Anforderungen an Prüfer der funktionalen Sicherheit

Von Johann Ströbl

Die häufigsten Fehler im Design von Schutzkreisen und ihren Sicherheitseinrichtungen sind systematische Fehler, die durch entsprechende Maßnahmen vermeidbar sind. Die DIN EN 61508 [1] fordert deshalb unabhängige Beurteilungen und formuliert umfassende Anforderungen an die Prüfungen. Besondere Qualifikationen der Prüfer verlangt sie indessen nicht. Allerdings: Um systematische Fehler bei Schutzkreisen und Sicherheitseinrichtungen zuverlässig zu vermeiden, muss auch die Qualifikation der Prüfer sehr wohl bedacht werden. Dafür eignet sich ein dreistufiges Aus- und Weiterbildungskonzept, das auch klare Voraussetzungen für die Teilnahme fordert.

Fehler, die dazu führen, dass ein technisches System versagt, lassen sich zwei Kategorien zuordnen: systematische Fehler und zufällige Fehler. Letztere sind prinzipiell nicht zu vermeiden. Folglich müssen bei zufälligen Fehlern Maßnahmen zur Fehlerbeherrschung umgesetzt werden. Dafür gibt es verschiedene Möglichkeiten wie eine entsprechende Architektur der Sicherheitseinrichtung (zum Beispiel redundante Systeme) oder eine Berechnung der Ausfallwahrscheinlichkeiten der Sicherheitskreise. Systematische, also menschengemachte Fehler hingegen lassen sich grundsätzlich verhindern. Schließlich sind sie bei einem systematischen, risikobasierten Ansatz per Definition während der gesamten Lebensdauer des Systems stets vorhersehbar.

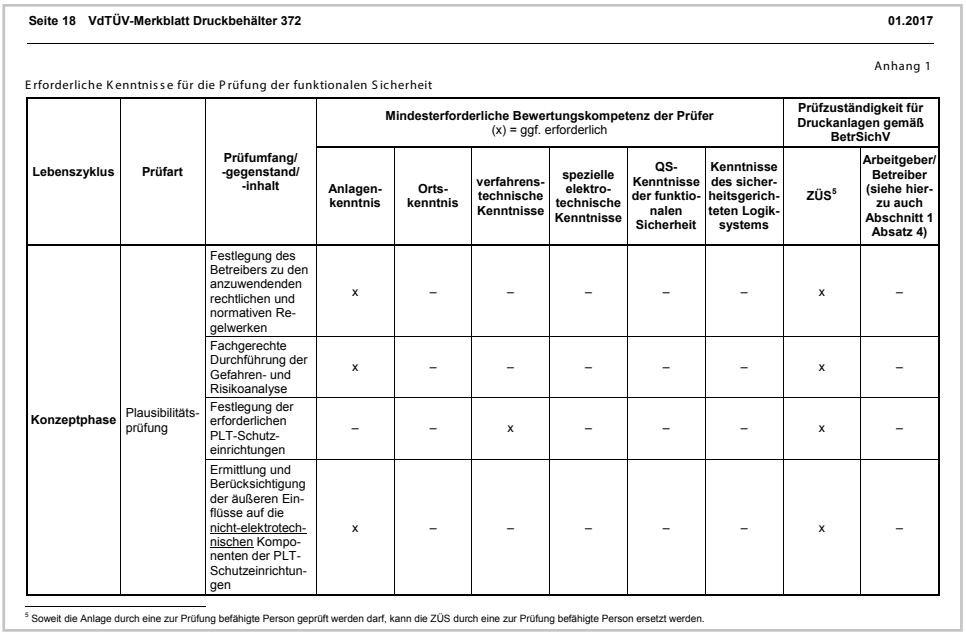
Laut einer Studie der britischen Health and Safety Executive (HSE) [2] waren 85 Prozent aller bei Sicherheitseinrichtungen auftretenden Fehler systematische und nur 15 Prozent zufällige Fehler. Die Studie zeigt außerdem, dass die Kosten durch Unfälle infolge fehlerhafter Sicherheitseinrichtungen in der Regel nur zu einem Bruchteil versichert sind. Der Großteil sind verdeckte Kosten wie etwa für die Aufarbeitung der Unfallursache, juristische Folgen oder Produktionsausfälle. Um sichere Arbeits- und verlässliche Produktions- und Investitionsbedingungen zu schaffen, gilt es also, Fehler zu vermeiden.

