Die Sicherheit eingebetteter Systeme

Mikrorechnerbasierte Systeme übernehmen immer mehr Sicherheitsaufgaben in unserem Alltag. Damit diese Funktionen auch richtig ausgeführt werden, gibt es Normen zur funktionalen Sicherheit und IT-Sicherheit, die nicht nur technische Fragen beantworten. Im Start unserer Artikelreihe zur funktionalen Sicherheit wird der Sicherheitsbegriff sowie die grundsätzliche Vorgehensweise erläutert.

von Ingo Rolle

In unsere technische Umgebung halten immer mehr mikrorechnerbasierte Systeme Einzug – und sie übernehmen dabei auch Sicherheitsfunktionen: Sie wachen über den richtigen Druck im Reaktionskessel von Anlagen der chemischen Industrie, sie sorgen dafür, dass Eisenbahnzüge auf dem richtigen Gleis mit der richtigen Geschwindigkeit fahren, sie kontrollieren die Kräfte im Bremssystem in unserem Automobil, lösen bei Bedarf den Airbag aus und sie verhindern Unfälle im Umgang mit Maschinen. Wir sprechen von eingebetteten Systemen, wobei die erwähnten Sicherheitsfunktionen eine Teilmenge ihrer Aufgaben bilden.

Die Menschen möchten auf diese Helfer in ihrer Umgebung vertrauen können und erwarten hierfür eine entsprechend befähigte Technik. Funktionale Sicherheit und IT-Sicherheit sind die Werkzeuge des Automatisierungsingenieurs, um hinreichend sicher zu sein, dass die Sicherheitsfunktionen richtig ausgeführt werden und unerlaubte Handlungen nicht die Hilfe der elektronischen Systeme in eine böse Überraschung verkehren können.

Funktionale Sicherheit und IT-Sicherheit

Funktionale Sicherheit bedeutet hierbei die Fähigkeit, die festgelegten Sicherheitsfunktionen zuverlässig und spezifikationsgemäß auszuführen. Die Auslegungsgrundsätze für Systeme, die diese Fähigkeit aufweisen sollen, sind Gegenstand der siebenteiligen Reihe der Internationalen Sicherheitsgrundnormen IEC 61508; sie wurde in das deutsche Normenwerk als Reihe DIN EN 61508 (VDE 0803) übernommen, siehe auch [1] bis [7] sowie [8]. Systeme, die Sicherheitsfunktionen ausführen, werden in der Norm „sicherheitsbezogene Systeme“ genannt; üblich sind auch die

Benennungen „sicherheitsgerichtete Systeme“ oder „sichere Systeme“.

Das Ziel der Informationssicherheit ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die ein System verarbeitet, sicherzustellen – je nach Betrachtungsweise können weitere Ziele hinzutreten. Diese Informationen können zur Ausführung von Sicherheitsfunktionen dienen oder auch nicht. Ein möglicher Angreifer könnte beispielsweise versuchen, die Ausführung einer Sicherheitsfunktion zu stören und damit Gefahren herbeizuführen, oder aber er kann unbemerkt vertrauliche Informationen gewinnen, ohne dass ein Sicherheitsproblem auftritt. Aus diesem Grunde ist es nicht vorteilhaft, die IT-Sicherheit als Spezialdisziplin der funktionalen Sicherheit aufzufassen. Die Auslegungsgrundsätze für eingebettete Systeme, die Eigenschaften der IT-Sicherheit aufweisen sollen, sind indes noch nicht fest gefügt, es gibt hierzu noch keinen „Stand der Technik“. Dieser wird gerade erst im Rahmen der internationalen Normung erarbeitet. Der zweite Teil der Artikelserie wird eine Vorausschau geben und diese mit den Grundsätzen der funktionalen Sicherheit vergleichen.

Diejenigen Anwendungsgebiete, in denen eingebettete Systeme eingesetzt werden, haben bereits ihre eigene Vorgehensweise zum Erreichen von Sicherheit – eine Sicherheitsphilosophie, die mit den Betrachtungsweisen der funktionalen Sicherheit und der IT-Sicherheit nicht unbedingt übereinstimmt. Insbesondere die Vorgehensweise der klassischen Elektrotechnik zur Erreichung von Sicherheit ist hier zu nennen. Mindestens Verständnisprobleme sind daher oft die Folge.

Erläutert beispielsweise der Ingenieur der funktionalen Sicherheit die Beherrschung der zufälligen Bauteilausfälle und die Vermeidung von systematischen Fehlern in der von ihm vorgeschlagenen sicherheitsgerichteten Steuerung, fragt sich sein Kollege aus der Starkstromtechnik, wo denn hier die Sicherheit unter normalen Bedingungen und denen des ersten Fehlers bleibt. Während des Vortrages über grundlegende Anforderungen der IT-Sicherheit des hierfür zuständigen Fachmanns legt sich die Stirn des für die Anlagensicherheit Verantwortlichen fragend in Falten, weil er im Geiste vergeblich versucht, diese als Ergebnis einer Risikoanalyse, die er gewohnt ist, herzuleiten.

Diese Verständigungsschwierigkeiten behindern in der Praxis die angemessene Behandlung von funktionaler und IT-Sicherheit in neuen Anwendungsgebieten und damit letztlich den Einsatz eingebetteter Systeme in diesen. Daher ist es hilfreich, die gemeinsamen Grundlagen sowie die Grundsätze der benachbarten Disziplinen zur Sicherheit zu erläutern, was im folgenden geschehen soll.

Sicherheitsbegriff und grundsätzliche Vorgehensweise

Der ISO/IEC Guide 51 dient den Komitees der beiden internationalen Normungsorganisationen ISO (International Standardisation Organisation) und IEC (International Electrotechnical Commission) als Anleitung zum Erstellen von Sicherheitsnormen. In Deutschland wurde er als DIN V 820-120 übernommen [9]. Er definiert u.a. den Begriff Sicherheit (Safety) als „Freiheit von unvertretbarem Risiko“. Das Adjektiv „unvertretbar“ weist darauf hin, dass nicht die Freiheit von sämtlichen Risiken, also „absolute“ Sicherheit, das Ziel technischer Auslegungen ist, denn die wäre nicht erreichbar. Welche Risiken vertretbar sind, hängt u.a. von gesellschaftlichen Wertvorstellungen ab und muss im Rahmen der Risikobewertung geklärt werden, die nach Guide 51 ein Teilschritt im Prozess der Risikobeurteilung ist.

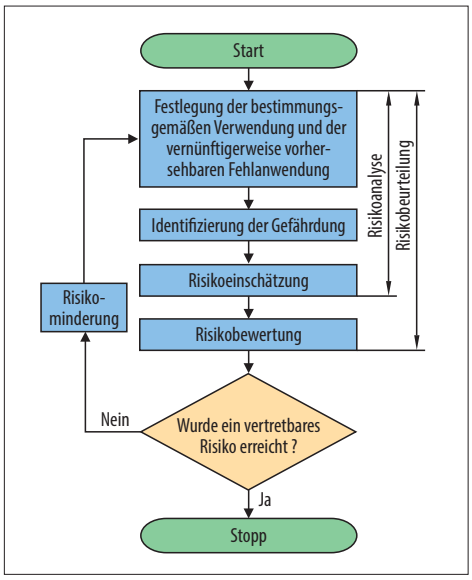


Bild 1. Flussdiagramm zur Risikoreduzierung nach ISO/IEC Guide 51.

Die Vorgehensweise zum Erreichen von Sicherheit in diesem Leitfaden stellt sich wie in **Bild 1** dar. Die im linken Ast dargestellte Risikoreduzierung hat zu erfolgen durch:

- Sichere Konstruktion,
- Schutzeinrichtung oder
- Informationen zur Sicherheit, z.B. Hinweise in der Bedienungsanleitung,

mit Vorrang für die jeweils erstgenannte Maßnahme, so wie es auch in verschiedenen gesetzlichen Vorschriften vorgeschrieben ist.

In den einzelnen Branchen wird die Vorgehensweise nach Guide 51 unterschiedlich umgesetzt. Das liegt an den unterschiedlichen Ausfallmodellen und Modellen von Gegenmaßnahmen. In jeder Branche, die sich mit Sicherheit beschäftigt, existiert mehr oder weniger ausgeprägt ein Modell

- vom Ablauf eines Schadensereignisses (Schadensmodell, Modell 1),
- davon, wie das damit verbundene Risiko zu reduzieren ist (Modell 2),
- vom Versagen dieser Risikoreduzierung (Ausfallmodell, Modell 3) und
- davon, welche Maßnahmen hiergegen zu treffen sind (Modell 4).

Man denkt sozusagen gleich in eine bestimmte Richtung: Der Ingenieur, der Tragwerke oder drucktragende Teile auslegt, befürchtet, dass diese den wirkenden Kräften einmal nicht Stand halten könnten. Dies ist sein Modell vom Ablauf eines Schadensereignisses (Modell 1). Er versucht dem mit Sicherheitszuschlägen bei seinen Auslegungen zu begegnen, was als sicherere Konstruktion zu klassifizieren ist (Modell 2). Schutzeinrichtungen oder Informationen zur Sicherheit übergeht er, denn sind Risse in der Decke über uns sichtbar, ist es nutzlos, einen Schutzhelm zu suchen oder eine Anleitung zu lesen.

Ebenso gibt es Modelle, wie diese Risikoreduzierung – also eine Konstruktion trotz Sicherheitszuschlägen – versagen könnte, z.B. infolge von Korrosion (Modell 3). Ebenso gibt es Vorstellungen, wie dem entgegengewirkt werden

kann, etwa durch Beschichtungen (Modell 4).

