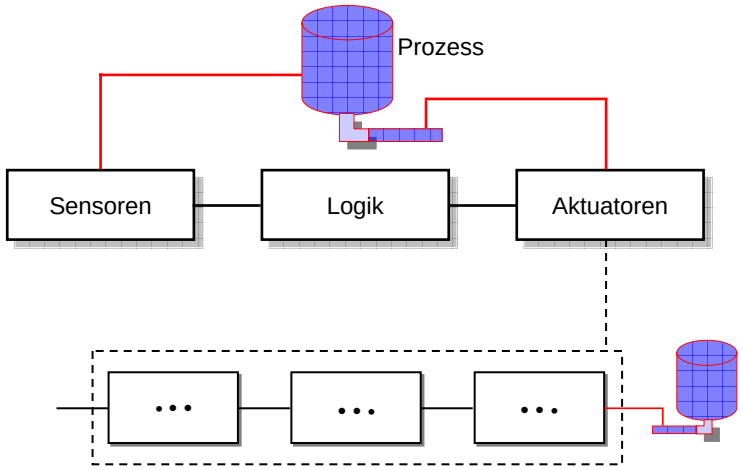


Struktur des verteilten Systems

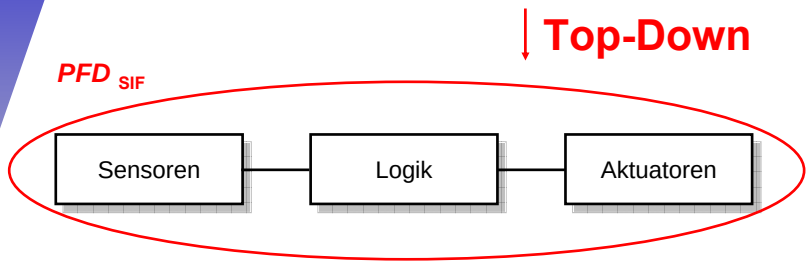
1. Information
2. Bottom-Up
3. Top-Down
4. Zusammen-fassung
5. Ausblick



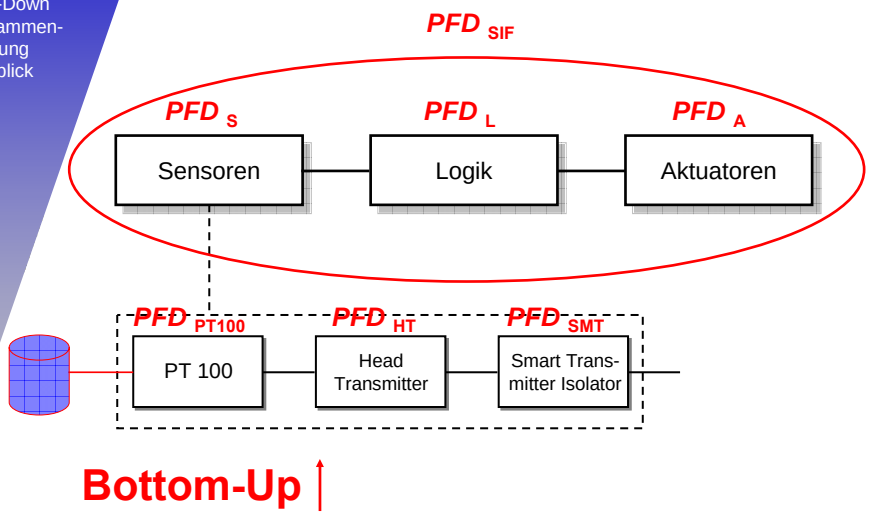
Struktur des verteilten Systems



Ansatzmöglichkeiten zur *PFD*-Bestimmung



Ansatzmöglichkeiten zur *PFD*-Bestimmung



Bottom-Up

Überblick

Prinzip:

PFD-Berechnung für die PLT-Schutzeinrichtung basierend auf den Fehlerraten der einzelnen Baugruppen.

Datenbasis:

SIL-Konformitätserklärungen der Hersteller.

Instrumentarium:

Markov-Modelle, Bayes-Netze, Fehlerbäume, …

Evaluierungsobjekt:

Typische Kreise aus der chemischen und pharmazeutischen Industrie.

SIL-Konformitätserklärungen:

- Zertifikate mit Fehlerraten für das jeweilige Produkt, bereitgestellt durch den Hersteller.
- Notwendiger Informationsgehalt zur *PFD*-Berechnung:
  λ_{DU} (Rate gefährlicher, unentdeckter Fehler)
- Softwaretools vorhanden, Benutzer muss Werte in die Datenbank einzupflegen

Achtung:

SIL-Konformitätserklärungen nur für neuere Produkte und generell problematisch für Komponenten mit Prozessanschluss.

