

	DIN IEC/TR 63074 (VDE 0113-74)	
	Dies ist zugleich eine VDE-Leitlinie im Sinne von VDE 0022. Sie ist unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	
ICS 13.110; 25.040.40; 35.030 Maschinensicherheit – Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen (IEC TR 63074:2019) Safety of machinery – Security aspects related to functional safety of safety-related control systems (IEC TR 63074:2019) Das vorliegende Dokument wurde nach den Verfahrensregeln einer VDE-Leitlinie erstellt und ist die Übernahme eines Technischen Reports der IEC (IEC TR). Gesamtumfang 28 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn dieses Dokuments ist 2021-05-01.

Inhalt	Seite
Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Zusammenhang mit europäischen und internationalen Dokumenten	5
Nationaler Anhang NB (informativ) Literaturhinweise.....	7
EINLEITUNG	9
Maschinensicherheit – Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen.....	10
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	10
4 Sicherheits- und Schutzübersicht.....	14
4.1 Allgemeines	14
4.2 Sicherheitsziele	15
4.3 Cybersicherheitsziele	15
5 Cybersicherheitsaspekte in Zusammenhang mit der funktionalen Sicherheit	17
5.1 Allgemeines	17
5.1.1 Cybersicherheitsrisikobeurteilung	17
5.1.2 Cybersicherheitsrisikoreaktionsstrategie.....	18
5.2 Gegenmaßnahmen der Cybersicherheit	19
5.2.1 Allgemeines	19
5.2.2 Identifizierung und Authentifizierung	20
5.2.3 Nutzungskontrolle.....	21
5.2.4 Systemintegrität.....	21
5.2.5 Datenvertraulichkeit.....	21
5.2.6 Eingeschränkter Datenfluss	21
5.2.7 Zeitnahe Reaktion auf Ereignisse	21
5.2.8 Ressourcenverfügbarkeit	22
6 Verifizierung und Aufrechterhaltung von Gegenmaßnahmen der Cybersicherheit.....	22
7 Informationen für den Anwender der Maschine(n).....	22
Anhang A (informativ) Grundlegende Informationen zu Bedrohungen und dem Bedrohungssimulationsansatz	23
A.1 Bewertung von Bedrohungen	23
A.2 Beispiele für Bedrohungen in Zusammenhang mit einem sicherheitsrelevanten Gerät	24
Anhang B (informativ) Auslöser der Sicherheitsrisikobeurteilung	26

B.1	Allgemeines	26
B.2	Ereignisbasierte Auslöser	26
Anhang C (informativ) Beispiel für den Informationsfluss zwischen dem Gerätelieferanten, dem Maschinenhersteller (Integrator) und dem Endanwender der Maschine		27
C.1	Allgemeines	27
C.2	Beispiel	27
Literaturhinweise		28

Bilder

Bild 1 — Zusammenhang zwischen Bedrohungen, Angriffsmöglichkeiten, Konsequenzen und Cybersicherheitsrisiken für SCS, die Sicherheitsfunktionen ausführen	16
Bild 2 — Mögliche Auswirkungen von Sicherheitsrisiken auf ein SCS	16
Bild A.1 — Sicherheitsrelevantes Gerät und mögliche Zugänge	25
Bild C.1 — Beispiel für den Informationsfluss während der Gestaltungsphase	27

Tabellen

Tabelle NA.1	5
Tabelle 1 — Überblick über grundlegende Anforderungen und mögliche Einflüsse auf ein SCS	20

Nationales Vorwort

Vorausgegangener Entwurf: E DIN EN 63074 (VDE 0113-74):2017-12.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/K 225 "Elektrotechnische Ausrüstung und Sicherheit von Maschinen und maschinellen Anlagen" der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Die VDE-Leitlinien enthalten sicherheitstechnische Festlegungen mit einem im Vergleich zu den VDE-Bestimmungen wesentlich erweiterten Ermessensraum für eigenverantwortliches sicherheitstechnisches Handeln.

VDE-Leitlinien sind angebracht, wenn die Vielfalt der zu betrachtenden Sachlagen oder Gestaltungsmöglichkeiten nach vorherrschender Meinung durch unmittelbar anwendbare Anweisungen nicht erfasst werden kann. Sie dienen dem Anwender als Beispielsammlung oder Grundlage für eigene sicherheitstechnische Entscheidungen. Für sich allein sind sie nicht als ausreichende Entscheidungsgrundlage für die Genehmigungs- und Überwachungsbehörden oder die Anwender geeignet.