Die Modelle der klassischen Elektrotechnik

Der Guide 104 der IEC dient den Komitees dieser Organisation als Leitfaden zur Erstellung von Sicherheitsnormen [10]. Er enthält in seinem Anhang A eine Aufzählung möglicher Gefährdungen, z.B. elektrischer Schlag, Brand, Explosion oder Gefährdungen mechanischer Natur wie scharfe Kanten oder Instabilität. Diese Aufzählung bildet eine Checkliste, die die Normungskomitees für ihr zu normendes Produkt oder die zu normende Produktfamilie teilweise übernehmen. In der Produktnorm werden diese Gefährdungen einzeln abgehandelt; man spricht auch von gefährdungsbasierten Normen (hazard based standard). Hierzu gehören z.B. die DIN EN 60950-1 (VDE 0805-1) [11] und die DIN EN 62368 (VDE 0868-1) [12] für Geräte der IT und der Heimelektronik, sowie die DIN EN 61010-1 (VDE 0411-1) [13] für Prüf-, Mess- und Automatisierungstechnik. Eingebettete Systeme fallen teilweise auch unter diese Normen, allerdings beschäftigen diese sich überwiegend nicht mit den programmgesteuerten Funktionen dieser Systeme. Der Geltungsbereich dieser Normen sowie derjenigen zur Installations- und Niederspannungstechnik sei im Folgenden als „klassische Elektrotechnik" bezeichnet.

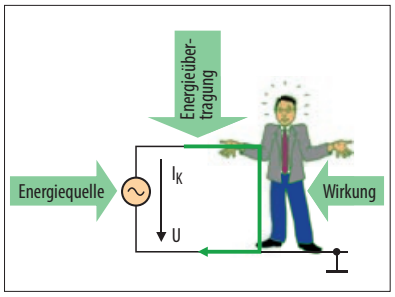


Bild 2. Modell vom Ablauf eines Schadensereignisses nach DIN EN 62368-1 (VDE 0868-1).

Mit der oben genannten Aufzählung ist das Schadensmodell der klassischen Elektrotechnik grob umrissen (Modell 1). Vielfach wird es jedoch als sogenanntes 3-Block-Modell weiter ausgeführt. Es geht von der Vorstellung aus, dass der Eintritt eines Schadens mit einem Energiefluss verbunden ist. In der DIN EN 62368-1 (VDE 0868-1) ist dieses Modell grafisch beschrieben; die Grafik wird hier sinngemäß in **Bild 2** wiedergegeben.

Ein gutes Beispiel hierfür ist ein elektrisches Gerät mit Metallgehäuse, das am Netz angeschlossen ist. Das Netz sei die Energiequelle und damit der erste Block. Nehmen wir an, die Isolation des Gerätes ist schadhaft geworden, so dass Netzspannung am Gehäuse anliegt, was den zweiten Block zur Energieübertragung bildet. Eine Person berührt dieses, in der Person findet die Wirkung statt und stellt somit den dritten Block dar. Das Unheil pflanzt sich sozusagen anhand einer Wirkungskette fort. Als Gegenmaßnahme sieht das Modell der klassischen Elektrotechnik vor, diese Wirkungskette mit Hilfe von Schutzmaßnahmen zu unterbrechen (Modell 2). Der Guide 104 beschreibt folgende:

- ➜ Schutz unter normalen Bedingungen, d.h. in diesem Beispiel, Konstrukteur und Hersteller haben für eine zuverlässige Isolation zu sorgen.
- ➜ Schutz unter den Bedingungen eines Einzelfehlers. Auch wenn der Isolationsfehler aufgetreten ist, darf keine Spannung am Gehäuse anliegen.

Um die zweite Bedingung zu erfüllen, kommt als Schutzmaßnahme der Anschluss des Metallgehäuses an den Schutzleiter in Frage, so dass bei Auftreten des Isolationsfehlers das Überstromschutzorgan („Sicherung") die Spannung automatisch abschaltet (ein Gerät nach Schutzklasse 1). Als alternative Schutzmaßnahmen bieten die meisten Normen verstärkte oder doppelte Isolation an (Gerät nach Schutzklasse 2) sowie den Betrieb des Gerätes mit ungefährlicher Kleinspannung (SELV, PELV, Gerät nach Schutzklasse 3). Das Erkennen der zusätzlichen Schutzmaßnahme in der verstärkten Isolierung setzt ein gewisses Abstraktionsvermögen voraus, so dass es für den Normenanwender eigentlich verständlicher wäre, diese Maßnahme als sichere Konstruktion zu klassifizieren. Ähnliches gilt für die Geräte mit Kleinspannung. Jedoch sieht die klassische Elektrotechnik als Modell der Risikoreduzierung ausschließlich Schutzmaßnahmen, und die im Guide 104 festgelegte Terminologie bestätigt dies.

Die Schutzmaßnahmen können aus den verschiedensten Gründen ausfallen. Über diese Gründe wird keine allgemeine Vorstellung in den Normen geäußert. Sie werden sozusagen vom gefahrbringenden Ereignis überlaufen (Ausfallmodell, Modell 3).

Um sich wiederum gegen den Ausfall der Schutzmaßnahmen zu schützen, werden in der Regel zwei Schutzmaßnahmen vorgesehen (Modell 4). Nach Guide 104 wird hierfür die Terminologie „Schutz unter normalen Bedingungen und Schutz unter den Bedingungen eines Einzelfehlers" verwendet. Gelegentlich liest man auch „Basisschutz und zusätzlicher Schutz" oder „Beherrschung des ersten Fehlers". Wurden diese Schutzmaßnahmen richtig eingesetzt und sind sie zudem hinreichend voneinander unabhängig, so fallen sie auch unabhängig voneinander aus. Die Wahrscheinlichkeit hierfür ist gering. Somit wird erfahrungsgemäß durch zwei voneinander unabhängige Schutzmaßnahmen die notwendige Risikoreduzierung erreicht.

Grenzen der Vorgehensweise der klassischen Elektrotechnik

Wie die folgenden Beispiele zeigen, kann die oben genannte Vorgehensweise in bestimmten Fällen unzureichend sein:

1. Kommen nicht ausreichend zuverlässige Schutzmaßnahmen zur Anwendung, wird das System auch unter den Bedingungen eines Einzelfehlers möglicherweise nicht mehr beherrscht. Diese Möglichkeit ist speziell dann zu betrachten, wenn die Schutzmaßnahmen auf elektronischen Mitteln beruhen, typischerweise mit einem eingebetteten Mikrorechnersystem. Ihr Ausfallverhalten ist, im Gegensatz z.B. zu einem Relais, nicht mehr einfach vorhersagbar. Hier bieten sich die Ausfallmodelle nach DIN EN 61508 (VDE 0803) an sowie deren Modelle zur Vermeidung und Beherrschung solcher Ausfälle, siehe hierzu Kapitel 4.

2. Der Entwurf des Systems sieht zwei gestaffelte, scheinbar unabhängige Schutzmaßnahmen vor, jedoch wird eine versteckte Abhängigkeit zwischen diesen übersehen. Eine solche liegt vor, wenn ein Ereignisablauf beide Schutzmaßnahmen überwinden kann. Um ein allseits bekanntes Beispiel zu verwenden: Ein Erdbeben zerstört zunächst einen Kernreaktor und macht dessen Regelsystem betriebsunfähig. Das Schutzsystem zur Reaktornotkühlung tritt daraufhin spezifikationsgemäß in

Tätigkeit, um diese Fehlerbedingungen zu beherrschen. Das gleiche Erdbeben löst jedoch auch einen Tsunami aus, der die Dieselaggregate der Reaktornotkühlung einige Minuten später zerstört und damit auch diese Schutzmaßnahme ausfallen lässt. Ein ähnlicher Fall liegt vor, wenn in einem Niederspannungsnetz vom Typ TN-C der PEN-Leiter durchtrennt wird. An den ordnungsgemäß an den Schutzleiter angeschlossenen Metallgehäusen liegt jetzt eine wahrscheinlich gefährliche Spannung an und keine der Schutzmaßnahmen gegen elektrischen Schlag ist wirksam.

Bereits während der Analysephase in der Systemauslegung sollte versucht werden, solche Ereignisabläufe zu untersuchen, mögliche Abhängigkeiten zu erkennen und zu bewerten. Im Falle des PEN-Leiters hat dies dazu geführt, dass das zuständige Normungskomitee konstruktive Eigenschaften des PEN-Leiters vorgeschrieben hat, mit dem Ziel, die Wahrscheinlichkeit des Auftretens dieses Falls und damit sein Risiko hinreichend zu verringern.

3. Bei Schutzmaßnahmen in der Betriebsart mit niedriger Anforderungsrate (nach DIN EN 61508 (VDE 0803) weniger als eine Anforderung pro Jahr) können redundante Teilsysteme zwischen den wiederkehrenden Prüfungen unerkannt ausfallen, so dass sie im Anforderungsfall nicht zur Verfügung stehen, obwohl sie voneinander unabhängig sind. In der oben genannten Terminologie heißt das: „Es kommt zu einer Häufung von ersten Fehlern". Nachdem sich auf der Förderplattform Deepwater Horizon am 20. April 2010 im Golf von Mexiko eine Explosion ereignet hatte, ging die Verbindung zum Anlagenteil in rund 1.500 m Tiefe auf dem Meeresgrund verloren. Um einen unkontrollierten Austritt von Gas und Rohöl auf dem Meeresgrund zu verhindern, hätte der sogenannte Blow-out Preventer als selbsttätig wirkendes Schutzsystem in diesem Anlagenteil die Förderleitung mit Hilfe eines hydraulischen Mechanismus verschließen (blind shear ram) sollen. Das System, um diesen auszulösen, war doppelkanalig ausgelegt. In einem Kanal versagte ein Magnetventil, im anderen Kanal waren die Batterien zur Versorgung der Steuerung entladen [14].

