Presse-Information

Press release ● Information de presse

Kontakt/Contact:
Dr. Kathrin Rübberdt
Tel. ++49 (0) 69 / 75 64 - 2 77
Fax ++49 (0) 69 / 75 64 - 2 72
e-Mail: presse@dechema.de

Trendbericht Januar 2018

Cybersicherheit im Cyberraum – Herausforderungen für die Anlagensicherheit

Erinnern Sie sich noch, wie Tom Cruise in „Minority Report“ über die holografischen Bildschirme wischte oder auf der „Enterprise“ der Replikator mehr Kaffeevarianten lieferte als ein Wiener Kaffeehaus? Nicht nur Kinobesucher träumen von einer Zukunft, in der Maschinen und digitale Anwendungen den Alltag erleichtern; Wissenschaftler arbeiten intensiv daran, diese Zukunft wahr werden zu lassen.

Die ersten Schritte sind längst getan: E-Mail, Internet und GPS sind selbstverständliche Alltagstools, das gerade mal zehn Jahre alte Smartphone nicht mehr wegzudenken. Gleichzeitig hat sich die Welt beschleunigt. Informationen werden in Echtzeit ausgetauscht, schnell, jederzeit, und das weltweit.

Allerdings hat diese neue und aufregende Welt auch Schattenseiten. Sind die Netzwerke unzureichend gesichert, können unbefugte Außenstehende an vertrauliche und persönliche Informationen gelangen.

Was für das offene WLAN am Bahnhof und die Privacy-Einstellungen bei Facebook gilt, lässt sich auf die Industrie übertragen: Auch dort werden immer mehr Konzepte entwickelt, die eine optimale Zusammenarbeit zwischen Mensch, Maschine und IT-Systemen gewährleisten. Gleichzeitig wird der Bedarf an individualisierten Produkten immer größer. Um für die anstehenden Veränderungen gerüstet zu sein, müssen Produktions- und Logistikprozesse neu überdacht und umstrukturiert werden. Das Schlüsselwort ist hierbei „Industrie 4.0“. „Cyber-physische Produktionssysteme“ sollen zukünftig neue Produktionsprozesse steuern.

Unter „cyber-physischen Produktionssystemen“ wird die Verknüpfung von realen (physischen) Prozessen mit informationsverarbeitenden Prozessen verstanden. Dies wird über globale und jederzeit miteinander verbundene Informationsnetze realisiert. Die physischen Prozesse bestehen aus eingebetteten Systemen, die in einem technischen Kontext eingebunden sind. Die virtuellen Prozesse sind Daten, Informationen und Dienste, die über das Informationsnetz bereitgestellt werden. Demzufolge besitzen die cyber-physischen Produktionssysteme den Vorteil, dass sie sich schnell und effizient an

geänderte Anforderungen anpassen können. In einer Welt, die sich in Sekunden ändern kann, ist diese Systemeigenschaft besonders wichtig, vor allem in der Prozessindustrie. Die Wahrnehmung von fehlerhaften Prozessabläufen wird durch Sensoren ermöglicht und führt nicht nur zur Selbstoptimierung und Gestaltung von Produkten, Maschinen und Anlagen, sondern sorgt auch für die nötige Sicherheit der Anlagen.

Im BMBF-Projekt „Industrie 4.0“ liest sich das so, dass „Maschinen […] miteinander kommunizieren, sich gegenseitig über Fehler im Fertigungsprozess informieren, knappe Materialbestände identifizieren und nachbestellen“. Denn erst „das ist eine intelligente Fabrik.“ Die Digitalisierung von Prozessen führt „durch das Internet getrieben“ zum Zusammenwachsen der „realen und virtuellen Welt zu einem Internet der Dinge“. Über dieses wird die Quervernetzung von einzelnen Prozessschritten erzielt und ermöglicht dadurch den Zugriff für Außenstehende auf die Produktionsanlagen.

Neue Technik = neue Sicherheitsrisiken?

Wenn aber künftig auch in der chemischen Industrie immer mehr im Cyberraum stattfindet und wenn die Pumpe womöglich auch noch drahtlos mit dem Sensor kommuniziert – wie sieht es dann mit der Anlagensicherheit aus?

Vor der Inbetriebnahme einer Anlage erarbeiten Fachleute ein Sicherheitskonzept, das die nötigen Schutzmaßnahmen umfasst. Das Ziel ist es, Risiken zu erkennen, zu bewerten und geeignete Maßnahmen zur Minimierung von Ereignissen zu treffen. Eine Anlage sollte nach Stand der Technik montiert, installiert und betrieben werden. Um dem gerecht zu werden, ist vor dem Betrieb der Anlage eine Gefährdungsbeurteilung durchzuführen. Dazu gehören Risikoanalysen, Auswirkungsbetrachtungen und Ausbreitungsrechnungen von Chemikalien, Brand- und Explosionsschutz sowie die Bewertung der durchgeführten Reaktionen. Am Ende der Sicherheitsanalyse steht das Sicherheitskonzept, realisiert unter anderem mittels Sicherheitseinrichtungen der Prozessleittechnik (PLT).

