Sicherheit für Mensch, Maschine und Umwelt

Betriebliches Risikomanagement und seine Auswirkungen auf die funktionale Sicherheit

Eine unzureichende Kontrolle der Prozessbedingungen ist die Ursache für viele schwere Unfälle in Anlagen auf der ganzen Welt und kann zu Leckagen, zu Schadstoffemissionen und sogar zu Explosionen führen. Die Anlagenausrüstung wird beschädigt und ernsthafte gesundheitliche Schäden bis hin zu Todesfällen bei Mitarbeitern und Anwohnern sowie gravierende Umweltschäden über etliche Jahre hinweg können die Folge sein.

Einige der größten Industriekatastrophen sind auf eine nachlässige Wartung zurückzuführen. Häufig wurden die Sicherheitssysteme abgeschaltet oder nicht ordnungsgemäß wieder in Betrieb genommen.


© Yokogawa

Änderungen am Sicherheitssystem müssen grundsätzlich unter Risikoaspekten evaluiert werden.

Mark Breese, Yokogawa RAP

Beispiele hierfür sind Bhopal in Indien und Buncefield in Großbritannien, um nur zwei zu nennen.

Die Control of Work (COW) Software von Yokogawa RAP sorgt seit über 25 Jahren für die Sicherheit von Mitarbeitern in hochgefährdeten Branchen. In modernen Anlagen spielt sicheres Arbeiten eine immer wichtigere Rolle. Die Vorteile sind nicht nur mehr Sicherheit, sondern auch eine höhere Zuverlässigkeit, eine größere Effizienz, weniger Ausfallzeiten und eine bessere Sichtbarkeit der Anlagenaktivitäten. Entscheidend hierbei ist die Frage, wie funktionale Sicherheitssysteme bewertet, verwaltet und überwacht werden können.

Was ist funktionale Sicherheit?

Funktionale Sicherheit sorgt dafür, dass Prozesssicherheitssysteme so konzipiert, installiert, betrieben, gewartet und verwaltet werden, dass die Anlagensicherheit im Falle einer Störung gewährleistet ist. Dies beinhaltet Alarmmanagement, Prozesssteuerung und sicherheitsgerichtete Systeme.

Prozessanlagen bergen per se potenzielle Gefährdungen für Menschen, Umwelt und den Betrieb selbst. Die Anlagensicherheit muss bewertet und die einzelnen Gefahrenquellen müssen identifiziert werden. Natürlich lassen sich nicht alle Gefährdungen beseitigen, aber sie müssen gemäß der Wahrscheinlichkeit ihres Auftretens und der Schwere der Folgen eines Zwischenfalls betrachtet werden. Dazu sind die auslösenden Ursachen und alle bestehenden Maßnahmen zur Verhinderung von Gefahrensituationen zu berücksichtigen.

In vielen verfahrenstechnischen Anlagen werden Sicherheitsfunktionen eingesetzt, um das Risiko potenzieller Gefährdungen zu mindern. Diese Systeme reagieren aber nur im Falle eines tatsächlichen Zwischenfalls, also sehr selten. Darum müssen diese Systeme über eine geringe Ausfallwahrscheinlichkeit im Anforderungsfall (PFD) verfügen.

Beispiele für Sicherheitssysteme sind Branderkennungs- und -bekämpfungssysteme, Hochintegritätsdruckschutzsysteme (HIPPS) und Notabschaltsysteme (ESD).

SIS, SIF und SIL

Die zwei meistzitierten Normen für sicherheitsgerichtete Systeme (SIS) sind die IEC 61508 (Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheitsbezogener Systeme) und die IEC 61511 (Funktionale Sicherheit – Sicherheitstechnische Systeme für den Bereich der Prozessindustrie).

Die meisten Prozessanlagen verfügen über Systeme mit geringen Anforderungsraten, einschließlich mechanischer Aktoren, die regelmäßige Kontrollen und Wartungsarbeiten erfordern, um einen sicheren Betrieb im Notfall zu gewährleisten.

