

PLT-Schutzeinrichtungen

Fehlerquellen durch menschliches Handeln

Seit Inkrafttreten der IEC 61511 und der nationalen Umsetzung in die VDI/VDE 2180 verstärken sich Forderungen, die Ausfallwahrscheinlichkeiten von PLT-Schutzeinrichtungen zu berechnen. Es lässt sich feststellen, dass der Einfluss menschlichen Verhaltens auf die sicherheitstechnische Verfügbarkeit der Einrichtungen im Vergleich zur gerätetechnischen Zuverlässigkeit nicht unterschätzt werden darf. Für die Gewährleistung der PLT-Anlagensicherheit sollte daher der Fokus neben der SIL-Berechnung auf die Verbesserung organisatorischer Abläufe mit Hilfe von Managementsystemen der funktionalen Sicherheit ausgeweitet werden.

SCHLAGWÖRTER PLT-Schutzeinrichtung / Menschlicher Faktor / Managementsystem

Safety Instrumented Systems – Sources Due to Human Error

Since the entry into force of the IEC 61511 and the national implementation in the VDI/VDE 2180, requirements are strengthened to calculate the probability of failure on demand of safety instrumented systems (SIS). It is shown that compared to technical reliability of apparatuses the influence of human behavior on the safety-related reliability of SIS should not be underestimated. To ensure plant safety by means of process control systems SIL-calculations as well as the improvement of organizational processes by means of functional safety management systems should be addressed.

KEYWORDS Safety instrumented system / Human factor / Management system

An die sicherheitstechnische Verfügbarkeit von PLT-Schutzeinrichtungen werden hohe Anforderungen gestellt. Der Safety Integrity Level (SIL) beschreibt dabei die Wahrscheinlichkeit eines Versagens der Sicherheitsfunktion im Anforderungsfall hervorgerufen durch passive Fehler. Die Ermittlung des entsprechenden Zahlenwertes scheint dabei bisweilen die Diskussionen um den Nachweis ausreichender Sicherheit prozessleittechnischer Schutzsysteme zu beherrschen. Die NAMUR hat mit der Empfehlung Nr. 93 „Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen“ [3] bereits 2001 einen Weg aufgezeigt, mit Hilfe der Auswertung bundesweiter Stördatenerfassungen die Gleichwertigkeit der bisher üblichen qualitativen Bewertungsverfahren mit den gerätebezogenen rechnerischen Verfahren nachzuweisen. Mit der NAMUR-Empfehlung NE 130 „Betriebsbewährte Geräte für PLT-Schutzeinrichtungen und vereinfachte SIL-Berechnung“ [4] werden weitere Hinweise gegeben, den SIL von Geräten auf Basis der Betriebsbewährtheit zu ermitteln. Auch die VDI/VDE 2180 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)“ [2] unterstützt als nationale Umsetzung der internationalen IEC 61511 „Functional safety - Safety instrumented systems for the process industry sector“ [1] die Beschreibung der Gerätesicherheit auf Basis der Betriebsbewährtheit.

Insbesondere Betreiber von Anlagen, die der Störfallverordnung unterliegen, müssen beachten, dass die VDI/VDE 2180 der Konkretisierung der Störfallverordnung in Bezug auf prozessleittechnische Einrichtungen zur Anlagensicherung dient. Neben den Anforderungen an die Zuverlässigkeit der Gerätetechnik sind hier insbesondere auch die Maßnahmen beschrieben, mit denen Betreiber die Zuverlässigkeit der gesamten PLT-Schutzeinrichtungen auf Dauer gewährleisten können. Ein Management der funktionalen Sicherheit (Functional Safety Management FSM) (Bild 1) soll die Umsetzung dieser Maßnahmen über den gesamten Lebenszyklus einer PLT-Schutzeinrichtung beschreiben.

Der sachgerechten Planung von PLT-Schutzeinrichtungen folgt dabei der Betrieb dieser Einrichtungen. Dazu zählen z. B. Festlegungen, die nach einem Gerätetausch den sicheren Weiterbetrieb gewährleisten, oder solche, die eine Aufdeckung passiver Fehler durch geeignete Prüfungen ermöglichen.

