datensicherheit.de

TÜV Rheinland und Open Sky

Cyber-Angriffe: Kritische Infrastrukturen und Industrie mehr denn je bedroht

TÜV Rheinland fordert: „Cyber Security bei Funktionaler Sicherheit integriert berücksichtigen“

[datensicherheit.de, 12.01.2017] Cyber-Angriffe auf **Kritische Infrastrukturen** (KRITIS) und die Industrie sind keine Frage des „Ob“, sondern des „Wann“ – es drohen Unterbrechungen in der Energieversorgung, der tagelange Ausfall von Telefon, Internet und TV bundesweit bis hin zu Störungen in der Produktion.

Funktionale Sicherheit nicht mehr isoliert betrachten!

Die Folgen solcher Attacken im Zuge der Digitalisierung und der wachsenden Vernetzung im **Internet der Dinge** bzw. im **„Industrial Internet of Things“** (IIoT) können massiv sein.

Der TÜV Rheinland hat deshalb nach eigenen Angaben sein Portfolio für Sicherheitsaudits und Zertifizierungen in der Industrie und in Kritischen Infrastrukturen durch umfassende Cyber-Security-Analysen und -Prüfungen erweitert.

„Mit dem Einzug von Industrie 4.0 lässt sich Funktionale Sicherheit nicht mehr isoliert betrachten“, betont **Heinz Gall**, Experte für **„Functional Safety & Security“** beim TÜV Rheinland.

Cyber Security als wesentlicher Erfolgsfaktor

Nigel Stanley, Spezialist für „Cyber Security“ beim TÜV Rheinland ergänzt: *„Cyber Security ist ein wesentlicher Erfolgsfaktor: zur Absicherung zentraler Versorgungssysteme, als wichtige Voraussetzung für die funktionale Sicherheit in Fertigungsprozessen, für den sicheren automatisierten Datenaustausch vernetzter Produktionssysteme und für die Verfügbarkeit und Ausfallsicherheit der Produktion.“*

Der Bedarf, die aktuellen Sicherheitsstrategien in der Industrie regelmäßig zu überprüfen und intelligente Konzepte weiter zu entwickeln, werde mit der fortschreitenden Vernetzung im IIoT weiter steigen, so Stanley.

Interdisziplinärer Risikomanagement-Ansatz

Für Komponentenhersteller und Systemintegratoren industrieller Steuerungssysteme hat der TÜV Rheinland demnach auf Basis einer fundierten Risikoanalyse einen „interdisziplinären Risikomanagement-Ansatz“ entwickelt, der funktionale Sicherheit und „Cyber Security“ gleichermaßen fokussieren soll – von der Entwicklungsphase („Safety & Security by Design“) über den gesamten Lebenszyklus.

Daraus abgeleitet seien tiefgreifende Sicherheitsprüfungen, unter anderem wiederkehrende Schwachstellen-, Härte- sowie Penetrationstests auf dem Gebiet der Funktionalen Sicherheit wie der „Cyber Security“.

Das Konzept wurde soeben vom TÜV Rheinland auf der „S4x17“ in Miami vorgestellt – diese sei eine „der wichtigsten internationalen Konferenzen für die Sicherheit industrieller Steuerungssysteme“ („ICS Security“).

Mehr als 15-jährige Erfahrung auf dem Gebiet der „Cyber Security“

Mit diesem integrierten Angebot für Funktionale Sicherheit und „Cyber Security“ möchte der TÜV Rheinland seine 145-jährige Expertise für Sicherheit in der Industrie und die mehr als 15-jährige Erfahrung auf dem Gebiet der „Cyber Security“ bündeln.

Neben der Rechtssicherheit gegenüber gesetzlichen Auflagen sollen Komponenten-Hersteller und Integratoren von Industrieanlagen mit diesem Ansatz die anspruchsvolleren „Security Levels“ bzw. Reifegrade („Maturity Levels“), die in der IEC 62443 definiert sind, einer internationalen Norm für „Security for industrial automation and control systems“, erreichen.

http://www.tuvasi.com
http://www.openskycorp.com