Bild: phaspirit-Fotolia.com

Cyber-Bedrohungen von PLT-Sicherheitseinrichtungen sind ein realistisches Szenario

NA-163-Verfahren bietet praxistaugliche Risiko-Beurteilungsmethode

Cyber Security für funktionale Sicherheit

Die Digitalisierung in der Prozessleittechnik (PLT) schreitet immer weiter voran. Der Segen der Digitalisierung hat jedoch auch Schattenseiten. Gerade beim Betrieb industrieller Anlagen spielt die Sicherheit eine große Rolle für einen störungsfreien und sicheren Produktionsprozess. PLT-Sicherheitseinrichtungen, die funktionale Sicherheit (Safety) gewährleisten sollen, müssen heute auch unter dem Aspekt der IT-Sicherheit (Security) betrachtet werden (Security for Safety).

PLT-Sicherheitseinrichtungen (Safety Integrated Systems, SIS) schützen Anlagen, Umwelt und Personal der chemischen Industrie vor nicht tolerierbaren Schäden. Die Integrität der PLT-Sicherheitseinrichtungen ist neuerdings Gefährdungen aus dem Cyberraum ausgesetzt. Standards wie IEC 61508/61511 tragen dieser Erkenntnis Rechnung und fordern IT-Risikobeurteilungen mit entsprechenden Maßnahmen. Namur hat mit dem Namur Arbeitsblatt 163 ein Handlungswerkzeug geschaffen, das eine effektive und ressourcenschonende IT-Risikobeurteilung ermöglicht. Darüber hinaus werden konkrete Handlungsmaßnahmen anhand einer Checkliste formuliert.

Wie „secure" ist die Safety?

PLT-Sicherheitseinrichtungen (Safety Instrumented Systems) werden in der chemischen Industrie eingesetzt um – unabhängig von anderen Schutzmaßnahmen – nicht tolerierbare Schäden an Anlagen, Umwelt und Menschen abzuwenden. Sie bestehen aus Komponenten, die eine mehr oder weniger große Angriffsfläche für Cyber-Gefährdungen darstellen. Angesichts der möglichen Auswirkungen, die eine kompromittierte PLT-Sicherheitseinrichtung in der chemischen Industrie nach sich ziehen würde, müssen folgende Fragen beantwortet werden:

- Wie sicher (secure) ist meine PLT-Schutzeinrichtung?
- Wie sicher muss sie – mindestens – sein?

Für die Beantwortung dieser Fragen benötigen Anlagenbetreiber neben ausgewiesenem Expertenwissen auch die erforderlichen Kapazitäten. Beide Ressourcen –

Kompetenz + Kapazität – sind in der Regel knapp bemessen. Mit dem NA-163-Verfahren der Namur zur Risikobeurteilung wird „Security for Safety“ für die Betreiber leichter umsetzbar.

Ziele des NA-163-Verfahrens

IEC 61511 „Funktionale Sicherheit für die Prozessindustrie“ fordert eine IT-Risikobewertung für SIS, liefert jedoch keine Empfehlungen zu den Details der Bewertung. Diese Lücke schließt das Namur-Arbeitsblatt 163. Ziel des Arbeitsblattes ist die Bereitstellung einer praxistauglichen Risiko-Beurteilungsmethode für PLT-Ingenieure. Der betriebliche Ablauf soll durch die Anwendung möglichst wenig beeinflusst werden. Die IT-Risikobeurteilung bildet die Grundlage für eine Erhöhung der Widerstandsfähigkeit der PLT-Sicherheitseinrichtung gegen IT-Bedrohungen. Die Besonderheit: Die Durchführung des NA-163-Verfahrens ist innerhalb eines Tages pro System ohne tiefere Cyber-Security-Kenntnisse durchführbar. Vorhandene Schwachstellen werden aufgedeckt und konkrete Verbesserungsmaßnahmen anhand einer Checkliste vorgeschlagen. Mit dem Namur-Arbeitsblatt sollen IT-Risikobeurteilungen selbstverständlicher Teil des Lebenszyklus einer PLT-Sicherheitseinrichtung werden.

PLT-Sicherheitseinrichtung

Beginnt man mit einer IT-Risikobeurteilung für PLT-Sicherheitseinrichtungen, stellt sich zuallererst die Frage, welche Komponenten zur PLT-Sicherheitseinrichtung gehören und welche nicht. Sensoren, Aktoren und die programmierbare Steuerung bilden den Kern der PLT-Sicherheitseinrichtung (Zone A). Aber auch das Programmiergerät und die Konfigurationseinrichtungen für Sensoren und Aktoren beeinflussen die Sicherheitsfunktion. Datenverbindungen zu Systemen im Umfeld der PLT-Sicherheitseinrichtung müssen betrachtet werden (Zone B). Dienste wie der Verzeichnisdienst zur Regelung des Benutzerzugriffs, Update-Dienste für Virenpattern und Betriebssystem-Updates, Zeitsynchronisation und Sicherung/Wiederherstellung sind für die Security der PLT-Sicherheitseinrichtung relevant und damit im Betrachtungsumfang (befinden sich üblicherweise in Zone C). Auch die Integrität von Daten (z. B. Applikationsprogramm, Risiko-Analysen, Anlagendokumentation) spielt – zusammen mit der Organisation und Personen – eine Rolle und wird entsprechend auf Risiken beurteilt. Gegenstand der Risikoanalyse sind also Komponenten (zumindest Zone A & B), Datenverbindungen, Dienste sowie Prozesse und Personen rund um die PLT-Sicherheitseinrichtung.