Der Sicherheitslebenszyklus von Sicherheitseinrichtungen der Mess-, Steuer- und Regelungstechnik (MSR) beschreibt und definiert die dafür erforderlichen Schritte. Sie reichen von der Ermittlung der Gefahren und der für den Einsatz erforderlichen Risikoreduzierung über die Planung, Errichtung und den Betrieb einer Sicherheitseinrichtung bis hin zur Außerbetriebnahme. Für die Abstimmung der geeigneten Maßnahmen ist ein Managementsystem der funktionalen Sicherheit erforderlich, um in allen Phasen des Sicherheitslebenszyklus die Planungs- und Beurteilungsschritte mit der erforderlichen Fachkenntnis durchzuführen.

Vorgaben für Sicherheitseinrichtungen

Die DIN EN 61508 als Grundnorm der funktionalen Sicherheit ist ein etabliertes und allgemein akzeptiertes Werkzeug für die Planung und das Design von Schutzkreisen. Von dieser Grundnorm ist für die Maschinensicherheit die Norm DIN EN 62061 sowie für die Sicherheit verfahrenstechnischer Anlagen die Norm DIN EN 61511 abgeleitet. Zudem basiert auch die für die Bewertung des Explosionsschutzes geltende Technische Regel für Gefahrstoffe (TRGS) 725 auf derselben Sicherheitsphilosophie wie die DIN EN 61508.

Die Norm folgt einem probabilistischen Fehleransatz, der mehr und mehr den jahrzehntelang angewandten deterministischen Ansatz ersetzt. Als Grundlage der probabilistischen Sicherheitsphilosophie dient das Lebenszyklusmodell, bei dem davon ausgegangen wird, dass eine in einer Gefährdungsbeurteilung ermittelte Gefahr für Leib und Leben von Menschen, für Sachen sowie für die Umwelt vermieden werden muss. Dazu muss das vorhandene Risiko beurteilt und auf ein tolerierbares Maß (= Restrisiko) reduziert werden. Das geschieht durch



Seite 18 VdTÜV-Merkblatt Druckbehälter 372 01.2017

Anhang 1

Erforderliche Kenntnisse für die Prüfung der funktionalen Sicherheit

Lebenszyklus	Prüfart	Prüfumfang/ -gegenstand/ -inhalt	Mindesterforderliche Bewertungskompetenz der Prüfer (x) = ggf. erforderlich						Prüfzuständigkeit für Druckanlagen gemäß BetrSichV	
			Anlagen-kenntnis	Orts-kenntnis	verfahrens-technische Kenntnisse	spezielle elektro-technische Kenntnisse	QS-Kenntnisse der funktio-nalen Sicherheit	Kenntnisse des sicher-heitsgerich-teten Logik-systems	ZÜS[5]	Arbeitgeber/ Betreiber (siehe hier-zu auch Abschnitt 1 Absatz 4)
Konzeptphase	Plausibilitäts-prüfung	Festlegung des Betreibers zu den anzuwendenden rechtlichen und normativen Re-gelwerken	x	–	–	–	–	–	x	–
		Fachgerechte Durchführung der Gefahren- und Risikoanalyse	x	–	–	–	–	–	x	–
		Festlegung der erforderlichen PLT-Schutz-einrichtungen	–	–	x	–	–	–	x	–
		Ermittlung und Berücksichtigung der äußeren Ein-flüsse auf die nicht-elektrotech-nischen Kompo-nenten der PLT-Schutzeinrichtun-gen	x	–	–	–	–	–	x	–

[5] Soweit die Anlage durch eine zur Prüfung befähigte Person geprüft werden darf, kann die ZÜS durch eine zur Prüfung befähigte Person ersetzt werden.

Bild 1: Auszug aus dem VdTÜV-Merkblatt Druckbehälter 372 [3]

eine Sicherheitsfunktion, die zum Beispiel die Verletzung einer Person durch eine sich schließende Aufzugstür verhindert, die wiederum durch eine Sicherheitseinrichtung, wie zum Beispiel ein Lichtgitter, realisiert wird. Je nach Einsatzgebiet und erforderlicher Gefahrenabsicherung kann das vom Not-Aus-Schalter über Zugangssperren wie Sicherheitstüren oder Schutzblechen bis zu berührungslos wirkenden Schutzeinrichtungen wie Lichtschranken reichen.

Diese Sicherheitseinrichtung muss für den entsprechenden Anwendungsfall geeignet sein und für die geforderte Risikoreduzierung ausreichen. Geeignet ist eine Sicherheitseinrichtung, wenn sie für den vorgesehenen Einsatzbereich funktional sicher ist. Funktionale Sicherheit bedeutet, dass ein Sicherheitssystem dann funktioniert und die Gefahr abwendet, wenn es gebraucht wird und einen sicheren Zustand herbeiführt, d. h. in unserem Fall, wenn es die Aufzugstür öffnet.