1. ERFAHRUNGEN BEI WIEDERKEHRENDEN PRÜFUNGEN

Seit vielen Jahren prüft die Infracor GmbH als akkreditierter sicherheitstechnischer Dienstleister PLT-Schutzeinrichtungen vor ihrer Inbetriebnahme, seit ca. 4 Jahren darüberhinaus auch wiederkehrend. Die folgenden Erfahrungen beruhen auf der Prüfung von etwa 10.000 Einrichtungen, die Bestandteil von PLT-Schutzeinrichtungen sind.

Bei den Beobachtungen handelt es sich dabei um Einzelfälle, die derzeit zwar keine statistische Auswertung zulassen, die aufgrund ihrer Nähe zu menschlichem Handeln aber geeignet sind, um auf den Einfluss des menschlichen Faktors bei der Bewertung der Sicherheit von PLT-Schutzeinrichtungen hinzuweisen.

1.1 Gerätedefekte

Herstellerangaben zu Ausfallwahrscheinlichkeiten beziehen sich stets ausschließlich auf die spezifikationsgerechte Auslegung/Installation und den ordnungsgemäßen Betrieb der Geräte ohne Feld-/Produktinfluss. Die Wahrscheinlichkeit, durch menschliches Handeln letztlich die Ausfallwahrscheinlichkeit der Geräte zu erhöhen, wird dabei nicht berücksichtigt.

Insgesamt lässt sich feststellen, dass typische Gerätefehler früherer analoger Geräte bei modernen mikroprozessorgesteuerten Geräten deutlich seltener auftreten. Zu diesen Fehlern zählte z.B. das Driften des Nullpunktes um einen Betrag, der die Auslösung von Schaltfunktionen beim Erreichen des sicherheitstechnischen Grenzwertes verhinderte.

Verbleibende Fehlerquellen, die häufig dem Gerät angelastet werden, sind:

- Prozessanschluss, z.B. zu kurze Temperaturfühler oder veränderte Messdynamik aufgrund veränderter Produkteigenschaften
- Installation, z.B. defekte Beheizung von Produktleitungen zum Messgerät oder elektromagnetische Einkoppelungen
- Umgebungsbedingungen, z.B. Vibrationen in der Nähe großer Maschinen oder Vereisungen von Entlastungsöffnungen

1.2 Gerätetausch

Beim Austausch von Geräten ist eine sorgfältige Prüfung der Übereinstimmung aller Geräteeigenschaften erforderlich. Änderungen in der Pin-Belegung von einem Gerät zum vermeintlich gleichen Nachfolgerät können beispielsweise dazu führen, dass nach dem Gerätetausch zwar eine ordnungsgemäße Anzeige des Messwertes im Prozessleitsystem vorliegt, die sicherheitsgerichtete (Schalt-) Funktion bei Erreichen des Grenzwertes aber nicht gegeben ist. Wenn der Austausch eines Gerätes gegen ein identisches und funktionstüchtiges Gerät nicht zweifelsfrei gewährleistet werden kann, muss vor der Wiederinbetriebnahme der PLT-Schutzeinrichtung stets eine Funktionsprüfung mit Simulation des sicherheitstechnischen Grenzwertes erfolgen.

Beim Austausch von Antrieben auf Stellgeräten ist auf die richtige mechanische Positionierung des Antriebes auf der Welle zu achten. Wenn beide Stellungen des Stellgerätes verfahrenstechnisch benötigt werden, kann eine falsche Positionierung des Antriebes dazu führen, dass sich das Stellgerät bei einer sicherheitsrelevanten Anforderung in die falsche Position bewegt.

Besondere Sorgfalt ist bei der Parametrierung moderner Feldgeräte erforderlich. So bieten z.B. Massedurchflussmesser in zahlreichen Menüs Parametrierungsmöglichkeiten für die Messgröße, die Anzeigeeinheit, Ein-, Ausgänge, Grund- und Spezialfunktionen, Überwachungsfunktionen usw. Werksseitig eingestellte Funktionen sind dabei häufig individuell an die jeweilige Aufgabenstellung anzupassen. Bei einem Gerätetausch ist hier ausreichend qualifiziertes und zuverlässiges Personal erforderlich, um nach einem Gerätetausch die ordnungsgemäße Parametrierung zu gewährleisten.

1.3 Prüfungsdurchführung

Abhängig von der Art der Prüfung ergeben sich unterschiedliche Anforderungen.

Erstprüfung/Prüfung nach Modifikation

Erstprüfungen und Prüfungen nach Modifikationen unterscheiden sich im Umfang der Prüfung. Während bei Erstprüfungen stets die gesamte PLT-Schutzeinrichtung im Detail zu prüfen ist, kann sich der Prüfumfang bei einer Prüfung nach Modifikation auf den geänderten Teil der PLT-Schutzeinrichtung beschränken.

