Prozess-anlagen im digitalen Zeit-alter sichern und schützen

IT-Sicherheit und
Funktionale Sicherheit
gehören zusammen

HIMA
SAFETY
NONSTOP

Prozessanlagen im digitalen Zeitalter sichern und schützen

IT-Sicherheit und Funktionale Sicherheit gehören zusammen

2014. Ein deutsches Stahlwerk wird zum Opfer einer gezielten Cyberattacke. Über Spearphishing und Social Engineering erhalten die Angreifer zunächst Zugriff auf das Büronetzwerk und darüber auf das Produktionsnetzwerk. Die Konsequenz: Steuerungselemente fallen aus und schließlich auch ganze Anlagen. Ein Hochofen wird dabei schwer beschädigt. Vorfälle wie diese sind Alarmsignale für Anlagenbetreiber, IT- und Automatisierungsunternehmen, Sicherheitsingenieure sowie viele andere. Sie zeigen, wie sehr Cybersecurity mit einem sicheren Industriebetrieb verknüpft ist.

Natürlich sind Cyberangriffe in kleinerem Ausmaß viel wahrscheinlicher. Ein Angriff auf eine Anlage offenbarte sich zum Beispiel erst, als das Datenübertragungsvolumen den vertraglichen Rahmen des Dienstleisters überschreitet. Hätte man die Systemwartung in diesem Fall über die einfache Authentifizierung (Benutzername/Kennwort) per Fernzugriff bedient, wäre der Angriff nicht zu beherrschen gewesen.

Jedoch können die mit der Cyberwelt zusammenhängenden Sicherheitslücken nicht nur zu kriminellen Aktivitäten führen. Ein Beispiel: Während der Inbetriebnahme einer Anlage verändert die Neukompilierung der Visualisierungsbilder die Sicherheitssteuerung. Der Grund: eine Kombination von zwei Fehlern im Engineering System. Die Kompilierung wird automatisch in die integrierte sicherheitsgerichtete Steuerung geladen und anschließend automatisch aktiviert.

Alle drei Beispiele zeigen, wie wichtig IT-Sicherheit heute ist. Daraus ergeben sich drei zentrale Fragen zum Verhältnis zwischen Cybersecurity und Anlagensicherheit:

1. **Kann die „Unsicherheit“ integrierter Steuerungssysteme die Funktionale Sicherheit einer Anlage beeinflussen?**
2. **Was muss geschützt werden?**
3. **Können die für die Funktionale Sicherheit entwickelten Prinzipien auf die IT-Sicherheit von Anlagen angewendet werden?**

Dieses Whitepaper untersucht diese Fragen und gibt einige betriebliche Beispiele sowie Empfehlungen, wie die IT-Sicherheit in Industrieanlagen gewährleistet werden kann.

Internationale Standards für die Sicherheit und Sicherung von Anlagen

Die Leser des Whitepapers kommen vermutlich aus unterschiedlichen fachlichen Bereichen. Manche sind IT-Spezialisten, die mit den Standards vertraut sind, die für die Cybersicherheit in Industrieanlagen gelten. Manche sind Spezialisten für Betrieb, Verfahrenstechnik und Sicherheit von Industrieanlagen, die mit den für sie geltenden Industriestandards vertraut sind. Andere sind unter Umständen Manager, die für den Gesamtkomplex der Sicherheit und Sicherung von Anlagen mitverantwortlich sind.

Um den Zusammenhang von Cybersecurity und Funktionaler Sicherheit zu verstehen, ist es wichtig, dass alle die gleiche Sprache sprechen.

Die Definition der Funktionalen Sicherheit ist ein guter Ausgangspunkt. Die IEC 61508 ist der internationale Standard für die Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen sicherheitsgerichteten Systemen, herausgegeben von der International Electrotechnical Commission (IEC). Gemäß dieser Norm ist die Funktionale Sicherheit „Teil der Gesamtsicherheit, die davon abhängt, dass Funktionseinheiten und physische Einheiten als Reaktion auf ihre Eingangswerte ordnungsgemäß funktionieren“.

Wikipedia beschreibt es so: „Funktionale Sicherheit bezeichnet den Teil der Sicherheit eines Systems, der eine zuverlässige und sicherheitsbezogene Funktion der (Sub-)Systeme und externer Einrichtungen sowohl im Normalbetrieb als auch bei Ausfällen und Fehlern garantiert.“

Anhand der Definition im engeren und weiteren Sinne muss die Antwort auf die Frage *„Kann die ‚Unsicherheit' eines integrierten Steuerungssystems die Funktionale Sicherheit einer Anlage beeinflussen?“* mit Ja beantwortet werden. Bei den eingangs zitierten Beispielen wurden Sicherheitslücken in Anlagen aufgedeckt. Offenkundig war die Funktionale Sicherheit beeinträchtigt. In Bezug auf die Informationssicherheit muss das Ziel sein, alle möglichen Einflüsse auf die ordnungsgemäße Funktion abzumildern: Die Gefährdung von Personen, Umwelt und Sachwerten soll ausgeschlossen bzw. minimiert werden.

