

Functional Safety Management in der Prozessindustrie

Ursachen bekämpfen statt Symptome kurieren



Aus Schaden klug zu werden, kann in der chemischen Industrie oder bei Feuerungstechnik und Verbrennungsanlagen teuer werden. Mit einem funktionalen Safety Management System lassen sich systematische Fehler vorab vermeiden. (Bild: Georg Lehnerer/fotolia)

In der Prozessindustrie aus Kostengründen auf Sicherheit zu verzichten, kann Anlagenbetreiber teuer zu stehen kommen. Ein drastisches Beispiel dafür ist die Ölpest im Golf von Mexiko, ausgelöst durch die Explosion der Ölplattform Deepwater Horizon. Eine Hauptursache der Explosion war die Abdichtung des Bohrlochs: Trotz Expertenwarnungen wurde eine kostengünstigere Lösung mit höherem Risiko von Gasaustritten gewählt. Rückblickend eine zu vernachlässigende Investition verglichen mit den Schadensersatzzahlungen an die US-Regierung in

zweistelliger Milliardenhöhe. Dazu kommt ein entstandener Schaden für das Firmenimage, die Umwelt und die betroffenen Menschen, der sich nicht beziffern lässt. Eine systematische Risikobeurteilung ist daher beim Anlagenbau unabdingbar, in der chemische Industrie ebenso wie in Verbrennungsanlagen.

Am falschen Ende zu sparen, kann für Unternehmen nicht nur in mehrerer Hinsicht teuer werden, sondern auch zu juristischen Kon-

sequenzen führen, denn die rechtlichen Vorgaben für den Einsatz von Maßnahmen für die funktionale Sicherheit sind klar: Die Betriebssicherheitsverordnung beispielsweise verpflichtet Betreiber von überwachungspflichtigen Anlagen, Sicherheit und Schutz der Gesundheit von Arbeitnehmern zu gewährleisten. Sie macht klare Vorgaben zur Gefährdungsbeurteilung sowie zu Schutzmaßnahmen und benennt explizit Tatbestände von Ordnungs-

widrigkeiten und Straftaten. Dennoch werden immer noch viele Sicherheitsmaßnahmen vor allem aus Kostengründen nicht oder nur halbherzig umgesetzt. Ein weiterer Hemmschuh sind fehlendes Wissen rund ums Thema funktionale Sicherheit oder die Unsicherheit, wie man sich im komplexen „Dschungel“ der Normen und Richtlinien zurechtfinden soll.

Aus rechtlicher Sicht ist klar: Der Einsatz eines Functional Safety Management Systems (FSM) ist ein Muss, wenn man Schutzeinrichtungen der Funktionalen Sicherheit betreibt. Ein FSM hilft aber nicht nur, große Sicherheitsrisiken zu vermeiden, sondern kann „im Kleinen“ auch Anlagenstillstände reduzieren. Somit rechnet es sich doppelt. Aber eins nach dem anderen.

Funktionale Sicherheit in der Praxis umsetzen

Was genau ist eigentlich ein FSM? Es ist ein systematisches Vorgehen, das bereits bei der Verfahrensentwicklung und in der Anlagenplanung dazu beitragen kann, Fehler zu vermeiden. Generell lassen sich die in einer Anlage auftretenden Fehler in zwei Gruppen aufteilen: stochastische und systematische Fehler. Stochastische Fehler treten zufällig auf und lassen sich vorab nicht vermeiden. Ein Beispiel ist der unvorhersehbare Ausfall einer Elektronikkomponente. Hier gilt es für den Fall der Fälle unter dem Stichwort Fehlerbeherrschung den Fehler mit Diagnosemechanismen zu erkennen und die Anlage in einen sicheren Zustand zu überführen. Mit Redundanzkonzepten lässt sich ein Abfahren und Stillstand der Anlage verhindern. Während stochastische Fehler zufällig auftreten und nicht präventiv vermeidbar sind, sind systematische Fehler vorher erkennbar und ihre Konsequenzen absehbar. Ein Fehler in der Prüfanweisung eines Schutzsystems beispielsweise zieht dann eine falsch ausgeführte Prüfung nach sich. Die bestimmungsgemäße Funktion des Schutzsystems ist somit nicht sichergestellt und kann zu einem Anlagenschaden, einem Umwelt-

Autoren:



Bernd Rastatter, Prokurist und Vertriebsleiter, Andre Günther Produktmanager Rösberg Engineering GmbH



Bild 1: Nur 15 Prozent aller Fehler haben eine stochastische Ursache. IBN= Inbetriebnahme (Bild: Rösberg)



Bild 2: Ein FSM orientiert sich am Sicherheitslebenszyklus, wie er in der DIN EN 61511 definiert ist. (Bild: Rösberg)

schaden und schlimmstenfalls zu einem Personenschaden führen.