Die Hauptaufgabe der Prozessleittechnik besteht darin, die Prozesse zu überwachen und zu steuern. PLT-Sicherheitseinrichtungen sind Schutzvorrichtungen, die bei Abweichung eines Sollzustands einen Alarm auslösen oder eine Sicherheitsfunktion. Die Aufgabe der Sicherheitseinrichtung ist es, einen Fehlzustand der Anlage zu verhindern. Besonders bei chemischen Prozessen kann die Abweichung von Reaktionstemperatur, Druck und Füllstand verheerende Folgen haben. Um so wichtiger ist, solche Abweichungen frühzeitig zu erkennen und möglichst zu vermeiden.

Die Ursachen von Gefährdungen und Schäden können vielseitig sein. In explosionsgefährdeten Bereichen kann eine Zündung des Luft-Gas-Gemisches oder Luft-Staub-Gemisches erfolgen und eine Explosion verursachen. Übersteigt der Druck die zulässigen Höchstwerte, kann es zu Undichtigkeiten und Leckagen kommen.

DECHEMA Gesellschaft für Chemische Technik und Biotechnologie e.V.
Theodor-Heuss-Allee 25 • 60486 Frankfurt am Main • Germany • T + 49(0)69 75 64-0 • F +49(0)69 75 64-201 • presse@dechema.de
www.dechema.de

Die Sicherheit von chemischen Anlagen hat oberste Priorität und wird durch sicherheitstechnische Normen und Regelwerke definiert. Im Bereich der „Funktionalen Sicherheit“ bildet die IEC 61508/61551 die Basis für die Sicherheitsnorm von Sicherheitseinrichtungen. Von „funktionaler Sicherheit“ spricht der Experte, wenn der Schutz vor Gefährdungen und Schäden durch eine korrekte und sicherheitsrelevante Steuerung einer Sicherheitseinrichtung gewährleistet ist.

Das Maß für die erreichte funktionale Sicherheit einer Anlage ist die Wahrscheinlichkeit aus gefährlichen Ausfällen, Fehlertoleranz und Qualität, der sogenannte „Safety Integrity Level“ SIL. Im Fehlerfall sollte die Sicherheitseinrichtung korrekt funktionieren und die Anlage in einem sicheren Zustand verweilen lassen oder wieder in den sicheren Zustand bringen. Um eine möglichst hohe funktionale Sicherheit zu erzielen, müssen systematische Fehler vermieden und zufällige Fehler beherrscht werden.

In den vergangenen Jahren ist im Bereich der chemischen Industrie die eingesetzte und zugrundeliegende Technik von Produktionsanlagen, System und Maschinen kontinuierlich weiterentwickelt worden. Das Abrufen, Erfassen und Verschicken großer Datenmengen ist ohne Probleme möglich. So kann auf wichtige Daten, Netzwerke und Baupläne zugegriffen und gleichzeitig können mit Experten über eine größere Distanz Informationen ausgetauscht werden. Die Überwachung der Anlage erfolgt über die Nutzung drahtlos vernetzter Tablets und Smartphones, die die Kontrolle von Anlagen, die Prüfung von Maschinen sowie Wartungs-, Inspektions- und Reparaturarbeiten einfach durchführbar macht.

Allerdings erhöhen veraltete Technologien, Fehlkonfigurationen von Systemen oder unzureichende Schulung der Mitarbeiter das Risiko eines unbefugten Eingriffs. Die Kontrolle über das ganze Anlagensystem kann durch den Zugang auf ein Industrial Automation Control System (IACS) zu hohen Kosten durch Produktionsausfälle und Anlagenschäden führen.

Cyber Security – Security for Safety

Die chemische Industrie reagiert auf den Wandel. Angesichts der steigenden Gefährdung im Bereich der IT-Sicherheit stellt sich in der Anlagen- und Prozesstechnik die Frage, ob und inwieweit die Integrität von PLT-Sicherheitseinrichtungen gefährdet sein könnte. Ein Schutzkonzept für die chemischen Anlagen ist erforderlich. Die Automatisierungstechnik ermöglicht in der funktionalen Sicherheit (Safety) die Sicherung der Geräte oder Anlagen, damit keine Gefahr für Mensch und Umwelt entsteht. Im Gegensatz dazu befasst sich die IT-Sicherheit (Security) mit der Abwehr von Gefahren, die dem System von außen zugefügt werden können. In beiden Bereichen kann durch den unbefugten Zugriff das System beeinflusst werden, so dass eine Fehlfunktion verursacht wird.