Selbst wenn man böswillige Bedrohungen ausschließt: Es bleibt die Tatsache, dass mit der Cybersecurity zusammenhängende Sicherheitslücken bei fast allen Arten von Automatisierungssystemen zu finden sind. Hierzu gehören sowohl das sicherheitsgerichtete System selbst als auch das verteilte Leitsystem (Distributed Control System, DCS), wobei das sicherheitsgerichtete System unter Umständen ein integrierter Bestandteil des DCS ist. Deshalb fordern viele Sicherheitsexperten, dass die Komponenten des Sicherheitssystems physisch von denen des DCS getrennt sind – und von unterschiedlichen Mitarbeitern und/oder Zulieferern geplant und gewartet werden.

Werfen wir den Blick auf zwei weitere Standards. Einer ist der internationale Standard IEC 61511 für Sicherheitssysteme (Safety Instrumented System, SIS). Unabhängig davon, ob das SIS in ein übergeordnetes Prozessleitsystem (Overall Basic Process Control System, BPCS) integriert oder getrennt von diesem ist, bildet das SIS eine grundlegende Komponente jeder industriellen Prozessanlage.

In der Praxis wird die IEC 61511 wie in Abbildung 1 umgesetzt:

Abbildung 1

Bei diesem Modell ist der Industrieprozess von unterschiedlichen „Schichten“ zur Risikominderung umgeben. Gemeinsam senken sie das Risiko auf ein zulässiges Maß. Zum Entwurf einer Anlage gehören Risiko- und Gefahrenanalyse. Diese ermitteln den Risikominderungsfaktor, der bei den einzelnen Schutzschichten erreicht werden muss. Dieser Risikominderungsfaktor ist durch die Sicherheitsanforderungsstufe (Safety Integrity Level, SIL) festgelegt.

Die unterste Schutzschicht jeder Anlage ist die Steuerungs- und Überwachungsschicht (Control & Monitoring), die das Prozessleitsystem (BPCS) enthält. Sie verringert das Risiko, dass unerwünschte Ereignisse eintreten. Der Risikominderungsfaktor eines BPCS muss größer als 1 und kleiner als 10 sein. Hintergrund ist, dass das BPCS üblicherweise keine SIL hat (dann wäre eine Risikoreduzierung von mindestens 10 = SIL1 gegeben), gleichzeitig jedoch einen Einfluss ausübt (kein Einfluss wäre ein Risikominderungsfaktor von 1).

Die nächste Schutzschicht des Modells (Prevention) enthält das SIS. Die Hardware und Software auf dieser Ebene übernehmen einzelne Sicherheitsfunktionen (Safety Instrumented Function, SIF). Bei vielen kritischen Industrieprozessen muss das SIS die Anforderungen der SIL 3 erfüllen, um das Gesamtrisiko auf einen zulässigen Wert zu senken. Dieser entspricht einem Risikominderungsfaktor von 1.000.

Auf der obersten Schadensbegrenzungsschicht (Mitigation Layer) sind technische Systeme angeordnet, die Schäden abmildern, sollten die unteren Schutzschichten einmal ausfallen. Meistens sind Abmilderungssysteme nicht Bestandteil des Sicherheitssystems, da sie erst nach Eintritt eines Ereignisses (das verhindert werden sollte) aktiviert werden. Hier kommen häufig mechanische oder bauliche Einrichtungen, wie z.B. Rückhaltebecken, zum Einsatz. Zu manchen gehören auch automatisch wirkende Feuerlöschsysteme.

In Fällen, in denen von der Anwesenheit des Schadensbegrenzungssystems Kredit für die anderen sicherheitstechnischen Festlegungen genommen wird, können hierfür ebenfalls Sicherheitsanforderungen postuliert werden.

Beispiel: Ein Feuerlöschsystem in einem Tanklager kann als sicherheitsrelevant betrachtet werden, wenn die Entfernung zwischen den Tanks aufgrund des vorhandenen Feuerlöschsystems verringert wird.