Es gilt also, solche systematische Fehler im Vorfeld zu vermeiden. Dass sich das lohnt, zeigt eine Studie der Health and Safety Executive (HSE). Die HSE regelt in Großbritannien wesentliche Bereiche des Arbeitsschutzes. Die Studie untersuchte 34 Unfälle, die zu größeren Schäden führten und kam zu der Erkenntnis, dass über 60 Prozent dieser Fehler bereits vor der Inbetriebnahme in eine Anlage eingebaut waren (Bild 1). Circa 25 Prozent der Fehler entstehen bei der Installation bzw. durch Änderungen nach Inbetriebnahme. Nur 15 Prozent der auftretenden Fehler hatten eine stochastische Ursache.

Wie kann ein Functional Safety Management System helfen?

Hauptverursacher systematischer Fehler ist in der Regel der Mensch. Ihn gilt es also während der Planungs- und Implementierungsphase so zu unterstützen, dass diese meist vom Management verursachten Fehler bestmöglich vermieden werden. Dort setzen FSM-Systeme an. Sie beruhen auf rechtlichen Verordnungen, Vorgaben und Normen. Ein FSM orientiert sich am Sicherheitslebenszyklus, wie er in der DIN EN 61511 definiert ist. Bild 2 zeigt alle Phasen von der Gefährdungs- und Risikobeurteilung über die Planung bis hin zur Inbetriebnahme und letzten Endes der Außerbetriebsetzung. Die Änderung z.B. Migration

von Steuerungssystemen wird auch bedacht. Gleich zu Beginn werden in einem Sicherheitsplan Verantwortliche für jede dieser insgesamt acht Phasen definiert. In jeder dieser Phasen nutzt das FSM im Wesentlichen zwei Instrumente: Die Prozessdefinition (Balken links: Management und Beurteilung der Funktionalen Sicherheit) und die Kontrolle, ob diese Prozessdefinitionen auch eingehalten werden (Balken rechts: Verifikation).

Prozessdefinition und Kontrolle

Prozessdefinitionen werden für jede einzelne Phase des Sicherheitslebenszyklus vorgenommen. In der Phase der Gefährdungs- und Risikobeurteilung werden Safety Integrity Level (SIL) festgelegt. Das wiederum hat Einfluss darauf, wer die Verifikation im Vier-Augen-Prinzip vornehmen darf. Bei geringem SIL können dies interne Mitarbeiter sein, je höher der SIL, desto unabhängiger muss die Verifikation stattfinden bis hin zur Verifizierung durch unabhängige Organisationen bei sehr gefährlichen Prozessen. Wer welche Prozesse verifizieren darf, hängt nicht nur von seiner Unabhängigkeit, sondern auch von seiner Kompetenz ab. Dabei spielt sowohl die fachliche Qualifikation als auch die berufliche Erfahrung im speziellen Bereich eine wesentliche Rolle. Formatvorlagen, wie man sie aus dem Qualitätsmanagement kennt, werden für die Kontrolle eingesetzt. Mit diesen

speziell vorgefertigten Checklisten, lassen sich potentielle Fehlerursachen systematisch abfragen. Zum Aufbau dieser Checklisten für eine bestimmte Anlage kann man zum Großteil die standardisierten Vorgaben aus verschiedenen Normen übernehmen. Nur in wenigen Fällen sind individuelle Anpassungen nötig. Ziel des Fragenkatalogs dieser Formatvorlagen ist es, keinen Interpretationsspielraum dabei zu lassen, ob und wie Aufgaben erledigt wurden. Bild 3 zeigt beispielhaft einen Ausschnitt einer Formatvorlage für die Phase 1 des Sicherheitslebenszyklus zur Verifizierung der jeweiligen Tätigkeit. Nach jeder Phase wird geprüft, ob alle Aufgaben regelkonform erledigt wurden. Erst dann gibt der Safety-Manager sein „Okay“ für den Start des nächsten Schrittes.