Selbstdiagnosefähigkeit der Systeme, Fehleraufdeckungsmöglichkeiten im Rahmen der wiederkehrenden Prüfungen sowie die Festlegung deren Intervalle bedürfen daher bei Systemen in der Betriebsart mit niedriger Anforderungsrate einer eingehenden Betrachtung.

Verschiedene Bereiche, verschiedene Sicherheitsphilosophien

Die Artikelserie zur funktionalen Sicherheit in eingebetteten Systemen soll eine Hilfestellung zur Verringerung von Schwierigkeiten zwischen den einzelnen Fachgebieten sein und gemeinsame Grundlagen zum Erreichen von Sicherheit vorstellen, die unterschiedlichen Vorgehensweisen in einigen Gebieten vergleichen und auf die Anwendungsgrenzen aufmerksam machen, denn die allein gültige Sicherheitsphilosophie gibt es nicht. Im zweiten Teil der Artikelserie werden die Modelle von funktionaler und IT-Sicherheit vorgestellt. Der Artikel erscheint in einer der nächsten Ausgaben. *ag*

Literatur

[1] DIN EN 61508-1 (VDE 0803-1):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Allgemeine Anforderungen (IEC 61508-1:2010). Deutsche Fassung EN 61508-1:2010.

[2] DIN EN 61508-2 (VDE 0803-2):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010). Deutsche Fassung EN 61508-2:2010.

[3] DIN EN 61508-3 (VDE 0803-3):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010). Deutsche Fassung EN 61508-3:2010.

[4] DIN EN 61508-4 (VDE 0803-4):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010). Deutsche Fassung EN 61508-4:2010.

[5] DIN EN 61508-5 (VDE 0803-5):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln (IEC 61508-5:2010). Deutsche Fassung EN 61508-5:2010.

[6] DIN EN 61508-6 (VDE 0803-6):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010). Deutsche Fassung EN 61508-6:2010.

[7] DIN EN 61508-7 (VDE 0803-7):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010.

[8] *DKE:* Muss bei der funktionalen Sicherheit auch die IT-Sicherheit beachtet werden? http://www.dke.de/de/DKE-Arbeit/MitteilungenzurNormungsarbeit/2011/Seiten/Erreichung-derfunktionalenSicherheit.aspx

[9] DIN V 820-120:1994-10, Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen.

[10] IEC Guide 104:2010-08, The preparation of safety publications and the use of basic safety publications and group safety publications.

[11] DIN EN 60950-1 (VDE 0805-1):2011-01, Einrichtungen der Informationstechnik – Sicherheit – Teil 1: Allgemeine Anforderungen (IEC 60950-1:2005, modifiziert + Cor.:2006 + A1:2009, modifiziert). Deutsche Fassung EN 60950-1:2006 + A11:2009 + A1:2010.

[12] E DIN EN 62368-1 (VDE 0868-1):2012-02, Einrichtungen für Audio/Video, Informations- und Kommunikationstechnik – Teil 1: Sicherheitsanforderungen (IEC 108/455/CD:2011).

[13] DIN EN 61010-1 (VDE 0411-1):2011-07, Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte – Teil 1: Allgemeine Anforderungen (IEC 61010-1:2010). Deutsche Fassung EN 61010-1:2010.

[14] BP-Bericht über das Deepwater-Horizon-Unglück: http://www.bp.com/sectiongenericarticle.do?categoryId=9040069&contentId=7067574

Ingo Rolle

war zunächst in verschiedenen Industriestellungen tätig, bevor er 1993 zur DKE (Deutsche Kommission Elektrotechnik, Elektronik, Informationstechnik im DIN und VDE) kam. Er betreut dort Normenausschüsse, die in der industriellen Automatisierung tätig sind. Hierzu gehört auch das GK 914, das für die IEC 61508 zuständig ist, und das UK 931.1 für die IT-Sicherheit.

Ingo.Rolle@VDE.com

Modelle der funktionalen Sicherheit

Im zweiten Teil unserer Artikelserie zum Thema funktionale Sicherheit werden die einzelnen Modelle der funktionalen Sicherheit beschrieben. Dabei wird auf die Grenzen der Ausfallmodelle der DIN EN 61508 ebenso eingegangen wie auf das Einbinden der Risikoanalyse in die Norm.

von Ingo Rolle

Die Definition der funktionalen Sicherheit lautet nach DIN EN 61508-4 (VDE 0803-4):2011, 3.1.12 [1] : „Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen E/E/PE-Systems und anderer risikomindernder Maßnahmen abhängt."

EUC bedeutet „Equipment under Control", also beispielsweise ein Rührkesselreaktor in einer chemischen Fabrik, und das EUC-Leit- oder Steuerungssystem ist die zugehörige Instrumentierung mit Automatisierungssystem. E/E/PE steht für „elektrisch, elektronisch und programmierbar elektronisch" und bezeichnet die eingesetzte Technologie; die ist heute üblicherweise programmierbar elektronisch, also die Verwendung eines mikrorechnerbasierten, eingebetteten Systems zur Ausführung der Sicherheitsfunktion. An der Abfassung der IEC 61508 haben sich viele Fachleute aus der chemischen Industrie beteiligt und die Wortwahl entsprechend beeinflusst. In anderen Anwendungsgebieten wäre das Equipment under Control beispielsweise der Antrieb eines Eisenbahntriebwagens, eine Einrichtung zur Weichenstellung oder eine Stanzmaschine. Der Begriff „korrekte Funktion" weist auf die spezifikationsgemäße Ausführung der Sicherheitsfunktion hin.

Der Trennung von „EUC-Leit- oder Steuerungssystem" und „sicherheitsbezogenes E/E/PE-System" liegt die Vorstellung eines „normalen" Automatisierungssystems zugrunde, das von einem sicherheitsbezogenen Schutzsystem überwacht wird, welches zur Abwendung von Gefahren eingreift. Das mag sich bei der Drucküberwachung eines Rührkesselreaktors anbieten, bei einer Stanzmaschine aber nicht unbedingt:

Bis ein übergeordnetes System hier erkannt hätte, dass sich die Hand des Bedieners unter dem niedergehenden Stempel befindet, und eingegriffen hätte, wäre letztere bereits gequetscht. Hier werden die Sicherheitsfunktionen – z.B.: „erkennt das Lichtgitter einen Gegenstand unter dem niedergehenden Stempel, hat der Antrieb der Stanze sofort zu stoppen" – deshalb bereits in die Antriebssteuerung eingebaut, die beiden oben genannten Systeme fallen zusammen.

Die Modelle im Überblick

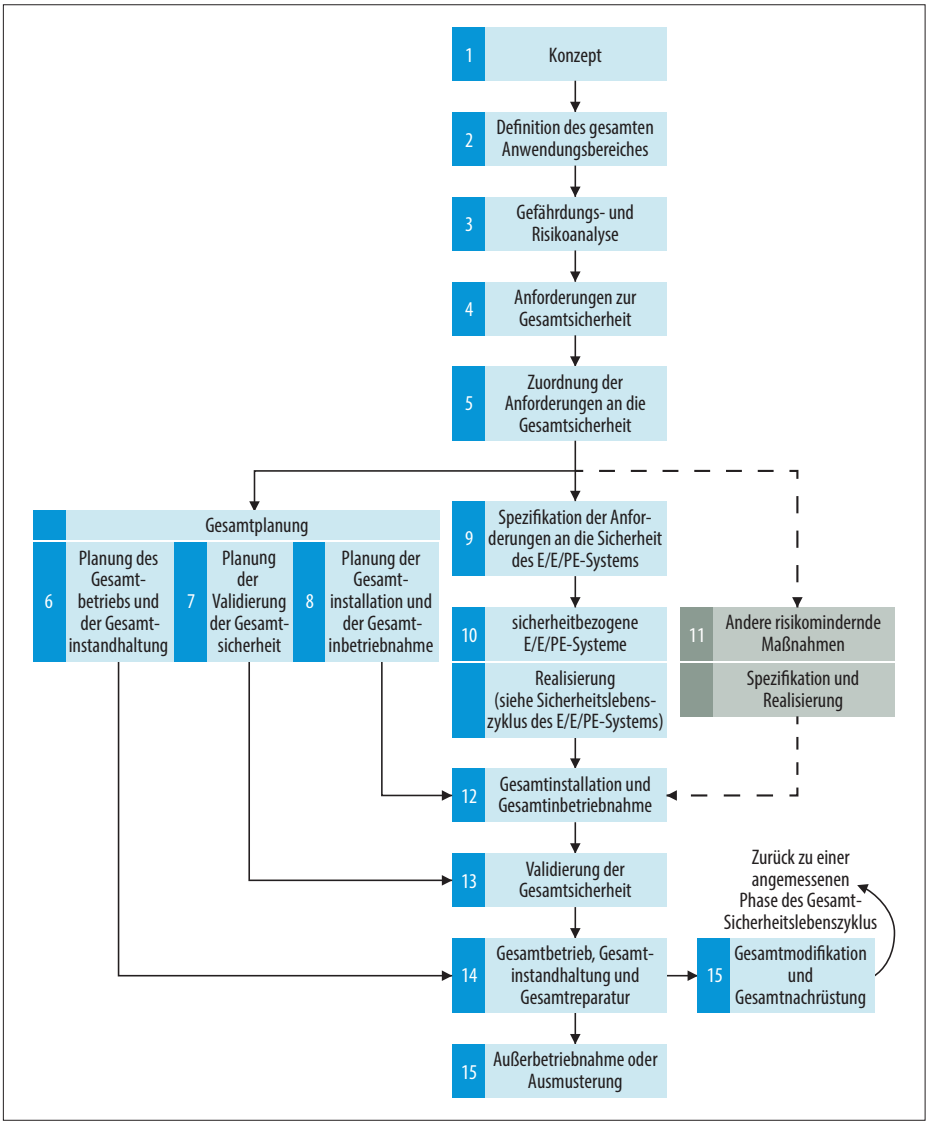
Über den Ablauf eines Schadensereignisses wird in denjenigen Normen zur funktionalen Sicherheit, die allgemeineren Charakter haben, z.B. in der Sicherheitsgrundnorm DIN EN 61508, keine allgemeine Vorstellung geäußert (Modell 1; [2]). Stattdessen wird angenommen, dass eine Risikoanalyse die notwendigen Sicherheitsfunktionen zur Reduzierung des Risikos festlegt. Um diese zu erfüllen, sind, abhängig von der Zuordnung einer Sicherheitsfunktion auf die sicherheitsbezogenen Systeme, möglicherweise elektronische Steuerungen notwendig. Das ist die Vorstellung von der Risikoreduzierung (Modell 2; [2]). In Normen zur funktionalen Sicherheit allerdings, die sich stärker an der Anwendung orientieren – also fachspezifischen Umsetzungen, Produktfamilien- oder -normen –, werden die Schadensquellen und risikomindernden Maßnahmen mehr oder weniger beschrieben, d. h., die Modelle 1 und 2 näher ausgeführt.

