

1. Ein Kunde wünscht, dass die Bauteile mit einem SIL-Aufkleber besonders gekennzeichnet werden. Gibt es hierzu Vorschriften bzw. Erfahrungen?

SIF Kennzeichnung JA – siehe VDI 2180.

Sandoz – Kennzeichnung mit Dreieck lt. Standard in Ordnung.

2. Welche Norm hat Gültigkeit bei Zentrifugen für Inertisierungs- und Vibrationsüberwachungen, die EN-61511 oder die EN-13849?

Vibro 13849 / EN62061– Inertisierung 61511

EN12547 als Zentrifugennorm (C Norm)

3. Darf man, wenn man z. B. für Schütze keine Berechnungswerte hat, dafür die Ersatzwerte aus der 13849 Anhang C, S. 58 verwenden?

HDM → Ja LDM → Nein

3. SIL-Einstufung: Ist die Anwendung der LOPA anstelle des Risikographen zulässig?

Ja .

4. Passive Bauteile (Pt100, Zenerbarrieren, exi-Trennungen): Muss man passive Bauteile in die Verifikation mit einbeziehen?

Ja und Nein – Bewerten auf jeden Fall (evtl. Fehlerausschluss)

Bsp.: Temperaturmesskopf Fa. Jumo, der nur mit „Original-Pt100“ zugelassen ist im Gegensatz zu Messkopf Fa. E&H wo keine Einschränkungen sind.

5. Komplizierte SIFs (z. B. Inertisierung einer Zentrifuge → 3 Wege die nacheinander gespült werden müssen): Wie könnte die Plausibilisierung in einer SI-Steuerung aussehen?

Durch die Dynamikerkenkung des FIZ können die N2 Ventile als MVZ ausgeführt werden und müssen nicht als Endlagenüberwachte SVZ ausgeführt werden.

6. Wie schaut die Verifikation bei Not-Stopp-Abschaltung aus und welche Norm kann ich anwenden?

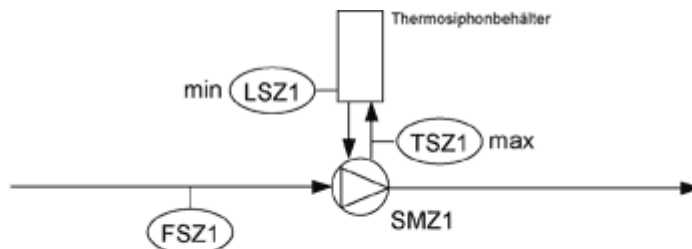
DIN EN 60204, DIN EN ISO 13850, EN 418 etc. – Zumeist als „Schadensbegrenzende Einrichtung“ in Verwendung (z.B. nach EN 12547 Zentrifugennorm) oder auch als „ergänzende Schutzeinrichtung“ – Faktor Mensch immer im Spiel !

7. Macht eine SIL-Einstufung bei einer Not-Stopp-Abschaltung überhaupt Sinn?

Nein, siehe Punkt 6 (obwohl in EN 60204 als Anmerkung unter 4.1.5 ein schwammiger Verweis auf eine Einstufung nach 13849/62061 zu finden ist !).

9. Eine Kreiselpumpe mit DGRD soll auf folgende Ereignisse abgesichert werden:
Die Pumpe wird abgeschaltet, wenn

- der FSZ1 anspricht (Trockenlauf Pumpe)
oder
- der LSZ1 anspricht (Überwachung Thermosiphonbehälter)
oder
- der TSZ1 anspricht (Temperaturüberwachung Sperrflüssigkeit)



$$\text{SIF} \rightarrow \text{PFD}_{\text{ges}} = \text{PFD}_{\text{lsz1}} + \text{PFD}_{\text{fsz1}} + \text{PFD}_{\text{tsz1}}$$

oder



SIF a \rightarrow PFD fsz1
SIF b \rightarrow PFD lsz1
SIF c \rightarrow PFD tsz 1

Wie erfolgt die Verifikation der dargestellten SIF?

