

DIN EN 61784-3-100

ICS 35.160; 35.240.50

Entwurf

Einsprüche bis 2015-01-28
Vorgesehen als Ersatz für
DIN EN 61784-3-2:2012-03,
DIN EN 61784-3-3:2012-03,
DIN EN 61784-3-8:2012-03 und
DIN EN 61784-3-13:2012-03

**Industrielle Kommunikationsnetze –
Profile –****Teil 3-x: Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie x
(IEC 65C/780/CDV:2014);
Englische Fassung FprEN 61784-3-X:2014**

Industrial communication networks –
Profiles –

Part 3-x: Functional safety fieldbuses – Additional specifications for CPF x
(IEC 65C/780/CDV:2014);
English version FprEN 61784-3-X:2014

Réseaux de communication industriels –
Profils –

Partie 3-x: Bus de terrain de sécurité fonctionnelle – Spécifications supplémentaires pour
CPF x
(CEI 65C/780/CDV:2014);
Version anglaise FprEN 61784-3-X:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-11-28 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 755 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Die englische Fassung des europäischen Dokuments FprEN 61784-3-X:2014 „Industrielle Kommunikationsnetze – Profile – Teil 3-x: Funktional sichere Übertragung bei Feldbussen – Zusätzliche Festlegungen für die Kommunikationsprofilfamilie x“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65C/780/CDV:2014 „Industrial communication networks – Profiles – Part 3-x: Functional safety fieldbuses – Additional specifications for CPF x“ unverändert in den Entwurf FprEN 61784-3-X:2014 übernommen worden.

Das internationale Dokument wurde vom SC 65C „Industrial networks“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium UK 914.1 „Profile für funktional sichere Kommunikationssysteme“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

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

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

DIN EN 61784-3 (VDE 0803-500-3) erläutert die Grundsätze für funktional sichere Kommunikation, bezogen auf die Normen der Reihe DIN EN 61508 (VDE 0803). Für sie ist eine deutsche Sprachfassung verfügbar.

Die Normen der Reihe DIN EN 61784-3 legen mehrere Sicherheitskommunikationsschichten (Profile und entsprechende Protokolle) basierend auf den Kommunikationsprofilen und Protokollschichten der DIN EN 61784-1, der DIN EN 61784-2 und der Reihe DIN EN 61158 fest. Für diese Kommunikationsnormen ist keine deutsche Sprachfassung verfügbar. Sie allein sind nicht ausreichend zur Auslegung eines sicherheitsbezogenen Systems nach DIN EN 61508 (VDE 0803), stets ist die Beachtung der letztgenannten Normenreihe und der DIN EN 61784-3 erforderlich.

Die Kommunikationsnormen der Reihe DIN EN 61784-3 weisen alle die gleiche Gliederung auf, sie ist in DIN EN 61784-3 (VDE 0803-500), Anhang C, in deutscher und englischer Sprache wiedergegeben, so dass ein Bezug zwischen der deutschsprachigen DIN EN 61784-3 (VDE 0803-500) und der englischsprachigen Reihe DIN EN 61784-3-x jederzeit möglich ist. Darüber hinaus sind in ersterer alle Begriffe und Abkürzungen jeweils in Deutsch und Englisch wiedergegeben.

— Entwurf —

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für den vorliegenden Normentwurf erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der E DIN EN 61784-3-100 veröffentlicht. Zu deren Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Änderungen

Gegenüber DIN EN 61784-3-2:2012-03, DIN EN 61784-3-3:2012-03, DIN EN 61784-3-8:2012-03 und DIN EN 61784-3-13:2012-03 wurden folgende Änderungen vorgenommen:

- a) Änderungen in den Normenteilen IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-8, IEC 61784-3-13 vorgenommen und neuer Normenteil IEC 61784-17 hinzugefügt.

Nationaler Anhang NA (informativ)

61784-3-2

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe

3.1.1.1

Verfügbarkeit

(en: **availability**)

Wahrscheinlichkeit eines automatisierten Systems, dass innerhalb einer bestimmten Zeitdauer keine unzureichenden Systembedingungen wie Produktionsausfall auftreten

3.1.1.2

Black Channel

(en: **black channel**)

Kommunikationskanal ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach IEC 61508

3.1.1.3**Bridge****(en: bridge)**

abstraktes Gerät, das auf der Sicherungsebene mehrere Netzwerksegmente verbindet

3.1.1.4**Kommunikationskanal****(en: communication channel)**logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem***3.1.1.5****Kommunikationssystem****(en: communication system)**Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von *Nachrichten* (ISO/IEC 7498-Anwendungsschicht) von einer Anwendung zur anderen**3.1.1.6****Verbindung****(en: connection)**

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.7**CRC****(en: Cyclic Redundancy Check (CRC))**

<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode> Prozedur zur Berechnung der redundanten Daten

ANMERKUNG 1 Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

ANMERKUNG 2 Siehe auch [34], [35]¹⁾.**3.1.1.8****Fehler****(en: error)**

Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

[IEC 61508-4:2010²⁾], [IEC 61158]

ANMERKUNG 1 Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder andere Effekte.

ANMERKUNG 2 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.**3.1.1.9****Ausfall****(en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder der Betrieb einer Funktionseinheit anders als gefordert

ANMERKUNG 1 Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.11, modifiziert]

¹⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

²⁾ Noch zu veröffentlichen.

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Softwareentwurfs oder eine Nachrichtenstörung).

3.1.1.10

Fehlzustand

(en: **fault**)

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, auslösen kann

ANMERKUNG IEC 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder aufgrund fehlender externer Betriebsmittel.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.10, modifiziert]

3.1.1.11

Feldbus

(en: **fieldbus**)

Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

3.1.1.12

Telegrammrahmen

(en: **frame**)

veraltetes Synonym für DLPDU

3.1.1.13

Hash-Funktion

(en: **hash function**)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einen (üblicherweise) kleineren Wertebereich abbildet

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[IEC/TR 62210, modifiziert]

3.1.1.14

Gefährdung

(en: **hazard**)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.1.15

Master

(en: **master**)

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einrichten und festlegen kann

3.1.1.16

Nachricht

(en: **message**)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.17

Fehlauslösung

(en: **nuisance trip**)

unberechtigte Auslösung ohne schädliche Wirkung

ANMERKUNG Interne außergewöhnliche Fehler können z. B. in Kommunikationssystemen wie Funkübertragung durch zu viele Wiederholungen unter Störeinfluss auftreten.

3.1.1.18

Performance Level (PL)

(en: performance level (PL))

diskrete Stufen zur Bestimmung der Fähigkeit eines sicherheitsrelevanten Teils eines Steuerungssystems, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[ISO 13849-1]

3.1.1.19

Redundanz

(en: redundancy)

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Beispielen und Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.12, modifiziert]

3.1.1.20

Zuverlässigkeit

(en: reliability)

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

ANMERKUNG 1 Es wird allgemein angenommen, dass sich das automatisierte System am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

ANMERKUNG 2 Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: Reliability Performance) genutzt und durch die Wahrscheinlichkeit bemessen.

ANMERKUNG 3 Innerhalb der MTBF- oder MTTF-Zeitspanne nimmt die Wahrscheinlichkeit ab, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Bedingungen ausführen kann.

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.21

Risiko

(en: risk)

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

ANMERKUNG Für die weitere Diskussion dieses Konzepts siehe IEC 61508-5:2010³⁾, Anhang A.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, Definition 3.2]

3.1.1.22

Sicherheitskommunikationsschicht

(en: safety communication layer (SCL))

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen in IEC 61508 zu gewährleisten

3.1.1.23

sichere Verbindung

(en: safety connection)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

³⁾ Noch zu veröffentlichen.

3.1.1.24**Sicherheitsdaten****(en: safety data)**

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.1.25**Sicherheitsgerät****(en: safety device)**

Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.26**Sicherheitsfunktion****(en: safety function)**

Funktion, die von einem sicherheitsrelevanten E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit einem zusätzlichen Beispiel und einer Referenz. [IEC 61508-4:2010, modifiziert]

3.1.1.27**Reaktionszeit einer Sicherheitsfunktion****(en: safety function response time)**

im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am Feldbus angeschlossenen Sicherheitssensors, bis der zugehörige sichere Zustand des Sicherheitsaktors erreicht wurde, unter Berücksichtigung von gleichzeitig auftretenden Fehlern und Ausfällen im Übertragungskanal der Sicherheitsfunktion

ANMERKUNG Dieses Konzept wird in IEC 61784-3:2010⁴⁾, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.28**Sicherheits-Integritätslevel****(en: Safety Integrity Level, SIL)**

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 in IEC 61508-1:2010⁵⁾ festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen verwendet, die den sicherheitsrelevanten E/E/PE-Systemen zugeordnet werden.

⁴⁾ In Bearbeitung.

⁵⁾ Noch zu veröffentlichen.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung des Ausdrucks „sicherheitsrelevantes System mit SIL n“ (wobei „n“ 1, 2, 3 oder 4 ist) ist, dass das System potentiell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

3.1.1.29

Sicherheitsmaßnahme

(en: **safety measure**)

<diese Norm> Mittel zur Beherrschung möglicher Kommunikationsfehler, welches in Übereinstimmung mit den Anforderungen in IEC 61508 entworfen und ausgeführt wurde

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2010, 5.3 und 5.4, beschrieben.

