

	DIN EN IEC 62443-3-2 (VDE 0802-3-2)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
<p>ICS 25.040.40; 35.030; 35.240.50</p> <p>IT-Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 62443-3-2:2020); Deutsche Fassung EN IEC 62443-3-2:2020</p> <p>Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design (IEC 62443-3-2:2020); German version EN IEC 62443-3-2:2020</p> <p>Sécurité des systèmes d'automatisation et de commande industriels – Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes (IEC 62443-3-2:2020); Version allemande EN IEC 62443-3-2:2020</p> <p>Gesamtumfang 39 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2020-07-29 angenommene Europäische Norm als DIN-Norm ist 2021-12-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62443-3-2 (VDE 0802-3-2):2018-10.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/UK 931.1 „IT-Sicherheit in der Automatisierungstechnik“ 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 enthaltene IEC-Publikation wurde vom IEC/TC 65 „Industrial-process measurement, control and automation“ 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.

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

Für den Fall einer undatierten Verweisung im normativen 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 normativen 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 IEC 62443-2-1	IEC 62443-2-1	DIN EN IEC 62443-2-1 (VDE 0802-2-1) ^a	VDE 0802-2-1 ^a
EN IEC 62443-2-4:2019	IEC 62443-2-4:2015	DIN EN IEC 62443-2-4 (VDE 0802-2-4):2020-07	VDE 0802-2-4
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
EN IEC 62443-4-2:2019	IEC 62443-4-2:2019	DIN EN IEC 62443-4-2 (VDE 0802-4-2):2019-12	VDE 0802-4-2
EN 61511-2:2017	IEC 61511-2:2016	DIN EN 61511-2 (VDE 0810-2):2019-02	VDE 0810-2
EN 62264-1:2013	IEC 62264-1:2013	-	-
EN IEC 62443-3-3:2019	IEC 62443-3-3:2013	DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01	VDE 0802-3-3
-	IEC TS 62443-1-1	-	-
-	IEC TR 62443-2-3:2015	-	-
-	IEC TR 62443-3-1:2009	-	-
-	ISO/IEC 18028-4:2005 zurückgezogen	-	-
-	ISO/IEC 27005:2018	-	-
-	ISO 31000:2018	DIN ISO 31000:2018-10	-
^a In Vorbereitung.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN IEC 62443-2-1 (VDE 0802-2-1), *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber*

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, mit CD-ROM

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

DIN EN IEC 62443-4-2 (VDE 0802-4-2):2019-12, *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)* (IEC 62443-4-2:2019); Deutsche Fassung EN IEC 62443-4-2:2019

DIN EN 61511-2 (VDE 0810-2):2019-02, *Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie - Teil 2: Anleitungen zur Anwendung von IEC 61511-1* (IEC 61511-2:2016); Deutsche Fassung EN 61511-2:2017

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 ISO 31000:2018-10, *Risikomanagement - Leitlinien* (ISO 31000:2018)

Deutsche Fassung

IT-Sicherheit für industrielle Automatisierungssysteme –
Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung
(IEC 62443-3-2:2020)

Security for industrial automation and control systems –
Part 3-2: Security risk assessment for system design
(IEC 62443-3-2:2020)

Sécurité des systèmes d'automatisation et de
commande industriels – Partie 3-2: Évaluation des
risques de sécurité pour la conception des systèmes
(IEC 62443-3-2:2020)

Diese Europäische Norm wurde von CENELEC am 2020-07-29 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brüssel

Europäisches Vorwort

Der Text des Dokuments 65/799/FDIS, zukünftige 1. Ausgabe der IEC 62443-3-2, erarbeitet vom IEC/TC 65 „Industrial-process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 62443-3-2:2020 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2021-04-29
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2023-07-29

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

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62443-3-2:2020 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 62443-2-1	ANMERKUNG	Harmonisiert als EN IEC 62443-2-1 ²¹ .
IEC 62443-2-4:2015	ANMERKUNG	Harmonisiert als EN IEC 62443-2-4:2019 (nicht modifiziert).
IEC 62443-4-1:2018	ANMERKUNG	Harmonisiert als EN IEC 62443-4-1:2018 (nicht modifiziert).
IEC 62443-4-2:2019	ANMERKUNG	Harmonisiert als EN IEC 62443-4-2:2019 (nicht modifiziert).
IEC 61511-2:2016	ANMERKUNG	Harmonisiert als EN 61511-2:2017 (nicht modifiziert).
IEC 62264-1:2013	ANMERKUNG	Harmonisiert als EN 62264-1:2013 (nicht modifiziert).

