PEPPERL+FUCHS

Your automation, our passion.

SIL-Sprechstunde

Mitschrift der Fragen und Antworten (2009 bis 2019)

Inhaltsverzeichnis

1. SIL-Sprechstunde 2009

Leider hab es 2009 kein Protokoll zu den Antworten

1. Benötigt auch eine Anlagenbauer bzw. Schaltschrankbauer ein „Functional Safety Management System“ oder nur der Gerätehersteller und evtl. der Anlagenbetreiber?

2. Safety Lifecycle Management (Leben oder nur Papierquälen) - gibt es eine Pflicht zur Ausbildung TÜV Functional Safety Engineer

3. Welche Informationen enthält das Safety-Manual? Wer muss es lesen bzw. wie wird dessen Beachtung sichergestellt? Wie hängt die SIL-Eignung des Geräts mit dem Safety-Manual zusammen? Wird es von der Norm gefordert?

4. Wie ist ein sicherer Alarm zu bewerten und auszuführen? Gibt es Realisierungskonzepte aus der Industrie?

5. Sind Not-Aus-Funktionen in die SIL-Betrachtung mit einzubeziehen

6. Wie ist die EN 50156 anzuwenden, wenn die Brenneranlage in eine Prozessanlage implementiert wird (hier EN 61511)?

7. Gibt es kraftwerksspezifische Festlegungen (VGB-Richtlinien) zu Risikoeinstufungen?

8. Nach VDI/VDE 2180 dürfen baumustergeprüfte Geräte einkanalig bis SIL-2 eingesetzt werden. Welche Ersatzwerte nimmt man in diesem Fall für eine SIL-Berechnung an? Welche Baumusterprüfungen sind hierbei für eine Tauglichkeit in SIL-Kreisen zulässig?

9. Ist es zulässig für MSR-Geräte ohne verfügbaren SIL-Produktbericht die statistischen Werte aus allgemeinen Quellen (z.B. OREDA) für den Nachweis der SIL-Integrität zu verwenden (z.B air operated globe valve MTBF=42)? Wenn ja, welche Quellen sind anerkannt?

10. Gebrauchsdauer: Welche praktische Auswirkung hat der Ablauf der Gebrauchsdauer von Komponenten/Bauteilen (üblicherweise 8-12 Jahre) auf einen SIL-Kreis? Müssen die fraglichen Komponenten getauscht werden? (Probabilistische Abschätzmethoden gehen ja von einer konstanten Ausfallrate aus, was nur innerhalb der Gebrauchsdauer angenommen werden darf.)

11. Sollten Geräte in Sicherheitskreisen in bestimmten Zyklen gegen neue Gerätschaften getauscht werden (Alterung von Bauteilen, Badewannenkurve)?

12. Sowohl die DIN EN 61508-6 als auch VDI/VDE 2180-4 liefern Formeln zur PFD-Berechnung für nicht-diversitäre Systeme. Gibt es - ggf. vereinfachte - Formeln für diversitäre Systeme, ohne statistische Berechnungsmethoden wie das Markov-Modell bemühen zu müssen? Kommt, in Anlehnung an VDI/VDE 2180-4, etwas in der Art von PFD(1oo2) = 4/3*PFD1(1oo1)*PFD2(1oo1) + Beta*sqrt(PFD1(1oo1)*PFD2(1oo1)) in Frage, ggf. unter besonderen Randbedingungen?

13. PFD-Nachweisrechnung der gesamten SIL-Kette bei mehrkanaliger diversitärer Auslegung?

14. Zur Verhinderung des Durchtrittsbetriebes bei Rührwerken benötigen wir eine SIL2 Schutzfunktion zur RW-Abschaltung. Füllstandssensor E+H Liquiphant mit SIL2 Zertifizierung, P&F Speisetrenner mit SIL2 Zertifizierung und ein Motorschütz ohne SIL-Zertifizierung (wir haben am Markt kein zertifiziertes Schütz gefunden. Siemens hatte in der Safety-Integrated Produktserie eines, das wurde jedoch abgekündigt). Wie erbringe ich den rechnerischen Nachweis der Ausfallwahrscheinlichkeit für das SIS, wenn ich über das Abschaltschütz keine Angaben wie PFDavg, SFF und SI-Level habe?

15. PFD-Nachweisrechnung der gesamten SIL-Kette von Sensor bis Aktor: Ersatzwertstrategien bei fehlender Datenbasis (keine PFD-Werte oder Lambda-Werte für Aktorik) (B10-Werte?)?

16. Werden rein mechanische Ausrüstungen fälschlicherweise mit SIL betrachtet?

17. Können im Aktorkreis Relais und Schütze verwendet werden, für die kein SIL-Zertifikat existiert und wie können aus B10-Werten die Lambda oder PFD-Werte berechnet bzw. abgeschätzt werden?

18. Gibt es „Bestandsschutz“ oder müssen bestehende Anlagen mit SIL-zertifizierten Komponenten nachgerüstet werden?

19. Was ist zu tun, wenn die Prozessleittechnik einer Anlage erneuert wird (z. B. verdrahtungsprogrammiert durch eine SSPS ersetzt wird). Müssen die Feldgeräte von z-Funktionen durch neue SIL-qualifizierte Geräte ersetzt werden?

20. Gibt es eine Verpflichtung zur SIL-Umstellung (jetzt und morgen)?

21. NE126 - wie kam es dazu und warum wird SIL so stark gefordert

22. Wie wird der Bestandsschutz gerichtsfest ("Stand der Technik" !)

23. Welche Daten werden benötigt um im Rahmen einer SIL-Berechnung die Betriebsbewährtheit eines Gerätes (z. B. Sensor) nachzuweisen und wie wird das gemacht?

24. Was muss man tun, damit eine Komponente als „betriebsbewährt“ gilt und in einer SIL-Applikation verwendet werden kann?

25. Wenn eine Komponente „betriebsbewährt“ ist, welchen SIL hat sie dann? Gibt es Unterschiede in den Anforderungen bei der „Betriebsbewährung“ je nach angestrebten SIL?

26. Welche Voraussetzungen sind für den Nachweis der Betriebsbewährung von Komponenten durch den Betreiber minimal zu erfüllen bzw. in welchem Umfang sind nachweisbare statistische Daten erforderlich.

27. Rückströmsicherungen bei Rohrleitungen im Werksverbund: Bei Rückström-sicherungen handelt es sich doch zweifellos um "ereignisverhindernde Schutz-einrichtungen", welche nach VDI/VDE 2180 zwingend klassifiziert werden müssen! 1. Mit dem herkömmlichen Riskographen kann man eine SIL-Stufe sehr schwer ableiten, da man in den meisten Fällen das Schadensausmaß nicht abschätzen kann. 2. Dürfen Rückströmsicherungen "regelnd" aufgebaut werden? (Problem: wenn keine Abnahme im Abzweig stattfindet, ist der Differenzdruck annähernd 0, was eine Auslösung der Schutzfunktion bei normalen Betriebszustand zur Folge hätte.)

28. Es sind bei uns im Unternehmen zwei Methoden zur Ermittlung des SI Levels bekannt: - Risiko Graph – LOPA. Beide Methoden sollten eigentlich vergleichbare Ergebnisse bringen. In einem konkreten Fall kommt es allerdings zu einer Abweichung von zwei SIL Stufen: - Risiko Graph: SIL 2 - LOPA: SIL 4 Möglicherweise werden bei LOPA bezüglich der Eintrittswahrscheinlichkeit oder dem Restrisiko zu hohe Werte angesetzt. Gibt es für beide Größen (Eintrittswahrscheinlichkeit und akzeptiertes Restrisiko) allgemein akzeptierte Einstufungsregeln?

29. Wie erfolgt die Berechnung (Nachweis für den Sensorteil) für die Erfassung komplexer Messwerte wie z.B. die Bildung eines Verhältnisses von 2 kompensierten Durchflüssen?

30. Wie sind Messgrößen, die zu einer Messwertkorrektur der eigentlichen SIL-relevanten Messung dienen (P,T), in die SIL-Nachweisrechnung mit einzubeziehen?

31. Welche Anforderungen gelten an vorgelagerte Hilfsenergieversorgungen (elektrisch, pneumatisch, hydraulisch) sowie Spannungsversorgungen allgemein? Sind diese in die SIL-Betrachtung und -Nachweisrechnung mit einzubeziehen?

32. In nichts zeigt sich der Mangel an mathematischer Bildung mehr, als in einer übertrieben genauen Rechnung" - CF Gauss => Sind die erhältlichen Daten (Exida,Tüv) vollkommen übertrieben?

2. SIL-Sprechstunde 2010

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): Wie könnte die Plausibilisierung in einer SI-Steuerung aussehen?

 3 Wege die nacheinander gespült werden müssen
Durch die Dynamikerkennung 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) || 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:
a. Der Regelkreis, der das Rel1 steuert, ist rückwirkungsfrei zum Schutzkreis, der das Rel3 steuert.
b. Der Regelkreis sowie der Schutzkreis werden vom selben Sensorstromsignal gespeist.
c. Für den Safety Loop Sensor ⇔ Schutzkreis im Auswertegerät ⇔ Aktor stehen jeweils die sicherheitstechnischen Kennzahlen SFF, PFD zur Verfügung.
Fragen:
d. Darf grundsätzlich der Regelkreis sowie der Schutzkreis vom selben Sensorstromsignal gespeist werden?
e. 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 SILEinstufung) 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!

3. SIL-Sprechstunde 2011

1. Benötigen Planungsbüros und Anlagenerrichter/Schaltschrankbauer ein Functional Safety Management?

2. Welche Qualifikation benötigen die Personen, die mit dem Design bzw. Aufbau einer SIL-Funktion betraut sind?

3. Welche Art der Dokumentation fordern die Normen?

4. Wie ist ein SIL-Kreis zu verifizieren, validieren und prüfen?

5. Wie lässt sich der SIL z. B. eines elektronischen Messumformers, eines Trennverstärkers oder eines Schaltverstärkers ermitteln?

6. Gebrauchsdauer von Feldgeräten in einer SIF: Sind Hersteller verpflichtet, Zeitangaben über die Gebrauchsdauer von Sensoren/Aktoren zu geben, oder nicht? Manche Hersteller geben klare Zeitangaben vor (z.B. 20 Jahre) und von manchen Firmen bekommt man diese Aussage: Sind solche Aussagen o.k.?

7. Kalibrierung von Pt100 in einer SIF: Müssen Pt100 bei der jährlichen SIWAKOAbschaltprüfung auch jeweils in einem Temperaturbad kalibriert werden? (SIWAKO = SIcherheits-, WArtungs- und KOntrollmaßnahmen)

8. Erforderliche Nachweise für Geräte-Software/-Firmware: Wie muss ein solcher Nachweis aussehen und wie wird das Thema in den Normen EN 61511 und EN 61508-3 behandelt?

9. Alarmbehandlung in einer SIF: Wie schaut die Alarmbehandlung (auf PLS oder SSPS) von sicherheitsgerichteten Sensoren/Aktoren bei anderen Firmen aus? Gibt es zum Handling dieser Alarme Betriebsanweisungen oder andere Vorschriften? Wie wird die Quittierung realisiert (in SIL Qualität oder PLS ausreichend) und wie werden die Alarme dokumentiert?

10. Jährliche Überprüfung der SIF: Messwerte „scharf anfahren“ oder genügt eine Simulation der Messwerte? Bringen Simulationen (z. B. Signalgeber auf die Sensoren) die erwünschten Ergebnisse? Können Fehler in der Prozessanbindung erkannt werden? Sind Funktionstests abweichend von Nennbedingungen (Nenndurchflüsse, Nenndrücke etc.) aussagekräftig genug?

11. Herstellerklärungen/SIL-Klassifizierung: Wie aussagekräftig sind solche SIL-Zertifikate (siehe Ausschnitte Beispiel 1 und 2)? Beispiel 1: Beispiel 2:

12. Wie sehen Sie, als SIL-Experten und Teilnehmer der SIL-Sprechstunde, die Qualität dieser SIL-Bewertung?

13. Wir haben eine PLT-Schutzeinrichtung, die ein Polymerisieren eines Stoffes in einem geschlossenen System verhindert. Mit einer weiteren PLT-Schutzeinrichtung kann eine voranschreitende Polymerisation gestoppt werden. Ich bezeichne die zweite Einrichtung als Hosenträger zum Gürtel. Meine Frage dazu lautet, wie eine SIL-Einstufung für diesen "Hosenträger" erfolgen kann, da die Eintrittswahrscheinlichkeit durch die erste PLT-Schutzeinrichtung theoretisch gegen Null läuft.

14. Welches Meinungsbild wird beim SIL-Nachweis bevorzugt: Betriebsbewährung oder der rechnerische Weg?

15. Welche Karenzzeit besteht für die Wiederholungsprüfung?

16. Die Prüfung vor der Erstinbetriebnahme ist ZÜS-pflichtig. Ist für Wiederholungsprüfungen die Prüfung durch eine befähigte Person ausreichend?

17. Wie geht man als Softwareprogrammierer mit Anlagenbetreibern um, die sich nicht mit dem Thema "Funktionale Sicherheit" auskennen und beschäftigen? Häufig kommt hinzu, dass der Anlagenbetreiber nur ein begrenztes Budget ausgeben will (so billig wie möglich) oder kann, so dass eine umfassende (Prüf-)Dokumentation der Software nicht möglich bzw. gewünscht ist. Wie ist hier die Rechtslage, falls etwas passiert? Der Programmierer hat schließlich "nur" das gemacht, was der Betreiber gewünscht hat.

18. In einer SIF wird bei der jährlichen SIWAKO-Prüfung festgestellt, dass der Sensor (z. B. ein Schwimmerschalter mit Reedkontakt) keinen Kurzschluss erkennt. Beim Gutzustand ist der Reedkontakt geschlossen. Wie sieht in diesem Fall das weitere Prozedere aus: → Darf man die Kurzschlussprüfung vernachlässigen? → Muss der Sensor gegen ein geeigneten Sensor getauscht werden?

19. Was muss man generell beachten, wenn Sensoren keine Kurzschlüsse oder Drahtbrüche erkennen?

20. Wie wird bei der Konfiguration mittels „unsicherem PC“ via FDT/DTM der SIL2/3 von Trennschaltverstärkern sichergestellt?

21. Wie ist das Verfahren der Konfiguration über Feldbussysteme, z. B. PROFIBUS-DP oder ethernetbasierte Systeme?

22. Die festgelegte Frist der wiederkehrenden Prüfung der Transmitter und Stellorgane steht bei kontinuierlichen verfahrenstechnischen Anlagen häufig im Widerspruch zur Betriebszeit der Anlage bis zum nächsten Stillstand, da z. B die Möglichkeit einer Demontage bzw. Vorgabe der physikalischen Größe nicht möglich ist. Welche Prüfmethoden, abweichend zum „Safety Manual“ bzw. VDE 2180 sind akzeptabel? Beispiel: Für die Überwachung des Durchflusses zu einem Reaktor sind zwei Vortexmeter mit örtlicher Anzeige direkt hintereinander installiert. Die Prüfung wird durch Vergleich der Messwerte/Trends zueinander und der Anzeigewerte am Gerät und der SSPS durchgeführt. Eine Kalibrierung erfolgt alle 5 Jahre.

23. Die Prüfung der kompletten SIF (Sensor/Logik/Aktor) während des laufenden Betriebes verfahrenstechnischer Anlagen erfordert bei komplexen Abschaltungen einen hohen Aufwand (zusätzliche Softwarebrücken, Ventilbypässe etc.). Unter Umständen werden für die Zeit der Prüfung wichtige Funktionen außer Kraft gesetzt. Ist es ausreichend die Prüfung der Sensoren und Stellorgane einzeln durchzuführen, wenn die Logik einer SSPS geprüft ist und keine wesentlichen Änderungen durchgeführt wurden?

24. Der Lebenszyklus einer SIF ist zu dokumentieren. In welcher Form wird diese Forderung praktisch umgesetzt? Welche Erfahrungen gibt es bei den Teilnehmern der SIL-Sprechstunde?

25. Ist es erforderlich, eine Dichtigkeitsprüfung der SIS-Ventile bei der Wiederholungsprüfung durchzuführen? Ein Funktionstest sagt nichts über die Dichtigkeit aus. Was ist, wenn das Ventil gerade an der Grenze der erlaubten Leckrate ist? Während des nächsten Betriebszyklus erhöht sich die Leckrate (unentdeckter gefährlicher Fehler).

26. Wie ist ein elektrischer Antrieb mit Pumpe als Aktor in eine Schutzeinrichtung einzubinden?

27. Gibt es "SIL-fähige" Geräte auch für die E-Technik? Beispiel: Eine 2v3 Drucküberwachung schaltet eine Pumpe aus.

Workshop 1: Loop-Design und SIL-Bewertung

Frage 5: Systematische Fehler und zufällige Fehler betrachten. Ersteres über FSM und Struktur, die zufälligen Fehler über PFD/PFH-Berechnung (probabilistische Methoden); Datenbanken über Fehlerraten der Einzelbauteile stehen zur Verfügung (z.B. SN 29500 oder IEC 62380, oder MIL HDBK 217);

Frage 9: Bsp.: 4...20 mA: Voralarm geht auf eine Nicht-SIL-Steuerung, Operator-Eingriff kann und soll ein Ansprechen der eigentlichen Schutzeinrichtung (diese ist SIL-bewertet) verhindern.

Frage 13: Möglich, dass die erste PLT – Schutzeinrichtung das Risiko nicht ausreichend reduziert (Restrisiko ist größer als das tolerierbare Risiko). Daher kann eine zweite PLT – Schutzeinrichtung erforderlich sein, um eine weitere Risikoreduzierung zu erreichen. Ermittlung der notwendigen SIL-Anforderung z. B. mit Risikograf, wobei bei der Abarbeitung des Risikografen das Vorhandensein der ersten PLT-Schutzeinrichtung berücksichtigt wird (Eintrittswahrscheinlichkeit des unerwünschten Ereignisses entsprechend klein).

Frage 14: Wichtig: Betriebsbewährung zielt primär auf Vermeidung von systematischen Fehler ab. Es ist nur bedingt eine probabilistische Betrachtung (Stichprobe zur Ermittlung der Fehlerrate im

Allgemeinen zu klein). PFD-Berechnung muss auf jeden Fall zusätzlich gemacht werden. Die erforderlichen Daten müssen durch weitere Quellen bzw. Gerätebeobachtung ermittelt werden.

In der Prozesstechnik wird in der Regel beides angewendet: Geräte sollen nach EN 61508 entwickelt werden. Zusätzlich werden diese dann noch der Betriebsbewährung unterzogen, um Einflüsse von Prozess (Medienberührung) zu hinterfragen.

Frage 26: Motor und Pumpe sind Teil eines sequentiellen Systems. Die PFD der beiden Komponenten können addiert werden. Aber: Frage ist nicht eindeutig gestellt: muss die Pumpe stehen oder laufen (Annahme: sicherer Zustand ist „Pumpe steht“). D.h. Hier wäre nur der Schütz kritisch, da weder Pumpe noch Motor alleine anlaufen oder weiterlaufen wenn die Schützkontakte geöffnet sind.

Frage 27: Ja, EN 61508 zielt ja expressis verbis auf elektrische/elektronische/programmierbar elektronische Geräte ab.

Workshop 2: Verifikation/Validierung und Prüfung

Frage 4: SIL-Kreis als solchen identifizieren, SRS erstellen, Prüfung bei jedem Planungsschritt. Validierung: sind die ausgewählten Produkte für die Applikation geeignet (z.B. Feuerungstechnik),

Frage 7/10: Regelwerk schreibt Prüfung im Medium vor; Vorschlag eines Teilnehmers: Pt100 vor Ort belassen, Temperatur-Anzeige ablesen und mit Ohm-Meter den Widerstand R messen. Problem: Schichten auf Pt-100 werden dadurch nicht entdeckt. Wichtig: Prüfung erst planen (inkl. Gefährdungsbeurteilung) und danach geeignete Prüfanweisung erstellen.

Lösung: in bestimmten Betriebszuständen (z.B. Anlagenstillstand) sind die Messstellen ohnehin verfügbar; für diese Zeitpunkte kann eine solche Detailprüfung durchgeführt werden. Hilfe: selektive Prüfung evtl. abhängig vom Zustand der Anlage, so dass nach einer Zeit x eine 100%-Prüfung durchgeführt wurde. Prüfanweisung sinnvollerweise in Zusammenarbeit mit dem Betreiber aufstellen, der Prozesskenntnisse hat.

Verzicht auf 100%-Prüfung: Ist unter Umständen möglich, wenn die gefährlichen unerkannten Fehler evtl. nicht auftreten können (Fehlerausschluss).

Im Vorfeld evtl. Prüfstand aufbauen, um bestimmte Zustände zu simulieren.

Evtl. liefert der Lieferant des Pt100 Prüfanweisungen, z.B. bei korrekten Durchfahren von 0...100°C sind auch andere Fehler ausgeschlossen.

Exida-Tool mit variabler Prüffrist: Abschätzung darüber vornehmen, wann ca. 80 oder 90% der

Prüfung durchgeführt werden. Exakte Vorgaben aus dem Regelwerk existieren nicht und sind individuell zu ermitteln und dokumentieren.

Nicht ausreichende Wiederholungsprüfungen führen unter Umständen zu einem Verlust der SIL-Einstufung.

Frage 15: Üblicher Weise wird toleriert, dass der Prüftermin um 1 Monat variiert werden kann. Vorsicht: kumulierte Verschiebung ist nicht zulässig.

Hinweis: Intervall der regelmäßigen Wiederholungsprüfung berücksichtigen (z.B. Standard: 3 Jahre, dann ist 1 Monat ok; bei monatlicher Wiederholungsprüfung aber Verschiebung nur um Tage)

Bsp.: Hersteller gibt PFD für 1 Jahr an; Verlängerung auf 3 Jahre möglich? Vorsicht bei Umgebungsbedingungen! Eine Umrechnung ausgehend vom PFD-Wert geht nicht immer (nur bei einkanaligen Systemen). Bei mehrkanaligen Systemen benötigt man auf jeden Fall Lambda_du.

Frage: unterschiedliche Prüffristen für Sensorik und Aktorik erlaubt? Ja, siehe NAMUR-Empfehlung NE 103.

Frage 16: Normen zur funktionalen Sicherheit kennen die Begriffe wie ZÜS, befähigte Person etc. nicht. Es ist jedoch im Einzelfall zu ermitteln, welche konkrete Prüfanforderungen gemäß BetrSichV bestehen. Diese können evtl. durch befähigte Personen erfolgen. (Z. B. befähigte Person zum Prüfen allgemeiner Arbeitsmittel)

Frage 18/19: Vernachlässigung ist nicht zulässig, aber: geeignete SPS-Karte mit LB/KS-Erkennung ist evtl. auch möglich. Oder: Zusätzliche Widerstandsbeschaltung vorsehen um LB/KS zu detektieren. Auch ein Fehlerausschluss kann in Betracht kommen, muss aber begründet und dokumentiert werden.

Frage 20/21: organisatorische Maßnahme, d.h. nur geschulte Personen haben Zugriff.

Einstellungen müssen nachträglich verifiziert werden. Hersteller muss sicherstellen, dass keine verbotenen Speicherbereiche versehentlich geschrieben werden können. Ferner müssen die Einstellungen über DIP-Schalter oder Passwort geschützt werden.

Frage 22: Verlängerung der Prüffrist ist unter bestimmten Bedingungen möglich. Situation wie bei Fragen 7/10 (siehe oben).

Frage 23: Stichwort: selektive Prüfung! Ist prinzipiell möglich, sofern entsprechend geplant und im Prüfplan dokumentiert. Bei Änderungen von Software: Anforderungen der Steuerungen beachten; unter Umständen ist eine 100%-Prüfung durchzuführen oder aber die Steuerung hat einen Versionsvergleich.

Frage 25: Kommt auf die Applikation bzw. den Prüfplan an: falls eine Dichtigkeitsprüfung erforderlich ist, dann ist diese auch durchführen. Automatische Dichtheitsprüfung im Prozess ist evtl. ebenfalls denkbar.

Workshop 3: FSM-System und Dokumentation

Frage 1: Ja, allerdings ist es unter Umständen ausreichend (z. B. als Schaltschrankbauer), sich eines vorhandenen FSM-Systems des Auftraggebers zu bedienen. Damit können die Anforderungen der Norm erfüllt werden.

In der Praxis werden von größeren Betreibern konkrete Vorgaben gemacht oder die Vertragspartner werden vom Auftraggeber auditiert.

Situation der Planungsbüros: Verantwortung liegt beim Betreiber und dieser muss Vorgaben machen oder auditieren.

Art der Dokumentation: lückenlose Dokumentation aller Projektphasen inkl. der entsprechenden Verantwortlichkeiten.

Verweise auf bereits vorhandene Dokumente bzw. QM-Systeme sind zulässig und durchaus sinnvoll.

Frage 2: Sinnvoll ist zeitnahe Berufserfahrung in ähnlichen Projekten, Erfahrungen mit der Gerätetechnik, internes Trainingsprogramm und Kenntnisse zu den Anforderungen des FSM-Systems. Es müssen bezüglich der o. g. Anforderungen entsprechende Nachweise vorliegen. ISO 9000 etc. erforderlich, ferner BetrSichV beachten

Frage 6: Lebensdauerangaben sind kritisch zu hinterfragen; Angaben sind nicht immer absolut erforderlich, da die Lebensdauer oft stark von den Umgebungsbedingungen abhängt. Eine Berücksichtigung der Gebrauchsdauer ist nach Norm erforderlich. Hierzu müssen Betreiber und Hersteller eng zusammenarbeiten.

Frage 8: Bei Software-basierten Geräten: Release-Datum dokumentieren, Anforderungen an die Software-Entwicklung beachten (EN 61508 Teil 3 bzw. EN 61511 Kapitel 12). Betriebsbewährung bei Software ist sehr schwierig und wird unter den Fachleuten kontrovers diskutiert.

Frage 11, 12: Anwendung von probabilistischen Modellen auf mechanische Komponenten ist oft problematisch (Bsp. 2). Weiterhin ist die Bewertung seitens des Herstellers auf Basis von Rückläufern evtl. kritisch. Bsp.: 1: Angabe Typ A oder B fehlt, Angabe des Wiederholungsprüfungs-Intervalls fehlt.

Frage 12 spez.: Folgende Lücken fallen unmittelbar auf: Architektur geht nicht eindeutig hervor, Geräte unbekannt, Quellen der Werte nicht bekannt, Fehlersicherheit aus Ex-Zertifikat ist nicht gleichbedeutend mit Fehlerausschluss gem. SIL

Frage 17: Verantwortung bleibt eindeutig beim Betreiber.

4. SIL-Sprechstunde 2012

Hier eine schriftliche Zusammenfassung der Fragestellungen und der Antworten.
Die Antworten zu den Fragen in **Blau** basieren vornehmlich auf Aussagen von Herrn Ströbl (TÜV Süd Industrie Service GmbH).
Die Antworten zu den Fragen in **Rot** basieren maßgeblich auf Aussagen von Herrn Klotz-Engmann (Endress + Hauser Messtechnik GmbH + Co. KG), Herrn Hug, BimSchG §29a Sachverständiger und Herrn Hildebrandt, Pepperl + Fuchs GmbH.
Die Antworten zu den Fragen in **Grün** basieren maßgeblich auf Aussagen von Herrn Klotz-Engmann (Endress + Hauser Messtechnik GmbH + Co. KG), und Herrn Hug, BimSchG §29a Sachverständiger.

1. Gibt es aktuelle bzw. zukünftige Änderungen in der IEC 61511?

Die Norm ist in der Überarbeitung. Folgende Änderungen sind geplant:
- SFF entfällt
- Security als Thema
- Zusätzlich wird der Eingriff eines Operators berücksichtigt
- Das Leitsystem darf bei der Berechnung das Risiko reduzieren
- Die Gebrauchsdauer von Komponenten wird berücksichtigt

Die VDI/VDE 2180 soll an diese neue IEC 61511 angepasst werden.

2. Gibt es aktuelle bzw. zukünftige Änderungen in der IEC 61508?

Derzeit ist keine Änderung in Sicht. Das Maintenance Team wird sich 2014 wieder treffen um eine neue Ausgabe zu diskutieren.

3. Wie schaut die SIL-Zukunft aus? Gibt es mögliche Veränderungen?

Siehe 1+2.

4. Ist das Thema SIL bei den Herstellern jetzt vollständig angekommen?

Je nach Hersteller finden sich mehr oder weniger Informationen zum Thema. Der Errichter sollte sich hier immer selbst ein Bild machen. Bei den großen Herstellern ist das Thema umgesetzt.

5. VDMA 4315 vs. VDE 2180 Risikograph – wer setzt sich durch?

VDMA 4315 gilt für Turbomaschinen und damit im Bereich Maschinensicherheit. VDE 2180 betrifft Prozesssicherheit. Damit sind die Gebiete eindeutig festgelegt, ein Angleichen ist aufgrund der unterschiedlichen Applikation nicht nötig.

6. Wie sind die rechtlichen/gesetzlichen Grundlagen zur SIL-Beurteilung von Geräten?

Es besteht vom Gesetz her keine Verpflichtung, eine SIL-Beurteilung von Geräten vorzunehmen oder Zertifikate erstellen zu lassen. Von der BetrSichV, Arbeitsschutzgesetz, Störfallverordnung etc. her ist für bestimmte Anlagen Errichter / Betreiber / Arbeitgeber eine Verpflichtung abzuleiten bei der Ermittlung von Schutzmaßnahmen den Stand der Technik zu beachten. Dazu bieten die Normen EN/IEC 61508 / 61511 eine Grundlage. Wenn Safety im Zusammenhang mit ATEX eine Rolle spielt ist die Norm DIN EN 50495:2010 zu benutzen.

7. Zur Erreichung einer ermittelten Risikoreduzierung mit Anforderung SIL 1, 2

oder 3 werden zertifizierte Sensoren, Final Elements & zertifizierte SPS (z. B.

SIL 3 zertifiziert) eingesetzt. A) Ist die Nutzung eines modernen DCS Systems (mit Redundanz für Power, CPU, IO Karten) für SIL 1 Loops tolerierbar? B) Ist die Verifizierung der SIL1 Loops zwingend erforderlich?

A) Nein.
B) Ja.
Es geht auch bei SIL 1 um eine Sicherheitseinrichtung. Diese muss identisch wie SIL 2 / 3-Einrichtungen betrachtet werden.

8. Für elektromechanische Komponenten geben die Hersteller "Standard Ausfallraten" (bei niedriger Anforderungsrate) in deren Werksnorm bekannt. Beispiel: Siemens SIRIUS Schütze: 100 FIT (Siemens Werknorm SN31920, Ausgabe 2011-09) Ist es für Anwender zulässig, diese "nicht zertifizierte Werksangabe" bei einer Verifizierung von z.B. SIL 1 Loops zu nutzen?

Ja. Es ist aber zu hinterfragen ob es im Einzelfall die richtige Einrichtung für den Zweck ist.

9. In IEC 61508-6 Ed.2 wurde Tabelle D.5 zur CCF-Bewertung (β) neu hinzugefügt. Dies hat für die häufig verwendete 2oo3-Struktur eine effektive Verschlechterung des PFD-Wertes um 50% gegenüber der ersten Version der Norm zur Folge. Wie ist hierzu die Meinung der Experten?

Die einfachste Lösung zur Festlegung eines CCF ist gegeben in der VDE 2180 Teil 4. Dort sind nur Abstufungen definiert (2%, 5%, 10%)

10. Brenner in thermische Prozessanlagen werden in der Industrie verschiedentlich eingestuft -> Low/High – Demand. Kommt es nicht einfach auf die Demand Rate an? Gibt es einen Bezug zur MRL 2006/42/EG (gemäß 746.2-2011), somit per Definition eine Maschine und daher PFH?

