Verifizierung der SIL-Eignung

Seit vier Jahren gilt die DIN EN 61511 als „best practice“ für die Auslegung von PLT-Schutzeinrichtungen in der Prozessindustrie. Der Betreiber garantiert während des Lebenszyklus jeder sicherheitsrelevanten Komponente, dass die definierte Sicherheitsstufe gewährleistet ist.

TEXT: Dirk Lippert, Thomas Gabriel, Udo Hug **BILDER:** Lippert Fuhrmann, Universität Kaiserslautern

Die Beurteilung des abzusichernden Risikos und die Beschaffung SIL-(Safety Integrity Level)-bescheinigter Komponenten ist heute bereits gängige Praxis. Defizite bestehen nach wie vor bei der Betriebsdatenerfassung zur nachhaltigen Validierung des Schutzkonzepts. Insbesondere für bereits seit Jahren betriebene Komponenten ohne SIL-Bescheinigung kann mit einer gezielten Stördatenerfassung die SIL-Eignung durch Betriebsbewährung nachgewiesen werden.

Die Festlegung der Sicherheitsstufe, des Safety Integrity Level, sowie der qualitative Eignungsnachweis der eingesetzten Komponenten, als auch der quantitative Nachweis der sicherheitstechnisch notwendigen Verfügbarkeit einer PLT-Schutzeinrichtung sind nach der DIN EN 61511 die grundlegenden Voraussetzungen für ein funktionierendes Sicherheitsmanagement. Dabei muss der Anlagenbetreiber sicherstellen, dass die geforderte Risikoreduzierung aller sicherheitstechnischen Funktionen (Safety Instrumentet Function (SIF)) während des Betriebes und der Instandhaltung permanent aufrecht erhalten wird. Dazu gehören neben der regelmäßigen Durchführung und Dokumentation von Funktionsprüfungen auch die Erfassung, Analyse und Korrektur von Systemausfällen.

Sicherheitsmanagement und Risikoanalyse

Der erste und wichtigste Schritt für eine sichere und kostenoptimale Auslegung von PLT-Schutzeinrichtungen ist die Analyse der möglichen Gefährdung durch den Prozess, das sogenannte Prozessrisiko. Hierzu wird nach VDI/VDE 2180 im Blatt 1 durch Anwendung eines Risikografen ein systematisches Vorgehen unterstützt. Der sich aus dem möglichen Schadensmaß ergebende SIL stellt eine Anforderung an die obere Grenze der sicherheitstechnischen Verfügbarkeit der zu installierenden PLT-Schutzeinrichtung dar. Die korrespondierende Kenngröße ist die mittlere Ausfallwahrscheinlichkeit im Anforderungsfall (Probability of Failure on Demand (PFD)). Die Risikoanalyse ist Voraussetzung zur Planung von PLT-Schutzeinrichtungen. Die Firma ABB unterstützt zum Beispiel mit dem Werkzeug TRAC bei dieser Risikoanalyse.

Durch die risikoreduzierende Maßnahme über eine PLT-Schutzeinrichtung wird mit der SIL-Einstufung die Ausfallsicherheit festgelegt. Bei der Auslegung der PLT-Schutzeinrichtung müssen demnach Maßnahmen für eine zuverlässige Instrumentierung berücksichtigt werden (siehe VDI/VDE 2180, Blatt 5). Im einzelnen sind dies Maßnahmen gegen systematische Fehler, gegen zufällige Fehler und zur Fehlertoleranz.

Bei systematischen Fehlern einer PLT-Schutzeinrichtung muss zwischen Fehlern des Gerätes selbst und Fehlern, die sich durch den Einbau des Gerätes in den Prozess ergeben, unterschieden werden. Bei Geräten mit einer Herstellererklärung für SIL 2 können systematische Fehler des Gerätes selbst ausgeschlossen werden. Jedoch wird die Herstellererklärung keine Aussage zu den Eigenschaften der Gesamtfunktion der Schutzeinrichtung treffen können, sodass die SIL-Eignung der sicherheitstechnischen Funktion zusätzlich durch den Anlagenbetreiber nachgewiesen werden muss. Bei Geräten ohne Herstellererklärung für SIL 2 muss grundsätzlich von systematischen und zufälligen Fehlern ausgegangen werden, die erst im Rahmen eines Betriebsbewährungsprozesses durch den Anlagenbetreiber aufgedeckt werden können.