²¹ In Vorbereitung. Dokumentstufe zum Zeitpunkt der Veröffentlichung: prEN IEC 62443-2-1:2019.

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 62443-3-3	2013	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	EN IEC 62443-3-3	2019

Inhalt

	Seite
Europäisches Vorwort.....	6
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	7
Einleitung.....	10
1 Anwendungsbereich.....	11
2 Normative Verweisungen.....	11
3 Begriffe, Abkürzungen, Akronyme und Konventionen.....	11
3.1 Begriffe.....	11
3.2 Abkürzungen und Akronyme.....	15
3.3 Konventionen.....	16
4 Anforderungen an Zonen, Conduits und Risikobeurteilungen.....	16
4.1 Überblick.....	16
4.2 ZCR 1: Identifizieren des zu betrachtenden Systems.....	18
4.2.1 ZCR 1.1: Identifizieren des SUC-Bereichs und der Zugangspunkte.....	18
4.3 ZCR 2: Anfangs-Cybersecurity-Risikobeurteilung.....	18
4.3.1 ZCR 2.1: Durchführen der Anfangs-Cybersecurity-Risikobeurteilung.....	18
4.4 ZCR 3: Aufteilung des SUC in Zonen und Conduits.....	19
4.4.1 Übersicht.....	19
4.4.2 ZCR 3.1: Zonen und Conduits festlegen.....	19
4.4.3 ZCR 3.2: Separate Geschäfts- und IACS-Betriebsmittel.....	19
4.4.4 ZCR 3.3: Separate sicherheitsgerichtete Betriebsmittel.....	20
4.4.5 ZCR 3.4: Separate vorübergehend angeschlossene Geräte.....	20
4.4.6 ZCR 3.5: Separate drahtlose Geräte.....	20
4.4.7 ZCR 3.6: Über externe Netzwerke verbundene separate Geräte.....	21
4.5 ZCR 4: Risikovergleich.....	21
4.5.1 Überblick.....	21
4.5.2 ZCR 4.1: Vergleich zwischen Anfangs-Risiko und vertretbarem Risiko.....	21
4.6 ZCR 5: Durchführen einer ausführlichen Cybersecurity-Risikobeurteilung.....	21
4.6.1 Überblick.....	21
4.6.2 ZCR 5.1: Bedrohungen identifizieren.....	22
4.6.3 ZCR 5.2: Schwachstellen identifizieren.....	23
4.6.4 ZCR 5.3: Folgen und Auswirkung bestimmen.....	23
4.6.5 ZCR 5.4: Bestimmen der ungeminderten Wahrscheinlichkeit.....	24
4.6.6 ZCR 5.5: Bestimmen des ungeminderten Cybersecurity-Risikos.....	24
4.6.7 ZCR 5.6: Bestimmen des SL-T.....	25
4.6.8 ZCR 5.7: Vergleich zwischen ungemindertem und vertretbarem Risiko.....	25
4.6.9 ZCR 5.8: Identifizieren und Bewerten bestehender Gegenmaßnahmen.....	25
4.6.10 ZCR 5.9: Wiederbewerten der Wahrscheinlichkeit und der Auswirkung.....	26
4.6.11 ZCR 5.10: Bestimmen des Restrisikos.....	26

