

Ganzheitliches Risikomanagement für Produkte und Prozesse der Industrie 4.0



Mit der zunehmenden Digitalisierung im Bereich der Fertigung und der neuen Konnektivität von Produkten und Maschinen muss nicht mehr nur der Mensch vor der Maschine, sondern auch die Maschine vor dem Menschen geschützt werden, um unbefugte Beeinflussung (Cyberattacken) von außen zu vermeiden.

Hersteller, Integratoren und Betreiber von funktional sicheren Produkten müssen dazu die vielfältigen Maßnahmen der IT-Sicherheit neu definieren. Dies betrifft vorrangig die Entwicklungs-, Herstellungs- und Betreiberprozesse unter anderem in folgenden Geltungsbereichen:

- Produkthaftungsgesetz
- Betriebssicherheitsverordnung
- Richtlinie für Medizinprodukte

Aktuell gültige Normen betrachten entweder Fragen der Informationssicherheit (Security) oder der Funktionalen Sicherheit (Safety). Ein vollständig integrierter Ansatz liegt momentan weder als Norm noch als Richtlinie vor. Zukunftsweisende Security4Safety-Strategien erfordern jedoch eine kombinierte Betrachtung der beiden bisher isoliert behandelten Themenfelder.

Branchenübergreifendes Risikomanagement

Durch die praxisorientierte Verknüpfung von Safety- und Security-Dienstleistungen können wir Ihnen einen integrierten Ansatz für Ihr Risikomanagement anbieten. Das Security4Safety-Leistungsportfolio deckt dazu alle wesentlichen Anwendungsbereiche ab:

- Transport & Verkehr (Automotive, Bahn, Luftfahrt, Schifffahrt)
- Ver- und Entsorgung (Energie, Wasser, Nahrungsmittel)
- Gesundheitswesen (Arzneimittel, Medizinprodukte)
- sicherheitsgerichtete Komponenten mit Schnittstelle zum Internet (Sensorik, Steuerungen, Aktorik, Office-IT etc.)
- private Güter mit Schnittstelle zum Internet (Konsumgüter, Smart-Home- Anwendungen etc.)

Prüfungen auf Grundlage anerkannter Standards und Normen

Unsere Security4Safety-Risikoanalyse basiert auf bestehenden Verfahren der Gefährdungs- und Risikobeurteilung wie:

- EN ISO 12100
- EN 62443-3-2
- VDI/VDE 2182

Im Rahmen eines anwendungs- und kundenorientierten ganzheitlichen Ansatzes haben wir daraus ein systematisches, strukturiertes Verfahren entwickelt, um nachvollziehbar die Vermögenswerte aller relevanten Prozesse, Systeme und Komponenten dokumentieren und bewerten zu können. Sowohl die Dokumentation als auch die Bewertung werden in unserem eigens dafür entwickelten S4S-Softwaretool durchgeführt, das Ihnen nach Beauftragung der Risikoanalyse auch zur Verfügung steht.

Inhalt einer Security4Safety-Risikobewertung

Die S4S Risikobewertung kann in zwei verschiedenen Modulen erfolgen. Im ersten Modul führen unsere Experten eine Statusanalyse bei Ihnen durch, in deren Verlauf zum einen die für Ihre Zwecke anzuwendenden Richtlinien und Standards definiert werden und dann eine Gefährdungsanalyse gemäß dieser Standards wie z.B. IEC 62443-3-2, IEC 61508 und anderer durchgeführt wird. Die Bedrohungsanalyse kann auf Ebene Ihrer Komponenten und Produkte oder auch auf Ebene Ihrer Organisationsprozesse durchgeführt werden. Sie erhalten als Ergebnis einen detaillierten technischen Bericht über diese Statusanalyse und können die Sicherheitslücken bei Ihren Produkten oder Prozessen erkennen. Auf dieser Basis sind Sie befähigt, die für Ihre Organisation geeigneten Maßnahmen zur Beseitigung der Risiken abzuleiten und umzusetzen. In einem zweiten Modul bieten wir Ihnen eine S4S Bewertung zur Evaluation Ihrer Umsetzung in Produkten oder Prozessen an. Das Ergebnis ist ein technisches Gutachten zur Ihrer S4S Umsetzung.

Während der Bewertung stellen wir Ihnen einen Projektverantwortlichen zur Seite, der als zentraler Ansprechpartner fungiert. Den Anfang bildet ein Workshop, danach folgen regelmäßige Meilensteinmeetings bis zum Projektabschluss. Unser Softwaretool zur S4S Risikobewertung dokumentiert vollständig und umfassend die durchgeführte Risikobewertung. Zum Abschluss erhalten Sie alle erzeugten Dokumentationen.

Ihr Weg zur Industrie-4.0-Readiness

Wir empfehlen, eine Security4Safety-Risikobewertung mit Ihren Komponenten oder Produkten zu beginnen und sie dann auf Ihre Organisationsprozesse auszuweiten. Wenn Sie dies mit positiven Ergebnissen durchlaufen haben, steht Ihnen die Zertifizierung nach IEC 62443 offen. Zusammen mit der Zertifizierung nach ISO 27001 demonstrieren Sie so die Industrie-4.0-Readiness Ihrer Organisation. Dieser Reifegrad belegt, dass Sie den aktuellen Stand der Technik im Bereich der Sicherheit einhalten und die notwendige Sorgfaltspflicht zur Inverkehrbringung sicherheitsgerichteter Produkte auf allen logischen Ebenen (Prozesse, Systeme, Komponenten) erfüllen.

Wir informieren Sie gerne persönlich über die einzelnen Phasen und deren Umsetzung. Senden Sie uns diese Antwort per E-Mail zu. Wir freuen uns auf das Gespräch mit Ihnen.

Absender (bitte in Blockschrift)

Unternehmen

Frau/Herr

Position

Straße

Kontaktieren Sie uns unter

TÜV NORD CERT GmbH

Tel.: 0800 245-7457 (kostenlose Service-Hotline)

info.tncert@tuev-nord.de

Ihre Vorteile

- Identifikation und Elimination von digitalen Schwachstellen im Entwicklungs-, Fertigungs- und Serviceprozess
- Sicherung der Qualität und Sicherheit der Produkte
- Verringerung des Risikos von Rückrufaktionen und Imageschäden sowie daraus resultierender Schadensersatzansprüche
- Vertrauensgewinn gegenüber Ihren Kunden durch die kompetente Bewertung von TÜV NORD CERT

TÜV NORD CERT ist ein international anerkannter und zuverlässiger Partner für Prüf- und Zertifizierungsdienstleistungen. Unsere Fachleute verfügen über fundiertes Wissen und haben grundsätzlich eine Festanstellung bei TÜV NORD. Hierdurch sind Unabhängigkeit und Neutralität sowie Kontinuität bei der Betreuung unserer Kunden gewährleistet. Der Vorteil für Sie liegt auf der Hand: Unsere Experten begleiten und unterstützen die Entwicklung Ihres Unternehmens und geben Ihnen ein objektives Feedback.



Ja, ich interessiere mich für Security4Safety-Risikobewertung. Bitte nehmen Sie Kontakt mit mir auf.

PLZ/Ort

Telefon

Telefax

E-Mail



Weitere Informationen finden Sie unter

www.tuev-nord-cert.de

und www.security4safety.de