IT-Security Risk Assessment nach IEC 61511

Cyberattacke, reale Gefahr für die Prozessindustrie

Der zunehmende Einsatz von Ethernet und offenen Standardprotokollen in der Prozessindustrie macht Anlagen verletzlicher denn je. Bedrohungen, ob durch unbeabsichtigtes menschliches Versagen oder aktive bösartige Manipulation verursacht, können in Anlagen der Prozessindustrie fatale Folgen haben (Leo Wolfert/Fotolia)

Jede Kette ist nur so stark wie ihr schwächstes Glied. Die zunehmende Vernetzung der Systeme in der Prozessindustrie und der Anschluss ans Internet machen Anlagen verletzlicher denn je. Nicht nur wegen der Erfahrungen mit Stuxnet ist die IT-Sicherheit auch für Anlagenbetreiber ein heißes Thema. Der Hackerangriff auf ein deutsches Stahlwerk vor gut zwei Jahren hat beispielsweise deutlich gemacht, welche Gefahren von mangelnder IT-Sicherheit in Industrieanlagen ausgehen können. Die Angreifer brachten einen Hochofen unter ihre Kontrolle, sodass der Anlagenbetreiber selbst nicht mehr eingreifen konnte. Die Anlage ließ sich nicht herunterfahren und wurde stark beschädigt. Einerseits ist der wirtschaftliche Schaden durch einen solchen Angriff immens. Andererseits entsteht auch Mensch und Umwelt dadurch ein hohes Risiko, das es unbedingt zu vermeiden gilt. Hier setzt nun die geänderte Gesetzgebung an. Die 2016 revidierte Norm IEC 61511 fordert ein Security Risk Assessment hinsichtlich der IT-Security, also eine Risikobewertung, für Sicherheitssysteme (Safety Instrumented Systems - SIS). Was bedeutet das für Anlagenbetreiber der Prozessindustrie in Bezug auf bereits realisierte Sicherheitssysteme und bei der zukünftigen Integration?

Autorin:

Dipl.-Ing. (BA) Denise Rebstock, Projektleiterin bei der Rösberg Engineering GmbH

Sicherheitsrelevant: IT von Sicherheitssystemen

Um systematische und stochastische Fehler in einer Anlage zu vermeiden bzw. ihre Auswirkungen einzudämmen, macht die IEC 61508 (funktionale Sicherheit) konkrete Vorgaben. Die Norm bezieht sich auf elektrische, elektronische und programmierbare elektronische sicherheitsgerichtete Systeme. Dennoch suchte man Fehlerursachen bislang fast ausschließlich bei den in einer Anlage verbauten Hardwarekomponenten. Ein Sicherheitssystem (SIS) besteht aber nicht nur aus Aktoren, die im Notfall Anlagen in den sichern Zustand führen und Sensoren, die den Aktoren die dafür notwendigen Signale liefern. Eine entsprechende Steuerung übernimmt die sichere Kommunikation. Hier sollten daher weitere Fragestellungen nicht außer Acht gelassen werden: Beeinflussen Sicherheitslücken in der Software der Sicherheitssteuerung die gesamte funktionale Sicherheit einer Anlage? Und wenn ja, wo sind die Gefahren? Lassen sich mit einer HAZOP (hazard and operability study) Gefahren bezüglich Security analysieren und dementsprechende Maßnahmen zur Vermeidung bzw. Beherrschung in Sicherheitssystemen umsetzen, wie sie die revidierte IEC 61511 fordert? Können auch auf Softwareseite durch konsequenten Einsatz eines Functional-Safety-Management-Systems systematische Fehler vermieden und stochastische Fehler schneller entdeckt und eingedämmt werden?

Norm fordert Risikoeinschätzung der IT-Security von Safety Instrumented Systems

Anlagenbetreiber sollten Angriffe auf Industrieanlagen nicht nur wegen dem potentiellen wirtschaftlichen Schaden und den möglichen Gefahren für Mensch und Umwelt tunlichst vermeiden. Der einhergehende Imageschaden, der durch einen solchen Angriff und seine Folgen entsteht, könnte immens sein. Gleichzeitig ist die Gesetzgebung deutlich. Sie fordert, dass der Anlagenbetreiber eine regelmäßige Risikoeinschätzung hinsichtlich IT-Security seiner Sicherheitssysteme durchführen muss, um Risiken zu identifizieren. Die IEC 61511:2016 ist seit gut einem Jahr als internationaler Standard für die Prozessindustrie gültig; auf nationaler Ebene wird derzeit die VDI 2180 vorbereitet, um die Forderungen des Standards für Deutschland festzulegen. Für Sicherheitssysteme relevant ist vor allem der Abschnitt 8.2.4 der IEC 61511 (siehe Kastentext 1).

