



## Funktionale Sicherheit in der Prozesstechnik mit der Sicherheitsnorm IEC 61511

Viertägige Personenzertifizierung mit wahlweiser Qualifizierung als  
**Functional Safety Certified Engineer Application (FSCEA)**  
incl. Demotools zur Durchführung von Schutzkreisberechnungen

Die Personenzertifizierung funktionale Sicherheit bei TÜV NORD: Wir freuen uns, unser Angebot zum Thema **Funktionale Sicherheit für Prozessingenieure** ankündigen zu können. Im Fokus steht die **überarbeitete IEC 61511**, die sich im wesentlichen an die Prozessindustrie einschließlich Chemieindustrie, Raffinerien, Öl- und Gasförderung, Papierherstellung, konventionelle Stromerzeugung, etc. richtet. Bei Teilnahme aller Workshopmodule besteht die Option einer Qualifikationsprüfung zum zertifizierten **Functional Safety Certified Engineer Application (FSCEA)**.

Die IEC 61511 beschreibt die Anwendung sicherheitstechnischer Systeme (SIS) in der Prozessindustrie und insbesondere die notwendigen Tätigkeiten im Sicherheitslebenszyklus um die Mindestanforderungen an ein SIS zu erfüllen. Mit dieser Personenzertifizierung möchten wir insbesondere folgenden Personenkreis ansprechen:

- Ingenieure aus Produktsicherheit und Sicherheitsmanagement.
- Anwender und System-Errichter sicherheitstechnischer Systeme
- Prozessingenieure, die im Bereich der Entwicklung und Prüfung von sicherheitstechnischen Systemen tätig sind.
- Führungskräfte, die sich mit dem Thema der funktionalen Sicherheit und der IEC-Norm 61511 beschäftigen müssen.
- Qualitätsmanagementbeauftragte die für die Einhaltung der IEC 61511 verantwortlich sind.

Wer am zweiten und dritten Tag des Workshops teilnimmt, erhält darüber hinaus **Tools zur Unterstützung bei der Berechnung von Sicherheitsketten** als Demoversion.

Die Teilnehmerzahl ist auf 20 Personen beschränkt. Die Anmeldung ist so lange möglich, bis der Workshop ausgebucht ist. *Für die Anmeldung füllen Sie entweder das beigefügte Formular aus und senden es per Fax an die Nummer 0821-450954-4269 zurück, oder Sie registrieren sich innerhalb der Anmeldefrist unter <http://www.tuev-nord.de/>. Ihre Fragen beantworten wir gerne entweder telefonisch unter 0821-450-954-0 oder per E-Mail [samoeller@tuev-nord.de](mailto:samoeller@tuev-nord.de).*



## Inhalte

### **Modul 1: (eintägig)**

#### **Funktionales Sicherheitsmanagement (FSM)**

#### **Lebenszyklusmodell – vom Konzept über die Gefährdungs- und Risikoanalyse bis zur Ausserbetriebnahme**

Hersteller und Betreiber von sicherheitsrelevanten technischen Einrichtungen und Produkten werden durch das ProdSG und BetrSichV verpflichtet, ihre technischen Systeme entsprechend dem Stand der Technik in allen Aspekten der Sicherheit zu entwickeln, aufzubauen und zu betreiben. Die Beweislast im Schadensfall obliegt dem Errichter bzw. Betreiber einer technischen Anlage. Das Workshop-Modul 1 liefert eine Übersicht über die Abgrenzung der Bereiche Feuerungstechnik (IEC 50156), Maschinenindustrie (ISO 13849) und Prozessindustrie (IEC 61511), sowie eine Darstellung der hierbei anzuwendenden Richtlinien. Weiterhin beinhaltet das Modul die normativ geforderten Vorgehensweisen im Rahmen von Entwicklungs-, Instandhaltungs-, Prüf und Änderungstätigkeiten. Die erforderlichen Verantwortlichkeiten von Mitarbeitern, Anforderungen an die Kompetenz der handelnden Personen, organisatorische Aspekte und Kenntnisse zu rechtlichen Aspekten und die möglichen Konsequenzen bei Versagen eingesetzter PLT-Schutzeinrichtung bestehend aus Feldgeräten, Steuerungen, Hard- und Software sowie die Anwendung des „Vier-Augen-Prinzips“ über den gesamten Lebenszyklus durch Verifikation von Arbeitsergebnissen durch eine zweite Person, die nicht direkt in den selben Arbeitsschritt eingebunden war, werden erörtert.