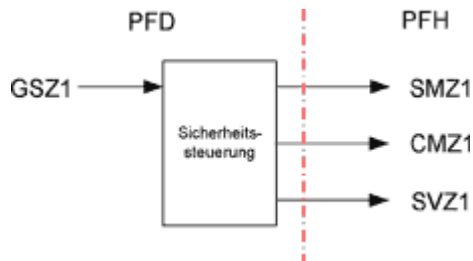
- a) Zählt man alle drei PFD-Werte zusammen oder
- b) rechnet man mit jedem einzelnen Sensor (SIFa, SIFb, SIFc)?

Die Schutzfunktionen gehören zu Einheiten zusammengefasst. Hier wäre TSZ mit LSZ eine Kombination für den Übertemperaturschutz, Also SIFbc als Kombination (SIFb und SIFc).

Der FSZ als Trockenlaufschutz mit eigener Spezifikation und Bewertung (SIFa).

10. Ein Näherungsschalter (GSZ1) soll bei Auslösung folgende Aktoren in die Sicherheitseinstellung bringen:

- a) SMZ1 – Pumpe stoppt
- b) CMZ1 – Antrieb stoppt
- c) SVZ1 – Ventil schließt



Wie erfolgt die Verifikation der grafisch dargestellten SIF?

- a) Zählt man alle drei PFH-Werte zusammen oder
- b) rechnet man mit jedem einzelnen Aktor (SIFa, SIFb, SIFc)?

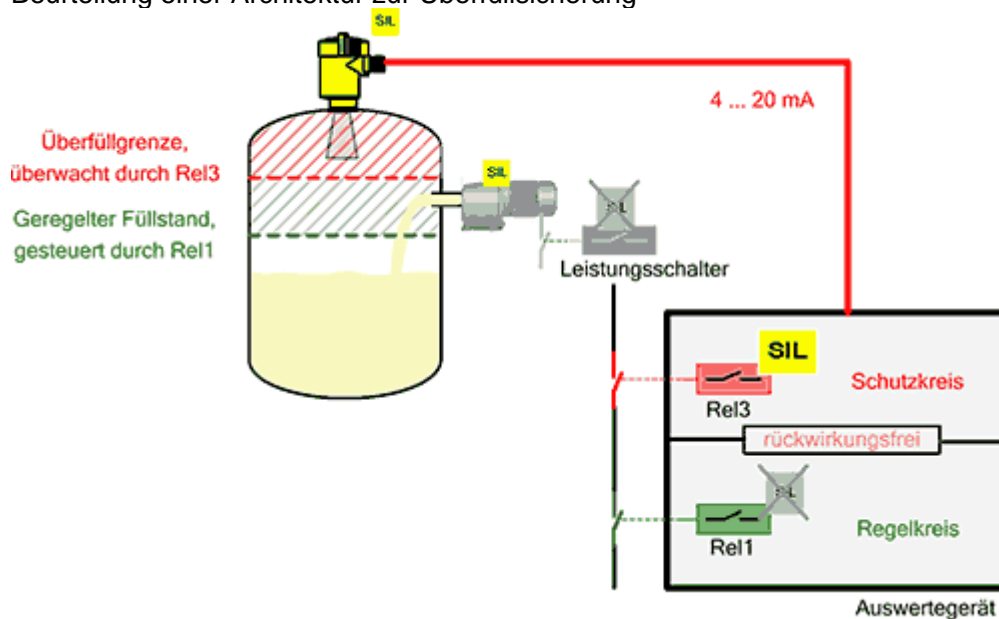
Lt. Aussage der Experten in der SIL-Sprechstunde ist eine Mischung von PFD und PFH zum rechnerischen Nachweis nicht zulässig.

Sandoz GmbH Kundl : Sicht bei Engineering-Partnern unterschiedlich – Handhabung wie bisher mit „Mischrechnung“ sollte so beibehalten werden, da teilweise Werte nicht verfügbar / sinnvoll sind.

Diskutiert wurde über Beispiel mit Schütz. Bei Betriebsart in High Demand Mode ginge es um Verschleiss und Schaltspiele (B10 Wert...), bei Betrieb in Low Demand Mode würden andere Faktoren ausschlaggebend wie Aushärten von Fett, Verschmutzung usw.