Als Maßnahme gegen zufällige Fehler fordert die DIN EN 61511 die Einhaltung zuverlässiger Höchstwerte für

die Versagenswahrscheinlichkeit (PFD) einer PLT-Schutzeinrichtung. Die Berechnung des PFD erfolgt auf Basis der gerätespezifischen Ausfallraten sowie betriebsabhängiger Parameter, wie dem Prüfintervall und der mittleren Reparaturdauer. Dabei kann nur dann auf die Herstellerangaben zurückgegriffen werden, wenn diese auch den Prozessanschluss eines Gerätes unter den gegebenen Randbedingungen einbeziehen und das Gerät spezifikationsgerecht betrieben wird.

Bei dem Nachweis der strukturellen Eignung einer PLT-Schutzeinrichtung errechnet sich die Versagenswahrscheinlichkeit (PFD) der sicherheitstechnischen Funktion aus der Summe der PFD-Werte der eingesetzten Komponenten. Das schwächste Glied begrenzt dabei den maximal zu erreichenden SIL-Wert der gesamten PLT-Schutzeinrichtung. Der Nachweis zur Eignung gegen systematische Fehler benötigt hingegen ein entsprechendes Sicherheitsmanagement.

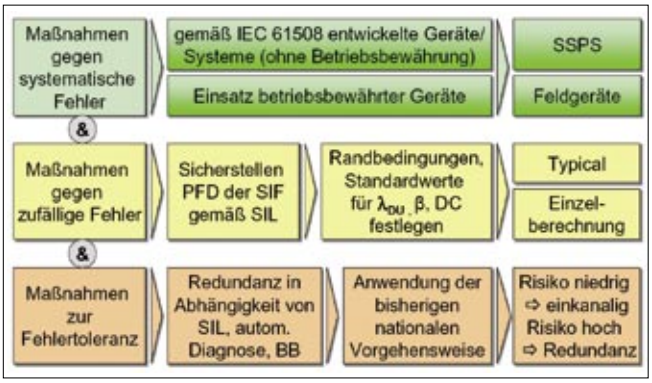
Sicherheitsmanagement nach Inbetriebnahme

Zu den Anforderungen an den Betrieb einer PLT-Schutzeinrichtung zählt neben der regelmäßigen Funktionsprüfung auch die kontinuierliche Erhebung und Auswertung von Störddaten, um so die notwendige Verfügbarkeit der Sicherheitsfunktion nachhaltig sicherzustellen. Bei dem Einsatz einer statistisch aussagefähigen Anzahl von Komponenten gleichen Typs und einer Fehlererhebung über einen längeren Zeitraum kann so die SIL-Eignung durch die Betriebswährung für die eingesetzten Geräte nachgewiesen werden.

Schwierigkeiten existieren bei der Störddatenerhebung in der Praxis allerdings bei der Abgrenzung zwischen systematischen Fehlern und zufälligen Fehlern. Auch das Erkennen von Fehlern mit gemeinsamer Ursache (common-cause-Fehler) erweist sich nicht immer als einfach.

Um den normativen Anforderungen eines nachhaltigen Sicherheitsmanagements gerecht zu werden, bedarf es also einer geeigneten Datenbank zur Störddatenerfassung aller PLT-Schutzeinrichtungen. Auf Basis der erfassten Ausfälle während des Betriebes und der bei der Instandhaltung festgestellten Fehler sowie den regelmäßigen Prüfungen lassen sich über statistische Verfahren betriebsbewährte Aussagen zur Ausfallwahrscheinlichkeit der eingesetzten Komponenten treffen.