3.1.1.30

sicherheitsrelevante Anwendung

(en: **safety-related application**)

Programme, welche in Übereinstimmung mit den Anforderungen in IEC 61508 ausgeführt sind, um die SIL-Anforderungen der Anwendung einzuhalten

3.1.1.31

sicherheitsrelevantes System

(en: **safety-related system**)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.32

Slave

(en: **slave**)

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten, seien es Master oder Slaves, senden kann

3.1.1.33

unberechtigte Auslösung

(en: **spurious trip**)

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.1.34

Zeitstempel

(en: **time stamp**)

Zeitinformation in einer *Nachricht*

3.1.2 CPF 2: Zusätzliche Begriffe

3.1.2.1

Basisformat

(en: **base format**)

Format, das für Verbindungs-RPIs von kleiner als 100 ms oder für Anwendungen, bei denen unterbrochene Verbindungen toleriert werden, verwendet wird

3.1.2.2

erweitertes Format

(en: **extended format**)

Format, das für Verbindungs-RPIs von größer als 100 ms oder für Anwendungen, bei denen unterbrochene Verbindungen dringend vermieden werden müssen, verwendet wird

3.1.2.3

Ping

(en: ping)

Anforderung an den Verbraucher, den Empfang einer Nachricht zu bestätigen

3.1.2.4

Ping-Antwort

(en: ping response)

Antwort auf einen Ping

3.1.2.5

Signatur

(en: signature)

Verfahren zur eindeutigen Identifizierung einer Datenmenge

ANMERKUNG Dies könnte durch Verfahren wie Änderung, Quersumme, oder andere Verfahren, die von den versendenden und Zielgeräten vereinbart wurden, umgesetzt werden.

61784-3-3

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe

3.1.1.1

Verfügbarkeit

(en: availability)

Wahrscheinlichkeit eines automatisierten Systems, dass innerhalb einer bestimmten Zeitdauer keine unzureichenden Systembedingungen wie Produktionsausfall auftreten

3.1.1.2

Black Channel

(en: black channel)

Kommunikationskanal ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach IEC 61508

3.1.1.3

Kommunikationskanal

(en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.4

Kommunikationssystem

(en: communication system)

Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von *Nachrichten* (ISO/IEC 7498-Anwendungsschicht) von einer Anwendung zur anderen

3.1.1.5

Verbindung

(en: connection)

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.6**CRC****(en: Cyclic Redundancy Check (CRC))**

<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode> Prozedur zur Berechnung der redundanten Daten

ANMERKUNG 1 Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

ANMERKUNG 2 Siehe auch [32], [33]⁶⁾.

3.1.1.7**Fehler****(error)**

Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

[IEC 61508-4:2010⁷⁾], [IEC 61158]

ANMERKUNG 1 Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder andere Effekte.

ANMERKUNG 2 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.

3.1.1.8**Ausfall****(en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder der Betrieb einer Funktionseinheit anders als gefordert

ANMERKUNG 1 Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.11, modifiziert]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Softwareentwurfs oder eine Nachrichtenstörung).

3.1.1.9**Fehlzustand****(en: fault)**

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, auslösen kann

ANMERKUNG IEC 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder aufgrund fehlender externer Betriebsmittel.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.10, modifiziert]

3.1.1.10**Feldbus****(en: fieldbus)**

Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

⁶⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

⁷⁾ Noch zu veröffentlichen.

3.1.1.11

Feldbussystem

(en: **fieldbus system**)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.12

Telegrammrahmen

(**frame**)

veraltetes Synonym für DLPDU

3.1.1.13

Blockprüfzeichenfolge

(en: **Frame Check Sequence (FCS)**)

redundante Daten, mittels Hash-Funktion aus einem Block von Daten in einer DLPDU (Telegrammrahmen) abgeleitet und mit diesen zusammen zur Aufdeckung von Datenverfälschungen gespeichert oder übertragen

ANMERKUNG 1 Eine FCS kann z. B. mittels einer CRC oder einer anderen Hash-Funktion abgeleitet werden.

ANMERKUNG 2 Siehe auch [32], [33].

3.1.1.14

Hash-Funktion

(en: **hash function**)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einen (üblicherweise) kleineren Wertebereich abbildet

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[IEC/TR 62210, modifiziert]

3.1.1.15

Gefährdung

(en: **hazard**)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.1.16

Master

(en: **master**)

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einrichten und festlegen kann

3.1.1.17

Nachricht

(en: **message**)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.18

Fehlauslösung

(en: **nuisance trip**)

unberechtigte Auslösung ohne schädliche Wirkung

ANMERKUNG Interne außergewöhnliche Fehler können z. B. in Kommunikationssystemen wie Funkübertragung durch zu viele Wiederholungen unter Störeinfluss auftreten.

3.1.1.19**Wiederholungsprüfung****(en: proof test)**

wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem *sicherheitsbezogenen System*, sodass nötigenfalls eine Reparatur das System in einen „Wie-Neu“-Zustand bringen oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand heranbringen kann

ANMERKUNG Eine Wiederholungsprüfung ist zur Bestätigung vorgesehen, dass sich das sicherheitsbezogene System in einem Zustand befindet, der die festgelegte Sicherheitsintegrität garantiert.

[IEC 61508-4 und IEC 62061, modifiziert]

3.1.1.20**Performance Level (PL)****(en: performance level (PL))**

diskrete Stufen zur Bestimmung der Fähigkeit eines sicherheitsbezogenen Teils eines Steuerungssystems, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[ISO 13849-1]

3.1.1.21**Schutzkleinspannung****(en: protective extra-low-voltage (PELV))**

Stromkreis, in dem unter Normalbedingungen oder unter den Bedingungen eines Einzelfehlers die Spannung AC 30 V Effektivwert, 42,4 V Scheitelwert oder DC 60 V nicht überschritten wird, ausgenommen durch Erungsfehler in anderen Stromkreisen

ANMERKUNG Ein PELV-Stromkreis ist wie ein SELV-Stromkreis, der mit Schutzerde verbunden ist.

[IEC 61131-2]

3.1.1.22**Redundanz****(en: redundancy)**

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Beispielen und Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.12, modifiziert]

3.1.1.23**Zuverlässigkeit****(en: reliability)**

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

ANMERKUNG 1 Es wird allgemein angenommen, dass sich das automatisierte System am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

ANMERKUNG 2 Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: Reliability Performance) genutzt und durch die Wahrscheinlichkeit bemessen.

ANMERKUNG 3 Innerhalb der MTBF- oder MTTF-Zeitspanne nimmt die Wahrscheinlichkeit ab, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Bedingungen ausführen kann.

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.24

Risiko

(en: risk)

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

ANMERKUNG Für die weitere Diskussion dieses Konzepts siehe IEC 61508-5:2010⁸⁾, Anhang A.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, Definition 3.2]

3.1.1.25

Sicherheitskommunikationsschicht

(en: safety communication layer (SCL))

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen in IEC 61508 zu gewährleisten

3.1.1.26

sichere Verbindung

(en: safety connection)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.27

Sicherheitsdaten

(en: safety data)

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.1.28

Sicherheitsgerät

(en: safety device)

Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.29

Sicherheitskleinspannung

(en: safety extra-low-voltage (SELV))

Stromkreis, in dem die Spannung AC 30 V Effektivwert, 42,4 V Scheitelwert oder DC 60 V unter Normalbedingungen oder den Bedingungen eines Einzelfehlers nicht überschritten wird, einschließlich Erdungsfehler in anderen Stromkreisen

ANMERKUNG Ein SELV-Stromkreis ist nicht mit Schutz Erde verbunden.

[IEC 61131-2]

3.1.1.30

Sicherheitsfunktion

(en: safety function)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit einem zusätzlichen Beispiel und einer Referenz.

[IEC 61508-4:2010, modifiziert]

⁸⁾ Noch zu veröffentlichen.

3.1.1.31 Reaktionszeit einer Sicherheitsfunktion**(en: safety function response time (SFRT))**

im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am Feldbus angeschlossenen Sicherheitssensors, bis der zugehörige sichere Zustand des Sicherheitsaktors erreicht wurde, unter Berücksichtigung von gleichzeitig auftretenden Fehlern und Ausfällen im Übertragungskanal der Sicherheitsfunktion

ANMERKUNG Dieses Konzept wird in IEC 61784-3:2010⁹⁾, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.32**Sicherheits-Integritätslevel****(en: safety integrity level (SIL))**

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 in IEC 61508-1:2010¹⁰⁾ festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen verwendet, die den sicherheitsbezogenen E/E/PE-Systemen zugeordnet werden.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung des Ausdrucks „sicherheitsbezogenes System mit SIL n“ (wobei „n“ 1, 2, 3 oder 4 ist) ist, dass das System potentiell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

3.1.1.33**Sicherheitsmaßnahme****(en: safety measure)**

<diese Norm> Mittel zur Beherrschung möglicher Kommunikationsfehler, welches in Übereinstimmung mit den Anforderungen in IEC 61508 entworfen und ausgeführt wurde

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2010, 5.3 und 5.4, beschrieben.

