DOI 10.5162/sensoren2016/1.3.1

Zuverlässigkeit durch Selbstdiagnose

Dipl.-Wirtschaftsing.Hans Joachim Fröhlich
Endress+Hauser Flowtec AG, Kägenstr. 7, 4153 Reinach, Schweiz

Zusammenfassung

Durch gezielt erweiterte Testabdeckung hat die Fähigkeit zur permanenten Selbstdiagnose die Verlässlichkeit aktueller Sensorsysteme stark verbessert und die Notwendigkeit zur wiederkehrenden Prüfung, etwa durch Kalibrieren, deutlich reduziert. Wesentlich getrieben wurde diese Entwicklung in den vergangenen zehn Jahren durch Umsetzung internationaler Normen zur Funktionalen Sicherheit, welche quantitative Methoden zur Risikoabwehr im Rahmen sicherheitstechnischer Einrichtungen vorgeben. Diese Normen stellen auf die Funktionszuverlässigkeit beteiligter Systemkomponenten im Betrieb ab. Im Fall von Messgeräten spielt deren Genauigkeit zwar eine Rolle als Kriterium bei der Bewertung von Fehlermöglichkeiten und deren Auswirkung auf die Funktionsfähigkeit des Sensorsystems, eine direkte Überwachung der Messunsicherheit ist jedoch nicht vorgeschrieben.
Am Beispiel moderner Durchflussmessgeräte wird diskutiert, unter welchen Bedingungen das im Rahmen der Funktionalen Sicherheit verwendete Modell angewendet und erweitert werden kann, um Aussagen im Hinblick auf die Verfügbarkeit auch von Messstellen zu gewinnen, die im Rahmen der Prozessautomatisierung primär einen genauen Messwert zu liefern haben. Wird die Prämisse einer spezifikationsgerechten Verwendung des Sensors fallen gelassen und mithin Verschleiß an medienberührenden Teilen zugestanden, zeigt sich zudem die Notwendigkeit einer Ergänzung des beschriebenen Ansatzes um verlässliche Diagnosen der mechanischen Integrität solcher Teile. Auf das erweiterte Diagnosekonzept wird beispielhaft für ein Coriolis-Messsystem eingegangen.

Keywords: Geräteverifikation, Funktionale Sicherheit, Messgenauigkeit, Verlässlichkeit, Selbstdiagnose

Funktionale Sicherheit: Wiederkehrende Prüfung von Schutzeinrichtungen als betriebliches Optimierungsproblem

Internationale Normen zur Funktionalen Sicherheit wie die IEC 61508 i.V.m. IEC 61511 [1] geben dem Betreiber einer verfahrenstechnischen Anlage umfangreiche Anleitung bzgl. der Planung, Einrichtung und Betrieb von Schutzeinrichtungen zur Abwehr von Risiken für Mensch, Betrieb und Umwelt. Wird die Schutzfunktion mit automatisierten Systemen erzielt, ist eine regelmässige Prüfung der Einrichtung und ihrer Teilsysteme vorgeschrieben. Prüfungsintervalle hängen u.a. von der Kritikalität der Schutzeinrichtung ab, ausgedrückt in der geforderten Sicherheitsintegrität. Diese ist definiert durch die Wahrscheinlichkeit, dass die Einrichtung ihre Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines bestimmten Zeitraums anforderungsgemäß ausführt [2]. Prüfungsintervalle werden danach gemäß der erwarteten Wahrscheinlichkeit des Versagens der Schutzeinrichtung bestimmt. Die Wiederholungsprüfung kann in einem bestimmten Intervall für das System insgesamt erfolgen, oder in Teilprüfungen mit eigener Periodizität bestehen. Für letzteres können wirtschaftliche Interessen des Betreibers insbesondere dann sprechen, wenn sich individuell bestimmte Prüfungsintervalle, sowie die Methoden zur Wiederholungsprüfung unter den Teilsystemen stark unterscheiden.
Die Optimierung der wiederkehrenden Prüfung mit einer Zielfunktion aus Wartungs- und Opportunitätskosten im Betrieb, sowie Nebenbedingungen, die sich aus den Auflagen der Norm ergeben, kann daher in Abhängigkeit der Prozess- und Betriebsbedingungen zu sehr unterschiedlichen Entscheidungen führen.