Unabhängig prüfen

Die DIN EN 61508 sieht neben Managementsystemen ein Vier-Augen-Prinzip vor: Während ein Team die Sicherheitseinrichtung plant, designt, aufbaut, in Betrieb nimmt, betreibt und unter Umständen außer Betrieb stellt, übernimmt ein unabhängiges Beurteilungsteam die Prüfung.

Dabei verlangt die Norm verschiedene Grade an Unabhängigkeit, je nach geforderter Risikoreduzierung, die in den Tabellen 4 und 5 der DIN EN 61508 beschrieben sind. In welchem Maß eine Sicherheitseinrichtung mögliche Risiken reduzieren muss, wird in Sicherheitsintegritätslevels (englisch: safety integrity level – SIL), angegeben. Diese Sicherheitsanforderungsstufen reichen von SIL 1 bis SIL 4 und sind ein Maß für den Grad der Risikoreduzierung des Systems. Die Risikoreduzierung ergibt sich aus der Zuverlässigkeit, den Schadensauswirkungen, der Häufigkeit und Dauer der Gefahrenexposition sowie der Möglichkeit, den Schaden zu vermeiden. Je höher das Risiko, desto höher ist die erforderliche Risikoreduzierung, also das SIL.

Abhängig davon ist die Anforderung an den Grad der Unabhängigkeit der beurteilenden Person. Bei Schutzkreisen mit einer Risikoreduzierung bis SIL 1 wird eine unabhängige, am Projekt nicht beteiligte Person zur Beurteilung gefordert. Diese darf aus der gleichen Abteilung kommen wie die Projektplaner. Ist eine Risikoreduzierung bis SIL 2 gefordert, soll die Beurteilung von einer Person vorgenommen werden, die nicht am Projekt

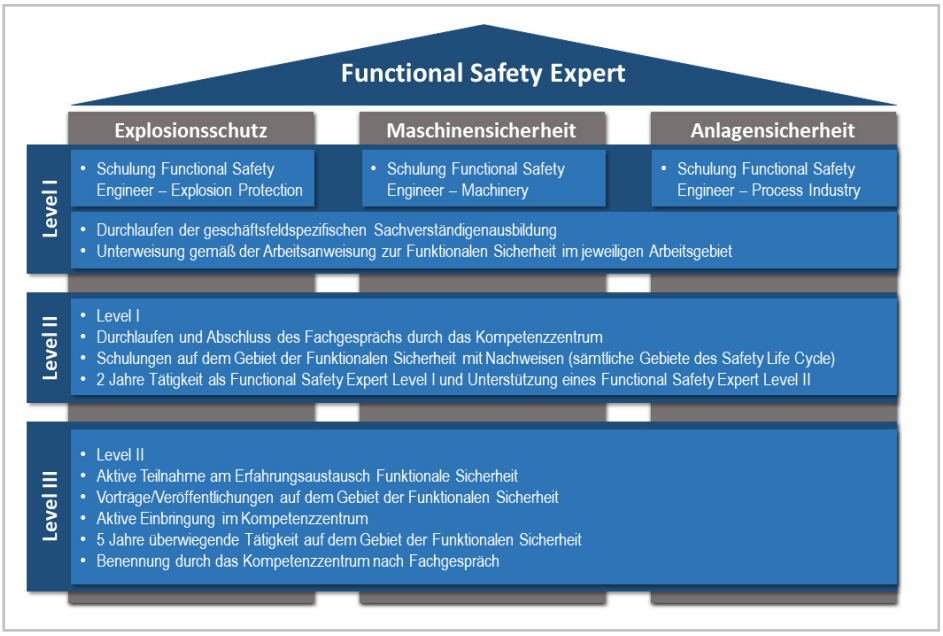


Bild 2: Ausbildungskonzept

beteiligt ist. Bei SIL 3 soll zur Beurteilung eine unabhängige Person herangezogen werden, die aus einer anderen, an dem Projekt nicht beteiligten Organisation kommt.

Prüfungsanforderungen

Für die an Sicherheitseinrichtungen verwendeten Komponenten gibt es klare normative Vorgaben für deren Eignung sowie erforderliche Eignungsnachweise für ihren Einsatz. Es ist derzeit kein großes Problem für Risikoreduzierungen SIL 1, 2 oder 3 geeignete Komponenten wie Sensoren, Steuerungen oder Aktoren zu finden.