Somit kommt der Betreiber zu einem Vergleich der durch den Hersteller bescheinigten Ausfallraten mit den realen Ergebnissen innerhalb seiner Betriebsumgebung und kann so den gemäß DIN EN 61511 geforderten quantitativen Nachweis der Zuverlässigkeit seiner PLT-Schutzeinrichtungen erbringen. Darüber hinaus können diese betriebsrealen Kenngrößen rückwirkend auf die während der Planung angesetzten sicherheitstechnischen Kenngrößen des Herstellers einwirken, sodass betriebsspezifische Aussagen zur Ausfallwahrscheinlichkeit getroffen werden können. Neben gegebenenfalls längeren Wartungszyklen resultiert durch die Störddatenanalyse auch der Nachweis der SIL-Eignung nicht bescheinigter Komponenten in normkonformer Form.



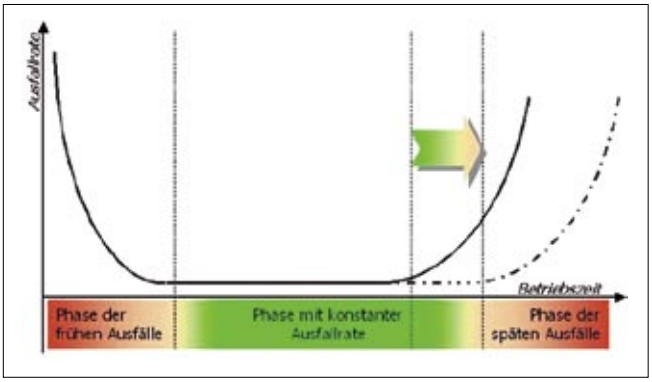
Geforderte Maßnahmen nach VDI/VDE 2180, Blatt 5

Diese Ergebnisse dienen nicht nur dem Sicherheitsaspekt, sondern können sich bei entsprechender Anwendung auch enorm kostensparend auswirken.

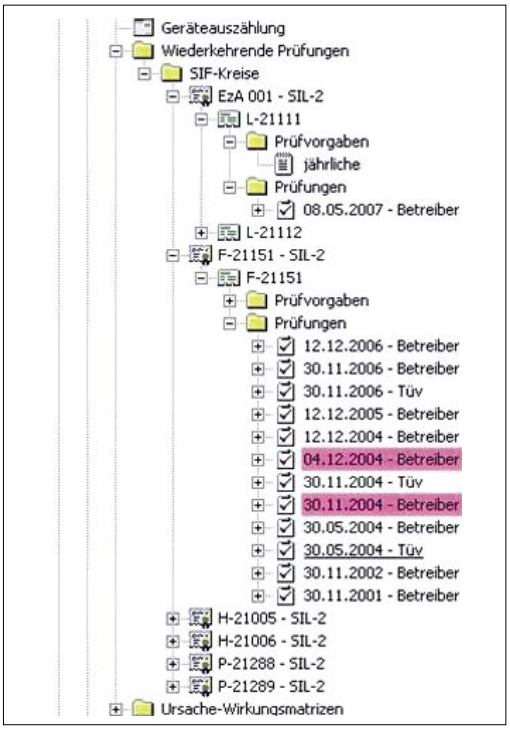
Die Anforderungen an eine geeignete und praktikable Störddatenerfassung sind im Sommer 2008 durch ein Projektteam, bestehend aus dem Dipl.-Ing. Thomas Gabriel, Institut für Automatisierungstechnik der technischen Universität Kaiserslautern unter der Leitung von Prof. Dr.-Ing. habil. Lothar Litz, Herrn Dipl.-Ing. Udo Hug, Sachverständiger nach §29A BImSchG und der Lippert Fuhrmann GmbH, Hersteller des CAE Systems MSR Office, formuliert worden.

Die wichtigsten Merkmale der angestrebten Lösung waren dabei: normgerechte Betriebsdatenerfassung und -analyse gemäß DIN EN 61511 bzw. VDI/VDE 2180 aller Komponenten in PLT-Schutzeinrichtungen, Datenbankbasierte Verwaltung mit der Differenzierung nach Komponententypen, typischen Komponentenstrukturen und den realen Komponenteninstanzen, Revisionssichere Speicherung aller erfassten Betriebsdaten, Störddatenerfassung „on the fly“ ohne großen Mehraufwand, Planung, Durchführung und Dokumentation regelmäßiger Prüfungen, Ermittlung der sicherheitstechnischen Kenngrößen der eingesetzten Komponenten über Betriebsbewährung sowie geeignete Analyse- und Auswertefunktionen.