Dazu werden Überlegungen zur Einführung eines Functional Safety Management (FSM)-Systems (Management der funktionalen Sicherheit) unter Berücksichtigung der Aufgaben/Rollen der am Prozess beteiligten Personen wie Safety Manager und Safety Coordinator präsentiert. Der gesamte Lebenszyklus einer technischen Anlage vom Konzept über die Gefährdungs- und Risikoanalyse bis zur Ausserbetriebnahme - wird anhand praktischer Übungen erklärt. Dabei wird anhand repräsentativer Beispiele intensiv auf die von der IEC 61511 empfohlenen Methoden zur interdisziplinären Ermittlung des Safety Integrity Level – SIL mittels Risikograph und Layer Of Protection Analysis - LOPA und die Ableitung der daraus resultierender funktionaler Sicherheitsanforderungen eingegangen.




## **Modul 2 (zweitägig): Entwurf der sicherheitstechnischen Schutzeinrichtungen Maßnahmen beim Einsatz von Geräten in Schutzeinrichtungen, Anforderungen an die Auswahl betriebsbewährter (prior use) Komponenten, Erfassung und Analyse von Fehlern in PLT-Schutzeinrichtungen und Berechnung der Schutzkreise gemäß IEC 61511**

Damit sicherheitstechnische Schutzeinrichtungen robust gegenüber Fehlern sind, fordert die IEC 61511 Maßnahmen gegen systematische Fehler, Maßnahmen gegen zufällige Fehler sowie Maßnahmen zur Fehlertoleranz. Für jede Schutzeinrichtung/sicherheitstechnische Funktion müssen also diese Maßnahmen gleichzeitig beachtet werden. Das Workshop-Modul 2 zeigt an praxisnahen Beispielen auf, wie systematische Fehler in Schutzeinrichtungen, wie z.B. die Verwendung von falsch dimensionierten Bauteilen, oder die Verwendung ungeeigneter Materialien für den Prozessanschluss usw. vermieden werden können. Dabei wird unterschieden zwischen systematischen Fehlern die sich im eingesetzten Subsystem selbst befinden können und systematischen Fehlern, die sich durch den Einbau dieses Subsystems in eine bestimmte Anlage ergeben können.

Als Maßnahme gegen zufällige Fehler fordert die IEC 61511 eine Ausfallwahrscheinlichkeit einer Schutzeinrichtung unterhalb eines vorgegebenen Werts. Beim Entwurf sicherheitstechnischer Systeme werden wesentliche Anforderungen an die Ermittlung der Restfehlerwahrscheinlichkeit ( $PFD_{avg}$ / PFH) von Schutzkreisen, d.h. die Bewertung von Schutzkreisen bezüglich ihrem quantitativen Ausfallverhalten, gestellt. Insbesondere ist zwischen Systemebene und Subsystemebenen zu unterscheiden. Das Gesamtsystem, z.B. bestehend aus Sensor, Logik und Aktuator, muss die geforderte Sicherheitsintegrität der Sicherheitsfunktionen erreichen. Alle Komponenten, inklusive der relevanten Software-Komponenten die zur Ausführung einer Sicherheitsfunktion zur Risikoreduktion beitragen, müssen gemeinsam betrachtet werden. Die SIL-Fähigkeit jeder Komponente muss dabei für den SIL der Funktion ausreichen.

Hersteller, Planer und Betreiber von Schutzkreise werden für den Nachweis einer Risikominderung vor verschiedene Aufgabenstellungen gestellt und müssen dabei folgende Fragestellungen beantworten:

- Welche quantitativen Anforderungen stellen die Standards IEC 61511 und ISO 13849?
- Wie sind diese mit Sicherheitsintegritäts -/ Performance - Level SIL/ PL verknüpft?

