DIN CLC IEC/TR 61511-4 (VDE 0810-4)

DIN

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.

VDE

ICS 25.040.40; 35.240.50

Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – Teil 4: Erläuterung und Gründe der Änderungen in der IEC 61511-1 von Edition 1 zu Edition 2 (IEC/TR 61511-4:2020); Deutsche Fassung CLC IEC/TR 61511-4:2020

Functional safety –
Safety instrumented systems for the process industry sector –
Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2
(IEC/TR 61511-4:2020);
German version CLC IEC/TR 61511-4:2020

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le secteur des industries de transformation –
Partie 4: Explication et justifications relatives aux modifications apportées entre l'Edition 1 et l'Edition 2 de l'IEC 61511-1
(IEC/TR 61511-4:2020);
Version allemande CLC IEC/TR 61511-4:2020

Das vorliegende Dokument wurde nach den Verfahrensregeln einer VDE-Leitlinie erstellt und ist die Übernahme eines Technischen Reports des CENELEC (CLC IEC/TR).

Gesamtumfang 53 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Anwendungsbeginn

Anwendungsbeginn für den von CENELEC am 2020-09-14 angenommenen Technischen Report als VDE-Leitlinie ist 2021-05-01.

Nationales Vorwort

Für dieses Dokument ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ 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/SC 65A „System 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.

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

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
–	IEC 60050-192	a	–
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61511-1:2004 ersetzt durch EN 61511-1:2017 + A1:2017	IEC 61511-1:2003 + Cor.:2004 ersetzt durch IEC 61511-1:2016 + Cor.1:2016 + A1:2017	DIN EN 61511-1 (VDE 0810-1):2005-05 ersetzt durch DIN EN 61511-1 (VDE 0810-1):2019-02	VDE 0810-1 VDE 0810-1
–	ISO/IEC Guide 51:2014	DIN 820-12:2014-06	–
–	IEC 60050 (alle Teile)	a	–
EN 61131-3:2003 ersetzt durch EN 61131-3:2013	IEC 61131-3:2003 ersetzt durch IEC 61131-3:2013	DIN EN 61131-3:2003-12 ersetzt durch DIN EN 61131-3:2014-06	– –
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN IEC 61508 (VDE 0803) (alle Teile)	VDE 0803 (alle Teile)
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7

AVA Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61511-2:2017	IEC 61511-2:2016	DIN EN 61511-2 (VDE 0810-2):2019-02	VDE 0810-2
EN 61511-3:2017	IEC 61511-3:2016	DIN EN 61511-3 (VDE 0810-3):2019-02	VDE 0810-3
EN 61703:2016	IEC 61703:2016	DIN EN 61703:2017-08	–
EN IEC 62443 (alle Teile)	IEC 62443 (alle Teile)	DIN EN IEC 62443 (VDE 0802) (alle Teile)	VDE 0802 (alle Teile)
EN ISO 9001:2015	ISO 9001:2015	DIN EN ISO 9001:2015-11	–
EN ISO 14224:2016	ISO 14224:2016	DIN EN ISO 14224:2017-04	–
[a] „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: http://www.dke.de/dke-iev.			

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Nationaler Anhang NB
(informativ)

Literaturhinweise

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

DIN EN 61131-3:2014-06, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (IEC 61131-3:2013); Deutsche Fassung EN 61131-3:2013*

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010*

DIN EN 61508-2 (VDE 0803-2):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010*

DIN EN 61508-3 (VDE 0803-3):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010*

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 61508-5 (VDE 0803-5):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010*

DIN EN 61508-6 (VDE 0803-6):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010*

DIN EN 61508-7 (VDE 0803-7):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010*

DIN EN 61511-1 (VDE 0810-1):2019-02, *Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61511-1:2016 + COR1:2016 + A1:2017); Deutsche Fassung EN 61511-1:2017 + A1:2017*

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 61511-3 (VDE 0810-3):2019-02, *Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2016); Deutsche Fassung EN 61511-3:2017*

DIN EN 61703:2017-08, *Mathematische Ausdrücke für Begriffe der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft (IEC 61703:2016); Deutsche Fassung EN 61703:2016*

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

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

DIN EN ISO 9001:2015-11, *Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015*

DIN EN ISO 14224:2017-04, *Erdöl-, petrochemische und Erdgasindustrie – Sammlung und Austausch von Zuverlässigkeits- und Wartungsdaten für Ausrüstungen (ISO 14224:2016, korrigierte Fassung 2016-10-01); Englische Fassung EN ISO 14224:2016, nur auf CD-ROM*

