SIL-Degradation für bestehende (Legacy-) Sicherheitssysteme: 4 Faktoren, die sich auf SIL-Leistung auswirken

PipeSystemConsult GmbH Newsbeitrag 4 - Mai 2018

Für bestehende (Legacy-)Sicherheitssysteme, die sich dem Alter von zehn Jahren nähern, gibt es vier wichtige Punkte, die Betreiber beachten sollten, um eine SIL-Degradation ihrer sicherheitstechnischen Systeme (SIS) zu vermeiden.

1. Einsatzzeitraum (engl.: Mission-Time)

Der Einsatzzeitraum (engl.: Mission Time, MT) ist das Zeitintervall, in dem ein SIS betrieben werden sollte, ohne dass eine umfassende Wartung oder ein vollständiger Austausch erforderlich ist. In der VDI/VDE 2180-3 ist die „Mission-Time" (T2) genauer definiert als das Intervall, nach dem alle Elemente mit vollständiger Prüftiefe (PTC = 100 %) getestet werden müssen; in der Praxis bedeutet dies meistens eine vollständige Wartung oder einen vollständigen Austausch. Der MT könnte basierend auf der Nutzungsdauer der Hauptgeräte gewählt werden, z. B. die sicherheitsgerichtete Steuerung (das „ESD-System"). Ein typischer Wert des MT ist 15 bis 20 Jahre.

Der MT sollte in der Spezifikation der Sicherheitsanforderungen (SRS) gemäß IEC 61511, §10 (VDI/VDE 2180-2, §6) festgelegt werden. Für Legacy-Systeme ist dieser Wert möglicherweise nicht eindeutig, daher könnte es für Betreiber verlockend sein, den MT zu verlängern, um Betriebskosten (OPEX) zu verzögern. Aber selbst für Anlagen, die die MT-Grenze nicht erreicht haben, kann die Auswirkung auf die SIL-Bewertung in Kombination mit einer unvollständigen Prüftiefe signifikant sein, wie unten gezeigt.

2. Prüftiefe

Die sog. „Prüftiefe" (engl.: Proof-Test Coverage CPT) ist der Anteil gefährlicher unentdeckter Fehler, der durch Wiederholungsprüfungen aufgedeckt werden kann. Die CPT hat einen Einfluss auf die PFDavg während des Einsatzzeitraums gemäß der unten dargestellten vereinfachten Formel:

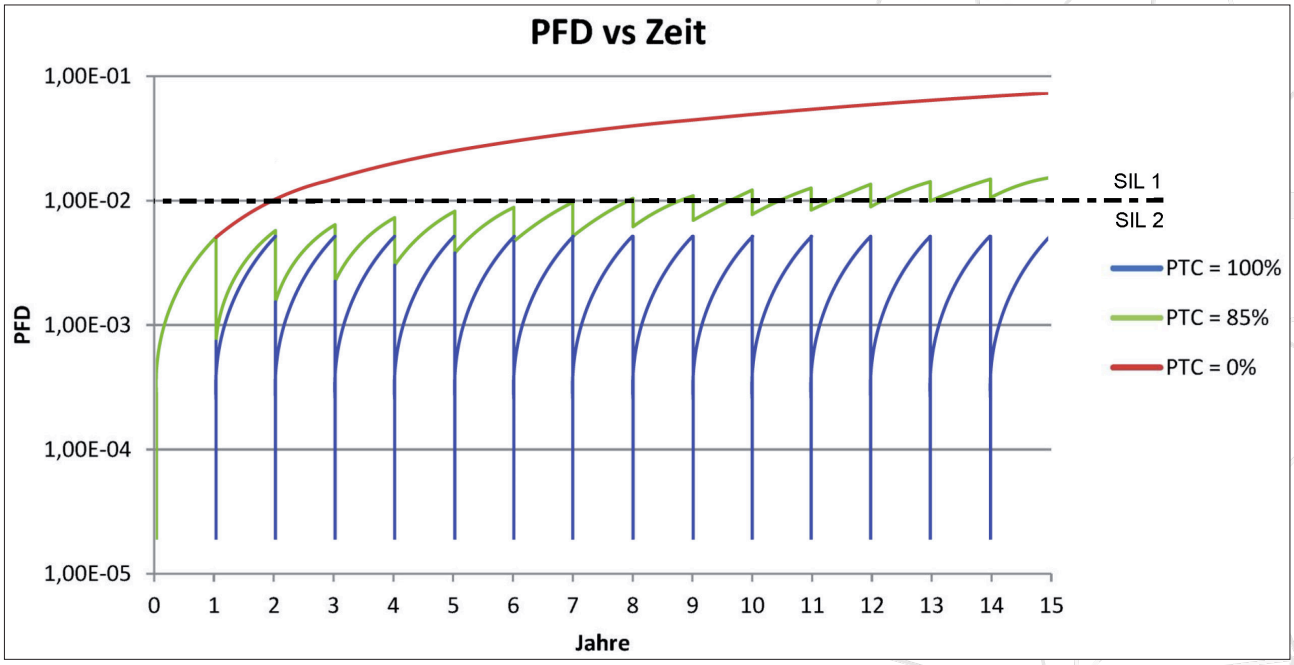
$$PFD_{AVG} = C_{PT} \lambda_D TI/2 + (1-C_{PT}) \lambda_D MT/2$$