Risikobewertung gemäß IEC 61508 bzw. IEC 61511 mittels gefährlicher unentdeckter Fehler und Versagenswahrscheinlichkeit

Im stochastischen Modell der Funktionalen Sicherheit kommt das Konzept der Wahrscheinlichkeit eines Ausfalls bei Anforderung (Probability of Failure on Demand, PFD) zur Anwendung [1]. Hierin werden für jede betrachtete Schutzeinrichtung vor allem die zu erwartenden Häufigkeiten des Auftretens von gefährlichen unentdeckten Fehlern λ_{DU} kumuliert, wobei die vorhandene Selbstüberwachungsfunktion aller Systemkomponenten berücksichtigt wird.

Im Rahmen einer Fehler-Möglichkeits-, Einfluss- und Diagnose-Analyse (FMEDA) werden für jedes Teilsystem der Schutzeinrichtung auf Bauteilebene Fehlerszenarien definiert und mit Eintrittswahrscheinlichkeiten quantifiziert. Diese Bewertung kann anhand der vom Hersteller für diesen Zweck angegebenen Parameter, oder mit Hilfe von akzeptierten, generischen Werten erfolgen. Diagnosefunktionen, die in das Teilsystem integriert sind, wirken in diesen Szenarien hemmend auf die Eintrittswahrscheinlichkeit. Die Diagnosefunktionalität wird sodann jedoch auch selbst einer entsprechenden Bewertung unterzogen. Um den Einfluss auf die Funktionszuverlässigkeit des Teilsystems insgesamt zu bewerten, wird ein einheitliches Kriterium gefordert, an dem sich die Bewertung der Bauteile orientiert. Wird als Teilsystem einer Schutzeinrichtung etwa ein Messgerät betrachtet, kann hierfür die vom Hersteller spezifizierte Messgenauigkeit herangezogen werden, d.h. ein Fehlerszenario für ein Bauteil trägt zum Risiko des Teilsystems erst dann bei, wenn die spezifizierte Messgenauigkeit im relevanten Betriebszustand nicht mehr eingehalten wird. Die IEC 61508 lässt jedoch auch hiervon abweichende Kriterien zu [2], so etwa eine inkrementelle Messunsicherheit, welche die spezifizierte Messgenauigkeit übersteigt.

Durchflussmessgeräte als Beispiel für Sensorsysteme in Schutzeinrichtungen

Abhängig von der Messaufgabe, den Prozess- und Umgebungsbedingungen kommen als Sensorsysteme für die Durchflussmessung in Schutzeinrichtungen sehr unterschiedliche Messprinzipien zum Einsatz:
So sind auch gegenwärtig noch Blenden mit Druckdifferenzdruck-Umformern anzutreffen, ebenso wie vielfältige Schwebekörpergeräte; beide Messprinzipien sind aufgrund höherer Risikobewertungen gegenüber moderneren Technologien im Nachteil. Dies hängt mit ihrer durch anfällige mechanische Wirkprinzipien geprägte Messaufnahme zusammen. Für eine in die Umformer-Elektronik integrierte Diagnosefunktion sind Fehler in diesem Bereich kaum zugänglich. Modernere Messprinzipien wie etwa Coriolis, Magnetisch-Induktiv, Wirbelzähler, Ultraschall oder Thermisch weisen an dieser Stelle eine wesentlich geringere Anfälligkeit für mechanische Fehler auf; jedenfalls solange die Geräte spezifikationsgerecht eingesetzt und betrieben werden. Die Normen zur Funktionalen Sicherheit [1] gehen bei der Berechnung von Systemgrößen wie λ_{DU} und PFD von dieser wichtigen Bedingung aus. Im Laufe der weiteren Betrachtung wird hierauf noch eingegangen.