KURZ UND BÜNDIG **NAMUR-ARBEITSBLATT 163**

Das Namur-Arbeitsblatt 163, das sich mit der Cyber Security für Safety Systeme beschäftigt, beantwortet Fragen wie

- Häufigkeit der Risikobeurteilung
- Voraussetzung/Qualifikation für die Durchführung einer Risikobeurteilung
- Prozess der Risikobeurteilung
- Festlegung von Muss- und Kann-Maßnahmen
- Notwendigkeit der Beurteilung von Engineering- und Konfigurationssystemen und Daten bzw. Dateien
- Organisatorische Verantwortung der Risikobeurteilung
- Auswirkungen eines kompromittierten PLT-Sicherheitssystems
- Zusammenhang mit konventionellen Automatisierungssystemen

Der Begriff „Risiko“

Risiko wird landläufig als Produkt aus der Schwere der negativen Auswirkung und der Eintrittswahrscheinlichkeit gebildet. Die negativen Auswirkungen einer Chemieanlage werden in HAZOP-Analysen ermittelt. Somit kann die Auswirkung einer kompromittierten PLT-Schutzeinrichtung als bekannt vorausgesetzt werden. Schwieriger gestaltet sich die Abschätzung der Eintrittswahrscheinlichkeit. Dies hat mehrere Ursachen: Erstens liegt einem Cyber-Security-Risiko häufig ein systematischer Fehler bzw. Mutwilligkeit zugrunde, deren Wahrscheinlichkeit kaum abzuschätzen ist. Belastbares Zahlenmaterial über Zwischenfälle ist nicht verfügbar.

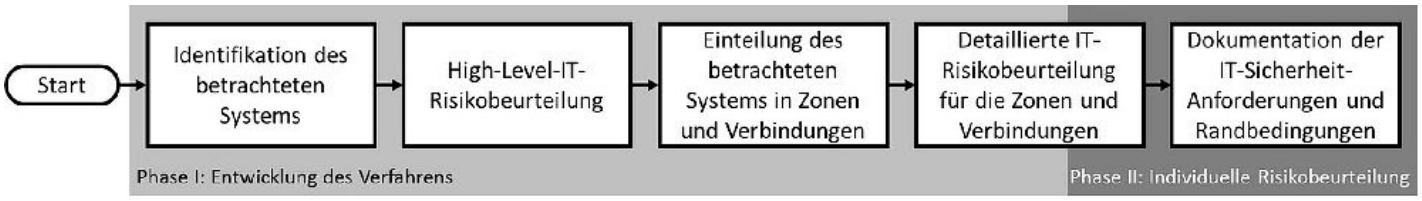
Zum zweiten werden PLT-Sicherheitseinrichtungen der chemischen Industrie fast ausschließlich mit Anforderungsrate „niedrig“ betrieben. D. h. der Anforderungsfall ist äußerst selten.

Schutzziele und Maßnahmen

Security verfolgt im Wesentlichen die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Die Funktionale Sicherheit zielt primär auf die Integrität der PLT-Sicherheitseinrichtung ab. D. h. Integrität von Sensor, Aktor und Sicherheits-SPS ist oberstes Schutzziel. Aus betrieblicher Sicht ist natürlich die Verfügbarkeit dieser Komponenten gleichfalls relevant, da das – unnötige – Auslösen der PLT-Sicherheitseinrichtung in den meisten Fällen einen Betriebsstillstand verursacht. Auf den ersten Blick erscheint die Vertraulichkeit der Daten rund um ein

Bild: Anapur

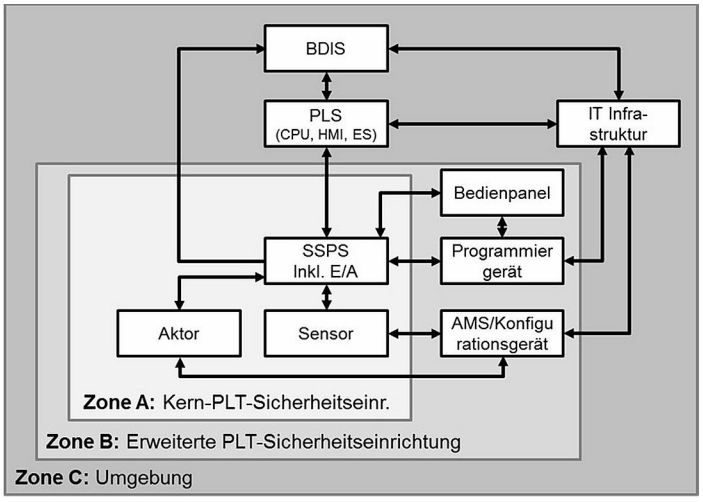
Die Digitalisierung ist zum grundlegenden Innovationstreiber in nahezu allen Industrien geworden. Sicherheitslücken stellen große Risiken dar.