Feuerungen sind thermische Prozessanlagen, fallen aber per Definition unter die Maschinenrichtlinie. Die Anforderungen sind aber realistischerweise als Low demand einzustufen. Dieser Konflikt erklärt die unterschiedlichen Betrachtungsweisen.

Ein weiterer Konflikt ist gegeben mit der 746.2-2011. Diese sagt auf Seite 69, dass PL e gefordert werden muss während die ISO 13849-1 das mit einer nicht sicherheitsgerichteten SPS nicht zulässt.
Eine Lösung bietet die Verwendung der EN 50156, die auf Seite 71 den Weg beschreibt wie mit einer Zweifehlersicherheit argumentiert werden kann. Das geht ohne SIL oder PL. Hier kann entweder mit einem Meldesignal gearbeitet werden wenn die Anlage beaufsichtigt wird oder mit einem Auslösesignal wenn die Anlage nicht beaufsichtigt ist.

11. Was gibt es Neues beim Thema SIL und Ex-Schutz

Seit Langem ist die EN 50495 für die Bewertung von Geräten etabliert. Diese soll in den nächsten 3 Jahren zu einer IEC werden.
Weitere Regelwerke werden gerade erstellt:
Technische Regel zur Betriebssicherheit TRBS 2152 Teil 5.

VDI/VDE 2180 Blatt 6
NE138
Hier sind zum Teil konkrete Angaben zu SIL-Anforderungen angegeben, diese befinden sich aber noch in Diskussion.

12. Risikograph: übliche/verallgemeinerte Ansätze? – Verletzung vs. Tod?

Beim Risikographen sind die Zahlen von Toten / Verletzten entscheidend. Die Norm EN 50126 macht sich Gedanken um die minimale endogene Mortalität und beziffert diese als 2×10^{-4} pro Person und Jahr. Dieser Wert entspricht der statistischen Mortalität eines europäischen Schulkindes.
Als gesellschaftlich akzeptabel wird oftmals angenommen, wenn sich dieser Wert um 10% erhöht. Es gibt aber auch Vorschriften die diese niedriger festlegen (z.B. 10^{-6} in IGE/ST/15 Ed.4).
Konsequenterweise wird aufgrund des in der Applikation zu reduzierenden Risikos der Risikograph individuell kalibriert.
Aber: ISO 13949-1 bewertet Tod und Invalidität gleich.

13. FSM (Functional Safety Management) – Tools -> Lebenszyklus in SAP integriert? Und:

14. Wie werden systematische Fehler vermieden?

Systematische Fehler werden durch FSM vermieden. Als Software ist laut Herrn Schroers (Bayer) das Tool ‚Meridium' für Anwender erhältlich.
Ein wesentlicher Bestandteil des FSM-Systems ist das Vier-Augen-Prinzip.

15. Wie können mögliche Fehler beherrscht werden?

Maßnahmen zur Fehlerbeherrschung sind:
Redundanz
Diagnose
Fail-Safe

16. Wie kann man die SIL-Einstufung der Geräte, soweit erforderlich, kosteneffizient abwickeln?

Dokumentation ist der Schlüssel, diese muss adäquat erstellt werden und verfügbar sein. Hier entstehen wenig Einsparpotenziale.

17. Wie soll eine SIL-Dokumentation aussehen? Gibt es hierfür eine Musterdoku?

Hersteller: Safety Manual ist laut IEC 61508-2:2010 Anhang D zu erstellen. Es gibt keine Musterdoku für den SIL-Nachweis.
Anwender: IEC 61511-1:2005 Anhang A.

18. In welchem Umfang greift der Bestandsschutz bei Änderungen von: - Feldgeräte (Austausch / Ersatz durch neue Technologie) - SW Änderungen im PES - Upgrade von PES - HW Ersatz der PES durch neues System

Aussagen die Bestandsschutz definieren finden sich in NE126. Ein grundsätzlicher Anspruch auf Bestandsschutz findet sich nicht, eine Prüfstelle wird aber üblicherweise nicht plötzlich und kurzfristig eine Umgestaltung fordern.

19. Gibt es Beispiele für Messkreisbewertungen bei denen keine SIL Verifikation machbar bzw. realisierbar ist?

Es gibt Fälle in denen die Normen IEC 61508 und IEC 61511 nicht angewendetwerden können, z.B. bei fehlender Gerätequalifizierung. Wenn keine SIL-Verifikation möglich ist kann eventuell nach EN 50156 eine Bewertung der Sicherheit vorgenommen werden.

20. Auf welche praktikable Art und Weise kann ich eine Stördatenstatistik führen? (was muss ich tun und was kann ich tun?)

Stördatenerfassung laut NE93. Ein entsprechendes Software-Tool ist in Arbeit. Nähere Informationen sind über den entsprechenden NAMUR-Arbeitskreis zur NE 193 verfügbar.

21. Problematik Rohrleitungen und Verkabelung – gibt es hierfür Regelungen/Vorgaben?

Bei el. Leitungen: Wo immer möglich Ruhestromprinzip bei analogen Signalen (4-20 mA) mit Leitungsbruch/Leitungskurzschluß-Erkennung (Diagnose). Bei Binärsignalen wenn möglich Fail-Safe-Prinzip (energieloser Zustand ist der sichere Zustand).
VDE 2180 Teil 3: Es ist auszuschließen dass ein Fehler in der Verkabelung die Redundanz aufhebt (Nagetiere!!!).
Bei Pneumatikleitungen: Für Rohrleitungen (z.B. Impulsleitungen zum Schalten von Pneumatikventilen) gibt es Regelwerke aus der Druckgeräterichtlinie. Bisher EN 892, EN 893. Heute EN ISO 4413, EN ISO 4414. Die Normen beziehen sich auf Ausschluss systematischer Fehler.
Wichtig: die Struktur muss bekannt sein, wie z.B. Verschaltungsbild von Ventilen in der Anlage (Entscheidung 1oo2, 1oo3, 2oo2). Maßgeblich ist die Sicherheitsfunktion. Muss sicher abgesperrt werden oder z. B. zur Druckentlastung sicher geöffnet werden?

22. 100 % SFF die Zukunft? – warum wird Mechanik betrachtet? Werbegag oder sinnvoll?

Bei Aktorik sind stochastische Fehler in der Regel sehr selten. Oft kommt es zu sehr kleinen Lambda-Werten.
Bei „Partial Stroke Test“ wird üblicherweise mit 70% - 80% Diagnosedeckungsgrad gerechnet
Bei Hydraulik weniger interessant, aber bei Pneumatik sehr wichtig: Drucktests (Partial Stroke Test hier meist nicht sinnvoll)
Je näher man an 100% SFF kommen will, umso aufwändiger (teurer) wird die Diagnose. Nahezu 100% eventuell durch verschiedene Meßmöglichkeiten erreichbar.

23. Wahrscheinlichkeiten Regelkreisausfall?

(Fragestellung war nich ganz klar, Interpretation war wie folgt)
Risikograph und LOPA: LOPA: Schutzeinrichtung als nicht vorhanden angenommen, Es kommt zum Ausfall, dann Frage nach dem Sicherheitskreis. Fragestellung war wohl, inwiefern die Ausfallwahrscheinlichkeit der Regelung in die Sicherheitsbetrachtung einfließen kann.
Wenn das Stellglied (oder ein anderer Teil) für beides benutzt wird kann man nicht das vermeintlich fehlerhafte Gerät zur Sicherheitsfunktion heranziehen.
Sensorik darf mitbenutzt werden wenn Rückwirkungsfreiheit gegeben ist.
Anmerkung Herr Schroers (Bayer): das betrachtete zu vermeidende (unerwünschte) Ereignis ist der Ausfall einer Regelung. Bei Mitbenutzung durch die Sicherheitsfunktion würde bei Ausfall der Regelung auch immer die selbige versagen.

24. Können "normale" Geräte in einer Schutzeinrichtung eingesetzt werden?

NE130 fordert dann Typprüfungen, was nicht ernsthaft realisierbar ist. NE79 erlaubt Herstelleranfrage nach Ausfallbewertung und Fehleranalyse. Gerätequalifizierung auf Basis „früherer Verwendung“ (Anwender) ist theoretisch ebenfalls denkbar, scheitert aber oft an zu geringer Datenbasis.

25. Wie wird die Versagenswahrscheinlichkeit berechnet?

Siehe Vortrag von Herrn Klotz-Engmann (Endress + Hauser).

26. Müssen im Zweifelsfall alle Komponenten einzeln beurteilt werden oder ist eine Gruppenbeurteilung (z.B. Sensoren, Messumformer) möglich?

Galvanisch trennende Elemente (z. B. Ex Barrieren) werden meist nicht als separates Element der Sicherheitsfunktion angesehen (gemeinsame Beurteilung mit Feldgerät möglich). Die Hersteller bewerten diese Geräte als „Einzelgerät“. Kugelhahn, Antrieb und Magnetventil werden überwiegend als Einheit bewertet.

27. In wie weit müssen Feldverteiler, Klemmen, Verkabelung, Schrankklemmen (der vorhandenen Infrastruktur) den "SIL-Anforderungen" genügen.

Siehe 21. Ob z.B. geschirmte Leitungen nötig sind hängt mit den Anforderungen aus den Betriebsanleitungen der Einzelgeräte zusammen. EMV und Blitzschutz sind für die gesamte Anlage zu betrachten, ebenso ob eine getrennte Verlegung von Signalleitungen nötig wird.

28. In vielen SIL-Kreisen nach 61511 (low demand) werden Komponenten (Schütze, etc.) aus dem Bereich der Maschinensicherheit verwendet. Für diese stehen in der Regel nur B10-Werte (Herstellerangaben angelehnt an ISO 13849) zur Verfügung. In der 2. SIL-Sprechstunde (Frage 3) wurde die Aussage getroffen, dass diese Werte im LDM nicht verwendet werden dürfen. Wie ist in diesen Fällen vorzugehen?

Die Frage ist, ob wirklich nur einmal im Jahr eine Anforderung kommt. Wenn ja gibt die NE142 die Möglichkeit zum Fehlerausschluss. Beispiel Schütz. Wenn die Schaltleistung unter 60 – 70 % des Nennwertes im AC3-Betrieb liegt ist die Überdimensionierung ausreichend um einen Fehlerausschluss zu erlauben (λ = 0). Anfrage beim Hersteller möglich ob dieser schon eine Überdimensionierung im Datenblatt vorgenommen hat. Wichtig ist: Ein Fehlerausschluss ist immer eine Einzelfallbetrachtung und muss vollständig dokumentiert werden.

Achtung: SIL 2 ist in der Chemie in der Regel einkanalig, im Maschinenbau aber typischerweise zweikanalig (Kategorie 3).

29. Wie führe ich den SIL-Nachweis wenn ich einen E-Motor in der SIL-Kette abschalten muss?

Wie üblich durch Kalkulation mit Werten der Komponenten im Sicherheitskreis die für die Abschaltung nötig sind.

30. Wie geht man mit Systemen um, die Energie brauchen um die Schutzfunktion auszuführen? Zum Beispiel eine Reaktorkühlung. Eine PFD-Berechnung von Sensor, Logic Solver und Final Element sagt noch nichts aus.

Hier muss die Zuverlässigkeit der Energieversorgung mitbetrachtet werden (wie groß ist die PFD der Energiequelle?). Das Zuverlässigkeitsblockschaltbild wird entsprechend komplexer. Schutz kann durch Redundanz und zusätzliche Einrichtungen (z. B. Energiespeicher) hergestellt werden.
Die folgenden Aussagen wurden maßgeblich von Herrn Strobl, TÜV Süd Industrie Service, gemacht.

31. Zusatzblatt Frage 1: Muss ich eine bestehende Anlage (2002) auf SIL umrüsten oder habe ich Bestandsschutz falls ich im Anlagenteil nichts verändere?

Bestandsschutz kann nicht garantiert werden. NE126 gibt aber Empfehlung. Gericht wägt ab zwischen Interessen von Betreiber und Geschädigtem.
VDE 0100 (Elektroinstallation): unveränderte Anlage hat Bestandsschutz.
Störfall- und Betriebssicherheitsverordnung: Abnahme vom TÜV. Dieser wird nicht ohne Grund das Abschalten der Anlage anordnen. Wenn aber eine Änderung in der grundlegenden Sichtweise eine Überprüfung der nötigen risikoreduzierenden Einrichtungen erforderlich macht, wird ggf. ein Hinweis zur Nachrüstung gegeben bzw. eine überarbeitete Gefährdungs- und Risikoanalyse eingefordert.

32. Zusatzblatt Frage 2: Warum werden Sicherheitseinrichtungen gegen Drucküberschreitung nach AD 2000-A6 in der Praxis so gut wie immer redundant ausgeführt? Laut Merkblatt wären auch andere Ausführungen denkbar.

Eine Möglichkeit ist die Verwendung von Sicherheitsdruckventilen. (Nachteil: nicht überwachbar, Auslösen ohne Vorankündigung). Ein getrennter Sicherheitskreis wird laut Blatt aber nie über die probabilistische Betrachtung qualifiziert bzw. entworfen. Dies ist aber trotzdem möglich, speziell bei Prozessen, bei denen keine Stofffreisetzung in die Umgebung stattfinden darf. Wird keine Ausfallwahrscheinlichkeitsberechnung durchgeführt, muss redundant bzw. fehlersicher ausgelegt werden. Regelkreisgeräte dürfen hier einbezogen werden.

5. SIL-Sprechstunde 2013

1. In welchem Umfang bestehen für den Profibus PA Einschränkungen hinsichtlich der Funktionalen Sicherheit?

2. Reicht bei einem Liquiphant (FTL71 mit FEL 58) die Betätigung des Testtasters als "Erstmalige Prüfung vor Inbetriebnahme" aus oder muss die Schaltung zwingend mit Produkt ausgelöst werden?

3. Kann ich mit drei SIL2-Transmittern (in 2v3 Verschaltung) in Summe SIL3 erreichen? Der PFDavg für SIL3 wird erreicht.

4. Kann ich mit zwei SIL2-Ventilen (in1v2 Verschaltung) in Summe SIL3 erreichen? Der PFDavg für SIL3 wird erreicht.

5. Ist ein eigenes Sicherheits-Managementsystem erforderlich, wenn eine Firma als Dienstleister Schutzeinrichtungen für einen Kunden bearbeitet?

6. Ist ein Zeitraum von sechs Jahren für die "Wiederkehrende Prüfung" möglich? Nach VDI/VDE 2180 sollte die Prüffrist ein Jahr betragen, es sollen aber auch längere Fristen möglich sein.

7. Wie kann die Zuverlässigkeit mechanischer Komponenten ermittelt werden und welche Normen können hierzu angewendet werden?

8. Ist es sinnvoll für einen Filterregulator eine SIL-Beurteilung durchzuführen?

9. Macht es Sinn für einen Entlüfter/Schalldämpfer eine SIL-Beurteilung durchzuführen? Schließlich ist in vielen Anlagen das Entlüften eines Antriebs eine Sicherheitsfunktion.

10. Ist es vertretbar mit Hilfe einer FMEDA Software Fehlerraten zu ermitteln und anhand dieser Werte eine Selbstzertifizierung durchzuführen?

11. Besteht die Möglichkeit ein Neuprodukt als Typ A einzustufen, wenn durch aussagekräftige Versuche das Ausfall- und Fehlerverhalten ausreichend bestimmt ist?

12. Welche Möglichkeiten bestehen, die im SIL-Zertifikat angegebene Verwendungsdauer eines Produktes zu verlängern?

13. Wie kann aus Sicht des Produktherstellers Betriebsbewährtheit nachgewiesen werden und welche Normen sind hierzu anwendbar?

14. Welche Hauptunterschiede bestehen zwischen IEC 61508 und ISO 26262?

15. Wie funktioniert die Umsetzung SIL auf der Energieseite? Sensorseite und Verarbeitung bei M&R scheint mir in unserem Betrieb geklärt. Doch dann kommt der Übergabepunkt im Rangierverteiler zur Energieseite bis zum E-Motor z.B. ...

16. Wie werden die SIL-Anforderungen auf der Energieseite (z.B. Abschaltung Motor) richtig umgesetzt? Auf der Seite Schaltanlagenhersteller ist das Thema unbekannt oder wird sehr ausweichend beantwortet. Zertifizierte Mittel- oder Niederspannungsschaltanlagen sind mir nicht bekannt.

17. In EN ISO 13849-1:2006 lese ich: 6.2.4 Kategorie 1 Für Kategorie 1 müssen die gleichen Anforderungen erfüllt sein wie diese nach 6.2.3 für Kategorie B. Zusätzlich gilt Folgendes. SRP/CS der Kategorie 1 müssen unter Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien gestaltet und gebaut werden (siehe ISO 13849-2). Ein bewährtes Bauteil für eine sicherheitsbezogene Anwendung ist ein Bauteil, das entweder: a) in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet worden ist, oder b) unter Anwendung von Prinzipien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen zeigen. Neu entwickelte Bauteile und Sicherheitsprinzipien können als gleichwertig bewährt betrachtet werden, wenn sie die in b) genannten Bedingungen erfüllen. Die Entscheidung, ein bestimmtes Bauteil als bewährt zu akzeptieren, hängt von der Anwendung ab. ANMERKUNG 1 Komplexe elektronische Bauteile (z. B. PLC, Mikroprozessor, anwendungsspezifische integrierte Schaltung) können nicht als gleichwertig zu bewährt betrachtet werden.“ Folgt daraus, dass Geräte der Kategorie 1 (entsprechend SIL 1) grundsätzlich keinen Prozessor enthalten dürfen, so dass jede Art von SPS hier unzulässig ist? Die höheren Kategorien referenzieren nur die „bewährten Sicherheitsprinzipien“, nicht die „bewährten Bauteile“. Heißt das, dass man in diesen Kategorien dann Prozessoren einsetzen kann?

18. Es sei angenommen, dass ein Regler eine sicherheitsrelevante Prozessgröße regelt. Bei einem Ausfall des Reglers könnte es daher zu einer gefährlichen Situation kommen. Somit wäre die Sicherheitsfunktion permanent gefordert, der Regler allein hätte also eine sehr hohe Sicherheitsanforderungshäufigkeit. Ist es das übliche Vorgehen, in diesem Fall eine Überwachung der Prozessgröße mit anderen Mitteln parallel zum Regler vorzusehen, die einfach aufgebaut sind? Diese Überwachung würde nur bei Ausfall des Reglers angefordert werden, also selten. Damit wären die Anforderungen an diese Einrichtung deutlich geringer. Für die Gesamtbetrachtung müsste sowohl die Ausfallwahrscheinlichkeit des Reglers als auch die der Überwachung evaluiert werden, da die Wahrscheinlichkeit der Anforderung der Sicherheitsfunktion vom Ausfall des Reglers abhängt. Wie ist das übliche Vorgehen, wenn die zu überwachende Prozessgröße nicht mit einfachen Mitteln anderweitig zu erfassen ist?

19. Bei meinem Problem geht es um das V-Modell im Software Lebenszyklus. Viele Firmen nutzen in Ihrer Software-Entwicklungsabteilung seit Jahren agile Methoden wie z.B. Scrum. In der Softwarebranche ist Scrum eines der am meisten verbreiteten Vorgehensmodelle. Für die Entwicklung von safety critical systems nach der IEC 61508 gab es in den letzten Jahren immer wieder Ansätze, agile Methoden wie Scrum (SafeScrum) statt des V-Modells zu nutzen. Auf der ICSEA 2012 hat Siemens ein Modell (Safety-oriented Scrum) vorgestellt, das Scrum an den safety lifecycle anpasst und gibt an, dass Sie dieses Modell zur Entwicklung von SIL Produkten nutzen wollen. Frage: Kann das Modell von Siemens oder ein anderes (SafeScrum) tatsächlich als alternative zum V-Modell verwendet werden?

Themen:

1.) Es gibt noch keine Geräte mit ProfiSafe-Stack für Profibus PA. NE97 würde aber beschreiben wie Topologien und Feldgeräte für diesen Fall aussehen müssten. Der Stack hätte SIL 3-Qualität.
Es ist zu beachten dass die IEC 62443 zur IT-Sicherheit eine physikalische Trennung von Bussystemen für Safety und Non-Safety fordert.
Das ProfiSafe-Protokoll geht nur über Profibus PA und ProfiNet. Für Profibus DP gibt es Safety Data Write.
2.) Eine Prüfung bei Inbetriebnahme sollte immer mit Produkt erfolgen. Um eine echte Validierung zu erreichen ist z.B. die Einbaulänge auf diese Weise zu prüfen. Der Taster ist ein gutes Mittel zur Prüfung des Sicherheitskreises, zusätzlich wird nur der Ausgang der Geräte geprüft.
3. + 4.) Entweder diversitär redundant oder für SIL 3 geeignet (systematic capability). Betriebsbewährung kann ebenfalls genutzt werden.
5.) Wenn er in das FSM des Endkunden eingebunden ist: ja. Üblicherweise gibt der Endkunde Strukturen für Abläufe und Dokumentation vor, demzufolge muß der Dienstleister auch wissen wie er mit diesem Teil der Unterlagen umgeht. FSMSystem wird von versch. Dienstleistern angeboten. VDI 2180 Bl. 2 Pt. 2.1 fordert das. Schween: Identifizieren der Teile der Norm die für Sie relevant sind und Nachweisen der Erfüllung. Muß Teil des QM-Systems sein.
6.) Die Probabilistik erlaubt Berechnung und individuell auf die Anwendung zugeschnittene Festlegung. Nicht vergessen: es könnte Notwendigkeiten aus systematischen Fehlerquellen geben, z.B. Verkleben eines Ventils wegen Medieneigenschaften. Ausnahme: EN 50156, dort 1 Jahr.
7.) NE142 / EN 50156 / ISO 13849 Teile 1 und 2 / EN 61508 kennt auch Fehlerausschluß (‚Begriff Unterlastung') / Weibull-Verteilung für Geräte mit B10d-Werten von Dr. Hildebrandt. Achtung: für mechanische Komponenten ist ein einfaches Umrechnen von High-Demand auf Low-Demand Mode nicht zulässig (wer rastet der rostet)
8. + 9.) Bezieht sich die Frage auf einen Druckminderer mit Filter? Der Druck wird mechanisch eingestellt. Beispiel Blitzableiter – dieser muß nicht betrachtet werden.
2/3 27.09.2013
Hildebrandt Andreas
Es ist schwierig für manche Teile eine SIL-Bewertung zu machen wegen fehlender Ausfallraten. Anteil der Aktoren an Fehlern ist üblicherweise höher als die 50% - da systematische Fehler überwiegen. Schrörs: es gibt keine SIL-Geräte. EN 61511 zur Betrachtung der systematischen Fehler heranzuziehen ist nicht falsch (FSM, …). Generische Werte wie z.B. 400 FIT für die Bewertung von Ventilen heranzuziehen ist in erster Näherung nicht falsch. Max. SIL 2 für ein Ventil. Für den Betreiber ist es gut, vom Anlagenplaner ein Safety Manual zu bekommen.
10.) Es geht um FMEDA-Tools. Es sollte ein FMEDA vorgelegt werden, nicht nur Fehlerraten. Ein FMEDA betrachtet aber auch keine systematischen Fehler. Schrörs: Für FMEDA ist eine unabhängige Abteilung nötig, nicht getrieben von der GL. Achtung: FMEA für Anlagen nötig, um systematische Fehler auszuschließen.
11.) Laut 61508 ist Betriebsbewährung nachzuweisen – dann könnte man Typ A vermuten. Programmierbare Elektronik Typ B: Ventiltreiber ist hier Ausnahme und kann als Typ A bezeichnet werden.
12.) Lebensdauer: eine Lebensdauer anzugeben ärgert den Betreiber. Der Betreiber möchte das selbst tun. Schrörs: es gibt Möglichkeiten, die Elektronik zu bewerten und die Geräte weiter zu betreiben. Es gibt Hersteller die Fehlermöglichkeiten angeben die die Lebenszeit limitieren. Die Laufzeit eines Zertifikates ist dabei nicht

maßgeblich – das Zertifikat gilt auch nach Ablaufen trotzdem für das gekaufte Gerät weiter. Bei Neubewertung der Anlage kann der Normenstand in Frage gestellt werden.
13.) Route 2H wird verwendet. Betriebsbewährung je nach Medienberührung schwieriger oder weniger schwierig zu benutzen. Emerson gibt für Geräte mit Medienberührung Beispielanwendungen an. Zusätzlich IEC 60300-3-2 / ISO 14224.
14.) ASIL statt SIL. Klarer definierte Dokumentation. Beschreibt QM-System genauer. Rieger TÜV Nord.
15. + 16.) ETT (energize-to-trip) / D-ETT (de-ETT) sind wichtig. Schween: Publikationen von Versorgern erhältlich, die Ausfallverhalten ihrer Netze angeben. Auf konkrete Konstellationen sollte Bezug genommen werden (evtl. werden redundante Netze aus einer einzelnen nächsthöheren Spannungsschiene versorgt, Redundanz nicht mehr gegeben).
17.) Nein. Aus b) ergibt sich, dass ein nach IEC 61508 zugelassenes Gerät durchaus hier eingeordnet werden könnte. Es wird ggf. bei Prozessoren eine Betriebsbewährungsangabe von Herstellern angefragt um hier weiterzukommen.
18.) Es gibt keine sicherheitsgerichteten Regler als Betriebseinrichtung. Für die ausfallenden Regler wird eine Schutzeinrichtung zusätzlich installiert. Regler wird öfter für Sicherheit verwendet (Beispiel: Füllstandssensor gibt Füllstand weiter und das Erreichen eines Limits). Die Überwachung ist die Schutzeinrichtung. ‚Ausfall des Reglers' bedeutet dass die Steuerung ausfällt. In der LOPA fällt dann ein ‚Layer of Protection' direkt weg: der Kredit auf den Regler die gleichzeitig die Sicherheitsfunktion darstellt entfällt. Ich benötige einen weiteren Layer.
Die ersten zwei Sätze beschreiben es: ich benötige genau dafür eine Schutzeinrichtung.
19.) V-Modell ist eine Möglichkeit, einen Software-Lebenszyklus abzubilden. Man darf das aber auch durch andere angemessene Methoden ersetzen.

6. SIL-Sprechstunde 2014

Rot = Organisatorische Maßnahmen, Regelwerke
Grün = Technische Realisierung
Blau = Sonderfälle, gängige Praxis, Grauzonen

1. Ist ein ISO 9001:2008 QM System ausreichen, um SIL2/3-Produkte im Dienstleistungsauftrag produzieren zu können? Falls nicht, welche spezifische Zertifizierung wird von einem EMS Dienstleister erwartet

Antwort:
Man sollte zwei Fälle unterscheiden, die bei der Vertragsgestaltung genau unterschieden werden sollten:
a. Reiner Fertigungsauftrag, bei dem durch den Auftragnehmer keinerlei eigene Entwicklungstätigkeiten durchgeführt werden und auch keine Testprozeduren entwickelt werden („verlängerte Werkbank“). Der Auftragnehmer muss nur in der Lage sein einen Fertigungsauftrag entsprechend der Spezifikation in der georderten Qualität durchzuführen. Eine ISO9001:2008 ist ausreichend.
b. Ein Funktionsgeschäft, bei dem der Auftragnehmer eigenständig Entwicklungsarbeiten übernimmt und sicherstellen muss, dass die Produkte der IEC61508 / IEC61511 entsprechen. In diesem Fall muss der Auftragnehmer die Anforderungen an Personal und Vorgehensweisen der genannten Standards erfüllen. Dies kann z.B. durch ein Audit nachgewiesen werden. Eine Zertifizierung nach IEC 61508 / IEC 61511 ist nicht notwendig.
Der Auftraggeber stellt ein Auftragspaket für den potentiellen Auftragnehmer zusammen, in dem er den durchzuführenden Auftrag konkret benennt. Der Auftragnehmer muss in seinem QM-System Prozeduren festgelegt haben, aus denen es hervorgeht, dass er den entsprechenden Auftrag gemäß den formulierten, konkreten Aufgaben, erledigen kann. Falls nicht, sollte er fairerweise dem Auftraggeber mitteilen, dass er den Auftrag nicht wunschgemäß erledigen kann. Möglich wäre auch, daqss der Auftraggeber den Auftragnehmer bezüglich des FSM im QM-System auditiert. Dabei sollte ein separater Punkt zum FSM im QM-System zu finden sein. Wichtig ist, dass die Rollen und Verantwortlichkeiten klar definiert werden.

2. Gibt es die SIL-Klassifizierung auch in englischer und spanischer Sprache?

Antwort:
Die SIL-Klassifizierung hat ihren Ursprung in der IEC 61508 / IEC 61511. Die Sprachen der IEC Regelwerke sind Englisch und Französisch (Englisch ist die Arbeitssprache). Sofern lokale Ausprägungen der Standards vorliegen sind diese oft in die jeweilige Landessprache übersetzt. Bei der Frage geht es wahrscheinlich darum, ob das Regelwerk auch ins spanische übersetz ist. Die Frage konnte nicht mit Gewissheit geklärt werden. Die Vermutung geht in Richtung: JA.

3. Nach wie vor herrscht bei den Betreibern von Anlagen große Unsicherheit, wenn es um Ex-Anforderungen mit Hilfe von SIL Einrichtungen geht:

a. Wann kommt die TRBS 2152-5?
b. Wird sie der vereinfachten Logik: „eine SIL-Stufe entspricht einer Reduzierung um eine Ex-Zone“ widersprechen?
lkjhjklkjhlkjh

c. Wird auch in der TRBS 2152-5 die Rede von Zonenreduzierung und Zündquellenüberwachung sein?
d. Wie ist eine UEG Ex Raumüberwachung einzustufen?
Antwort:

a. Die TRBS 2152-5 wird in 2015 erscheinen. Angestrebt wird, dass sie zusammen mit dem Inkrafttreten der neuen Betriebssicherheitsverordnung erscheint. Die VDI/VDE 2180 Blatt 6 sowie die Namur-Empfehlung NE 138 sind bereits verfügbar und behandeln das Thema aus praxisnaher Perspektive (man findet dort u. a. Applikationsbeispiele)
b. Tabelle 2 der VDI/VDE 2180 Blatt 6 legt diesen Ansatz nahe. Mit dieser Methode kann z. B. erreicht werden, dass ein Analyse-Geräteraum keine Ex-Zone ist, wenn die technische Lüftung entsprechend „sicher“ ist.
c. Ja, zur Zeit ist geplant, die Begriffe beizubehalten.
d. Eine UEG-Ex-Raumüberwachung ist eine ereignisverhindernde Schutzeinrichtung

4. Mein System soll die Kat. 3 PL "d" erfüllen. a. Bin ich hierbei an die vorgesehene zweikanalige Struktur nach Kat. 3 gebunden? b. Kann ich mit einer einkanaligen Struktur und einem Fehlerausschlussverfahren (FMEA) auch die Kat.3 PL "d" erreichen?

Antwort:
a. Ja, die vorgegebene Architektur der Iso 13849-1 für Kat. 3 ist einzuhalten. Es ist aber auch mit Kat. 2 möglich, Performancelevel „d“ zu erreichen.
b. Abweichung von der vorgegebenen Architektur müsste genau definiert und begründet werden. Ein Fehlerausschluss ist denkbar, muss aber sehr gut begründet werden. Beispielsweise muss nachgewiesen werden, dass es keine gefährlichen Fehler gibt oder diese zu nahezu 100% aufgedeckt würden.

5. Betriebsbewährung von Geräten a. Welche Geräte brauchen eine Betriebsbewährung – Sensoren, Logikteil und/ oder Aktoren? b. Wo (genau) ist das in der Norm nach zu lesen? c. Betriebsbewährung vom Hersteller und/oder vom Anwender? d. Wie wird die Betriebsbewährung nachgewiesen, formlos?