- 
- Wie wirken sich verschiedene Sicherheitsarchitekturen aus und welche werden gefordert?
  - Wie werden Ausfälle infolge gemeinsamer Ursache berücksichtigt?
  - Wie können die Ausfallwahrscheinlichkeiten  $PFD_{avg}$ , PFH von Schutzkreisen ermittelt werden?
  - Was ist der Anteil ungefährlicher Ausfälle SFF und der Diagnosedeckungsgrad DC
  - Wie werden Testintervalle, Reparaturzeiten berücksichtigt und optimiert?
  - Wie können Tools die Lösung der Aufgabestellungen bei der Berechnung des Ausfallverhaltens von Schutzkreisen unterstützen?

Im letzten Abschnitt dieses Moduls wird die Anforderung zu den Maßnahmen hinsichtlich der erforderlichen Fehlertoleranz in Abhängigkeit des zu erreichenden SIL durch mögliche HW-Architekturen von Schutzkreisen gegenübergestellt.

Gegenstand des Workshops-Moduls 2 ist Antworten und Lösungswege zu den oben beschriebenen Fragenkomplexen aufzuzeigen. Hierbei wird insbesondere auf die eigenständige Ermittlung der normativ geforderten quantitativen Werte (u.a. mit der Hilfe von Tools) Wert gelegt.

In diesem Workshop wird weiterhin auf die Anforderungen an die Betriebsbewährtheit (Prior Use) von Komponenten entsprechend IEC 61511 eingegangen. Die Erfüllung und Umsetzung der Anforderungen stehen hierbei im Vordergrund und werden anhand von Beispielen veranschaulicht.

### **Modul 3 (eintägig): SIS Software und Dokumentation**

#### **Anforderung an die Entwicklung von SIS Software und an die projektspezifische Dokumentation**

Über die Vorschriften bisheriger Software-Qualitätsstandards hinaus sieht die IEC 61511 weitere softwarebezogene Anforderungen mit dem Fokus auf funktionale Sicherheit vor.

In diesem Modul wird auf die drei Arten von Software (Anwendungssoftware, Software Hilfsmittel und Embedded Software) und die drei Sprachtypen (feste Programmiersprachen, Programmierungssprachen mit eingeschränktem Sprachumfang und Programmierungssprachen mit nicht eingeschränktem Sprachumfang) zur Erstellung von



Software eingegangen. Die Anforderungen entsprechend IEC 61511 an die SIS Software werden hierbei anschaulich vermittelt.

Ein weiterer wichtiger Bestandteil bei der Entwicklung von SIS ist die Dokumentation. Die IEC 61511 verlangt, dass die notwendigen Informationen vorliegen und in einer Form dokumentiert sind, dass alle Phasen des Lebenszyklus effektiv durchgeführt werden können und dass Verifikation, Validierung und Maßnahmen zur Beurteilung der funktionalen Sicherheit effektiv durchgeführt werden können.

In diesem Modul wird detailliert und anschaulich auf die Anforderungen an die Dokumentation entsprechend IEC 61511 eingegangen.

Zum Abschluss des Moduls erfolgt eine prüfungsvorbereitende Fragerunde.

#### **Modul 4 (halbtägig): Qualifizierungsprüfung zum Functional Safety Certified Engineer Application (FSCEA)**

Interessierte Teilnehmer können sich zur FSCEA-Qualifizierungsprüfung anmelden. Voraussetzung dafür ist die Teilnahme an den Modulen 1-3. Nach erfolgreichem Absolvieren der Prüfung erhalten sie von TÜV NORD Systems ihr persönliches FSCEA-Zertifikat. Die Prüfungsfragen werden auf Deutsch gestellt und können in Deutsch beantwortet werden. Die Vorträge werden in deutscher Sprache gehalten. Die Zertifizierung ist drei Jahre lang gültig und kann durch den Besuch eines Folge-Workshops mit anschließender bestandener Wiederholungsprüfung um weitere drei Jahre verlängert werden. Um eine weitergehende Zertifizierung zum Functional Safety Certified Coordinator Application bzw. Consultant Application (FSCCA) bzw. Functional Safety Certified Manager Application (FSCMA) zu erhalten, müssen Sie mindestens zwei bzw. vier Jahre berufspraktische Erfahrung anhand relevanter Sicherheitsprojekte nachweisen und ein von TÜV NORD durchgeführtes Qualifizierungs-Audit erfolgreich bestanden haben. Weiterführende Informationen entnehmen Sie bitte aus unserem Flyer „IEC 61511 Personenzertifizierung“