Der Ansatz der Namur-Empfehlung NE 93 sieht dabei die Störddatenerfassung nur bis zu der Ebene des vollstän- ›



„Badewannenkurve“ als typischer Verlauf der Ausfalldichte



SIL Office, wiederkehrende Prüfungen im Überblick

digen Schutzkreises vor, womit eine Aussage zur Ausfallrate der individuellen Komponente und eine Interpolation auf den jeweiligen Komponententyp ohne weiteres nicht möglich ist. Vor diesem Hintergrund wurde die Erhebung von Fehlern und Betriebszeiten auf der Ebene der Komponenten als wesentliche Anforderung an eine geeignete Stördatenanalyse formuliert.

Verwaltung des gesamten Safety Lifecycle

Mit SIL Office steht seit Anfang 2009 eine praktikable und effiziente Software-Lösung zur Erhebung, Dokumentation und Auswertung der sicherheitsrelevanten Ereignisse aller Sicherheitsfunktionen zur Verfügung. Daneben werden die regelmäßigen Prüfungen der Sicherheitsfunktionen geplant, durchgeführt und überwacht.

SIL Office ist vollständig in das CAE-System MSR Office integriert, das Lippert Fuhrmann seit nunmehr zehn Jahren entwickelt und vertreibt. MSR Office ist als datenbankbasierte Lösung bei einer Vielzahl von Betreibern MSR-technischer Einrichtungen zur Planung und Betriebsbetreuung im Einsatz und stellt somit als praxiserprobte und etablierte Lösung eine gute Plattform für SIL Office dar.

Die eingesetzten Komponententypen werden in einem nach Hersteller, Einsatzgebiet und Messprinzip strukturierten Gerätekatalog beschrieben. Neben den Grundangaben können zu jedem Gerätetypen die SIL-Bescheinigung des Herstellers, sowie die sich daraus ergebenden sicherheitstechnischen Kenngrößen aufgenommen werden. Dabei wird zwischen expliziten Ausfallraten λS (Lambda Safe), λDU (Lambda Dangerous Undetected) , λDD (Lambda Dangerous Detected) und impliziten Angaben λT (= λs + λDD + λDU), SSF (Safe Failure Fraction) und DC (Diagnostic Coverage) unterschieden. Durch implementierte Umrechungsformeln können die Kenngrößen ineinander überführt werden. Häufig bescheinigen Hersteller die Zuverlässigkeit ihrer Komponenten unter Angabe impliziter Kenngrößen, für eine komponentenübergreifende Betrachtung sind jedoch einheitliche, vergleichbare explizite Angaben notwendig.

Die eingesetzten Geräte sind jeweiligen PLT-Stellen zugeordnet, wobei die sicherheitsrelevanten PLT-Stellen zu PLT-Schutzkreisen (SIF) zusammengefasst werden. Innerhalb einer PLT-Schutzeinrichtung sind alle verbauten Komponenten getrennt nach Sensorik, Aktorik und Steuerung beschrieben. Zu jeder Komponente kann im Rahmen der Auslegungsspezifikation die Betriebsumgebung detailliert dokumentiert werden.

Die Erfassung der für den Safety Lifecycle benötigten Ereignisse, wie die Inbetriebnahme, die planmäßige Prüfung, eine Außer- und Wiederinbetriebnahme sowie eine Komponentenstörung erfolgt im Rahmen des Gerätelebenslaufs. Wesentlich ist dabei zur Ermittlung der Gerätezuverlässigkeit die Erhebung der störungsfreien Betriebsstunden, sowie die Verwaltung und Klassifizierung von Gerätestörungen und deren Zeitpunkt. Für die Inbetriebnahme, die Außer- und Wiederinbetriebnahme, sowie die Stördatenerfassung stehen entsprechende Dokumentvorlagen zur Verfügung. Das Design der Dokumente orientiert sich dabei an den Empfehlungen der NE 93, kann aber individuell angepasst werden. Bei der Stördatenerfassung wird zwischen Gerätestörungen während des Betriebs und Fehlern unterschieden, die (erst) während der Durchführung einer planmäßigen Überprüfung erkannt werden. Der diagnostizierte Fehler wird gemäß NE 93 verschiedenen Fehlerklassen zugeordnet.

