Bild: ©cookelma/Photodune.net

*Funktionale Sicherheit und Cyber Security*

# Sicherheit 4.0 in der Industrie

***Was haben der Stromausfall in der Ukraine 2015 und NotPetya 2017 gemeinsam? Sie zählen zu den bislang wirksamsten Attacken auf Prozesssteuerungsssysteme. Da IT und das Internet unerlässliche Eckpfeiler der vierten industriellen Revolution sind, muss die vernetzte Industrie umdenken. Denn Industrie 4.0 lässt sich nur realisieren, wenn funktionale Sicherheit und Cyber Security integriert betrachtet werden.***

Industrielle Verarbeitungs-, Herstellungs- und Produktionssysteme bestehen heute aus zahlreichen Hardware- und Software-Komponenten, die für die Erzeugung und Bereitstellung von Produkten oder Dienstleistungen unerlässlich sind. Dieser Umstand wiederum sorgt für eine Fehleranfälligkeit, die den Prozess in geringfügigem oder schwerwiegendem Maß beeinträchtigen können. Einige sind in der Lage, für die gesamte Anlage akute Gefahrensituationen heraufzubeschwören. Selbst Anlagen mit rigorosen funktionalen Sicherheitskonzepten sind nicht automatisch gegen Cyber-Attacken gefeit. Ein industrieller HMI-PC mit ausgereiften und ordnungsgemäß implementierten Steuersystemen ist ohne Cyber-Security-Schutz anfällig für Angriffe. Dazu ist nicht einmal die Kompromittierung sicherer Verarbeitungssysteme notwendig. Sinnlose Befehle an die übergeordnete Steuerung von RTUs sind ausreichend, um den gesamten Prozess in der Produktion lahmzulegen. Das bedeutet: Prozesse oder Hardware-Komponenten, die auf irgendeine Weise in Computer- oder Internettechnik integriert oder mit ihr verbunden sind, lassen sich nicht mehr länger als sicher im herkömmlichen Sinn betrachten, sofern die Steuerungssysteme nicht auch in puncto Cyber Security abgesichert sind. Problematisch für die integrierte Absicherung von Industrie 4.0 ist, dass sich die Schutzziele von Funktionaler Sicherheit und Cyber Security stark voneinander unterscheiden – und vielfach Funktionale Sicherheit noch Priorität hat vor Cyber Security.

## Unternehmensinterne IT-Systeme

Die Lebensdauer von Steuerungssystemen übersteigt die eines unternehmensinternen IT-Systems nicht selten um das Zehnfache. Software-Aktualisierungen werden hier nur sehr unregelmäßig oder gar nicht durchgeführt. Diese Praxis wiederum steht im Gegensatz zur stetig steigenden Patches-Anzahl für unternehmensinterne IT-Systeme. Die Anwendung unternehmensinterner IT-Technik, -Tools und -Verfahren kann desaströse Auswirkungen auf betriebstechnische Systeme haben. Gleiches gilt aber auch umgekehrt. Bei funktionaler Sicherheit geht es darum, die Menschen vor den Auswirkungen der Technik zu schützen, z.B. durch Fehlfunktionen von Maschinen und Anlagen, hervorgerufen durch ungewollte oder unberechtigte Eingriffe in die IT-Komponenten. Funktionale Sicherheit sichert gewünschte Abläufe wie vorgesehen ab und gewährleistet, dass beim Auftreten von Fehlern entsprechende Maßnahmen greifen, wie z.B. das Abschalten von Anlagen. Cyber Security zielt darauf ab, Fabrikautomation und Prozesssteuerungen abzusichern. Hier geht es um Schutz und Verfügbarkeit von Kontroll- und Steue-

**Auszug aus dem SPS-MAGAZIN**, Fachzeitschrift für Automatisierungstechnik, Ausgabe 1+2/2018.

rungssystemen gegen absichtliche herbeigeführte oder ungewollte Fehler – z.B. durch Cyber-Kriminelle und Hacker. Ziel muss es sein, eine Störung oder gar einen Ausfall der Produktion zu verhindern. Vor dem Hintergrund aktueller Sicherheitsvorfälle wird klar: Kein Produktionsunternehmen kann sich mehr leisten, Cyber Security zu vernachlässigen.

## Normenkataloge und Standards

Da Hacker jeglicher Art mittlerweile ein gesteigertes Interesse an industriellen Prozessen und Steuersystemen demonstrieren, müssen diese Bedrohungen analysiert und auf eine Weise gehandhabt werden, die die Identifizierung der wichtigsten potenziellen Schwachstellen und Risiken für ein Unternehmen ermöglicht. Neu entwickelte Standards wie IEC62443 – ein Normenkatalog, der sich mit den Verfahren zur Sicherung industrieller Steuersysteme befasst – und IEC61508 – ein Standard, der vom Ausfall der Sicherheitsfunktionen eines Geräts ausgeht – bieten eine strukturierte Herangehensweise für die Integration von Funktionaler Sicherheit und Cyber Security. Betreiber, Anbieter und Systemintegratoren industrieller Automation können diese Problemstellung nur auf effiziente und kostengünstige Art und Weise bewältigen, wenn sie diese und ähnliche Normen verstehen lernen bzw. annehmen. Wichtig: Standards der funktionalen Sicherheit bzw. Cyber Security sollten über den gesamten Produkt- oder Prozesslebenszyklus hinweg – von der Spezifizierung über das Design bis hin zu Betrieb und Wartung – berücksichtigt werden. Dazu ist eine effiziente Risiko- und Gefahrenanalyse bzw. eine Spezifizierung der geeigneten Sicherheitslevels erforderlich.

## Gutes Risikomanagement

Dafür sind eine Reihe organisatorischer und technischer Kontrollen notwendig: So sollten Produktanbieter genau prüfen, wie Probleme der Funktionalen Sicherheit bzw. Cyber Security

Bild: ©koldunov/Photodune.net

*Wirksames Risikomanagement beginnt schon bei sicherem Design der Systeme.*

gehandhabt werden und dabei nicht nur die einfache Erfüllung von Normen in Betracht ziehen. Denn ein gutes Risikomanagement beginnt schon bei einem sicheren Design. Systemintegratoren müssen die Systeme gemäß den relevanten Normen zur Funktionalen Sicherheit und Cyber Security designen. Dazu gehört auch ein gutes Management der Funktionalen Sicherheit und Cyber Security, in dem Prozesse und Dokumente festgelegt sind. Systembetreiber sollten zudem sicher sein, dass sie über die entsprechende Sicherheitsdokumentation für Systeme und Produkte verfügen und einen sicheren Betrieb gewährleisten können. Industrie 4.0 lässt sich nur realisieren, wenn funktionale Sicherheit und Cyber Security für alle Elemente der industriellen Automation kombiniert werden können. ■

**Autor:** ***Nigel Stanley,***
***TÜV Rheinland***
***www.tuv.com/de/ics-security***

**Autor:** ***Jörg Krämer,***
***TÜV Rheinland***
***www.tuv.com/de/ics-security***