Antwort:
a. Geräte können betriebsbewährt sein, müssen es aber nicht zwangsläufig. Der große Vorteil der Betriebsbewährung insbesondere für Feldgeräte liegt in der nachgewiesen Eignung eines Gerätes für eine bestimmte Applikation oder Umgebungsbedingungen.
b. IEC 61508: 7.4.10 Anforderungen an betriebsbewährte Elemente, IEC 61511: 11.5.3 Anforderungen an die Auswahl von Komponenten und Teilsystemen auf Basis einer früheren Verwendung, VDI/VDE 210 Kap.2.2.2: „Alle Komponenten von Schutzeinrichtungen müssen einen SIL-Nachweis haben, baumustergeprüft oder betriebsbewährt sein“.
c. Ziel einer Betriebsbewährung eines Gerätes ist der Ausschluss möglichst vieler systematischer Fehler in einem Gerät bzw. beim Einsatz dieses Gerätes. Der Gerätehersteller kann einen erheblichen Beitrag zum Minimieren bzw. Ausschließen systematischer Fehler im Rahmen der Entwicklung und Herstellung leisten, indem er seine Produktion nach einem internem QM betreibt sowie bereits bewährte Gerätekomponenten oder Messverfahren z.B. Bauelemente erst dann einsetzen, wenn sie mindestens 1 Jahr erfolgreich am Markt platziert sind, verwendet. Der Nachweis einer grundsätzlichen Eignung für eine Anwendung des Gerätes in der Prozessindustrie liegt durch alleinige Erklärung des Herstellers in der Regel noch nicht vor. Der endgültige Betriebsbewährungsnachweis kann prozessspezifisch nur vom Betreiber bestätigt werden, indem er alle umgebungsbedingten Einflüsse für die Anwendung berücksichtigt. Der Anwender prüft die vom Hersteller des Gerätes angegebenen Spezifikationen der grundsätzlichen Anwendung auf Übereinstimmung mit seinen, speziellen, einmaligen Umgebungsbedingungen.
Die NAMUR Empfehlung NE130 „Betriebsbewährte Geräte für PLTSchutzeinrichtungen“ beschreibt dazu ein geeignetes Anwendungsmodell.
d. Jede Entscheidung ein Gerät als „betriebsbewährt“ zu bezeichnen muss

nachvollziehbar begründet und dokumentiert werden. In der VDI/VDE 2180 Bl.5 Kap.8 sind Beispiele dafür, wie eine Erklärung der Betriebsbewährung von PLTSchutzeinrichtungenkomponenten sowohl durch den Hersteller wie auch durch den Betreiber dokumentiert werden kann. Ebenso finden sich Formblätter in der NAMUR Empfehlung 130 „Betriebsbewährte Geräte für PLTSchutzeinrichtungen“.

6. Muss man bei einem SIL-Kreis mit einem Sensor, der 10 Aktoren abschaltet in der PFD-Nachweisrechnung für den Ausgang mit einer 10oo10 Funktion rechnen oder erstellt man 10 einzelne Berechnungen mit jeweils einem Sensor, der auf einen Aktor geht? Bsp: Überfüllsicherung an einem Behälter mit 10 Zulaufleitungen.

Antwort:
Es kommt auf die Sicherheitsfunktion an. Genauer gesagt kommt es darauf an, welches Ausgangsrisiko reduziert werden soll. Ist das Ausgangsrisiko, dass alle 10 Zuläufe gleichzeitig in geöffneter Stellung hängen bleiben, dann muss bei der Sicherheitsfunktion aktorseitig mit 10oo10 gerechnet werden. Ist das Ausgangsrisiko, dass einer der 10 Zuläufe nicht schließt, dann wird aktorseitig nur mit 1oo1 gerechnet.

7. Welchen Stellenwert hat der rechnerische Nachweis? Unter welchen Voraussetzungen können die Anforderungen der Norm auch ohne rechnerischen Nachweis erfüllt werden?

Antwort:
Der rechnerische Nachweis der Ausfallwahrscheinlichkeit einer Schutzeinrichtung dient neben andern Kriterien (z.B. Hardware Fehler Toleranz, ...) zum Nachweis der sicherheitstechnischen Hardwarezuverlässigkeit einer PLT-Schutzeinrichtung und bezieht sich ausschließlich auf unentdeckte, zufällige, gefährliche Hardwarefehler. Zum Nachweis der Eignung einer PLT-Schutzeinrichtung für einen spezifischen SIL ist jedoch deutlich mehr notwendig. Unberücksichtigt bei der Berechnung sind systematische Fehler, die einen deutlich größeren Einfluss auf die Schutzeinrichtung haben als zufällige Hardwarefehler. Dazu gehören z.B. die richtige Auswahl und Auslegung von Geräten, eine vollständige und widerspruchsfreie Spezifikation, fehlerfreie Programmierung, Einflüsse durch Umgebungsbedingungen, usw. Eine Berechnung allein ist nicht ausreichend um die Erfüllung der Anforderungen an einen bestimmten SIL nachzuweisen. Sollten keine Zuverlässigkeitskenndaten einzelner Geräte vorliegen, muss nachgewiesen werden, dass das Auftreten eines Fehlers in diesem System hinreichend unwahrscheinlich ist. Dies kann z.B. durch eine FMEDA erfolgen. Durch den rechnerischen Nachweis werden ca. 15% der erforderlichen Bedingungen für den Einsatz einer PLT-Einrichtung als PLTSchutzeinrichtung, erreicht. Viele bedeutende Einzelheiten werden von der Rechnung nicht erfasst, die aber großen Einfluss auf die SIL-Eignung haben, z.B. Einfluss der Umgebungsbedingungen, Medienberührung etc.
Eine gute, erschöpfende und genaue verbale Beschreibung ist einem rechnerischem Nachweis gleich zu stellen.

8. Die AD-Merkblätter AD2000 A6 und A403 stellen Anforderungen für MSRSchutzeinrichtungen an Druckgeräten zum Erkennen und Begrenzen von Druck und Temperatur. Wie gehen die Betreiber vor? Nach AD2000 oder risikobasiert (Funktionale Sicherheit)?

Antwort:
Das AD-Merkblatt A6 definiert technische Anforderungen, die für eine sichere Funktion notwendig sind, ohne auf eine Ausführung nach SIL (risikobasiert) zu verweisen. Durch eine Risikoanalyse kann der notwendige SIL identifiziert werden und daraus ebenfalls technische Mindestanforderungen abgeleitet werden. Ziel der Betrachtung ist eine zu jeder Zeit sichere Anlage zu betreiben. Somit ist der gewählte Weg, d.h. nach AD oder

risikobasiert, so genau wie möglich zu beschreiben und zu dokumentieren. Genaue Dokumentation räumt im Falle eines „Problems“ den Verdacht einer fahrlässigen Handlung aus.

9. In der Praxis begegnen mir immer wieder Überfüllabsicherungen mit einer „Z“-Kennzeichnung. Eine typische Bezeichnung wäre: L- 4711 /A+(Z+)/_/_/ (Alarmierung und Z im PLS) a. Welche Regelwerke und Vorschriften müssen bezüglich des „Z“ beachtet werden? b. Ist so eine Überfüllsicherung vergleichbar mit einer SIL-Schutzeinrichtung?

Antwort:
Mit „Z“ werden typischerweise PLT-Schutzeinrichtungen gekennzeichnet, die als Ergebnis einer Risikobetrachtung zur notwendigen Risikominderung implementiert werden müssen. PLT-Schutzeinrichtungen müssen z.B. entsprechend den Anforderungen der IEC 61511 gebaut und errichtet werden. Dies kann auch eine Überfüllsicherung sein. Überfüllsicherungen nach dem WhG sind typischerweise keine PLT-Schutzeinrichtungen, werden somit also auch nicht mit „Z“ gekennzeichnet und unterliegen den Anforderungen des WhG. Gemäß der VDI/VDE 2180 Bl.3, Kap.2.2.7 gilt: „Bei Sensoren ohne Schaltfunktion sind sicherheitsrelevante Meldungen durch „Z in Klammern“ zu kennzeichnen, z. B. QR(Z)A+“. Weiterhin gilt: „Bei PLT-Schutzeinrichtungen ist eine Kennzeichnung der Stellgerätefunktion erforderlich. Diese erfolgt ebenfalls durch „Z in Klammern“, z. B. UV(Z)“. Diese zwei Aspekte regeln aber nicht, ob die Signale in eine separate Sicherheitskette oder über das PLS laufen. Weiterhin ist es nicht geregelt, wie das Wartungspersonal vor Ort die PLT-Einrichtungen mit Z in Klammern von denen ohne Klammern unterscheidet und behandelt. Um eine abschließende Antwort auf die Frage zu geben, fehlen die o.g. Informationen.

10. Welche Kriterien müssen für ein Gerät erfüllt sein, um in einem SIL-Kreis eingesetzt werden zu können?

a. Welche Norm 61508/61511 ist für das jeweilige Gerät anzuwenden?
b. Wann ist ein Zertifikat durch ein externes Prüfunternehmen zwingend erforderlich,
c. Wann reicht eine Bescheinigung des Herstellers?
Antwort:
a. Geräte können entweder nach IEC 61508 entwickelt worden sein oder eine Betriebsbewährung nach IEC 61511 haben. IEC 61508 regelt die Pflichten des Herstellers bei der Entwicklung von Geräten, die IEC 61511 regelt die Pflichten des Betreibers vor und während des Betreibens von Geräten.
b. Ein Zertifikat ist niemals erforderlich. Ein bloßes Zertifikat ist für sich alleine nie erforderlich, egal von wem geprüft.
c. Eine Bescheinigung des Herstellers sagt lediglich aus, dass dieses Gerät mit hinreichender Wahrscheinlichkeit von systematischen Fehlern „frei“ ist und einen SIL-Kreis bis zum SIL X möglicherweise (IEC 61508-4, Kap.3.5.8 Anm.3) unterstützen kann. Eine Bescheinigung des Herstellers kann zur Feststellung der Betriebsbewährung bis SIL 2 hilfreich und/oder ergänzend wirken. Ab SIL 3 ist eine Bewertung einer „unabhängigen Organisation“ erforderlich.

11. Frage zum Bestandsschutz: Wie sind folgende Varianten zu behandeln: a. SSPS bleibt bestehen, Nachrüstung einer zusätzlichen Sicherheitsfunktion (ggf. mit zusätzlichen Sensoren) ohne Änderung vorhandener SIF: i. Muss nur für diese neue SIF Risikoanalyse und SIL-Nachweis (incl. aktuelles Zertifikat für SSPS) erbracht werden oder auch für alle vorhandenen SIF? ii. Wie können vorhandene Sensoren und Aktoren bewertet werden, die oft älter als 10 Jahre sind? iii. Falls für SSPS kein aktuelles Zertifikat vorliegt, darf keine zusätzliche SIF nachgerüstet werden? <-> Weiterbetrieb ohne Verbesserungen wäre aber möglich!? b. Ersatz einer VPS oder einer alten SSPS durch eine neue SSPS mit SIL3-Zulassung, Risiko unverändert, Sicherheitsfunktionen unverändert, Feld unverändert: i. keine neue Risikoanalyse + kein SIL-Nachweis erforderlich, vgl. NE126 (2009)? c. Ersatz einer VPS oder einer alten SSPS durch eine neue SSPS mit SIL3-Nachrüstung einer zusätzlichen Sicherheitsfunktion ohne Änderung vorhandener SIF: i. Muss nur für diese neue SIF Risikoanalyse und SIL-Nachweis erbracht werden oder auch für alle vorhandenen SIF?

Antwort:
Grundsätzlich ist anzumerken, dass es keinen Bestandsschutz gibt. Dies heißt jedoch nicht, dass immer eine Nachrüstpflicht besteht. Vielmehr kommt es auf das Ergebnis einer Gefährdungsbeurteilung an, ob eine Nachrüstung erforderlich ist oder nicht. Ist das Ergebnis der Gefährdungsbeurteilung, dass etwas nach heutigem Kenntnisstand immer noch sicher ist, dann besteht in der Regel kein Nachrüstbedarf (Ausnahmen sind gesetzliche Vorgaben). Grund für die nicht nötige Nachrüstung ist aber nicht der Bestandsschutz (denn den gibt es nicht), sondern die Tatsache, dass die „Sache" nach wie vor sicher ist.
Zu a), i.
Nach NE 126 müssen die bestehenden SIFs nicht nach SIL neu bewertet werden. Üblicherweise wird in einem solchen Fall von einem Team entschieden, ob alle SIFs bewertet werden oder nur die neu hinzugekommene. Wichtig ist auf jeden Fall, die Schnittstelle genau zu beschreiben um die neue SIF gegenüber den vorhandenen genau abzugrenzen.
Zu a), ii.
Es wird keine Rechnung durchgeführt, aber es wird die maximale Gebrauchsdauer kritisch hinterfragt. Hierzu werden betriebliche Erfahrungen und – falls vorhanden – andere Informationsquellen herangezogen.
Zu a), iii.
Eine weitere SIF darf nachgerüstet werden, wenn damit eine Erhöhung der Sicherheit einhergeht und durch die Nachrüstung neue Risiken bzw. Fehlerquellen an anderer Stelle ausgeschlossen werden können.
Zu b), i.
Hardwaretechnisch kein Problem, aber die SW-Entwicklung ist nach EN 61511 durchzuführen (incl. Verifikation nach dem 4-Augenprinzip)
Zu c), i.
siehe Antworten a) und b) (sinngemäß bereits beantwortete)

12. SIL-Betrachtung bei Erweiterungen von Bestandsanlagen! a. Was muss beachtet werden, wenn Anlagen erweitert werden und sich daraus Änderungen bei bereits bestehenden Sicherheitsfunktionen ergeben? i. Z. B. soll ein Aktor zusätzlich durch einen Drucksensor abgeschaltet werden. Der Aktor ist bereits seit 10 Jahren Teil einer Sicherheitseinrichtung, d.h. die Auslegung erfolgte nicht nach SIL (IEC 61508 bzw. IEC 61511). ii. Wie könnte hier der erforderliche SIL-Nachweis aussehen? iii. Ist es ausreichend die Eignung der neuverbauten Komponenten (Sensorkreis) nachzuweisen und bei den bereits Bestehenden auf „betriebsbewährt“ zu argumentieren? (jährliche Funktionsprüfungen wurden durchgeführt und dokumentiert) b. Können für diese Erweiterungen bestehende Komponenten genutzt werden, die nicht nach IEC 61508 entwickelt wurden, wie beispielsweise der zweiter Kanal einer Grenzwertkarte oder bei hartverdrahteten Systemen weitere Eingänge von Logikbaugruppen? c. Kann der Bestandsschutz bei einem Austausch der Sicherheitssteuerung geltend gemacht werden? Was ist hier zu beachten?

Antwort:
Zu a), i.
Der Aktor wird bewertet hinsichtlich seiner Gebrauchsdauer. Ist der Aktor nach wie vor brauchbar, dann wird die geplante Änderung durchgeführt und alles (auch die Bewertung des Aktors) wird dokumentiert.
Zu a), ii.
Ein SIL-Nachweis ist in solchen Fällen oft nicht möglich (und auch nicht erforderlich)
Zu a), iii.
ja
Zu b).
ja
Zu c)
Zum Bestandsschutz siehe Frage 11. Wenn die Funktion nicht geändert wird und die Sicherheit nicht verschlechtert wird (neue Steuerung ist mindestens so gut wie die alte Steuerung), ist keine Neubewertung nötig. Falls die Software jedoch neu geschrieben werden muss (oder umgeschrieben werden muss), so ist dabei die EN 61511 zu beachten (incl. Verifikation nach dem 4-Augen Prinzip)

13. Bei komplexen Steuerungen (dreifach-redundante SSPS) ist es schwierig den Wert für die PFD aus den Einzelwerten der Komponenten mit einfachen Mitteln zu bestimmen. In einer mir vorliegenden SIL-Betrachtung wird deshalb bei Verwendung eines HIMatrix-Systems folgender Ansatz gemacht. Zitat "*IEC 61508-1 legt für SIL3 einen PFD von 10 hoch -4 ..... 10 hoch -3 pro Stunde fest. Für die Steuerung (PES) werden 15% des Grenzwertes für PFD angenommen. Damit ergeben Sich als Grenzwert für den Anteil der Steuerung PFD = 1,5 * 10 hoch -4 pro Stunde.*" Weiterhin wird angegeben, dass die HIMatrix in allen Kombinationen die im Zitat genannten Bedingungen bei einem Testinterwall von 10 Jahren erfüllt. Da der Nachweis lediglich für eine SIL2 Applikation zu führen war, gab es mit dem Wert PFD = 1,5 * 10 hoch -4 für die Steuerung kein Problem. Ist das praktikabel?

Antwort:
Die PFD-Werte der einzelnen Komponente werden von HIMA gestellt und werden vom Anwender eingesetzt. Je nach Anwendung müssen diese Werte dann addiert werden. Näherungsweise werden die PFD-Werte aller Komponenten addiert auch wenn es sich um 1oo2-Komponenten handelt, um die Rechnung einfach zu halten. Andernfalls müssen bei mehrkanaligen Geräten die einzelnen Lambda-Werte bekannt sein. Dies würde zu einer komplexeren Rechnung führen. Es können ggf. auch typische Konstellationen von

Komponenten im Voraus berechnet werden. Unter Berücksichtigung der Voraussetzungen dieser Berechnung kann dann mit diesen typischen Konstellationen ohne Berechnung weiterhin gearbeitet werden.

14. Wie ist mit der Herstellervorgabe "Die EX-Pumpe darf nicht Trockelaufen" bei Batchanlagen umzugehen? Hier ist ein kurzeitiges Trocklaufen (30 s) beim An- und Abfahren oft nicht zu vermeiden.

Antwort:
Man führt eine Risikobeurteilung durch unter Berücksichtigung von Herstellerangaben durch und Begrenzt die Trockenlaufzeit auf unkritische Werte. Die Zeitbegrenzung ist als Schutzfunktion (SIL) auszuführen. Folgende Fragen sollen zusammen mit dem Hersteller geklärt werden: Warum darf die Pumpe nicht trocken laufen? Gilt das Verbot auch für kurzzeitiges Trockenlaufen? Was versteht der Hersteller unter „Trockenlaufen"? (Wenn unmittelbar vor dem „Trockenlauf" Flüssigkeit gefördert wurde, sind die Dichtungen ja evtl noch benetzt). Wichtig ist, Gründe für derartige Einschränkungen zu ermitteln und deren Relevanz für die betreffende Situation zu bewerten. Dokumentation!!!

15. Vergleichbarkeit von SIL-Zertifikaten und Bewertungsmethoden im Bereich der Aktorik? a. Welche Daten und Informationen sind für Endanwender interessant? b. Wie ist die Vergleichbarkeit der Bewertungsverfahren? Die resultierenden Kennwerte weichen voneinander ab. – Felddaten - Generische Tabellenwerke - Testreihen

Antwort:
a. Prinzipiell alle Daten, die im Sicherheitshandbuch angegeben sind. Darüber hinaus sind die Daten zu berücksichtigen, die Aufschluss über die Eignung für die geplante Applikation geben. Eine Checkliste findet man z. B. in der VDI/VDE 2180 Blatt 5. Insbesondere sind die Umgebungsbedingungen und z. B. die Antriebsleistung von großer Bedeutung.
b. Eine Auslegung sollte niemals auf Basis von Ausfallraten erfolgen. Diese sind bei Mechanik oft ohne Aussagekraft und im Extremfall sogar schlichtweg falsch. Bei Aktoren ist - mehr noch als bei elektronischen Komponenten - das gute Engineering von erfahrenen und kompetenten Fachleuten für die korrekte Funktion entscheidend. Im Zweifelsfall sollte das Prüfintervall für die regelmäßige Wiederholungsprüfung verkürzt werden, bis entsprechende Erfahrungswerte vorliegen, die die korrekte Funktion in der Praxis bestätigen.

16. Folgendes Szenario: Verdichter mit Schütz (nicht überdimensioniert) Danfoss Umrichter (SIL 2) 24V Spannung sicher abgeschaltet (über HIMA H 4116) für Ansteuerung 227K1 Motorschütz a. Reicht mir der Hilfskontakt des Motorschützes auf den sicheren Stop des Umrichters oder muss ich ein zusätzliches HIMA Relais in die Abschaltkette einbauen? b. Wie werden die Relais bewertet, 1oo2 oder 2oo2?

Antwort:
a. Der Hilfskontakt muss als zwangsgeführt oder als Spiegelkontakt vom Hersteller ausgewiesen sein, sonst ist der Einsatz im Sicherheitspfad nicht möglich. Spiegelkontakte und zwangsgeführte Kontakte seien laut Siemens sicherheitstechnisch gleichwertig. SN31920 Fehlerraten für Schaltelemente.
b. Hier 2oo2

17. -Kann mit nur einem Schaltelement (Schütz, Leistungsschalter) der Performance Level D erreicht werden. Was ist zu tun, wenn es bei größeren Leistungen keine zwangsgeführten Kontakte gibt? Wie -werden Spiegel Kontakte verwendet? a. -Wie geht die Überdimensionierung eines Schaltgliedes (Betrieb mit halben Nennstrom) in die Berechnung des Performance Levels ein? b. - Was ist bei der Berechnung des Performance Levels zu tun, wenn man bei divergenter Technik (z.B. Geschwindigkeitserfassung) keine Sicherheitsgerichteten Komponenten verwendet, und keine Daten für B10 vorliegen?

Antwort:
a. Wenn die Überdimensionierung einen Einfluss haben soll, dann vermutlich über einen Fehlerausschluss. Nach 13849-2 „Bewährte Bauteile, Schütze“ gibt es auf Schütze keinen Fehlerausschluss. Ein einkanaliger Aufbau kann durch Überdimensionierung nicht begründet werden. Artikel zum Thema von der Fa. Siemens: „Zwangsgeführte Kontaktelemente von Hilfsschützen und Spiegelkontakte von Leistungsschützen“. Bei Niederspannungsschaltern kann Überdimensionierung zu einem höheren SIL führen, bei Mittelspannungsschalter geht das nicht, da der elektrische Verschleiß dort keine Rolle spielt. Nach SN31920 kann mit Siemens Schützen aber einkanalig SIL2 erreicht werden.
b. Der Einsatz nicht sicherheitsgerichteter Komponenten ist zweikanalig möglich, wenn Fehler durch Dynamik aufgedeckt werden. Der Ausschluss des Versagens einkanaliger mechanischer Komponenten muss nachgewiesen werden.

18. Wird eine Schutzeinrichtung in der Prozesstechnik im Low Demand Mode oder im High Demand Mode betrieben, wenn sie auch für die Prozessleittechnik mitbenutzt wird?

Antwort:
Low- oder High-Demand hat nichts mit der Art Schutzeinrichtung zu tun, sondern allein von der Häufigkeit der Anforderung einer Schutzfunktion. Wenn die Schutzfunktion im Mittel häufiger als einmal pro Jahr angefordert wird, dann spricht man vom „High-Demand Mode“ (hohe Anforderungsrate). Hierbei zählt nur die „echte“ sicherheitstechnische Anforderung. Wenn ein Betriebsmittel aber auch noch betriebsmäßig geschaltet wird, kann es sein, dass einzelne Komponenten mit den Ausfallraten des „High-Demand-Modes“ berechnet werden müssen, auch wenn die Schutzfunktion im Low-Demand-Mode betrieben werden. In diesem Fall wird die PFD berechnet und in die Formel für die PFD-Berechnung die Ausfallrate Lambda des „High Demand Mode“ eingesetzt. Diese wird bei mechanischen Komponenten üblicherweise aus dem B10d-Wert ermittelt.

7. SIL-Sprechstunde 2015

Fragen zur 7. SIL-Sprechstunde 22. – 23.Sept. 2015

Rot = Fragen zur Interpretation des Normentextes
Grün = Fragen zutechnischen Aspekten des Normentextes
Frage 1

1. Einige Geräte sind explizit nach DIN EN 62061 für SIL-Kreise einsetzbar und nach dieser Norm zertifiziert. So gibt Phoenix Contact bspw. für das Relais mit der Bestellnumer 2981033 folgendes an: "SILCL 3 according to IEC 62061, SIL 3 according to IEC 61508". Kann das Relais, da eine Bezugnahme auf die 61508 erfolgt ist bzw. das Gerät nach dieser Norm zertifiziert wurde, für Anwendungen in der Prozessindustrie eingesetzt werden? Die Frage rührt daher, weil in der DIN EN 61511-1 unter 11.4.5 folgendes steht: "Alternative Anforderungen an die Fehlertoleranz dürfen verwendet werden, wenn eine Beurteilung nach den Anforderungen der IEC 61508-2, Tabellen 2 und 3 durchgeführt wurde."

Ströbl: nicht direkt. Die Anforderungen aus der Peripherie dieser Anwendung müssen passen. Die DIN EN 62061 gilt für intermittierenden Betrieb. Es gibt viele Umgebungsbedingungen die dem direkten Einbau widersprechen (Verharzen).
Gabriel: Prozessautomation realisiert meist separate Kanäle (Sensor bis Steuerung). Fabrikautomation realisiert Sicherheitsfunktionen mit verbundenen Kanälen über Vergleicher, ggf. Rücklesen der Ausgänge. Nachfrage nötig ob Low Demand Mode auch abgedeckt. Achtung, auch ein nicht sicherheitstechnisch nötiges Schalten (nicht der Demand) könnte Fehler wie im High Demand Mode aufdecken.
Hildebrandt: Bei Low Demand Mode kommt nicht Verschleiß sondern „Einrosten“ zum Tragen. Falls mehrfach zur Überprüfung der Funktion geschaltet wird ist trotzdem für „Low Demand“ zu kalkulieren. Dann muss der λ-Wert auf den B10-Werten basieren.
Blessing (VEGA): Angabe der Diagnosezeit, der Kunde darf entscheiden ob er diese mit berücksichtigt oder nicht.
Allgemeine Diskussion (Herr Lohmann, Emerson): Berechnung fast irrelevant gegenüber Fehlervermeidung / Fehlerbeherrschung
Hildebrandt: Fehlervermeidung / Fehlerbeherrschung hilft für Systematik und Probabilistik.
Brockschmidt: Es hilft, „Typicals“ zu bilden mit denen die Rechnung durchgeführt werden kann. Das Management der funktionalen Sicherheit, mit geeigneter Auslegung der Anlage, spielt heutzutage eine deutlich größere Rolle als die Berechnung en.
Frage 2

2. Siemens gibt für seine Frequenzumformer eine SIL 2 Zertifizierung nach DIN EN 62061 an. Ein solcher Frequenzumformer soll nun in einem Sicherheitskreis der Prozessindustrie zum Einsatz kommen. 1. Wie erfolgt die Umsetzung zur Berechnung der Ausfallwahrscheinlichkeit? Siemens gibt lediglich einen PFH-Wert von 5x10-8 für die Kontrolleinheit CU240E-2 an. (Siehe Handbuch A5E02299792A AB) 2. Das Gerät wird betrieblich mitgenutzt. Ist eine Berechnung der PFD-Werte erforderlich. Wenn ja, wie erfolgt diese?

Schween: kann nicht zurückgerechnet werden da die interne Architektur eine Rolle spielt. Geht nur wenn einkanalige Architektur (Lambda gleich PFH). Man kann beim Hersteller anfragen, entweder nach Architektur oder Lambda.
Siehe Frage 4: wenn „Low Demand“ (Zahl der Sicherheitsanforderungen im Jahr <1) dann per PFD berechnen.

Frage 3

3. In der jüngsten Überarbeitung des AD 2000 Merkblatt A6 (Entwurf 2015-06) wurde der Punkt 3.2 neu definiert. Bestand: 3.2 Verwendung fehlersicherer, selbstüberwachender oder redundanter Sicherheitseinrichtungen. PLT-Sicherheitseinrichtungen müssen entweder - fehlersicheres Verhalten besitzen oder - redundant oder - selbstüberwachend ausgeführt sein. In der Vergangenheit wurden diese Sicherheitseinrichtungen in der Regel redundant aufgebaut. (Dieses Thema wurde auch schon in der SIL-Sprechstunde 2012 behandelt) Entwurf: 3.2 Anforderungen an die Zuverlässigkeit von PLT-Sicherheitseinrichtungen wird durch den Parameter SIL (Sicherheits-Integritätslevel) ausgedrückt. Die Anforderungen an die Zuverlässigkeit der Sicherheitseinrichtung ist durch eine Risikoanalyse gemäß Normreihe DIN EN 61511 unter Verwendung des Risikografen im Anhang D der DIN EN 61511-3 zu ermitteln. Eine ausreichende Zuverlässigkeit kann erreicht werden z.B. durch - fehlersicheres (fail safe) Verhalten; - Redundanz; - Selbstüberwachung. Der SIL der vollständigen PLT-Sicherheitseinrichtung ist gemäß Normreihe DIN EN 61511 zu bewerten. 1.Müssen Einrichtungen die Druckgeräte vor Überschreiten ihres zulässigen Drucks schützen (nach AD2000 A6) zwingend als PLT-Sicherheitseinrichtung aufgebaut werden? 2.Was, wenn bei der Risikoanalyse keine Notwendigkeit einer Schutzeinrichtung festgestellt wird? 3.Wie sind die beiden Begriffe „fail safe“ und „Selbstüberwachung“ definiert? 4.Ist zukünftig das Ergebnis der Risikoanalyse entscheidend für die Ausführung der Sicherheitsfunktion d.h. Redundanz erst bei SIL3?

1. Ströbl: Ja.
2. Ströbl: Dann muss keine Schutzeinrichtung implementiert werden.
3. Ströbl: Fail safe ist in verschiedenen Normen beschrieben. Selbstüberwachung wie z.B. beim Shutter in optischen Systemen ist nicht vordefiniert und wird anwendungsbezogen bewertet
Wird heutzutage äquivalent zu Diagnose angesehen, stammt aus Normen vor der Zeit der SPSsen.
Tewes: TRBS 1201 Teil 2 beschreibt diese Begriffe.
4.
Ströbl: keine Redundanz nötig wenn eine Risikoanalyse keine Redundanz erfordert.
Kuboth: Bei Risikoanalyse hier ist wohl die systematische Gefährdungsanalyse gemeint. Das was passiert ist ungefährlich? Dann keine Sicherheitsfunktion nötig.
Ströbl: TRBS 1201 Teil 2 beschreibt Anforderungen.

Frage 4

4. Die IEC 61508-2, 7.4.9.5, Note 3 nennt als Erfahrungswert für die Gebrauchsdauer den Zeitraum von 8 bis 12 Jahren. Dies ist natürlich ein sehr weiter Bereich, wobei eine große Abhängigkeit von den verschiedenen Betriebsbedingungen und den verbauten Bauelementen besteht. Von Seiten der Anwender werden wir als Gerätehersteller immer wieder aufgefordert, eine Aussage zur „nutzbaren Gebrauchsdauer“ (Useful lifetime) zu machen. Da wir aber die Betriebsbedingungen nicht kennen, ist das nicht möglich. 1.Gibt es von Seiten der Experten einen Vorschlag, wie eine einigermaßen stichhaltige Antwort aussehen könnte? Vielleicht die Idee einer Matrix mit den Parametern Umgebungsbedingungen, verbaute Bauteile in den Geräten, … Anmerkung: Es gibt auch Spezialisten, die anfragen, ob sie ein 9 Jahre auf Lager liegendes Gerät in einen SIL-Loop einbauen können.