3.1.1.34**sicherheitsbezogene Anwendung****(safety-related application)**

Programme, welche in Übereinstimmung mit den Anforderungen in IEC 61508 ausgeführt sind, um die SIL-Anforderungen der Anwendung einzuhalten

3.1.1.35**sicherheitsbezogenes System****(en: safety-related system)**

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

⁹⁾ In Bearbeitung.

¹⁰⁾ Noch zu veröffentlichen.

3.1.1.36

Slave

(en: slave)

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten, seien es Master oder Slaves, senden kann

3.1.1.37

unberechtigte Auslösung

(en: spurious trip)

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.2 CPF 3: Zusätzliche Begriffe

3.1.2.1

Bit (Binärziffer)

(en: bit (Binary Digit))

verschlüsselte Binärinformation ohne eine technische Einheit

3.1.2.2

Codename

(en: codename)

eindeutige Identifikation zwischen sicheren Kommunikations-Peers

ANMERKUNG Beispiel für die *Verbindungsauthentizität*, wie in IEC 61784-3 beschrieben.

3.1.2.3

Konfiguration

(en: configuration)

Festlegung der standardmäßigen Kommunikationsverbindungen und Kommunikationsparameter für Buseinheiten einer bestimmten Anwendung

ANMERKUNG Die Konfiguration für eine sichere Kommunikation umfasst die Festlegung der sicheren Verbindungen und F-Parameter für sicherheitsbezogene Buseinheiten einer bestimmten sicherheitsbezogenen Anwendung.

3.1.2.4

fortlaufende Nummer

(en: consecutive number)

Mittel, um die Vollständigkeit und richtige Reihenfolge der übertragenen Sicherheits-PDUs zu gewährleisten

ANMERKUNG 1 Beispiel für eine *Laufnummer* wie in IEC 61784-3 beschrieben.

ANMERKUNG 2 Die fortlaufende Nummer kann mit jeder Sicherheits-PDU (V1-Modus) oder nur über eine übertragene CRC-Signatur gesichert übertragen werden.

3.1.2.5

CPD-Tool

(en: CPD-Tool)

zugehöriges Programm in Service-Rechnern, das mit dem Feldbus zum Zweck der Konfiguration, Parametrisierung und Diagnose bestimmter Feldgeräte verbunden ist

3.1.2.6

Zyklus

(en: cycle)

Intervall, in dem eine Liste von Anweisungen oder eine Aktivität wiederholt und ununterbrochen ausgeführt wird

3.1.2.7

Gerätezugangspunkt

(en: device access point (DAP))

Element, das verwendet wird, um ein modulares E/A-Gerät als Einheit zu adressieren

ANMERKUNG Üblicherweise als Kopfstation bezeichnet.

3.1.2.8

Geräterückmeldungszeit

(en: **device acknowledgement time (DAT)**)

benötigte Zeit in einem F-Gerät für das Starten des Empfangs einer Sicherheits-PDU mit einer laufenden Nummer im DAP bis zu dem Zeitpunkt, an dem die entsprechende Sicherheits-PDU als Antwort generiert und an den DAP zurückgegeben wurde

3.1.2.9

Treiber

(en: **driver**)

Softwaremodul, das für die Abstraktion der Hardware in Bezug auf die restliche Anwendungssoftware verwendet wird

3.1.2.10

ausfallsicher

(en: **fail-safe (F)**)

Fähigkeit eines Systems, Gefährdungen bei entsprechenden technischen oder organisatorischen Maßnahmen entweder deterministisch oder indem das Risiko auf ein toleriertes Maß verringert wird, zu verhindern

3.1.2.11

ausfallsichere Werte

(en: **fail-safe values (FV)**)

Werte, die anstelle von Prozesswerten ausgegeben werden, wenn die Sicherheitsfunktion auf einen ausfallsicheren Zustand festgelegt wurde

ANMERKUNG In diesem Normteil müssen die ausfallsicheren Werte (FV) immer auf „0“ festgelegt werden.

3.1.2.12

ausfallsicherer Zustand

(en: **fail-safe state**)

Betriebsmodus einer Sicherheitsfunktion oder eines Endelements (Aktor), in dem Gefährdungen bei entsprechenden technischen Maßnahmen entweder deterministisch oder indem das Risiko auf ein toleriertes Maß verringert wird, verhindert werden

ANMERKUNG In Abhängigkeit von der bestimmten Sicherheitsfunktion stellt das Abschalten möglicherweise nicht die einzige Möglichkeit für einen ausfallsicheren Zustand dar.

3.1.2.13

F-Gerät

(en: **F-Device**)

passiver CP 3/RTE-Kommunikations-Peer, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

3.1.2.14

F-Treiber

(en: **F-Driver**)

Software zur Verwaltung der Sicherheits-PDUs in F-Hosts und F-Geräten entsprechend der FSCP 3/1-Spezifikationen

3.1.2.15

F-Host

(en: **F-Host**)

Datenverarbeitungseinheit, die das FSCP 3/1-Protokoll ausführen kann und die den Black Channel bedient

ANMERKUNG Hierbei handelt es sich üblicherweise um einen PLC oder einen IPC mit einem entsprechenden Betriebssystem.

3.1.2.16

F-Modul

(en: **F-Module**)

passiver Kommunikations-Peer in einem modularen F-Gerät oder F-Slave, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

ANMERKUNG Hierbei handelt es sich üblicherweise um ein sicherheitsbezogenes Eingabe- oder Ausgabemodul.

3.1.2.17

F-Slave

(en: **F-Slave**)

passiver CP 3/1- oder CP 3/2-Kommunikations-Peer, der das FSCP 3/1-Protokoll ausführen kann und der üblicherweise von dem F-Host für den Datenaustausch aktiviert wird

3.1.2.18

Fehlreaktion

(en: **fault reaction**)

Angabe einer Kommunikationsfehlfunktion durch Setzen der Fehlerbits im Status-Byte und einer entsprechenden automatischen sicheren Reaktion innerhalb der Komponenten

ANMERKUNG

Innerhalb einer F-Ausgabe: Abschalten der Ausgabegeräte und/oder automatische sichere Reaktion der Aktoreinheit.

Innerhalb einer F-CPU: Entsprechende Reaktion des Benutzerprogramms möglich. F-E/A-Daten sind auf ausfallsichere Werte festzulegen.

Innerhalb einer F-Eingabe: Bei Kommunikationsfehlern, die durch die F-Eingabe ermittelt wurden: Fehlerbits werden im Status-Byte gesetzt.

Bei Kommunikationsfehlern, die durch den F-Host ermittelt wurden: F-Eingabedaten sind auf ausfallsichere Werte festzulegen.

3.1.2.19

Funktionsblock (FB)

(en: **function block (FB)**)

eigenständiger Programmteil mit besonderer Funktionalität

3.1.2.20

Hostrückmeldungszeit

(en: **host acknowledgement time (HAT)**)

Zeit, die in einem F-Host für das Starten des Empfangs einer Sicherheits-PDU mit einer bestimmten laufenden Nummer bis zu dem Zeitpunkt, an dem die entsprechende Sicherheits-PDU mit einer inkrementierten laufenden Nummer generiert und an den Master bzw. E/A-Controller zurückgegeben wurde, benötigt wird

3.1.2.21

E/A-Controller

(en: **IO-Controller**)

aktive Kommunikationseinheit, die CP 3/RTE-Kommunikationsaktivitäten anderer Einheiten, seien es E/A-Controller oder E/A-Geräte, einrichten und festlegen kann

ANMERKUNG Im CP 3/1 entspricht diese Task einem Master Klasse 1.

3.1.2.22

E/A-Gerät

(en: **IO-Device**)

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an eine andere CP 3/RTE-Kommunikationseinheit, sei es ein E/A-Controller oder ein anderes E/A-Gerät, senden kann

ANMERKUNG Im CP 3/1 entspricht diese Task einem Slave.

3.1.2.23**E/A-Modul****(en: IO-Module)**

adressierbare untergeordnete Eingabe/Ausgabe-Einheit in einem modularen E/A-Gerät

3.1.2.24**E/A-Supervisor****(en: IO-Supervisor)**

Engineering-Station, die Daten aus einem E/A-Gerät lesen und auf ein E/A-Gerät schreiben kann

ANMERKUNG Ein E/A-Supervisor wird zu Installations- und Diagnosezwecken verwendet. Im Gegensatz zu einem E/A-Controller übernimmt der E/A-Supervisor keine aktive Rolle während des Hochfahrens eines E/A-Systems. Ein E/A-Supervisor ist nicht Teil des E/A-Systems.

3.1.2.25**E/A-System****(en: IO-System)**

E/A-Controller und die zugehörigen E/A-Geräte

3.1.2.26**iParameter****(en: iParameter)**

individuelle oder technologiespezifische Parameter für F-Geräte

ANMERKUNG Typische iParameter sind die Koordinaten der Schutzzone eines Laserscanners.

