



5 Minute Guide

Mit Sicherheit in die Zukunft – In der Prozess-, Petrochemie- und Öl und Gas Industrie.

Warum Safety ohne Security nicht mehr möglich ist.

Künstliche Intelligenz, Industrie 4.0, Internet der Dinge (IoT), modulare Automation – das ist die Zukunft in der Prozessindustrie, die bereits jetzt schon begonnen hat. Die zunehmende und umfassende Digitalisierung und somit das Zusammenspiel von Informations- und Kommunikationstechniken in industriellen Produktionsanlagen ermöglicht die Vernetzung von Maschinen, Geräten, Sensoren und Menschen. Damit können Produkte flexibler und effizienter auf den Markt gebracht und Kosten gesenkt werden. Gleichzeitig müssen Anforderungen der Funktionalen Sicherheit sowie Cybersecurity erfüllt werden, um eine sichere Automatisierung in der Prozessindustrie zu erreichen. Anlagen und Prozessabläufe sind nur dann „safe“ wenn sie auch „secure“ sind.

VERÄNDERUNGEN



- Smartes Equipment: intelligente Komponenten und Anlagen
- Verstärkter Einsatz von Künstlicher Intelligenz (KI)
- Modulare Automation
- Technik des Digitalen Zwilling einer Anlage führt zu Verschmelzung von Engineering-, Operational und Informations-Technologie

RISIKEN UND GEFAHREN



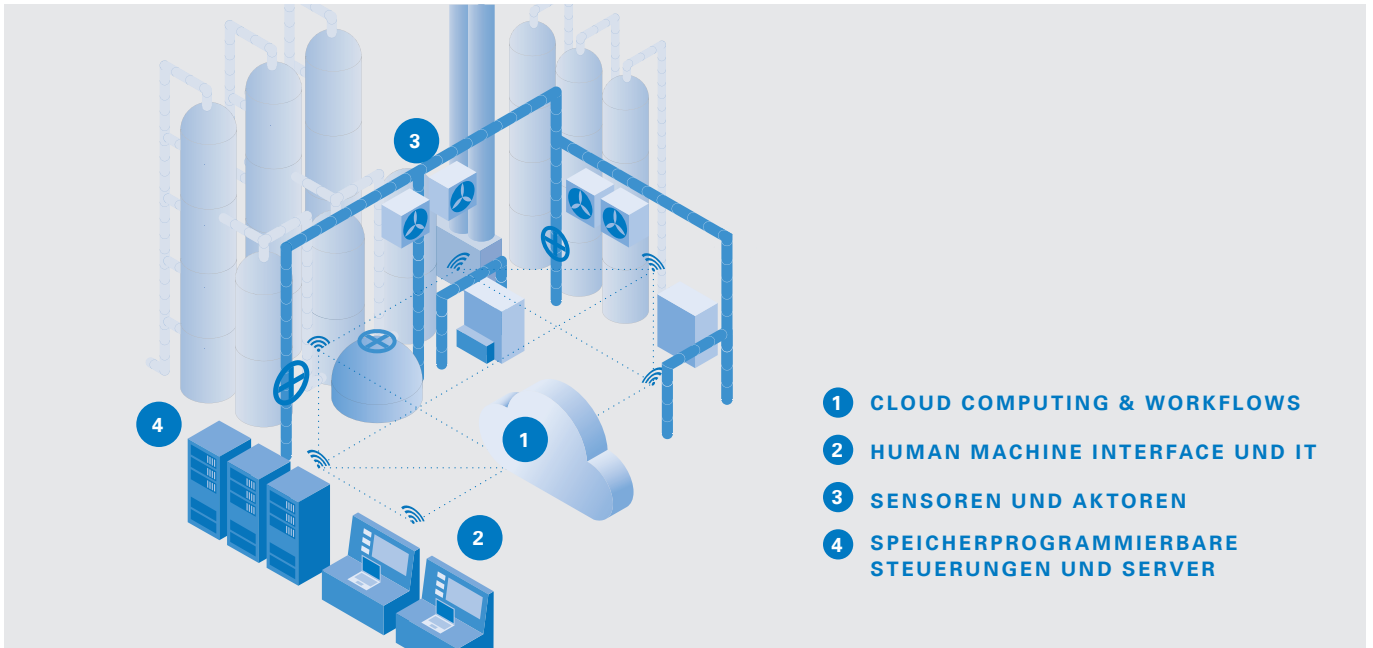
- Verletzen von Menschen, Verschmutzung der Umwelt sowie Ausfall der Produktion
- Ungewollte, unberechtigte oder böswillige Eingriffe in die IT/OT-Systeme
- Fehlfunktionen von Maschinen und Anlagen
- Manipulation von Steuerungs- und Verarbeitungssystemen
- Manipulation von Sensoren

SCHUTZMASSNAHMEN



- Risikobewertung hinsichtlich Funktionaler Sicherheit und Cybersecurity
- IT/OT Sicherheitsanalysen zur Identifikation von Sicherheitslücken
- Bewertung und Prüfung der Funktionalen Sicherheit bei Anlagen sowie Penetrationstests vor Inbetriebnahme
- Überwachung von Anlagen während des Betriebs

FUNKTIONALE SICHERHEIT & CYBERSECURITY TOUCHPOINTS IN DER PROZESS-, PETROCHEMIE- UND ÖL & GAS INDUSTRIE.



INTERNATIONALE STANDARDS, NORMEN UND RICHTLINIEN.

Eine Vielzahl von relevanten Standards und Normen definieren Sicherheitsanforderungen, die Betreiber einer Anlage, Hersteller von Maschinen sowie Systemintegratoren von sicherheitstechnischen Komponenten und Systemen erfüllen müssen. Diese Normen sind weltweit gültig und empfohlen.

Für die Funktionale Sicherheit und für Cybersecurity Aspekte sind folgende Standards relevant:

WELTWEIT

- IEC 61511
- IEC 61508
- IEC 62443
- VDI/VDE 2180
- Empfehlungen der Normur (NA 163, NA 169)

EUROPAWEIT GÜLTIG

- NIS Richtlinie
- EU Cybersecurity Act
- DSGVO

DEUTSCHLANDWEIT GÜLTIG

- IT-Sicherheitsgesetz
- 12. BImSchV
- Leitfäden der Kommission für Anlagensicherheit (KAS 44, KAS 51)

HEUTE FÜR DIE SICHERHEIT DER ZUKUNFT SORGEN.

Neue und smarte Technologien erfordern Expertenwissen. 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 ENTSCLOSSEN HANDELN.

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

Kontaktieren Sie uns für Ihre individuelle IT/OT-Sicherheitsanalyse.

ONLINE KONTAKT

TÜV Rheinland Industrie Service & Cybersecurity
Am Grauen Stein · 51105 Köln
cybersecurity@tuv.com
www.tuv.com/fscs-de

 **TÜVRheinland**[®]
Genau. Richtig.