Werfen wir jetzt einen Blick auf den IEC-Standard für Cybersecurity: Die IEC 62443 – die gegenwärtig als Entwurf vorliegt – behandelt die Sicherungsverfahren, die Cybersicherheitsattacken auf Netzwerke und Systeme von Anlagen unterbinden können (Abbildung 2).

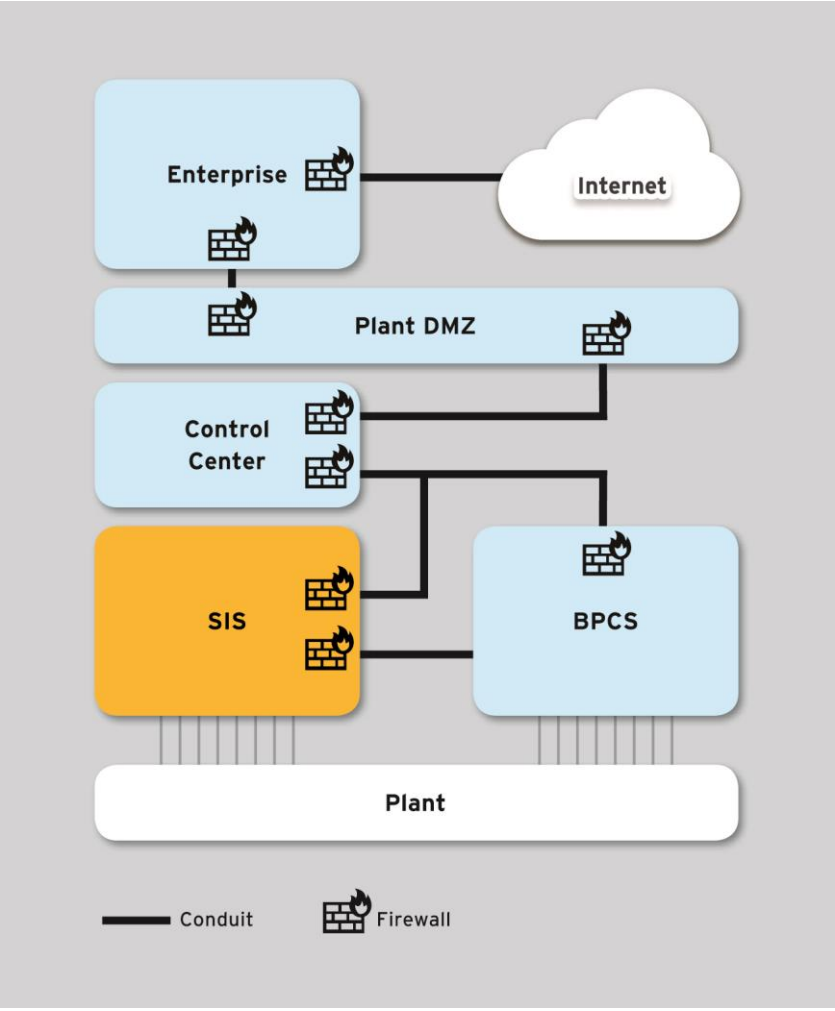

Abbildung 2

Die IEC 62443 fordert, dass Gesamtanlagen aufgeteilt werden. Sie führt das Konzept von Sicherheitszonen, festgelegten Kanälen und zusätzlichen Firewalls in jedem Kanal ein, welcher von einer Sicherheitszone zur nächsten führt. Je nachdem, welches Schutzniveau in den einzelnen Zonen angestrebt wird, gibt es unterschiedliche technische Anforderungen an die Firewalls.

Die IEC 62443 beinhaltet sieben Arbeitsfelder, die unterschiedliche Schutzziele verfolgen, wie beispielsweise die Zugriffskontrolle, also den Schutz einer Einrichtung vor

unberechtigtem Zugriff. Eine solche Gliederung führt zu einem gestaffelten System unterschiedlicher Schutzmechanismen (Defence in Depth).

Normen und Strukturen verlangen einen Schutz

„Was müssen Anlagenbetreiber schützen?“ Gemäß der jüngsten Version der IEC 61511 lautet die Antwort, dass organisatorische Forderungen und vorgegebene physische Strukturen gleichermaßen beachtet werden müssen.

Hinsichtlich der Organisation fordert der Standard Folgendes:

- Einschätzung des Sicherheitsrisikos des SIS,
- Herstellung einer ausreichenden Widerstandsfähigkeit des SIS gegenüber den ermittelten Sicherheitsrisiken,
- Gewährleistung der Leistungsfähigkeit, Diagnose- und Fehlerbehandlung des SIS, Schutz vor unerwünschten Programmveränderungen, Schutz der Daten zur Fehlersuche an den SIF und Schutz vor der Umgehung von Beschränkungen, sodass Alarme und die manuelle Abschaltung nicht deaktiviert werden,
- Aktivierung/Deaktivierung des Lese- und Schreibzugriffs mithilfe eines ausreichend sicheren Verfahrens.