3.1.2.27**iPar-Server****(en: iPar-Server)**

genormter Mechanismus, mit dem individuelle oder technologiespezifische Parameter für F-Geräte im Standardteil eines F-Hosts oder seines gesteuerten Teilsystems gespeichert und abgerufen werden können

3.1.2.28**Master (Klasse 1)****(en: master (class 1))**

aktiver CP 3/1-Kommunikations-Peer, der Slaves für den Datenaustausch aktiviert

3.1.2.29**Prozesswerte****(en: process values (PV))**

Eingabe- und Ausgabedaten (in einer Sicherheits-PDU), die für die Steuerung eines automatisierten Prozesses erforderlich sind

3.1.2.30**Wertstatus****(en: qualifier)**zusätzliche kennzeichnende Bits in *Prozesswerten*, die den Status jeder individuellen Eingabe angeben**3.1.2.31****gemeinsame E/A****(en: shared I/O)**

Eingaben und Ausgaben in Feldgeräten, auf die über mehrere Controller zugegriffen werden kann

ANMERKUNG Obwohl gemeinsame E/A im CP 3/RTE zulässig ist, ist sie im FSCP 3/1 nicht erlaubt.

3.1.2.32**Toggle-Bit****(en: toggle bit)**

ein Bit des Control- und Status-Bytes, das die (virtuellen) laufenden Zähler sowohl im F-Host als auch im F-Gerät synchronisiert

3.1.2.33

USB

(en: universal serial bus (USB))

externer Busstandard, der Datenübertragungsraten von bis zu 480 Mbit/s unterstützt

ANMERKUNG USB ersetzt serielle und parallele Computerports und wird für schnelle Direktverbindungen zwischen Service-Rechnern und Feldgeräten verwendet.

3.1.2.34

V1-Modus

(en: V1-mode)

FSCP 3/1-Dienste und Protokoll nach [48]

3.1.2.35

V2-Modus

(en: V2-mode)

FSCP 3/1-Dienste und Protokoll nach diesem Normteil

3.1.2.36

VLAN-Tag

(en: VLAN tag)

Erweiterung innerhalb Ethernet-Nachrichten, die es bestimmten Benutzergruppen in großen Netzwerken ermöglicht, ihre eigenen virtuellen Netzwerke über Prioritäten und VLAN-IDs unter Verwendung geeigneter Switches auszuführen, ohne sich gegenseitig zu beeinflussen

61784-3-8

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe

3.1.1.1

Verfügbarkeit

(en: availability)

Wahrscheinlichkeit eines automatisierten Systems, dass innerhalb einer bestimmten Zeitdauer keine unzureichenden Systembedingungen wie Produktionsausfall auftreten

3.1.1.2

Black Channel

(en: black channel)

Kommunikationskanal ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach IEC 61508

3.1.1.3

Kommunikationskanal

(en: communication channel)

logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.4

Kommunikationssystem

(en: communication system)

Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von *Nachrichten* (ISO/IEC 7498-Anwendungsschicht) von einer Anwendung zur anderen

3.1.1.5**Verbindung****(en: connection)**

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.6**CRC****(en: Cyclic Redundancy Check (CRC))**

<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode> Prozedur zur Berechnung der redundanten Daten

ANMERKUNG 1 Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

ANMERKUNG 2 Siehe auch [32], [34]¹¹⁾.

3.1.1.7**Fehler****(en: error)**

Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

[IEC 61508-4:2010¹²⁾], [IEC 61158]

ANMERKUNG 1 Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder andere Effekte.

ANMERKUNG 2 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.

3.1.1.8**Ausfall****(en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder der Betrieb einer Funktionseinheit anders als gefordert

ANMERKUNG 1 Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.11, modifiziert]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Softwareentwurfs oder eine Nachrichtenstörung).

3.1.1.9**Fehlzustand****(en: fault)**

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, auslösen kann

ANMERKUNG IEC 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder aufgrund fehlender externer Betriebsmittel.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.10, modifiziert]

¹¹⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

¹²⁾ Noch zu veröffentlichen.

3.1.1.10

Feldbus

(en: **fieldbus**)

Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

3.1.1.11

Telegrammrahmen

(en: **frame**)

veraltetes Synonym für DLPDU

3.1.1.12

Hash-Funktion

(en: **hash function**)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einen (üblicherweise) kleineren Wertebereich abbildet

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[IEC/TR 62210, modifiziert]

3.1.1.13

Gefährdung

(en: **hazard**)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.1.14

Master

(en: **master**)

aktive Kommunikationseinheit, die Kommunikationsaktivitäten anderer Stationen, seien es Master oder Slaves, einrichten und festlegen kann

3.1.1.15

Nachricht

(en: **message**)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.16

Performance Level (PL)

(en: **performance level (PL)**)

diskrete Stufen zur Bestimmung der Fähigkeit eines sicherheitsbezogenen Teils eines Steuerungssystems, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[ISO 13849-1]

3.1.1.17

Schutzkleinspannung

(en: **protective extra-low-voltage (PELV)**)

Stromkreis, in dem unter Normalbedingungen oder unter den Bedingungen eines Einzelfehlers die Spannung AC 30 V Effektivwert, 42,4 V Scheitelwert oder DC 60 V nicht überschritten wird, ausgenommen durch Erungsfehler in anderen Stromkreisen

ANMERKUNG Ein PELV-Stromkreis ist wie ein SELV-Stromkreis, der mit Schutzterde verbunden ist.

[IEC 61131-2]

3.1.1.18**Redundanz****(en: redundancy)**

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Beispielen und Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.12, modifiziert]

3.1.1.19**Zuverlässigkeit****(en: reliability)**

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

ANMERKUNG 1 Es wird allgemein angenommen, dass sich das automatisierte System am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

ANMERKUNG 2 Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: Reliability Performance) genutzt und durch die Wahrscheinlichkeit bemessen.

ANMERKUNG 3 Innerhalb der MTBF- oder MTTF-Zeitspanne nimmt die Wahrscheinlichkeit ab, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Bedingungen ausführen kann.

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.20**Risiko****(en: risk)**

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

ANMERKUNG Für die weitere Diskussion dieses Konzepts siehe IEC 61508-5:2010¹³⁾, Anhang A.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, Definition 3.2]

3.1.1.21**Sicherheitskommunikationsschicht****(en: safety communication layer (SCL))**

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen in IEC 61508 zu gewährleisten

3.1.1.22**sichere Verbindung****(en: safety connection)**

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.23**Sicherheitsdaten****(en: safety data)**

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

¹³⁾ Noch zu veröffentlichen.

3.1.1.24**Sicherheitsgerät****(en: safety device)**

Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.25**Sicherheitskleinspannung****(en: safety extra-low-voltage (SELV))**

Stromkreis, in dem die Spannung AC 30 V Effektivwert, 42,4 V Scheitelwert oder DC 60 V unter Normalbedingungen oder den Bedingungen eines Einzelfehlers nicht überschritten wird, einschließlich Erdungsfehler in anderen Stromkreisen

ANMERKUNG Ein SELV-Stromkreis ist nicht mit Schutz Erde verbunden.

[IEC 61131-2]

3.1.1.26**Sicherheitsfunktion****(en: safety function)**

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit einem zusätzlichen Beispiel und einer Referenz.

[IEC 61508-4:2010, modifiziert]

3.1.1.27**Reaktionszeit einer Sicherheitsfunktion****(en: safety function response time)**

im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am Feldbus angeschlossenen Sicherheitssensors, bis der zugehörige sichere Zustand des Sicherheitsaktors erreicht wurde, unter Berücksichtigung von gleichzeitig auftretenden Fehlern und Ausfällen im Übertragungskanal der Sicherheitsfunktion

ANMERKUNG Dieses Konzept wird in IEC 61784-3:2010¹⁴⁾, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.28**Sicherheits-Integritätslevel****(en: safety integrity level (SIL))**

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 in IEC 61508-1:2010¹⁵⁾ festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen verwendet, die den sicherheitsbezogenen E/E/PE-Systemen zugeordnet werden.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung des Ausdrucks „sicherheitsbezogenes System mit SIL n“ (wobei „n“ 1, 2, 3 oder 4 ist) ist, dass das System potentiell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

¹⁴⁾ In Bearbeitung.

¹⁵⁾ Noch zu veröffentlichen.

3.1.1.29**Sicherheitsmaßnahme****(en: safety measure)**

<diese Norm> Mittel zur Beherrschung möglicher Kommunikationsfehler, welches in Übereinstimmung mit den Anforderungen in IEC 61508 entworfen und ausgeführt wurde

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2010, 5.3 und 5.4, beschrieben.