4.6.12	ZCR 5.11: Vergleich zwischen dem Restrisiko und dem vertretbaren Risiko.....	26
4.6.13	ZCR 5.12: Identifizieren zusätzlicher Cybersecurity-Gegenmaßnahmen.....	26
4.6.14	ZCR 5.13: Dokumentieren und Kommunizieren von Ergebnissen.....	27
4.7	ZCR 6: Dokumentieren von Cybersecurity-Anforderungen, -Annahmen und -Beschränkungen.....	27
4.7.1	Überblick.....	27
4.7.2	ZCR 6.1: Festlegung der Cybersecurity-Anforderungen.....	27
4.7.3	ZCR 6.2: SUC-Beschreibung.....	28
4.7.4	ZCR 6.3: Zeichnungen der Zonen und Conduits.....	28
4.7.5	ZCR 6.4: Eigenschaften der Zonen und Conduits.....	29
4.7.6	ZCR 6.5: Annahme zur Betriebsumgebung.....	30
4.7.7	ZCR 6.6: Bedrohungsumgebung.....	31
4.7.8	ZCR 6.7: Organisatorische Security-Leitlinien.....	31
4.7.9	ZCR 6.8: Vertretbares Risiko.....	31
4.7.10	ZCR 6.9: Behördliche Vorschriften.....	31
4.8	ZCR 7: Genehmigung des Betreibers.....	32
4.8.1	Überblick.....	32
4.8.2	ZCR 7.1: Einholen der Genehmigung des Betreibers.....	32
	Anhang A (informativ) Security-Level.....	33
	Anhang B (informativ) Risikomatrizen.....	34
	Literaturhinweise	39

Bilder

Bild 1 – Arbeitsablaufdiagramm zur Darstellung der erforderlichen Hauptschritte zur Festlegung der Zonen und Conduits und zur Beurteilung des Risikos.....	17
Bild 2 – Arbeitsablauf der ausführlichen IT-Sicherheitsrisikobeurteilung je Zone oder Conduit.....	22

Tabellen

Tabelle B.1 – Beispiel für eine 3 × 5-Risikomatrix.....	34
Tabelle B.2 – Beispiel für eine Wahrscheinlichkeitsskala.....	35
Tabelle B.3 – Beispiel für eine Folge- oder Schweregradskala.....	36
Tabelle B.4 – Beispiel für eine einfache 3 × 3-Risikomatrix.....	37
Tabelle B.5 – Beispiel für eine 5 × 5-Risikomatrix.....	37
Tabelle B.6 – Beispiel für eine 3 × 4-Risikomatrix.....	38

Einleitung

Es gibt kein einfaches Rezept zur Absicherung eines industriellen Automatisierungssystems (en: industrial automation and control system, IACS) und dies hat einen guten Grund. Security ist eine Frage des Risikomanagements. Jedes IACS stellt je nach den Bedrohungen, denen es ausgesetzt ist, der Wahrscheinlichkeit, dass diese Bedrohungen auftreten, den inhärenten Schwachstellen des Systems und den Folgen der Kompromittierung des Systems ein anderes Risiko für die Organisation dar. Darüber hinaus besteht in jeder Organisation, die ein IACS besitzt und betreibt, eine unterschiedliche Risikotoleranz.

Ziel dieses Dokuments ist es, eine Reihe von Engineering-Maßnahmen festzulegen, die eine Organisation durch den Prozess der Beurteilung des Risikos eines bestimmten IACS und der Identifizierung und Anwendung von Security-Gegenmaßnahmen, um das Risiko auf ein vertretbares Maß zu reduzieren, führen.

Das Grundkonzept dieses Dokuments ist die Anwendung von Security-Zonen und Conduits für IACS. Zonen und Conduits werden in IEC TS 62443-1-1 eingeführt.

Dieses Dokument wurde in Zusammenarbeit mit ISA99 erstellt. ISA99 ist das Komitee für Cybersecurity von industriellen Automatisierungssystemen der International Society of Automation (ISA).

Dieses Dokument richtet sich an Betreiber, Systemintegratoren, Produktlieferanten, Dienstleister und Konformitätsbewertungsstellen.

Dieses Dokument bietet eine Grundlage für die Festlegung von Security-Gegenmaßnahmen durch Abstimmung der zu erreichenden Security-Level (en: target security levels, SL-Ts), die in dieser Norm festgelegt werden, mit den erreichbaren Security-Level (en: capability security levels, SL-Cs), die in **IEC 62443-3-3** festgelegt sind.