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

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

TECHNISCHER REPORT

TECHNICAL REPORT

RAPPORT TECHNIQUE

CLC IEC/TR 61511-4

September 2020

ICS 13.110; 25.040.01

Deutsche Fassung

Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – Teil 4: Erläuterung und Gründe der Änderungen in der IEC 61511-1 von Edition 1 zu Edition 2

(IEC/TR 61511-4:2020)

Functional safety –
Safety instrumented systems for the process industry sector –
Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2
(IEC/TR 61511-4:2020)

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le secteur des industries de transformation –
Partie 4: Explication et justifications relatives aux modifications apportées entre l'Edition 1 et l'Edition 2 de l'IEC 61511-1
(IEC/TR 61511-4:2020)

Dieser Technische Report wurde von CENELEC am 2020-09-14 angenommen.

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

© 2020 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. CLC IEC/TR 61511-4:2020 D

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Europäisches Vorwort

Der Text des Dokuments (65A/911/DTR), zukünftige 1. Ausgabe der IEC/TR 61511-4, erarbeitet vom SC 65A „System aspects“ des IEC/TC 65 „Industrial-process measurement, control and automation“ wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als CLC IEC/TR 61511-4:2020 angenommen.

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/TR 61511-4:2020 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.[N1]

[N1] Nationale Fußnote: Der Satz muss korrekt lauten: „Der Text Internationalen Technischen Reports IEC/TR 61511-4:2020 wurde von CENELEC ohne irgendeine Abänderung als Europäischer Technischer Report angenommen.“.

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

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.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 60050-192	–	International electrotechnical vocabulary – Part 192: Dependability	–	–
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations (see Functional Safety and IEC 61508)	EN 61508-4	2010
IEC 61511-1	2016	Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements	EN 61511-1	2017
+A1	2017		+ A1	2017
ISO/IEC Guide 51	2014	Safety aspects – Guidelines for their inclusion in standards	–	–

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Inhalt

Seite

Europäisches Vorwort ... 2

Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 3

Einleitung ... 7

1 Anwendungsbereich ... 8

2 Normative Verweisungen ... 8

3 Begriffe und Abkürzungen ... 8

3.1 Begriffe ... 8

3.2 Abkürzungen ... 8

4 Hintergrund ... 10

5 Management der funktionalen Sicherheit (IEC 61511-1, Ausgabe 2, Abschnitt 5) ... 10

5.1 Warum ist dieser Abschnitt wichtig? ... 10

5.2 Häufige Missverständnisse ... 10

5.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 11

5.3.1 Existierende Systeme ... 11

5.3.2 Änderungsmanagement ... 11

5.3.3 Leistungsmetriken und Qualitätssicherung ... 11

5.3.4 Kompetenz ... 12

5.3.5 Mehr Anforderungen an Anbieter von Produkten und Dienstleistungen für funktionale Sicherheit ... 12

5.4 Zusammenfassung über das „Wie“ ... 12

6 Sicherheitslebenszyklus (IEC 61511-1, Ausgabe 2, Abschnitt 6) ... 13

6.1 Warum ist dieser Abschnitt wichtig? ... 13

6.2 Häufige Missverständnisse ... 13

6.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 13

6.4 Zusammenfassung über das „Wie“ ... 13

7 Verifikation (IEC 61511-1, Ausgabe 2, Abschnitt 7) ... 13

7.1 Warum ist dieser Abschnitt wichtig? ... 13

7.2 Häufige Missverständnisse ... 13

7.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 14

7.4 Zusammenfassung über das „Wie“ ... 14

8 Gefährdungs- und Risikobeurteilung (IEC 61511-1, Ausgabe 2, Abschnitt 8) ... 14

8.1 Warum ist dieser Abschnitt wichtig? ... 14

8.2 Häufige Missverständnisse ... 14

8.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 15

8.4 Zusammenfassung über das „Wie“ ... 15

9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen (IEC 61511-1, Ausgabe 2, Abschnitt 9) ... 16