3.1.1.30**sicherheitsbezogene Anwendung****(en: safety-related application)**

Programme, welche in Übereinstimmung mit den Anforderungen in IEC 61508 ausgeführt sind, um die SIL-Anforderungen der Anwendung einzuhalten

3.1.1.31**sicherheitsbezogenes System****(en: safety-related system)**

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.32**Slave****(en: slave)**

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten, seien es Master oder Slaves, senden kann

3.1.1.33**Zeitstempel****(en: time stamp)**

Zeitinformation in einer *Nachricht*

3.1.2 CPF 8: Zusätzliche Begriffe**3.1.2.1****Zyklus****(en: cycle)**

Intervall, in dem eine Aktivität wiederholt und fortlaufend ausgeführt wird

3.1.2.2**Sicherheitsanwendungsbeziehung****(en: safety application relationship (SAR))**

Anwendungsbeziehung zwischen zwei oder mehreren Beziehungsendpunkten sicherheitsbezogener Anwendungen

3.1.2.3**SASE****(en: safety application service element (SASE))**

Serviceelement einer sicherheitsbezogenen Anwendung

3.1.2.4**Zeitschalter für Sicherheitsdatenüberwachung****(en: safety data monitor timer)**

Zeitschalter, der von der Zeiterwartungsfunktion für die Übertragung von Sicherheitsdaten verwendet wird

3.1.2.5**Zeitschalter für Sicherheitsüberwachung****(en: safety monitor timer)**

Zeitschalter, der von der Zeiterwartungsfunktion für die Verwaltung der sicheren Verbindung verwendet wird

3.1.2.6**Sicherheits-PDU****(en: safety PDU)**

Synonym für sicherheitsbezogene DLPDU

3.1.2.7**Slot****(en: slot)**

eine Menge (Granularität) der positionsabhängigen Zuordnung der zyklischen Datenfelder

3.1.2.8**Station****(en: station)**

Gerät und die entsprechenden SAREPs, die für die Übertragung und den Empfang von Sicherheitsdaten vorgesehen sind

ANMERKUNG Die Nummer der Station wird in der positionsabhängigen Zuordnung der zyklischen Datenfelder verwendet (eine Station belegt einen oder mehrere Slots).

3.1.2.9**Übertragungsinformation des Sicherheitsprotokolls****(en: safety protocol transmission information)**

Information, die sicherheitsbezogene Nachrichten voneinander unterscheidet

61784-3-13**3.1 Begriffe**

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe**3.1.1.1****Verfügbarkeit****(en: availability)**

Wahrscheinlichkeit eines automatisierten Systems, dass innerhalb einer bestimmten Zeitdauer keine unzureichenden Systembedingungen wie Produktionsausfall auftreten

3.1.1.2**Black Channel****(en: black channel)***Kommunikationskanal* ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach IEC 61508**3.1.1.3****Kommunikationskanal****(en: communication channel)**logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem*

3.1.1.4**Kommunikationssystem****(en: communication system)**

Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von *Nachrichten* (ISO/IEC 7498-Anwendungsschicht) von einer Anwendung zur anderen

3.1.1.5**Verbindung****(en: connection)**

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.6**CRC****(en: Cyclic Redundancy Check (CRC))**

<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode> Prozedur zur Berechnung der redundanten Daten

ANMERKUNG 1 Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

ANMERKUNG 2 Siehe auch [37], [38]¹⁶⁾.

3.1.1.7**Fehler****(en: error)**

Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

[IEC 61508-4:2010¹⁷⁾], [IEC 61158]

ANMERKUNG 1 Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder andere Effekte.

ANMERKUNG 2 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.

3.1.1.8**Ausfall****(en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder der Betrieb einer Funktionseinheit anders als gefordert

ANMERKUNG 1 Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.11, modifiziert]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Software-entwurfs oder eine Nachrichtenstörung).

3.1.1.9**Fehlzustand****(en: fault)**

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, auslösen kann

¹⁶⁾ Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

¹⁷⁾ Noch zu veröffentlichen.

ANMERKUNG IEC 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder aufgrund fehlender externer Betriebsmittel.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.10, modifiziert]

3.1.1.10

Feldbus

(en: **fieldbus**)

Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

3.1.1.11

Feldbussystem

(en: **fieldbus system**)

System mit einem *Feldbus* und angeschlossenen Geräten

3.1.1.12

Telegrammrahmen

(en: **frame**)

veraltetes Synonym für DLPDU

3.1.1.13

Hash-Funktion

(en: **hash function**)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einen (üblicherweise) kleineren Wertebereich abbildet

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[IEC/TR 62210, modifiziert]

3.1.1.14

Gefährdung

(en: **hazard**)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.1.15

Nachricht

(en: **message**)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.16

Performance Level (PL)

(en: **performance level (PL)**)

diskrete Stufen zur Bestimmung der Fähigkeit eines sicherheitsbezogenen Teils eines Steuerungssystems, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[ISO 13849-1]

3.1.1.17

Redundanz

(en: **redundancy**)

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Beispielen und Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.12, modifiziert]

3.1.1.18

Zuverlässigkeit

(en: reliability)

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

ANMERKUNG 1 Es wird allgemein angenommen, dass sich das automatisierte System am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

ANMERKUNG 2 Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: Reliability Performance) genutzt und durch die Wahrscheinlichkeit bemessen.

ANMERKUNG 3 Innerhalb der MTBF- oder MTTF-Zeitspanne nimmt die Wahrscheinlichkeit ab, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Bedingungen ausführen kann.

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.19

Risiko

(en: risk)

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

ANMERKUNG Für die weitere Diskussion dieses Konzepts siehe IEC 61508-5:2010¹⁸⁾, Anhang A.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, Definition 3.2]

3.1.1.20

Sicherheitskommunikationsschicht

(en: safety communication layer (SCL))

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen in IEC 61508 zu gewährleisten

3.1.1.21

Sicherheitsdaten

(en: safety data)

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.1.22

Sicherheitsgerät

(en: safety device)

Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.23

Sicherheitsfunktion

(en: safety function)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalles einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit einem zusätzlichen Beispiel und einer Referenz.

¹⁸⁾ Noch zu veröffentlichen.

[IEC 61508-4:2010, modifiziert]

3.1.1.24

Reaktionszeit einer Sicherheitsfunktion

(en: **safety function response time**)

im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am Feldbus angeschlossenen Sicherheits-sensors, bis der zugehörige sichere Zustand des Sicherheitsaktors erreicht wurde, unter Berücksichtigung von gleichzeitig auftretenden Fehlern und Ausfällen im Übertragungskanal der Sicherheitsfunktion

ANMERKUNG Dieses Konzept wird in IEC 61784-3:2010¹⁹⁾, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.25

Sicherheits-Integritätslevel

(en: **safety integrity level (SIL)**)

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 in IEC 61508-1:2010²⁰⁾ festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen verwendet, die den sicherheitsbezogenen E/E/PE-Systemen zugeordnet werden.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung des Ausdrucks „sicherheitsbezogenes System mit SIL n“ (wobei „n“ 1, 2, 3 oder 4 ist) ist, dass das System potentiell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

3.1.1.26

Sicherheitsmaßnahme

(en: **safety measure**)

<diese Norm> Mittel zur Beherrschung möglicher Kommunikationsfehler, welches in Übereinstimmung mit den Anforderungen in IEC 61508 entworfen und ausgeführt wurde

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2010, 5.3 und 5.4, beschrieben.

3.1.1.27

sicherheitsbezogene Anwendung

(en: **safety-related application**)

Programme, welche in Übereinstimmung mit den Anforderungen in IEC 61508 ausgeführt sind, um die SIL-Anforderungen der Anwendung einzuhalten

3.1.1.28

sicherheitsbezogenes System

(en: **safety-related system**)

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

¹⁹⁾ In Bearbeitung.

²⁰⁾ Noch zu veröffentlichen.

3.1.1.29**Slave****(en: slave)**

passive Kommunikationseinheit, die Nachrichten empfangen und sie als Antwort an andere Kommunikationseinheiten, seien es Master oder Slaves, senden kann

3.1.1.30**Zeitstempel****(en: time stamp)**

Zeitinformation in einer *Nachricht*

3.1.2 CPF 13: Zusätzliche Begriffe**3.1.2.1****Bitfehlerquote****(en: bit error rate)**

Wahrscheinlichkeit einer Fehldeutung eines Bits aufgrund von Elektroräuschen

3.1.2.2**DVI****(en: Device Vendor Information (DVI))**

Informationen für die Identifizierung eines Sicherheitsknotens

3.1.2.3**Sicherheitsadresse****(en: Safety Address (SADR))**

Adresse eines Sicherheitsknotens in einer Sicherheitsdomäne

3.1.2.4**SCM****(en: Safety Configuration Manager (SCM))**

Dienst, der für die Verwaltung von sicherheitsbezogenen Diensten verantwortlich ist

ANMERKUNG Beispiele von verwalteten sicherheitsbezogenen Diensten sind Konfiguration, Parametrisierung.