Hildebrandt: Beide Parteien müssen ihr Wissen in die Waagschale werfen.
Schween: Schwierig bei aktuellen Geräten mit Mikrocontrollern. Aufgrund immer kleinerer Strukturen, Zwischenschichten und anderer verwendeter Materialien sind Lambda-Werte und Lebensdauer schwer abzuschätzen. Maßnahme: Es werden Werte angenommen die aus üblichen Datenbanken stammen und mit Rückläuferstatistiken abgeglichen.
Aber: der Betreiber müsste z.B. auch Umgebungsbedingungen aufzeichnen.
Hima macht deshalb nur in Verbindung mit Wartungsverträgen (die gewisse Überwachungen vorschreiben) konkretere Aussagen.
Hot Standby hat laut Hima bessere Möglichkeiten um Lebensdauern zu gewährleisten (andere Firmen empfehlen unbestromte Lagerung).
Stördatenerfassung ist die geeignete Methode um eine echte "useful lifetime" zu bestimmen.
Mechanische Komponenten: Relais in Steuerungen werden auf Ströme und Schaltzyklen überwacht.
Karte: Stördatenerfassung / Betriebserfahrung ist die geeignete Methode um eine "useful lifetime" zu bestimmen.
Unerkannte systematische Fehler können nicht bewertet werden.
Wiederholungsprüfung ist oft nicht einmal geeignet dokumentiert.
Auslegung der Ventile ist maßgeblich.
Siehe Toolbox in Vortrag von Herrn Gabriel.
Gabriel: Die Aussage kann konkretisiert werden wenn Bauteile mit limitierter Lebensdauer bekannt sind.

Frage 5 a-b(c)

5. a) In der 2nd Edition der IEC 61511 wird die „Systematic Capability“ (SC 1 bis SC4) definiert, für Geräte entwickelt nach den Anforderungen der IEC 61508. 1.Kann bei Vorhandensein der entsprechenden SC Deklaration /Zertifizierung auf den Nachweis der Betriebsbewährtheit der Geräte verzichtet werden und dennoch die NE-130 angewandt werden? b) „Diagnostic Coverage“ wird in der IEC 61508-6 beschrieben. 1.Wieviel Prozent DC ist in der PFD Berechnung zulässig (reasonable) bei einer permanenten Überwachung der Abweichung einer 2oo3 Sensor Architektur in der Sicherheitssteuerung? 2. In der NAMUR NE 130 wird kein DC berücksichtigt. Warum? c) Low Demand Mode In der IEC 61508-6 (2010) wird ein deutlich größeres Demand Intervall gegenüber dem Proof Test Intervall gefordert: Unter B.3.1: „.. the expected interval between demands is at least an order of magnitude greater than the proof test interval … “. Exida definiert im „Safety Equipment Reliability Handbook“ Third Edition: „A SIF is considered to be operating in the low demand mode if the ratio of demand interval to proof test interval is greater or equal to 2 AND if the demand interval is greater than 1 year. …… In all other situations the SIF is considered to operate in high or continuous demand mode.“ IEC 61511, 2nd Edition: „Low Demand Mode: where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year; …” Mit der 2nd Edition von IEC 61511 sollte diese Anforderung des Verhältnis zwischen Demand Intervall und Proof Test Intervall nicht mehr relevant sein, oder?

a. Schween: Betriebsbewährung ist etwas Anderes als die systematische Entwicklung nach 61508. Wenn beide Betrachtungen möglich sind sollten die konservativeren Werte angestrebt werden.
Gabriel: Systematic Capability beschreibt die Eignung für die angegebene Applikation. NE130 beschreibt etwas ganz anderes, eine Betriebsbewährung um die Eignung für die spezielle Applikation festzustellen.
Der Prozessanschluss muss mitbewertet werden.
b. 1 Gabriel: in der Diskussion bei der NAMUR. Ein Wert um die 90%wird sich wohl ergeben.
b.2 Gabriel: in der NE 106 wird der DC genannt, deshalb nicht berücksichtigt in der NE 130.
c. Hildebrandt: Das Verhältnis ist ein Parameter der für eine geeignete Auslegung einer Sicherheitseinrichtung nötig ist.
Beispiel: Nach Ausfallrate wird alle 10 Jahre jemand verletzt. Gleichzeitig wird die Sicherheitsfunktion bei Anforderung mit 100% Proof Test Coverage getestet. Wenn ich weiss dass Kollege Müller alle 15 Minuten die Sicherheitsfunktion benötigt dann ist die Wahrscheinlichkeit dass er sich bei der nächsten Anforderung verletzt verhältnismäßig gering. Wenn ich weiss dass Kollege Müller nur alle 10 Jahre die Sicherheitsfunktion benötigt bin ich fast sicher dass er sich dann verletzt. Herr Müller würde im zweiten Fall sicher einen Proof Test in geeigneter Frequenz für sinnvoll erachten. Im ersten Fall würde er wohl fordern dass die Ausfallwahrscheinlichkeit reduziert wird, ein Proof Test ist fast wirkungslos. Es ist also weiter sinnvoll, in manchen Fällen einen Proof Test-Intervall oder ein Verhältnis zum Demand vorzuschreiben.

Frage 6

6. Laut Norm IEC 61511 ist es möglich SIF im DCS zu realisieren bis zu einem RRF von 10. Kann durch Kombination mehrerer SIF im DCS ein höherer RRF erzielt werden? Rechnerisch würden parallel realisierte Funktionen zu einem höheren RRF führen, auch wenn die individuellen SIF nur einen RRF von etwa 10 haben.

Gabriel: Layer wie in A9.3.5 nach 61511 dürfen realisiert werden, dies wird dort als adäquat erachtet für bis zu 2 Schichten (Protection Layers).
Schween: wenn in der selben Hardware (SSPS) die Regelung (RRF 10) und die Sicherheitsabschaltung (SIL 3) realisiert werden sollen, dann müsste die SSPS eigentlich für SIL 4 ausgelegt sein – Vorsicht!

Frage 7

7. Die Ausgestaltung der Risikomatrix in Hinblick auf die Granulierung und Form ist Sache des Betriebes und soll individuellen Bedürfnissen angepasst werden. 1.Wo bestehen Grenzen bei der Anpassung der Matrix? 2. Können SIL-Stufen entfallen, wenn ja unter welchen Voraussetzungen?

Risikomatrizen sind sehr vielfältig, auch in der Literatur zu finden. Es können verschiedene Möglichkeiten zur Gestaltung genutzt werden. Wenn laut Risikoanalyse die Vereinfachung möglich ist auf ‚kein SIL' oder ‚SIL 2' oder ‚SIL 3' zu reduzieren dann ist das statthaft. Es gab aber schon Fälle bei der eine solche Schematisierung von Dritten hinterfragt und die Matrix korrigiert wurde.

Frage 8

8. In der 2nd Edition der IEC 61511 wird die "Systematic Capability" definiert in SC1 bis SC4. Es herrschte bisher das Verständnis, dass Hersteller von Instrument & Ventil Equipment per "Manufacturer Declaration" die Eignung für SIL-Applikationen bestätigen/ bescheinigen können. Mit einer 1oo1 Architektur (HFT= 0) war das auf SIL 2 begrenzt. Ist es im Sinne von "Functional Safety" nach der IEC 61511 akzeptabel, dass nun die Hersteller eine Eignung für SIL 3 Loops deklarieren (mit HFT= 1) ohne Assessment eine unabhängigen, autorisierten Organisation? Siehe Beispiel Declaration.

Der Hersteller stellt das Beiblatt 1 der NE 130 zur Verfügung in dem die Eignung für SIL 3 bei HFT von 1 konstatiert wird. Dies darf der Hersteller tun, Tabelle 5 in 61508-1 zeigt wer das ohne zusätzlichen Nachweis von Dritten darf. Prinzipiell ist kein Nachweis von Dritten erforderlich, die Aussage des Herstellers genügt.

Frage 9

9. Für eine SIF, die mittels Reißleinenschalter (NOT-HALT) auf einen Antrieb wirkt, ist rechnerisch eine SIL-Stufe 2 im Low-Demand-Modus (meines Wissens normativ: Low Demand bis 1 Betätigung/a) nachgewiesen. Welche Konsequenzen sind angezeigt, wenn sich im realen Betrieb, eine Betätigungsrate von z.B. 100 mal jährlich einstellt?

Maschinenkontext ist bei NOT-HALT ganz evident: muss für ‚High Demand' ausgelegt werden.
Eberle: diese Einrichtung ist wohl nicht adäquat wenn der Demand so hoch ist. Hier greifen eigentlich andere Normen als die 61508.
Ströbl: keine Schutzeinrichtung, sondern schadensbegrenzende Einrichtung (NOT-HALT gegenüber NOT-AUS). Der Bediener müsste dann in die Berechnung einbezogen werden, das macht eigentlich keinen Sinn.

Frage 10

10. Wegfall des Proven-in-use durch Hersteller: 2006 wurde ein Typ B-Gerät mit SFF< 90% aufgrund einer FMEDA und Proven-in-use – Assessment beim Hersteller SIL2-qualifiziert. 1. Darf ein solches Gerät im ungeänderten Zustand noch in Verkehr gebracht werden? 2. Wird nun aufgrund der IEC 61508, 2nd Edition die FMEDA angepasst und das PIU-Argument gestrichen – kann dann der Anwender dieses altbewährte Gerät nach der IEC 61511 als betriebsbewährt erklären? 3. Wie liegt der Fall bei einem Typ A-Gerät (SFF<60%)?

Schween: Proven-in-use (Begriff) nur in 61508. Aber aufgrund der verstrichenen Zeit kann auch hier eine gewisse Betriebsbewährung angenommen werden.
Hildebrandt: FMEDA ist das Schauen in die Zukunft während hier konkrete Erfahrung vorliegt. Es kann verglichen werden ob die angenommenen Werte sich bestätigt haben.
Ströbl: Der Bestand in Anlagen wäre akzeptiert. Bei Erweiterung einer Anlage würde geschaut ob die neuen Teile hinreichend ähnlich sind um das Schutzziel auch mit der damaligen Bewertung zu erreichen.

8. SIL-Sprechstunde 2016

1. Wie ist der Ablauf und Aufwand einzuschätzen, um ein "normales" Betriebsgerät (Programmierbar), das nicht nach Sicherheitsnormen entwickelt wurde, für SIL 1 / PLc zu qualifizieren?

SIL1:
Die EN 61511 kennt die Einstufung ‚prior use', macht aber nur vage Vorgaben. Hilfestellung gibt hier die MAMUR Empfehlung NE 142. Wenn nicht nach EN/IEC 61508 entwickelt wurde, dann sind Basisanforderungen nach NE 95 zu erfüllen. 10 Geräte müssen für 1 Jahr im Betrieb erprobt werden. Die Eignung für PLT-Schutzeinrichtungen ist zu prüfen.
Eine Stördatenerfassung nach NE93 muss gegeben sein.
Ein Update der Software darf in der Zwischenzeit nicht erfolgt sein.
Ein Hersteller kann prinzipiell keine Aussagen zu Betriebsbewährung machen da er selten Erfahrung zu Medienkontakt und Einbaubedingung der Geräte aufbauen kann. Ausnahmen können z.B. Schaltschrankgeräte ohne Medienberührung sein. Ein Auswerten von Rückläuferstatistiken allein kann aber auch kein Rezept sein da nicht alle Ausfälle sicher zurückgemeldet werden.
Felderfahrung wird in EN/IEC 61508-2:2010 Tabelle B.6 als Maßnahme zur Vermeidung systematischer Fehler erwähnt, bei Software findet sich EN/IEC 61508-7:2010 Anhang D.
PLc:
Die EN 13849 lässt dies eigentlich nicht zu.
Betriebsbewährung setzt vergleichbaren Betrieb voraus. Nachweis der Eignung (nicht die Zertifizierung des Gerätes) ist entscheidend. (Umgebungsbedingungen, Medium, Vibrationen sind entscheidend). Daher ist eigentlich eine Betriebsbewährung besser als eine Zulassung eines Gerätes.
Bei Software nur durch Einhaltung eines Software-Entwicklungsprozesses nach ISO 9000 möglich (V-Model, Änderungsmanagement, …). Informationen beim Hersteller einholen.
Ein FMEDA auf Applikationsebene ist erforderlich.

2. Inwieweit ist eine Baumusterprüfung einer Betriebsbewährung gleichzusetzen?

Bitte sehen Sie dazu auch die detailliertere Recherche der Fa. Samson, die diesen Punkt in einem Vortrag beim Dechema-SIL Tag im Juli 2016 angesprochen hat. Darin hieß es: *"..... Meine Aussage „die Baumusterprüfung könne bzgl. der Eignung" der Betriebsbewährung*
gemäß VDI/VDE 2180 gleichgesetzt werden, bezieht sich auf VDI/VDE 2180 ,
Blatt 5, Seite 4 , Abschnitt 3.1 „Geräteauswahl…" wie folgt: Es müssen gleichzeitig auch Maßnahmen gegen systematische Fehler und Maßnahmen zur Fehlertoleranz ergriffen werden (Bild 1). Im Einzelfall kann auch eine der folgenden Vorgehensweisen angewendet werden:
· Baumusterprüfung des Geräts für den Einsatzfall entsprechend der jeweiligen Norm
· Einzelprüfung für spezifische Anwendungsfälle durch unabhängige Organisationen
Bei Anwendbarkeit der Norm können Sie die Baumusterprüfung deswegen als Begründung für Ihre Geräteauswahl im Sicherheitskreis verwenden (… oder die genannte Einzelprüfung durch eine unabhängige Organisation). Im Einzelfall stellt dies eine Alternative auch zur Betriebsbewährung dar.
Bei einer Baumusterprüfung sind die Randbedingungen zu beachten: es werden keine Aussagen über spezielle Anwendungen gemacht. Wenn die gemachten Randbedingungen auf die Applikation zutreffen (z.B. nach Brennernorm EN 50156) ist die Baumusterprüfung ein sehr guter Weg. Achtung, wenn die Baumusterprüfung auf ein SIS (Konstrukt aus mehreren Geräten) Bezug nimmt, dann gilt die Baumusterprüfung nur für dieses Konstrukt,

und nicht für einzelne Geräte. (Sensor, Ventil, Antrieb). Solch eine Bewertung einer ganzen Kette von Geräten wäre z.B. für Druckgeräte-Richtlinie sinnvoll.
In der Prozessindustrie nicht üblich da keine für eine Applikation baumustergeprüften Geräte verfügbar sind.

3. Kann ich durch Kombination mehrerer SIL2-Schutzfunktionen (unabhängige Layer – LOPA = Layer of Protection Analysis) einen höheren SIL als SIL2 erreichen?

Nicht direkt möglich bei Geräten mit Software die nur für SIL2 entwickelt wurde (nur mit diversitäre Redundanz). Demnach ist die Systematische Eignung der SW zu berücksichtigen. Bayer (Covestro) verbaut homogen redundant SIL2 Geräte für SIL3 Applikationen, bekannt auch von anderen Firmen. Nach der VDI/VDE 2180 Blatt 5 sind auch hier systematische Fehler zu beachten.
Zitat aus der DIN EN 61508-6:Feb.2011 (IEC 61508-6,Ed.2:2010-04 Effects of a nonperfect
proof test): *B.3.2.5 Auswirkungen einer unvollständigen Wiederholungsprüfung … Wenn…Fehler nicht...erkannt werden, sollte angenommen werden, dass sie über die Laufzeit der Betriebsmittel erhalten bleiben. …Wiederholungsprüfung…T_1…Anteil der Fehler, der bei der Ausführung der Wiederholungsprüfung erkannt wird, als PTC (Deckungsgrad der Wiederholungsprüfung) bezeichnet…und der Anteil der Fehler,…nicht erkannt wird, als (1-PTC) bezeichnet... Diese letzteren Fehler werden nur erkannt, wenn eine Anforderung*
an das sicherheitsbezogene System erfolgt, hierfür wird das Intervall der Anforderungen T_2 angenommen.
Interpretation zu B.3.2.5: In der DIN EN 61508 wird mit T_1 das Intervall der Wiederholungsprüfung
beschrieben. Wird eine Wiederholprüfung durchgeführt, bei der nicht alle Fehler im Sicherheitssystem erkannt werden konnten (Deckungsgrad der Wiederholprüfung = PTC), so muss in der Berechnung mit Angabe von T_2 ein Intervall festgelegt werden, zu dem auch diese nicht erkannten Fehler erkannt werden können z.B. durch eine Anforderung (1-PTC).
Behauptung: Viele Hersteller beschreiben in den entsprechenden Sicherheitshandbüchern eine Prüfmethode die dem Anforderungsfall gleichzusetzen ist (z.B. für Standmessungen: Anfahren der Ansprechhöhe im Rahmen einer Befüllung). Eine so durchgeführte Prüfung mit erfolgreichem Ergebnis zeigt auf, dass zum Zeitpunkt dieser Prüfung kein gefährlicher,
unentdeckter, zufälliger Fehler dazu geführt hat, dass die Sicherheitseinrichtung versagt.

4. Frage: Welche PTC sollte in diesem Fall (T_2) in der PFD_{avg}-Wert Berechnung verwendet werden?

Die VDI/VDE 2180 wird in Zukunft Grundlagen zum Rechnen mit verschiedenen PTC vorgeben.
Üblicherweise ist es richtig dass gefährliche Fehler (der sichere Zustand wird nicht geeignet erreicht) bei einer Prüfung von Typ A-Geräten (Hardware) nachgewiesen werden kann. Bei softwarebehafteten Geräten wird auch heute schon nicht von 100% PTC gesprochen.
98% machen im Allgemeinen vernachlässigbare Unterschiede. Für Ventile ist die Spezifikation verschiedener Tests mit verschiedenen PTCs üblich. Ein Partial Stroke Test kann hier geringe Abdeckung zeigen aber die in der Praxis geeignetste Variante darstellen.

5. Wie ist vorzugehen bei sich (teilweise, im Detail) widersprechenden Standards/ Normen, z.B. für Brenneranwendungen?

Es gibt prinzipiell keine Normen die sich widersprechen. Es gibt immer eine Norm die der Anwendung am Nächsten ist, diese ist einzuhalten. Bei Schnittstellenanwendungen ist zu prüfen welche Norm die anspruchsvolleren Forderungen stellt, diese sind einzuhalten.
Beispiel Brenner: EN 50156 fällt unter die Maschinenrichtlinie die üblicherweise High Demand betrachtet, die Schutzanforderung wird allerdings als Low Demand betrachtet. Der TÜV Süd würde Bewertungen deshalb auf Low Demand einfordern.

6. Noch immer werden für manche Komponenten nur SIL-Zertifikate mit Zuverlässigkeitsdaten zur Verfügung gestellt, aber weder Sicherheitshandbücher noch (unter Verweis auf den KnowHow-Schutz) die zu den Zertifikaten gehörenden Prüfberichte. Ist das berechtigt?

DIN EN 61508-2 Kap. 7.4.9.3:
Die folgenden Informationen müssen für jedes sicherheitsbezogene Teilsystem und Element im angemessenen Rahmen verfügbar sein (siehe auch 7.4.9.4):
ANMERKUNG Für einen Lieferanten eines Teilsystems oder Elements, für das Übereinstimmung
mit IEC 61508 beansprucht wird, ist es notwendig, diese Informationen dem Konstrukteur eines sicherheitsbezogenen Systems (oder eines anderen Teilsystems oder Elements) im Sicherheitshandbuch für konforme Objekte zugänglich zu machen…
DIN EN 61508-2 Kap. 7.4.9.6
Lieferanten müssen für jedes konforme Objekt, das sie liefern und für das sie Übereinstimmung
mit IEC 61508 in Anspruch nehmen, ein Sicherheitshandbuch für konforme Objekte gemäß Anhang D zur Verfügung…
Prüfberichte müssen nicht ausgegeben werden. Ein Zertifikat ist auch nicht notwendig.
Falls ein Gerät der EN/IEC 61508 entsprechen soll ist ein Sicherheitshandbuch notwendig.
Prinzipiell gilt aber dass die laut Anhang D geforderten Inhalte zur Verfügung stehen, wie das Dokument heißt ist nicht von Belang.

7. Ein 15kV-Antrieb soll in SIL2 abgeschaltet werden. Die 1. Trip-Spule im geeigneten Leistungsschalter wird über geeignete Relais energized to trip angesteuert, im Steuerspannungskreis befindet sich eine Sicherung. Eine 2. unabhägige Trip-Spule im Leistungsschalter soll energized to trip mit einer unabhängigen Steuerspannung (auch mit Sicherung) über Nicht-SIL-Schaltgeräte angesteuert werden. Könnte mit dieser Struktur SIL2 erreicht werden, obwohl der 2. Trip-Pfad nicht SILfähig ist? Wie könnte SIL2 nachgewiesen werden? Könnte man evtl. Kredit auf eine Überwachung der beiden Steuerspannungen nehmen (hinter den Sicherungen), verbunden mit organisatorischen Maßnahmen beim Ausfall einer der Steuerspannungen?

Leistungsbetrachtung durchführen. Wenn eine Diagnose (Reaktionszeit) ausreicht (um andere Maßnahmen zu ergreifen), muss keine Versorgungsbetrachtung durchgeführt werden.
Dow Chemicals hat in so einem Fall schon mit der ZÜS einen FMEDA durchgeführt und sich dafür an der NE142 orientiert – und so solch eine Anwendung qualifiziert.

8. Def. / Unterschiede zwischen SIS, SIF und SF

Hinweis: VDI/VDE 2180 Blatt1 Seite: 9

Oder nach EN 61508-4
Eine sicherheitstechnische Funktion (ohne Instrumentierung)(Safety Instrumented Function, SIF) besteht bei elektrischen und elektronischen Geräten selten aus einer einzelnen Komponente. Für eine vollständige Reaktion auf eine Übertemperatur in einem Prozess oder an einer Anlage werden immer mehrere Komponenten benötigt:
Bei einer Kette von Geräten spricht man von einem sicherheitstechnischen System (Safety Instrumented System, SIS):
- Sensor
- informationsverarbeitende Einheit (programmierbare Steuerung, SPS)
- Aktor für den Eingriff in den Prozess, z. B. zur Unterbrechung der Energieversorgung, zum Betätigen der Bremsen, zum Betätigen der Ventile, ggf. Ex-Trennbausteine
- ggf. Signalumformer im Verbindungskabel

Ein sicherheitstechnisches System realisiert eine oder mehrere sicherheitstechnische Funktionen

9. Kann ein Gerät (ein LogicSolver) mehrfach in einer Sicherheitskette vorkommen?

Ja, ein definierter Ablauf in einer Sicherheitskette kann zusätzlich eine Rückmeldung enthalten.
Die Zuverlässigkeit der Rückmeldung sollte aber untersucht und bewertet werden.

10. Kann ein Gerät (Sensor oder Aktor) in verschiedenen Sicherheitsketten vorkommen?

Ja - aber beachten, dass der Ausfall einer Komponente mehrere Sicherheitsketten außer Kraft setzen kann.
Gefahr dass dies in der Planung nicht erkannt wird, deshalb sollten unabhängige Sicherheitsketten
für unterschiedliche Schutzfunktionen realisiert werden. Empfehlung: Lopa.
Falls das trotzdem nötig ist müssen Diagnosesignale in hoher Zuverlässigkeit ausgeführt werden.

11. Kann ein Gerät (z.B. Überfüllsicherung) sowohl in einer low-demand-Sicherheitskette als auch in einer high-demand-Sicherheitskette vorkommen?

Wenn das Gerät für High Demand bewertet wurde ja, wenn nicht dann beim Hersteller nachfragen (z.B. Verschleiß von Relais).
Bei High Demand muss die Zeit der Diagnose beachtet werden. (notfalls λ_{dd} zu den λ_{du} addieren
und prüfen ob ausreichend)
Kann eigentlich nicht vorkommen da fast immer von der Anwendung bestimmt.
Wenn ein Gerätetyp in zwei verschiedenen Anwendungen eingesetzt wird, dann sind die jeweiligen Werte für die Demand Modes dem Sicherheitshandbuch zu entnehmen.

12. Kann eine Gruppe von Aktoren in 10 Sicherheitsketten vorkommen?

Ja. Lopa durchführen!

13. Ein Gerät hat kein SIL-Zertifikat. 13a. Gibt es so etwas wie einfache Betriebsmittel (Leitungen, Klemmen)? Wo ist das beschrieben? 13b. Wie bewertet man ein PT100 ohne Transmitter? Wo ist das dokumentiert? 13c. Wenn Feuerungsanlagen, BMA, … (die keine SIL-Werte haben, weil sie nach anderen Normen betrachtet werden) in eine SIL-Betrachtung mit einbezogen werden sollen, was für Ersatzwerte setzt man dann ein (SIL, PFD)? Wo ist das dokumentiert? 13d. wenn ein Kugelhahn schon 10 oder 20 Jahre alt ist, 13d1. "Wie bekommt man ihn" "sicher"? 13d2. Wie viele Versuche muss man in welcher Zeit mit ihm machen? Gibt es Vorgaben / Anleitungen? 13d3. Kann es eine Übergangsfrist geben oder muss immer sofort abgeschaltet werden, wenn eine Bestandsanlage als nicht sicher vermutet / eingeschätzt wird? 13d4. Welche anderen Szenarien gibt es? 13d5. Kann man eine FMEDA selbst erstellen? Wie? Muss man befähigt sein? Wie? 13d5a. Welche Fähigkeiten benötigt man dafür und wie erlangt man diese? 13e. Wie verfährt man mit Leistungsschaltgliedern (Schütze haben B10-Werte) im lowdemand-mode?

a. Kein Zertifikat nötig, da SIS Betrachtung und Bewertung durchgeführt werden muss. Dies auch unbedingt dokumentieren.
Bei diesen Beispielen ist λ_{du} meist vernachlässigbar klein oder 0. Systematische Fehler bewerten!
b. Kurzschluss und Leitungsbruch untersuchen und dokumentieren. Auch den Prozessanschluss
bewerten. Der PT100 fällt auch unter die regelmäßige Prüfung. Z.B. Datenbank
von Exida enthält Werte, berücksichtigt auch Einbaubedingungen. Oft nicht einzeln ohne Diagnose für Sicherheitsanwendungen geeignet wegen hoher Ausfallraten.
Wenn ein Transmitter vorhanden ist, muß der PT auch in der regelmäßigen Wiederholungsprüfung
getestet werden.
Wenn C-Normen vorhanden und angewendet werden wird keine SIL Betrachtung benötigt.
Wenn eine C-Norm nicht angewendet wird, muss das begründet werden.
d1 Sollte geprüft und ggf. ausgetauscht werden. End of Lifetime (Herstellerangaben) beachten.
d2 Ausbauen und prüfen, ggf. als betriebsbewährt bewerten. Wenn unbedingt notwendig Ersatzwerte
verwenden.
Wenn er in einer stillgelegten Anlage wieder in Betrieb genommen wird, dann die Lagerbedingungen
(z.B. Lagertemperatur) beachten und auf jeden Fall vor Inbetriebnahme prüfen.
d3 Wenn bei der Risikoanalyse herauskommt dass das Risiko zu groß ist abschalten.
d4 Weitere Schutzmaßnahmen installieren? Gefahren auf andere Art vermeiden?
d5 Mitarbeiter muss geschult sein und sich regelmäßig weiterbilden (nachweisbar, z.B. durch Teilnahmebestätigungen, auch mit externen Schulungspartnern), Erfahrung sammeln (z.B. durch einige FMEDA die von externen Stellen kontrolliert sind). Mehraugenprinzip: technische Experten und Spezialisten für FMEDA mit geeignetem Hintergrund einbinden.
d5a Systematisches Vorgehen, Blick für das Wesentliche.
e. Generische Werte gibt es in der EN/ISO 13849.

14. Wie lautet die Universalformel für eine moon-Auswahl? Wo steht das? 14a. Z.B. um den PFD-Wert aus Lambda und T1 für eine 5oo7-Auswahl zu berechnen? 14b. Wie berechnet sich die HFT? (m-n?)? Ist also HFT=5 möglich?

Siehe VDI/VDE 2180 Blatt 4. Diese ist derzeit nur für 100% Prüftiefe.

a. HFT = 2
b. 10 Sensoren im Kessel in unterschiedlichen Positionen detektieren Hot Spots. Das muss nicht 1 aus 10 sein, kann auch zu HFT = 5 führen (5oo10)

15. Was ist mit mehrkanaligen Modulen? Gilt hier der PFD-Wert je Kanal oder je Gerät? 15b1. z.B. zweikanalige Trennbarrieren in einem Gehäuse? 15b2. z.B. zwei zweiadrige Überspannungsableiter in einem Gehäuse?

Üblicherweise pro Kanal. Dokumentation lesen, es muss daraus hervorgehen.

16. Was ist mit zusammengesetzten Baugruppen? (hier Armatur im low-demandmode) 16a. Eine dritte Partei setzt einen sicheren Antrieb, einen sicheren Federkraftspeicher und einen sicheren Kugelhahn zu einer Armatur zusammen. Ist die Summe der Einzelteile dann sicher? (wenn er schludrig Sand in das Getriebe mit einarbeitet, verkantet sich der Rückstellmechanismus und der Kugelhahn geht nicht sicher zu.) 16b. Wenn die dritte Partei nun eine Konformitätserklärung abgibt und die PFD-Werte ohne Aufschlag addiert, ist das vertrauenswürdig? 16c. Wenn die dritte Partei den low-demand-Wert mit B10-Werten oder PFH-Werten ermittelt, wie verhält man sich dann? Rechnet man mit diesen Werten einfach weiter? (leicht / grob fahrlässig)

a. Drei Komponenten werden in der SIS zusammengeführt, die Werte werden addiert. Derjenige,
der die Komponenten zusammenführt muss die Bewertung durchführen und die nötige Fachkompetenz haben.
b./c. Der Hersteller übernimmt hier die Verantwortung. Der Schilderung nach scheint das Vorgehen
nicht in Ordnung zu sein.

17. Wie muss eine Spezifikation einer SIS, SIF oder SF aussehen?

Nicht in wenigen Worten zu erläutern. Bitte dafür vorgesehene Seminare besuchen.
Zu Fragen von Fachkompetenzen gibt die VDI/VDE 2180 Blatt 2 weitere Informationen.

18. Wie plane ich Validierung und Verifizierung? Was gehört zur Validierung und Verifizierung?

Siehe Frage 17
Definition Verifikation in EN/IEC 61508-4 Kap. 3.8.1
Definition Validierung in EN/IEC 61508-4 Kap. 3.8.2

19. Muss man SIL-Verifikationen unterschreiben? (nur mit Namen oder i.A.?) 19a. Muss der Unterschreibende wirtschaftlich und rechtlich Unabhängig sein? Wo steht das? 19b. Wie sieht es mit der Haftung aus?

Im FSM sind die Verantwortungen zu definieren und die definierte Person muss bestätigen, unterschreiben, und ist dafür haftbar. Da Ersteller und Prüfer entkoppelt sind ist ein Mehraugenprinzip gegeben.
a. Grad der Unabhängigkeit ist in EN/IEC 61508-1 je nach SIL-Level definiert. Die rechtliche Unabhängigkeit ist nicht genau definiert. Ein Vieraugenprinzip muss vorhanden sein um systematische Fehler auszuschließen.
b. Muss in der Firma je nach Kompetenz des Mitarbeiters nach Stellenbeschreibung festgelegt werden – keine allgemeingültige Regelung.

20. Muss ein 4-Augen-Prinzip angewandt werden? Müssen diese unabhängig voneinander sein?

Laut EN/IEC 61508-1 Kap. 8 ist ein unabhängiges Assessment nötig, das beinhaltet dass es einen Handelnden und einen Assessor gibt. Ja.

21. Der Kunde möchte im Schriftkopf einer Verifikation „bearbeitet“, „geprüft“ und „freigegeben“ stehen haben. Kann sich der Bearbeiter selbst prüfen und die Verifikation dann selbst freigeben? Müssen alle drei Personen hohe Fachkompetenz in der Funktionalen Sicherheit nachweisen können? Wie?

Es muss im Team geprüft werden. Wer freigibt ist eine organisatorische Frage.
Die Fachkompetenz ist notwendig. Grundlagen, Ausbildung und Weiterbildung müsen vorhanden
und nachweisbar sein.

