TÜVNORD

Inspired by Knowledge

Cyber Security Management für industrielle Automatisierungs- und Steuerungssysteme (IACS)

Überblick: OT-Sicherheit im industriellen und regulatorischen Umfeld
Industrielle Automatisierungs- und Leitsysteme (Industrial Automation and Control Systems, IACS) sind ein zentraler Bestandteil moderner Produktions-, Prozess- und Infrastrukturlandschaften. Die fortschreitende Digitalisierung, der Einsatz von IoT-Technologien, Fernwartungskonzepte sowie die zunehmende Konvergenz von IT und OT steigern Effizienz und Transparenz – erhöhen jedoch gleichzeitig die Angriffsflächen und Cyberrisiken erheblich.

Im industriellen Umfeld stehen insbesondere die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit von Steuerungs- und Prozessdaten im Fokus. Sicherheitsvorfälle können unmittelbare Auswirkungen auf Produktionsfähigkeit, Produktqualität, Umwelt- und Personensicherheit sowie auf die wirtschaftliche Stabilität und Reputation eines Unternehmens haben. Parallel verschärfen regulatorische Vorgaben sowie Kunden- und Partneranforderungen den Bedarf an einem strukturierten, nachweisbaren OT-Sicherheitsniveau.

Die Norm IEC 62443-2-1:2024 (Edition 2.0) ist der zentrale internationale Standard für Betreiber (Asset Owner) industrieller Automatisierungs- und Steuerungssysteme. Sie definiert Anforderungen an Richtlinien, Prozesse und organisatorische Maßnahmen für ein systematisches Security Programm (SP) zur Gewährleistung der Cybersicherheit im Betrieb von IACS. In der aktuellen Edition wurde der Begriff des Cyber Security Management Systems (CSMS) bewusst durch den Begriff Security Programm ersetzt, um eine bessere Anschlussfähigkeit an bestehende Informationssicherheitsmanagementsysteme (ISMS) zu erreichen und Überschneidungen konsistent zu integrieren.

Die Norm berücksichtigt explizit die langen Lebenszyklen industrieller Anlagen und adressiert den sicheren Umgang mit Legacy-Systemen durch risikobasierte und kompensierende Maßnahmen. Dabei werden technische, organisatorische, personelle und physische Aspekte der OT-Security integriert betrachtet und entlang des gesamten Anlagen- und Betriebslebenszyklus gesteuert.

Mit einer Zertifizierung nach IEC 62443-2-1 bestätigt TÜV NORD CERT, dass das Security Programm wirksam implementiert ist und OT-Cybersecurity systematisch, risikoorientiert und nachvollziehbar in der Unternehmensführung verankert wurde.

Kernmerkmale der IEC 62443-2-1 Zertifizierung

- International anerkannter Standard für den Aufbau und Betrieb eines Security Programms für industrielle Automatisierungs- und Steuerungssysteme
- Risikobasierter, lebenszyklusorientierter Ansatz zur Steuerung von IACS-Cyberrisiken
- Klare Governance-Strukturen mit definierten Rollen und Verantwortlichkeiten (z. B. Asset Owner, OT-Betrieb, Instandhaltung, Dienstleister)
- Integration von organisatorischen, technischen und prozessualen Sicherheitsmaßnahmen
- Kontinuierlicher Verbesserungsprozess (z. B. PDCA-Ansatz) zur nachhaltigen Erhöhung der Cyber-Resilienz
- Gute Kombinierbarkeit mit bestehenden Managementsystemen, insbesondere ISMS nach ISO/IEC 27001 (z. B. integrierte Audits, gemeinsame Governance-Strukturen und Synergien in Dokumentation und Risikomanagement)

Zielgruppen der Zertifizierung

Die Zertifizierung nach IEC 62443-2-1 richtet sich an Organisationen mit industriellen Steuerungs- und Automatisierungsumgebungen unterschiedlicher Branchen, Größen und Reifegrade.

Typische Zielgruppen sind Organisationen, die:

- Industrie-, Prozess- oder Energieanlagen betreiben (z. B. Fertigungsindustrie, Chemie, Öl & Gas, Energieversorgung, Wasser/Abwasser, Verkehr, Gebäudetechnik)
- Kritische Infrastrukturen oder hochverfügbare Produktionsumgebungen betreiben, bei denen OT-Störungen erhebliche Auswirkungen auf Sicherheit, Versorgung oder Lieferfähigkeit haben
- bereits ein ISMS nach ISO/IEC 27001 betreiben und ihre OT-Systeme normkonform und nachweisbar absichern möchten
- von Kunden, OEMs oder Betreibern Anforderungen an ein strukturiertes OT-Security-Management erfüllen müssen (z. B. im Rahmen von Liefer-, Betriebs- oder Serviceverträgen)
- ihre Cyber-Resilienz, Anlagenverfügbarkeit und Geschäftskontinuität über den gesamten Lebenszyklus von IACS stärken wollen

Die Norm eignet sich sowohl für Organisationen mit etablierten Managementsystemen (z. B. ISO 9001, ISO/IEC 27001) als auch für Unternehmen, die OT-Security erstmals ganzheitlich und systematisch einführen möchten.

Ihr Weg zur IEC 62443-2-1 Zertifizierung in 6 Schritten

Der Zertifizierungsprozess nach IEC 62443-2-1 folgt der bewährten Struktur von Managementsystem-Audits und wird an Größe, Komplexität und Risikoprofil der Organisation angepasst.

1. Anfrage & Angebot
2. Internes Audit
3. Audit Stufe 1 – Readiness-Bewertung
4. Audit Stufe 2 – Zertifizierungsaudit
5. Zertifizierungsentscheidung & Zertifikat
6. Überwachung & Re-Zertifizierung

Unser Know-how für Ihren Erfolg

TÜV NORD CERT ist ein international anerkannter und zuverlässiger Partner für Prüf- und Zertifizierungsdienstleistungen. Unsere Sachverständigen und Auditoren 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 Auditoren begleiten und unterstützen die Entwicklung Ihres Unternehmens und geben Ihnen ein objektives Feedback.

Kontakt

TÜV NORD CERT
ISMS Sales &
Projectmanagement

sales.isms@tuev-nord.de
tuev-nord-cert.de

Weitere Informationen und Kontaktformular:

24-0612-03/26