Die Anlagensicherheit muss bewertet und die einzelnen Gefahrenquellen müssen identifiziert werden.

Sicherheitsfunktionen (SIF) dienen dazu, einen sicheren Zustand der Anlage zu erhalten bzw. wieder herzustellen. Dies sind überwiegend Schutzfunktionen, aber auch Schadensbegrenzungsmaßnahmen. SIF haben ein Sicherheitsintegritätslevel (SIL), der die spezifischen betrieblichen und anwendungsbezogenen Aspekte berücksichtigt, die für die erforderliche Funktion relevant sind. SIL ist definiert als relativer Grad der Risikominderung, der von einer Sicherheitsfunktion bereitgestellt wird.

SIL werden durch mathematische Analysemethoden berechnet, die auf der Ausfallwahrscheinlichkeit der einzelnen Bauteile eines Systems basieren. Die IEC 61508 fordert als wichtigen Aspekt eine bestimmte Hardware-Fehlertoleranz (HFT). Die HFT gibt an, wie viele Fehler bis zum Verlust der Sicherheitsfunktion auftreten können.

Gängige Architekturen verbessern die HFT, indem das System über ein Ergebnis „votieren" kann. Das Sicherheitssystem entscheidet aufgrund der Redundanzauswertung, wann eine Anforderung erfolgt, z.B. wenn ein Druckwert die zulässigen Werte überschreitet. Parallelsysteme und andere komplexere Architekturen können je nach erforderlicher Reaktion der Bauteile im Gesamtsystem die HFT weiter optimieren.

Eine wichtige Rolle spielt auch die Ausfallrate, die sog. „Safe Failure Fraction" (SFF) der Bauteile. Der SFF-Faktor repräsentiert den Anteil der sicheren und erkannten Ausfälle zu den gesamten Ausfällen. Sobald der Anwender den HFT und die SFF kennt, kann er den anwendbaren SIL-Level anhand einer Tabelle ermitteln. Die Tabelle für Bauteile des Typs A umfasst Bauteile, deren Ausfallarten und Verhalten hinlänglich bekannt und definiert sind und für die genügend Daten vorliegen, um die Ausfallraten nachzuweisen.

Je nach Anwendung wird für Prozessanlagen maximal SIL 2 oder SIL 3 angestrebt, in Branchen mit höherem Risikopotenzial wie z.B. in der Nuklearindustrie auch SIL 4.

Bestimmung des maximal zulässigen SIL eines Elements

Ausfallrate (SFF)	Bauteile Typ A		
	Hardware-Fehlertoleranz (HFT)		
	0	1	2
<60 %	SIL 1	SIL 2	SIL 3
60 % – <90 %	SIL 2	SIL 3	SIL 4
90 % – <99 %	SIL 3	SIL 4	SIL 4
>=99 %	SIL 3	SIL 4	SIL 4

(Quelle: IEC 61508-2, Tabelle 2)

Wie wirkt sich Wartung auf die funktionale Sicherheit aus?

Sicherheitssysteme müssen regelmäßig gewartet werden, um ihre Sicherheitsintegritätslevel zu gewährleisten. Anhand von Proof-Test-Intervallen wird die zulässige Dauer bis zur Überprüfung des Systems festgelegt. Sicherheitssysteme können entweder durch eine Vollprüfung des Systems oder eine Diagnoseprüfung, z.B. eine Teilhubprüfung (PST), getestet werden. In jedem Fall sind Wartungs- bzw. Offline-Arbeiten erforderlich, deren Durchführung die Wirksamkeit des Sicherheitssystems beeinträchtigen kann.

Änderungen am Sicherheitssystem müssen grundsätzlich unter Risikoaspekten evaluiert werden, da sich das Gesamtrisiko für den Prozess erhöht. Bei der Außerbetriebnahme eines Bauteils z.B. muss das System während dieser Zeit überwacht werden. Alarme sorgen dafür, dass das System nach Abschluss der Arbeiten wieder ordnungsgemäß in Betrieb genommen wird. Das SORM-Modul für Safety Override Risk Management der Control of Work (COW) Software RAP stellt sicher, dass alle Aktivitäten und damit verbundenen Risiken aufgezeichnet, den zuständigen Verantwortlichen übermittelt und angemessen überwacht werden.