3.1.2.5**Sicherheitsknoten****(en: Safety Node (SN))**

Knoten mit Sicherheitsfunktion

3.1.2.6**Sicherheitsdomäne****(en: Safety Domain (SD))**

Adressbereich für bis zu 1023 Sicherheitsknoten

3.1.2.7**Sicherheitsdomänen-Gateway****(en: Safety Domain Gateway (SDG))**

Gateway für den Austausch von Daten zwischen verschiedenen Sicherheitsdomänen

3.1.2.8**Nummer der Sicherheitsdomäne****(en: Safety Domain Number (SDN))**

Identifikation einer Sicherheitsdomäne

3.1.2.9**SNMT****(en: Safety Network Management (SNMT))**

Dienste für die Verwaltung der Sicherheitsschicht

3.1.2.10**SOD****(en: Safety Object Dictionary (SOD))**

Repositorium für alle Datenobjekte, die mittels Diensten des funktionalen Sicherheitsfeldbusses zugänglich sind

3.1.2.11**Sicherheitsprozessdatenobjekt (SPDO)****(en: Safety Process Data Object (SPDO))**

Objekt für den Austausch von Prozessdaten zwischen verschiedenen Sicherheitsknoten

3.1.2.12**Sicherheitsservicedatenobjekt (SSDO)****(en: Safety Service Data Object (SSDO))**

Objekt für den Austausch von Servicedaten zwischen Sicherheitsknoten

3.1.2.13**Initialisierung****(en: initialization)**

Ausgangskommunikationszustand von Sicherheitsknoten

3.1.2.14**Betrieb****(en: operational)**

Kommunikationszustand von Sicherheitsknoten, in dem alle funktionalen Sicherheitsfunktionen ordnungsgemäß ausgeführt werden

3.1.2.15**Vor-Betrieb****(en: pre-operational)**

Kommunikationszustand von Sicherheitsknoten, in dem sich alle Anwendungsausgaben in einem sicheren Zustand befinden

3.1.2.16**UDID****(en: Unique Device Identification (UDID))**

weltweite eindeutige Identifikation eines Geräts

61784-3-17**3.1 Begriffe**

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1 Allgemeine Begriffe**3.1.1.1****Verfügbarkeit****(en: availability)**

Wahrscheinlichkeit eines automatisierten Systems, dass innerhalb einer bestimmten Zeitdauer keine unzureichenden Systembedingungen wie Produktionsausfall auftreten

3.1.1.2**Black Channel****(en: black channel)**

Kommunikationskanal ohne verfügbaren Nachweis des Entwurfs oder der Validierung nach IEC 61508

3.1.1.3**Kommunikationskanal****(en: communication channel)**logische Verbindung zwischen zwei Endpunkten in einem *Kommunikationssystem***3.1.1.4****Kommunikationssystem****(en: communication system)**Anordnung von Hardware, Software und Ausbreitungsmedien zur Übertragung von *Nachrichten* (ISO/IEC 7498-Anwendungsschicht) von einer Anwendung zur anderen**3.1.1.5****Verbindung****(en: connection)**

logische Verbindung zwischen zwei Anwendungsobjekten in demselben oder in unterschiedlichen Geräten

3.1.1.6**CRC****(en: Cyclic Redundancy Check (CRC))**

<Wert> redundante Daten, abgeleitet von einem Block von Daten und mit diesen zusammen gespeichert oder übertragen zur Aufdeckung von Datenverfälschungen

<Methode> Prozedur zur Berechnung der redundanten Daten

ANMERKUNG 1 Begriffe wie „CRC-Code“ und „CRC-Signatur“ und Bezeichnungen wie CRC1, CRC2 können ebenfalls in dieser Norm verwendet sein, um redundante Daten zu kennzeichnen.

ANMERKUNG 2 Siehe auch [34], [35]^[1)].**3.1.1.7****Fehler****(en: error)**

Unterschied zwischen einem berechneten, beobachteten bzw. gemessenen Wert oder Zustand und dem wahren, spezifizierten bzw. theoretisch korrekten Wert oder Zustand

[IEC 61508-4:2010^[2)]], [IEC 61158]

ANMERKUNG 1 Fehler können auf einem Entwurfsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder andere Effekte.

ANMERKUNG 2 Fehler führen nicht notwendigerweise zu einem *Ausfall* oder einem *Fehlzustand*.**3.1.1.8****Ausfall****(en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, oder der Betrieb einer Funktionseinheit anders als gefordert

ANMERKUNG 1 Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.11, modifiziert]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Softwareentwurfs oder eine Nachrichtenstörung).

[1)] Zahlen in rechteckigen Klammern beziehen sich auf die Literaturhinweise.

[2)] Noch zu veröffentlichen.

3.1.1.9

Fehlzustand

(en: fault)

nicht normale Bedingung, die eine Verringerung oder den Verlust der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen, auslösen kann

ANMERKUNG IEC 191-05-01 definiert „fault“ als einen Zustand, der durch das Unvermögen gekennzeichnet ist, eine geforderte Funktion auszuführen, jedoch nicht ein Unvermögen während vorbeugender Instandhaltung, anderer geplanter Aktionen oder aufgrund fehlender externer Betriebsmittel.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.10, modifiziert]

3.1.1.10

Feldbus

(en: fieldbus)

Kommunikationssystem basierend auf serieller Datenübertragung und eingesetzt in der industriellen Automatisierung oder in Prozessleitsystemen

3.1.1.11

Feldbussystem

(en: fieldbus system)

System mit einem Feldbus und angeschlossenen Geräten

3.1.1.12

Telegrammrahmen

(en: frame)

veraltetes Synonym für DLPDU

3.1.1.13

Blockprüfzeichenfolge

(en: Frame Check Sequence (FCS))

redundante Daten, mittels Hash-Funktion aus einem Block von Daten in einer DLPDU (Telegrammrahmen) abgeleitet und mit diesen zusammen zur Aufdeckung von Datenverfälschungen gespeichert oder übertragen

ANMERKUNG 1 Eine FCS kann z. B. mittels einer CRC oder einer anderen Hash-Funktion abgeleitet werden.

ANMERKUNG 2 Siehe auch [34], [35].

3.1.1.14

Hash-Funktion

(en: hash function)

(mathematische) Funktion, die Werte aus einem (möglicherweise sehr) großen Wertebereich in einen (üblicherweise) kleineren Wertebereich abbildet

ANMERKUNG 1 Hash-Funktionen können zur Aufdeckung von Datenverfälschung eingesetzt werden.

ANMERKUNG 2 Gebräuchliche Hash-Funktionen schließen Parity-Bit, Quersummen oder CRC mit ein.

[IEC/TR 62210, modifiziert]

3.1.1.15

Gefährdung

(en: hazard)

Zustand oder Umstände in einem System, der/die zusammen mit weiteren Bedingungen zwangsläufig zu einem Schaden an Personen, Eigentum oder der Umwelt führt/führen

3.1.1.16

Nachricht

(en: message)

geordnete Folge von Oktetts, bestimmt für die Übermittlung von Informationen

[ISO/IEC 2382-16.02.01, modifiziert]

3.1.1.17**Fehlauslösung****(en: nuisance trip)**

unberechtigte Auslösung ohne schädliche Wirkung

ANMERKUNG Interne außergewöhnliche Fehler können z. B. in Kommunikationssystemen wie Funkübertragung durch zu viele Wiederholungen unter Störeinfluss auftreten.

3.1.1.18**Wiederholungsprüfung****(en: proof test)**

wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem sicherheitsbezogenen System, sodass nötigenfalls eine Reparatur das System in einen „Wie-Neu“-Zustand bringen oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand heranbringen kann

ANMERKUNG Eine Wiederholungsprüfung ist zur Bestätigung vorgesehen, dass sich das sicherheitsbezogene System in einem Zustand befindet, der die festgelegte Sicherheitsintegrität garantiert.

[IEC 61508-4 und IEC 62061, modifiziert]

3.1.1.19**Performance Level (PL)****(en: performance level (PL))**

diskrete Stufen zur Bestimmung der Fähigkeit eines sicherheitsbezogenen Teils eines Steuerungssystems, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[ISO 13849-1]

3.1.1.20**Redundanz****(en: redundancy)**

Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit zusätzlichen Beispielen und Anmerkungen.

[IEC 61508-4:2010, modifiziert], [ISO/IEC 2382-14.01.12, modifiziert]

3.1.1.21**Zuverlässigkeit****(en: reliability)**

Wahrscheinlichkeit, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Voraussetzungen in einem bestimmten Zeitintervall (t_1 , t_2) ausführen kann

ANMERKUNG 1 Es wird allgemein angenommen, dass sich das automatisierte System am Anfang des Zeitintervalls in einem Zustand befindet, um die geforderte Funktion ausführen zu können.

ANMERKUNG 2 Der Begriff „Zuverlässigkeit“ wird ebenfalls zur Kennzeichnung der Überlebenswahrscheinlichkeit (en: Reliability Performance) genutzt und durch die Wahrscheinlichkeit bemessen.

ANMERKUNG 3 Innerhalb der MTBF- oder MTTF-Zeitspanne nimmt die Wahrscheinlichkeit ab, dass ein automatisiertes System eine geforderte Funktion unter bestimmten Bedingungen ausführen kann.

ANMERKUNG 4 Zuverlässigkeit unterscheidet sich von Verfügbarkeit.

[IEC 62059-11, modifiziert]

3.1.1.22**restliche Fehlerwahrscheinlichkeit****(en: residual error probability)**

Wahrscheinlichkeit eines unentdeckten Fehler der SCL Sicherheitsmaßnahmen

3.1.1.23

restliche Fehlerrate

(en: **residual error rate**)

geschätzte Rate, bei welcher die Sicherheitsmaßnahmen der SCL nicht mehr in der Lage sind Fehler zu entdecken.