Wiederkehrende Prüfungen der PLT-Schutzeinrichtungen werden auf einfache, übersichtliche und handhabbare Weise definiert, verwaltet und überwacht. Auf Basis der Komponenten der Sicherheitsfunktionen sowie Prüfmethoden können Prüfvorgaben und Prüfszenarien definiert werden, die unter anderem durch Sollwertvorgaben, Prüfinstanzen (z.B. TÜV) und dem Prüfintervall beschrieben sind. Das Prüfintervall orientiert sich dabei an den Festlegungen aus der durchgeführten Risikoanalyse.

Nachweis der betriebsbewährten SIL-Eignung

Für das Einstellen und die Durchführung von Prüfaufträgen sowie eine lückenlose Dokumentation der durchgeführten Prüfungen inklusive der Prüfungsergebnisse und etwaiger festgestellter Mängel stehen Assistenten und Übersichten zur Verfügung. Diverse Auswertungen, wie zum Beispiel eine Ressourcenplanung, bieten einen gezielten Überblick über zukünftig anstehende Prüfungen sowie den dafür notwendigen Zeitbedarf. Sicherheitsschaltungen können darüber hinaus als Ursache-Wirkung zwischen Sensoren sicherheitsrelevanter Funktionen und Aktoren in Matrizen beschrieben werden.

Auf Basis der erhobenen Lebenslauf-Ereignisse ergeben sich für die Komponenten der Sicherheitsfunktionen die störungsfreien Betriebszeiten, sowie die Anzahl und die Klassifizierung aufgetretener Gerätefehler im jeweiligen Beobachtungszeitraum. Betrachtet man nun eine statistisch ausreichend große Zahl unterschiedlicher Komponenten (Geräte) gleichen Typs über einen hinreichend langen Zeitraum, so kann über eine Konfidenzintervallschätzung eine Ausfallrate der Komponententypen unter den vorliegenden Betriebsbedingungen attestiert werden. Für die Berechnung des Konfidenzintervalls gelten dabei die Rahmenbedingungen der DIN EN 61508 bzw. DIN EN 61511.

Somit werden unter Berücksichtigung der realen Betriebsumgebung die sicherheitstechnisch relevanten Kenngrößen λS (Lambda Safe), λDU (Lambda Dangerous Undetected) und λDD (Lambda Dangerous Detected) ermittelt. Diese Kenngrößen werden direkt am Komponententyp im Gerätekatalog gespeichert und können direkt mit den Angaben des Herstellers in Bezug gesetzt werden. Ein rückwirkender Einfluss in die Risikoanalyse ist somit möglich.

Kontinuierliche Stördatenerfassung

Hersteller prognostizieren in der sogenannten „Badewannenkurve" die Anzahl der zu erwartenden Komponentenausfälle, die insbesondere in der Phase nach der Inbetriebnahme und nach Ablauf der empfohlenen nutzbaren Lebensdauer (zum Beispiel 10-12 Jahre) sprungartig ansteigen. Dieser Kurvenverlauf wird von dem Hersteller pessimitischen Annahmen unterzogen.

