

## 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.