22. Muss man Überhaupt Fachkompetenz nachweisen? Wie? Was ist für welche Tätigkeiten notwendig?

Siehe Frage 17

23. Was gehört zur Verifikation? 23a. Nur der rechnerische Nachweis? 23b. Oder auch eine schriftliche Fixierung von Randbedingungen und Erläuterungen?

a. Nein, jeder Arbeitsschritt wird verifiziert, die Sicherheitsbetrachtung wird verifiziert, die Pläne werden verifiziert,… die SIS wird dann validiert. Auch der rechnerische Nachweis muss verifiziert werden.
b. Ja, da der Verifizierungsplan vorhanden sein muss.

24. Kann man als abhängig Beschäftigter eine SIL-Verifikation erstellen und ist man dann gezwungen, diese zu unterschreiben? Und das unter marktwirtschaftlichen Zeitdruck? Wo man doch gerne noch mal recherchieren, eine zweite Meinung einholen oder den TÜV befragen wollte.

Ja, kann man machen, aber eine unabhängige Person muss verifizieren.

25. Einige SIL-Zertifikate sind von ihrer Gültigkeitsdauer beschränkt, andere nicht. 25a. Was macht man z.B. mit Siemens-Steuerungen in Bestandsanlagen? 25b. Wenn auf dem Exida-Zertifikat eine Gültigkeit von 2 Jahren vermerkt ist, muss der zugehörige Drucktransmitter dann innerhalb dieser 2 Jahre verbaut und in Betrieb genommen werden? 25b1. Ein drei Jahre alter Transmitter aus dem Lager kann also nicht verbaut werden? 25b2. Oder muss man ihn einfach nur rechtzeitig irgendwo einbauen?

a. Aussagen in Zertifikaten die bei der Inverkehrbringung gültig waren behalten ihre Gültigkeit. Systematische Eignung damit nachgewiesen.

b. Normativer Lebenszyklus, eventuell bei Inbetriebnahme Überprüfung notwendig. Daher die Gültigkeit der Zertifikate hier beachten, ggf. beim Hersteller nachfragen.
b1/b2. Lagerbedingungen beachten. Als Ersatzbedarf direkt nutzbar.

26. Wie sieht es mit der „sicheren“ E-Installation, der mechanischen Konstruktion, der Impulsverrohrung für Drucktransmitter oder der Druckluftverrohrung für die Hilfsenergie von Ventilen aus? Gibt es da Vorgaben? (z.B. die Druckluft / das Gas muss gefiltert mit Filtergröße ??? sein, die Druckluft, das Gas muss getrocknet (mit einer relativen / absoluten Feuchte von …) sein.)

Allgemeines Regelwerk für Installationen beachten. Die EN 61508 verweist auf ordnungsgemäße
Installation. Herstellerinformationen / Installationsvorschriften beachten.

27. Wie interpretiert man Angaben in Datenblättern wie „...bis SIL3“, „...SIL CL 3 (CI = claim = Anspruch, aus der EN 62061)“ 27a. Wie unterscheidet man SIL3 nach EN 62061 (Maschinensicherheit -> eigentlich ISO 13849) und SIL3 nach EN 61511 (Anlagensicherheit)? a1 SIL ist doch sicherlich in der 61508 definiert. 27b. Kann ich davon ausgehen, dass solche Geräte immer mindestens SIL1 erfüllen? 27c. Unter welchen Bedingungen erfüllen Sie SIL2? Und wann SIL 3? Das wird oft nicht oder nur indirekt angegeben.

Die EN 62061 kennt nur High Demand, EN 61511 üblicherweise eher Low Demand. Bei High Demand ist laut neuer EN 61511 für SIL 2 zweikanalige Ausführung erforderlich.

a1 Nicht nur.
b. Wenn SIL 2 / 3 angegeben ist kann davon ausgegangen werden.
c. In homogener Redundanz max. SIL 3. SC beachten. Es können spezielle Maßnahmen erforderlich
sein (ein Gerät kann kein SIL erfüllen sondern nur dafür geeignet sein).

28. Ich bin der Meinung, dass man PFH-Werte nicht in PFD-Werte umrechnen darf. Und auch nicht umgekehrt. Nun gibt es ein Schriftstück (siehe kommentierten Anhang), das suggeriert, dass man dies doch darf. Darf man oder darf man nicht? Oder darf man manchmal? Wo steht das?

Verschleiß beachten. Wenn Verschleiß vorhanden, dann nicht.
Als Anwender bitte nicht so durchführen. Nur mit Rücksprache mit dem Hersteller. Wenn einkanalig und rein elektrisch dann möglich.

29. Welche Bedingungen müssen erfüllt sein, damit zwei SIF im SIS zwei verschiedenen Schutzebenen (layer of protection) entsprechen?

Lopa müssen unabhängig sein. -> CCF (common cause failure) und mechanische Fehler berücksichtigen. In einem SIS können per Definition eigentlich keine 2 unabhängigen Layer realisiert werden.

30. Mittlerweile werden immer häufiger PTC-Werte (Prüftiefen) zu den SIL-Geräten angegeben, die das Ergebnis der PFD-Berechnungen und die SIL-Eignung der Geräte beeinflussen. Gibt es eine (MooN)-Formel für die PFD-Berechnungen in Abhängigkeit des PTC? Die IEC61508 gibt leider nur eine Formel für (1oo2) an. Wie berücksichtigen ich also die jeweiligen PTC-Werte, wenn ich keine (1oo2) sondern andere Architekturen habe?

Siehe neue VDI/VDE 2180 Blatt 4. Hier sind PTC und diversitäre Betrachtung behandelt. Ein Tool zur Eingabe und automatischen Berechnung ist in Arbeit.

31. Darf man "SIL-Eignungsnachweise" nach IEC 61508 (rechnerisch) und EN 50156 (qualitativ) innerhalb einer Prozessanlage mischen? z.B. eine Bestandsanlage wird nur in Teilen umgebaut, so dass es Altanlagenteile und Neuanlagenteile gibt, aber auch eventuell Mischfälle (keine Trennung möglich). Kann man so z.B. eine Feuerungsanlage nach EN 50156 rein qualitativ bewerten, und die anderen Anlagenteile außerhalb der Feuerungsanlage nach IEC61508? Muss bei einem Mischfall der Altanlagenteil komplett auf die IEC 61508 aktualisiert werden (Geräteaustausch?)? Bisher zeigt die Erfahrung, dass es immer nur "schwarz/ weiß"-Denken gibt: entweder alles qualitativ oder alles rechnerisch nachweisen. Es ist unüblich, dass ein SIL-Kreis z.B. rechnerisch nach IEC 61508 nachgewiesen werden soll, aber ein Gerät in diesem Kreis rein qualitativ bewertet/ beschreiben wird. Die bisherigen Prüfstellen fordern dann auch von dem qualitativ-bewerteten Gerät eine SIL-Kalkulation ein. Gibt es hierzu eine klare Definition für den Umgang bei diesen Mischfällen und wo steht dies geschrieben?

Die EN 61508 ist zuständig für Geräte, die EN 50156 für Anlagen. Daraus ergibt sich die Grundlage für die Bewertung. Es ist möglich, Anlagenteile getrennt zu betrachten.

32. Grundsatz: für SIL-Nachweise werden die zum Zeitpunkt der Komponentenlieferung gültigen Zuverläsigkeitsdokumente verwendet. Sonderfall nachträgliche verfahrenstechnische Erweiterung: Erweiterung bestehender SIF um zusätzliche Aktoren (gleicher Typ wie in Bestandsanlage, aber geänderte Zuverlässigkeitsdaten). Müssen im zu revidierenden SIL-Nachweis die neuen Zuverlässigkeitsdaten für alle Geräte dieses Typs verwendet werden oder nur für die nachgerüsteten?

Warum sind die Daten geändert worden? Wenn die ersten Daten falsch waren hat der Hersteller ein Problem. Dann müssen auch bestehende Anlagen mit den alten Werten neu bewertet werden. Wenn sich das Produkt geändert hat, gelten die jeweiligen Daten. (erkennbar
an der im Sicherheitshandbuch angegebenen Typenangaben).

33. IO-Kanäle/Kanalbaugruppen bieten oft die Möglichkeit eine Leitungsfehlerüberwachung (auf Drahtbruch, Kurzschluss o.ä.) zu aktivieren und im Falle eines Ansprechens definierte Reaktionen auszulösen (LED, Schaltkontakt, sicherer Zustand...). In welchen Fällen kann es bei SIFs erforderlich werden LF-Überwachungen zu realisieren? Zitat eines SV (Beispiel): Der einfache Fehler "Kurzschluss" wird hier nicht überwacht! In der Regel sind einfache Fehler zu beherrschen, gibt es einen bestimmten Grund weshalb hier darauf verzichtet werden kann? 32a. Wo steht das? 32b. Welche Signalkreise sind ggfs. betroffen? Aktor Feld, Sensor Feld, zwischen Trenner und Logic-IO 32c. Wie wird die erforderliche Qualität/Quantität (Signalisierung, ... sichere Abschaltung) festgelegt?

a. Verbindung zwischen Aktor und Steuerung ist zu betrachten. Leitungsüberwachung um den gesamten Loop zu überwachen. Im Sicherheitshandbuch muss erklärt sein ob aus der Leitungsfehlerübewachung für die FMEDA Kredit genommen wurde. Wenn dann keine Fehlerüberwachung verwendet wird müssen die λ_{dd} Fehler als λ_{du} gewertet werden (also addiert).
b. Siehe Herstellerdokumentation für die Einzelgeräte.
c. Ein erkannter Fehler wird als eine Grenzwertausgabe gewertet. Wenn statt einer Abschaltung
eine Alarmierung ausgegeben wird dann müssen andere Formeln verwendet werden
da der Kanal in dieser Zeit sicherheitstechnisch nicht verfügbar ist. (Alarm mitprüfen bei Wiederholungsprüfung).

9. SIL-Sprechstunde 2017

1. SIL Nachweis für Anlagen "energize to trip" wie. z.B. Entrauchung etc.. ?

Aufbau von Sicherheitsfunktionen mit Wirkrichtung „energize to trip“ ist prinzipiell möglich aber mit deutlichem Aufwand verbunden. Der komplette Weg von Energieversorgung, Auslöseeinrichtung, Ansteuerung muss betrachtet werden. (Ströbl)
Üblicher Einsatz z.B. bei Brandmeldeanlagen. Möglichkeit: wenn die Brandmeldeanlage nicht funktioniert, dann evakuieren (wie z.B. auf Messen oder in Bankzentralen).
Hier ist eine organisatorische Maßnahme Teil der Sicherheitsbewertung. Wenn die Erstmaßnahme nicht greift dann muss eine Sekundärmaßnahme einspringen. Weitere Hinweise auch in den Präsentationsfolien der letzten SIL-Sprechstunde bezüglich „energize-to-safe“ / „de-energize-to-safe“ (oder bei HIMA Paul Hildebrandt GmbH anfragen). In der Gebäudetechnik gibt es noch kein Regelwerk das mit SIL-Bewertungen arbeitet. (Hanspach)
Aufgaben im Betrieb einer Brandmeldeanlage sollten automatisiert sein (übliche Reihenfolge ist: technisch, organisatorisch, persönlich).
EN ISO 13849-1:2015 gibt „de-energize-to-safe“ als übliches Wirkprinzip vor, mit geschützter Leitungsverlegung und Redundanzen. Sicherungsautomaten wie in der Gebäudetechnik vorgeschrieben können für gefahrbringenden Ausfall der Sicherheitsfunktion führen.

2. SAL/ IT-Security (IEC 62443) vs. SIL/ Funktionale Sicherheit (IEC 61508): Warum werden normativ diese beiden Themen vermischt? a. IT-Security betrachtet unvorhersehbare, gewollt böswillige, externe Eingriffe (misuse) über einen ei-genständigen Lebenszyklus und Risikoanalysen (SAL-Einstufungen), aber Funktionale Sicherheit betrachtet vorhersehbare, ungewollte, anlageninterne Fehlerarten (systematische & zufällige Fehler) über eigenständiges Lebenszyklen und Risikoanalysen (SIL-Einstufungen). IEC 61508-1, 7.4.2.3, note 3 und 7.5.2.2 note enthalten bereits Hinweise auf die IEC 62443. Genauso ist es in der Überarbeitung der EN 50156 geplant, in dem das FSM detaillierter beschrieben werden soll und auch "IT-security" und "misuse". Sollte man die beiden Bereiche SIL und SAL nicht zu 100% getrennt behandeln? b. Die Anforderungen zu SIL werden für die Unterlieferanten/ Hersteller von SIL-fähigem Equipment bereits immer höher/ strenger, genauso wie die Kosten, die ein Hersteller mittlerweile für seine SIL-Befähigungen oder die SIL-Fähigkeit seines Equipments aufwenden muss. Sind die bisherigen SIL-Equipment-Hersteller grundsätzlich für das Thema SAL/ IT-Security & misuse heute schon gerüstet (z.B. SAL-Zertifikate o.Ä.)? Gibt es solche Zertifikate bereits? Muss ein Anwender/ Kraftwerksbauer sowie der Betreiber nun immer SIL & SAL abfragen, um seinen heutigen Pflichten zur Anlagensicherheit nachzukommen? Muss zum üblichen QM-System in einem Unternehmen jetzt auch ein FSM und ein Management zur IT-Sicherheit installiert sein, damit Anlagen heute noch von den Prüfstellen abgenommen werden? Gibt es Erfahrungswerte bei Unternehmen? Wie gehen die Betreiber damit um?

a. Die beiden Themen sollten getrennt behandelt werden, da die Maßnahmen sich unterscheiden (Ströbl, Hanspach). Meinung wird nicht uneingeschränkt geteilt (Kuboth). Bei Safety gilt die Bewertung für Jahre, bei Security muss ständig erneuert und nachgebessert werden da die Bedrohungen sich ständig ändern.
Anders in China, dort gibt es eine Behörde die Regularien festlegt und beide Themen gleich behandeln will.

Sicherheitsfunktionen die Feldbusgeräte nutzen können über den Feldbus (Internet) angegriffen wer-den. Dies war bei konventionellen Stromausgängen nicht im Fokus.
Für die funktionale Sicherheit ist eine funktionierende IT-Sicherheit die Basis.
FS wird eher als aktive Technik und IT-Sicherheit als passive Technik angesehen da die IT-Sicherheit auf Ereignisse reagieren muss und weniger vorbeugend arbeiten kann.
Die EN 62443 beschreibt die Notwendigkeiten für IT-Sicherheit ausreichend und sollte als Basis dienen. Die EN 61511 verweist auf die EN 62443.

Bei SPSsen war IT-Sicherheit schon immer eine Grundfunktion. Durch die nun fortschreitende Vernetzung wurde diese Aufgabe komplexer. SIL und SAL sollten getrennt behandelt werden, auch weil man bei SAL nicht rechnen kann.
Bei der CASS gibt es einen Arbeitskreis, der sich um Bedrohungen wie Drohnen und ähnlichem beschäftigt. Dieser wird zukünftig ein Regelwerk zum Thema veröffentlichen.
Der Hersteller muss sicherstellen dass von seinen Geräten keine Bedrohung ausgeht (z.B. Viren).
Der Hersteller muss die Risiken für den Betreiber nennen, z.B. durch Hinweise im Manual (Schnittstellen, Passwörter wie in der EN 62443 beschrieben).
Für Ethernet gibt es z.B. eine Achilles-Zulassung (Bescheinigung) die aussagt wie robust die Geräte gegen Angriffe sind (https://www.ge.com/digital/products/achilles-vulnerability-testing-platform) oder Penetration-Tests (z.B. bei kanadischen Firmen). Solche Tests sind momentan noch nicht vereinheitlicht und werden von Kunden gelegentlich verlangt. Zukünftig wird sich hier noch viel verändern und hoffentlich auch vereinheitlichen. Bei analogen Geräten besteht wenig Handlungsbedarf, bei SPSsen ist der Punkt unbedingt zu beachten. Aus Marktdruck wird es vermutlich Herstellererklärungen oder Zertifikate geben die Aussagen zur IT-Sicherheit machen.
Die Anlage ist bei Lieferung zwar autark, aber wenn sie eine Verbindung nach außen hat muss der Betreiber eine geeignete Schutzmaßnahme vorsehen. Prinzipiell ist der Betreiber verantwortlich – wenn nicht anders delegiert. Ein Delegieren ist aber nicht ohne Weiteres möglich da Zugriff auf Personal nötig (disziplinarisch).
b. Das Thema wird nur selten von Prüfstellen mit behandelt da der prozessrelevante Teil in vielen Geräten abgeschottet ist und die Aussage gegeben wird, dass niemand direkt auf sicherheitsrelevante Parameter zugreifen kann.
Aus Maschinensicht: Die EN 62443 ist noch nicht harmonisiert. Im Rahmen der Risikobeurteilung wird die Internet-Security schon mit betrachtet, aber da Vernetzung der Anlagen erst langsam Einzug hält gibt noch keine allgemeingültigen Handlungsmaßnahmen. Es ist kein KO-Kriterium wenn in einem Feldgerät keine Maßnahme implementiert ist.

3. SIL bei mechanischen Komponenten, z.B. Hauptventile, die die eigentliche Aktion der Sicherheits-funktion ausführen. Üblicherweise kommen immer wieder die Diskussionen auf, dass die Mechanik einer SIL-Sicherheitsfunktion (SIF) immer von der IEC 61508 (E/E/PE) ausgenommen sei. Entweder sollte in einer Normen-Überarbeitung ein Hinweis, z.B. in der Einleitung, eingestellt werden, der die SIF-ausführende Mechanik einschließt in der SIL-Betrachtung oder es sollte eine eigenständige Norm in Anlehnung an die IEC 61508 für Mechanik erarbeitet werden. Gibt es dahin gehend einen Fort-schritt oder eine Planung bei den IEC-Normungen, damit die Diskussionen über den mechanischen Teil des SIS reduziert/ vermieden werden können?

Aktuell läuft bei der EN 61508 nichts in diese Richtung da sie per Definition für elektrische/elektronische/programmierbar elektronische Sicherheitsfunktionen vorgesehen ist. Die EN 13849 behandelt explizit auch Mechanik. Die EN 13849 gilt für den high demand mode, für low demand kann die EN 61511 mitverwendet werden. (siehe EN 61508-1, Kap. 1.2, Anmerkung 4) .
Es muss üblicherweise ein Eignungsnachweis erbracht werden über eine Prüfung in der Anwendung (für das Medium, für die Umgebung, für die Anforderung).
Für Mechanik werden oft keine Ausfallraten spezifiziert da es weniger um zufällige Ausfälle geht sondern um Überlastungen oder Ermüdung die sich nach Weibull verhalten. Daher ist eine

Berechnung nach Regeln der SIL-Welt nicht direkt möglich. Wenn z.B. Ventile korrekt ausgelegt nach einer gültigen Norm und geeignet für die Anwendung sind gibt es keine zufälligen Ausfälle (Systematische Fehler). Die Berechnung sollte nur da ausgeführt werden wo berechnet werden kann, der Rest kann verbal begründet werden (z.B. über Eignung nach traditionelle Normen).

4. Wann werden die PFD-Formeln, mit Berücksichtigung des PTC-Wertes, z.B. in der neuen VDI/ VDE2180-4, veröffentlicht? Wie soll jetzt der PFD-Wert mit PTC-Wert des Herstellers berechnet werden, obwohl es noch keine veröffentlichten PFD-Formeln hierzu gibt?

Zukünftig werden die Formeln in Blatt 3 der VDI/VDE 2180 zu finden sein.
Für einkanalige Systeme ist die Formel schon jetzt in Handbüchern von Emerson gegeben, für mehr-kanalige Systeme wird es bald die neue Ausgabe der Norm geben. Momentan ist kein Datum für die Freigabe bekannt. Für 2 kanalige Systeme gibt es eine Grundlage in der EN 61508 Teil 6, daraus kann auch Weiteres hergeleitet werden.
Alternativ kann man alte Formeln verwenden und zusehen, dass die Prüftiefe möglichst hoch ist. O-der (teure) Tools verwenden.

5. Fallbeispiel unvollständige Wiederholungsprüfung: Ein Hersteller lässt sein Produkt für SIL3 für die Betriebsarten „low demand“ und „high demand“ von einer Prüfstelle zertifizieren. Über eine versprochene Gebrauchsdauer von 10 Jahren kann der Anwender drei verschiedene Wiederholungsprüfungen (einmal jährlich) laut Safety Manual durchführen: 1. Einfache Prüfung: Prüfung durch Anwender im eingebauten Zustand, PTC = 23%; 2. Erweiterte Prüfung: Prüfung durch Anwender im eingebauten Zustand, PTC = 35%; 3. Werksprüfung des Herstellers: ausbauen, einschicken, prüfen lassen durch Hersteller, PTC = 37%; d.h. der Hersteller kann 63% der unentdeckten, gefährlichen Fehler nicht erkennen und das Gerät dann auch nicht in einen „Wie-Neu-Zustand“ versetzen?

Vorgehen hier nach traditionellen Normen wie z.B. Flammenwächter nach EN 298 - keine Berechnung nötig.
Andere Möglichkeit: Wenn λdu nur 10 fit sind, ist eine prüftiefe von 30% egal. Das Gerät ist dennoch sicher über Jahre einsetzbar.

 Muss der Anwender zu Sicherstellung eines „Wie-Neu-Zustands“ nach der Wdh.-Prüfung dann das Alt-Gerät durch ein Neu-Gerät (kein instandgesetztes Gerät) austauschen?

PFDavg berechnen, und wenn diese in Ordnung ist, dann nicht. Wenn „wie neu“ unbedingt gefordert wird dann muss getauscht werden, ist aber nicht nötig wenn die PFDabvg geeignet ist (siehe EN 61508-2 Cl. 7.6.2.3 Anmerkung 2).
 Ist PTC = 37% vertrauenswürdig, um dieses Produkt einzukaufen und zu betrieben?

Eine NE106 ist in Vorbereitung. Diese wird solche generischen Werte liefern, aber Vorsicht, da jeder Hersteller eigentlich unterschiedliche Prüfungen vorgibt. Die 37% sind geeignet wenn der FIT-Wert gering genug ist.
 Ist bei einer SIL-Zertifizierung das Safety Manual des Herstellers (mit solchen PTC-Angaben) eigentlich zwingend vorzulegen und Prüfbestandteil?

Ja
 Wird die SIF-Betriebsart zwischen dem Hersteller und der Prüfstelle bei einer Produkt-Zertifizierung diskutiert?

Vorher Eignung (auch für den erforderlichen Demand Mode) des Gerätes prüfen.
 Wird die vollständige und unvollständige Wiederholungsprüfung zwischen Hersteller und Prüfstelle bei einer Produkt-Zertifizierung diskutiert, wie Angaben der verschiedenen PTC-Werte (proof test coverage)?

Ja. PTC war früher nicht im Fokus, wenn Zweifel beim Hersteller nachfragen.
 Wie ermittelt ein Hersteller seine PTC-Werte, die die PFD-Berechnung und SIL-Einstufung während der „Useful lifetime“ (Gebrauchsdauer) beeinträchtigen können?

Beim Proof Test geht es darum, die gefährlich undetektierten Fehler aufzudecken. Das kann meist anhand der FMEDA nachvollzogen werden.

6. Bei mechanischen Komponenten mit SIL-Anforderung in einer SIF wird immer wieder zwischen Hersteller, Prüfstellen und Anwendern diskutiert über die Verwendung der richtigen SIL-Kennzahlen bzw. die SIF-Betriebsart des Equipments. Es wird oft auch die normale Betriebsfunktion mit der eigentlichen SIF verwechselt. Warum werden diese beiden Funktionen nicht explizit für das Equipment in der Herstellererklärung oder dem TÜV-Bericht oder dem Safety Manual definiert, um Missverständnisse zu vermeiden und damit der Anwender ganz klar erkennen kann, ob er die angegebenen SIL-Kennzahlen auch in seiner Anwendung verwenden kann?

Antwort siehe Frage 3.

7. Viele Hersteller verwenden Normen und Kennzahlen, die eigentlich für die Anwendung im „high/ continuous demand mode (HDM)“ (z.B. ISO 13849, EN 13611, EN 62061) gedacht sind, rechnen den PFH in einen PFD um und übersetzen den PL in ein SIL, obwohl explizit in der Tabelle der ISO 13849 darauf hingewiesen wird, dass die „Übersetzung“ PL in SIL nur für HDM gilt. Man findet viele TÜV-Testberichte, in denen nach ISO 13849, EN 62061 und EN 61508 geprüft wurde, die von Herstellern für den „low demand mode(LDM)“ zur Verfügung gestellt werden. Ist diese Umrechnung der SIL-Kennzahlen eine von Prüfstellen akzeptierte Vorgehensweise? Wenn ja, dann auch wenn die Fehler im HDM (Verschleiß, B10, Schalthäufigkeit) nicht gleich der Fehler im LDM (Festsetzen, Klebenbleiben, fehlende Beweglichkeit) sind?

Siehe Frage 9
Bei Elektronik ja, bei Mechanik mit Verschleiß (auch Relais) nein. Der Anwender darf die Umrechnung nicht machen wenn die PFD auf Basis der EN 13849 berechnet wurde, denn diese ist auf high demand ausgelegt. Der Hersteller muss die Daten für high und low demand liefern, da der Kunde nicht raten kann.
Beispiel: ein Gerät mit Relaisausgang, das nur 1x im Jahr schalten soll. Hier kann eine Evaluierung nach high demand nicht direkt auf low demand umgerechnet werden. Hier kann die Siemens Norm SN 31920 benutzt werden.

8. Wie ist mit der "Useful Lifetime" umzugehen? Was besagen Herstellerangaben? Regulatorische/Konstruktive Lebensdauer - Was muss der Hersteller, was der Betreiber tun? - Etablierung in den Regelwerken? Betreiber wollen keine Einschränkung in den Geräten haben. Geräte sind doch kein Joghurt.

Betreiber müssen sich grundsätzlich an die gegebenen Daten halten, da es Produkte mit z.B. flüchtigen Stoffen in Kunststoffen und Schmiermitteln gibt, die die Eigenschaften des Gerätes oder Produktes beeinflussen. Alterung z.B. durch Korrosion ist auch nicht zu unterschätzen.
Wenn bewusst Maßnahmen ergriffen werden die Lebensdauer zu verlängern (klimatisiert, nicht über 40°C) dann kann auch länger verwendet werden. Der Anwender muss die Eignung dann selbst verantworten. Es ist aber möglich dass Lambdawerte nicht weiter gelten weil sie auf anderen Annahmen basieren.
Situation: Ein Final Element (FE) ist Bestandteil einer SIF im LDM. Zusätzlich wird dieses FE für "Nor-mal Operation" mitgenutzt durch stündliche Zu- und Abschaltung.

9. Frage: Eine SIL Bewertung wird für diese SIF im LDM ausgeführt. Für die Berücksichtigung des Verschleißes des FE wäre eine zusätzliche SIL Eignung im HDM erforderlich?

Wenn die Anforderung im low demand anfällt, aber eine Nutzung des „Schalters oder Relais“ öfter (nach high demand) geschieht, müssen für die Berechnung der Ausfallraten die Werte des high demand verwendet werden um Verschleiß zu berücksichtigen:
PFH = λdu
PFD = λdu*T1/2 nicht wissen wie oft,
Üblicherweise wird λ aus dem B10d-Wert ermittelt bei häufiger Betätigung. Bei Nutzung nur nach low demand muss auf andere Effekte (z.B. Korrosion) eingegangen werden.

Situation: Die Risiko-Bewertung von Maschinen (z.B. Kompressoren) kann nach der IEC 62061 bzw. der ISO 13849-2 erfolgen. Gemäß IEC 62061 under 3.2.27 Note 1: " Low demand mode of operation is not considered to be relevant for SRECS (Safety-Related Control Function) applications at machinery. Therefore, in this standard SRECS are only considered to operate in the high demand or continuous mode."gibt es keine LDM für Maschinen.

10. Frage: Es werden Maschinen in Prozessanlagen mit LDM eingesetzt. Warum wird die IEC 62061 nicht harmonisiert, so dass Maschinen im LDM bewertet werden können?

ISO 13849 und IEC 62061 beschreiben auch low demand, aber es wird hingewiesen dass Maschinen üblicher Weise nicht im low demand mode betrieben werden. Warum die IEC 62061 nicht harmonisiert ist, ist nicht bekannt. Wenn aber keine harmonisierte Norm existiert darf eine nicht harmonisierte herangezogen werden. Daher eigentlich kein Problem.
Es geht nicht darum nach welcher Norm ausgelegt wird sondern welche Anforderungen die Risiko-analyse ergibt. Danach wird entschieden welche Norm verwendet wird.
Emergency Stop Push Button für Maschinen Not Halt: IEC 61511-1: Under 11.2.8: "Manual means (e.g. emergency push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by SRS."

11. Frage: Der ESD Taster für einen Maschinen Not Halt sollte direkt zur Schaltanlage verdrahtet werden, also nicht via Safety PLC (falls es keine anders lautende Aussage in der SRS gibt). Wäre das so richtig interpretiert?

In der deutschen Version liest sich dies anders. Hier ergibt sich, dass ein Nothalt vorgesehen werden muss, aber es geht nicht daraus hervor, dass dieser an der PLC vorbeigehen muss. Es muss allerdings ein manueller Nothalt unabhängig zu den Aufgaben der PLC möglich sein.
Hier muss allerdings Prozess (IEC 61511) oder Maschine (ISO 13849) unterschieden werden. Die IEC 61511 beschreibt nicht die technische Lösung sondern die Anforderung.
Ich habe zwei Fragen zur funktionalen Sicherheit, die für mich ineinander übergehen, obwohl diese in der EN 61508/511 getrennt sind.

12+13: Thema: Nutzung von SIS-Armaturen für betriebliche Zwecke und der SIL-Nachweis der Gerätekombinationen im SIF sowie Definition von Low und High Demand bei SIS-Armaturen mit betrieblichen Aufgaben.

Ich habe vom Prozess die Vorgabe im BPCS Ventile als Doppelblock auszuführen. Für SIL2 Schutzeinrichtungen, die ich in HFT1 ausführen möchte, habe ich dann leider nur noch ein Ventil über so dass ich eine HFT0-Instalalltion hätte. Ich habe Ventile mit SIL2-Daten, so dass ich auch ein PFD_average für HFT0 für SIL2 über alle Subsystem (Sensor, Logic Solver und Final Element) nachweisen kann.
Dennoch bekomme ich bei der TÜV-Zertifizierung häufig die Vorgabe ein SIL2 für die Aktorik in HFT1 auszuführen (wäre nach EN 61511/508 die Mindestforderung für SIL3). Für Sensorik nicht – ok die Mechanik der Aktorik ist anfälliger.
Damit habe ich SIS-Ventile, die betriebliche Schaltungen übernehmen (Verriegelungen und Schaltungen aus der Phasenlogik des BPCS – Batch-Anlage). Es würde für die Sicherheitsschaltungen beim Low Demand bleiben. Es gibt auf der Sensorseite diversitäre Redundanzen (z.B. Überdruck im BPCS durch

Transmitter abgefangen, die SIS-Abschaltung durch höher eingestellten Schaltpunkt eines Kontakt-manometers).
Die Einbausituation stellt sich wie folgt dar: *siehe Bild*
Der Demand ist nur für Sicherheitsschaltungen definiert. D.h. solange ich nur eine Schaltung durch SIS-Trips im Jahr habe und nicht öfter als zweimal im Jahre prüfe, habe ich einen Low Demand. Nun gibt es aber noch recht viele Schaltungen aus dem Batch-Teil des BPCS zum SIS. D.h. die SIS/BPCS-Armaturen werden bis zu 750 mal im Jahr bewegt. Da die Armatur und auch der fehlersichere Digital-Ausgang nicht zwischen betrieblicher und sicherheitsgerichteter Schaltung unterscheiden kann, wäre dies für mich ein High Demand (auch wenn es nur eine Sicherheitsschaltung im Jahr gibt).
Wenn ich beim Low-Demand bleibe, dürfte ich für das 1oo2 Aktorsubsytem eine PFD-Rechnung machen. Ich glaube aber, das ist nicht das Ziel der EN 61508/511, sicherheitsgerichtete Armaturen mit hunderten betrieblichen Schaltungen zu belegen.
Theoretisch dürfte ich nun keine PFD-Analyse unter Verwendung des Proof-Test-Intervalls für das 1oo2 Aktorsubsystem durchführen (Für die reine SIS-Armatur kann ich aber den SIL2-Nachweis für 1oo1 HFT0 erbringen).
Siehe Frage 9, Nutzung der Ausfallraten von high demand, aber Berechnung nach low demand.