3.1.1.24

Risiko

(en: **risk**)

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

ANMERKUNG Für die weitere Diskussion dieses Konzepts siehe IEC 61508-5:2010^{[3])}, Anhang A.

[IEC 61508-4:2010], [ISO/IEC Guide 51:1999, Definition 3.2]

3.1.1.25

Sicherheitskommunikationskanal

(en: **safety communication channel**)

Kommunikationskanal, beginnend an der Spitze der SCL der Quelle und endend an der Spitze der SCL der Senke.

ANMERKUNG zum Begriff 1 Er kann als zwei SCL's modelliert werden, die von einem Black Channel, von einem festgelegten Kommunikationssystem oder einem festgelegten Kanal verbunden sind.

3.1.1.26

Sicherheitskommunikationsschicht

(en: **Safety Communication Layer (SCL)**)

Kommunikationsschicht, die sämtliche notwendigen Mittel beinhaltet, um die sichere Übertragung von Daten entsprechend den Anforderungen in IEC 61508 zu gewährleisten

3.1.1.27

sichere Verbindung

(en: **safety connection**)

Verbindung, welche das Sicherheitsprotokoll für Kommunikationstätigkeiten nutzt

3.1.1.28

Sicherheitsdaten

(en: **safety data**)

Daten, die in einem Sicherheitsnetzwerk unter Nutzung eines Sicherheitsprotokolls übertragen wurden

ANMERKUNG Die Sicherheitskommunikationsschicht garantiert nicht sichere Daten an sich, sondern nur den gesicherten Transport.

3.1.1.29

Sicherheitsgerät

(en: **safety device**)

Gerät, welches nach IEC 61508 ausgeführt wurde und das funktional sichere Kommunikationsprofil zur Anwendung bringt

3.1.1.30

Sicherheitsfunktion

(en: **safety function**)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

ANMERKUNG Die Definition in IEC 61508-4 ist die gleiche, jedoch mit einem zusätzlichen Beispiel und einer Referenz.

^{[3])} Noch zu veröffentlichen.

[IEC 61508-4:2010, modifiziert]

3.1.1.31

Reaktionszeit einer Sicherheitsfunktion

(en: **safety function response time**)

im ungünstigsten Fall benötigte Zeit nach Aktivierung eines am Feldbus angeschlossenen Sicherheits-sensors, bis der zugehörige sichere Zustand des Sicherheitsaktors erreicht wurde, unter Berücksichtigung von gleichzeitig auftretenden Fehlern und Ausfällen im Übertragungskanal der Sicherheitsfunktion

ANMERKUNG Dieses Konzept wird in IEC 61784-3:2010^{[4])}, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.32

Sicherheits-Integritätslevel

(en: **safety integrity level (SIL)**)

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

ANMERKUNG 1 Die Ausfallgrenzwerte (siehe IEC 61508-4:2010, 3.5.17) für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 in IEC 61508-1:2010^{[5])} festgelegt.

ANMERKUNG 2 Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen verwendet, die den sicherheitsbezogenen E/E/PE-Systemen zugeordnet werden.

ANMERKUNG 3 Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung des Ausdrucks „sicherheitsbezogenes System mit SIL n“ (wobei „n“ 1, 2, 3 oder 4 ist) ist, dass das System potentiell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

3.1.1.33

Sicherheitsmaßnahme

(en: **safety measure**)

<diese Norm> Mittel zur Beherrschung möglicher Kommunikationsfehler, welches in Übereinstimmung mit den Anforderungen in IEC 61508 entworfen und ausgeführt wurde

ANMERKUNG 1 In der Praxis werden mehrere Sicherheitsmaßnahmen kombiniert, um den geforderten Sicherheits-Integritätslevel zu erzielen.

ANMERKUNG 2 Kommunikationsfehler und zugehörige Sicherheitsmaßnahmen sind ausführlich in IEC 61784-3:2010, 5.3 und 5.4, beschrieben.

3.1.1.34

sicherheitsbezogene Anwendung

(en: **safety-related application**)

Programme, welche in Übereinstimmung mit den Anforderungen in IEC 61508 ausgeführt sind, um die SIL-Anforderungen der Anwendung einzuhalten

3.1.1.35

sicherheitsrelevantes System

(en: **safety-related system**)

System, welches Sicherheitsfunktionen nach IEC 61508 ausführt

[4]) In Bearbeitung.

[5]) Noch zu veröffentlichen.

3.1.2 CPF 17: Zusätzliche Begriffe

3.1.2.1

Herzschlag

(en: heartbeat)

Timer für Sender oder Empfänger, um zu überwachen, ob der Kommunikationspartner am Leben ist

3.1.2.2

Aufrufer

(en: Initiator)

Funktion eines FSCP 17/1-Geräts, welches zur Herstellung einer Verbindung verantwortlich ist

3.1.2.3

Antwortender

(en: Responder)

Funktion eines FSCP 17/1-Geräts, welches den Aufbau einer Verbindung, die vom Aufrufer hergestellt wird, einhält

3.1.2.4

Empfänger

(en: Receiver)

passive Kommunikationseinheit, die in der Lage ist, Nachrichten zu empfangen und sie als Antwort an eine andere Kommunikationseinheit zu senden, welche ein Sender oder Empfänger sein kann

3.1.2.5

Sender

(en: Sender)

aktive Kommunikationseinheit, die in der Lage ist, Kommunikationsaktivitäten von anderen Stationen einzuleiten und zu planen, welche Sender oder Empfänger sein können

3.1.2.6

SUID

(en: SUID safety Unique Identification)

64 Bit-Wert der logischen Verbindungs-Identifikationsnummer der FSCP 17/1, welche eine Kombination der UIDs von zwei Geräten ist

3.1.2.7

UID

(en: UID Unique Identification)

Identifikationsnummer der CPF 17, welche eine Kombination aus der 48 Bit-MAC-Adresse und der 16 Bit-Geräteadresse ist

3.1.2.8

virtuelle Ablaufnummer

(en: virtual sequence number)

interner Wert für jedes FSCP 17/1-Gerät, verwendet, um den Nachrichtenablauf zu prüfen, aber nicht im Nachrichtenrahmen übertragen

– Leerseite –

INCLUDED SUBPARTS

NOTE 1: The page numbers of each subpart are prefixed with the CPF number of the subpart to facilitate identification, and so that the numbering of each subpart can be independent of those that precede it.

NOTE 2: The Contents of each subpart begins on page xxx2, so that the page numbering will be unchanged when the final International Standard is issued with its IEC-Central-Office-provided cover sheet.

NOTE 3: Part 3-1 (Ed 2.0), Part 3-6 (Ed 2.0), Part 3-12 (Ed 1.0) and Part 3-14 (Ed 1.0) are not included since they are simply reconfirmed, as indicated in 65C/712A/RR.

IEC 61784-3-2 Ed3.0, Industrial communication networks - Profiles – Part 3-2: Functional safety fieldbuses - Additional specifications for CPF 2	2002
IEC 61784-3-3 Ed3.0, Industrial communication networks - Profiles – Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3	3002
IEC 61784-3-8 Ed2.0, Industrial communication networks - Profiles – Part 3-8: Functional safety fieldbuses - Additional specifications for CPF 8	8002
IEC 61784-3-13 Ed2.0, Industrial communication networks - Profiles – Part 3-13: Functional safety fieldbuses - Additional specifications for CPF 13	13002
IEC 61784-3-17 Ed1.0, Industrial communication networks - Profiles – Part 3-17 Functional safety fieldbuses - Additional specifications for CPF 17	17002
IEC 61784-3-18 Ed1.0 Amd.1, Industrial communication networks - Profiles – Part 3-18: Functional safety fieldbuses - Additional specifications for CPF 18	18002

CONTENTS

FOREWORD.....	2012
0 Introduction	2014
0.1 General	2014
0.2 Patent declaration	2016
1 Scope	2017
2 Normative references	2017
3 Terms, definitions, symbols, abbreviated terms and conventions	2018
3.1 Terms and definitions	2018
3.1.1 Common terms and definitions	2019
3.1.2 CPF 2: Additional terms and definitions	2023
3.2 Symbols and abbreviated terms.....	2023
3.2.1 Common symbols and abbreviated terms	2023
3.2.2 CPF 2: Additional symbols and abbreviated terms	2024
3.3 Conventions	2025
4 Overview of FSCP 2/1 (CIP Safety™).....	2025
4.1 General	2025
4.2 FSCP 2/1	2026
5 General	2027
5.1 External documents providing specifications for the profile	2027
5.2 Safety functional requirements	2027
5.3 Safety measures	2027
5.4 Safety communication layer structure	2028
5.5 Relationships with FAL (and DLL, PhL)	2028
5.5.1 General	2028
5.5.2 Data types	2029
6 Safety communication layer services	2029
6.1 Introduction	2029
6.2 Connection object	2029
6.2.1 General	2029
6.2.2 Class attribute extensions	2029
6.2.3 Service extensions	2030
6.2.4 Explicit message response format for SafetyOpen and SafetyClose	2030
6.3 Connection Manager object	2031
6.3.1 General	2031
6.3.2 ForwardOpen for safety	2031
6.3.3 Safety network segment	2033
6.3.4 Originator rules for calculating the connection parameter CRC	2036
6.3.5 SafetyOpen processing flowcharts	2036
6.3.6 Checks required by Multipoint producers with existing connections	2039
6.3.7 Electronic key usage for safety	2040
6.3.8 RPI vs. API in safety connections	2040
6.3.9 Application path construction for safety	2040
6.3.10 Safety Validator connection types	2041
6.3.11 Application reply data in a successful SafetyOpen response	2043
6.3.12 Unsuccessful SafetyOpen response	2045
6.3.13 ForwardClose for safety	