9.1 Warum ist dieser Abschnitt wichtig? ... 16

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Seite

9.2 Häufige Missverständnisse 16
9.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? 16
9.3.1 Abgrenzung der PLT-Betriebseinrichtung als Schutzebene 16
9.3.2 Anforderungen an eine Gesamtrisikominderung > 10 000 für sicherheitsrelevante PLT-Einrichtungen 17
9.4 Zusammenfassung über das „Wie“ 17
10 Spezifikation der Sicherheitsanforderungen für PLT-Sicherheitseinrichtung (IEC 61511-1, Ausgabe 2, Abschnitt 10) 18
10.1 Warum ist dieser Abschnitt wichtig? 18
10.2 Häufige Missverständnisse 18
10.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? 19
10.4 Zusammenfassung über das „Wie“ 19
11 Entwurf und Planung (IEC 61511-1, Ausgabe 2, Abschnitt 11) 19
11.1 Warum ist dieser Abschnitt wichtig? 19
11.2 Häufige Missverständnisse 20
11.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? 21
11.3.1 Hardware-Fehlertoleranz 21
11.3.2 Anforderungen an die Informationssicherheit (security) 21
11.3.3 Sicherheitshandbuch 22
11.3.4 Anforderungen an das Systemverhalten beim Erkennen eines Fehlers 22
11.3.5 Einschränkungen beim Kommunikationsdesign von Feldgeräten 22
11.4 Zusammenfassung über das „Wie“ 22
12 Entwicklung des Anwendungsprogramms (IEC 61511-1, Ausgabe 2, Abschnitt 12) 23
12.1 Warum ist dieser Abschnitt wichtig? 23
12.2 Häufige Missverständnisse 23
12.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? 23
12.4 Zusammenfassung über das „Wie“ 24
13 Werksendprüfungen (IEC 61511-1, Ausgabe 2, Abschnitt 13) 24
13.1 Warum ist dieser Abschnitt wichtig? 24
13.2 Häufige Missverständnisse 24
13.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? 24
13.4 Zusammenfassung über das „Wie“ 25
14 Montage (IEC 61511-1, Ausgabe 2, Abschnitt 14) 25
14.1 Warum ist dieser Abschnitt wichtig? 25
14.2 Häufige Missverständnisse 25
14.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? 25
14.4 Zusammenfassung über das „Wie“ 25
15 Validierung (IEC 61511-1, Ausgabe 2, Abschnitt 15) 26
15.1 Warum ist dieser Abschnitt wichtig? 26

Documents
Document Sharing Hub
Full document details: DIN CLC IEC/TR 61511-4:2021-05

Seite

15.2 Häufige Missverständnisse ... 26
15.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 26
15.4 Zusammenfassung über das „Wie“ ... 26
16 Betrieb und Instandhaltung (IEC 61511-1, Ausgabe 2, Abschnitt 16) ... 27
16.1 Warum ist dieser Abschnitt wichtig? ... 27
16.2 Häufige Missverständnisse ... 27
16.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 27
16.3.1 Fehlererkennung, Überbrückungs- und Ausgleichsmaßnahmen ... 27
16.3.2 Funktionstests nach Reparatur und Änderung ... 28
16.4 Zusammenfassung über das „Wie“ ... 28
17 Modifikation (IEC 61511-1, Ausgabe 2, Abschnitt 17) ... 28
17.1 Warum ist dieser Abschnitt wichtig? ... 28
17.2 Häufige Missverständnisse ... 28
17.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 29
17.4 Zusammenfassung über das „Wie“ ... 29
18 Außerbetriebnahme (IEC 61511-1, Ausgabe 2, Abschnitt 18) ... 29
18.1 Warum ist dieser Abschnitt wichtig? ... 29
18.2 Häufige Missverständnisse ... 29
18.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 30
18.4 Zusammenfassung über das „Wie“ ... 30
19 Dokumentation (IEC 61511-1, Ausgabe 2, Abschnitt 19) ... 30
19.1 Warum ist dieser Abschnitt wichtig? ... 30
19.2 Häufige Missverständnisse ... 30
19.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 30
19.4 Zusammenfassung über das „Wie“ ... 30
20 Definitionen (IEC 61511-1, Ausgabe 2, Abschnitt 3) ... 31
20.1 Warum ist dieser Abschnitt wichtig? ... 31
20.2 Häufige Missverständnisse ... 31
20.3 Was wurde von Ausgabe 1 zu Ausgabe 2 geändert und warum? ... 31
20.4 Zusammenfassung über das „Wie“ ... 45
Literaturverzeichnis ... 46