Die DIN EN 61508 macht detaillierte Vorgaben zum Inhalt der Prüfung, den Prüfmitteln sowie zu den einzelnen Schritten und der Tiefe bei wiederkehrenden Prüfungen. Demgegenüber formuliert die Norm nahezu keine Anforderungen an die Qualifikation der Prüfer selbst. Auch die TRBS 1201-4 definiert keine detaillierten Anforderungen an die Qualifikation der Prüfer. Das VdTÜV-Merkblatt Druckbehälter 372 „Prüfung der funktionalen Sicherheit“ beschreibt in Teil 1 „PLT-Sicherheitseinrichtungen in Anlagen“, Anhang 1 die erforderlichen Kenntnisse für die Prüfung der funktionalen Sicherheit.

Qualifikation des Prüfpersonals

Im Hinblick auf die Vermeidung systematischer Fehler bei der Planung, Realisierung und Prüfung von Anlagen ist es erforderlich, die Qualifikation der am Beurteilungsteam beteiligten Prüfer näher zu definieren. Es ist auch hier sinnvoll, auf eine strukturierte Form der Aus- und Weiterbildung zurückgreifen zu können.

Im Folgenden wird ein Best-Practice-Beispiel beschrieben, das im Rahmen der Qualitätssicherung als unternehmensinternes Aus- und Weiterbildungskonzept dient. Entwickelt wurde es vom Kompetenzzentrum für funktionale Sicherheit innerhalb eines Prüfunternehmens. Zunächst sind spezifische Zugangsvoraussetzungen definiert, die gewährleisten sollen, dass sich ein potenzieller Prüfer für funktionale Sicherheit einen Überblick über die technische Ausführung einer Sicherheitseinrichtung verschaffen kann:

- eine elektrotechnische Ausbildung oder eine andere, für die vorgesehenen Prüfaufgaben geeignete, vergleichbare elektrotechnische Qualifikation oder Elektrofachkraft für festgelegte Tätigkeiten

- Erfahrung mit der Prüfung elektrischer Anlagen allgemein
- Grundkenntnisse auf dem jeweiligen Arbeitsgebiet
- Grundkenntnisse auf dem Gebiet der Gefährdungsbeurteilung, der Philosophie der funktionalen Sicherheit sowie im Umgang mit speicherprogrammierbaren Steuerungen
- Kenntnisse im Lesen von R&I-Schemata und Logikplänen sowie elektrischen Schaltplänen

Qualifikation in drei Stufen

Die eigentliche Ausbildung ist in drei Stufen gegliedert, mit denen verschiedene Berechtigungen und Aufgaben verbunden sind: Im ersten Schritt werden die Teilnehmer in einer 1,5-tägigen Einführung mit den Grundlagen der funktionalen Sicherheit vertraut gemacht. Hier werden unter anderem Begriffe der funktionalen Sicherheit, Unterschiede zwischen systematischen und zufälligen Fehlern, der Umgang mit mechanischen Komponenten, die Berechnung von Sicherheitskreisen und die Unterschiede zwischen Low, High und Continuous Demand Mode behandelt. Am Ende dieses Grundmoduls ist ein Leistungsnachweis vorgesehen.

Im Anschluss erfolgt eine Spezialisierung auf das jeweils gewünschte Arbeitsgebiet. Es gibt eigene Ausbildungslinien für die drei Bereiche Maschinensicherheit, Explosionsschutz und Sicherheit von Prozessanlagen. Dies ist nötig, weil sich die einzelnen Bereiche sowohl in der Terminologie als auch in den Verantwortungsbereichen (Hersteller, Betreiber) wesentlich voneinander unterscheiden. Auch hier erfolgt am Ende ein Leistungsnachweis je Modul. Die geschilderte 3-Level-Qualifikation ist in jeder der drei Ausbildungslinien identisch.

Nach bestandener Prüfung sowie nach der Unterweisung mit den einschlägigen Arbeitsanweisungen „Funktionale Sicherheit“ des jeweiligen Geschäftsfeldes (Elektro- und Gebäudetechnik, Fördertechnik, Anlagensicherheit) erhält der Sachverständige die FuSi-Level-1-Anerkennung und darf wiederkehrende Prüfungen von Sicherheitseinrichtungen auf der Basis der schon durchgeführten Abnahmeprüfungen alleine durchführen.

Nach zweijähriger Tätigkeit auf Level 1 und regelmäßigem Monitoring durch einen Level-2-Sachverständigen sowie einem Nachweis von Schulungen und Ausbildungen auf sämtlichen Gebieten des Safety Life Cycles kann der Sachverständige die Anerkennung für Level 2 beantragen. Es erfolgt eine Bewertung der bisher durchgeführten Tätigkeiten und der Schulungsnachweise sowie ein Fachgespräch mit Mitgliedern des Kompetenzzentrums für funktionale Sicherheit.