14. Wie ist die geforderte Risikoabschätzung für das 1oo2 HFT1 Aktorsubsystem zu erbringen? Für einen Fault Tree der Aktorik fehlen mir die Daten.

Wie zuvor beschrieben ist evtl. kein Rechnen nötig sondern die Anwendung anderer Normen zur Aus-legung. Falls generische Zahlen vorhanden sind könnten diese benutzt werden.

15. Kann analog zum High Demand eine PFH-Analyse für das 1oo2 HFT1 System durchgeführt wer-den respektive ist dies akzeptiert?

Die EN 61511 empfiehlt zwar eine Trennung SIS/BPCS (also ein Ventil mehr in meiner Anwendung), spricht aber bei Nichttrennung nur von zusätzlichen Nachweisen ohne ins Detail zu gehen.
Die Sicherheitsfunktion hat Priorität. Das muss sichergestellt werden sonst wurden alle Notwendigkeiten schon in anderen Fragen betrachtet. Das Restrisiko muss vertretbar sein (und die Beurteilung dokumentiert).

16. Inwieweit kann eine Betriebsanweisung die Einstufung einer PLT-Schutzeinrichtung beeinflussen bzw. kann eine Betriebsanweisung eine PLT-Schutzeinrichtung "ersetzen"? Gibt es grundsätzlich Unterschiede in der Bedeutung einer Betriebsanweisung zwischen Prozesssicherheit und Maschinensicherheit?

Es kann durchaus vorkommen, dass bei langsamen Abläufen (Prozess) auch der Mensch eine Aktorik ersetzen kann. Dann ist dafür eine Betriebsanweisung nötig (ebenso eine ständige Schulung des Personals die ebenfalls dokumentiert wird). Beispiel Prüfung der Funktion von Schiebern.
In der Maschinenwelt eher nicht. Hier muss erst die Aktorik die SIF ausführen und wenn dies nicht geht oder die Aktorik ausfällt, dann kann der Mensch (mit Schulung und Anleitung) dies durchführen.

Grundsätzlich gilt für die Realisierung der SIF die Reihenfolge: Technisch, organisatorisch, persönlich.

17. Eine Frage zur Berechnung von mechanischen Komponenten im Low-Demand-Mode: Bei Relais und Schützen ist normalerweise nur ein B10/B10d-Wert angegeben. Alternativ sind die Werte aus der ISO 13849 zu verwenden. Daraus lässt sich dann der PFH für den High Demand Mode errechnen. Wie kann ich derartige Komponenten in SIL-Kreisen im Low-Demand-Mode einsetzen? In der Praxis gibt es diese Konstellation leider relativ oft. Auch ein Kunde fordert aktuell eine Berechnung im Low-Demand-Mode für einen SIL-Kreis mit einigen Hilfsschützen.

In der Siemens Norm SN 31920 wird der Unterschied erklärt. Kap. 4.3 für HDM und Seite 12/25 für LDM. Umrechnung ist nicht immer möglich, z.B. B10d nicht sinnvoll bei < einer Anwendung pro Jahr. Wenn 1x am Tag geschalten wird dann high demand Werte verwenden (Siehe auch Siemens Dokumenten-Nr. 802-9145.9, SF6-Schalter_SiL_Claim level NXPLUS C).

10. SIL-Sprechstunde 2018

1. Der TÜV Rheinland verfolgt derzeit eine Initiative, mechanische Komponenten mit ähnlichen Methoden wie elektronische zu bewerten (Auftreten zufälliger Fehler). Wie bewerten Experten diesen Ansatz, der bei den Betreibern Verwunderung auslöst?

Ausfälle mechanischer Bauteile werden üblicherweise nicht als zufällige Ausfälle betrachtet.
Für die Entwicklung von Geräten mit mechanischen Komponenten werden
Normen verwendet die mit Sicherheitspuffer arbeiten um über die Lebenszeit die
Funktion zu garantieren. Solche Regelungen werden als nicht sinnvoll erachtet und
auch von TÜVs wird diese Sicht in der Normung unterstützt. (TÜV Süd)
Laut Kommentar aus dem Publikum wird dieser Ansatz in Skandinavien schon benutzt,
es hatte aber noch niemand konkrete Erfahrung damit.
In der Produktnorm für thermische Relais gibt es einen ähnlichen Ansatz. Vielleicht
kann das als Anregung gelten. Die Ausfallraten für zufällige Fehler werden aber als
insignifikant angesehen.
Bei Normen zu Sicherheitsarmaturen wurde dieser Gedanke schon verfolgt, ein Anhang,
als mögliche Lösung, wird aber wie oben geschildert als unnötig gehalten. (Dr.
Karte)
Für Betreiber ist nur die Eignung in der Applikation wichtig, eine Norm mit Fehlerraten
erscheint nicht nötig.

2. Spurious trip level (STL): Wie ist die Aussagekraft von dem STL und wie ist das Verhältnis zum PFD? Sollte man den STL zusätzlich zum SIL bestimmen oder halten Sie diesen für komplett überflüssig?

Eine PFD oder PFH mit Angabe zu Verfügbarkeit genügt. (HIMA)
Die Angabe eines STL im Sicherheitshandbuch macht wenig Sinn, da er nur eine
nicht sicherheitsrelevante Aussage zur Verfügbarkeit darstellt. (BASF)
Wenn der Betreiber dies möchte kann er sich diesen selbst ausrechnen, daher muss
der Hersteller dies nicht angeben. (E+H)

3. Für betriebsbewährte Sauerstoffmessungen gibt es in der NE130 keine Ersatzwerte. Ist es ausreichend 1000 FIT (worst case Wert für Sensorik in der NE130) anzunehmen oder sollte man mit anderen Werten rechnen?

Bei Geräten ohne Angaben sollte man eine relevante Aussage mit Betriebsbewährung
untermauern, redundant ausführen oder den Hersteller wechseln.
Dies ist ein Fall aus der Prozess und Analysetechnik, dort gilt die NE146. Am besten
auf eine eigene Datenrate zurückgreifen, sonst evtl. 10 000 FIT annehmen wenn die
Datenbasis zu gering ist. Die Aussage dann über der Zeit im Betrieb prüfen und
Dokumentieren,
da diese besser belastbar ist als angenommene Werte.
Wichtig ist es, vorab eine geeignete Risikobewertung für die Anlage zu erstellen.
Eher bei betriebsbewährten Geräten bleiben als unbekannte neue zugelassene Geräte
verwenden. (Fa. HIMA)
IEC 61508/ IEC 61511 sind internationale Normen, die als „Richtlinie“ freiwillig umzusetzen
sind und keinen Gesetzes-Charakter haben. Diese Normen sind keine „harmonisierten“
Normen, wie z. B. die EN ISO 13849 (für HDM), die den Komponenten-
Lieferanten oft und gerne als Prüfgrundlage dient, auch wenn sie ihre Komponenten
für den LDM „anbieten“. Innerhalb der EU wird die Funktionale Sicherheit verbindlich
als „Stand der Technik“/ „Stand der anerkannten Regeln der Technik“ eingefordert

und muss von allen Beteiligten demonstriert werden (können).
(a) Außerhalb der EU und der USA sind die „Funktionale Sicherheit (FS)“ und IEC 61508/ IEC 61511 nach bisheriger Erfahrung kein Thema, obwohl die Normen international zu sehen sind. Gesetzliche Regelungen zur FS sind meist auch nicht für das Land vorhanden, in welchem die Anlage gebaut und betrieben wird, auch keine ähnliche Anforderungen zur FS.

4. Wie soll in internationalen Projekten (für Anlagenbau, außerhalb EU/ USA) damit umgegangen werden, vor allem wenn es weder gesetzliche noch vertragliche Anforderungen für die FS gibt? Ist es fahrlässig, auf Grund der vermeintlich zusätzlichen Kosten, die FS in diesem Fall dann nicht zu berücksichtigen?

Selbst wenn die EN/IEC 61508 nicht genannt wurde verweisen heutige Sicherheitsnormen auf diese. Daher ist die Anwendung doch nicht ganz freiwillig. (E+H)
Laut BGH Urteil ist der Stand der Technik anzuwenden oder es gelten lokale Anforderungen im Zielland falls höher. Die benutzte Argumentation sollte schriftlich festgehalten werden und es muss vom Planer ein Hinweis auf Gefahren im Betrieb geben.
Konkretisierung der Fragestellung: Auftraggeber in Indien und Afrika geben ganz klar die Vorgabe auch wegen des Preises nicht nach 61508 zu entwickeln.
Laut Gerichten gilt das Recht des Landes, in dem die Anlage erstellt und betrieben wird. Daher muss die juristische Lage im Zielland beachtet werden. Bei Planung in Deutschland ist heute aber auch eine Klage in Deutschland wegen Nichtbefolgung deutscher Regelungen möglich.
Gefährdungsbeurteilungen müssen lokale Gefahren berücksichtigen, denn in der Wüste sind z.B. andere Gefahren zu berücksichtigen als in Mitteleuropa.
Die Auslegung kann nicht Aufgabe des Fachplaners sein, wenn die Vorgaben nicht in der Sprache zur Verfügung stehen die der Fachplaner versteht.
Prüfen, ob das Zielland den Regelungen von IEC oder ISO unterliegt, dann gilt die 61508 auch wenn der Auftraggeber dies nicht möchte. Eine abschließende Bewertung kann aber nur ein Jurist für den betreffenden Einzelfall vornehmen.
In SIL-Zertifikaten werden diverse SIL-Normen als Prüfgrundlage herangezogen, z. B. zeitgleich EN ISO 13849, EN 62061 und EN 61508, die in Kombination sehr wahrscheinlich nur den HDM darstellen („Übersetzungstabelle“: PL => SIL), Laut Kennzahlenliste wird hier gerne auch der PFD-Wert für den LDM angeben (ohne weitere Hintergrundinformationen für den Anwender, ob der Anwendungsfall LDM eintritt).
Nicht immer ist für eine Detailprüfung ein Prüfbericht verfügbar. Anhand der im Sicherheitshandbuch
oder im TÜV-Beiblatt angegebenen Kennzahlen kann aber angenommen werden, dass Lambda du (LDM) = Lambda du (HDM) = PFH gesetzt wurde.
Die Fehler zum Verschleiß (häufige Nutzung, HDM) eines Geräts sind üblicherweise nicht gleich der Fehler durch „Festsetzen“ (seltene/ keine Nutzung, LDM).

5. Wie soll der Anwender damit umgehen, damit er nicht fahrlässig handelt?

Wenn der Flammenwächter nach EN 298 ausgelegt wurde ist dies geeignet nachgewiesen. (TÜV Süd)
Bei Schützen werden oft unterschiedliche Angaben für high und low demand mode angegeben. Eine einzelne Angabe wird aufgrund der Abhängigkeit von mechanischen Belastungen stark hinterfragt. Wenn es um ein rein auf Leistungselektronik basiertes Gerät geht ist das aber möglich.
Wenn nur low demand mode angegeben ist wird nur die EN 61508 betrachtet – andere genannte Normen betreffen nur den high demand mode.

6. PTC-Angaben: Sofern der Gerätehersteller (und ggfs. sein Prüfer) keine Angaben zu einer „unvollständigen Prüfung“ und den PTC-Werten in den einschlägigen SIL-Unterlagen (wie Zertifikat/ Erklärung, Testbericht, Sicherheitshandbuch etc.) angibt, darf der Anwender davon ausgehen, dass PTC = 100% ist (z.B. wenn nur eine Prüfanweisung vorhanden ist)?

Endress und Hauser nimmt 98% bei Grenzwertprüfung an, wenn mit dem Medium geprüft wird. Bei Simulation mit verschieden Werten muss der Hersteller die Prüftiefe angeben.
Pepperl+Fuchs rüstet Safety Manuals nach, gibt für viele Interface-Geräte 100% PTC an da alle Abweichungen in der Übertragungskennlinie (was gefährlich wäre) extern beobachtet werden können.
Gebrauchsdauer und „Mission Time“ sowie die Verfahren der Namur NE 106 sind zu beachten.
Hersteller/ Prüfstellen geben PTC = 0% an und setzen das Intervall der Wiederholungsprüfung (TI) gleich mit der Lebensdauer des Geräts (z.B. T = 20 Jahre), u. a. für die Angabe des PFD-Wertes. Die PFD-Berechnungen unterstellen gewöhnlich PTC = 100% statt PTC = 0%, oder?

7. Wie soll der Anwender mit der Herstellerangabe PTC = 0% umgehen? Der Hersteller gibt auch an, dass das Gerät wartungsfrei ist und ohne jegliche Überprüfung bis zu 20 Jahre betrieben werden kann, so dass es auch keine Prüfanweisungen zum Gerät (bzw. auch kein Sicherheitshandbuch) gibt.

Ein PTC =0 unterstellt, dass keine Prüfung nötig ist. Wenn eine sehr wirksame Diagnose vorhanden ist oder die geringe PFD/PFH Angaben sehr klein sind, spielen die gefahrbringenden Fehler keine Rolle mehr, daher ist keine Prüfung notwendig. Systematische Fehler sind zu beobachten da diese hier große Auswirkungen haben.
Relais gehören trotzdem geprüft, ebenso Aktorik im Feld ohne direkte Rückmeldung.

8. Ist es aus Sicht des Systemintegrators ausreichend, wenn unterstellt wird, dass das Gerät in der Gesamtprüfung der SIL-Kreis-Kette (z.B. jährlich) mit geprüft wird?

Prüfintervalle sollten immer hinterfragt werden, bei Geräten bei denen systematische Ausfälle zu befürchten sind, sind häufigere Prüfungen sinnvoll als durch PFH/PFD bestimmt. Bei > 20 Jahren sollte zumindest häufiger externe Beschädigung angeschaut werden.

9. Ist es bei einem rechnerischen Nachweis ausreichend, wenn der Anwender mit dem Herstellerwert PFD (T = 20 Jahre, PTC = 0%) ins Rennen geht? Wenn nicht, wie lauten die Maßnahmen, die der Anwender ergreifen sollte?

Siehe 8. Nur bei Schaltraumgeräten, nicht bei Medienkontakt. (BASF)
Wie lange möchte ich die Anlage ohne Unterbrechung betreiben. Prüffristen nur auf Grundlage der PFD ist nicht geeignet.
Einige Hersteller, deren Geräte auf dem Markt als „konform mit der IEC 61508“ angeboten werden, besitzen (immer noch) kein Sicherheitshandbuch (gem. IEC 61508-2, Annex D) für ihre konformen Geräte. Der Anwender / Systemintegrator ist auf dieses Handbuch (oder etwas inhaltlich Vergleichbares) angewiesen, um bewerten zu können, ob er das Gerät in der gewünschten Applikation einsetzen kann. Gerade wenn Testberichte (mit wichtigen Anwenderinformationen) als „vertraulich“ eingestuft wurden und nicht veröffentlicht werden, muss das Functional Safety Manual oder das Kapitel „Funktionale Sicherheit“ im IOM die Grundlagen liefern, wonach der Systemintegrator

die Geräte prüfen kann.

10. Wie soll der Anwender damit umgehen, wenn der Hersteller nicht die standardmäßig benötigen Informationen zur Verfügung stellt bzw. nicht zur Verfügung stellen will?

Der Hersteller muss die Werte für die Berechnung liefern.
Wenn kein Sicherheits-Handbuch verfügbar ist dann ist das Gerät nicht konform bezüglich der Ed2 der EN 61508. Das Dokument darf anders heißen – die Information muss verfügbar sein.
Wenn keine interne Diagnose verwendet wird dann reichen PFD, PFH und PTC, es sind evtl. keine Lambda Werte gegeben. (Anm.: für Redundanz sind die Lambda-Werte oft doch nötig, siehe Formeln in 61508-6)

11. Brauchen wir eine unterschiedliche Vorgehensweise bzgl. Cybersecurity für BPCS und SIS? Wenn ja, warum und worin unterscheidet sie sich?

Man muss nicht trennen, es kann aber sinnvoll sein zu trennen. Die TR 63069 liefert Hinweise.
Unter keinen Umständen darf ein Unberechtigter in die Anlage kommen, egal ob Sicherheitseinrichtung
oder Betriebseinrichtung. Wenn keine Sicherheitseinrichtung betroffen ist kann das anders sein. (Lanuv)
NAMUR-Arbeitsblatt NA 163 behandelt diese Anwendung und beschreibt auch Maßnahmen, derzeit das verständlichste Werk mit klaren Vorschlägen.

12. Wann wird DIN EN 61511 Edition 2 veröffentlicht? (wegen Fehler seit 2016 zurückgestellt)

Januar 2019 ist geplant. Die englische Version ist schon verfügbar.
Ein weiterer Teil soll erscheinen, in dem Änderungen zur alten Version und Erklärungen enthalten sind.

13. Die Hersteller von Antrieben und Stellgeräten, die in PLT-Schutzeinrichtungen eingesetzt werden, stellen zunehmend Anforderungen an den Betreiber und versuchen, die Verantwortung klar abzugrenzen. Anforderungen sind beispielsweise: Beschränkung der Einsatzdauer, jährliche Funktionstests, Wartung nach Schaltspiel oder Einsatzdauer, Inspektionen und Instandsetzung nur durch zertifizierte Werkstätten. Wie stehen die Betreiber dazu?

Anderen Hersteller suchen. Die Gebrauchsdauer liegt beim Betreiber. Die in der Norm aufgeführten 8-12 Jahre gelten für Elektronik. Für mechanische Geräte macht das keinen Sinn. (Dow)

14. Sind nach der neuen Ausgabe der IEC 61511 betriebsbewährte Geräte nötig um SIL 2 einkanalig zu instrumentieren?

Die neue Ausgabe stellt klare Anforderungen an die Zuverlässigkeit. Entweder durch Zuverlässigkeitsnachweis oder nach EN 61508 entwickelt.

15. Der TÜV Rheinland treibt beim CEN vehement die Betrachtung und Bewertung von mechanischen Komponenten analog zu elektronischen Komponenten. Nach Auffassung der Betreiber ist dies nicht sinnvoll, weil mechanische Komponenten keinen zufälligen Ausfällen unterliegen, sondern Fehler immer eine systematische Ursache haben. Wie sehen die Experten dieses Vorgehen?

Siehe Frage 1

16. Wie sehen die aktuellen Zahlen der NE 93 aus, ergeben sich grundsätzliche neue Erkenntnisse?

Die Zahlen werden über das Namur Smart Tool gesammelt. Daten werden noch gesammelt, haben aber noch keine belastbaren Ergebnisse geliefert aus denen sich eine Konsequenz ableiten würde. Die NE130 wird überarbeitet, die Zahlen sollen in die NE93 übergehen. (BASF)

17. Welche juristischen Konsequenzen hat das Versagen einer Sicherheitsfunktion in den beiden nachfolgend geschilderten Fällen? Gibt es prinzipielle (juristische) Unterschiede zwischen den beiden Szenarien? Fall 1: Eine Sicherheitsfunktion versagt aufgrund eines Softwarefehlers (Der Programmierer hat eine Funktion fehlerhaft programmiert). Fall 2: Eine Sicherheitsfunktion versagt, weil ein Hacker die Software so verändert hat, dass diese gefährlich versagt.

1. War der Entwicklungsprozess für die Software geeignet wurde zumindest nicht fahrlässig gehandelt. Bei Versagen einer Sicherheitseinrichtung ist zuerst der Betreiber in der Haftung.
Juristische Entscheidungen sind nicht vorhersehbar, basieren auf dem Einzelfall.
Wenn der Betreiber ein Management der Funktionalen Sicherheit hat ist auch hier keine Fahrlässigkeit zu unterstellen. Die Nachweise müssen aber verfügbar sein.

18. Für einen Kunden wurde eine Detail-Planung zum Umbau einer Tankentladestation durchgeführt. Wie verhält man sich, wenn der Kunde zwar Sicherheitstechnik einsetzen möchte, jedoch keine Sicherheitsgespräche (HAZOP, Risikomatrix, PLT-Einstufung) für die neue Nutzung durchgeführt hat? Der Umbau soll auch ohne vorab durchgeführte Sicherheitsgespräche durchgeführt werden. Unter diesen Umständen ist eine normgerechte Planung nicht durchführbar.

Sicherheitsgespräche sind die Grundlage für die Planung, der Kunde hat hier nicht die Wahl. Die Gefährdungsbeurteilung ist Pflicht und basiert darauf. Regelwerke müssen eingehalten und angewandt werden. Wenn dies dokumentiert und begründet ist genügt dies.
Die Umbauten dürfen keine Sicherheitseinrichtung betreffen. Sonst muss eine Risikobetrachtung
durchgeführt werden. Die TRBS (Technische Regeln zur Betriebssicherheit) legen das Vorgehen fest.
Der Betreiber hat Daten zu liefern, der Planer kann nur auf das reagieren was er weiß. Wenn seine Arbeit dem Stand der Technik entspricht dann ist das geeignet, er muss aber deutlich machen wenn er seine Planung nur auf eingeschränkten Informationen basiert.
Die Basis der Planung dem Kunden liefern und auf evtl. notwendige Änderungen hinweisen. Auf keinen Fall in Betrieb nehmen wenn Zweifel an der Vollständigkeit der

Risikobeurteilung vorliegen.
Die NE130 schreibt sinngemäß in Kap.3 – Maximal erreichbarer SIL einer PLT-Schutzeinrichtung:
Wenn alle Geräte des Sensor- und Aktorteils einer PLT-Sicherheitseinrichtung den Status „Betriebsbewährt“ haben sowie der Logikteil (SSPS incl. E/A-Module) eine Zulassung für den angestrebten SIL-Level besitzt, kann auf einen rechnerischen SIL-Nachweis verzichtet werden und darüber hinaus die SIL-Strukturtabelle aus NE 130 verwendet werden.

19. Ist es bei der Auslegung von hybrid aufgebauten PLT-Sicherheitseinrichtungen (z.B. Sensoren „BBW“ und Aktoren ohne „BBW“, jedoch mit entsprechendem SIL-Level) zulässig, die NE130-Kanalrichtwerte der Sensorik ersatzweise für den rechnerischen SIL-Nachweis heranzuziehen? Falls nein, warum?

Die Zahlen der NE sind geschätzt. Nur wenn das Gerät bei der Schätzung zugrunde lag ist dies geeignet. Die Zahlen sind ein guter Ansatz, aber wenn der Hersteller selbst Zahlen liefert dann sind diese zu beachten und Prüfungen daran zu orientieren. Es sind nur Ersatzwerte. Vor der Verwendung erst Eignung des Gerätes prüfen.

20. Könnte ich mit vorgenannter Auslegung „Sensorik 1oo2-BBW und Aktorik 1oo3-ohne BBW“ strukturell ein SIL3-Level im Sinne der NE130-Tabelle erreichen? Falls nein, warum?

Mit der neuen EN 61511 geht das nicht mehr. Deterministik statt Probabilistik anwenden. Einzelfallbetrachtung, HFT erhöhen, ingenieursmäßig handeln. Es sollten Daten für die Eignung vorhanden sein, sonst ist es kein geeignetes Gerät für die Sicherheitseinrichtung (Medienberührung).

21. Thema "Bestandsschutz": Die Normen sind sehr vage (detailliertere Aussagen nur in NE 126). Betreiber legen die Definition "keine wesentliche Änderung" z.T. sehr weit aus und schlussfolgern dann, dass keine neue Sicherheitsbetrachtung erforderlich ist. Die Grauzone ist recht groß, aber m.E. wäre spätestens z.B. der Ersatz von Öl-Brennern durch Brenner mit anderen Brennstoffen (z.B. Gas) eine "wesentliche Änderung". Gibt es eine Grenze, ab der der LTLieferant dem Betreiber dringend eine neue Sicherheitsbetrachtung empfehlen sollte?

Bestandsschutz ist nicht definiert. Daher ist es eine Einigung zwischen Betreiber und Prüfer. Wenn das System gleich bleibt besteht üblicherweise keine Notwendigkeit zu handeln.
Wenn eine Steuerung ersetzt wird zählt das nicht als wesentliche Änderung.
Wenn von Ölfeuerung auf Gas umgestellt wird schon. Die Steuerung würde nicht mehr passen da auch die Temperaturen und Auslegungen der Bauteile nicht mehr passen.

22. Ist absehbar, wann die neue Ausgabe von VDI/VDE 2180 Blatt 4 verfügbar sein wird (mit PFD-Formeln für PTC < 100%)?

Gar nicht mehr, da Blatt 4 entfällt. Anfang 2019 soll die neue Auflage kommen. Blatt 4 wird Blatt 3.

23. Muss man bei einem SIL-Kreis mit einem Sensor, der 10 Aktoren abschaltet in der PFD-Nachweisrechnung für den Ausgang mit einer 10oo10 Funktion rechnen oder erstellt man 10 einzelne Berechnungen mit jeweils einem Sensor, der auf einen Aktor geht? Bsp: Überfüllsicherung an einem Behälter mit 10 Zulaufleitungen.

Es kommt auf die Sicherheitsfunktion und das Ausgangsrisiko an. Genauer gesagt kommt es darauf an, welches Ausgangsrisiko reduziert werden soll. Ist das Ausgangsrisiko, dass alle 10 Zuläufe gleichzeitig in geöffneter Stellung hängen bleiben, dann muss bei der Sicherheitsfunktion aktorseitig mit 10oo10 gerechnet werden. Ist das Ausgangsrisiko, dass einer der 10 Zuläufe nicht schließt, dann wird aktorseitig nur mit 1oo10 gerechnet.
Siehe Antworten von 2014
Die andere Konstellation, die mich interessiert wäre, wenn ein Sensor im Feld auf ein z. B. Kühlmittelzulaufventil wirkt aber es gibt mehrere Optionen für das Ansprechen des Sensors.
Beispiel: ein Reaktionsbehälter, in dem exotherme Reaktionen ablaufen, soll mittels einer Kühlschlange gekühlt und so vor Überhitzung geschützt werden. Die Überhitzung kann aus mehreren Gründen zu Stande kommen. Die Gefahrenquellen wären:
zu schnelle Katalysator Zugabe, falsches Edukt und dadurch zu schnelle Aufheizgeschwindigkeit,
zu schnelle Zugabe des richtigen Edukts, Rührerausfall, zu langsame Kühlung etc. Jede der o.g. Gefahrenquellen im Feld hätte das Aufheizen des Reaktionsbehälters
zu Folge. Und der soll eben gegen das Überhitzen geschützt werden.
Bei deterministischer Vorgehensweise üblich jede einzelne Gefahrenquelle einzeln zu betrachten, wie im folgenden Beispiel:
- 1. Quelle (S2, A1, G2, W1 ergibt SIL 1)
- 2. Quelle (S2, A2, G2, W2 ergibt SIL 2)
- 3. Quelle (S2, A2, G2, W3 ergibt SIL 3)

Die Eintrittswahrscheinlichkeiten sind hier lediglich als Größenordnung angegeben und nicht als konkrete Zahlenwerte. Bei deterministischen Vorgehensweise würde der o.g. Loop in SIL 3 ausgelegt. Bei Anwendung eines Fehlerbaumes müssten korrekterweise
die Eintrittswahrscheinlichkeiten (wenn Zahlenwerte vorhanden) addiert werden.
In der Gefährdungsanalyse muss jeder Sensor einzeln betrachtet werden, erst dann ist die Entscheidung zu fällen. Alle Dinge die zur Kühlung beitragen berücksichtigen. Die Risiken richtig betrachten, **Einzelfunktionen betrachten** und Risiken bewerten. Den höchsten SIL wählen.
Beachten dass die 3 Sicherheitsfunktionen nicht öfter als 1x im Jahr angefordert werden und damit nicht der high demand mode gilt. Ausschalgebend ist, wie oft die Temperatur unzulässig hoch ist.

24. In dem oben geschilderten Fall würden die Eintrittswahrscheinlichkeiten der einzelnen Gefahrenquellen addiert. Somit würde man im Risikographen mit der Eintrittswahrscheinlichkeit eines Schadens immer mehr nach links rutschen und die SIL wäre um eine Klasse höher ausfallen. Sehen sie das auch so? Was ist hier zu tun oder wie ist es bei einer deterministischen Vorgehensweise vorzugehen? Hier müssten die Wahrscheinlichkeiten doch auch addiert werden. Oder kommt bei einer deterministischen Vorgehensweise, d. h. ohne Zahlen für die Wahrscheinlichkeiten, die als Größenordnung angegeben werden, das Addieren gar nicht zum Tragen, weil es nicht möglich ist Größenordnungen zu addieren. Aber unerheblich kann das nicht sein. Was ist hier zu tun? Oder wird hier ein Denkfehler gemacht?

Gefahren können nur einzeln betrachtet werden und das Risiko das sich aus der Quelle ergibt eingeschätzt. Das Gesamtrisiko aus dem Betrieb einer Anlage ergibt sich immer aus sämtlichen Risiken und deren Abstellmaßnahmen, oft sind es nicht nur drei sondern eine dreistellige Anzahl Gefahrenquellen in einer Anlage. Es ist wichtig dass die ‚Layers of protection' geeignet gewählt werden. Falls das Schadensausmaß sehr groß ist weil man intuitiv den errechneten SIL nicht glaubt ist evtl. die Einstufung mit S=2 zu überdenken.

25. Gibt es (abgesehen von Einschränkungen durch die Reaktionszeit) grundsätzliche Einwände gegen standortübergreifende Sicherheitsfunktionen mit kaskadierten SSPS?

Prinzipiell ja. Es wird vermutet dass auch die Verfügbarkeit limitiert ist durch verteilte Funktionen mit Busleitungen – das wäre als Indiz für die Verlässlichkeit heranzuziehen. Wenn zusätzliche Risiken die sich aus dieser Konstellation ergeben beurteilt wurden ist das aber durchaus denkbar.

11. SIL-Sprechstunde 2019

1. Unter welchen Voraussetzungen kann die VDE 2180 auch für High-Demand Anwendungen herangezogen werden?

Die EN 61511 steht ursprünglich für Low Demand-Problemstellungen, ein großer Anteil der Norm kümmert sich aber um Vermeidung von systematischen Fehlern. Daher also auch für High Demand geeignet. (Hablawetz, BASF)
Aktorik unterliegt Verschleiß. Ebenso müssen Anforderungsrate und Diagnose betrachtet werden. Die Diagnose muss schnell genug arbeiten um zu wirken (Faktor 100). (Klotz-Engmann, E+H)
Es ist kein High Demand wenn das Ventil sich ständig bewegt, es muss betrachtet werden wie oft es auf eine Sicherheitsanforderung reagiert. (Hablawetz, BASF)
High Demand wenn > 1 Sicherheitsanforderung pro Jahr, klare Definition im Standard (EN 61508).