Veranschaulichung des Zusammenhangs zwischen Fehlerbewertung und Intervall zur Wiederholungsprüfung für Coriolis-Geräte

Im folgenden Beispiel wird ein Coriolis-Durchflussmessgerät des Typs Promass 200 von Endress+Hauser der Vorgängergeneration Promass 83 gegenüber gestellt.
Die wesentlichen Kenngrößen sind folgender Abbildung zu entnehmen:

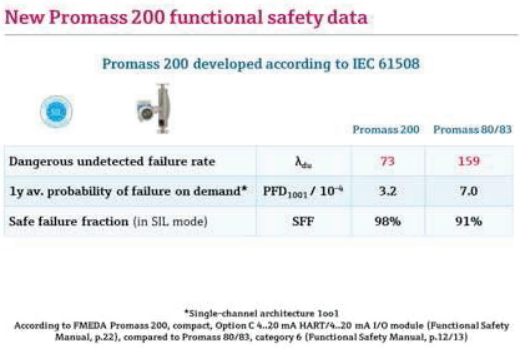

Abb. 1: SIL-Kenngrössen von Promass 200 gegenüber Promass 83 (λ_{DU} in rot)

Im Beispiel einer einfachen Schutzeinrichtung, die aus Sensorsystem, Logikeinheit und einem aktiven Element besteht, wird eine Sicherheits-Integrität von SIL-2 gefordert, d.h. die PFD für das System darf über die Nutzungsdauer einen Wert von durchschnittlich 1% nicht übersteigen [1]. Dem Sensorsystem werde davon ein Anteil an 0,25% zugeordnet, da das aktive Element aufgrund von Betriebsbewährung eine höhere Risikobewertung erhält und für die Logikeinheit als Teilsystem SIL-3 gefordert wird:

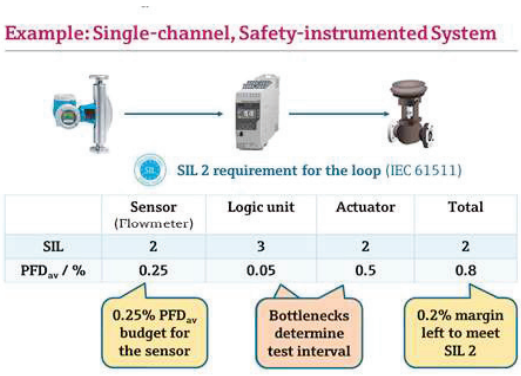

Abb. 2: Schema (vereinfacht) einer Einkanal-Schutzeinrichtung mit PFD-Zuteilung

Die wiederkehrende Prüfung des Vorgänger-Messgerätes Promass 83 wird in Form einer partiellen Prüfmethode, nämlich mit dem Verifikationssystem Fieldcheck vorgenommen. Für diese auf Signalsimulation beruhende Methode ist eine Testabdeckung von ca. 90% angegeben. Das Messgerät verbleibt in der Anwendung, Prozess und Messbetrieb sind jedoch für die Verifikation zu unterbrechen. Bei jährlicher Durchführung wird für das Messgerät eine mittlere PFD von unter 0,25% erzielt, die Nutzungsdauer erreicht leicht 10 Jahre:

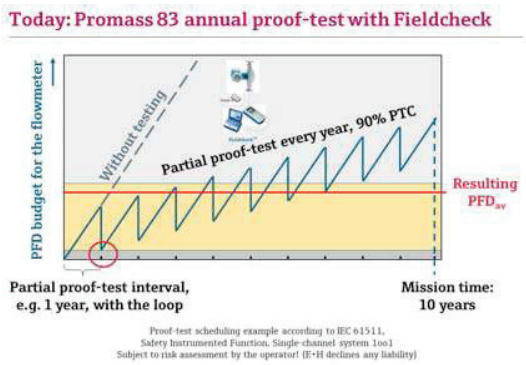

Abb. 3: PFD, Nutzungsdauer Promass 83 bei jährlicher Wiederholungsprüfung durch Verifikation mit Fieldcheck

Der nach IEC 61508 entwickelte Gerätetyp Promass 200 ist zwecks λ_{DU}-Reduktion mit erweiterten Diagnosefunktionen ausgestattet. Für die wiederkehrende Prüfung wird vom Hersteller eine Kalibrierung alle fünf Jahre nahegelegt. Hierbei handelt es sich im Sinne der Norm um eine vollumfängliche Prüfung, welche die PFD nahezu auf null zurücksetzt. Die resultierende mittlere PFD liegt nun wesentlich unterhalb der geforderten 0,25%, was nahelegt, die Nutzungsdauer des Messgeräts entsprechend zu verlängern:

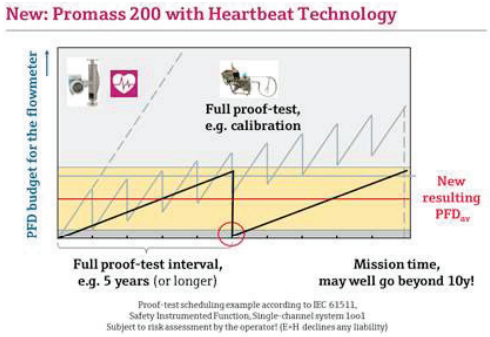

Abb. 4: PFD, Nutzungsdauer Promass 200 bei 5-jähriger Wiederholungsprüfung durch Kalibrierung

Erfordern andere Teilsysteme der Schutzeinrichtung ein kürzeres Prüfintervall, können die integrierten Diagnosefunktionen des Sensors auf Anforderung zu einem Testablauf zusammengefasst werden. Die Prüfergebnisse einer solchen Verifikation werden im Gerät gespeichert. Sie können mittels Asset Management Tool ausgelesen und in einem Bericht dokumentiert und sodann archiviert werden. Da nahezu alle verwendeten Tests auch Teil der Selbstüberwachung sind, die permanent im Gerät abläuft, lässt sich hiermit indessen keine Verbesserung der mittleren PFD oder der Nutzungsdauer mehr erzielen.
Unter wirtschaftlichen Gesichtspunkten ergibt sich als Zusatznutzen jedoch die gewonnene Flexibilität, anderen Teilsystemen ein höheres PFD-Budget zuzuteilen und somit die Prüfintervalle für diese bzw. für die Schutzeinrichtung insgesamt zu verlängern. Längere Prüfintervalle erweitern ferner generell den Spielraum, bei wiederkehrender Prüfung mehr Rücksicht auf die Anlagenverfügbarkeit zu nehmen und Opportunitätskosten durch Produktionsausfall zu vermeiden.

Übertragbarkeit des PFD-Modells für Messgeräte auf Anwendungsgebiete jenseits der Funktionalen Sicherheit