Tabellen

Tabelle 1 – Verwendete Abkürzungen in IEC TR 61511-4 ... 9
Tabelle 2 – Begründung für Definition in IEC 61511-1, Ausgabe 2 ... 32

Documents
Document Sharing Hub
Full document details: DIN CLC IEC/TR 61511-4:2021-05

Einleitung

IEC 61511 (alle Teile) behandelt PLT-Sicherheitssystem (Sicherheitstechnische Systeme, SIS) der Prozessindustrie. Sie wurde geschrieben, um in diesem Sektor vertraute Begriffe zu verwenden und um praktische Umsetzungsanforderungen auf der Grundlage der in der Sicherheitsgrundnorm IEC 61508 vorgestellten branchenunabhängigen Abschnitte zu definieren. IEC 61511-1 wird in vielen Ländern als gute Ingenieurpraxis und in immer mehr Ländern als regulatorische Anforderung anerkannt.

Dennoch entwickeln sich Normen mit der Anwendungserfahrung der betroffenen Branche weiter. Die zweite Ausgabe von IEC 61511-1 wurde auf der Grundlage der zehnjährigen internationalen Erfahrung in der Prozessindustrie bei der Anwendung der ersten Ausgabe der IEC 61511-1:2003 herausgegeben. Die Änderungen von Ausgabe 1 zu Ausgabe 2 wurden durch Kommentare von nationalen Komitees initiiert, die ein breites Spektrum von Anwendern der Norm weltweit vertreten.

In Ausgabe 1 wurden die Anforderungen an die Vermeidung und Beherrschung systematischer Fehler, die während des Entwurfs, der Konstruktion, des Betriebs, der Wartung und der Modifikation auftreten, in erster Linie angepasst, um unabhängige Sicherheitsfunktionen bis zu einem SIL 3-Leistungsziel zu unterstützen. Im Gegensatz dazu musste Ausgabe 2 (2016) dem vorherrschenden Trend der gemeinsamen Nutzung von Automatisierungssystemen über mehrere Sicherheitsfunktionen hinweg Rechnung tragen.

Ausgabe 2 musste auch auf die gängigen Fehlinterpretationen von Ausgabe 1 eingehen, die dem IEC 61511-Wartungsteam (MT 61511) in den vergangenen Jahren offensichtlich wurden. Zum Beispiel wurde in Ausgabe 2 die Notwendigkeit bekräftigt, das Design auf das Management der funktionalen Sicherheit auszurichten, anstatt sich eng auf eine Berechnung zu konzentrieren und die tatsächliche Leistung des PLT-Sicherheitssystem im Laufe der Zeit zu verwalten.

IEC TR 61511-4 wurde geschaffen, um einem allgemeinen Publikum eine kurze Einführung in die oben genannten Themen zu geben, wobei die detaillierteren Inhalte in den Hauptteilen der Normenreihe IEC 61511 verbleiben. IEC TR 61511-4 beschreibt die zugrundeliegende Begründung der Hauptabschnitte von IEC 61511-1, erklärt einige häufige Missverständnisse bei der Anwendung, enthält eine Liste der Hauptunterschiede zwischen der ersten und zweiten Ausgabe von IEC 61511-1 und gibt eine kurze Erläuterung der typischen verfahrenstechnischen Industrieansätze für die Anwendung jedes Primärsatzes.

AVA Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

1 Anwendungsbereich

Dieser Teil der Normenreihe IEC 61511, der ein Technischer Report ist,

- legt das Grundprinzip aller Abschnitte und die Beziehung zwischen ihnen fest,
- schärft das Bewusstsein für die häufigsten Missverständnisse und Fehlinterpretationen der Klauseln und die damit verbundenen Änderungen,
- erklärt die Unterschiede zwischen Ausgabe 1 und 2 der IEC 61511-1 und die Gründe für die Änderungen,
- präsentiert übersichtliche Zusammenfassungen, wie die Anforderungen der Klauseln zu erfüllen sind, und
- erklärt Unterschiede der Begriffe zwischen IEC 61508-4:2010 und IEC 61511-1, Ausgabe. 2.

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 60050-192, *International Electrotechnical Vocabulary (IEV) – Part 192: Dependability (verfügbar unter http://www.electropedia.org)*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 4: Definitions and abbreviations*

IEC 61511-1:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*
IEC 61511-1:2016/AMD1:2017

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC Guide 51, IEC 60050-192, IEC 61508-4 und IEC 61511-1.