Vom Versagen der risikoreduzierenden Maßnahmen (dazu gehört das E/E/PES-sicherheitsbezogene System) wird in der DIN EN 61508 eine klare Vorstellung entwickelt (Modell 3; [2]). Folgende Ausfallmodelle sind angegeben:

- Zufällige Ausfälle von Bauteilen. Zufall bedeutet hier, dass wir mit den uns zur Verfügung stehenden Mitteln keine Ursache und keinen Zusammenhang zwischen den Ausfällen erkennen können.
- Systematische Ausfälle. Das sind Ausfälle, die auf eine bestimmte Ursache zurückgeführt werden können und meistens durch die Begrenztheit des menschlichen Geistes entstehen. Diejenigen, die ein System entwerfen, machen Fehler. Diejenigen, die eine Risikoanalyse anfertigen, schätzen Gefahren falsch ein und/oder übersehen Abhängigkeiten. Diejenigen, die die Sicherheitsspezifikation schreiben, geben Sicherheitsfunktionen unzureichend an, und diejenigen, die die Instandhaltung planen oder ausführen, unterschätzen Fehlerquellen oder die Möglichkeiten zur technischen Umsetzung der Maßnahmen in der betrieblichen Umgebung. Eine weitere Art systematischer Ausfälle kann dadurch entstehen, dass das System außerhalb seiner Spezifikation betrieben wird, z.B. bei zu hoher Umgebungstemperatur oder die Bediener suchen nach Manipulationsmöglichkeiten, „tricksen" das System sozusagen aus.

Ebenfalls besitzt die Disziplin der funktionalen Sicherheit eine klare Vorstellung davon, welche Maßnahmen gegen diese Arten von Ausfällen zu treffen sind (Modell 4; [2]):

- Die Maßnahmen gegen zufällige Ausfälle von Bauteilen sehen vor, die Anzahl der Ausfälle zu begrenzen, da man Zufälle nicht gänzlich verhindern kann. Dabei wird von jeder Art von Bauteil (Transistor, Widerstand, IC, Relais usw.) das Ausfallverhalten



Der Sicherheitslebenszyklus nach DIN EN 61508-1 (VDE 0803-1):2011.

beobachtet, d.h., es wird erfasst, wie oft und in welcher Art es ausfällt, z.B. Kurzschluss oder Unterbrechung. Die Ergebnisse dieser in der Regel langjährigen Beobachtungen werden in Form einer Statistik zusammengefasst. Einige dieser Statistiken sind öffentlich zugänglich, z.B. IEC/TR 62380 [3] oder die Siemens-Werksnorm SN 29500, andere werden unternehmensintern geführt. Auf der Grundlage dieser Statistiken und mit Hilfe von Rechenverfahren, die in der DIN EN 61508-2 und anderen Normen zur funktionalen Sicherheit beschrieben sind, wird das zukünftige Verhalten in Bezug auf zufällige Ausfälle vorhergesagt. Das System muss nun so ausgelegt werden, dass diese Vorhersage unter einer vorgegebenen Grenze liegt.

- Die systematischen Ausfälle sollen durch ein Managementsystem vermieden werden, genannt „Safety Lifecycle" oder „Sicherheitslebenszyklus" (**Bild**).

Die funktionale Sicherheit geht davon aus, dass es schwierig ist, das Verhalten des Systems durch eine Prüfung vollständig aufzudecken – im Gegensatz zu den oben genannten klassischen Sicherheitsnormen, die in der Regel die vollständige Prüfbarkeit annehmen. Durch ein Managementsystem soll erreicht werden, dass Fehler nicht erst aus dem fertigen System heraus geprüft werden müssen oder dort verbleiben, sondern gar nicht erst hineinkommen. Ferner werden bestimmte Techniken zur Vermeidung systematischer Fehler vorgeschrieben, z.B. umfangreiche Prüfungen oder das Verbot bestimmter Programmierarten. All diese Techniken sind in der DIN EN 61508-7 [4] zusammenfassend dargestellt. Es ist also nicht ausreichend, alleine das Arbeiten nach einem Qualitätssicherungssystem nachzuweisen.

Insbesondere die Vorschriften, welche sich auf die Entwicklung beziehen, machen es für einen Hersteller schwierig, laufende Altprodukte nachträglich für die Verwendung in Sicherheitsfunktionen zu qualifizieren:

- Falls während des Einsatzes des Systems trotz dieser Maßnahmen dennoch zufällige oder systematische Ausfälle auftreten, muss das System hiergegen eine gewisse Toleranz aufweisen, für die ebenfalls bestimmte Techniken vorgeschrieben sind. Dies muss auch für die Software nachgewiesen werden [5].
- Auch die Architekturanforderungen seien hier genannt. Die DIN EN 61508-2 [4] schreibt, in Abhängigkeit von den Anforderungen, eine gewisse Mehrkanaligkeit vor, so dass allein das Vorrechnen von Wahrscheinlichkeiten nicht unbedingt ausreichend ist. An dieser Stelle wirkt also die aus der klassischen Elektrotechnik bekannte Vorgehensweise der gestaffelten Schutzmaßnahmen (Beherrschung des n-ten Fehlers) nach.

Grenzen der Modelle

Es stellt sich die Frage: Sind die der DIN EN 61508 zugrundeliegenden Modelle 3 und 4, also das Ausfallmodell der risikomindernden Maßnahmen und das Modell der hiergegen zu ergreifenden Maßnahmen, so allgemeiner Natur, dass alle anderen Vorgehensweisen als Untermenge aufgefasst werden können?

Zunächst ist zu bemerken, dass die Anwendung dieser Modelle für „einfache Systeme", d.h. für Systeme, deren Ausfallverhalten eindeutig vorhergesagt werden kann, schlicht übertriebenen Aufwand bedeutet. Für den richtigen Anschluss des Schutzleiters an ein Metallgehäuse oder für die Auslegung von Ohrenschützern ist zum Erreichen des Sicherheitszieles weder ein probabilistischer Ansatz noch ein Qualitätsmanagementsystem erforderlich.

Die Anwendung des Ausfallmodells mit zufälligen Ausfällen und seine Fortführung zu einer Vorhersage mit Wahrscheinlichkeiten stößt bei bestimmten Bauteilen auf Schwierigkeiten. Zum einen werden einige Bauteile in so geringen Serien gefertigt, dass eine statistische Beobachtung unmöglich ist; zum anderen gibt es Bauteile, die in der Praxis fast nur systematisch ausfallen. Ein Beispiel hierfür sind Stellventile in Anlagen der chemischen Industrie. Für die dort verwendeten speziellen Medien werden sie oft einzeln angefertigt. Ein wichtiges Bauteil in vielen dieser Ventile ist die mechanische Rückstellfeder: Sie fällt meist aufgrund systematischer Einflüsse aus, z.B. aggressive Umgebung, im Winter festgefroren oder ähnliches. Es ist nicht zulässig, solche Ausfälle in eine allgemeine Statistik einfließen zu lassen, denn sie berücksichtigt nicht die Bedingungen, unter denen sie sich wiederholen. An dieser Stelle ist zu erwähnen, dass die meisten deutschen Experten die richtige Systemauslegung für wichtiger halten als statistische Nachweise.

Es wird deutlich, dass eine nutzbringende Anwendung der Vorgehensweise der funktionalen Sicherheit wie in der DIN EN 61508 die oben genannten Ausfallmodelle voraussetzt.

Einbinden der Risikoanalyse in die Norm

Der klassische Ansatz zur Erstellung einer Sicherheitsnorm ist der, dass das erstellende Normungskomitee mit den in ihm vertretenen Fachleuten eine Risikoanalyse anfertigt und das Ergebnis in der Norm mitteilt, nämlich in Form der darin niedergelegten Sicherheitsanforderungen. Der Hersteller, der ein Produkt nach der Norm herstellen möchte, prüft, ob dieses im Anwendungsbereich der Norm liegt und dass die bei der Erstellung der Norm getroffenen Voraussetzungen auch für sein Produkt gelten. Sodann beachtet er bei dessen Auslegung die Sicherheitsanforderungen der Norm.

