OVE-Richtlinie R 32

Ausgabe: 2022-06-01

Maschinensicherheit
Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen

Safety of machinery –
Security aspects related to functional safety of safety-related control systems

Sécurité des machines –
Aspects de la cybersécurité en relation avec la sécurité fonctionnelle des systèmes de commande de sécurité

Medieninhaber und Hersteller:
OVE Österreichischer Verband für Elektrotechnik

OVE Österreichischer Verband für Elektrotechnik
Eschenbachgasse 9, 1010 Wien
E-Mail: verkauf@ove.at
Internet: http://www.ove.at
Webshop: www.ove.at/webshop
Tel.: +43 1 587 63 73

ICS 13.110; 25.040.40; 35.030

Ident (IDT) mit IEC TR 63074:2019 (Übersetzung)

zuständig OVE/TK E
Elektrische Niederspannungsanlagen

Nationales Vorwort

Der Technische Bericht IEC/TR 63074:2019 wurde durch das Technische Komitee IEC TC 44 „Safety of machinery - Electrotechnical aspects“ erarbeitet.

Dieser Technische Bericht wurde vom Technischen Komitee Elektrische Niederspannungsanlagen (TK E) des OVE als OVE-Richtlinie veröffentlicht. Das Projekt wurde vom AK mit Beschluss OEK/AK/2022/C02 genehmigt.

Die nationalen Anhänge NA und NB wurde vom OVE Österreichischer Verband für Elektrotechnik hinzugefügt.

Hinweis des nationalen Spiegelgremiums zu IEC und CLC TC 44: Es bestehen auch weitere Leitlinien für IT-Sicherheits-(Cybersicherheits-) Aspekte – siehe zB ONR CEN ISO/TR 22100-4.

Inhalt

Bilder

Tabellen

Einleitung

Industriesysteme können Cyberangriffen ausgesetzt sein durch:

– möglichen Zugriff auf das Steuerungssystem, z. B. Reprogrammierung von Maschinenfunktionen (einschließlich Sicherheitsfunktionen);

– die zunehmende „Konvergenz“ zwischen Standard-IT- und Industriesystemen;

– Betriebssysteme in eingebetteten System, z. B. IP-basierte Protokolle ersetzen eigene Netzwerkprotokolle und Daten werden direkt aus dem SCADA-Netzwerk in die Büroumgebung übertragen;

– Softwareentwicklung durch die Wiederverwendung vorhandener Drittanbieter-Softwarekomponenten;

– die Tatsache, dass der Fernzugriff durch Lieferanten sich zum Standardverfahren für den Betrieb/die Instandhaltung entwickelt hat und ein erhöhtes Cybersicherheitsrisiko im Hinblick auf z. B. den unbefugten Zugang, die Verfügbarkeit und die Integrität mit sich bringt.

Als Teil eines industriellen Automatisierungssystems können sicherheitsrelevante Steuerungssysteme von Maschinen auch Cyberangriffen ausgesetzt sein, die zum Verlust der Fähigkeit führen können, den sicheren Betrieb einer Maschine aufrechtzuerhalten.

ANMERKUNG 1 Das Risikopotential von Angriffschancen ist angesichts der Trends und Entwicklungen der Bedrohungen und der Anzahl bekannter Angriffsmöglichkeiten signifikant. Sicherheitsziele werden hauptsächlich im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit beschrieben, die im Allgemeinen durch einen risikobasierten Ansatz priorisiert werden müssen.

Funktionale Sicherheitsziele betrachten das Risiko durch Schätzung des Schweregrads des Schadens und die Wahrscheinlichkeit des Auftretens dieses Schadens: Die Auswirkungen eines Risikos (gefährliches Ereignis) bestimmen die Anforderungen an die Sicherheitsintegrität (Sicherheits-Integritätslevel (SIL) nach IEC 62061 oder IEC 61508 oder Performance Level (PL) nach ISO 13849-1).

Hinsichtlich der Sicherheitsfunktion können Cybersicherheits-Bedrohungen (intern oder extern) die Sicherheitsintegrität und die gesamte Systemverfügbarkeit beeinflussen.

ANMERKUNG 2 Um die Sicherheitsziele sicherzustellen, empfiehlt und legt IEC 62443-3-3 Sicherheitsanforderungen („grundlegende Anforderungen“) fest, die von dem relevanten System zu erfüllen sind.

ANMERKUNG 3 Die allgemeine Sicherheitsstrategie wird in dieser Norm nicht behandelt. Weitere Informationen sind z. B. in IEC 62443 (alle Teile) oder ISO/IEC 27001 enthalten.

Missbrauch durch physische Manipulation wird in einigen Normen zur funktionalen Maschinensicherheit (z. B. IEC 61496 (alle Teile) und ISO 14119) behandelt.

ANMERKUNG 4 „Missbrauch durch physische Manipulation“ wird nicht als gleichbedeutend mit „physische Cybersicherheit“ in IEC 62443 (alle Teile), z. B. in IEC 62443-2-1:2010, 4.3.3.3, angesehen. Physische Cybersicherheit betrifft zum Beispiel die Zugangskontrolle (-beschränkung) durch physische Hindernisse.

Maschinensicherheit – Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen

1 Anwendungsbereich

Dieser Technische Bericht gibt eine Anleitung zur Verwendung von IEC 62443 (alle Teile) in Bezug auf solche Aspekte von Cybersicherheits-Bedrohungen und Angriffsmöglichkeiten, die die implementierte und durch sicherheitsrelevante Steuerungssysteme (SCS) umgesetzte funktionale Sicherheit beeinflussen und zu einem Verlust der Fähigkeit, den sicheren Betrieb einer Maschine aufrechtzuerhalten, führen könnten.

ANMERKUNG 1 Zum Beispiel ein Angriff auf eine Maschine (Sicherheitsfunktion), so dass die Verfügbarkeit der Maschine beeinträchtigt ist und eine Sicherheitsfunktion umgangen werden kann.

Die betrachteten Sicherheitsaspekte der Maschine mit potentiellem Zusammenhang mit dem SCS umfassen:

– Angriffsmöglichkeiten des SCS – entweder direkt oder indirekt durch die anderen Teile der Maschine –, die von Sicherheitsbedrohungen für Sicherheitsangriffe (Sicherheitsverletzungen) genutzt werden können;
– den Einfluss auf die Sicherheitseigenschaften und die Fähigkeit des SCS, seine Funktion(en) einwandfrei erfüllen zu können;
– die typische Festlegung von Anwendungsfällen und die Anwendung eines entsprechenden Bedrohungsmodells.

ANMERKUNG 2 Für andere Aspekte der Cybersicherheits-Bedrohungen und Angriffsmöglichkeiten können die Festlegungen von IEC 62443 (alle Teile) gelten.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ISO 12100:2010, *Safety of machinery – General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter http://www.electropedia.org/
- ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

3.1.1
Schutzobjekt Betriebsmittel
physikalisches oder logisches Objekt, das für ein Steuerungssystem entweder einen wahrgenommenen oder einen tatsächlichen Wert hat