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

3.2 Abkürzungen

Die in diesem Dokument verwendeten Abkürzungen sind in Tabelle 1 aufgeführt. Es werden auch einige gebräuchliche Abkürzungen im Zusammenhang mit der funktionalen Sicherheit im Prozessbereich aufgeführt.

Documents
Document Sharing Hub

Full document details: DIN CLC IEC/TR 61511-4:2021-05

Tabelle 1 – Verwendete Abkürzungen in IEC TR 61511-4

AIChE	Amerikanische Organisation der Chemie-Ingenieure (en: American Institute of Chemical Engineers)
ANSI	US-amerikanische Normungsorganisation (en: American National Standards Institute)
BPCS	PLT-Betriebseinrichtung (en: Basic process control system)
CCPS	Zentrum für Sicherheit chemischer Prozesse (en: Centre for Chemical Process Safety (AIChE))
Ed.	Ausgabe (en: edition)
FAT	Werksendprüfung (en: Factory acceptance test)
FMEA	Fehlermöglichkeits- und -einflussanalyse (en: Failure mode and effects analysis)
FMEDA	Fehlermöglichkeits-, -diagnose- und -einflussanalyse (en: Failure modes, effects, and diagnostic analysis)
FPL	Feste Programmiersprache (en: Fixed program language)
FSA	Betrachtung der Funktionalen Sicherheit (en: Functional safety assessment)
FVL	Programmiersprache mit nicht eingeschränktem Sprachumfang (en: Full variability language)
HFT	Hardware-Fehlertoleranz (en: Hardware fault tolerance)
H&RA	Gefährdungs- und Risikobeurteilung (en: Hazard and Risk Assessment)
HAZOP	Gefahren- und Funktionsfähigkeitsanalysen (en: Hazard and Operability Study)
HMI	Mensch-Maschine-Schnittstelle (en: Human Machine Interface)
IEC	Internationale Elektrotechnische Kommission (en: International Electrotechnical Comission)
IPL	unabhängigen Schutzebenene (en: Independent Protection Layer)
ISA	Internationale Gesellschaft für Automatisierung (en: International Society of Automation)
ISO	Internationale Organisation für Normung (en: International Organization for Standardization)
LOPA	Schutzebenenanalyse (en: Layers of Protection Analysis)
LVL	Sprache mit eingeschränktem Sprachumfang (en: Limited variability language)
MOC	Änderungsmanagement (en: Management of change)
MooN	M von N (en: “M” out of “N” channel architecture)
MPRT	Maximal zulässige Reparaturzeit (en: Maximum permitted repair time)
MRT	Mittlere Reparaturzeit (en: Mean repair time)
MTTR	Mittlere Zeit bis zur Wiederherstellung (en: Mean time to restoration)
NP	nicht programmierbar (en: Non-programmable)
PE	Programmierbare Elektronik (en: Programmable electronics)
PES	Programmierbares elektronisches System (en: Programmable electronic system)
PFD_{avg}	Mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls bei Anforderung (en: Average probability of dangerous failure on demand)
RRF	Risikominderung (en: Risk reduction factor)
SAT	Vor-Ort-Abnahme (en: Site acceptance test)
SIF	PLT-Sicherheitsfunktion (en: Safety instrumented function)
SIL	Sicherheits-Integritätslevel (en: Safety integrity level)
SIS	PLT-Sicherheitseinrichtung oder PLT-Sicherheitssystem (en: Safety instrumented system)
SRS	Spezifikation der Sicherheitsanforderungen (en: Safety requirement specification)

Documents
Document Sharing Hub
Full document details: DIN CLC IEC/TR 61511-4:2021-05

4 Hintergrund

Die Dokumentenstruktur, die vom ursprünglichen IEC 61511-Team gewählt wurde, bietet keine ausreichenden Details für die Klarheit über die Absicht oder die Gründe für die Schaffung oder Änderung eines Abschnittes. Es besteht die Notwendigkeit, die Änderungen zu erklären, die Gründe für jeden Abschnitt der Norm anzugeben und einführende Informationen zur funktionalen Sicherheit in der Prozessindustrie zu liefern.