Beispiel einer Herstellererklärung (NE 79) :
–gekürzt-

Beispiel einer Herstellererklärung

Der Hersteller..... bestätigt, dass
das Gerät.....mit der Softwareversion.....
nach NAMUR-Empfehlung 53
und der Hardwareversion .....
nach IEC 61508 für SIL 2 entwickelt und gefertigt wurde.
Die durchgeführte FMEDA ergab folgende Werte:
- Ausfallraten für
  - -sichere unentdeckte Ausfälle (λ_{SU}): .....
  - -sichere entdeckte Ausfälle (λ_{SD}): .....
  - -gefährliche unentdeckte Ausfälle (λ_{DU}): .....
  - -gefährliche entdeckte Ausfälle (λ_{DD}): .....

Daraus ergeben sich:
- der Anteil sicherer Ausfälle (*SFF*): .....
- die mittlere Betriebszeit (*MTBF*): .....
- die Diagnoseabdeckung (*DC*): .....

Evaluierungsobjekt

Typicals:

Über Jahre im Einsatz bewährte Standardlösungen für PLT-Schutzeinrichtungen (hier: einkanalig).

Quelle: NAMUR-Firmen

Geräteauswahl von internen Standardgerätelisten
⇨ meist Produkte ohne SIL-Konformitätserklärungen
⇨ Referenzdaten ähnlicher Produkte

⇨ kein exakter *PFD*-Wert, sondern *PFD*-Bandbreite

Bewertung von Typicals für:
- Druck (P)
- Temperatur (T)
- Füllstand (L)

Standardinstrumentierung

Typicals – Sensor und Logik

Druck

Sensor	Transmitter	Transmitter-speisegerät	SPS-Eingang	CPU
Rosemount 3051 TA		Cooper/ CEAG MS 271	HIMA F 6217	HIMA H51q F 8652 A

Temperatur

Sensor	Transmitter	Transmitter-speisegerät	SPS-Eingang	CPU
HERAEUS Pt 100	ABB TR01 - L	Cooper/ CEAG AH 77261	HIMA F 6217	HIMA H41q F 8652 A

Füllstand

Sensor	Transmitter	Transmitter-speisegerät	SPS-Eingang	CPU
VEGA Vegapuls 54 K		Cooper/ CEAG AH 420	HIMA F 6217	HIMA H51q F 8652 A

Daten

keine Daten

Typicals – Aktuator

Druck

SPS-Ausgang	Ventilsteuer-baustein	Magnetventil	Antrieb	Kugelhahn
HIMA F 3330	HIMA F 3328	SAMSON 3963	NORBRO 40 pneu.	ARGUS FK 79

Temperatur

SPS-Ausgang		Magnetventil	Antrieb	Kugelhahn
HIMA F 3331		SAMSON 3963	NORBRO 40 pneu.	VOLLMER TOPI 210

Füllstand

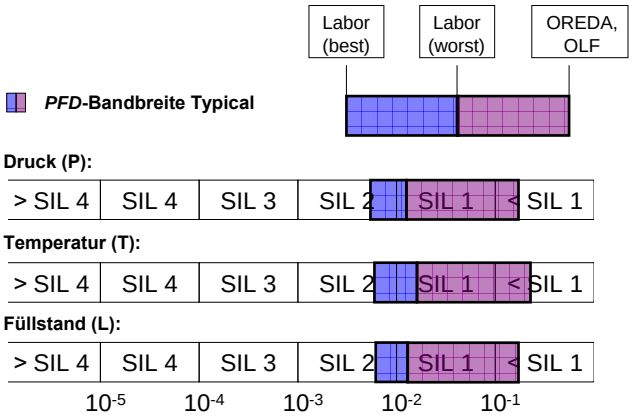
SPS-Ausgang		Magnetventil	Antrieb	Kugelhahn
HIMA F 3331		Seitz 1590 NoH /39	NORBRO 40 pneu.	VOLLMER TOPI 210

Daten

keine Daten

PFD-Bandbreiten

Prüfintervall ca. 11 Monate in Anlehnung an die jeweilige Gruppe der NAMUR-Daten



Überblick

Prinzip:

PLT-Schutzeinrichtung als Einheit.

Datenbasis:

NAMUR-Daten.

Instrumentarium:

Modifizierte, statistische Verfahren, z.B.
- Hypothesentest
- Konfidenzintervallschätzung

Evaluierungsobjekt:

Realisierte PLT-Schutzeinrichtungen in der chemischen und pharmazeutischen Industrie.

Datenbasis

NAMUR-Daten

Herkunft:

Mitgliedsfirmen der NAMUR aus chemischer und pharmazeutischer Industrie.

Teilnehmende Firmen:

33 (2003), 37 (2004).

Untersuchte Strukturen:

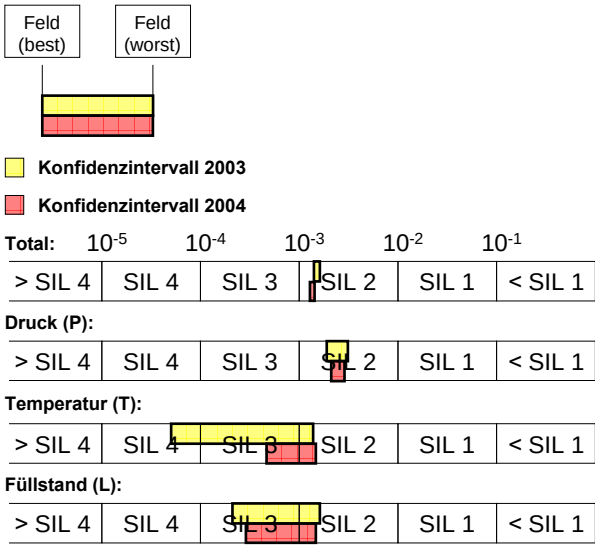
Ein- und zweikanalige Kreise.