Dies ist im folgenden Bild grafisch dargestellt.

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 München, Deutschland

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

PSC | PipeSystem Consult GmbH



SIL-Degradation (PFD vs Zeit)

Die blaue Linie zeigt, wie die PFD nach der Wiederholungsprüfung (z. B. alle 12 Monate) zurückgesetzt wird, unter der Annahme einer theoretischen Prüftiefe von 100 %, d. h., alle möglichen Fehler werden detektiert. Umgekehrt zeigt die rote Linie, wie die PFD logarithmisch ansteigt, wenn überhaupt kein Prüftest durchgeführt wird. Die grüne Linie zeigt eine realistische CPT von 85 %; selbst in diesem Fall nimmt die PFD mit der Zeit zu, sodass am Ende des Einsatzzeitraums (in diesem Fall 15 Jahre) die PFDavg für das hypothetische SIS die Schwelle zwischen SIL-2 und SIL-1 überschritten hat (SIL-Degradation). Daher können, wie oben erwähnt, der MT und die CPT in Kombination eine signifikante Auswirkung auf die erreichte SIL-Bewertung über die Lebensdauer der Anlage haben.

Was sind die tatsächlich erreichbaren CPTs in der Praxis? Exida zum Beispiel hat Daten veröffentlicht, die zeigen, dass die CPT für eine Antrieb-/Armatur-Kombination von 57-99 % variieren kann, abhängig davon, ob ein Teil- oder Vollhubtest durchgeführt wird, im besten Fall kombiniert mit der Überwachung der Sitzleckage unter Betriebsbedingungen.

Um eine realistische Schätzung der tatsächlichen CPT zu machen, soll der Betreiber seine dokumentierten Proof-Testverfahren mit den veröffentlichten Daten des Herstellers (gemäß dem Sicherheitshandbuch) und/oder mit Industriequellen wie der SERH-Datenbank von Exida vergleichen. Die nächste Version von NAMUR NE 106 (geplant für 2018) wird CPT-Bänder für generische Proof-Test-Aktivitäten veröffentlichen und damit zusätzliche Hinweise geben.