Hinsichtlich der Struktur verlangt die IEC 61511 von den Betreibern, eine Einschätzung ihres SIS durchzuführen. Sie sollten:

- voneinander unabhängige Schutzschichten einführen,
- verschiedenartige Schutzschichten etablieren,
- Schutzschichten physisch trennen,
- gemeinsame Ausfallursachen der Schutzschichten frühzeitig erkennen bzw. vermeiden.

Eine weitere Anforderung der IEC 61511 betrifft insbesondere das Verhältnis von Cybersecurity und Anlagensicherheit:

„Sofern praktisch möglich, sollten die SIF von nicht sicherheitsgerichteten Funktionen physikalisch getrennt sein.“

Voneinander unabhängige Schutzschichten von entscheidender Bedeutung

„Können die für die Funktionale Sicherheit entwickelten Prinzipien auch auf die Cybersecurity von Anlagen angewendet werden?“

Die Standards IEC 61511 (Anlagensicherheit) und IEC 62443 (Cybersecurity) fordern übereinstimmend unabhängige Schutzschichten. Diese beiden Standards schreiben vor:

- voneinander unabhängige Steuerung und Anlagensicherheit,
- Maßnahmen zur Verringerung systematischer Entwurfsfehler,
- Trennung der Verantwortung für Technik und Management,
- Verringerung der Auswirkung von Fehlern mit gemeinsamen Ursachen.

Außerdem bekräftigen die Standards, dass das gesamte System nur so stark sein kann wie sein schwächstes Glied. Bei der Verwendung integrierter Sicherheitssysteme (Sicherheitssystem und Standardautomatisierung auf der gleichen Plattform) muss jegliche Hardware und Software, die sich negativ auf die Sicherheitsfunktion auswirken kann, als Teil der Sicherheitsfunktion betrachtet werden. Die Folge: Das Standard-Automatisierungssystem muss, sowohl im Bereich des Engineerings als auch im Bereich von Änderungen, dem gleichen Managementprozess unterworfen werden, wie er für die jeweiligen Sicherheitssysteme gefordert wird.

Dabei ist hervorzuheben, dass die beschriebene Integration Folgendes bedeutet: Das BPCS unterliegt den gleichen Anforderungen wie denen im Bereich der Funktionalen Sicherheit, jedoch können die Anforderungen an das Sicherheitssystem nicht reduziert werden.