1 Anwendungsbereich

Dieser Teil von IEC 62443 legt Anforderungen fest für:

- die Festlegung eines betrachteten Systems (en: system under consideration, SUC) für ein industrielles Automatisierungssystem (IACS);
- die Aufteilung des SUC in Zonen und Conduits;
- die Beurteilung des Risikos für jede Zone und jeden Conduit;
- die Festlegung des zu erreichenden Security-Level (SL-T) für jede Zone und jeden Conduit; und
- die Dokumentation der Security-Anforderungen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

3 Begriffe, Abkürzungen, Akronyme und Konventionen

3.1 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: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1.1

Kanal

en **channel**

eine spezifische logische oder physische Kommunikationsverbindung zwischen Betriebsmitteln

Anmerkung 1 zum Begriff: Ein Kanal ermöglicht die Herstellung einer Verbindung.

3.1.2

Konformitätsbewertungsstelle

en **compliance authority**

eine Stelle, die für die Bestimmung der Angemessenheit einer Security-Beurteilung oder der Effektivität der Implementierung in Übereinstimmung mit einem maßgebenden Dokument zuständig ist

Anmerkung 1 zum Begriff: Beispiele für Konformitätsbewertungsstellen sind Regierungsbehörden, Regulierer, externe und interne Prüfer.

3.1.3

Conduit

en **conduit**

eine logische Gruppierung von Kommunikationskanälen, die gemeinsamen Security-Anforderungen unterliegen und zwei oder mehr Zonen miteinander verbinden

3.1.4

Vertraulichkeit

en **confidentiality**

Bewahrung autorisierter Beschränkungen des Zugangs zu Informationen und deren Offenlegung, dies schließt auch Mittel zum Datenschutz und Schutz eigener Informationen ein

3.1.5

Folge

en **consequence**

Ergebnis eines Zwischenfalls, üblicherweise beschrieben durch seine Gesundheits- und Sicherheitsauswirkungen, Umweltauswirkungen, Sachschäden, Informationsverlust (zum Beispiel geistiges Eigentum) und/oder die Kosten von Betriebsunterbrechungen aufgrund eines bestimmten Zwischenfalls

3.1.6

Gegenmaßnahme

en **countermeasure**

Tätigkeit, Gerät, Verfahren oder Technik, durch das/die eine Bedrohung, eine Sicherheitslücke oder die Folgen eines Angriffs verringert werden, und zwar durch Beseitigen, Verhindern, Verringern des möglichen Schadens oder durch Entdeckung und Bericht, so dass Korrekturmaßnahmen eingeleitet werden können

Anmerkung 1 zum Begriff: Im Englischen wird in einigen Zusammenhängen auch die Benennung „control“ benutzt, um diesen Begriff zu beschreiben. Die Benennung „countermeasure“ wurde im englischen Dokument verwendet, um eine Verwechslung mit der Benennung „control“ im Zusammenhang mit „process control“ zu vermeiden.

3.1.7

Cybersecurity

en **cyber security**

getroffene Maßnahmen zum Schutz eines Computers oder Computersystems gegen nicht autorisierten Zugriff oder Angriff

Anmerkung 1 zum Begriff: IACS sind Computersysteme.

3.1.8

Datenfluss

en **data flow**

Bewegung von Daten durch ein aus Software, Hardware oder einer Kombination aus beidem bestehenden System

3.1.9

externes Netzwerk

en **external network**

mit dem SUC verbundenes Netzwerk, das nicht Teil des SUC ist

3.1.10

Auswirkung

en **impact**

Maß des gesamten Verlusts oder Schadens in Verbindung mit einer Folge

BEISPIEL Die Folge eines Vorfalls war verschüttetes Material. Die Auswirkung des Verschüttens bestand in einer Geldstrafe von 100 000 \$ und 25 000 \$ Reinigungskosten.

Anmerkung 1 zum Begriff: Eine Auswirkung kann als Anzahl von Verletzungen und/oder Todesfällen, Maß von Umweltschäden und/oder Höhe von Verlusten wie etwa Sachschäden, Materialverluste, Verlust geistigen Eigentums, Produktionsverluste, Marktanteilverluste und Wiederherstellungskosten ausgedrückt werden.

3.1.11

Wahrscheinlichkeit

en **likelihood**

Möglichkeit, dass etwas geschieht