Die DIN EN 61508-1 schreibt als Sicherheitsgrundnorm, die sich an alle Fachgebiete richtet, hingegen nur vor, dass der Hersteller eine Risikoanalyse anzufertigen, ihr Ergebnis zu dokumentieren und für die Systemauslegung zu verwenden hat. Dieses ist Bestandteil des Sicherheitslebenszyklus. Die DIN EN 61508-5 nennt informativ einige Beispiele für Risikoanalysen.

Normungskomitees, die anwendungsbezogene Normen zur funktionalen Sicherheit erarbeiten, werden, je nachdem wie stark das Produkt im Rahmen der angestrebten Vereinheitlichung spezifiziert werden kann, einen Ansatz zwischen diesen beiden Extrempunkten wählen. Beispielsweise können für die Risikoanalyse bestimmte Randbedingungen vorgeschrieben werden, so dass die Risikoanalysen der Hersteller vergleichbar werden, was dem einzelnen Hersteller mehr Rechtssicherheit gibt und ihn in die Lage versetzt, seine Risikoanalyse mit seinen Zulieferern zu koordinieren. Die ISO 26262 für funktionale Sicherheit für Kraftfahrzeuge ist hierfür ein Beispiel [6].

Gestufte Anforderungen

Die im Lebenszyklus der DIN EN 61508-1 vorgeschriebene Risikoanalyse stellt die zu erreichende Risikoreduzierung fest. Dazu werden bei den meisten Verfahren zur Risikoanalyse die Parameter Schwere und Wahrscheinlichkeit des zu erwartenden Schadens verwendet; vielfach kommen noch weitere hinzu, die beispielsweise ausdrücken, ob man sich einem auftretenden Schadensereignis noch entziehen oder dieses abwenden kann. Die zu erreichende Risikoreduzierung wird mit Hilfe von vier möglichen Stufen ausgedrückt, den sogenannten Safety Integrity Levels, kurz SIL. SIL 1 ist die geringste Risikoreduzierung, SIL 4 die höchste. Diese gestuften Anforderungen werden auf die Unterpunkte des Modells 4 der funktionalen Sicherheit, Maßnahmen gegen das Versagen der Risikoreduzierung, angewendet:

- *SIL-abhängige Anforderung zur Beherrschung zufälliger Bauteilausfälle:* Die Sicherheitheits-Integrität wird als Wahrscheinlichkeit aufgefasst, mit der die Sicherheitsfunktion ausgeführt wird . Den Zusammenhang zwischen dem in der Risikoanalyse ermittelten SIL und den erforderlichen Wahrscheinlichkeitswerten stellen die Tabellen 2 und 3 der DIN EN 61508-1:2011 her. Der Hersteller eines Systems muss nun mit Hilfe der oben erwähnten Datenbanken und Berechnungsverfahren nachweisen, dass dieses die geforderten Wahrscheinlichkeitswerte voraussichtlich erbringen wird.
- *SIL-abhängige Anforderungen zur Vermeidung systematischer Ausfälle:* Die für den Entwurf und die Ausführung des Gesamtsystems zuständige DIN EN 61508-2 und die für die Software zuständige DIN EN 61508-3 fordern die einzusetzenden Techniken in Abhängigkeit von den zu erreichenden SILs. Diese sind in mehreren Tabellen festgelegt. Das gleiche gilt für die Techniken, mit denen Fehlertoleranz erreicht wird.
- *SIL-abhängige Architekturanforderungen:* In diese geht, ebenfalls SIL-abhängig, der erforderliche Redundanzgrad (1, 2 oder 3 parallele Kanäle) ein. Der Hersteller von Systemen, die solche Anforderungen erfüllen, muss in der Lage sein, Diagnosemechanismen einzurichten, die Fehler in den Kanälen erkennen und die Aufdeckungswahrscheinlichkeit einschätzen können. Sodann muss ein Systemverhalten bei Erkennung eines Fehlers verwirklicht werden („Degradations-Strategie").

Die Stufung von Anforderungen als Ergebnis einer individuellen Risikoanalyse sucht man in den klassischen Sicherheitsnormen der Elektrotechnik, so wie sie im ersten Teil der Artikelserie genannt sind, meist vergeblich. Ein Schutzleiteranschluss wird stets in der gleichen, in der Norm vorgeschriebenen Qualität ausgeführt – gleichgültig, ob damit zu rechnen ist, dass das Metallgehäuse eines Gerätes oft von Laien berührt wird oder nur gelegentlich durch Reinigungspersonal. Eine derartige Stufung von Anforderungen ist schlicht nicht üblich und würde wohl auch nicht zu nennenswerten Unterscheidungen und wirtschaftlichen Vorteilen führen.

Die IT-Sicherheit kommt bestimmt

Während die Pioniere des Internet sich noch darauf verließen, dass die Gemeinde ihrer Netzteilnehmer aus ehrbaren Wissenschaftkollegen bestehen würde, wogen sich die ersten Entwickler, die ihre Steuerungen IP-adressierbar machten, mit der Hoffnung in Sicherheit, dass Zeitgenossen mit fragwürdigen Absichten diese ausschließlich in die Banken- und Bürowelt richten würden. Nicht nur davon mussten wir inzwischen Abschied nehmen; wir mussten auch lernen, dass Steuerungen, die überhaupt nicht an das Internet angeschlossen sind, über das Entwicklungssystem angegriffen werden können.

Ob es uns gefällt oder nicht: Der Bedarf nach einer neuen Sicherheitsdisziplin, der IT-Sicherheit in der Automatisierungstechnik, wurde überall artikuliert. Eine normierte Betrachtungsweise hierfür nimmt inzwischen Gestalt an und im dritten Teil wird dargelegt werden, wie sich diese neue Disziplin in das bis jetzt dargestellte Vergleichsmuster einfügt. *ag*

Literatur

[1] DIN EN 61508-4 (VDE 0803-4): 2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010). Deutsche Fassung EN 61508-4:2010.

[2] *Rolle, I.:* Die Sicherheit eingebetteter Systeme. Artikelserie zur Funktionalen Sicherheit – Teil 1. Elektronik 03/2013; Seite 41ff.

[3] IEC/TR 62380:2004-08, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment.

[4] DIN EN 61508-7 (VDE 0803-7): 2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010.

[5] DIN EN 61508-3 (VDE 0803-3): 2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010). Deutsche Fassung EN 61508-3:2010.

[6] ISO 26262 (Reihe):2011-11, Straßenfahrzeuge – Funktionale Sicherheit.

Ingo Rolle
war zunächst in verschiedenen Industriestellungen tätig, bevor er 1993 zur DKE (Deutsche Kommission Elektrotechnik, Elektronik, Informationstechnik im DIN und VDE) kam. Er betreut dort Normenausschüsse, die in der industriellen Automatisierung tätig sind. Hierzu gehört auch das GK 914, das für die IEC 61508 zuständig ist, und das UK 931.1 für die IT-Sicherheit.
Ingo.Rolle@VDE.com

Industrial Security – Stand der Normung und Risikominimierung

Der dritte Teil unserer Artikelserie zur funktionalen Sicherheit befasst sich mit Industrial Security. Der Bedarf nach einer neuen Sicherheitsdiziplin, der IT-Sicherheit in der Automatisierungstechnik, ist gegeben. Der Artikel beschreibt, wie sich diese neue Disziplin in das in Teil 1 und 2 dargestellte Vergleichsmuster einfügt.

Von Dr. Pierre Kobes und Ingo Rolle

Der Begriff IT-Sicherheit oder Informationssicherheit wird allgemein verwendet, um den Schutz von Informationen gegen Manipulation und Diebstahl zu bezeichnen. Das Ziel der Informationssicherheit ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die ein System verarbeitet, sicherzustellen. Die Reihenfolge entspricht hier auch der Priorität der Schutzziele. So ist es im Büroumfeld wichtiger, eine Information gegen unerlaubten Zugriff zu schützen, als die Information unmittelbar und jederzeit dem Anwender zur Verfügung zu stellen. Es ist nicht ungewöhnlich, dass es am PC-Arbeitsplatz einige Sekunden dauern kann, bis sich das gewünschte Bild aufgebaut hat, oder dass der PC für einige Minuten nicht zur Verfügung steht, weil eine Aktualisierung des Betriebssystems vorgenommen wird.

Die IT-Sicherheit im Umfeld der Automatisierung hat einen etwas anderen Schwerpunkt. Hier geht es um den Schutz industrieller Anlagen vor unerlaubten physischen und digitalen Zugriffen. Diese können kriminell motiviert sein oder durch fahrlässiges Verhalten bewirkt sein, z.B. könnte ein Mitarbeiter in einer Notsituation versuchen, die Festplatte des Produktionsrechners während der laufenden Produktion zu formatieren. Im Vordergrund der IT-Sicherheit in Automatisierungslösungen steht die Verfügbarkeit der Anlage. Es muss sichergestellt sein, dass die Produktion aufrechterhalten bleibt, auch wenn sie durch Falschbehandlung oder Angriff beeinträchtigt wird. Die Priorität der Schutzziele liegt in erster Linie auf der Verfügbarkeit und der Integrität der Automatisierungslösung in ihrer Kernfunktion, nämlich die Produktionsanlage zu steuern. Der Schutz von Informationen gegen Datendiebstahl steht nicht im Vordergrund. Um sich von der IT-Sicherheit im Büroumfeld zu unterscheiden, wird oft der englische Begriff „Industrial Security" für die IT-Sicherheit in Automatisierungslösungen verwendet. Es gibt im Deutschen keinen einfachen Begriff für IT-Sicherheit in Automatisierungslösungen; daher wird im Folgenden in Abgrenzung von der Office-IT der Begriff „Industrial Security" verwendet.