2. Wieso gibt es SIL-Daten für Magnetventile und auch für rein mechanische Armaturen?

Derzeit wird eine Norm mit Ausfallraten erarbeitet. Es wird aber angezweifelt ob Mechanik überhaupt signifikant zufällige Ausfälle aufweist, Ausfälle basieren auf systematischen Fehlern. (Eberle, TÜV Süd)
Man kann keine Fehlerraten veröffentlichen da die Anwendung entscheidend ist. Auslegung der Geräte ist wichtig. Qualifikation durch Prüfung. Mit kurzen Prüfintervallen anfangen, dann diese immer mehr verlängern wenn Vertrauen aufgebaut. (Menck, Dow Chemicals)
Wie stabil oder unzuverlässig ein Gerät ist geht über Betriebsbewährung im Anwendungsfall. Es ist höchstens akzeptabel, für spezielle Anwendungen Werte zu veröffentlichen als Richtwert für Betriebsbewährung. (Ströbl, TÜV Süd)
Öffentlichkeitsarbeit ist nötig um mehr Verständnis für dieses Vorgehen zu generieren. (Ebel, Samson)
Die Anwendung ist entscheidend. Einzelbetrachtungen, kurze Intervalle sind ein guter Ansatz. (Hablawetz, BASF)

3. Können PFH-Werte in PFD-Werte umgerechnet werden?

Vereinfachte Formeln in VDI/VDE 2180: PFH = λ_{du} PFD = PTC * λ_{du} * T1/2
Grundsätzlich möglich, es ist aber zu prüfen ob Komponenten für High-Demand akzeptabel sind, Verschleiß beachten z.B. mit B10d-Werten. Diagnose muss schnell genug arbeiten, ist ansonsten nicht wirksam (siehe Frage 1). Diagnose kann evtl. herausgerechnet werden. (Klotz-Engmann, E+H)

4. Wie komme ich zum PFD- oder PFH-Wert eines Leistungsschützes?

In der EN 13849 sind typische Ausfallraten gegeben für High Demand, es sind aber Schaltspiele mit in die gefahrbringend undetektierten Ausfälle einzuberechnen. (M. Mast, RAMSYS)
Nicht direkt übertragbar auf Low Demand, ggf. ist Verschweißen der Kontakte ein Problem. Spiegelt sich auch in SN-31920 mit unterschiedlichen Werten je nach Demand Mode wider. Als Richtwert bei Mittelspannung nur auf 90% der Maximallast auslegen. Bei Siemens und ABB geben die Datenblätter oft gute Hinweise. (Hanspach, Hima)
Namur-Richtlinie NE142 die man nutzen kann. Auch für Mittelspannungen. (Menck, Dow Chemicals)

5. Wenn ich eine Schutzeinrichtung mit SIL für die Auswirkung "Explosion" betrachte, muss ich dann noch eine Bewertung nach TRGS725 vornehmen?

Anmerkung: Technische Regel für Gefahrstoffe TRGS725 - Gefährliche explosionsfähige Atmosphäre – Mess-, Steuer-und Regeleinrichtungen im Rahmen von Explosionsschutzmaßnahmen. In Deutschland ja. (Hablawetz, BASF)
Bei er Erstellung des Explosionsschutzdokumentes wird entschieden ob nötig oder nicht, bzw. vorab in der Gefährdungsbeurteilung bzw. Risikoanalyse. Abhängig auch davon ob Explosion über explosible Stoffe oder durch hohen Druck ausgelöst, dort sind evtl. ausschließlich Sicherheitsfunktionen nötig (M. Mast, RAMSYS)
TRGS725 anwenden, aber immer Situation betrachten. Beliebt, z.B. nach Tabelle 4 zu arbeiten, aber die Anwendung analysieren. (Herrmann, Evonik)
Systematische Sicherheitsbewertung sinnvoll. Je nach Anwendung können zusätzliche Regeln greifen (TRGS, TRBS) (Strobl, TÜV)

6. Warum werden rein mechanische Bauteile wie z. B. Armaturen mit PFDs bewertet, obwohl diese Betrachtung nur für elektrische Komponenten sinnvoll ist?

Siehe Frage 2

7. Bei einer SIL-Einstufung kommt man z. B. auf SIL 1, es ist aber nur eine organisatorische Maß-nahme nach einer Alarmmeldung möglich. Muss die Alarmmeldung dann zwingend über eine SSPS erfolgen?

Ja. Da es SIL ist, muss es eine SSPS sein. (Menck, Dow)
Achtung, Alarme sind immer ‚Energize to trip', Versorgung muss zusätzlich sicher sein. (Bode, TÜV Nord)
Reaktion auf Alarm stellt organisatorische Maßnahme dar. Regelungen müssen vorhanden sein, auch schriftlich festlegt. Einfach einen sicheren Ausgang zu nutzen ist oft falsch. (Hanspach, Hima)
„4 Augen-Prinzip" sollte eingehalten werden. Das Personal muss geschult sein, es empfiehlt sich auch regelmäßige Überprüfung der Kenntnisse und Training. (Hablawetz, BASF)
Reaktion auf Alarm bleibt eine Ausnahme wenn es um sicherheitsrelevante Maßnahmen geht. Übli-cherweise hat der Bediener 15 Minuten um die Situation einschätzen zu können. Daher als schnelle Reaktionen nicht geeignet. (Hablawetz, BASF und Menck, Dow)
ROGA-Methode für Gefahrenanalyse verwenden – damit ist es möglich, organisatorische Maßnah-men für Risikoreduzierung zu nutzen. Eher nicht möglich in Hazop. Typisch ist Alarmmanagement bei manueller Befüllung von Tanks.
Wird möglichst vermieden da Schulungen und Trainings unbeliebt und Aufwand für den Betreiber beachtlich. Doku immer ausgedruckt in der Warte, aktuell usw. (Menck, Dow)
Auch Totmannschalter als Anwendung. Problem bei vielen Alarmen auch durch Stress für Personal. Wenn ein Tank vor Ort befüllt wird ist evtl. manuelles Abschalten vor Ort ausreichend (Hanspach, Hima)
Vorsicht - der Bediener darf nicht durch den Alarm in den Gefahrenbereich geschickt werden weil er das evtl. nicht ausführt. (Menck, Dow)
Bedienereingriff ist unzuverlässigste Methode im Standard und zu vermeiden. (Hablawetz, BASF)

8. Wenn z. B. ein Tank in Ex-Zone 1 eine Inertisierungsstufe 1 nach TRGS 509 erhält, dann müsste die Druckmessung zur Alarmierung eines zu hohem und/oder zu tiefem Druckes der Inertisierung eine Klassifizierungsstufe K1 gemäß Tabelle 10 aus TRGS 725 erhalten und somit SIL 1 entsprechen, oder? Was genau muss dann SIL 1 entsprechen, nur die Druckmessung und/oder die Alarmierung im Leitsystem? Wir sprechen ja hier nicht von einem SIL Loop mit klassischen Aktor. Reicht es aus, dass nur der Sensor also die Druckmessung SIL 1 entspricht oder muss die Druckmessung zusammen mit dem Leitsystem und/oder der Steuerung SIL 1 entsprechen ggf. mit Aktor (z.B. Hupe)?

Anmerkung: TRGS 509 - Lagern von flüssigen und festen Gefahrstoffen in ortsfesten Behältern sowie Füll-und Entleerstellen für ortsbewegliche Behälter Die TRGS ist richtig, allerdings muss sie komplett befolgt werden: erst inertisieren, abhängig von der Stufe muss Be- und Entlüftung vorhanden sein. (Herrmann, Evonik)
Druckregelung erforderlich. Achtung, bei Ausfall ist oft Zone 0 vorhanden. Erst Konzept erstellen, erst am Ende muss die Frage nach der TRGS725 gestellt werden – üblicherweise ist die Regelung in SIL1.
Reduzierung 1 bezieht sich auch auf die Überwachung - K-Stufe könnte reduziert werden. ZÜS würde das Konzept überprüfen (TÜV)

9. Wenn ich mit der TRGS auf eine Maßnahme stoße, die nach K2/3 gebaut werden muss, wie weit muss ich das "normale" SIL-Prozedere (Berechnung, TÜV,...) führen?

Wenn K2 umgesetzt werden soll, dann mit SIL laut EN 61511, dann ist auch der Ablauf klar. (M.Mast, RAMSYS)
Der Nachweis der Stufe ist zu führen, auch der Nachweis der Wirksamkeit der Einrichtung - egal ob hydraulische oder pneumatische Einrichtung. (Strobl, TÜV)

10. Wenn ich eine potentielle Gefahr in einer HAZOP aufdecke, die zu einer Explosion führen könnte, gehe ich dann weiter mit der DIN EN 61511 (VDE 2180) oder mit der TRGS725? Oder muss ich beides betrachten?

Klassisches Ex-Thema, zu behandeln mit 60079-Reihe. SIL nur wenn eine Rest-Zündgefahr vorhanden ist, dann darf die IEC 60079-42 herangezogen werden. Aber sonst durch klassische Installation gege-ben. (Klotz-Engmann, E+H)
Gutes Beispiel Pipelines, dort geht es nicht um Zone aber trotzdem um Risiken im Bereich Explosions-schutz. Wenn HAZOP für Ex dann Richtung TRGS. Oft sind Szenarien im Rahmen der Risikoanalyse schwierig zu bewerten, Risikoreduzierung reicht evtl. nicht aus. (Menck, Dow)
Z.B. bei Feuerungsanlagen hilft auch die TRGS nicht, bessere Regelwerke vorhanden wie EN 50156. (Ströbl, TÜV-Süd)
Bewertungen je nach Teilnehmern in Risikoanalyse sehr unterschiedlich, Entscheidungen spannend. (Hablawetz, BASF)
Üblicherweise betrachtet das Sicherheitskonzept (SIKO) umfassend die Risiken, daraus Entscheidung für SIL oder andere Lösungen (Herrmann, Evonik)

11. Gemäß Tabelle 8 und 10 der TRGS725 erfolgt die Zuordnung SIL über K-Stufe. Ob Zündquellen beim "selten ..." oder "zu erwartenden Fehler" vorliegen, hat großen Einfluss auf SIL-Ergebnis. Wie lautet deren Begriffsdefinition und wie bindend ist das Resultat für Betreiber?

Keine eindeutige Begriffsdefinition. Die Person die sich Gedanken macht benötigt Erfahrung. Bei Ex entsprechen diese Definitionen den Formulierungen für Zonen 0/1/2. Mögliche Zuordnung von Schutzmaßnahmen auch über die Begriffe einfehlersicher/zweifehlersicher. (Herrmann, Evonik)

12. Die TRGS 725 beschreibt keine organisatorischen Reduzierungsstufen. Kann hier jeder selber die Reduzierungsstufen festlegen?

Siehe Vortrag von Evonik. Es gibt keine direkte Zuordnung, aber die Empfehlung Risikoreduzierung nicht durch organisatorische Maßnahmen herzustellen. (Herrmann, Evonik)

13. Bei mir landen oft Fragen auf dem Tisch, die die Mitbenutzung von Sicherheitskomponenten in der „normalen“ betrieblichen Prozesstechnik betreffen. o Inwieweit zulässig? o Berücksichtigung im SIL-Nachweis, SIL-Berechnung, HDM, LDM? o Nachweis der Rückwirkungsfreiheit? o Weitere zu berücksichtigende Faktoren/Parameter?

Das ist möglich wenn die Mitbenutzung rückwirkungsfrei ist. Bei einkanaligen Systemen aber unwahrscheinlich weil bei Wegfall eines Signales sowohl Steuerung als auch Sicherheitstechnik betroffen. (Schrörs, Bayer)
Zentrale Frage ist, was passiert wenn das Element kaputt geht? Führt das zu dem Fehler dass die Si-cherheitsfunktion auslöst? Beispiel Lagertemperatur: wenn die Temperaturmessung kaputt ist, dann könnte die automatische Schmierung unterbleiben als auch die Übertemperatursicherung nicht mehr funktionsfähig sein – führt direkt kritischen Fehler herbei. (Hablawetz, BASF)
Nach der EN 61511 ist Unabhängigkeit nachzuweisen. (Strobl, TÜV)

14. In der DIN EN 61511 taucht der Begriff der Betriebsbewährung unter "prior use" auf. Im Folgetext erscheint dann wieder der Begriff "proven in use". Darf ein Feldgerät mit ausschließlicher Eigenschaft "proven in use" noch eingesetzt werden?

In der EN61511 wird „proven in use“ auf den Hersteller beschränkt, „prior use“ berücksichtigt nur betriebliche Erfahrung innerhalb einer Applikation. Prüfintervalle spielen eine Rolle. (Hablawetz, BASF)
Welche Rolle spielt die VDE 2180 bei Betriebsbewährung: Tabelle der HFT beachten. Eignung für Applikation ist zu begründen. EN 61511 Teil 4 soll Ende des Jahres kommen und diese Frage behandeln.

15. Welche Schulungen sollten absolviert werden, um SIL-Kreise planen zu können/dürfen?

Systematische Fehler müssen vermieden werden, Schulungen sind im FSM System zu verankern. Erst Grundlagenschulung, dann applikationsspezifische Ausbildung, dann Fachkenntnisse zu eingesetzten Produkten.
Aus Erfahrung werden ältere Kollegen angesprochen, da diese Erfahrung und Kontakte haben. (Menck, Dow)

16. Ist die betriebliche Zündquelle aus Tabelle 8 aus der TRGS 725 mit der betriebsmäßigen Zündquelle aus Tabelle 2 gleichzusetzen? Oder kann auch argumentiert werden, wenn ein Gerät/Produkt nicht nach 2014/34/EU hergestellt ist und der Betreiber argumentiert, die Zündquelle ist nur im seltenen Fehlerfall vorhanden, da z.B. die Pumpe selten leerläuft, dieses auch so realisiert werden kann? Sogar ohne Reduzierungsstufen/Überwachung?

Tabelle 8 ist fehlerhaft, hat falsche Überschrift. Lieber Ex-Geräte verwenden, in vielen Fällen zwingend erforderlich (z.B. ein Puffertank mit Zone 0 dessen Füllstand erwartungsgemäß stark variiert). Zündquellenanalyse könnte dieses Resultat haben, Pauschalaussage aber nicht möglich, abhängig vom Medium und Applikation. (Herrmann, Evonik)

17. Thema: Notwendigkeit der Abnahme der Software nach Änderung / Anpassung durch eine zu-gelassenen Überwachungsstelle Beispiel: Ein thermischer Reaktor dient der Verbrennung von nicht destillierbaren flüssigen Kohlen-wasserstoffen. Der Reaktor hat einen Doppelmantel zwecks Kühlung der Reaktorwandung zugehörig eine darüber gelagerte Dampftrommel. Der anfallende Dampf wird in der Anlage verwendet. Die Anlage wurde 1981 errichtet und ist laut Genehmigung eine Anlage im Sinne des §4 des BImSchG. Die Dampftrommel und der Reaktor sind intern der BetrSichV (Gefahr Druck) zugeordnet. Beide haben ein Sicherheitsventil. In 2015 wurde die SSPS (H41 gegen HIMAX) erneuert und durch eine zugelassenen Überwachungs-stelle geprüft. 2019 wurde die Software im Rahmen eines MoC Prozesses geringfügig geändert.

Anmerkung: MoC = Management of Change

18. Wäre die heutige anzuwendende technische Regel bezüglich der Feuerungsanlage die EN746-2 "Thermoprozessanlagen"

Korrekt - industrielle Thermo-Prozess-Anlage, beheiztes Druckgerät. ZÜS-Abnahme erforderlich (Ströbl, TÜV Süd).
Anmerkung: ZÜS = Zugelassene Überwachungs-Stelle

19. Muss diese Änderung wieder durch eine zugelassenen Überwachungsstelle geprüft werden, wenn ausreichend eigene Fachkompetenz zur Verfügung steht.

Wenn Grenzwerte oder Steuerungen geändert werden, dann wird dringend empfohlen der Überwachungsstelle ein Verify-Protokoll zukommen zu lassen, zu belegen dass Änderung nicht „aus Versehen“ erfolgt ist.

20. Was versteht man bezüglich PLT unter prüfpflichtigen Änderungen (Beispiele)

Wenn nur einfache Geräte (Sensoren) ausgetauscht werden, sollte nur die Doku gepflegt werden. Im Allgemeinen nicht prüfpflichtig.
Es gibt aber Unterschiede bei Gewichtung der Änderung. Daher die Empfehlung, die Änderungen in der Doku zur eigenen Absicherung immer der Prüfbehörde weiterleiten. Bei beheizten Druckanlagen kommt es leider öfter zu Störfällen, daher die ZÜS als Partner ansehen und in Kenntnis setzen (Ströbl, TÜV Süd).
Die Prüfzuständigkeiten sind in der Betriebssicherheitsverordnung definiert. Die Prüfinhalte sind in der TRBS 1201 Teil 2 geregelt. Prüfpflichtige Änderungen in der TRBS 1123. Je nachdem wie

groß die Änderung ist muss sogar beim zuständigen Landratsamt oder der Bezirksregierung eine Genehmigung beantragt werden (Bode, TÜV Nord).

21. Wie interpretiert man den Satz aus der VDE2180 Blatt 3 (2007) Absatz 3.4.1 Optimierung der Schutzeinrichtung "Die PLT-Fachkraft ist verantwortlich dafür, dass die gegebenenfalls erforderlichen Schritte Planung, Montage und insbesondere die durch die unabhängige Stelle durchzuführende Erst-prüfung vor Inbetriebnahme erfolgen"

Warum will man interpretieren, wieso nicht tun? (Menck, Dow)

Unabhängigkeit in EN 61508 Kap. 8 definiert. SIL 1 gleiche Abteilung, SIL 2 andere Abteilung die nicht mit dem Projekt konfrontiert (involviert) ist, SIL 3 unabhängige Stelle. (Ströbl, TÜV Süd)

22. Gibt es gängige Prozedere bei Prüfintervallüberschreitungen oder muss das jedes Unternehmen individuell regeln?

Tagesgenau Funktionsprüfungen dokumentieren und bei Abweichung die Daten kommunizieren. Es ist möglich, Aufweitung von einem auf 2 oder 3 Jahre vorzuschlagen, auch basiert auf Stördatenerfassung / Unauffälligkeit bei der Überprüfung. Aufweitung von Prüfintervallen teilweise sogar mit Bezirksregierung abgesprochen, offizielle Stellen sind zu unterrichten (Schrörs, Bayer).

23. Hersteller geben in ihren SIL-Zertifikaten eine Mission Time an. Müssen die Geräte nach Ablauf dieser Zeit getauscht werden? Gibt es Alternativen zur Verlängerung z.B. via NAMUR SMART Tool?

Beschreibung des Begriffes anschauen, Ausfallraten gelten üblicherweise nur in der Mission Time. Aufweitung aber auch über Stördatenerfassung möglich, ähnliche Applikationen erlauben Rückschlüsse.
Es kann aber auch einfacher sein zu tauschen. (Laible, Siemens)
Man kann das Tool der NAMUR nutzen um Fehler in Sicherheitseinrichtungen zu finden, um Rückschlüsse zu ziehen wenn man häufige Fehler hat. Dies entbindet aber nicht von eigener Überwachung. (Hablawetz, BASF)
Nationale Abweichung N3 in DIN 61508-2 erlaubt Stördatenerfassung. Feste Limitierung von Lebens-dauer in Produktdoku kann zu Ablehnung der Geräte führen (Menck, Dow)
Siemens gibt keine Lebensdauer an, allerdings ist z.B. Verschleiß an Relais zu beachten. (Laible, Siemens)
Hima macht nach Rücksprache und Bewertung vor Ort evtl. Zugeständnisse für eine Verlängerung. Bei härteren Umgebungsbedingungen kann das allerdings ein Problem sein. (Hima)

24. Definition Low Demand/High Demand: binärer Sensor (z. B. Temperaturschalter (z. B. Bimetall)) - Eintrittshäufigkeit eines unsicheren Betriebszustandes größer als 1 Jahr = low demand - Eintrittshäufigkeit eines unsicheren Betriebszustandes kleiner als 1 Jahr = high demand - Kontinuierlicher Temperatursensor (z. B. PT 100) immer high demand?

Wie oft wird die Schutzanforderung genutzt? Wenn < 1x pro Jahr dann low-Demand auch bei ständiger Nutzung. (Klotz-Engmann, E+H)
Wenn es nur ein Schalter ist, dann häufig prüfen. Wenn es ein Temperatursensor ist, dann ist ständig die Funktion im Eingriff, Ausfälle und Auswirkung eines fehlenden Signales hinterfragen. NA 106 beachten. Schalter in Sicherheitstechnik oder Regelungstechnik nicht üblich (Menck, Dow)

25. Elektrischer Sensor als potentielle Zündquelle (Temperatur, Füllstand etc.) in Zone 0 bzw. 20 nach Tab 2 TRGS 725 sind 3 Reduktionsstufen erforderlich um in den sicheren Bereich zu kommen. Kann man davon ausgehen, dass ein Sensor mit Baumusterprüfbescheinigung einer notifizierten Stelle für die Gerätekategorie 1G bzw. 1D und korrekter Montage die erforderliche Reduzierung sicherstellt?

Sensor mit 1G/1D ist direkt geeignet für Einsatz in Zone 0 / 20, keine Reduzierungsstufe erforderlich (Bode, TÜV Nord)
Bei elektrischen Betriebsmitteln im Ex-Bereich müssen die notwendigen Schutzmaßnahmen für die Zone eingehalten werden – kein Bezug zur TRGS725. Erst wenn durch betriebliche Störungen eine Rest-Zündquelle erkannt ist, dann die TRGS725 anwenden. Die in der Frage angesprochen 3 Reduzierungsstufen erfüllt der klassische Explosionsschutz. (Klotz-Engmann, E+H)

26. Wie ist ein PT100 zu prüfen, der in einer Sensor-Logik-Aktorkette zur Messung der Oberflächen-temperatur mit dem Ziel der Zündquellenvermeidung eingesetzt wird? - ist es ausreichend, den Sensor abzuklemmen und den Widerstandswert zu simulieren um die Sensor-Logik-Aktorkette zu prüfen, da man davon ausgehen kann, dass der high-Demand Einsatz ausreicht die Funktion permanent zu bestätigen? - PT 100 ausbauen und im angeklemmten Zustand in Kalibrier- oder Prüfeinrichtung auf die Schalttemperatur aufheizen?

Für funktionale Sicherheit wäre NA106 zu verwenden. Dort sind verschiedene Varianten beschrieben. Ein Abklemmen des Sensors ist nicht optimal da dann nicht in der üblichen Umgebung geprüft. (Menck, Dow)
Ins Sicherheitshandbuch schauen, dort sind meist Prüfungen und Prüftiefe beschrieben. Nötig auch zur Erstellung des Prüfkonzeptes. (M. Mast, RAMSYS)

27. Welche Fundstellen für die Fristen wiederkehrender SIL Prüfungen von Sensor-Logik-Aktorketten gibt es?

SIL Berechnung, Sicherheitsanforderungsspezifikation SAS und Sicherheitshandbücher, da hier auch Angaben über den Prüfzeitraum gegeben sein können. Nicht nur auf die funktionale Sicherheit ach-ten, es gibt oft noch andere Gesetze und Richtlinien die beachtet werden müssen. z.B. WHG (Wasser-haushalts-Gesetz) fordert regelmäßige Prüfungen (M. Mast, RAMSYS).
SIL-Prüfung zur Bestätigung der Berechnung, und zur Aufdeckung zufälliger Fehler. Ablagerungen, Anbackungen usw. können systematische Fehler haben, andere Regelwerke (z.B. EN 746-2) schreiben eine jährliche Prüfung vor (Ströbl, TÜV Süd).
Siehe NA106. Zusätzlich Erfahrung mit dem Prozess berücksichtigen (Menck, Dow)
Thema: TRGS 725 Bewertung der Risikominderung von Ex-Vorrichtungen: In einer Mühle (Luftmenge 20000 m³/h) werden brennbare Feststoffe vermahlen und in einem Filter (Zone 20) von der Mühlenluft abgetrennt. In der Mühle entstehen Schlagfunken. **A)** Feststoffe aus lose bezogenem Schüttgutmaterial (Mulden-LKW) werden vermahlen. Aufgrund von möglichen Verunreinigungen im Mahlgut muss mit der Entstehung von Schlagfunken im Betriebsfall gerechnet werden. Gem. TRGS sind 3 Reduzierungsstufen erforderlich um von der Funken-entstehung im Normalfall zur Funkenentstehung im sehr seltenen Fehlerfall zu gelangen. Da die Zone in einem Filter aufgrund der Luftmenge verfahrensbedingt nicht reduziert werden kann wird folgen-des Konzept überlegt: Maßnahme R1: Funkenerkennung und Löschung in der Leitung zw. Mühle und Filter (Ausgeführt gem. VDS 2518:2017-05 (02)) zur Reduktion der Funkenhäufigkeit. Maßnahme R2: Druckentlastung des Filters, der der Mühle nachgeschaltet ist mit Berstscheiben (Bemessen nach VDI /DIN) und Entkopplung der Rohrleitungen mit

explosionsdurchschlagsicheren Zellradschleusen. Die Zellradschleusen werden über den Berstsensor der Berstscheibe angehalten. Ab-schaltung der Zellradschleusen auf SIL 2)
B) Der Mühle aus A wird ein Magnetabscheider vorgeschaltet. Maßnahme R1: Magnetabscheider Maßnahme R2: Funkenerkennung und Löschung zur Reduktion der Funkenhäufigkeit Maßnahme R3: Druckentlastung/entkopplung des Filters wie A. Abschaltung der Zellradschleusen SIL 1 möglich?
C) In der Mühle aus Fall B wird nun ein industriell hergestelltes sauberes, als Blattware bezogenes Papier vermahlen, das vor der Vermahlung im eigenen Werk zerkleinert wird. In diesem Fall können Fremdkörper nur durch Metallteile, die sich in der Anlage lösen auftreten. Andere Feststoffe wie Steine etc. sind praktisch ausgeschlossen. Einstufung der Zündquelle aufgrund der geringen Verschmutzung des Mahlgutes: Im vorhersehbaren Fehlerfall. Gemäß TRGS 725 sind nur 2 Reduzierungs-stufen erforderlich Maßnahme R1: Magnetabscheider Maßnahme R2: Funkenerkennung und Löschung zur Reduktion der Funkenhäufigkeit Maßnahme R3: erf.: Druckentlastung/Entkopplung des Filters wie A. Abschaltung der Zellradschleusen ohne SIL möglich? Prinzipiell ok, das Ex-Schutz-Konzept sollte extern abgenommen werden. **Zusätzliche Fragen**: Unter welchen Umständen kann ein Magnetabscheider eine Reduktionsstufe er-reichen? Die Wirksamkeit ist kaum belastbar quantifizierbar.
Mit dem Abscheider wird keine Reduktionsstufe erreicht sondern eine Reduzierung der Häufigkeit – Risikograph verändert.
In allen Fällen A, B und C ist die Häufigkeit des Auftretens der Zündquelle und damit die Wahrscheinlichkeit einer Explosion unterschiedlich aber die Maßnahme Entkopplung greift immer erst dann, wenn eine Explosion tatsächlich vorhanden ist. In allen Fällen Abschaltung der Zellradschleusen auf SIL 2?
Nicht allgemeingültig lösbar. Eine Bewertung nach TRGS 725 scheint SIL 2 ergeben zu haben. Nicht auf die letzte (tertiäre) Ex-Schutz-Maßnahme - die Ex-technische Entkopplung - verzichten. Maßnahmen primär, sekundär, tertiär gut beschreiben. Werden hier benötigt da zündfähige Funken nicht ausgeschlossen. Daher ist Auswirkung der Explosion zu verringern. (Herrmann, Evonik)
Auf welchem Niveau muss die Abschaltung erfolgen?
Beispiel: Berstscheibe spricht an, dann Abschaltung in SIL 2 - Berstscheibe nicht nach SIL2 beurteilbar. Das Ex-Schutzkonzept sollte gut beschrieben sein. Ex-technische Entkopplung vernünftig auslegen (z.B. Zellenradschleuse). Qualitativ gute Abschaltung ist wichtig. Tabellen zweitrangig. Die Abschaltung so sicher wie möglich, also SIL2. (Herrmann, Evonik)
Explosionsschutzkonzept prüfen lassen, unabhängige Meinung ist wichtig inklusive funktionaler Sicherheit und der Verwendung von Schutzsystemen. Dann ist die Gefährdungsbeurteilung richtig. (Bode, TÜV Nord)

28. Risikograph für Explosion:
Tod: S=4
Häufigkeit der Exposition (Aufenthaltsdauer des Mitarbeiters im gefährdeten Bereich) mehrfach täglich: F =5 Wahrscheinlichkeit des Auftretens einer Explosion unwahrscheinlich W=1 Schadensbegrenzung: Betrachtung 1: P=5 (keine Möglichkeit für den Mitarbeiter) Betrachtung 2: P=1 (aber möglich für den Planer) K=F+W+P=5+1+5=11 Mit S=4 folgt SIL 3 K=F+W+P=5+1+1=7 Mit S=4 folgt SIL 2 Wahrscheinlichkeit des Auftretens: Bei der Risikoeinschätzung mit Risikograph nach DIN 62061 Schritt 4 „Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens“ wird auf Definitionen der DIN 12100 verwiesen. In dieser bezieht sich Abs. 5.5.2.3.3 ausschließlich auf die persönlichen Möglichkeiten von Mitarbeitern sich aus einer Gefahr zu entfernen. (Reduktion der Auswirkung durch Flucht) Diese Möglichkeit besteht im Falle von Explosionen für einen Mitarbeiter niemals. Für P müsste also immer 5 gewählt werden, was in der Regel zu SIL 3 führt.
Bei korrektem Vorgehen der Analyse sind viele Orte an denen Explosionen stattfinden bekannt. Mit technischen Mitteln kann der Schaden für den Mitarbeiter mit sehr hoher Wahrscheinlichkeit sozusagen durch die Möglichkeiten des Technikers begrenzt werden. Z. B. Entlastung der Explosion im Behälters/Silo durch Berstscheiben gem. VDI 3673/ DIN 14491/DIN 14494 und geeignet Entkopplung etc. Bei dieser weitergefassten Sicht auf die Reduzierung der Aus-wirkung ergäbe sich nur noch P =1 Ist das zulässig?

Änderung im Schaden für den Mitarbeiter, Parameter S. Weglaufen nicht mehr möglich. Laut Ex-Schutz genügt die Reaktionszeit nicht als Schutz. Daher SIL 3. (M. Mast, RAMSYS)
Frage nach dem Design stellt sich nicht, Ex-Schutz wird benötigt. (Laible, Siemens)
Berstscheiben könnten helfen auf SIL 2 zu kommen. Ex-Konzept prüfen lassen, dann (dabei) prüfen ob die angewendete Norm die richtige ist. (Bode, TÜV Nord)

29. Können gem. TRGS 725 mehrere potentielle unabhängige Zündquellen wie z. B. Messgeräte/Mo-toren/Ventile etc. im räumlichen Zonenzusammenhang, die jeweils eine hinreichende Baumusterzu-lassung haben, unabhängig betrachtet werden, oder ist ein Risikoaufschlag aufgrund der Anzahl not-wendig? Wenn ja ab welcher Anzahl?

Wenn die Betriebsmittel mit Baumusterprüfung nach Atex geprüft sind und die Anforderungen der Zone einhalten dürfen beliebig viele Geräte eingesetzt werden. (Klotz-Engmann, E+H)

30. Müssen beim zeitgleichen Betrieb mehrerer identischer und parallel betriebener Apparate, die jeweils eine hinreichende individuelle Baumusterzulassung besitzen, Sicherheitszuschläge gemacht werden?

Siehe vorherige Frage

31. Zur Überwachung einer potentiellen Zündquelle in einer Ex-Zone, z.B. einer Lagertemperatur, ist die Einbringung einer zusätzlichen potentiellen Zündquelle (Sensor) in die Zone erforderlich. Kann bei Verwendung eines baumustergeprüften Sensors dessen zusätzliches Risiko vernachlässigt werden?

Siehe vorherige Frage - der Sensor hat eine entsprechende Baumusterprüfbescheinigung, also ist nichts weiter zu beachten außer evtl. vorhandener Bedingungen laut Baumusterprüfbescheinigung.