Risikoanalyse ist Pflicht des Betreibers

Allerdings bildet für viele die Umsetzung der Norm eine große Hürde, da sie Know-how in den Bereichen Prozessautomatisierung, funktionale Sicherheit und der IT-Security erfordert, das meist weit über die eigenen Kernkompetenzen hinausgeht. Dennoch ist der Anlagenbetreiber in der Pflicht sicherzustellen, dass seine Sicherheitssysteme nicht angreifbar sind. Betroffen sind Industrieanlagen im Neubau ebenso wie Bestandsanlagen. In beiden Fällen kann es sinnvoll sein, Experten von außen mit ins Boot zu nehmen. Denn laut Norm ist die Risikobeurteilung zwingend Teil einer Anlagenentwicklung im Lebenszyklus der funktionalen Sicherheit, muss aber auch bei jeder Änderung des Sicherheitssystems und in regelmäßigen Prüfungen wiederholt werden, um sicherzustellen, dass eine Anlage in Bezug auf die funktionale Sicherheit auf dem aktuellen Stand der Technik ist.

Externe Dienstleister wie beispielsweise die Rösberg Engineering GmbH können von der Entwurfsplanung bis hin zu Anlagenänderungen dabei helfen, die notwendigen Risikobeurteilung durchzuführen und für die Nachweispflicht sicher zu dokumentieren. Laut Forderung der Norm muss für Cybersecurity ebenso wie bei der funktionalen Sicherheit der gesamte Sicherheitslebenszyklus einer Anlage betrachtet werden. Daher ist es sinnvoll, den Berater für das Thema funktionale Sicherheit bereits frühzeitig mit ins Projekt zu nehmen. In Bezug auf Cybersecurity gilt es immer das gesamte Kommunikationsnetzwerk samt Systemsteuerung zu betrachten, mögliche Schwachstellen ausfindig zu machen und Sicherheits-

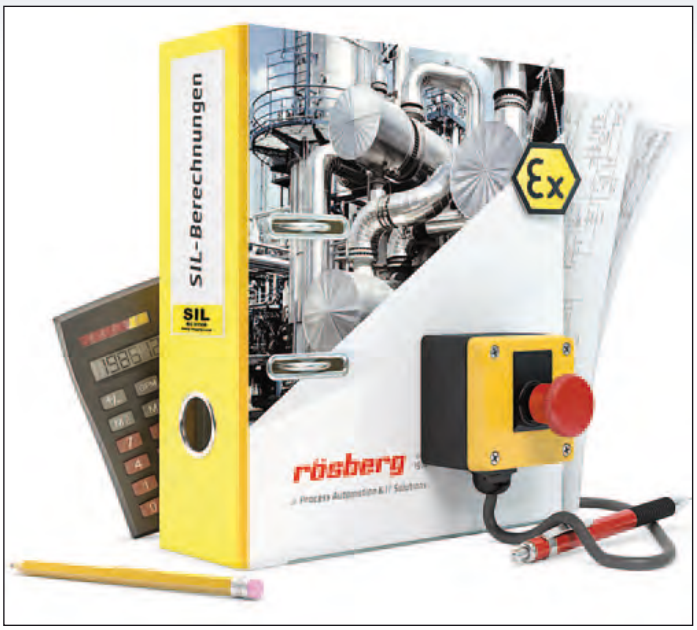

Bild 1: Zuverlässigkeit eines SIS kann die gesamte funktionale Sicherheit einer Anlage beeinflussen.(Quelle: Rösberg)

lücken zu schließen. Externe Dienstleister überzeugen an dieser Stelle nicht nur durch ihren neutralen Blick, sondern auch durch die Spezialisierung auf die Themen funktionale und IT-Sicherheit sowie den geübten Umgang mit den entsprechenden Vorgehensweisen.

Functional Safety Management System und IT-Security

Rösberg hat den Bedarf am Markt nach Unterstützung im Bereich funktionale Sicherheit frühzeitig erkannt. Daher beschäftigen sie sich seit Jahren nicht nur mit der Automatisierungsseite einer Anlage, sondern auch mit den dazugehörenden Themen rund um die funktionale Sicherheit. Experten für beide Bereiche arbeiten Hand in Hand. Die Kollegen aus dem Bereich funktionale Sicherheit waren bereits in zahlreichen Unternehmen bei der Integration eines Functional Safety Management-Systems verantwortlich. Das eingesetzte FSM-System baut auf den einschlägigen rechtlichen Verordnungen, Vorgaben und Normen auf und orientiert sich am Sicherheitslebenszyklus, wie er in der IEC 61511 definiert ist. Zum Vermeiden systematischer Fehler nutzt das FSM-System z. B. sogenannte Formatvorlagen. Diese helfen, potentielle Fehlerursachen beispielsweise in Instandhaltungsarbeiten systematisch abzufragen. Zudem hat Rösberg eigene Formatvorlagen entwickelt. Diese werden Anlagenbetreibern im Zuge der Beratung zur Verfügung gestellt. Ebenso wichtig wie diese Dokumentation ist die systematische Benennung von SIL-Leveln und Verantwortlichen für die Verifikation einzelner Schritte.