Dieses Dokument hilft bei der Verbesserung der Umsetzung der Anforderungen der IEC 61511-1, Ausgabe 2 in der gesamten Industrie, indem es einen Überblick über das „Was", „Warum" und „Wie" gibt. Mit dieser Zusammenfassung sollen Neueinsteiger in die funktionale Sicherheit einen einfachen Weg finden, die zugrunde liegenden Konzepte hinter den Abschnitten dieser Norm zu verstehen.

5 Management der funktionalen Sicherheit (IEC 61511-1, Ausgabe 2, Abschnitt 5)

5.1 Warum ist dieser Abschnitt wichtig?

Das Management der funktionalen Sicherheit adressiert systematische Ausfälle, meist von Menschen verursacht, die als mathematische Modelle nicht quantifizierbar sind. Diese Aktivitäten, die den gesamten Sicherheitslebenszyklus abdecken, werden durch Prozesse und Verfahren angewandt.

Funktionale Sicherheit kann nicht umgesetzt werden ohne die Einbeziehung von Menschen wie das beteiligte Personal, das an den Aktivitäten des Sicherheitslebenszyklus eines Betriebs, eines Ingenieurbüros, eines Lieferanten oder jeder anderen Person, die mit dem Sicherheitssystem interagiert, beteiligt ist. In diesem multidisziplinären Umfeld müssen alle Aktivitäten klar identifiziert und Personen zugeordnet werden. Dies erhöht die Wahrscheinlichkeit, dass nichts von der Aufgabenliste weggelassen wird und stellt sicher, dass es für jede Aufgabe eine verantwortliche Person gibt.

Um die Erfolgsquote bei jeder Aufgabe zu erhöhen, fordert IEC 61511-1 die Kompetenz aller Mitarbeiter in den ihnen zugewiesenen Verantwortlichkeiten für den Sicherheitslebenszyklus einer PLT-Sicherheitseinrichtung. Sowohl verantwortliche als auch rechenschaftspflichtige Personen sind eingeschlossen. Die rechenschaftspflichtige Person ist die Person, die am Ende für die Aktivität oder Entscheidung verantwortlich ist. Einer Aktion kann nur eine rechenschaftspflichtige Person zugeordnet werden. Die verantwortliche Person ist(sind) die Person(en), die die Aufgabe erfüllt (erfüllen).

Es wird zwischen der Beurteilung der funktionalen Sicherheit und dem Audit der funktionalen Sicherheit unterschieden. Die Beurteilung der funktionalen Sicherheit ist eine detaillierte Überprüfung aller Aspekte einer bestimmten Phase des Sicherheitslebenszyklus. Der Zeitplan für die einzelnen Beurteilungszeitpunkte der funktionalen Sicherheit 1, 2 und 3, die auf verschiedene Projektmeilensteine abgestimmt sind, richtet sich danach, wo die Arbeit am kosteneffizientesten durchgeführt wird, im Gegensatz zu einer einzelnen Beurteilung der funktionalen Sicherheit, die am Ende des Projekts durchgeführt wird. Beim Audit der funktionalen Sicherheit hingegen werden Informationen, Dokumente und Aufzeichnungen überprüft, um festzustellen, ob das Managementsystem für die funktionale Sicherheit vorhanden ist.

5.2 Häufige Missverständnisse

Es besteht der Irrglaube, dass die Strenge von Managementsystem und Entwurfsanforderungen der IEC 61511-1 für SIL 1 weniger wichtig ist als für SIL 3. Die übergeordneten Managementsysteme für funktionale Sicherheit (wie z. B. Qualifizierung, Management von Änderungen, Bewertung und Auditierung) in IEC 61511-1 sind die gleichen und zielen darauf ab, systematische Fehler zu vermeiden oder zu beherrschen. Obwohl die Implementierung von Sicherheits- und Nicht-Sicherheitsfunktionen in ein und demselben System nicht angeregt wird, könnten einige Aspekte des Managements der funktionalen Sicherheit für kritische Nicht-Sicherheitssysteme wie z. B. Anlagenschutzsysteme vorteilhaft genutzt werden.

Der Wunsch der Projektteams nach fertig umsetzbaren Lösungen führt manchmal zu einer „Checklisten-Mentalität" (Erstellung einer Liste von Projektergebnissen, die abgehakt werden müssen, ohne dass ein wirksamer Inhalt sichergestellt ist). Managementsysteme sind „lebendige" Systeme, die ständig gepflegt

Documents
Document Sharing Hub
Full document details: DIN CLC IEC/TR 61511-4:2021-05