Redundanz-Architekturen und Hardware-Fehlertoleranz (HFT)

Architektur	Bedeutung
1oo1	1 out of 1 – 1 von 1 Bauteil löst aus. Die HFT beträgt 0, da es bei einem Ausfall keine Redundanz gibt.
1oo2	1 out of 2 – 1 von 2 Bauteilen im System löst aus. Die HFT beträgt 1, da das System bei Ausfall eines Bauteils trotzdem funktionsfähig bleibt.
2oo2	2 out of 2 – Beide Bauteile lösen aus. Dies reduziert das Risiko einer Fehlauslösung, aber da beide Bauteile für Auslösung votieren müssen, fällt die HFT auf 0 zurück.
2oo3	2 out of 3 – Vermeidet das Risiko einer Fehlauslösung, da 2 von 3 Bauteilen für die Auslösung votieren. Die HFT beträgt weiterhin 1, da ein Bauteil ausfallen kann und die beiden anderen immer noch auf den Ausfall reagieren können.

Kalibrierung des Drucksensors eines ESD-Systems

Bei diesem System sind die Ventilaktoren sowie die Drucksensoren redundant ausgelegt. Bei der Kalibrierung eines Drucksensors wird das System je nach Risikoeinschätzung vom normalen 2oo3-System entweder auf ein 2oo2-System oder ein 1oo2-System umgeschaltet. Dadurch kann der SIL des Systems während der Durchführung der Arbeiten sinken.

In der Regel werden solche Arbeiten im Rahmen einer freigegebenen Tätigkeit durchgeführt. Während des Wartungszeitraums können weitere, z.B. zusätzliche manuelle Kontrollen erforderlich sein, um die Anlagensicherheit zu gewährleisten. Nach der Kalibrierung muss durch erneute Überprüfung sichergestellt werden, dass sich das System wieder im Normalbetrieb befindet.

Ein effizientes Sicherheitssystem zur Überwachung von Änderungen an kritischen Bauteilen unterbindet nicht nur die Genehmigung, bis alle erforderlichen Isolierungen vorhanden sind, sondern überwacht auch das Überbrücken von Sicherheitsfunktionen. Es verhindert zudem, dass die Isolierungen nach Abschluss der Arbeiten entsperrt werden, bevor nicht alle betreffenden Genehmigungen zurückgegeben wurden, und überwacht die Wiederherstellung von Überbrückungen, bevor der Genehmigungsprozess abgeschlossen werden kann.

Das System RAP von Yokogawa ermöglicht die Rücksendung einer Genehmigung nach Abschluss der Arbeiten, lässt aber die endgültige Genehmigung erst nach Erhalt einer weiteren Bestätigung zu. So wird gewährleistet, dass Überbrückungen wiederhergestellt wurden, wobei das System einen Alarm ausgibt, wenn sie nicht gemäß den vorgegebenen Zeitplänen überwacht werden. Gilt eine zurückgesendete Genehmigung zu lange als unvollständig, kann dies bedeuten, dass entweder eine Überbrückung nicht aufgehoben wurde oder dass sie zwar aufgehoben wurde, aber möglicherweise nicht alle Verantwortlichen informiert wurden.

Die Überwachung sicherheitskritischer Komponenten mit RAP bietet enorme Vorteile für Prozessanlagen, da der Anwender die Wechselwirkungen zwischen kritischen Bauteilen, zulässigen Tätigkeiten und der Isolierung aller Formen von Energie-, Flüssigkeits- oder Antriebsquellen zentral verwalten kann und so ein Höchstmaß an Sichtbarkeit über alle Aspekte erzielt.

Mark Breese,
Principal Consultant,
Yokogawa RAP
■ www.yokogawa.de