Auch für Messstellen zur Abrechnung von Erzeugnissen oder Zwischenprodukten der Prozessindustrie, sowie von Hilfs- und Betriebsstoffen, die in Rohrleitungen geführt werden, besteht die Verpflichtung des Betreibers zur wiederkehrenden Prüfung. Messstellen in Großbetrieben, die etwa zur Berichterstattung über CO_2-Ausstoss bzw. zur Erstellung von Wärmebilanzen dienen, sind regelmäßig zu prüfen.
Zudem ist schon jeder Betrieb, der sich einem Qualitätsmanagement nach ISO 9001 unterwirft, zur regelmäßigen Prüfung seiner Messstellen mittels metrologisch rückführbarer Verifikation oder Kalibrierung verpflichtet [3].
Die integrierte Diagnosefunktionalität kann, wie oben bereits geschildert, in jedem dieser Fälle zur Messstellenprüfung im Sinne einer Geräteverifikation herangezogen werden. Anders als zuvor, spielt die Darstellung einer zuverlässigen Schutzfunktion zwischen zwei Prüfterminen bei den hier genannten Anwendungen grundsätzlich keine Rolle. Ob die Diagnose auch während des Betriebes läuft, oder nicht, ist genauso unerheblich, wie die Frage, ob im Moment der Verifikation eine erweiterte Testabdeckung erreicht wird, als schon während des Betriebes, oder nicht.
Wo immer spezifische Regelungen, wie etwa das Eichgesetz, oder Direktiven der EU zum

Emissionsrechtehandel, keine Prüfintervalle vorgeben, steht der Betreiber vor einem vergleichbaren Optimierungsproblem, wie oben diskutiert bei der wiederkehrenden Prüfung sicherheitstechnischer Einrichtungen.

Nutzung der im Rahmen einer FMEDA nach IEC 61508 gewonnenen Daten zur Risikobewertung eines Messgerätes

Grundsätzlich lassen sich die erwarteten Häufigkeiten gefährlicher unentdeckter Fehler λ_{DU} auch für die Anwendung eines Messgeräts jenseits der Funktionalen Sicherheit nutzen. Da die SIL-Bewertung hierbei ihre Relevanz verliert, ist eine Gesamttestabdeckung (etwa TTC: Total Test Coverage) zu definieren, welche in Ergänzung zu λ_{DU} und PFD noch die bedingte Wahrscheinlichkeit der Entdeckung von Fehlern beschreibt, für den Fall, dass ein überhaupt Fehler eingetreten ist.
Zulässig ist dieser Ansatz indessen nur, sofern hierbei das zugrunde liegende Kriterium gültig bleibt, mittels dessen die Fehlereinflüsse im Rahmen der FMEDA nach IEC 61508 bewerten wurden.
Ist in einer bestimmten Anwendung eines Messgerätes die spezifizierte Messgenauigkeit von Bedeutung, so kann der für jedes Bauteil ermittelte Wert λ_{DU} nur dann gültig bleiben, wenn diese Messgenauigkeit auch Kriterium bei der Bewertung der Auswirkungen in Fehlerszenarien gewesen ist. Wie zuvor erwähnt, wird dies von der IEC 61508 nicht gefordert, so dass in der Praxis auch weniger enge Kriterien in die sicherheitstechnische Bewertung vieler Messgeräte Einzug erhalten. Mittels PFD-Modell ausgelegte Prüfintervalle sowie auch die SIL-Zertifizierung verlieren damit nicht nur sachlich ihre Gültigkeit für Anwendungen außerhalb der Funktionalen Sicherheit. Sie führen grundsätzlich zu Fehlschlüssen und können bestenfalls zu einer groben Abschätzung einer sinnvollen Prüfplanung dienen. In solchen Szenarien ist der nicht unbeträchtliche Aufwand für eine FMEDA ggf. mit einem zutreffenden Kriterium zu wiederholen. Die Frage der Zertifizierung durch unabhängige Sachverständige stellt sich ebenfalls von neuem. Das im o.g. Beispiel referenzierte Durchflussmessgerät des Typs Promass 200 erfüllt jedoch die Anforderung zur Übertragbarkeit der im Rahmen der SIL-Zertifizierung erstellten FMEDA, weil die Bewertung des Einflusses der Fehlerszenarien im Einklang mit der spezifizierten Messgenauigkeit steht. In diesem Fall lässt sich die integrierte Diagnose auch zur Messstellenverifikation heranziehen. Geben einschlägige Regeln kein festes Prüfungsintervall vor, kann somit auch das PFD-Modell für die Bestimmung einer sinnvollen Prüfperiode genutzt werden.