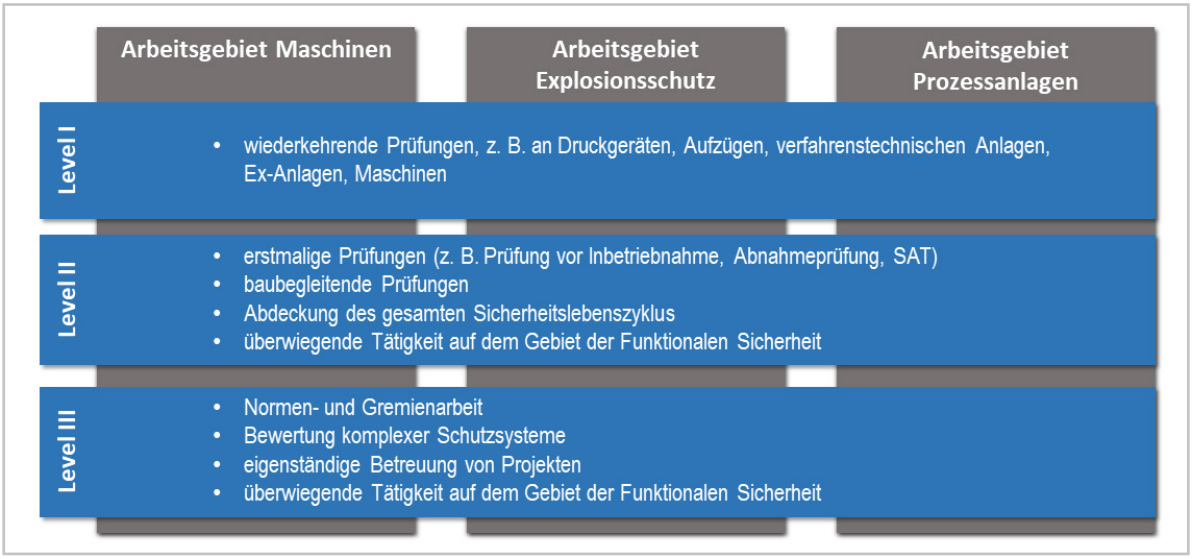


Bild 3: Tätigkeitsbereiche

Bild 4: Funktionale Sicherheit ist die Basis für die Zuverlässigkeit komplexer Anlagen

Bei positivem Abschluss bekommt der Sachverständige die Anerkennung für Level 2. Damit darf er erstmalige Prüfungen (zum Beispiel Abnahmeprüfungen, Site Acceptance Tests) an Systemen der funktionalen Sicherheit durchführen. Zu seinen Aufgaben gehören auch baubegleitende Prüfungen und Prüfungen über den gesamten Lebenszyklus einer Sicherheitseinrichtung. Um die Gültigkeit der Anerkennung zu erhalten, muss der Sachverständige überwiegend auf dem Gebiet der funktionalen Sicherheit arbeiten.

Nach weiteren drei Jahren überwiegender Tätigkeit auf dem Gebiet der funktionalen Sicherheit kann sich der Sachverständige um die Level-3-Qualifikation bewerben. Seine Aufgaben umfassen dann die aktive Teilnahme am Erfahrungsaustausch „Funktionale Sicherheit“, das Erstellen von Vorträgen und Veröffentlichungen auf dem Gebiet der funktionalen Sicherheit sowie die aktive Mitarbeit und Gestaltung im unternehmenseigenen Kompetenzzentrum für funktionale Sicherheit. Die Benennung des Level-3-Sachverständigen erfolgt durch das Kompetenzzentrum nach einem Fachgespräch.

Zur Aufrechterhaltung der Qualifikation der Sachverständigen wird ein jährlicher Erfahrungsaustausch durch das Kompetenzzentrum organisiert, wobei die Teilnahme für die anerkannten Sachverständigen verpflichtend ist. Die jeweiligen Anerkennungen werden über das unternehmensinterne Qualitätsmanagementsystem dokumentiert.

Quellen

[1] DIN EN 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

[2] HSE Health and Safety Executive: Out of Control – Why control systems go wrong and how to prevent failure. 2003

[3] VdTÜV-Merkblatt Druckbehälter 372, Ausgabe 01/2017

Dipl.-Ing. (FH) Johann Ströbl

TÜV SÜD Industrie Service GmbH