FSM-System plus IT-Security Risk Assessment

Das bewährte FSM-System haben die Automatisierungsexperten nun um ein Modul für IT-Security Risk Assessment erweitert. Auch hier fließt die über Jahre gesammelte Erfahrung ein. Mit dem Tool werden Anwender systematisch durch die Gefahrenanalyse und Risikobeurteilung geführt, um beispielsweise konkrete Angriffspunkte für Cyberattacken zu finden (Bild 2). Die Vorgehensweise kann ebenfalls aufdecken, wo Probleme im gesamten Sicherheitssystem, also auch in der Software des PLCs, Auswirkungen auf die funktionale Sicherheit der Gesamtanlage haben können. Mit diesen Informationen lässt sich dann klären, welche präventiven oder die Auswirkung reduzierenden Maßnahmen der Anlagenbetreiber ergreifen kann, um die funktionale Sicherheit einer Anlage auch im Falle von Problemen mit dem Sicherheitssystem zu gewährleisten. Wesentlicher Teil einer Gefahrenanalyse und Risikobeurteilung ist zudem die nachvollziehbare Dokumentation nach rechtlichen Vorgaben. Das kombinierte Know-how aus den Bereichen Cybersecurity und funktionaler Sicherheit macht das Unternehmen zum idealen Ansprechpartner für Fragen rund um die funktionale Sicherheit, FSM-Systeme und IT-Security Risk Assessment.

■ *Rösberg Engineering GmbH*
info.ka@roesberg.com
www.roesberg.com

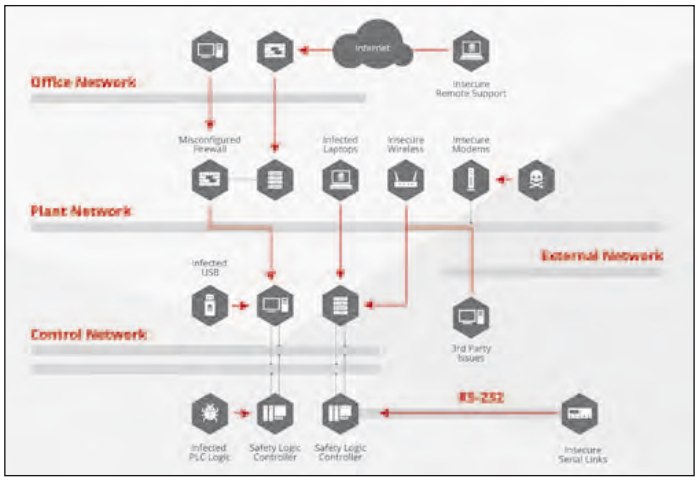

Bild 2: Mögliche „Einfallstore" für Cyberangriffe (Quelle: Rösberg)

Forderung für Sicherheitssysteme nach Abschnitt 8.2.4 der IEC 61511

Laut Norm muss sowohl für das Sicherheitssystem selbst als auch das BPCS (Basic Process Control System) samt aller mit dem Sicherheitssystem verbundenen Systeme eine Risikobeurteilung hinsichtlich der IT-Sicherheit durchgeführt werden. Es gilt alle möglichen Bedrohungen zu benennen, gleichgültig ob diese nun durch unbeabsichtigtes menschliches Versagen oder aktive bösartige Manipulation verursacht werden. Für diese Bedrohungen sind dann die möglichen Konsequenzen in Schadensausmaß, Wahrscheinlichkeit ihres Eintretens, Aufenthaltsdauer von Personen und Abwendbarkeit der potentiellen Gefahr zu bewerten. Dabei ist es wichtig, alle Phasen des Lebenszyklus des Sicherheitssystems zu betrachten, von der Entwicklung über Implementierung, Inbetriebnahme und Betrieb bis hin zu Wartung und Instandhaltung. Für all diese Phasen gilt es Maßnahmen zur Risikoreduzierung festzulegen und entsprechend zu dokumentieren. Um ein sicheres vernetztes System zu gewährleisten, muss folgendes berücksichtigt werden: Die Leistungsfähigkeit, Diagnose- und Fehlerbehandlung des Sicherheitssystems, der Schutz vor unerwünschten Programmveränderungen, der Schutz der Daten zur Fehlersuche an den Sicherheitsfunktionen und der Schutz vor der Umgehung von Beschränkungen, damit Alarme und die manuelle Abschaltung nicht deaktiviert werden. Zudem gilt es, die Aktivierung bzw. Deaktivierung des Lese- und Schreibzugriffs mithilfe eines ausreichend sicheren Verfahrens zu gewährleisten.

Sehr konkrete Vorgaben für die Risikoanalyse zum Schutz vor Cyberattacken macht die IEC 62443 (Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme), auf die die IEC 61511 in diesem Zusammenhang verweist: Generell darf das IT-Security Risk Assessment des Sicherheitssystems ausdrücklich Teil einer Risikoanalyse der gesamten Prozessautomatisierung einer Anlage sein. Somit haben es die Unternehmen mit der Umsetzung der IEC 61511 leichter, die bereits ein Functional Safety Management System in ihrem Unternehmen implementiert haben.