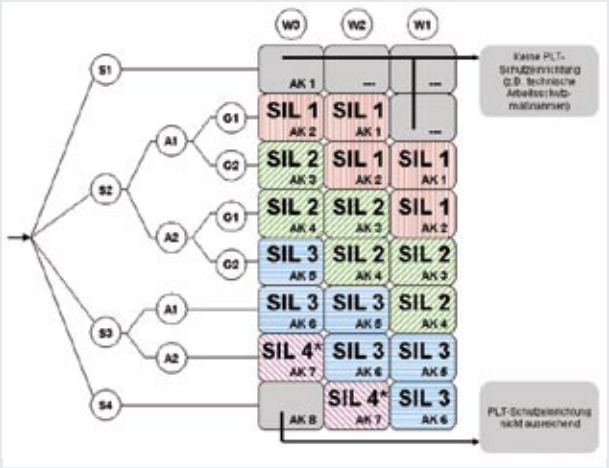
Aus der Ermittlung der betriebsbedingten Ausfallwahrscheinlichkeit kann die Phase der nutzbaren Lebensdauer besser bewertet und gegebenenfalls verlängert werden. Somit wird ein verfrühter Komponentenaustausch vermieden, was zu einer Betriebskostenoptimierung führt.

Darüber hinaus wird durch die kontinuierliche Stördatenerfassung der Beginn der Phase der „Spätfolgen" automatisch erkannt, da eine auftretende Häufung von Ausfällen eines Komponententyps gemäß der Badewannenkurve einen weiteren Anstieg ankündigt. Entsprechende Maßnahmen können frühzeitig eingeleitet werden, was sich positiv auf die Anlagenverfügbarkeit auswirkt.

Als weiterer Aspekt ist das Aufdecken von systematischen Fehlerschwerpunkten ein gewichtiges Argument für eine kontinuierliche Stördatenerfassung. Fehlerschwerpunkte in bestimmten Anlagenbereichen, wie zum Beispiel Verbackungen oder Kristallisierungen können aufgedeckt und gezielt beseitigt werden.

Durch die Ermittlung der betriebsbewährten Ausfallraten können Zykluszeiten für planmäßige Prüfungen verlängert werden, ohne dabei die Einhaltung bestehender Auflagen zu verletzen. Als weiterer Punkt ist der quantitative Nachweis der SIL-Eignung der Sicherheitsfunktionen auf Basis der Betriebsbewährung zu nennen, der gemäß DIN EN 61511 nicht nur für unbescheinigte Komponenten, sondern auch für SIL-bescheinigte Geräte verpflichtend ist.

Risikomatrix zur Ermittlung des Safety-Levels



- Schadenausmaß S:
  S1: leichte Verletzung einer Person; kleinere schädliche Umwelteinflüsse
  S2: Schwere irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person; vorübergehende größere schädliche Umwelteinflüsse
  S3: Tod mehrerer Personen; langandauernde größere schädliche Umwelteinflüsse
  S4: Katastrophale Auswirkungen, sehr viele Tote
- Aufenthaltsdauer von Menschen im Gefahrenbereich A:
  A1: selten bis öfter
  A2: häufig bis dauernd
- Gefahrenabwendung durch Reaktion des Menschen G:
  G1: möglich unter bestimmten Bedingungen
  G2: kaum möglich
- Eintrittswahrscheinlichkeit des unerwünschten Ereignisses W:
  W1: sehr gering
  W2: gering
  W3: relativ hoch

Resümee

Mit dem Programmpaket SIL Office steht – als vollständig in das etablierte CAE-System MSR Office integriertes System – eine praktikable und effiziente Lösung zur kontinuierlichen Stördatenerfassung zur Verfügung. Die Verwaltung des gesamten Safety Lifecycle der eingesetzten Komponenten in Sicherheitsfunktionen ist handlich und bedarf keiner großen Mehrarbeit.

Durch statistische Verfahren werden auf Basis der Gerätelebensläufe betriebsbewährte Ausfallraten ermittelt, die gemäß DIN EN 61511 rückwirkend in die Betrachtungen der Risikoreduzierung einfließen können und den quantitativen Nachweis der SIL-Eigung erbringen. Aus einer möglichen Verlängerung von Prüfzyklen, dem Aufdecken von Fehlerschwerpunkten und der Verlängerung der nutzbaren Lebensdauer der Komponenten resultieren für den Betreiber neben allen Sicherheitsaspekten auch enorme Einsparpotenziale. □

> MORE@CLICK SIK10118