VDE-Leitlinien sind nicht Bestandteil des Deutschen Normenwerks.

Die enthaltene IEC-Publikation wurde vom IEC/TC 44 "Safety of machinery - Electrotechnical aspects" erarbeitet und unterliegt dem Copyright der IEC .

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter "<http://webstore.iec.ch>" zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

Für den Fall einer undatierten Verweisung im Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 60204-1	IEC 60204-1, mod.	DIN EN 60204-1 (VDE 0113-1)	VDE 0113-1
EN IEC 61496 (alle Teile)	IEC 61496 (alle Teile)	DIN EN IEC 61496 (alle Teile)	–
EN 61508	IEC 61508	DIN EN 61508 (VDE 0803)	VDE 0803
EN 61508-2	IEC 61508-2	DIN EN 61508-2 (VDE 0803-2)	VDE 0803-2
EN 61508-3	IEC 61508-3	DIN EN 61508-3 (VDE 0803-3)	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 62061:2005 + AC:2010 + A1:2013 + A2:2015	IEC 62061:2005 + Cor 1:2005 + Cor 2:2008 + A1:2012 + A2:2015	DIN EN 62061 (VDE 0113-50):2016-05	VDE 0113-50
–	IEC TR 62351-12	–	–
EN IEC 62443	IEC 62443 (alle Teile)	DIN EN IEC 62443 (VDE 0802) (alle Teile)	VDE 0802
–	IEC TS 62443-1-1:2009	–	–
–	IEC 62443-2-1:2010	–	–
EN IEC 62443-2-4:2019 + A1:2019	IEC 62443-2-4:2015 + Cor 1:2015 + A1:2017	DIN EN IEC 62443-2-4 (VDE 0802-2-4):2020-07	VDE 0802-2-4
–	IEC 62443-3-2	–	–
EN IEC 62443-3-3:2019 + AC:2019	IEC 62443-3-3:2013 + Cor 1:2014	DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01	VDE 0802-3-3
EN IEC 62443-4-1:2018	IEC 62443-4-1:2018	DIN EN IEC 62443-4-1 (VDE 0802-4-1):2018-10	VDE 0802-4-1
–	ISO/IEC Guide	DIN 820-12:2014-06	–

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
	51:2014		
EN ISO/IEC 27001	ISO/IEC 27001	DIN EN ISO/IEC 27001	–
EN ISO 12100:2010	ISO 12100:2010	DIN EN ISO 12100:2011-03	–
EN ISO 13849-1:2015	ISO 13849-1:2015	DIN EN ISO 13849-1:2016-06	–
EN ISO 13849-2:2012	ISO 13849-2:2012	DIN EN ISO 13849-2:2013-02	–
EN ISO 14119	ISO 14119	DIN EN ISO 14119	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60204-1(VDE 0113-1), *Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen*

DIN EN IEC 61496 (alle Teile), *Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen*

DIN EN 61508 (VDE 0803), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*

DIN EN 61508-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

DIN EN 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

DIN EN 61508-4 (VDE 0803-4):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010*

DIN EN 62061 (VDE 0113-50):2016-05, *Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005 + A1:2012 + A2:2015); Deutsche Fassung EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015*

DIN EN IEC 62443 (VDE 0802) (alle Teile), *IT-Sicherheit für industrielle Automatisierungssysteme*

DIN EN IEC 62443-2-4 (VDE 0802-2-4):2020-07, *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2015 + Cor.:2015 + A1:2017); Deutsche Fassung EN IEC 62443-2-4:2019 + A1:2019*

DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01, *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019*

DIN EN IEC 62443-4-1 (VDE 0802-4-1):2018-10, *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1:2018); Deutsche Fassung EN IEC 62443-4-1:2018*

DIN 820-12:2014-06, *Normungsarbeit – Teil 12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51:2014)*

DIN EN ISO/IEC 27001, *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen*

DIN EN ISO 12100:2011-03, *Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010); Deutsche Fassung EN ISO 12100:2010*

DIN EN ISO 13849-1:2016-06, *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015*

DIN IEC/TR 63074 (VDE 0113-74):2021-05

DIN EN ISO 13849-2:2013-02, *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012*

DIN EN ISO 14119:2014-03, *Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl*

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.