Im praktischen Betrieb wird weder definitionsgem. Low Demand noch High Demand vorliegen, da oft (speziell bei Schützen) Sicherheitsfunktion und Betriebsschaltung nicht getrennt sind.

11. Beurteilung einer Architektur zur Überfüllsicherung



Der Anwendungsfall zeigt, wie mit einem SIL2-Auswertegerät, einem SIL2-Sensor und einer SIL2- Pumpe eine Füllstandregelung und parallel eine Überfüllsicherung realisiert werden kann. Im Normalbetrieb wird die Pumpe bei Überschreiten der Schaltschwelle Rel1 mit dem Nicht-SIL-Relais 1 ausgeschaltet (betriebliche Abschaltung). Der Bereich oberhalb der Schaltschwelle Rel3 darf im Normalbetrieb nicht erreicht werden. Die eigentliche Überfüllsicherung wird mit dem SIL-Relais 3 realisiert: wird die Schaltschwelle Rel3 überschritten, schaltet das SIL-Relais 3 die Pumpe ab. Dieser Fall, dass z. B. das Relais 1 ausfällt und es so zum Überschreiten der Schaltschwelle Rel3 kommt, soll bei Betriebsart mit niedriger Anforderungsrate nicht mehr als einmal pro Jahr auftreten.

Anmerkungen:

- Der Regelkreis, der das Rel1 steuert, ist rückwirkungsfrei zum Schutzkreis, der das Rel3 steuert.
- Der Regelkreis sowie der Schutzkreis werden vom selben Sensorstromsignal gespeist.
- Für den Safety Loop Sensor \Leftrightarrow Schutzkreis im Auswertegerät \Leftrightarrow Aktor stehen jeweils die sicherheitstechnischen Kennzahlen SFF, PFD zur Verfügung.

Fragen:

- Darf grundsätzlich der Regelkreis sowie der Schutzkreis vom selben Sensorstromsignal gespeist werden?
- Wie wird der PFD für den genannten Safety Loop berechnet?

Sicherheitsfunktion und Betriebsreinrichtung sollten nicht dieselbe Messung verwenden. Das dürfte nur in speziellen Fällen passieren wo dadurch keine zusätzliche Gefährdung entsteht (Einzelbewertung z.B. als LOPA oder in Risikomatrix). Eventuell denkbar wären

Anwendungen wo man bestimmten gesetzl. Anforderungen unterliegt und spezielle Zulassungen dafür hat (Bsp. Deutsches WHG).

12. Was ist BPCS genau?

Wird unterschieden zwischen einerseits z. B. BPCS-Regelungen und -Steuerungen für den täglichen Betrieb und andererseits BPCS-Schutzeinrichtungen (ähnlich wie SIS)?
Zählen Operator-Alarme auch zu BPCS?

BPCS = „Basic Process Control System“ (das normale Prozessleitsystem). Bewertung ob BPCS Loop als Schutzeinrichtung dienen darf z.B. mit LOPA.

13. Wie groß ist der maximal erreichbare Risikominderungsfaktor für BPCS?

Kann man z. B. für a + b zusammen 100 ansetzen?

Steht dies eindeutig in der Norm?

Welche Anforderungen (Dokumentation etc.) werden an eine BPCS-Schutzeinrichtung gestellt? Wo ist das beschrieben?

Kann man auf einem SIS-zertifizierten Logic Solver mit BPCS mehr als Risikominderungsfaktor 10 erreichen?

In Österreich LOPA Werte im Zuge TÜV Arbeitskreis vorgeschlagen (voraussichtlich im 1 Q. 2011)

14. Was muss ich tun, wenn eine Werksnorm von der IEC61511 abweicht (z. B. mehrere BPCS-Loops in einem Szenario anstatt eines weiteren SIL1-Loop)?

Werksnorm darf Standard einer B oder C Norm nur übertreffen oder vergleichbar gut sein.

Wie groß ist der gesetzliche Interpretationsspielraum zum 'Gutsprechen' (nachträgliche Risikoanalyse mit der Umsetzung) von Altanlagen?

