Diesmal im Fokus:

Safety meets Security

Carsten Gregorius, Senior Specialist Safety

Gemeinsame Strategie erforderlich

Der in Maschinen und Anlagen verbauten Sicherheitstechnik kommt über den gesamten Lebenszyklus der Applikation eine stetig steigende Bedeutung zu. Durch die zunehmende Vernetzung der Automatisierungssysteme mit der IT-Welt können Szenarien auftreten, die insbesondere von Safety-Anwendungen eine neue Herangehensweise erfordern.

Ein wichtiges Einfallstor für Hacker stellen die Netzwerkübergänge zwischen der Office-IT und dem Produktionsnetz dar.

Werden Automatisierungslösungen zur Realisierung der funktionalen Sicherheit zum Ziel von Hackerangriffen, treffen die Welten von „Safety" und „Security" aufeinander. Zukünftig muss daher eine gemeinsame Strategie entwickelt werden.

Cyber Security vs. funktionale Sicherheit

Der Aspekt der funktionalen Sicherheit bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion des sicherheitsbezogenen Steuerungsteile und anderen risikomindernden Maßnahmen abhängt. Tritt hier ein kritischer Fehler auf, z.B. ein Kurzschluss, übernimmt die Steuerung die Einleitung des sicheren Zustands. Die Anforderungen an die Beschaffenheit von sicherheitsrelevanten Steuerungsteilen sind in der B-Norm EN ISO 13849 sowie der IEC-Reihe 61508/61511/62061 beschrieben. Je nach Risikohöhe werden die entsprechenden risikoreduzierenden Maßnahmen in unterschiedliche Sicherheitsniveaus eingestuft: Performance Level (PL) oder Safety Integrity Level (SIL).

Im Gegensatz zur funktionalen Sicherheit schützt die Cyber Security Güter vor einer nachteiligen Beeinträchtigung durch beabsichtigte oder versehentliche Attacken auf die Verfügbarkeit, Integrität und Vertraulichkeit der Daten. Dazu werden vorbeugende, technische sowie organisatorische Maßnahmen verwendet.

Pragmatischer Ansatz gemäß NAMUR-Arbeitsblatt

Um den Produktlebenszyklus sicherheitsgerichteter Systeme oder Komponenten sicherzustellen, sind Hersteller, Systemintegratoren und Betreiber aufgefordert, innerhalb eines „Functional Safety Managements" ein bedarfsgerechtes Qualitätsmanagement gemäß IEC 61508 anzuwenden.

Einen ersten pragmatischen Ansatz, Safety und Cyber Security zu verzahnen, bietet das von der NAMUR (Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie) veröffentlichte Arbeitsblatt „IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen" (PLT steht für Prozessleittechik). Das darin beschriebene Verfahren zur IT-Risikobeurteilung in Anlehnung an die Security-Norm IEC 62443 bildet dabei die Grundlage für die Erhöhung der Widerstandsfähigkeit der PLT-Sicherheitseinrichtung gegen IT-Bedrohungen. Zu diesem Zweck wurde in der ersten Phase einmalig exemplarisch ein Verfahren entwickelt wie es typischerweise in der chemischen Industrie vorzufinden ist. Damit kann der Anwender die Nutzbarkeit des Verfahrens für seine zu beurteilende PLT-Sicherheitseinrichtung überprüfen. Die zweite Phase bildet die Kontrolle der Umsetzung der Maßnahmen sowie die Dokumentation der IT-Sicherheitsanforderungen. Dieser Schritt muss für jede zu evaluierende PLT-Sicherheitseinrichtung individuell durchlaufen werden.

Sie wollen noch mehr Detailwissen, Insider-Informationen und Infografiken zu diesem Thema? Dann erfahren Sie Weiteres auf:

http://www.phoenixcontact.net/webcode/#2312

Autor
Dipl.-Ing. (FH) C. Gregorius, Senior Specialist Safety, Phoenix Contact Electronics GmbH, Bad Pyrmont

Kontakt

Phoenix Contact GmbH & Co.KG
Blomberg
cgregorius@phoenixcontact.com
www.phoenixcontact.com