Arbeit erleichtern, Sicherheit erhöhen

Dipl.-Ing. (FH) Andre Günther arbeitet als Produktmanager für funktionale Sicherheit bei der Rösberg Engineering GmbH. Er ergänzt: „Oft bedeutet erhöhte Sicherheit ja Verzicht auf Freiheit und Flexibilität. So soll es bei einem FSM aber gerade nicht sein. Ein gut aufgesetztes FSM-System hilft den Anwendern dabei, die beste und sicherste Lösung möglichst einfach zu entwickeln.“ Er und seine Kollegen unterstützen Anlagenbauer und -betreiber bei allen Aufgaben rund um das Thema funktionale Sicherheit und helfen auch bei der Integration eines FSM-Systems. Anlagenbetreiber, die bereits ein Quali-

tätsmanagementsystem nach DIN EN ISO 9001 aufgesetzt haben, sind hier schon auf einem guten Weg. Günther erläutert: „Die Abteilungen mit ihren Mitarbeitern sind dann bereits an definierte Prozesse und die Anwendung von Formatvorlagen gewöhnt. Gleichzeitig bestehen schon einzelne Prozesse wie z.B. Lenkung und Revision von Dokumenten.“ Die Rösberg-Mitarbeiter helfen dann bei der Verzahnung von QM- und FSM-Systemen durch die Definition entsprechender Schnittstellen. Aber auch in anderen Fällen unterstützen sie natürlich beim Aufsetzen eines FSM: Von der umfangreichen Beratung über das Bereitstellen einer Dokumentation bis hin zum abschließenden Rollout. Die Mitarbeiter verfügen dazu über die notwendigen Qualifikationen und die von den einschlägigen Normen ebenfalls geforderte Berufserfahrung. Das Unternehmen hat unter anderem eigene vom TÜV verifizierte Formatvorlagen entwickelt. Diese können dem Kunden nach Beratung zur Verfügung gestellt werden. Günther resümiert: „Obwohl die rechtlichen Forderungen für funktionale Sicherheiten klar sind, schrecken immer noch viele vor dem Einsatz eines FSM-Systems zurück. Wir wollen durch unsere Dienstleistungen in diesem Bereich helfen, die Hemmschwelle so weit herabzusetzen, dass der Einsatz einfach möglich und präventiv durchgeführt wird und man nicht erst aus Schaden klug wird.“

■ Rösberg Engineering GmbH
www.roesberg.com
www.livedok.com

#	Prüfungskriterium	Kriterium	Ergebnis	Bemerkung
1	Überwachung Phasen Sicherheitslebenszyklus	Personen wurden im Sicherheitsplan benannt und wurden über die ihnen übertragene Verantwortung informiert.	☑ ☒ ☐	
2	Kompetenz / prozessrechtliche Anforderungen	Technisches Wissen, Ausbildung und Erfahrung bezogen auf die prozessrechtliche Anwendung ist vorhanden?	☑ ☒ ☐	
3	Kompetenz zur gewählten Technologie	Technisches Wissen, Ausbildung und Erfahrung bezogen auf die eingesetzte Technologie ist vorhanden?	☑ ☒ ☐	
4	Kompetenz bezogen auf Sensoren / Aktoren	Technisches Wissen, Ausbildung und Erfahrung bezogen auf die Sensoren und Aktoren ist vorhanden?	☑ ☒ ☐	
5	Sicherheitsrechtliche Kompetenz	Sicherheitsrechtliches Wissen ist vorhanden (z.B. IEC 61508)?	☑ ☒ ☐	
6	Kompetenz gewerbliche Anforderungen	Kenntnis der gewerblichen und betrieblichen Anforderungen hinsichtlich des funktionalen Sicherheits ist vorhanden?	☑ ☒ ☐	
7	Management- und Führungswilligkeit	Ausreichende Management- und Führungswilligkeit für die jeweilige Aufgabe im Sicherheitslebenszyklus ist vorhanden?	☑ ☒ ☐	

Bild 3: Ausschnitt einer Formatvorlage für die Phase 1 des Sicherheitslebenszyklus zur Verifizierung der jeweiligen Tätigkeit. (Bild: Rösberg)