Siehe NE 126 „Bestandsschutz für PLT-Schutzeinrichtungen“

15. Wie sicher ist Software über den Lebenszyklus (Bibliotheken, Änderungen, Testen von Software)?

Darf SIL2-Software auf einer Software-SPS für die offizielle Validation verwendet werden (oder muss die spätere Hardware eingesetzt werden)?

Unterliegt komplett QM System wie z.B. in IEC 61511 vorgeschlagen.

Validation darf nur auf Zielsystem erfolgen.

16. Welche Folgen hat ein Firmware-Update auf einer SIL3-SPS (muss der SIS-Loop neu getestet werden)?

Je nach System – Wie in Herstellerhandbuch vorgegeben.

17. Wer ist offiziell und gerichtsfest befähigt SIL-Loops abzunehmen (mind. Nachweise)?

Deutsche Lage (in Österreich verm. ähnlich): Bei Druckgerät z.B. nur zugelassene Stelle, bei „normalen“ VT-Anlagen „jeder der sich berufen fühlt“ (Zitat Dr. Ströbl TÜV Süd).

Vorschlag aus IEC 61511 für Beurteilungsteam: „mindestens eine unabhängige sachkundige/qualifizierte Person“

18. Müssen Equipments ausgetauscht werden, nachdem das Zertifikat (für eine SIL-Einstufung) abgelaufen ist?

Durch welche Maßnahmen kann der Austausch verzögert/vermieden werden (Betriebsbewährtheit!)?

Wie ist zu verfahren, wenn es sich um betriebsbewährte Geräte handelt.

Meinungen und Aussagen dazu **unterschiedlichst** !

Ganz klare Aussage oft nicht möglich, gelten würde immer eine Festlegung in der Bedienungsanleitung eines Herstellers, wobei hier oft auf die 8-12 Jahre aus der Norm verwiesen wird. Letztendlich bleibt das wohl am Anwender hängen, da sich eine Reihe von theoretischen Überlegungen zu Zuverlässigkeit von elektronischen Systemen nicht ohne weiteres durch beobachten durch den Anwender neu bewerten lässt.

19. Wie geht man mit "Fail-Run"-Systemen um, z. B. einem Kühlsystem, das Pumpen und Kühlwasser benötigt?

Nachdenken →. (z.B. Umsetzung wie bei Notkühlsystemen mit Diesel Not Versorgung usw.)

20. Kann eine SIL3-Motorabschaltung (400 V) mit einem Schütz realisiert werden, insbesondere bei Hochspannungsanwendungen (6 KV und mehr), wo die Spulen zum Ausschalten bestromt werden müssen?

Schaltungsstruktur nicht geeignet für SIL 3 (HFT 1 gefordert).

21. Welche Qualifikation muss Wartungspersonal aufweisen, um SIL-Loops warten (prüfen, instandsetzen, austauschen) zu können?

In Deutschland. „befähigte Person“ nach BetrSichV

In Österreich nicht ganz eindeutig geregelt – teilw. Hinweise in bestimmten Normen auf Notwendigkeit von regelm. Schulungen (z.B. EN 60079)...

22. Es soll ein SIL1-Loop verifiziert werden: Welche Unterlagen sind dazu notwendig? Gibt es dazu Mindestanforderungen?

Punkt 19.2 aus IEC EN 61511:2004 Teil 2

23. Wie kann ich als Planer die Qualität eines Zertifikats für ein Gerät gemäß IEC61508 beurteilen (Glaubwürdigkeit, weltweiter Einkauf)?

Bis SIL 2 Herstellererklärung möglich, bei SIL 3 zertifizierte Stelle notwendig.

Allgemein kann gesagt werden das die Qualität solcher Zertifikate (speziell für bestimmte Anwendungen) sehr zweifelhaft ausfällt. Hier helfen wohl nur Erfahrungswerte.

24. Gibt es Regeln für Inhalt und Form für ein Zertifikat gemäß IEC61508? Wenn nein, ist dafür zukünftig etwas geplant?

Beispiele dafür in VDI 2180 und in NE 130 – allerdings sind dies nur Vorschläge!