DAS SICHERHEITSDILEMMA ÜBERWINDEN

Industrie 4.0 lässt sich nur realisieren, wenn Funktionale Sicherheit und Cyber Security integriert betrachtet werden. Was ist damit genau gemeint und wie können Anlagenbetreiber sowie Systemanbieter und Systemintegratoren diesen Weg erfolgreich beschreiten? Nigel Stanley und Joerg Krämer, Experten für Sicherheit in der Produktion von TÜV Rheinland, zeigen Lösungswege auf.

Ein Unternehmen und seine Anlagen und Systeme müssen so abgesichert sein, dass sich die Organisation weiterentwickeln und Innovationen vorantreiben kann. Produktionssysteme bestehen heutzutage aus zahlreichen Hardware- und Software-Komponenten, die für die Fertigung und Bereitstellung von Produkten oder Dienstleistungen unerlässlich sind. „Dies sorgt für eine Fehleranfälligkeit, die die Prozesse in der Produktion mehr oder weniger stark beeinträchtigen kann“, so Joerg Krämer, Experte für Funktionale Sicherheit in der Produktion bei TÜV Rheinland. „Einige Fehler können für die komplette Anlage akute Gefahrensituatio-

nen heraufbeschwören. Das bedeutet: Prozesse oder Hardware-Komponenten, die in Computer- oder Internettechnologie integriert oder mit ihr verbunden sind, können nicht mehr länger als ‚sicher' im herkömmlichen Sinn gelten, sofern nicht auch die Steuerungssysteme in puncto Cyber Security abgesichert sind."

Selbst Anlagen mit rigorosen funktionalen Sicherheitskonzepten sind nicht automatisch gegen Cyber-Attacken gefeit. Ein Human Machine Interface (HMI)-PC mit ausgereiften und ordnungsgemäß implementierten Steuersystemen ist ohne Cyber-Security-Schutz anfällig für Angriffe. Dazu ist nicht einmal die Kompromittierung sicherer Produktionssysteme notwendig. Sinnlose Befehle an die übergeordnete Steuerung von Real Time Units (RTUs) sind ausreichend, um den Prozess in der Produktion lahmzulegen.

FUNKTIONALE SICHERHEIT UND CYBER SECURITY GLEICHRANGIG BEHANDELN

Problematisch für die integrierte Absicherung der 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.

Die Lebensdauer von Steuerungssystemen übersteigt die eines unternehmensinternen IT-Systems nicht selten um das Zehnfache. Nigel Stanley, Experte für Cyber Security in der Produktion bei TÜV Rheinland: „Software-Aktualisierungen werden hier nur unregelmäßig oder gar nicht durchgeführt." Diese Praxis wiederum stehe im Gegensatz zur stetig steigenden Anzahl an Patches für unternehmensinterne IT-Systeme. Die Anwendung unternehmensinterner IT-Tools, -Techniken und -Verfahren könne 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 schafft die Voraussetzungen dafür, dass gewünschte Abläufe wie vorgesehen vonstattengehen und beim Auftreten von Fehlern entsprechende Maßnahmen greifen, z. B. die Einstellung von Aktivitäten.

Cyber Security zielt darauf ab, Fabrikautomation und Prozesssteuerungen abzusichern. Hier geht es um Schutz und Verfügbarkeit von Kontroll- und Steuerungssystemen gegen absichtlich herbeigeführte oder ungewollte Fehler – z. B. durch Hacker. Ziel muss es sein, eine Störung oder gar einen Ausfall der Produktion zu verhindern.

Angesichts der dynamischen Bedrohungslage wird klar: Kein Produktionsunternehmen kann sich mehr leisten, Cyber Security zugunsten von Funktionaler Sicherheit zu vernachlässigen. Da Hacker jeglicher Art ein gesteigertes Interesse an industriellen Prozessen und Steuersystemen demonstrieren, müssen diese Bedrohungen analysiert und so gehandhabt werden, dass die Identifizierung der wichtigsten potenziellen Schwachstellen und Risiken für das Unternehmen möglich werden.

Neu entwickelte Standards wie IEC 62443 (ein Normenkatalog, der sich mit den Verfahren zur Sicherung industrieller Steuersysteme befasst) und IEC 61508 (ein Standard, der vom Ausfall der Sicherheitsfunktionen eines Geräts ausgeht) bieten eine strukturierte Herangehensweise für die gleichberechtigte Integration von Funktionaler Sicherheit und Cyber Security. Anlagenbetreiber, Systemanbieter und Systemintegratoren können diese Problemstellung nur auf effiziente und kostengünstige Art und Weise bewältigen, wenn sie diese und ähnliche Normen verstehen lernen bzw. annehmen.

NIGEL STANLEY, EXPERTE FÜR CYBER SECURITY IN DER PRODUKTION BEI TÜV RHEINLAND

Kein Produktionsunternehmen kann sich mehr leisten, Cyber Security zugunsten von Funktionaler Sicherheit zu vernachlässigen

Wichtig: Standards der Funktionalen Sicherheit bzw. Cyber Security sollten über den kompletten Produkt- oder Prozess-Lebenszyklus 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 Safety Integrity Level (SIL) und Security Level (SL) erforderlich sowie eine Reihe organisatorischer und technischer Kontrollen:

- Produktanbieter sollten genau prüfen, wie Probleme der Funktionalen Sicherheit bzw. Cyber Security gehandhabt werden (vom Design bis hin zur Installation ihrer Produkte) 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 Funktionale Sicherheit bzw. Cyber Security über ihr Systemdesign verwalten. Systembetreiber sollten sicher sein, dass sie über die entsprechende Sicherheitsdokumentation für Systeme und Produkte verfügen und einen sicheren Betrieb gewährleisten können.

Fotos: *Aufmacherfoto Fotolia, TÜV Rheinland*

bit.ly/ics-security