Sicherheitsstandards in der Praxis

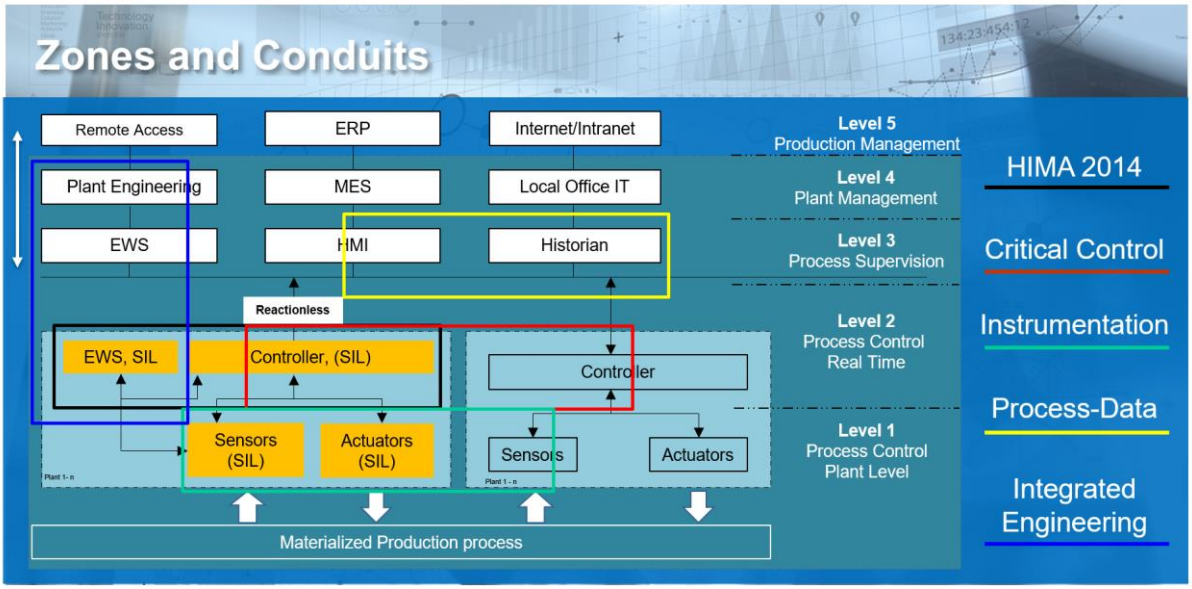

Abbildung 3

Betrachten wir jetzt die Konfiguration in Abbildung 3. Sie beschreibt die komplexen Prozessanwendungen (Hinweis: Aus Gründen der Vereinfachung ist die Architektur bewusst nicht der ISA 95 entsprechend dargestellt).

Die Struktur zeigt unterschiedliche Schichten von Komponenten mit Funktionen unterschiedlicher Kritikalität. Auf Ebene 1 sehen wir Feldgeräte wie Sensoren und Aktoren, die je nach Art des einzelnen Gerätes ihre eigene IT-Relevanz haben können. Die Infrastruktur der Ebene 1 kann auf einer reinen Verdrahtung beruhen, aber auch Funktionen wie die drahtlose Hart-Datenübertragung oder verkabelte Feldbus-Anlagen nutzen.

Auf der Ebene 2 sehen wir Komponenten, die die Daten verarbeiten, die durch die Sensoren erfasst wurden bzw. von den Aktoren benötigt werden.

Auf beiden Ebenen ist es entscheidend, Daten in Echtzeit zu übertragen und zu verarbeiten. Daher ist ein auf Software beruhender Schutz vor Malware (z.B. Virenscanner) nicht geeignet. Alternative Maßnahmen sind gefragt. Dazu zählen ein begrenzter Zugang zum

Datenaustausch (Deaktivierung von Datenaustauschanschlüssen) und die logische Trennung von Teileinheiten. Diese Maßnahmen müssen während des gesamten Lebenszyklus der Anlage in jeder der einzelnen Anwendungen aufrechterhalten werden.

Im abgebildeten SIS der SIL 3 ist das gesamt SIS – einschließlich der Engineering Workstation – vom Rest des DCS getrennt. Wird diese Trennung aufgehoben, weil beispielsweise eine gemeinsame Engineering Workstation verwendet wird, müssen die folgenden Konsequenzen berücksichtigt werden:

- Gemäß IEC 61511 müsste die DCS Engineering Workstation (EWS) ein Bestandteil des SIS sein. Das gesamte für diese Einrichtung zum Einsatz kommende Änderungsmanagement muss an die Sicherheitsanforderungen angepasst werden.

- Die Schnittstelle zwischen SIS und DCS, die im ursprünglichen Konzept nur für den Lesezugriff vorgesehen war (aus Sicht des SIS), muss eine Schreib-/Lesefunktionalität aufweisen, die das Risiko unerwünschter Veränderungen des SIS erhöht.

- Um eine ausreichende Unabhängigkeit des SIS sicherzustellen, wird ein Mechanismus benötigt, mit dem unerwünschte Veränderungen verhindert werden – also in einer Weise, die nicht durch die Engineering Workstation umgangen werden kann (vgl. Abbildung 4).