Die Erstprüfung/Prüfung nach Modifikation an PLT-Schutzeinrichtungen gliedert sich in Dokumentationsprüfung, Installationsprüfung und Funktionsprüfung.

Die Dokumentationsprüfung dient dem Nachweis, dass die geplante PLT-Einrichtung geeignet ist, auf Grund der vorgesehenen Gerätetechnik und ihrer vorgesehenen Installation die Anforderungen des Schutzzieles zu erfüllen.

Die Installationsprüfung dient der Überprüfung, ob die tatsächlich installierten Geräte mit ihren Spezifikationen und ihren Installationsausführungen dem geplanten Aufbau entsprechen und damit geeignet sind, die Schutzfunktion wahrzunehmen.

Im Rahmen der Funktionsprüfung wird kontrolliert, ob die gemäß der Planung ordnungsgemäß installierten Geräte die vorgesehene Schutzfunktion bei dem festgelegten Grenzwert in einer sicherheitstechnisch akzeptablen Zeit auch tatsächlich herbeiführen.

Wiederholungsprüfung

Die Wiederholungsprüfung dient der Aufdeckung passiver Fehler in der jeweiligen PLT-Schutzeinrichtung. Diese können z.B. auftreten durch Alterungsprozesse der Geräte oder der Installation, Umwelteinflüsse oder ein verändertes Geräteverhalten nach der Änderung von Prozessbedingungen.

Die Prüfung der Dokumentation kann sich auf die Plausibilität zu vorangegangenen Prüfungen beschränken, z.B. ob noch das gleiche Gerät installiert ist und weder der Grenzwert noch die Schaltungsunterlagen geändert wurden.

Die Installationsprüfung erfolgt im Wesentlichen in Form einer Sichtprüfung, durch die auf eine nach wie vor ordnungsgemäße Installation kontrolliert wird.

Kern der Wiederholungsprüfung ist die Funktionsprüfung, deren Umfang in der Regel dem der Erstprüfung/Prüfung nach Modifikation entspricht.

Fehlerquellen bei der Funktionsprüfung

Wegen der ohnehin geringen Wahrscheinlichkeit passiver Fehler an PLT-Schutzeinrichtungen ist es wichtig, durch menschliche Handlungen im Rahmen der Prüfung keine zusätzlichen passiven Fehler zu erzeugen. Üblich ist es, die Prozessankopplung einer Messung zu unterbrechen, z.B. durch Schließen eines Kugelhahns bei der Prüfung einer Verdrängermessung. Wird der Kugelhahn nach der Prüfung nicht wieder geöffnet, kann das im Verdrängergefäß eingeschlossene Medium sehr wohl zu



BILD 1: Sichere Geräte und sicheres Handeln

einer plausiblen Messwertanzeige führen, ohne dass die Prozessankopplung wieder hergestellt ist.

Zusätzlich zum Einfluss durch menschliches Handeln müssen technische Fehlerquellen der Prüfungsabwicklung ausgeschlossen werden. Neben der Verwendung ausreichend genauer und kalibrierter Prüfhilfsmittel ist eine geeignete Prüfmethode zu wählen. So ist z.B. zu beachten, dass die Simulation eines Messumformer-Ausgangssignales keine Aussage über die ordnungsgemäße Umsetzung der physikalischen Messgröße im Umformer selbst zulässt. Auch ist zu berücksichtigen, dass die verfahrenstechnischen Einflüsse auf eine Messung im normalen Anlagenbetrieb anders sein können, als die Bedingungen, die im Rahmen der Prüfung vorherrschen. Dies ist z. B. der Fall, wenn die Prüfung mit Wasser anstatt mit dem Betriebsmedium durchgeführt werden muss und die gegenüber dem Betriebsmedium andere Dichte oder Dielektrizität von Wasser das Messverfahren beeinflusst.