Stand der Normung

Die Industrial Security ist eine relativ junge Disziplin. Viele Lösungen aus der allgemeinen Office-IT können nicht ohne weiteres oder überhaupt nicht eingesetzt werden. Beispielsweise können Patches nicht auf einen Produktionsrechner in der Frequenz eingespielt werden, wie sie in der Office-IT üblich ist, da alle möglichen Nebenwirkungen vor dem Aufspielen gründlich abgeklärt werden müssen. Die Ablaufzeit der Programme spielt hier eine entscheidende Rolle. Auch Virenscanner können das System verlangsamen und in seinem Zeitverhalten nicht mehr vorhersagbar machen. Zudem sollten nicht alle Bedie-

nereingriffe die Eingabe eines Passwortes erfordern, um z.B. in Ausnahmesituationen schnell reagieren zu können.

Welche technischen Lösungen zur Erfüllung der IT-Sicherheitsanforderungen sich künftig in der Automatisierungstechnik durchsetzen werden, lässt sich zur Zeit noch nicht absehen. Angesichts dieser Ungewissheit konzentrierten sich die meisten Standardisierungsbemühungen bis jetzt auf Verhaltensnormen für den Anlagenbetreiber. So wurde in der Normreihe IEC 62443 „Industrial communication networks – network and system security" als einer der ersten Standards der Teil 2-1 „Establishing an industrial automation and control system security program" bereits 2010 als internationale Norm verabschiedet [1]. Der kürzlich überarbeitete Entwurf der Edition 2 wurde nun als Profile der in der Office-IT langjährig etablierten Normenreihe ISO/IEC 27000 [2] erstellt. Es wurde erkannt, dass es wichtig ist, die Gemeinsamkeiten und Unterschiede der Managementsysteme im Büro und in der Produktion darzustellen, und dass grundsätzlich die gleichen wesentlichen Verfahrensschritte bestehen (PDCA-Zyklus):

- Plan: Managementsystem für die Industrial Security festlegen
- Do: implementieren und betreiben
- Check: Wirksamkeit prüfen und ggf. überarbeiten
- Act: aufrechterhalten und ggf. verbessern

Die vier Schritte müssen regelmäßig immer wieder durchlaufen werden, um ein Aufrechterhalten und die Aktualität des Managementsystems sicherzustellen (**Bild 1**).

Die Ausarbeitung der Normreihe IEC 62443 hat in den letzten drei Jahren deutlich an Geschwindigkeit aufgenommen. Es wurde vereinbart, dass die meisten Dokumente in den Komitees der ISA-99 erarbeitet werden und international nach den Prozeduren der IEC abgestimmt werden. Die Struktur wurde erweitert und schließt heute alle Seiten der Industrial Security ein (**Bild 2**). Neben dem Managementsystem des Anlagenbetreibers werden auch die Prozeduren und Vorschriften des Lösungsanbieters adressiert sowie funktionale Anforderungen spezifiziert, die die Hersteller zukünftig in ihren Systemen und Geräten zu erfüllen haben. Eine Übernahme als europäische und deutsche Norm erfolgte bis jetzt nicht.

Damit zeichnet sich folgende Situation ab: Die Grundnormen über das Security Management System werden von ISO/IEC 27000 und 27001 gebildet; Sektor-spezifische Profile definieren die spezifischen Ausprägungen der Grundnormen. So ist geplant, dass der Teil 2-1 der IEC 62443 auch gleichzeitig als Profil für die Automatisierungstechnik mit einer noch zu definierenden Nummer aus der ISO/IEC-27000-Normenreihe geführt wird.

Der Stand der Ausarbeitung ist je nach den einzelnen Teilen der Normenreihe IEC 62443 unterschiedlich und in der **Tabelle** nachzulesen. Es sei darauf hingewiesen, dass wesentliche Teile auch im jetzigen Zustand für die Erstellung von Maßnahmen zum Schutz von Produktionsanlagen sehr hilfreich sind.

Im Teil 2-1 der als Norm veröffentlichten Edition 1.0 sind bereits alle für einen Anlagenbetreiber relevanten Maßnahmen beschrieben. Mit der überarbeiteten Edition 2.0 wird zusätzlich sichergestellt, dass für eine Firma die gleiche Basis – die ISO/IEC-27000-Normenreihe – für ihre Prozeduren und Vorschriften im Bürobereich und in der Produktion gilt und somit im Einklang sind. Teil 2-1 beschreibt lediglich die Besonderheiten, die für den Betrieb der Automatisierungslösungen zu berücksichtigen sind.

Der Teil 3-3 wurde im Jahr 2012 einstimmig als „Committee Draft for Vote" angenommen. Es ist zu erwarten, dass der in Kürze veröffentlichte FDIS (Final Draft International Standard) technisch unverändert angenommen wird. Damit kann sich ein Systemhersteller bei der Entwicklung der Security-Funktionen bereits heute an dem Dokument orientieren. Darin werden sogenannte Security Level (SL) spezifiziert. Diese sind an die vier möglichen Stufen der funktionalen Sicherheit, die sogenannten Safety Integrity Levels, kurz SIL, angelehnt, siehe Teil 2 dieser Artikelserie. Das Konzept des sogenannten SL Vector ermöglicht, die Security-Anforderung an ein System in ihrer Wirkung zu differenzieren.

Weitere Dokumente, die das Gesamtbild abrunden, werden in Kürze veröffentlicht:

- Teil 2-4 spezifiziert die Anforderungen an die Prozesse und Richtlinien des Lösungsanbieters (Systemintegrator oder Anlagenbauer). Das Dokument basiert auf der bereits veröffentlichten Spezifikation „Process control domain – Security requirements for vendors" V 2.0 [5], so dass zu erwarten ist, dass die Inhalte bereits heute schon relativ stabil sind.
- Teil 4-1 spezifiziert die Anforderungen an den Entwicklungsprozess von Geräten und Systemen. Das Dokument lehnt sich stark an die im zweiten dieser Artikelserie erwähnte DIN EN 61508-3 (VDE 0803-3) und an die Spezifikation „Software Development Assessment Specification" [6] des ISA Security Compliance Institute. Auch hier ist wegen der umfangreichen Vorarbeiten zu

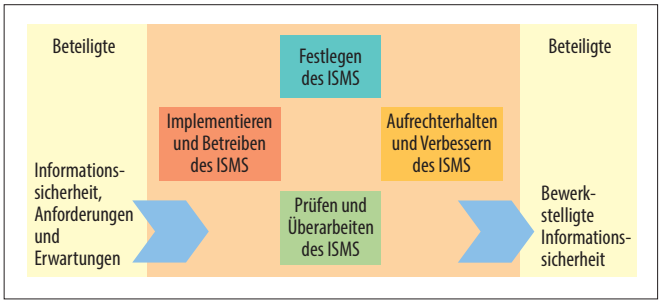


Bild 1. PDCA-Zyklus: Das Information Security Management System, kurz ISMS, muss regelmäßig von den Beteiligten überprüft werden. (Quelle: ISO/IEC 27001)

Normungsteile	Stand der Ausarbeitung
Teil 1-1	„Technical Specification" Ed. 1 bereits veröffentlicht [3]. Ed. 2 für 2013 geplant.
Teil 1-2	In Arbeit.
Teil 1-3	Veröffentlichung eines „Draft for Comment" im ersten Quartal 2013 geplant.
Teil 2-1	„International Standard" Ed. 1 bereits veröffentlicht [1]. Ed. 2 als „Draft for Comment" im Oktober 2012 veröffentlicht.
Teil 2-3	In Arbeit.
Teil 2-4	Veröffentlichung eines „Committee Draft" im ersten Quartal 2013 geplant.
Teil 3-1	„Technical Report" Ed. 1 bereits veröffentlicht [4].
Teil 3-2	In Arbeit.
Teil 3-3	Veröffentlichung eines "Final draft for international standard" (FDIS) im ersten Quartal 2013 geplant.
Teil 4-1	Veröffentlichung eines „Draft for Comment" im ersten Quartal 2013 geplant.
Teil 4-2	Veröffentlichung eines „Draft for Comment" im ersten Quartal 2013 geplant.

erwarten, dass der Inhalt sich nicht wesentlich ändern wird.

Risikominimierung und Modelle

Die Vorgehensweise zur Risikominimierung und die Modelle sind bei Industrial Security und der funktionalen Sicherheit vergleichbar. Die Vorstellung vom Ablauf eines Schadensereignisses ist in der Industrial Security die, dass ein Angreifer mit Hilfe von Schwachstellen in die zu schützende Lösung eindringt. Da er intelligent vorgehen kann, lässt sich sein Verhalten nicht vorhersagen. Im Gegensatz zur Risikoanalyse in der funktionalen Sicherheit lassen sich Ereignisabläufe im Voraus nicht vollständig festlegen. Bei der Industrial Security kann man nicht einmalig auf Basis der Risikoanalyse die Schutzmaßnahmen festlegen, sondern muss immer wieder im Laufe der Lebenszeit der Anlage die Bedrohungslage neu bewerten und gegebenenfalls neue Maßnahmen einführen. Hier ist die VDI/VDE 2182 [7] zu erwähnen, die das Zusammenspielen der drei Rollen Betreiber, Lösungsanbieter und Hersteller beschreibt.