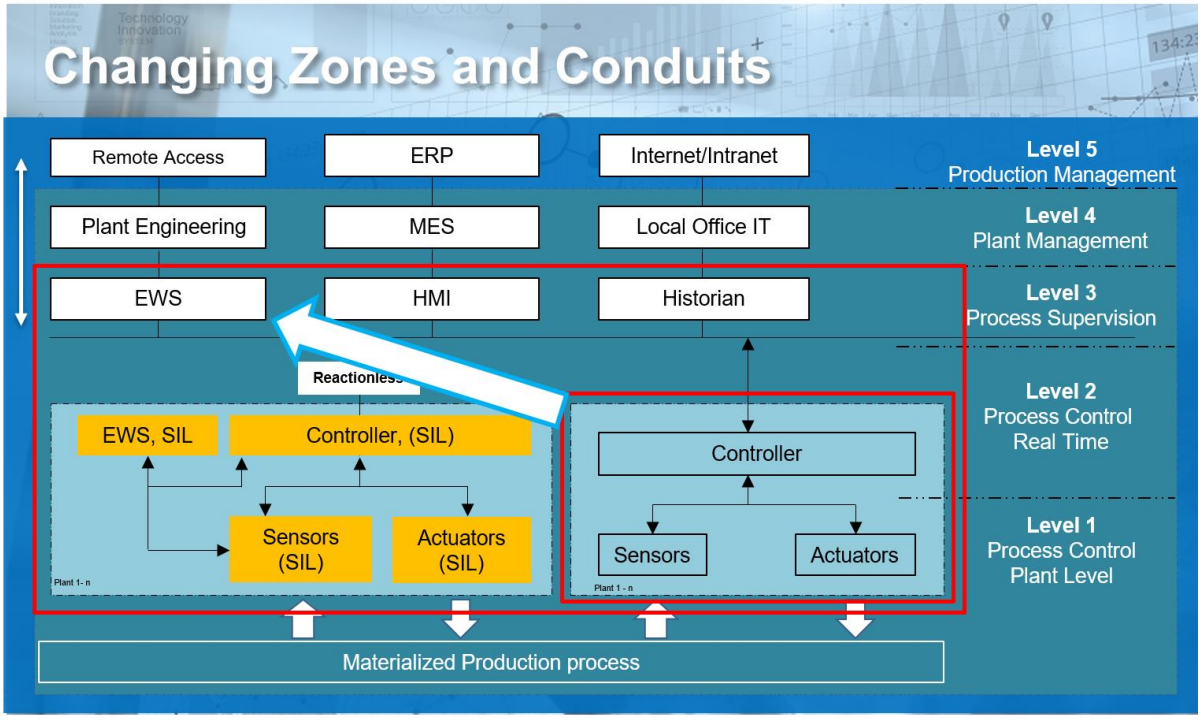

Abbildung 4

Angenommen, es gibt einen direkten Fernzugriff auf das SIS, so muss das Fernzugriffsgerät ein Bestandteil des SIS sein (vgl. IEC 61511) – sofern es keine anderen Maßnahmen gegen unerwünschte Zugriffe über die Verbindung gibt. Die Anforderung an das Schutzniveau lässt sich ggf. durch zusätzliche Maßnahmen senken. Ein Beispiel ist das Abschalten des Fernzugriffs, wenn dieser nicht benötigt wird. Dies gelingt über ein Gerät, das nicht durch die

Software gesteuert wird und funktionale Veränderungen des SIS blockiert (z.B. ein Schlüsselschalter, der mit einem physischen Eingang des SIS verbunden ist).

Hinweis: Bei diesem Beispiel bedeutet „Abschalten“ das Stromlosschalten des Verbindungsgerätes.

Sicherheitstechnische Bewertung beim Zusammenlegen von Schutzebenen

Wenn Schutzebenen zusammengelegt werden, müssen auch sicherheitstechnische Aspekte beachtet werden.

Die IEC 61511 fordert unterschiedliche und voneinander unabhängige Schutzebenen. Werden zwei Schutzebenen zusammengelegt, müssen Betreiber die Risikominderung neu einschätzen. Hierbei ist nachzuweisen, dass dieselbe Gesamt-Risikominderung erreicht wird wie bei zwei bestehenden unterschiedlichen Schutzschichten.

Normalerweise wird im Rahmen der Risikoanalyse ermittelt, welche Risikominderung erforderlich ist. Dabei wird nicht berücksichtigt, welche technische Lösung zur Realisierung des SIS verwendet wird. Schließlich steht in dieser Phase der Projekte die technische Plattform in der Regel noch nicht fest.

Dazu ein Beispiel: Angenommen, ein Prozess wird durch ein Leitsystem automatisiert und die Risikoanalyse ergibt, dass eine zusätzliche Risikoreduzierung durch ein SIL-3-konformes SIS erforderlich ist (Risikominimierung um Faktor 1.000). Wird in diesem Fall eine Lösung mit zwei voneinander unabhängigen (unterschiedlichen) Systemen (air gapped) zur Automatisierung und Überwachung sowie zum Schutz ausgerüstet, so ergibt sich eine Risikoreduzierung von 1.000 durch das SIS (SIL 3) sowie eine Risikoreduzierung von >1 und <10 durch das BPCS. Gemeinsam betrachtet liefert diese Lösung eine Risikoreduzierung von >1.000 und <10.000.

Wird in einem solchen Fall die Anwendung mit einer Lösung ausgeführt, die Sicherheit und betriebliche Steuerung integriert, so muss diese hinsichtlich ihrer Fähigkeit zur Risikominderung die gleiche Risikoreduzierung erreichen, wie dies bei der Lösung mit einem getrennten Sicherheitssystem der Fall wäre.