32. SIL-konformes Abschalten von Antrieben:

Mit FU Sil 1 mit einem für SIL 1 geeigneten FU einkanalig an SSPS Sil 2 mit einem für SIL 2 geeigneten FU zweikanalig an SSPS Sil 3 mit einem für SIL 2 geeigneten FU zweikanalig an SSPS und zusätzlich einen SIL 1 Hauptschütz mit Überwachung der Hauptschützposition über einen Hilfskontakt (als Diagnosesystem)

Anmerkung: FU = Frequenzumrichter.
Fälle laut NE 142 anwenden. Einige Lieferanten haben Hilfskontakte die das zusätzliche Schütz für SIL 3 ersetzen. Auf gemeinsame Nutzung achten (Rückwirkungsfreiheit) und Überlast beachten (Menck, Dow). Siehe IEC 61800 für FU.
Ohne FU SIL 1 ein SIL 1 Hauptschütz an SSPS SIL 2 zwei separate SIL 1 Hauptschütze in Reihe an SSPS SIL 3 zwei separate Hauptschütz in Reihe an SSPS jeweils mit Überwachung der Hauptschützposition über je einen zwangsgeführten Hilfskontakt
Oft ist ein Hauptschütz nur eine betriebliche Einrichtung (nicht Safety). Bei SIL 2 über ein Hauptschütz die Mitbenutzung für betriebliche Zwecke beachten, evtl. 2 Hauptschütze erforderlich (Bode, TÜV Nord).
Für SIL 3 sind die Hilfskontakte evtl. nicht die richtige Wahl wenn Schütze selten schalten, da ein Ver-sagen zu spät auffällt (wenn die Sicherheitsfunktion benötigt wird).

33. **Wie berücksichtigt man mehrere Zündquellen an einer Anlage, wenn diese über funktionaler Sicherheit vermieden werden müssen? Muss dann das Einzelrisiko stärker gemindert werden, wie es in der EN 50126 für Bahnanwendungen dargestellt ist?** Oder anders gefragt: Wenn eine Person mehreren Gefahren ausgesetzt ist, dann werden in der EN 50126 (für Bahnanwendungen) die Anforderungen an die Risikominderung jeder Einzelgefahr entsprechend erhöht. **A)** Wie berücksichtigt man, wenn über funktionaler Sicherheit mehrere Zündquellen an einer Anlage vermieden werden müssen?

o Mehrere eigenständige Zündquellen bewirken unabhängig voneinander eine messbare physikalische Sammelgröße (Temperaturanstieg des Systems). Nur der Gesamttemperaturanstieg, nicht die Einzelursache, ist als Messsignal auswertbar. Alle drei Ursachen können durch rechtzeitige Abschaltung des Antriebs zeitgleich unwirksam gemacht werden.

o Mehrere eigenständige Zündquellen bewirken jeweils eine Gefahr. Jeder Fehler kann eindeutig messtechnisch erkannt werden. Für jede Zündquelle ist eine separate Sensor- Logik-Aktor-Kette aufgebaut. Jede Gefahr kann durch abschalten der verursachenden Teileinheit jeweils separat unwirksam gemacht werden.

o Mehrere eigenständige Fehler bewirken jeweils eine Gefahr. Jeder Fehler kann eindeutig messtechnisch erkannt werden. Für jede Zündquelle ist eine separate Sensor-Logik-Kette aufgebaut. Alle Gefahren können durch abschalten des Hauptantriebs unwirksam gemacht werden.

o BSP: 4 GLRD (Gleitringdichtung) an einem Apparat, jede GLRD wird separat mit einem Tempera-tursensor überwacht. Jeder Sensor bewirkt bei lokaler Übertemperatur jeweils die Abschaltung des Apparates.

Im Maschinenbau wird diese Betrachtung nicht gemacht. Einzelne Betrachtung reicht. (Laible, Siemens)

Die Art der Betrachtung sollte geeignet sein. Der deterministische Weg schreibt das so nicht vor. (Schween, Hima)
B) Wie muss vorgegangen werden, wenn mehrere identische Apparate der o.g. Eigenschaften zeit-gleich in einer Anlage/in einem Arbeitsplatzbereich betrieben werden?
Siehe Antwort für A)
34. Kann man temporär einen nicht Ex(i) zugelassenen Sensor in einem Ex(i) betreiben (Zone 2)? Der Produktionsbetrieb kann auch eine Heiss-(Feuer-) Erlaubnis ausstellen und mehr Rundgänge machen. Die fehlersicheren Sensoren in EX(i) und [nicht Ex(i)] sind baugleich.

Nein, da dort nur Bauart zugelassene Geräte verwendet werden. Es sei denn, es wäre laut Gefährdungsbeurteilung möglich (die Gefahrstoff-Verordnung erlaubt das). (Herrmann, Evonik)
Manchmal haben die Sensoren für Ex und Nicht-Ex den gleichen Namen und das gleiche aussehen, intern sind aber die parallelen Schutzelemente für Ex nicht bestückt. Beim Hersteller nachfragen (Kindermann, P+F).
Geht bei einfachem Bauteil (ohne Induktivitäten und Kapazitäten) - Schalter oder PT100 nach EN 60079-11 das am eigensicheren Stromkreis betrieben werden darf. Dokumentieren der Bewertung aber dennoch nicht vergessen.
Zusätzliche Fragen am Tag
35. Wie sind Ausfälle der Diagnose zu berücksichtigen? Es gibt Nachweise, in denen Ausfallraten der Diagnose gesondert dargestellt werden. Sie könnten als gefährlich undetektiert gewertet werden (Definition von gefährlich undetektiert), als ‚nicht Teil' der Sicherheitsfunktion oder safe (wenn der Ausfall den sicheren Zustand herbeiführt).

Eine FMEDA macht eigentlich nur Einfehlerbetrachtung. Die Diagnoseausfälle sollten nicht in den Ausfall der Sicherheitsfunktion eingerechnet werden. (Klotz-Engmann, E+H).
Die Diagnose sollte dann auch eine entsprechende Reaktion auslösen. Bei Steuerungen geht das, bei Sensoren ist das nicht immer möglich und hängt auch von der Architektur ab. (Schween, Hima).
In der Chemie kann die Diagnose auch über die Steuerung laufen und wird getrennt betrachtet. Die Diagnose muss dann regelmäßig geprüft werden. (Hablawetz, BASF)

36. Wie wird praktisch Security Risk Assessment gemacht? Wird aus einem SIL das Schutzniveau für Security abgeleitet? Welches Schutzniveau bzgl. SIL ist für eine prozesstechnische Anlage praktisch notwendig?

Keine konkreten Festlegungen, Ansätze in der NE163. Momentan eher quantitativ bestimmte Ni-veaus (hoch, mittel oder niedrig) nach ‚Cybersecurity-Act' (siehe Vortrag des DKE), aber nicht allge-mein definiert. (Schween, Hima).
Es gibt keine Zuordnung von SIL zu Security-Niveau. (Klotz-Engmann, E+H).
Hier werden ökonomische und sicherheitstechnische Belange gemischt. Die Frage ist, ob man das wirklich möchte. Es darf aus sicherheitstechnischer Sicht kein Risiko darstellen. (Hablawetz, BASF).
Shell untersucht Security schon seit 2008. Für Anlagen an der Küste der USA wurde das schon gefor-dert. Seither wird das Thema grundsätzlich in allen Produktionsbereichen untersucht, sehr umfang-reich und teuer. Alle 2 Jahre erfolgt ein Audit. Der FSM sollte das zumindest abschnittweise beach-ten, damit es nicht vergessen wird.

37. Gibt es Bestrebungen die Anforderungen bzgl. Ex-Schutz international zusammenführen?

C-Normen, siehe Vorträge.

38. Ist die Zuordnung von 35% Sensor, 15% Logik und 50% Aktor beim Anteil der Sicherheitsfunktion noch aktuell?

Kann man als Richtschnur anwenden, aber nicht immer umsetzbar. (HIMA)
Standen nie in der EN 61508. Die Zahlen stimmen oft für systematische Fehler aber nicht für zufällige Fehler. Daher nicht anwendbar. (Hablawetz, BASF)

12. SIL-Sprechstunde 2021

1. Laut 61508 ist es möglich, ein einzelnes Gerät in SIL3 zu verwenden, wenn auch die SC entsprechend SC3 ist. Wie sieht das die 61511 vor? Kann der Nachweis über die SC ausreichend sein? Sollte somit in der Bewertung dokumentiert werden? Konkretes Beispiel: KCD2-SCD-Ex1.ES

Die IEC 61508 fordert für SIL3 normalerweise eine HFT1. Für Typ A – Elemente ist unter bestimmten Bedingungen nach Teil 2 Kap. 7.4.4.3 eine HFT0 gestattet. Die IEC 61511 bestätigt dies in Teil 1 Kap. 11.4.
Bei der Sprechstunde anwesende Industrievertreter gaben an, dass die meisten Firmen der Prozessindustrie Redundanz für SIL3 nutzen. Daher sollte unbedingt eine SC3 angegeben sein.
Es gab zwar auch den Hinweis auf eine Einzelfallbetrachtung, dies wäre aber sehr Prozess abhängig. Dann könne man mit nur einem Gerät mit SIL3 und einer SC3 einen SIL3 erreichen.
Beide Aussagen deckten sich auch mit einem Erfahrungsbericht einer Anlagenplanerin. Ihre Firma habe zwar auch schon einen SIL3 mit nur einem Gerät realisiert, habe dabei aber eine sehr enge Absprache mit dem TÜV gepflegt und es sei auch nur realisiert worden, weil die sehr engen Platzverhältnisse 2 Geräte nicht zugelassen haben.
Dazu kam von einem anderen Teilnehmer der Hinweis, dass eine lange Diskussion mit dem TÜV und ein aufwändiges Dokumentieren der Begründung (wieso nur ein Gerät verwendet wird) nicht unbedingt eine „Ersparnis“ (finanzieller Art) erbringen würde.

2. Wie kritisch ist es, die Sicherheitsbudgets von Sensor, Logik und Aktor zu ignorieren? Es könnte immer wieder Anwendungen geben, wo es ein komplettes Übergewicht in eines der Bereiche gibt.

Sicherheitsbudgets in der PFD-Berechnung wurden in der veralteten NE106 angegeben. Dort unter Kapitel 6.4 stand: „die typischen PFD-Anteile für die einzelnen Teilsysteme müssen allerdings beachtet werden - für das Sensorsystem ca. 35 % der PFD, für das Aktorsystem ca. 50 % der PFD.“
Es gab aber den Hinweis, dass die NE106 überarbeitet wurde, und nun NA106 lautet. In dieser neuen Fassung sei diese Angabe auf PFD-Anteile entfallen.
Daher gab es in der anschließenden Diskussion Stimmen aus der Industrie, für die eine Verteilung, oder Aufteilung des PFD-Wertes keine Rolle spielt, da dies ja auch kein Bestandteil in einer Norm sei.
Es gab aber auch Teilnehmer die angaben, dass bei Ihnen versucht würde eine solche Gewichtung einzuhalten (auch ohne Rechnung) um einzelnen Komponenten kein übermäßiges Gewicht in der Sicherheitsfunktion zu geben. Dies hätte sogar Einfluss auf die Geräteauswahl. Für Gerätehersteller ist es wichtig, ein realistisches Budget für die Erstellung eines Sicherheitskreises an-geben zu können.
Einigkeit bestand nur darin, dass auch aus Erfahrungsberichten heraus bei der Abnahme vom TÜV eine solche Verteilung keine Rolle spielen würde. Da würde nur das Gesamtbudget nach Norm geprüft.
Quintessenz: je nach Anwendung agieren und den Sachverstand nutzen. Nicht stur nach Vorgaben oder Mustern bewerten.

3. Was wird getan (Instandhaltungsmaßnahmen, Dokumentation, Betriebsbewährtheit), um die Geräte nach End of Life weiter betreiben zu können?

Eigentlich ist der Begriff „End of Life“ mit dem Ausmustern der Komponente (verschrotten) verbunden – damit wäre die Frage nicht sinnvoll. Es könnten das Ende der Gebrauchsdauer oder die Angabe im Handbuch gemeint sein. Auf Rückfrage wurde die Angabe im Handbuch (z.B. 8-12 Jahre) diskutiert.

Die Betreiber fordern eine „Öffnungsklausel“ um eigene Stördatenerfassung zu erlauben - in Firmen in denen mehrere Hundert oder gar Tausend gleiche Komponenten im Einsatz sind können Ausfallgrenzen gut beobachtet, ermittelt und bestimmt werden. Daher würden in solchen Firmen die Geräte wesentlich länger eingesetzt. Manchmal wird die Angabe „8-12 Jahre“ schon als „Öffnungsklausel“ angesehen wenn der Hersteller nicht explizit eine Entsorgung nach dem Zeitraum vorschreibt. Komponenten mit solchen Vorgaben würden sonst nicht eingesetzt (gekauft) werden. **Der Nachweis und die Begründung sind dann natürlich selbst zu führen**. Auch die Proof Tests sind dann näher zu betrachten. **Sinnvoll erscheinen dann kürzere Prüfintervalle**. Hier kommt es aber wieder auf die Einzelfallbetrachtungen an.
Fragestellungen:
Handelt es sich um einen Sensor oder Aktor?
Wird die Komponente in einem redundanten System verwendet oder nicht?
Macht der Hersteller eine Aussage was das begrenzende Element ist und ob das speziell geprüft werden kann?
Ein Teilnehmer vertrat die Meinung, dass auch ein Austausch als neue Fehlerquelle gelten kann – auch weil nach Jahren kein identisches Ersatzgerät zu bekommen ist.
Bei einer SSPS (als sehr komplexe Komponente) kann eine solche Prüfung allerdings nicht er-bracht werden - daher sehen deren Hersteller die Angabe der Nutzungsdauer als verbindlich an.
Fazit: Bei einer Nutzung über die vom Hersteller angegebene Nutzungsdauer, geht die Verantwortung an den Betreiber über. Die Proof Tests (Intervalle) sind für eine solche Nutzung zu überdenken. Wo möglich können diese Komponenten noch in Nicht-Sicherheits-An-wendungen eingesetzt werden.
Die aktuelle DIN EN 61508-2 beschreibt Möglichkeiten in einer Fußnote, die NA106 gibt konkretere Hinweise.

4. Ist eine (vollständige) Abnahme eines Schutzkreises durch einen Sachverständigen erforderlich, wenn Komponenten im Kreis nicht 1:1 ausgetauscht wurden? Beziehungsweise welchen Maßnahmen werden in solch einem Fall ergriffen?

Grundsatzfrage: was ist überhaupt ein 1:1 Austausch? Reicht die HW, oder muss auch die SW identisch sein? Genügt es schon wenn die Ex-Kenndaten identisch sind?
Hierzu wurde auf die TRBS1115 Kapitel 8.3.3 verwiesen: *„Falls der Austausch von Bauteilen zu einer Änderung der sicherheitsrelevanten Eigenschaften der sicherheitsrelevanten MSR-Einrichtung führt, ist eine Überprüfung der Wirksamkeit der Schutzmaßnahmen der sicherheitsrelevanten MSR-Einrichtung notwendig.“*
In Kapitel 8.3.2 ist beschrieben, wann es sich um eine prüfpflichtige Änderung handelt.
Es wurde auch darüber diskutiert, ob es eine ZÜS (Zugelassene Überwachungs-Stelle) sein muss. Allerdings sei dieser Begriff nicht geschützt. In der TRBS seien aber auch Kriterien für Prüfer beschrieben.
In der Diskussion wurde darauf hingewiesen, dass die kritischen Punkte übereinstimmen müssen. (Einzelfallbetrachtung). Um eine Beeinträchtigung der Sicherheitseinrichtung auszuschließen wäre eine neue Betrachtung mit unabhängigem Dritten (Sachverständiger) erforderlich.
Des Weiteren wurde auf die NE126 (bezüglich Bestandsschutz) hingewiesen. Bei Überarbeitung entfällt aber der Bestandsschutz. Man müsse immer darüber nachdenken, bewerten und dokumentieren, ob die Sicherheit beeinträchtigt ist und ggf. Maßnahmen ergreifen. Sich auf Bestands-schutz zu berufen sei der falsche Weg.

5. Was sollen Prüfanweisungen für die Erst- und Wiederholungsprüfung enthalten bzw. gibt es Beispiele dafür wie diese aufgebaut sind?

Ein Anwender gab folgend „Schlagworte als Beispiel: – Sichtprüfung außen, Sichtprüfung An-schlüsse, „wedded parts“. Genauigkeit, Settings, Delay, Fehlergrenzen, - stimmen diese mit dem PLS überein; Prozessarbeitsschritte. Er verwies auch darauf, dass Reparaturen zu protokollieren seien.
Die „useful lifetime“ wird innerhalb des Maintenance Management separat geregelt.
Eine Teilnehmerin verwies auf die Handbücher. Dort sind mittlerweile gute Vorgaben gegeben.
Ein weiterer verwies auf die VDI 2180 Blatt 2 und NA106.

6. Welche Qualifikation wird bei den Prüfern bei Erst- und Wiederholungprüfungen gefordert?

Der Referent einer Prüfstelle verwies darauf dass dies jeder Betreiber selbst entscheiden müsse. **Oft werden 3 Jahre für Stufe 1 mit externer Prüfung, dann weitere Qualifikationen für die Stufe 2, bis zur Stufe 3 (z.B. Mitarbeit im Normengremium) genutzt.**
Dies gelte auch für externe Dienstleister. Diese müssten sich auch Gedanken über die Qualifikation ihrer Mitarbeiter machen. Der Auftraggeber sollte diese Nachweise der Qualifikation prüfen (verlangen).
Ein weiterer Teilnehmer aus der Industrie meinte dazu: „Ausbildung, Erfahrung, Training ist die übliche Reihenfolge. Im Arbeitsprozess stellt sich die Frage: „Was mache ich wenn ein Fehler auftritt und was muss im Prozess beachtet werden.“ Auch verschiedene Regelwerke (TRBSen) geben das vor.

7. Müssen nach einem Austausch einer SPS E/A Karte (Karte wird gesteckt, Verkabelung ist nicht betroffen) die entsprechenden Signalkreise wieder geprüft werden? Falls ja, in welchem Umfang?

Bei HIMA muss das nicht geprüft werden. Laut Anwender wurde im speziellen Fall eine HIMax – XDO Karte getauscht aber es gab Diskussionen ob und in welchem Umfang nun geprüft werden muss.
Der Referent antwortete, dass bei der HIMax keine Verwechslungsgefahr bestünde, und daher keine Prüfung durchgeführt werden muss.
Ein Referent gab zu bedenken dass es bei speziellen 19“ Karten leider aus Ex-Gründen eine andere Steckleistenbelegung gab. Daher hatte die Nachfolgekarte eine andere Funktion und es musste daher getestet werden. Daher hängt es wohl auch vom Einzelfall ab.

8. SIL-Berechnung: Armatur nicht bekannt – Reicht das Rechnen bis zum Magnetventil aus? Da Aktorik (Armatur) Mechanik?

Ein Referent aus der Industrie verwies auf die VDE 2180 - Blatt 4 – bei Mechanik würde mit typischen Werten (100 FIT) gerechnet.
Prüfstellen richten sich auch nach der VDE 2180 und schauen nach der Applikation, systematische Eignung muss stimmen (z. B. geeignete Materialbeständigkeit der Armatur und Dichtungen, Auslegung des Antriebs, etc.). Rechnen sei nicht so relevant.
Die Anlagenplanerin gab zu bedenken, dass bei einer unbekannten Armatur Eignung nicht bekannt wäre weil auch nicht geprüft. Fraglich, wie dann systematische Fehler ausschließbar sind. Es sollte doch Prüfanweisungen und / oder Nachweise geben um auf Eignung rückzuschließen.
Es wurde auch auf die Unterscheidung zwischen berechnen und betrachten hingewiesen. Ein SIL-Nachweis ist nicht nur die Berechnung. Man könne auch bis zum Ventil rechnen, muss aber die Betrachtung für den kompletten „Zweig“ (Pfad) durchführen.

9. Ist es von Nöten beim Tausch (anderer Hersteller) einer sicherheitsgerichteten Steuerung eine Neubetrachtung vorzunehmen? Software, Sensorik, Aktorik und Sicherheitsfunktionen bleiben dabei unberührt. Handelt es sich um eine wesentliche Veränderung? Allgemein: Wann kann ich von Bestandsschutz ausgehen? Welche Voraussetzungen müssen erfüllt sein? Die Fra-gen beziehen sich in Hinsicht auf die Funktionale Sicherheit und die Maschinenrichtlinie.

Ein Hersteller meinte dazu, dass es dafür auch in der MRL (Maschinenrichtlinie) Papiere gäbe.
Bei einer Modernisierung ohne wesentliche Änderung (wie definiert) sei keine Neubetrachtung not wendig.
Auch von Betreibern kam die Einschätzung, dass eine Neubetrachtung des Risikos oder der gleichen Technik, bei Modernisierung nicht nötig / zwingend sei aber ausgiebige Tests erfolgen soll-ten.
Der Fragesteller wollte weiterhin wissen, ob er validieren und verifizieren muss, oder was getan werden müsse. Aus der Industrie wurde auf die NE 126 Anhang 4 verwiesen - verifizieren auf je-den Fall.
Validierung nicht wenn wie hier beschrieben alles gleich bleibt. Vorsicht ist aber bei Bewertung von Relais durch einen SPS-Eingang geboten - dann sei die SPS schneller und reagiere auch auf EMV oder Schalterprellen. Es gebe einen fließenden Übergang in der Norm zwischen V&V. Daher sei dies auch eher eine Grauzone.
Ein Teilnehmer gab an, dass bei Änderung an einer alten Anlage auch die Sicherheitsbetrachtung neu durchgeführt werden muss - da gibt es keinen Bestandsschutz. Das gibt auch die BetrSichV so vor.
Wenn keine wesentliche Änderung vorgenommen wird, dann kann auch nur eine Teilbetrachtung erfolgen. Aber bei einer wesentlichen Änderung gebe es keine Ausrede. Dann muss alles neu betrachtet werden, nach allen Regeln.
TRBS verlangt immer einen risikobasierten Ansatz. Daher muss immer eine Risikobewertung durchgeführt werden.

10. Ist bei einer schadensbegrenzenden Maßnahme, wie bei einer schadenverhindernden Maßnahme ebenfalls ein rechnerischer Nachweis der Ausfallwahrscheinlichkeit (SIL-Berechnung) vorzuweisen?

Ein Referent antwortete: „Wenn man bei der Risikobetrachtung Kredit daraus zieht ja, sonst nicht.“ Dies ist wie so oft von einer Einzelbetrachtung abhängig.

11. Welche Funktionen müssen in der Firmware eines Feldgerätes implementiert sein, um SIL2 Zertifizierung zu erreichen? Wie hoch ist der Entwicklungsaufwand für die Software, wenn von NULL gestartet wird? Wie komme ich zu weiteren Unterlagen/Spezifikation, in denen zu implementierende Funktionen beschrieben werden?

HIMA gibt für 1 Stunde Änderung ca. 10 Stunden Prüfung als Richtwert. Der Unterschied in der SW für SIL2 und SIL3 sei nicht sehr hoch. Eine generische Antwort ist schwierig, hängt von Fak-toren wie der Risikoanalyse, Aufbau, erforderliche Komponenten und Maßnahmen, common cause und Diagnose ab.
Der größte Aufwand ist die Dokumentation.
Andere Teilnehmer gaben an, dass der Mehraufwand vermutlich mit einem Faktor zwischen 3-5 beziffert werden kann.

12. Häufig wird in Multi Purpose-Anlagen eine Abhängigkeit einer Sicherheitsfunktion von einer Betriebsart oder einer Wegstellung/Wegwahl gewünscht. Wie kann ich damit umgehen? Ist es zulässig z.B. eine Stellungsrückmeldung einer Armatur als "Freigabe" einer Sicherheitsfunktion zu verwenden? Wenn ja, wie muss ich diese Abhängigkeit im Nachweis darstellen/berechnen?

Ein Teilnehmer meinte dazu, dass die Pumpensteuerung nicht sicherheitsrelevant sein müsse. Nur die Armatur da diese das sicherstellende Element ist.
Prüfstellen sehen kritisch dass z.B. die Pumpe nicht mehr Drehmoment hat als die Armatur verkraften kann. Dann könne auch das Schaltsignal von der tatsächlichen Stellung abweichen.
Da sie die Sicherheitsfunktion beeinträchtigen kann muss die Überwachung in die Betrachtung / Berechnung mit berücksichtigt werden.

13. NAMUR Papier - Gerätegebrauchsdauer – Umgang mit Herstellerangaben: Die Betrachtungen im genannten NAMUR Dokument beziehen sich auf „PLT-Geräte“. Sind darin auch die fehlersicheren Steuerungen inkl der IO-Module eingeschlossen? Können aus Sicht des NAMUR AK die ursprünglich von den Herstellern ermittelten PFD-Werte und die damit verbundenen SIL-Berechnungen auf Basis dieser Betrachtungen auch jenseits der zugundeliegenden Gebrauchsdauer / Mission Time als weiterhin gültig angesehen werden, insbesondere wenn keine Proof-Tests vorgesehen bzw. möglich sind?

Ein Referent gab dazu an, dass es ab und an den Fall gäbe, dass der Betreiber keinen Proof Test machen möchte. Doch wie kann man dann sicherstellen, dass ein Ventil nach der Lebens-dauer noch das tut was es soll. Es müsse auch bei einem Austausch das Gerät noch einmal geprüft werden, um nachzuweisen, dass das Gerät bei Ende der Gebrauchsdauer noch die Funktion erfüllt hätte. Dies trage entscheidend zur Ermittlung einer realen Gebrauchsdauer bei.
Ein Hersteller gab an, dass niemand gezwungen würde das Gerät nach 20 Jahren zu tauschen, aber ein Nachweis dass man sich als Betreiber noch im Rahmen der geforderten PFD befindet (Ausfallrate) wäre erforderlich.
Der Kunde muss mehrere dieser Geräte in Betrieb haben um die Ausfallrate auch bestimmen zu können. Dazu gehöre auch die Betrachtung von gleichen Geräten, die nicht in sicherheitsgerichteten Anwendungen genutzt werden. Wenn die Ausfallrate ansteigt, egal ob in sicherheitsgericheten Anwendungen oder nicht stellt das einen Hinweis auf die Notwendigkeit eines Austauschs dar.
Es kam noch der Hinweis, dass nur der Hersteller einen Proof Test angeben könne.
Eine weitere Anmerkung verwies darauf, dass das Gerät unendlich betrieben werden könnte wenn im Prozess alle gefährlichen Fehler aufdeckbar sind - alle gefährlichen Fehler können aber meist nicht aufgedeckt werden.
Es ist eigentlich davon auszugehen dass z.B. ein Sensor eine Stunde nach proof Test immer noch funktioniert - wenn das Ende der theoretischen Lebensdauer schon überschritten sei wäre das aber nicht immer gegeben.
Fazit: Der Betreiber übernimmt bei Abweichung von Herstellerangaben die Verantwortung – er muss sich sicher sein.

14. Herr Laible hat in seinem Vortrag erwähnt, dass bei Sicherheitsfunktionen eine "Fail Safe"-Verhalten gefordert wird. Woher kommt diese Forderung (Quelle) und gibt es eine Definition, was "Fail Safe" bedeutet?

Laible: Im Rahmen von KI (Article 15 of proposal for a regulation of the eu parliament and of the council) für “high risk” Systeme ist fail safe gefordert.
Ein anderer Referent gab zu bedenken, dass die 61508 das Gegenteil aussage.

15. Dokumentation – SSPS Firmware update Dokumentation: Welche Arten von Änderungen an den Steuerungssystemen erfordern ein MOC (Management of Change)?

Prüfstellen verweisen auf die Vorgaben des Herstellers. Wenn sich die Signatur ändert müsse das dokumentiert werden. Bei HW-Änderungen erst recht.
Der Referent von HIMA meinte, man könne die Firmware von der Applikation trennen. Wenn es Änderungen am CRC gibt dann muss das in der MOC beschrieben werden. Bei Firmware Änderungen (z.B. im Modul) ist das Zertifikat maßgebend. In TÜV-Revisionslisten sind die Ausgabe-stände gelistet. Wenn das Upgrade dem Zertifikat entspricht, dann muss keine MOC Dokumentation erfolgen.
Wenn Funktionsänderungen (der Firmware) eine CRC Änderung der Applikation ergeben, und das vom TÜV Dokumentiert ist (vom Hersteller), dann muss auch kein MOC erfolgen.
Ein Referent aus der Industrie hielt entgegen, dass nicht jeder Hersteller so sei. Ein Hersteller hatte ihm einmal angeboten den Aufbau im Werk selbst zu prüfen was der Anwender gar nicht kann.

16. Wie werden BPCS Funktionen betrachtet? Diese sind zwar nicht SIL, aber zumindest die vor-geschaltete Maßnahme, um in den low demand mode zu kommen. Wie oft und in welche Tiefe sollten diese geprüft werden?

Der Referent der Firma HIMA antwortete darauf, dass eine BPCS (BPCS=Basic Process Controll System (also die “normale” Prozessleittechnik)) keine probabilistischen Werte hätte, und man da-her nicht rechnen könne. In der EN 61511 Teil 2 soll das aber ausführlicher erklärt sein.
Von Betreiberseite kam der Hinweis auf die NE165. Ein Teilnehmer meinte dass sich diese Regelwerke unterscheiden (Widersprüchlich seien). Eine Erklärung dazu von Dr. Hildebrandt:
Die IEC 61511 und die VDI/VDE 2180 unterscheiden sich an dieser Stelle. Der Grund dafür ist folgender:
Wenn die Amerikaner (also IEC 61511) von BPCS sprechen, dann haben sie ein System vor Au-gen, das typischerweise aus mehreren unabhängigen Teilsystemen besteht. Wenn die Anlage ausfällt und nicht mehr so läuft wie es sein soll, dann ist nach deren Sicht nicht das gesamte BPCS ausgefallen, sondern nur ein bestimmter Teil davon. Andere Teile des BPCS laufen noch und daher können diese (noch funktionierenden Teile) eine Sicherheitsfunktion übernehmen. Also kann man mit dem BPCS ohne „Klimmzüge“ risikomindernde Funktionen realisieren.
In Deutschland versteht man das BPCS eher als eine homogene Einheit. Wenn das BPCS nicht mehr wie vorgesehen funktioniert, dann unterstellt man, dass auch eine Sicherheitsfunktion, die mit diesem (kaputten) BPCS realisiert wurde, evtl. nicht mehr funktioniert. Daher fordert die VDI/VDE2180, dass man mit besonderen Maßnahmen die „BPCS-Sicherheitsfunktionen“ so realisiert, dass dies nicht geschehen kann.
Diese Diskussion wird schon sehr lange und leidenschaftlich geführt.

17. Gibt es normative Anforderungen oder betriebliche Leitfäden, z.B. NAMUR-Empfehlungen, zur Realisierung von Bedienfunktionen, die im laufenden Betrieb des SIS durch einen Operator durchgeführt werden können. Z.B. • Quittierung von Gerätefehlern und anschließende Wiedereingliederung in die SIF • Ändern von Grenzwerten im Rahmen von vorher fest definierten Bereichen • Überbrückungen von Signalen zur vorbeugenden Instandhaltung von Geräten

In der 61511-1 Kap. 16 werden „compensating measures“ gefordert.

Kompensierende Maßnahmen sind erforderlich
Die Anlagenplanerin berichtete, dass nur sie als Dienstleister das Passwort wenn sie bei sehr kleinen Firmen die SPSS programmieren. Als weiterer Hinweis kam ein Verweis auf die VDE 2180 Blatt 2 für eine genauere Erklärung - oder die NE154 für Batchbetrieb).
Von Betreibern kam der Verweis auf die NE154. Typischer Fehler bei Änderung von Schaltpunkten ist die Befragung des Instrumentierers - der kenne die Anlage am besten.
Ein weiterer Teilnehmer gab an, dass das HAZOP Team darüber spreche und es würde abgestimmt.
Ein Schlüssel-Schalter ist normativ nicht vorgegeben, sei aber vorzusehen aus gesundem Menschenverstand.