5 Minute Guide

Warum Funktionale Sicherheit ohne Cybersecurity nicht mehr möglich ist.

Was bei überwachungsbedürftigen Anlagen im Hinblick auf Cybersecurity zu beachten ist.

Technische Anlagen, die aufgrund besonderer Gefährdung im Bereich Dampf, Druck, Absturz oder Brand bzw. Explosion regelmäßig überprüft werden müssen, sollten neben der Prüfung auf Funktionale Sicherheit zusätzlich auch auf Cybersecurity überprüft werden. Die Digitalisierung macht sich durch neue Informations- und Kommunikationstechnologien auch bei überwachungsbedürftigen Anlagen bemerkbar. Die Vernetzung von Anlagen und Maschinen, deren Geräte, Aktoren und Sensoren bergen Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können. Daher besteht die umfassende Sicherheit einer technischen Anlage nicht nur aus Funktionaler Sicherheit, sondern somit auch aus Cybersecurity. Anlagen und Prozessabläufe sind nur dann „safe“, wenn sie auch „secure“ sind.

VERÄNDERUNGEN

- Vernetzungen verschiedener Anlagenkomponenten und Steuerungen über Kommunikationsschnittstellen, z.B. Profi BUS (W-)LAN, TCP/IP
- Anwendung von Prozessen, Methoden und Verfahren der Informations- und IT-Sicherheit in der industriellen Automatisierung
- Prozesse werden digitalisiert und in eine Cloud verlagert

GEFAHREN UND RISIKEN

- Verletzung von Menschen, Schädigung der Umwelt sowie Ausfall der Produktion
- Ungewollte, unberechtigte oder böswillige Eingriffe in die IT/OT-Systeme
- Fehlfunktionen von Maschinen und Anlagen
- Beeinträchtigung der Funktionsfähigkeit von sicherheitsrelevanten MSR-Einrichtungen

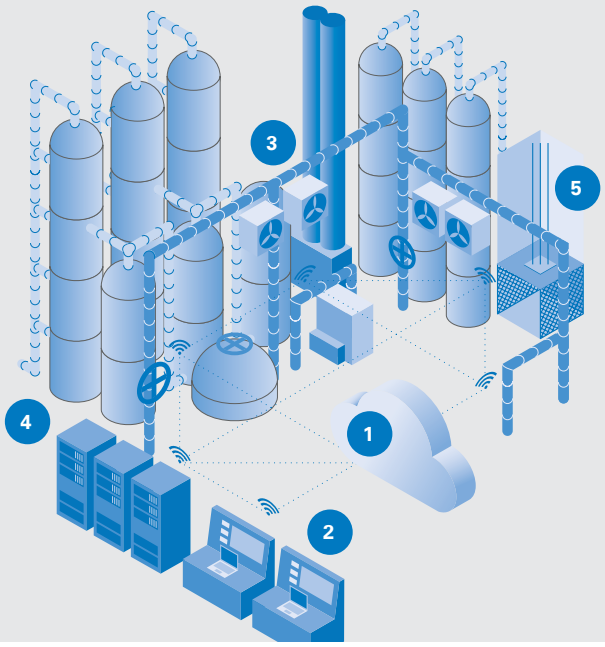
SCHUTZMASSNAHMEN

- Gefährdungsbeurteilung hinsichtlich Cybersecurity
- Identifizierung von Sicherheitszonen und deren Schutzbedarf
- Prüfungen der umgesetzten Maßnahmen zur Cybersicherheit
- Penetrationstests
- Fortlaufende Identifizierung von Schwachstellen und Cybersecurity-Ereignissen

www.tuv.com/fscs-de

TÜVRheinland®
Genau. Richtig.

FUNKTIONALE SICHERHEIT & CYBERSECURITY TOUCHPOINTS FÜR ÜBERFACHUNGSBEDÜRFTIGE ANLAGEN.



1. CLOUD COMPUTING & WORKFLOWS
2. HUMAN MACHINE INTERFACE UND IT
3. SENSOREN UND AKTOREN
4. SPEICHERPROGRAMMIERBARE STEUERUNGEN UND SERVER
5. STEUERUNGSSYSTEME VON AUFZÜGEN UND KRANEN

INTERNATIONALE STANDARDS, NORMEN UND RICHTLINIEN.

Eine Vielzahl von relevanten Standards und Normen definieren Sicherheitsanforderungen, die Betreiber von überwachungsbedürftigen Anlagen zu beachten haben. Diese sind weltweit gültig und empfohlen.

Für die Anlagensicherheit und Cybersecurity-Aspekte sind folgende Standards relevant:

WELTWEIT
- ISO 27001
- IEC 62443

EUROPAWEIT
- EU Cybersecurity Act
- NIS Richtlinie

DEUTSCHLANDWEIT
- Betriebssicherheits-verordnung (BetrSichV)
- Störfall-Verordnung (12. BImSchV)
- EmpfBS 1115
- TRBS 1115
- IT-Sicherheitsgesetz 2.0
- BSI-ICS Security Kompendium

HEUTE FÜR DIE SICHERHEIT DER ZUKUNFT SORGEN.

Neue und smarte Technologien erfordern Expertenwissen. Profitieren Sie von unserer langjährigen Expertise im Bereich der Anlagen- und Cybersicherheit. Wir unterstützen Sie bei der Gefährdungsbeurteilung und Umsetzung der für Sie relevanten Standards.
Mit unseren themenspezifischen Trainings zur Funktionalen Sicherheit und Cybersecurity können Sie Ihre Mitarbeiter zum FS Engineer (TÜV Rheinland) oder CySec Specialist (TÜV Rheinland) mit entsprechenden Zertifikaten weiterbilden.

UMDENKEN UND ENTSCHLOSSEN HANDELN.

Als weltweit führender Prüfdienstleister in Funktionaler Sicherheit und Cybersecurity bieten wir Anlagenbetreibern ein breites Dienstleistungsportfolio. Unsere Experten analysieren alle Aspekte der Funktionalen Sicherheit und Cybersecurity entlang des gesamten Lebenszyklus Ihrer Anlage – vom Konzept über die Realisierung bis hin zur Inbetriebnahme und Wartung. Lassen Sie uns heute gemeinsam für die Sicherheit von morgen sorgen.

ONLINE KONTAKT

TÜV Rheinland Industrie Service GmbH
Am Grauen Stein · 51105 Köln
industrie@de.tuv.com
www.tuv.com/fscs-de

TÜVRheinland®
Genau. Richtig.

DE21_I07_FSCS_2100934