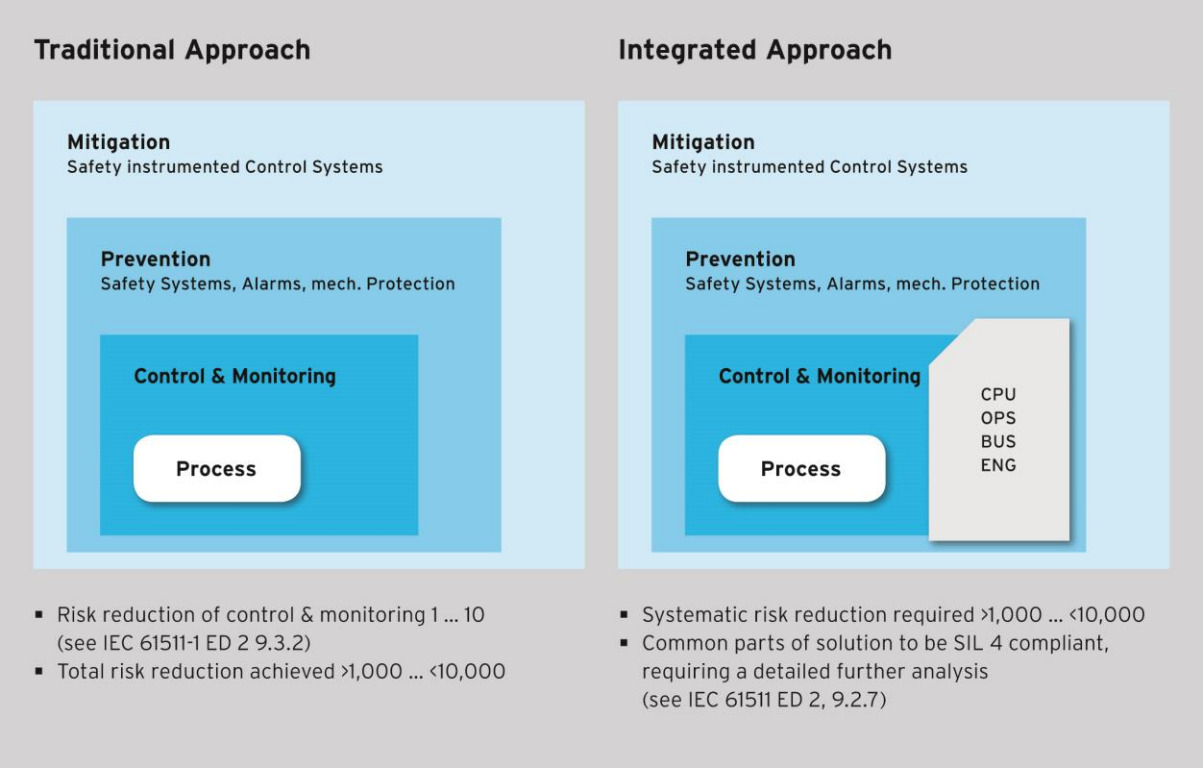

Abbildung 5

Zu beachten ist, dass in der IEC 61508 Anforderungen bezogen auf die Fehlerausfallrate bei Zufallsfehlern (Hardware) sowie auf systematische Fehler wie Konstruktions- und Softwarefehler festgelegt sind.

Während dieses Prozesses sind in IEC 61511 definierte Strukturen als Ausgangspunkt vorzufinden, auf deren Basis die durch das SIS zu realisierende erforderliche Risikominderung definiert wird.

Mathematisch gesehen gilt bei einer Gesamtanlage mit einem SIS nach SIL 3:
BPCS in Kombination mit einem SIS:

$$R_R = (> 1 \ldots > 10) * 1.000 => 1.000 \ldots < 10.000$$

R_R = Risiko Reduzierung

Bei Realisierung einer derartigen Anwendung mit einer homogenen integrierten Lösung ist zu fordern, dass, im Vergleich zu einer getrennten Lösung (air gapped), die gleiche Risikoreduzierung erreicht wird. Damit müssen die gemeinsamen Bestandteile der integrierten Lösung eine Risikominderung von 1.000 … 10.000 erreichen. Dies entspricht SIL 4.

Konsequenzen eines integrierten BPCS und SIS

Bei der integrierten Lösung sind gemeinsame Komponenten für das BPCS und SIS vorhanden. Je nach betreffendem Aufbau sind dies entweder die CPU, E/A-Busse oder die (oder Teile der) Software (z.B. Betriebssystem) und Symbolbibliotheken.

Man kann an dieser Stelle einwenden, dass unterschiedliche Komponenten (desselben Fabrikats) für das SIS und BPCS verwendet werden. Werden jedoch gemeinsame Elemente (z.B. Betriebssysteme, Bus-Protokoll) verwendet, müssen die systematischen Fähigkeiten dieser Komponenten den oben erwähnten Anforderungen entsprechen.