Schritte des Risikobeurteilungsverfahrens

PLT-Sicherheitssystem nicht relevant. Aus der Perspektive eines Angreifers sind für eine wirkungsvolle Manipulation der PLT-Schutzeinrichtung die Kenntnis von Anlagendokumentation, Risikoanalyse und die Dokumentation der PLT-Schutzeinrichtung sehr hilfreich. Insofern sind auch Vertraulichkeitsaspekte zu berücksichtigen.

Maßnahmen zur Minderung von IT-Risiken werden als Teil des Managementsystems für Funktionale Sicherheit an Komponenten, Daten, Organisationen, Personen und Prozessen appliziert. Die Wirksamkeit dieser Maßnahmen orientiert sich an dem schwächsten Glied in der Kette. Dies trifft sowohl technisch als auch organisatorisch zu. Security-Maßnahmen sollten über Organisationsgrenzen hinweg (Hersteller, Systemintegrator, Betreiber) implementiert sein.



Zonenmodell nach Namur NA 163, (Quelle: Namur AK 4.18, NA 163)

Prinzipien bei der Umsetzung

Je weniger Komponenten die PLT-Sicherheitseinrichtung enthält, desto weniger Sicherheitsmaßnahmen werden notwendig sein, um diese zu schützen. Diesem Prinzip folgend ist die Verringerung von Verbindungen, Hard- und Softwarekomponenten und Personen mit Zugriff auf das absolut notwendige Minimum die erste und effizienteste Maßnahme.

Die Kompetenz der Organisationen und Personen, die eine PLT-Sicherheitseinrichtung planen, implementieren, betreiben oder warten, muss der Komplexität der Einrichtung gewachsen sein. Grundbaustein für Kompetenz ist die Kenntnis und Dokumentation der Systemkomponenten (Hard- und Software inkl. Versionsstände, Daten und Personen mit Zugang und/oder Zugriff, Verbindungen) sowie deren Konfiguration (Applikationsprogramme, Firewallregeln, Sensor-Aktor-Konfiguration, Bus-Konfiguration etc.). Auf Basis der Dokumentation werden regelmäßige Schulungen und Übungen durchgeführt.

Das Dilemma der Trennung

Nach IEC 61508/61511 sollen PLT-Sicherheitseinrichtungen getrennt und damit unabhängig und rückwirkungsfrei von ihrer Umgebung (z. B. Prozessleitsystem, IT-Infrastruktur etc.) betrieben werden. Denn es ist immer davon auszugehen, dass die Umgebung kompromittiert ist. In der Praxis ist dies insbesondere für Programmiergeräte und Konfigurationsdaten kaum einzuhalten. Insbesondere Sicherheitsmaßnahmen wie Verzeichnisdienst, Zeitsynchronisation, Betriebssystemupdates, Firewall-Management, Event-Monitoring werden nicht exklusiv für das PLT-Sicherheitssystem betrieben („gemeinsam genutzte Komponenten"). Unter „gemeinsam genutzt" wird hier die Kombination von „Sicherheits- und betrieblichen" Funktionen innerhalb einer Komponente verstanden. Der Umgang mit diesen Komponenten muss einen entsprechend hohen Grad an Zuverlässigkeit aufweisen, um möglichst geringe Rückwirkungen anderer Systeme auf das PLT-Sicherheitssystem zu gewährleisten. Nur dann zahlt sich die Nutzwirkung gemeinsam genutzter Komponenten aus.

Ausblick

Die Digitalisierung ist zum grundlegenden Innovationstreiber in nahezu allen Industrien geworden. Sicherheitslücken stellen große Risiken dar. Derzeit werden reaktiv Sicherheitslücken mit aufwändigen und teuren Patches geschlossen. Für die Zukunft reift die Erkenntnis, dass die Sicherheit bereits bei der Entwicklung und Integration einer PLT-Sicherheitseinrichtung viel stärker berücksichtigt werden muss. Aus Sicht der chemischen Industrie sollen zukünftige Generationen von PLT-Sicherheitseinrichtungen bereits „Security by Design" (d.h. Security ab Werk) mitbringen. Die Anzahl der zur Sicherung notwendigen Zusatzmaßnahmen kann damit minimiert und Risikobeurteilung stark vereinfacht werden.

www.prozesstechnik-online.de
Suchwort: cav0617anapur

AUTOR
ERWIN KRUSCHITZ
Mitglied im Namur AK 4.18 Automation Security und Vorstand,
Anapur

ALLES IM RICHTIGEN FLUSS

Elektrische Stellantriebe für alle Industriearmaturen

Zuverlässig und langlebig. AUMA bietet eine breite Palette von Stellantrieben.

- Maßgeschneiderte Lösungen durch modulares Konzept
- Einfache Energieversorgung
- Niedrige Betriebskosten
- Integration in alle gängigen Leitsysteme
- Weltweiter Service

Mehr über unsere
Automatisierungslösungen