DECHEMA Gesellschaft für Chemische Technik und Biotechnologie e.V.
Theodor-Heuss-Allee 25 • 60486 Frankfurt am Main • Germany • T + 49(0)69 75 64-0 • F +49(0)69 75 64-201 • presse@dechema.de
www.dechema.de

Die drei wichtigen Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Mithilfe von Normen und Standards kann die Sicherheitsgrundlage für die firmenübergreifende Vernetzung geschaffen werden. Das Ziel der Experten auf dem Gebiet der Cyber-Sicherheit ist die sichere und zuverlässige Gestaltung von automatisiertem Datenaustausch vernetzter Produktionssysteme und der damit verbundene Schutz von Produkten und Anlagen.

In der chemischen Industrie werden PLT-Sicherheitseinrichtungen eingesetzt, um Personen, Umwelt und Anlagen vor Schäden zu schützen. Den Mittelpunkt von PLT-Sicherheitseinrichtungen bilden Komponenten wie Sensoren, Aktoren und programmierbare Steuerungselemente. Diese bieten eine Angriffsfläche für Cyber-Angriffe. Konfigurationseinrichtungen für Sensoren und Aktoren beeinflussen die Sicherheitsfunktion, sodass die Datenverbindung zu Systemen im Umfeld geschützt werden müssen. Verzeichnisdienste zur Regelung des Benutzerzugriffs, Update-Dienste für Virenpatter und Betriebssystem-Updates, Zeitsynchronisation und Sicherungen bzw. Wiederherstellungen sind wichtige Elemente, die in einer Risikoanalyse und Anlagendokumentation einbezogen werden müssen. Eine kleine Änderung im System kann zum Ausfall einer PLT-Sicherheitseinrichtung führen und die Sicherheit der Anlage ist gefährdet.

Je weniger Komponenten eine PLT-Sicherheitseinrichtung enthält, desto weniger Sicherheitsmaßnahmen werden zum Schutz benötigt. Deshalb ist eine effektive Schutzmaßnahme, die Zahl von Verbindungen, Hard- und Softwarekomponenten und Personen möglichst gering zu halten.

In der Theorie sollten PLT-Sicherheitseinrichtungen getrennt und unabhängig von der Umgebung betrieben werden. Die Theorie in die Praxis umzusetzen, erweist sich jedoch in vielen Fällen als problematisch. Der Erfahrungsaustausch zwischen Naturwissenschaftlern, Ingenieuren und IT-Experten hat eine Schlüsselfunktion in der Entwicklung von Lösungsansätzen zur Absicherung von Anlagen. Die Arbeitsausschüsse der NAMUR und der KAS haben durch ihre Arbeiten an Empfehlungen und Normen die Basis für die IT-Sicherheit der Anlagen gelegt. Deren Umsetzung verschafft dem Anlagenbetreiber eine gewisse Sicherheit für seine Systeme.

Fazit: Die Cyber-Sicherheits-Welt der Sicherheitstechnik ist noch im Aufbau und eine gewisse Unklarheit über die Ausmaße von unbefugten Angriffen ist vorhanden. Erst die Kombination aus funktionaler Sicherheit und dem Schutz der IT-Systeme schafft ein adäquates Sicherheitsniveau in Industrieanlagen. Das vorhandene Wissen nutzen und einen gegenseitigen Ehrfahrungsaustausch zu bewahren, ist der Weg zur Optimierung von Sicherheitseinrichtungen.

Auf der ACHEMA 2018 vom 11. Juni bis 15. Juni in Frankfurt am Main stellen Unternehmen die neu entwickelten Produkte, Technologien und Systemlösungen zur IT-Sicherheit vor.

DECHEMA Gesellschaft für Chemische Technik und Biotechnologie e.V.
Theodor-Heuss-Allee 25 • 60486 Frankfurt am Main • Germany • T + 49(0)69 75 64-0 • F +49(0)69 75 64-201 • presse@dechema.de
www.dechema.de

http://www.achema.de

10.650 Zeichen inkl. Leerzeichen

Die Trendberichte werden von internationalen Fachjournalisten zusammengestellt. Die DECHEMA ist nicht verantwortlich für unvollständige oder falsche Informationen. Die Trendberichte können unentgeltlich für redaktionelle Zwecke unter Angabe der Quelle genutzt werden (s. dazu auch www.achema.de)

DECHEMA Gesellschaft für Chemische Technik und Biotechnologie e.V.
Theodor-Heuss-Allee 25 • 60486 Frankfurt am Main • Germany • T + 49(0)69 75 64-0 • F +49(0)69 75 64-201 • presse@dechema.de
www.dechema.de