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 München, Deutschland

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

3. Nutzungsdauer (engl.: Useful Life)

Die Berechnung der PFD basiert auf der Annahme einer konstanten Fehlerrate während der sogenannten Nutzungsdauer einer Komponente. Die Nutzungsdauer ergibt sich aus dem „Badewannen" -Modell und berücksichtigt, dass Verschleißbedingungen eventuell zu zunehmenden und unvorhersehbaren Ausfällen führen. Die Hersteller definieren die Nutzungsdauer auf der Grundlage einer statistischen Analyse von vor Ort installierten Feldgeräten, oder alternativ kann dies durch theoretische Methoden wie FMEDA berechnet werden.

Die Nutzungsdauer kann überraschend kurz sein. Ein Hersteller z.B. definiert die Nutzungsdauer eines Magnetventils zwischen 3 und 10 Jahren, abhängig von der Leistungsaufnahme und der Ausfallsicherheit (z. B. Ruhestromprinzip). Die Nutzungsdauer kann durch erhöhte Einsatzbedingungen weiter reduziert werden.

Der Hauptgrund für die Beachtung der Lebensdauer ist, dass, die gesamte Basis für die SIL-Berechnung nicht mehr gültig ist, sobald diese für eine einzelne Komponente einer Sicherheitsschleife überschritten wird (da die Annahme einer konstanten Fehlerrate nicht länger gilt). Wartungsprogramme sollten eine Aufzeichnung der Nutzungsdauer von sicherheitskritischen Komponenten enthalten, sodass diese rechtzeitig ausgetauscht oder überholt werden können, um eine SIL-Degradation zu vermeiden.

4. Stördatenerfassung/Betriebserfahrung

Schließlich haben die HAZOP/SIL/LOPA-Analysen, die zu Beginn eines Projekts durchgeführt wurden, bestimmte Annahmen für die Anforderungs- und Ausfallrate getroffen. Diese beruhen häufig auf der Erfahrung des Betreibers mit ähnlichen Anlagen oder Standardwerten aus Industriequellen. Nach IEC 61511-1 §16.2 muss der Betreiber die tatsächlichen Betriebsdaten erfassen, um sicherzustellen, dass die ursprünglichen Risikoanalyseannahmen noch gültig sind (siehe auch VDE/VDI 2180-1 und Namur NE 93/130). Für eine Anlage, die seit zehn Jahren in Betrieb ist, sollten ausreichende Betriebsdaten verfügbar sein, um die Annahmen von HAZOP/LOPA zu bestätigen oder zu aktualisieren. Diese Daten können auch eine Evaluierung der „Betriebsbewährtheit" (engl.: „Proven-In-Use") unterstützen, für Elemente bei denen die Herstellerzertifizierung fehlt oder veraltet ist. In vielen Fällen kann die Auswertung solcher Daten für den Betreiber von Vorteil sein, da die Bestätigung einer niedrigeren Anforderungsrate bzw. einer besser als angenommenen Geräteausfallrate eine Reduzierung der SIL-Anforderungen ermöglichen können. Auf der anderen Seite können eine erhöhte Anforderungshäufigkeit oder mehrere gefährliche Ereignisse die Installation zusätzlicher Schutzmaßnahmen oder eine Verbesserung des Integritätslevels existierender SIFs erfordern..

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 München, Deutschland

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

Hier sind nun die Fragen, die Betreiber von bestehenden Anlagen sich stellen sollten:

-Wie hoch ist meine Einsatzzeit?

-Was ist die eigentliche Prüftiefe meiner Wiederholungsprüfung?

-Haben die Komponenten in meinen Sicherheitsschleifen ihre Nutzungsdauer überschritten?

-Verfüge ich über Betriebsdaten, um die Annahmen der Anforderungs- und Ausfallrate zu stützen?

PSC bietet Audit- und Bewertungsdienstleistungen gemäß DIN EN 61511, um Lücken in der FSM-Dokumentation und Betriebspraktiken zu identifizieren, die zu einer „SIL-Degradation" führen können.

PipeSystemConsult GmbH
Adelheidstrasse 12
80798 München, Deutschland

Telefon: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Email: info@pipesyscon.com

PSC | PipeSystem Consult GmbH