Metrologische Rückführbarkeit stellt hohe Anforderung dar, die mittels redundanter Referenzen im Gerät erfüllt werden kann

Die integrierte Prüffunktionalität ist nur so lange gut, wie die Referenzen im Gerät stabil bleiben. Dies gilt grundsätzlich sowohl für die permanente Diagnose, wie auch für die darauf aufbauende interne Verifikationsfunktion. Jeder Funktionstest, der im Gerät an einem Teilsystem oder einer Komponente erfolgt, besteht in dem Vergleich des aktuellen Zustandsparameters mit mindestens einem Grenzwert. Auch wenn die technischen Konzepte moderner Messgeräte darauf ausgelegt sind, fehleranfällige Analogtechnik weitgehend zu vermeiden, geht jeder interne Vergleich von Ist und Soll auf zuverlässige, d.h. stabile Referenzen zurück. Um der Anforderung der Rückführbarkeit zu entsprechen, muss deshalb Drift in den Referenzen ausgeschlossen werden.
Dies gelingt durch redundante, d.h. mehrfach vorhandene Referenzen im Gerät, so dass ein permanenter Vergleich der Referenzen in die Prüfprozedur mit aufgenommen werden kann. Darüber hinaus muss eine ununterbrochene Kette von Vergleichen auf amtliche Normale dokumentiert werden. Im Fall der in einem Messgerät integrierten Referenzen, wie für das o.g. Durchflussmessgerät vom Typ Promass 200, besteht die Möglichkeit einer Kalibrierung im Werk, welche sinnvoll nach dem Einbau der Referenzen in die Geräteelektronik erfolgt. Eine Kalibrierung des fertigen Sensorsystems in einer akkreditierten Werkstatt rundet die rückführbare Prüfung ab, weil sie schadhafte Einflüsse zwischen dem Einbau der Komponenten und der Fertigstellung des Geräts ausschließt; sie versieht die Einhaltung der Spezifikation noch mit einem Prüfzertifikat.

Sind spezifikationsgerechter Einbau oder Betrieb nicht gewährleistet, werden weitergehende Diagnosen notwendig

Alle bis hierhin getroffenen Aussagen beruhen auf der Annahme eines Einbaus, wie einer Nutzung des Messgeräts entsprechend der vom Hersteller spezifizierten Bedingungen. IEC 61508 erfasst grundsätzlich nur sog. zufällige Fehler am Material [1]. In der Praxis erweist sich die Einhaltung dieser Prämisse über die gewöhnlich sehr lange Nutzungsdauer von Messgeräten nicht immer als haltbar. Ist deshalb vielmehr von Prozesseinflüssen, ungünstigen Einbaubedingungen oder anderen systematischen Fehlermöglichkeiten auszugehen, ist etwa die o.g. FMEDA zu

erweitern – und das Prüfkonzept um Tests zu ergänzen, welche die Integrität mechanischer Teile zuverlässig mit abdeckt.
Moderne Coriolis-Messgeräte bieten hierfür Kombinationen an Testparametern an, die in angemessenen Perioden ausgelesen werden können, um Art und Umfang allmählicher Einflüsse auf das Schwingsystem wie Schichtaufbau, Abrasion oder Korrosion zu detektieren. Dies eröffnet die Möglichkeit, durch Trendanalysen eine verbleibende Nutzungsdauer abzuschätzen.

Literaturnachweis

[1] IEC61508/ Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer / programmierbarer elektronischer Systeme, sowie IEC 61511/ Funktionale Sicherheit- Sicherheitstechnische Systeme für die Prozessindustrie.
[2] Namur-Empfehlung 106 (NE 106), Prüfintervalle von PLT-Schutzeinrichtungen
[3] ISO / EN / DIN 9001:2008 Kapitel 7.6 a) Lenkung von Überwachungs- und Messmitteln