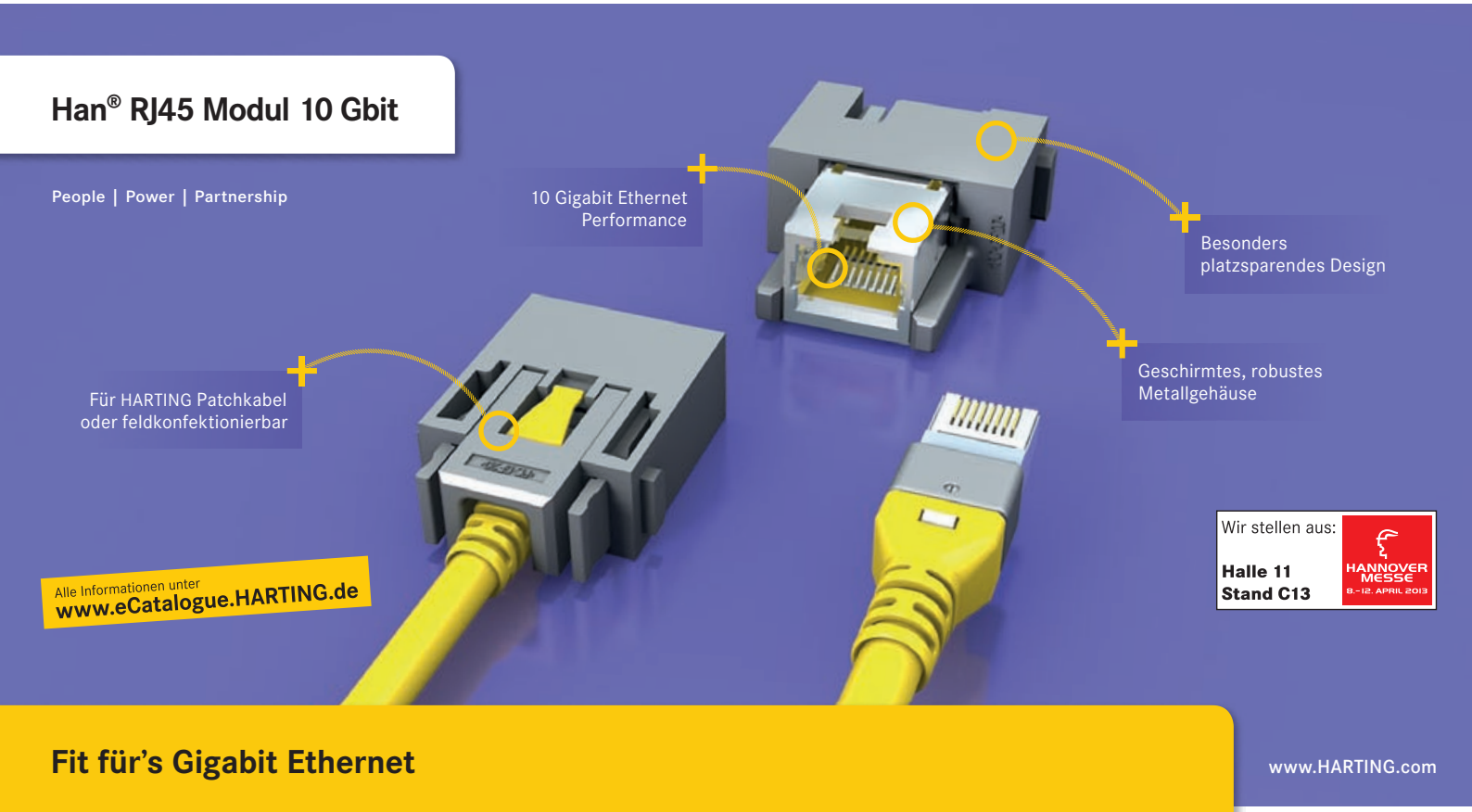
Nach den vorliegenden Entwürfen zur IEC 62443 wird der Einsatz und der Nachdruck, mit dem ein Angriff erwartet wird, mit Hilfe einer vierstufigen Skala, der sogenannten Security Levels (SL), beschrieben.

IEC 62443 Industrial communication networks - network and system security			
General	Policies and procedures	System	Component
1-1 Terminololgy, concepts and models	2-1 Industrial automation and control system security management system	3-1 Security technologies for industrial automation and control systems	4-1 Product developement requirements
1-2 Master glossary of terms and abbreviations	2-3 Patch management in the IACS environment	3-2 Security levels for zones and conduits	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-4 Requirements for IACS solution suppliers	3-3 System security requirements and security levels	
Definitionen, Metriken	Managementsystem des Anlagenbetreibers und des Lösungsanbieters	Funktionen der Systeme	Entwicklungsprozess Funktionen der Geräte

Bild 2. Struktur der Normreihe IEC 62443.

- SL 1: Schutz gegen ungewollten, zufälligen Missbrauch.
- SL 2: Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Fähigkeiten und niedriger Motivation.
- SL 3: Schutz gegen gewollten Missbrauch unter Verwendung von technisch hochentwickelten Mitteln, mit moderatem Aufwand, automatisierungstechnisch spezifischen Fähigkeiten und moderater Motivation.
- SL 4: Schutz gegen gewollten Missbrauch, unter Verwendung von technisch hochentwickelten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Fähigkeiten und hoher Motivation.

Es war in den vergangenen Jahren zu beobachten, dass die Mittel und Fähigkeiten für einen Angriff immer leichter



Fit für's Gigabit Ethernet

Das bewährte RJ45 Ethernet Modul aus der Han-Modular® Serie ist jetzt Kat. 6 tauglich.
Mit dem neuen, komplett geschirmten RJ45 Buchsenmodul lassen sich äußerst platzsparend Übertragungsraten bis 10 Gbit/s realisieren. Auf der Buchsenseite ist das Modul als Gender Changer ausgeführt, so dass der Anschluss einfach durch Einstecken eines HARTING RJ45 Patchkabels erfolgt. Auf der Stiftseite stehen zwei Kat. 6 taugliche Lösungen zur Verfügung: Eine feldkonfektionierbare Variante mit dem RJ Industrial oder ein Modul, das entsprechende HARTING Patchkabel aufnehmen kann.
HARTING: Mit Pushing Performance zu innovativen Lösungen.

Nehmen Sie Kontakt auf: HARTING Deutschland GmbH & Co. KG
Simeonscarré 1 | D-32427 Minden | Tel +49 571 8896-0 | Fax +49 571 8896-990604 | de@HARTING.com

HARTING®
Pushing Performance

und mit weniger Aufwand zu erlangen waren. Heute wird hochentwickelte Schad-Software im Internet zum Kauf angeboten oder ist gar frei verfügbar. In der Beschreibung der Schutzstufen hat man daher bewusst Fähigkeiten, Motivation und Mittel des Angreifers und nicht Schutzmaßnahmen gegen einen Angriff gewählt. Damit ist sichergestellt, dass die Definitionen gültig bleiben, auch wenn die Bedrohungslage sich mit der Zeit verändert.

Im Gegensatz zur funktionalen Sicherheit mit ihren Sicherheitsfunktionen gibt es übergeordnete Ziele, die durch die Industrial Security abgedeckt werden müssen. Diese wurden daher als sogenannte Foundational Requirements nach IEC 62443-1-1 (zur Zeit in der Überarbeitung) definiert:

- *FR 1: Identification and authentication control.* Sicherstellung, dass Benutzer erkannt und deren Identitäten geprüft werden, bevor der Zugang zu dem System gewährt wird.
- *FR 2: Use control.* Sicherstellung, dass identifizierte und authentisierte Benutzer nur die für sie berechtigten Aktionen durchführen können.
- *FR 3: System integrity.* Sicherstellung, dass Informationen und Funktionen des Systems nicht unzulässig verändert werden.
- *FR 4: Data confidentiality.* Sicherstellung, dass Informationen sowohl bei der Übertragung als auch bei der Speicherung nicht zu unzulässigen Empfängern gelangen können.
- *FR 5: Restricted data flow.* Sicherstellung, dass Datenflüsse innerhalb des Systems sowie von und zum System nur durch die dafür festgelegten Kommunikationskanäle geführt werden.
- *FR 6: Timely response to events.* Sicherstellung, dass bei einem gewollten oder ungewollten Missbrauch eine geeignete Reaktion einschließlich Benachrichtigung ausgelöst wird.
- *FR 7: Resource availability.* Sicherstellung, dass die Verfügbarkeit des Systems nicht durch Überlast einer oder mehrerer seiner Bestandteile beeinträchtigt wird.

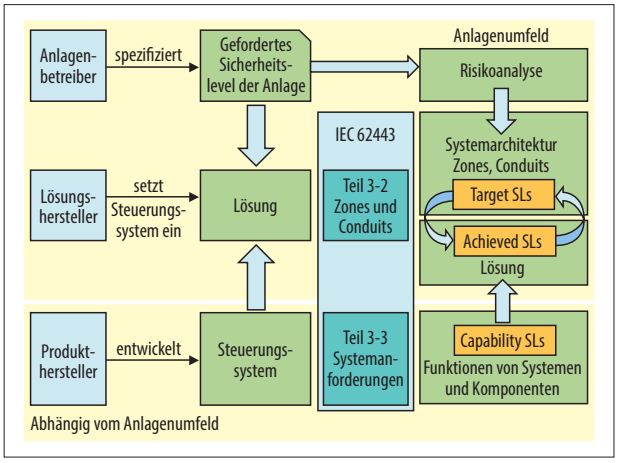


Bild 3. Vorgehensweise beim Umgang mit Security Levels.