Datenbasis

NAMUR-Daten (einkanalig):

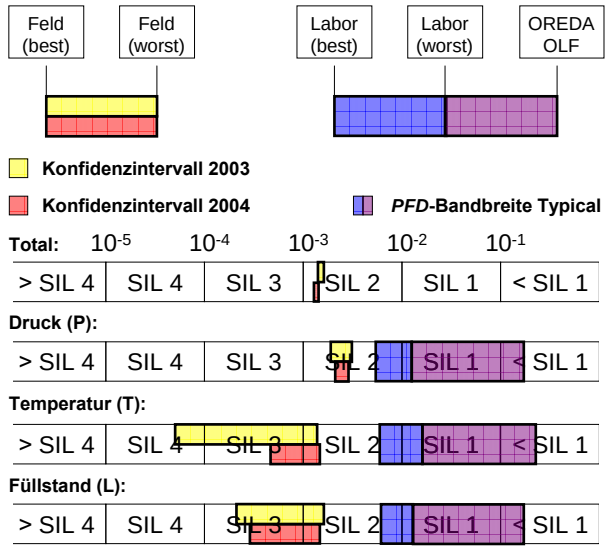
Jahr	Gruppe	Anzahl [abs.]	du-Fehler [abs.]	T_I [Jahre]	ΔT [Jahre]
2003	Total	12132	41	1	1
	P	1479	11	0,93	1
	T	1154	1	0,93	1
	L	1020	2	0,95	1
2004	Total	16260	43	1	1
	P	2292	18	0,93	1
	T	1936	5	0,93	1
	L	1368	3	0,95	1

PFD-Konfidenzintervalle der NAMUR-Daten



Konfidenz-niveau
1-α = 70%

Ergebnisvisualisierung



Konfidenz-niveau
1-α = 70%

Analyse

Einkanalige PLT-Schutzeinrichtungen

Bottom-up (Typicals)	Top-down (NAMUR-Daten)
Labor (worst case): SIL 1 Oreda, OLF: < SIL 1	Feld (worst case): SIL 2
Keine signifikanten Unterschiede zwischen Druck, Temperatur und Füllstand.	Ranking zwischen den Untergruppen. Ranking: Temperatur and Level fast gleich, Druck schlechter.

Zweikanalige PLT-Schutzeinrichtungen

Keine *PFD*-Analyse bisher.
Strukturanalyse kürzlich abgeschlossen.

Bisherige Publikationen

2005:

Litz, L.; Düpont, D.; Netter, P.: *SIL-Validation of Safety Instrumented Loops in Use by Statistical Methods.* Proceedings of the 2nd European Conference on Electrical and Instrumentation Applications in the Petroleum and Chemical Industry (IEEE PCIC Europe 2005), pp. 69-76, Basel (Schweiz), Oktober 2005.

Düpont, D.; Litz, L.; Netter, P.: *Evaluierung bestehender Sicherheitskreise anhand statistischer Methoden.* Poster, Dechema Jahrestagungen 2005, Chemie Ingenieur Technik, 77. Jahrgang, No. 8, Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim, S. 1143, 2005.

2006:

Litz, L., Düpont, D., Netter, P.: *SIL validation of safety instrumented loops in use by statistical methods.* atp International - Automation Technology in Practice, 1/ 2006, pp. 29-32, R. Oldenbourg Verlag, April 2006.

Düpont, D.; Litz, L., Netter, P.: *Evaluation of the analytical bottom-up SIL proof by statistical top-down methods.* Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (PSAM8), New Orleans (USA), Mai 2006.

Ausblick

Untersuchung weiterer Typicals

- einkanalig
- zweikanalig

Detailliertere NAMUR-Datenerfassung:

- Bestimmung einer De-Facto-Fehlerverteilung
- Isolation charakteristischer Werte

Fernziel: Verzahnung von Bottom-Up- und Top-Down-Ansatz

- Analyse der Zertifizierungspraxis von Herstellern elektronischer Komponenten
- Bestimmung von Korrekturfaktoren

Ausblick

Eingeworbenes neues Projekt mit 2-Jahresfinanzierung durch die BAYER AG, Start August 2006

TITEL:
Erweiterung von SIL-Nachweismethoden auf komplexere Strukturen

- Mitbenutzung von Komponenten des BPCS in PLT-Schutzeinrichtungen
- SIL-Einstufung komplexer Messsysteme
- *PFD*-Berechnungen für komplexe verteilte eingebettete Systeme (Abschaltketten)