1.4 Dokumentation

Eine aktuelle und vollständige Dokumentation ist zwingende Grundlage für eine ordnungsgemäße Prüfung. Auch wenn diese Anforderung selbstverständlich erscheint, ist zu beachten, dass der Betrieb von verfahrenstechnischen Anlagen in der Regel begleitet wird von Modifikationen mit dem Ziel der Anlagenoptimierung oder Produktänderung. So kann es beispielsweise erforderlich sein, sicherheitstechnische Grenzwerte an die betrieblichen Gegebenheiten anzupassen, wenn diese im ursprünglichen Sicherheitskonzept der Anlage näher an den geplanten Betriebszustand statt an die sicherheitstechnischen Auslegungsgrenzen der Anlage gelegt wurden. Die entsprechende Modifikation muss dabei in allen betroffenen Unterlagen dokumentiert werden, um die Konsistenz der Unterlagen, z.B. Sicherheitskonzept, Funktionsplan, Grenzwertliste, zu gewährleisten.

Wichtig ist es, bei verfahrenstechnischen Modifikationen die Auswirkungen auf die Funktionstüchtigkeit der prozessleittechnischen Einrichtungen zu berücksichtigen. So kann z.B. der nachträgliche Verzicht auf Inhibitoren bei der Handhabung von Medien mit Polymerisationsneigung für den Produktionsgang mit strömendem Medium unkritisch sein, während stehendes Produkt Armaturen durch Polymerisation festsetzt, so dass sich die Armatur nicht mehr in die sichere Stellung bewegen lässt.

Auch wenn kurze Innovationszyklen und eine rasche Anpassung der Prozessanlagen an die Anforderungen des Marktes überlebenswichtig für ein Unternehmen sein können, muss vor der (Wieder-) Inbetriebnahme nach Modifikation eine Prüfung der PLT-Schutzeinrichtung erfolgen.

3. EINFLUSS ORGANISATORISCHER VERÄNDERUNGEN

Wenn ausscheidendes Fachpersonal nicht in vollem Umfang ersetzt wird, kann das auf der operativen Ebene zu höherem Zeitdruck für das verbleibende Personal führen, auf der Führungsebene darüberhinaus zu einem Abbau fachlicher Detailkenntnisse. Wichtig ist, dass Führungskräfte mit technischer Verantwortung trotz vielfältiger betriebswirtschaftlicher Aufgaben ausreichend Zeit und Know-how für die Lösung technischer Probleme behalten.

Fachpersonal, das durch sein operatives Handeln die Zuverlässigkeit von PLT-Schutzeinrichtungen gewähr-

leisten soll, braucht ausreichend Zeit für eine qualifizierte Aus- und Fortbildung. Dabei ist zu berücksichtigen, dass die alleinige Teilnahme an Schulungsmaßnahmen nicht die intensive Betreuung und Einarbeitung durch einen Fachvorgesetzten ersetzen kann.

Die Zusammenlegung von Instandhaltungs- und Betriebspersonal darf nicht zu Zielkonflikten führen, wenn z.B. einerseits Prüftätigkeiten die operative Anlagenverfügbarkeit stören, andererseits das für die Prüfung verantwortliche Personal gleichzeitig auch für die Aufrechterhaltung der Anlagenverfügbarkeit verantwortlich ist.

FAZIT

Für eine Verbesserung der Anlagensicherheit mit Mitteln der Prozessleittechnik muss der Fokus neben der SIL-Bestimmung der verwendeten Geräte auch die Sicherstellung und ggf. Verbesserung organisatorischer Abläufe auf Basis von Managementsystemen der funktionalen Sicherheit beinhalten.

MANUSKRIPTEINGANG
01.12.2009

AUTOR



Dipl.-Ing. **CHRISTOPH THUST** (geb. 1959) ist Leiter der Abteilung Technische Überwachung der Infracor GmbH. Seit seinem Studium der Elektrotechnik an der Universität Bochum ist er als Sachverständiger im Bereich des Explosionsschutzes und der prozessleittechnischen Anlagensicherheit tätig.

Infracor GmbH,
Paul-Baumann-Straße 1, D-45772 Marl,
Tel. +49 2365 495837,
E-Mail: christoph.thust@infracor.de

REFERENZEN

- [1] IEC 61511: Functional safety - Safety instrumented systems for the process industry sector, entspricht DIN EN 61511: Funktionale Sicherheit - sicherheitstechnische Systeme für die Prozessindustrie, Mai 2005
- [2] VDI/VDE 2180: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT), April 2007
- [3] NAMUR-Empfehlung NE 93: Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen, Februar 2003
- [4] NAMUR-Empfehlung NE 130: Betriebsbewährte Geräte für PLT-Schutzeinrichtungen und vereinfachte SIL-Berechnung, Mai 2009