In der Praxis bedeutet dies, dass SIL-4-Anforderungen zu erfüllen wären. Das ist nach dem gegenwärtigen Stand der Technik für softwarebehaftete Funktionseinheiten nicht erreichbar!

Verringerung des Patch-Verwaltungsaufwands mit proprietären Systemen

Es ist zu beobachten, dass Betreiber immer komplexere Funktionen auf der Automatisierungsplattform realisieren. Handelsübliche Standardbetriebssysteme (COTS-Betriebssysteme) für Automatisierungsplattformen stellen eine breite Palette an Möglichkeiten bereit. Diese sind auf der Automatisierungsplattform meist weder nötig noch erwünscht, denn sie erhöhen die Komplexität der jeweiligen Anwendung. Es müssen häufig Aktualisierungen (Patches) installiert werden, um ggf. vorhandene Sicherheitslücken zu beseitigen. Im Falle eines SIS gilt, dass nach jeder Aktualisierung ein Nachweis über die ordnungsgemäße Funktion erbracht werden muss. Nur so lässt sich belegen, dass die Funktionalität des SIS nicht beeinträchtigt wurde. Dies bedeutet in der Regel, dass Tests durchgeführt werden, die dem Aufwand einer Inbetriebnahme der Anlage nahekommen. Mit Rücksicht darauf sollte das SIS so aufgebaut werden, dass möglichst wenige Updates und Patches erforderlich sind.

HIMA setzt keine COTS-Betriebssysteme ein. Die Laufzeitanwendungen von HIMA-Automatisierungsprodukten werden durch Betriebssysteme betrieben, die HIMA ausschließlich für HIMA-Produkte entwickelt hat. Diese Betriebssysteme unterstützen alle Merkmale, die zum Betrieb eines SIS erforderlich sind, enthalten aber keine weiteren Funktionalitäten. Diese eindeutige Konzentration macht HIMA-Produkte robuster, verringert die Sicherheitslücken aufgrund von Problemen bei der IT-Sicherheit und erfordert weniger Patches.

Empfehlungen zu Cybersecurity und Anlagensicherheit

Cybersecurity und Anlagensicherheit sind untrennbar miteinander verbunden. Die empfohlenen internationalen Standards zur Funktionalen Sicherheit für SPS-Systeme (IEC 61508), zu Sicherheitssystemen (IEC 61511) und zu Cybersecurity (IEC 62443) ermöglichen eine sichere und gesicherte Anlage.

Ziel ist es, einen robusten Anlagenschutz zu erreichen und Sicherheitsrisiken zu senken. Empfehlenswert ist daher das Konzept eigenständiger SIS- und BPCS-Einheiten – idealerweise von unterschiedlichen Herstellern – anstelle eines integrierten Systems vom selben Anbieter.

Aus Gründen der Anlagensicherung und Anlagensicherheit ist es für Unternehmen ratsam, auf ein Sicherheitssystem zu setzen, das ein proprietäres Betriebssystem nutzt. Selbstverständlich kann und muss ein derartiges System mit DCS-Produkten vollständig kompatibel sein. Es sollte anwenderfreundliche Entwicklungstools mit integrierten Funktionen für Konfiguration, Programmierung und Diagnose enthalten.

Anlagenbetreiber, die diese Empfehlungen umsetzen und internationale Standards einhalten, schützen Menschen, die Gesellschaft und die Umwelt – und gewährleisten ihre eigene finanzielle Sicherheit. Die gute Nachricht lautet: Hardware, Software und Fachkenntnisse dafür stehen heute zur Verfügung.

Über den Autor

Peter Sieber ist Vice President Global Sales & Regional Development bei HIMA. Er ist seit 1985 auf dem Gebiet der Fabrik- und Prozessautomatisierung tätig und Mitglied von Lenkungsausschüssen zur Funktionalen Sicherheit (IEC 61508) und IT-Sicherheit (IEC 62443). Sieber ist am Prozess zur Festlegung von Richtlinien zur Funktionalen Sicherheit und von IT-Sicherheitsrichtlinien für Anwendungen in der Prozessautomatisierung aktiv beteiligt.

Pressekontakt HIMA Headquarters

HIMA Paul Hildebrandt GmbH
Daniel Plaga
Pressereferent

Albert-Bassermann-Str. 28
68782 Brühl, Germany
Tel.: +49 6202 709-405
Fax: +49 6202 709-123
d.plaga@hima.com
www.hima.com