Die angestrebten Schutzniveaus können in den verschiedenen FRs unterschiedlich sein. So kann es z.B. wichtig sein, den Zugriff und den Betrieb einer Anlage oder eines Anlagenteils besonders stark zu schützen (FR 1 und FR 2), während die Datenvertraulichkeit (FR 4) nicht so sehr im Fokus steht. Man spricht daher von einem sogenannten SL Vector mit sieben Dimensionen – entsprechend der sieben FRs. Im Teil 3-3 der 62443-3-3 wird der Umgang mit den Security Levels beschrieben. Es werden folgende Ausprägungen unterschieden (**Bild 3**):

- Target SLs (SL-T) sind die angestrebten Schutzniveaus einer Automatisierungslösung. Diese werden als Ergebnis einer Risikobewertung und des akzeptablen Restrisikos bestimmt.
- Achieved SLs (SL-A) beschreiben die erreichten Schutzniveaus nach der Designphase oder bei einer vorhandenen Automatisierungslösung.
- Capability SLs (SL-C) sind die Schutzniveaus, die durch die Funktionen von Systemen und Komponenten erreicht werden können, wenn diese richtig eingesetzt werden. Sie drücken aus, dass die Komponente oder das System in sich fähig ist, die SL-T zu erreichen, ohne zusätzliche, ausgleichende Gegenmaßnahmen.

Als Basis der Vorgehensweise ist immer eine Risikoanalyse durchzuführen. Das Ziel ist es, Bedrohungen und deren Auswirkung zu identifizieren und daraus eine Segmentierung der Automatisierungslösung in Zellen (Zones) und Kommunikationskanäle (Conduits) festzulegen. Mit dem Wissen über den Prozess oder die Produktion werden Schutzziele zur Risikominimierung vorgegeben. Dieser Schritt ist projektspezifisch und erfordert immer das Einwirken des Betreibers. Die Unterteilung des Netzwerks ist sehr sinnvoll, um einen möglichen Schaden auf eine Zelle zu begrenzen. Die Schutzziele der verschiedenen Zellen können durchaus unterschiedlich sein. So ist es sinnvoll, für einen Anlagenteil, der z.B. die verfahrenstechnische Produktion eines gefährlichen Stoffs steuert, besonders aufwendige, ggf. auch teure Maßnahmen zu implementieren. Ein weniger kritischer Anlagenteil kann durch eine weniger geschützte Zelle gesteuert werden. Das Ergebnis dieser Übung ist eine Architektur in Zellen und Kanälen und die Festlegung des SL-T-Vektors für jede dieser Einheiten.

Als Antwort auf die o.g. Vorgaben konfiguriert der Systemintegrator oder der Anlagenbauer eine Automatisierungslösung auf Basis von verfügbaren Komponenten oder Systemen. Dabei setzt er deren Funktionen ein, um möglichst die SL-T der Zellen und Kanäle zu erreichen. Sind diese nicht ausreichend, ergreift er zusätzliche Maßnahmen, sogenannte „compensating countermeasures", die das Schutzniveau erhöhen. Das kann z.B. das Begrenzen des physikalischen Zugangs zu der Anlage oder das Verwenden von geeigneten Firewalls sein. Falls die erreichten Schutzniveaus SL-A die Ziele nicht erfüllen können, muss der Betreiber das dann vorhandene Restrisiko akzeptieren oder durch weitere Maßnahmen in seinem Verantwortungsbereich kompensieren; z.B. kann durch Schulung, Organisation und Kontrolle das Risiko weiter reduziert werden.

Im Teil 3-2 der Norm IEC 62443, der noch in Arbeit ist, wird der Vorgang der Segmentierung in Zones und Conduits und der Festlegung der SL-T beschrieben. Im Teil 3-3 werden die funktionalen Anforderungen an ein System spezifiziert. Die System Requirements sind in dem Dokument nach den sieben FRs gegliedert und den jeweiligen SL-Cs entsprechend der Skala zugeordnet. Damit können die Funktionen verschiedener Systeme in den sieben Dimensionen bewertet und differenziert werden.

Defense in Depth

Im vorhergehenden Abschnitt wird ersichtlich, dass alle Teilnehmer in der Festlegung der Schutzmaßnahmen be-

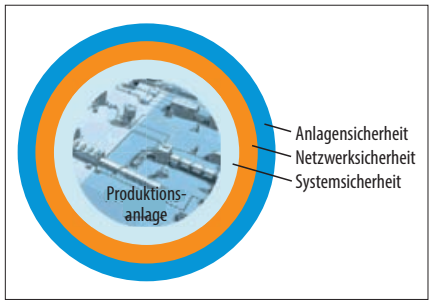


Bild 4. Ausgewählte Maßnahme zu Defense-in-Depth-Strategie. (Quelle: Siemens)

teiligt sind: Der Anlagenbetreiber, der Lösungsanbieter und der Produkthersteller. In der Regel reicht eine einzige Maßnahme nicht aus, um einen gegebenen Schutz zu erreichen, sondern es sind mehrere aufeinander abgestimmte Maßnahmen erforderlich, die jeweils eine eigene Barriere gegen einen Angriff bilden. Diese werden als Verteidigungslinien und die Abwehrstrategie als Defense in Depth bezeichnet (**Bild 4**). Die Norm 62443 adressiert alle Teile dieser Strategie.

Die ersten Verteidigungslinien sind beim Anlagenbetreiber zu finden und werden durch den Teil 2-1 adressiert (Anlagensicherheit). Eine erste Barriere ist schon vorhanden, wenn das Personal auf die Gefahren durch Angriffe über das Netz geschult wird und Abläufe und Maßnahmen zur Erhöhung des Schutzes in den Prozessen und der Organisation klar definiert sind. Dazu zählen u.a. die Absperrung und die Zugangskontrolle der Räume, die Sicherstellung der Vertrauenswürdigkeit des Personals, die Festlegung von Rechten und Pflichten der Benutzer und das Sicherstellen der Kontinuität des Betriebs im Falle eines Angriffs.

Weitere Schichten in der Defense in Depth sind in der Auslegung der Automatisierungslösung zu finden, beispielsweise durch Segmentierung des Netzwerks und Absicherung über Firewalls, Schutz des Zugriffs mit Passwörtern oder Eingrenzung der Aktionen der Benutzer auf das minimal Erforderliche (Netzwerksicherheit). Diese Maßnahmen werden in der Regel durch den Lösungsanbieter auf Basis von Systemfunktionen getroffen und in den Teilen 3-2 und 3-3 adressiert.

Die inneren Schichten betreffen Maßnahmen, die in den Komponenten und Systemen selbst zu finden sind (Systemsicherheit). Sie werden durch die Produkthersteller angeboten und in den Teilen 3-3 und 4-2 adressiert. Typische Maßnahmen sind der Schutz gegen Malware durch Virenscanner oder White Listing, der Schutz von Software-Teilen, den Einsatz von Signatur beim Herunterladen von Software-Komponenten oder der Schutz gegen das Raten von Passwörtern durch Verzögerungszeiten.

Weitere Beiträge werden dadurch erreicht, dass der Schutz bei der Instandsetzung und Instandhaltung der Automatisierungslösung durch geeignete Prozeduren und Richtlinien sichergestellt (Teil 2-4) und dass durch die Gestaltung des Entwicklungsprozesses möglichst die Anzahl der Schwachstellen in den Komponenten und Systemen gering gehalten wird (Teil 4-1).

Im industriellen Umfeld müssen Anlagen im laufenden Betrieb gegen Angriffe geschützt werden. Alle Teilnehmer müssen dabei ihren Beitrag zur Defense-in-Depth-Strategie leisten. Komponenten und Systeme müssen Funktionen enthalten, die einen integrierten Schutz bilden und das Konfigurieren geschützter Automatisierungslösungen unterstützen. Der Lösungsanbieter muss diese in Automatisierungslösungen einsetzen, um das Eindringen eines Angreifers möglichst zu erschweren. Der Anlagenbetreiber muss dafür sorgen, dass die Anlage sicher betrieben wird, indem er in seiner Organisation die geeigneten Vorschriften einführt und während der Lebenszeit der Anlage umsetzt. *ag*

Dr. Pierre Kobes
ist seit über 30 Jahren bei Siemens im Bereich Prozess-Instrumentierung und industrielle Automatisierung tätig. Seine Laufbahn deckt Aufgaben in Entwicklung, Marketing, strategische Planung und Management ab. Seit drei Jahren ist er Mitglied der Organisation für Industrial Security, in der er für Standards & Regulations zuständig ist. In dieser Funktion ist er Product and Solution Security Officer.
pierre.kobes@siemens.com

Ingo Rolle
war zunächst in verschiedenen Industriestellungen tätig, bevor er 1993 zur DKE (Deutsche Kommission Elektrotechnik, Elektronik, Informationstechnik im DIN und VDE) kam. Er betreut dort Normenausschüsse, die in der industriellen Automatisierung tätig sind. Hierzu gehört auch das GK 914, das für die IEC 61508 zuständig ist, und das UK 931.1 für die IT-Sicherheit.
ingo.rolle@vde.com

Literatur

[1] IEC 62443-2-1: Industrial communication networks – network and system security. Part 2-1: Establishing an industrial automation and control system security program. Ed. 1.0 2010-11.
[2] Serie ISO/IEC 27000: Information technology – Security techniques – Security management systems
[3] IEC/TS 62443-1-1: Industrial communication networks – network and system security. Part 1-1: Terminology, concepts and models. Ed. 1.0 2009-07.
[4] IEC/TR 62443-3-1: Industrial communication networks – network and system security. Part 3-1: Security technologies for industrial automation and control systems. Ed. 1.0 2009-07.
[5] Process control domain-security requirements for vendors. Report: M 2784 X-10. WIB; Ausgabe 2, Oktober 2010.
[6] EDSA-312 Embedded Device Security Assessment – Software Development Security Assessment (SDSA) V1.4 2010-08
[7] VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung. Beuth Verlag GmbH, Berlin.