➤ **Um Industrie 4.0 sicher zu gestalten, müssen neue und gemeinsame Schutzziele für Safety und Security definiert werden.**

Nur gemeinsam sicher

Sicherheitstechnik Nur wenn Funktionale Sicherheit und Cybersecurity gemeinsam betrachtet werden, wird die digitalisierte Industrie sicher und performant realisierbar. Unternehmen müssen jetzt umdenken, da die Harmonisierung verschiedener Schutzziele eine Herausforderung darstellt.
Nigel Stanley, Jörg Krämer*

Mit zunehmender Vernetzung von Maschinen treffen in Bezug auf das Thema Sicherheit zwei Welten aufeinander: Die Welt der Automatisierung verschmilzt mit der IT-Welt. Die unterschiedlichen Welten der Funktionalen Sicherheit und der Cybersecurity müssen mit Aspekten wie industrieller Verarbeitung, Steuerungssystemen, Internet of Things (IoT) und Industrial Internet of Things (IIoT) ganzheitlich berücksichtigt werden. Selbst Anlagen mit rigorosen Funktionalen Sicherheitskonzepten sind nicht automatisch gegen Cyberattacken geschützt. Ein industrieller HMI (Human Machine Interface)-PC mit ausgereiften und ordnungsgemäß implementierten Steuersystemen ist ohne Cybersecurity-Schutz anfällig für Angriffe. Dazu ist nicht einmal die Kompromittierung sicherer Verarbeitungssysteme notwendig. Sinnlose Befehle an die übergeordnete Steuerung von RTUs (Real Time Units) sind ausreichend, um den gesamten Prozess in der Produktion lahmzulegen. Das bedeutet: Prozesse oder Hardwarekomponenten, die in Computer- oder Internettechnologie integriert oder verbunden sind, können nicht mehr länger als sicher betrachtet werden, sofern die Steuerungssysteme nicht auch in punkto Cybersecurity abgesichert sind.

Schutzziele: Safety wichtiger als Security?

Bei der Funktionalen Sicherheit geht es darum, den 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. Safety sichert dabei die gewünschten Abläufe ab und gewährleistet, dass beim Auftreten von Fehlern entsprechende Maßnahmen greifen. Die Cybersecurity hingegen zielt darauf ab, Fabrikautomation und Prozesssteuerungen abzusichern. Dabei geht es um den Schutz und die Verfügbarkeit von Kontroll- und Steuerungssystemen gegen absichtlich herbeigeführte oder ungewollte Fehler – z.B. durch Sabotage eines Hackers. Mit Cybersecurity soll eine Störung oder gar ein Ausfall der Produktion verhindert werden. Problematisch für die integrierte Absicherung der Industrie 4.0 ist, dass sich die Schutzziele von Funktionaler Sicherheit und Cybersecurity stark voneinander unterscheiden – und vielfach Funktionale Sicherheit noch Priorität vor Cybersecurity hat. Denn 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-Tools, -Techniken und -Verfahren kann verhängnisvolle Auswirkungen auf betriebstechnische Systeme haben. Gleiches gilt aber auch umgekehrt. Zahlreiche Sicherheitsvorfälle haben deutlich gemacht: Kein Produktionsunternehmen kann es sich leisten, Cybersecurity zugunsten von Funktionaler Sicherheit zu vernachlässigen. Da immer mehr

*Nigel Stanley, Practice Director für Cybersecurity, TÜV Rheinland, und Jörg Krämer, Head of Sales Functional Safety & Cybersecurity, TÜV Rheinland

Sariana Kunze,
Redakteurin
sariana.kunze@vogel.de

Erfahren Sie, wie Sie Anlagen vor Cyber-Kriminalität absichern: www.elektrotechnik.de/k26

Hacker nach Einfallstoren bei industriellen Prozessen und Steuerungssystemen suchen. Nur eine genaue Analyse der Bedrohungen sowie die Identifizierung der potenziellen Schwachstellen und Risiken kann Unternehmen sensibilisieren und schützen.

Risikomanagement beginnt bei sicherem Design

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 Cybersecurity. Betreiber, Anbieter und Systemintegratoren industrieller Automation können diese Problemstellung bewältigen, wenn sie diese und ähnliche Normen verstehen lernen bzw. annehmen. Dabei gilt es stets zu beachten, dass Standards der Funktionalen Sicherheit bzw. Cybersecurity über den gesamten Produkt- oder Prozess-Lebenszyklus hinweg – von der Spezifizierung über das Design bis hin zu Betrieb und Wartung – berücksichtigt werden sollten. Dazu ist eine effiziente Risiko- und Gefahrenanalyse bzw. eine Spezifizierung der geeigneten Safety Integrity Level (SIL) und Security Level (SL) erforderlich. Dafür sind organisatorische und technische Kontrollen notwendig:

- So sollten Produktanbieter prüfen, wie – vom Design bis zur Installation ihrer Produkte – Probleme der Funktionalen Sicherheit bzw. Cybersecurity gehandhabt werden und dabei nicht nur die Erfüllung von Normen in Betracht ziehen. Denn ein gutes Risikomanagement beginnt schon bei einem sicheren Design.
- Systemintegratoren müssen die Funktionale Sicherheit bzw. Cybersecurity über ihr Systemdesign verwalten. Betreiber sollten sicher sein, dass sie über die Sicherheitsdokumentation für Systeme und Produkte verfügen und einen sicheren Betrieb gewährleisten können.

Industrie 4.0 lässt sich also nur realisieren, wenn Funktionale Sicherheit und Cybersecurity für alle Elemente der Automation kombiniert werden können. [kun]

FUNKTIONALE SICHERHEIT & CYBERSECURITY

Mit Standards strukturiert vereinen

IEC 62443 (vorher ANSI/ISA-99) ist ein Normenkatalog, der sich mit den Verfahren zur Sicherung industrieller Steuersysteme befasst. Die Richtlinie gilt für alle Hersteller, Systemintegratoren und Betreiber industrieller Steuersysteme. IEC 62443-4-2 integriert sieben Funktionale Anforderungen:

- FR 1: Schutz von Geräten durch Identifizierung und Authentifizierung von Zugriffsanforderungen (Nutzern);
- FR 2: Schutz gegen nicht autorisierte Maßnahmen in Bezug auf die Geräteressourcen durch Verifizierung der geforderten Nutzerprivilegien vor der Genehmigung;
- FR 3: Gewährleistung der Integrität der Anwendung zwecks Vermeidung einer unerlaubten Manipulation;
- FR 4: Gewährleistung der Vertraulichkeit von Informationen auf Kommunikationskanälen und in Data Repositories zwecks Vermeidung einer unerlaubten Offenlegung;
- FR 5: Segmentierung des Steuersystems über Zonen und Kanäle zwecks Limitierung eines übermäßigen Datenflusses;
- FR 6: Reaktion auf Sicherheitsverletzungen per Benachrichtigung der zuständigen Behörden, Weiterleitung von dahingehendem Beweismaterial sowie die Einleitung zeitnaher Maßnahmen bei der Feststellung von Ereignissen; und
- FR 7: Gewährleistung der Verfügbarkeit der Anwendung/des Geräts durch Vermeidung von Störungen bzw. die Sicherstellung grundlegender Dienste.

Diese Anforderungen können dabei helfen, die Cyberbedrohungen für industrielle Steuersysteme zu reduzieren.