Schutz und Sicherheit kritischer Infrastrukturen bedürfen der ständigen Weiterentwicklung von Branchenstandards und Regelwerken. Weite Teile der Industrie und Energiewirtschaft haben dies bereits als Gemeinschaftsaufgabe erkannt. Betreiber, Hersteller von Sensoren und die Hersteller von sicherheitsgerichteten Schaltungen müssen hier stärker als bisher zusammenarbeiten.

Foto: shutterstock

Schützen wir unsere Anlagen ausreichend vor Hackerangriffen?

„Zuerst Saudi-Arabien, dann Deutschland? Ein beispielloser Angriff auf ein Kraftwerk am Persischen Golf sollte auch den Deutschen zu denken geben." titelte Spiegel-Online am 06.04.2018. Betroffen war ein Kraftwerk. Nur durch einen Zufall war es nicht zu einem Großschaden gekommen. Die Art des Angriffs hat viele Experten aufgeschreckt. Ein Kraftwerk anzugreifen, um gezielt einen großen Sachschaden anzurichten, das Leben von Menschen in Kauf zu nehmen und dabei das „Herz" – die sicherheitsgerichtete Steuerung – zu hacken war neu. Und es hätte gelingen können. Doch betrifft uns dies in Deutschland? Die Antwort lautet (leider): Ja! Die sicherheitsgerichtete Steuerung in dem arabischen Kraftwerk ist in sehr vielen deutschen Kraftwerken ebenfalls verbaut. Ebenso in einer Reihe von weiteren technischen Anlagen anderer Industriezweige bis hin zur Gasinfrastruktur. Der Hersteller verkauft diese Steuerungen weltweit. Haben wir einfach nur Glück gehabt bisher?

Einen absoluten Schutz vor Cyberangriffen gibt es nicht und wird es wahrscheinlich auch künftig nicht geben. Das Problem: Cyber ist schnell und einem permanenten Wandel unterzogen. Eine einzelne Lücke im System ist oft schon ausreichend. Bei der technischen Sicherheit von Gasfernleitungen ist man dagegen gewohnt, sorgfältig Gefahrenanalysen durchzuführen und im Zeitraum von ca. einigen Jahren zu reviewen – mehrere Jahre, das sind Generationen in der Cyberzeit.

Security ist bei den heutigen Gefahrenanalysen in der Regel gar kein Thema. Dafür gibt es die OT-Abteilung. Safety und Security müssen sich jedoch annähern. Am CSE Center of Safety Excellence nennen wir das Plant Security. Die Kommission für Anlagensicherheit als Beratungsgremium der Bundesregierung beschäftigt sich mit dem Thema "Eingriffe Unbefugter" (Neufassung des SFK-GS-38 ist in Planung), die NAMUR hat die Richtlinie NA 163 (IT- Risikobeurteilungen für PLT-Sicherheitseinrichtungen) für die Prozessindustrie herausgegeben und auch das Bundesamt für Informationssicherheit in der Informationstechnik überarbeitet die Richtlinien für sicherheitsgerichtete Steuerungen. Offensichtlich ist die Brisanz des Themas branchenübergreifend erkannt worden. Allerdings stecken alle in einem Dilemma: Keines der Regelwerke und Richtlinien enthält klare Handlungsanweisungen und Maßnahmen zum Schutz individueller Anlagen vor cyberphysischen

Foto: shutterstock

Angriffen. Es wird befürchtet, dass eine Veröffentlichung konkreter Umsetzungen Tür und Tor für neue Angriffe öffnen könnte. Doch wie soll dann der Schutz tatsächlich gelingen?
Das CSE Center of Safety Excellence hat zusammen mit dem IT-Partner 8COM das CeSIS (Center of Safety Integrity and Security, vgl. https://cse-engineering.de/cesis/psm2x/) gegründet und erarbeitet in einem Kreis von derzeit rund 12 namhaften Firmen neue Schutzkonzepte für PLT-Sicherheitseinrichtungen (SIS) mit denen technische Anlagen typischerweise abgesichert werden. Betreiber, Hersteller und Dienstleister sitzen an einem Tisch. Angriffsszenarien und Penetrationstests sind neben der Risikobewertung Themen dieses Arbeitskreises. Statt die Peripherie um die Anlage zu schützen sollen die PLT-Sicherheitseinrichtungen unmittelbar vor cyberphysischen Angriffen geblockt werden. Weitere Teilnehmer in der CeSIS Gruppe sind herzlich willkommen.
Es wird höchste Zeit, dass diese Themen in die Breite der Industrie vordringen und branchenübergreifend diskutiert werden. Plant Security wird in allen Industriezweigen dringend gebraucht. Der Trend in der Sicherheitstechnik geht seit einiger Zeit in die Richtung Zero-Emission. PLT-Sicherheitseinrichtungen und auch mechanische Sicherheits-einrichtungen werden intelligent. Leckagen sollen möglichst vollständig unterbunden bzw. frühzeitig sicher detektiert werden. Mit künstlicher Intelligenz werden modulare Sicherheitseinrichtungen entwickelt, die sich an den jeweiligen Prozessen adaptieren und die zu jedem Betriebszeitpunkt die Sicherheit und Wirtschaftlichkeit von Anlagen optimieren (Smart High Integrity Protection Devices). Sicherheitseinrichtungen entwickeln sich zu cyberphysischen Anlagen in einem Kommunikationsnetzwerk, das mit den neuen 5G Standards immer leistungsfähiger wird. Die Integrität von Sicherheitseinrichtungen lässt sich künftig über die Auswertung sehr vieler Betriebsdaten und Prozessfahrweisen individuell bewerten und festlegen. Während die Sicherheitstechniker gerne das Festhalten an mechanischen Sicherheitseinrichtungen beschwören, entwickeln die Hersteller von Sensoren, Steuerungen und Aktoren immer intelligentere Systeme. Systeme, die in Kommunikationsnetzwerke eingebunden werden und drahtlos Diagnosen und eine Vielzahl von Daten weiterleiten. Schöne neue Welt – es wird Zeit, dass Safety und Security zu einer gemeinsamen Disziplin Plant Security verschmelzen. Setzen Sie sich mit Thema auseinander, bevor Sie durch einen Angriff dazu gezwungen werden.

CSE CENTER OF SAFETY EXCELLENCE

CeSIS

Center of Safety Integrity and Security des CSE (https://cse-engineering.de/cesis/psm2x/)

Prof. Dr.-Ing. Jürgen Schmidt
CSE Institut
juergen.schmidt@cse-institut.de

Foto: shutterstock