6.4	Identity object.....	2047
6.4.1	General	2047
6.4.2	Changes to common services	2047
6.4.3	Extensions for CP 16/3 devices	2048
6.5	Link objects	2048
6.5.1	DeviceNet object changes	2048
6.5.2	TCP/IP Interface object changes	2049
6.5.3	SERCOS III Link object	2049
6.6	Safety Supervisor object.....	2050
6.6.1	General	2050
6.6.2	Safety Supervisor class attributes.....	2051
6.6.3	Subclasses	2051
6.6.4	Safety Supervisor instance attributes.....	2051
6.6.5	Semantics	2054
6.6.6	Subclasses	2061
6.6.7	Safety Supervisor common services	2061
6.6.8	Safety Supervisor behavior	2072
6.7	Safety Validator object	2078
6.7.1	General	2078
6.7.2	Class attributes	2078
6.7.3	Instance attributes	2079
6.7.4	Class services	2084
6.7.5	Instance services.....	2084
6.7.6	Object behavior	2085
6.8	Connection Configuration Object	2088
6.8.1	General	2088
6.8.2	Class attribute extensions	2088
6.8.3	Instance attributes, additions and extensions.	2088
6.8.4	Instance attribute semantics extensions or restrictions for safety	2090
6.8.5	Special Safety Related Parameters – (Attribute 13)	2094
6.8.6	Object-specific services	2099
6.8.7	Common service extensions for safety.....	2099
6.8.8	Object behavior	2101
7	Safety communication layer protocol	2102
7.1	Safety PDU format	2102
7.1.1	Safety PDU encoding	2102
7.1.2	Safety CRC	2114
7.2	Communication protocol behavior.....	2115
7.2.1	Sequence of safety checks	2115
7.2.2	Connection termination.....	2115
7.2.3	Cross checking error	2115
7.3	Time stamp operation.....	2116
7.4	Rollover counts in the EF	2116
7.5	Protocol sequence diagrams	2117
7.5.1	General	2117
7.5.2	Normal safety transmission.....	2117
7.5.3	Lost, corrupted and delayed message transmission	2118
7.5.4	Lost, corrupted or delayed message transmission with production repeated	2118

7.5.5	Point-to-point ping	2122
7.5.6	Multipoint ping on CP 2/3 Safety.....	2123
7.5.7	Multipoint ping on CP 2/2 safety networks	2124
7.5.8	Multipoint ping – retry with success	2125
7.5.9	Multipoint ping – retry with timeout	2126
7.6	Safety protocol definition	2126
7.6.1	General	2126
7.6.2	High level view of a safety device	2126
7.6.3	Safety Validator object	2127
7.6.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	2127
7.6.5	Extended Format time stamp rollover handling	2128
7.6.6	SafetyValidatorClient function definition	2132
7.6.7	SafetyValidatorServer function definition	2140
7.7	Safety message and protocol data specifications.....	2153
7.7.1	Mode octet	2153
7.7.2	Time Stamp Section	2153
7.7.3	Time Coordination Message	2153
7.7.4	Time correction message.....	2154
7.7.5	Safety data production.....	2155
7.7.6	Producer dynamic variables.....	2161
7.7.7	Producer per consumer dynamic variables	2163
7.7.8	Consumer data variables	2164
7.7.9	Consumer input static variables	2166
7.7.10	Consumer dynamic variables	2166
8	Safety communication layer management.....	2168
8.1	Overview	2168
8.2	Definition of the measures used during connection establishment	2169
8.3	Originator-Target relationship validation	2172
8.4	Detection of mis-routed connection requests	2173
8.5	SafetyOpen processing	2173
8.6	Ownership management	2173
8.7	Bridging different physical layers	2174
8.8	Safety connection establishment	2175
8.8.1	Overview	2175
8.8.2	Basic facts for connection establishment	2176
8.8.3	Configuring safety connections	2176
8.8.4	Network time expectation multiplier	2177
8.8.5	Establishing connections	2179
8.8.6	Recommendations for consumer number allocation	2182
8.8.7	Recommendations for connection establishment	2183
8.8.8	Ownership establishment.....	2183
8.8.9	Ownership use cases	2184
8.8.10	PID/CID usage and establishment	2186
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections	2187
8.8.12	Network supported services.....	2189
8.8.13	FSCP 2/1 safety device type.....	2190
8.9	Safety configuration process	2193
8.9.1	Introduction to safety configuration	2193

8.9.2	Configuration goals	2193
8.9.3	Configuration overview	2194
8.9.4	User configuration guidelines	2195
8.9.5	Configuration process SIL3 justification	2196
8.9.6	Device functions for tool configuration	2196
8.9.7	Password security	2197
8.9.8	SNCT interface services	2197
8.9.9	Configuration lock	2197
8.9.10	Effect of configuration lock on device behavior	2198
8.9.11	Configuration ownership	2199
8.9.12	Configuration mode	2199
8.9.13	Measures used to ensure integrity of configuration process	2199
8.9.14	Download process	2201
8.9.15	Verification process	2204
8.9.16	Verification process	2206
8.9.17	Configuration error analysis	2207
8.10	Electronic Data Sheets extensions for safety	2211
8.10.1	General rules for EDS based safety devices	2211
8.10.2	EDS extensions for safety	2211
8.11	Requirements for CP 2/2	2216
8.11.1	EPI rules for safety messages that travel over CP 2/2	2216
8.11.2	Default safety I/O service	2216
8.11.3	Duplicate IP detection	2216
8.11.4	Priority for safety connections	2217
8.12	Requirements for CP 2/3	2217
8.12.1	Allocation of CP 2/3 identifiers	2217
8.12.2	Additional requirements	2219
8.13	CP 16/3 requirements	2219
8.13.1	General architecture for CPF 2 on CP 16/3	2219
8.13.2	Baseline FSCP 2/1 on CP 16/3 device	2220
8.13.3	Supported objects and services in CP 16/3 devices	2220
8.13.4	Transport layer requirements	2221
8.13.5	FSCP 2/1 and the CP 16/3 device model	2223
8.13.6	UNID assignment on CP 16/3	2224
9	System requirements	2226
9.1	Indicators and switches	2226
9.1.1	General indicator requirements	2226
9.1.2	LED indications for setting the device UNID	2226
9.1.3	Module Status LED	2226
9.1.4	Indicator warning	2227
9.1.5	Network Status LED	2227
9.1.6	Switches	2228
9.2	Installation guidelines	2230
9.3	Safety function response time	2230
9.3.1	Overview	2230
9.3.2	Network time expectation	2231
9.3.3	Equations for calculating network reaction times	2232
9.4	Duration of demands	2234
9.5	Constraints for calculation of system characteristics	2234

9.5.1	Number of nodes	2234
9.5.2	Network PFH	2234
9.5.3	Bit Error Rate (BER)	2236
9.6	Maintenance	2237
9.7	Safety manual	2237
10	Assessment	2237
Annex A (informative) Additional information for functional safety communication profiles of CPF 2		2238
A.1	Hash function example code	2238
A.2		2252
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2		2253
Bibliography		2254
Table 1 – Communications errors and detection measures matrix		2027
Table 2 – New class attributes		2029
Table 3 – Service extensions		2030
Table 4 – SafetyOpen and SafetyClose response format		2030
Table 5 – Safety network segment identifier		2033
Table 6 – Safety network segment definition		2033
Table 7 – Safety network segment router format		2035
Table 8 – Safety Network Segment Extended Format		2035
Table 9 – Multipoint producer parameter evaluation rules		2040
Table 10 – ForwardOpen setting options for safety connections		2042
Table 11 – Network connection parameters for safety connections		2043
Table 12 – CP 2/3 Safety target application reply (size: 10 octets)		2043
Table 13 – EF CP 2/3 Safety target application reply (size: 14 octets)		2044
Table 14 – SafetyOpen target application reply (size: 18 octets)		2044
Table 15 – EF SafetyOpen target application reply (size: 22 octets)		2044
Table 16 – New and extended error codes for safety		2045
Table 17 – SafetyOpen error event guidance table		2046
Table 18 – Identity object common service changes		2048
Table 19 – Identity object extensions for CP 16/3 devices		2048
Table 20 – New DeviceNet object instance attribute		2048
Table 21 – New TCP/IP Interface object instance attribute		2049
Table 22 – SERCOS III Link object class attributes		2049
Table 23 – SERCOS III Link object instance attributes		2050
Table 24 – SERCOS III Link Object Common Services		2050
Table 25 – Safety Supervisor class attributes		2051
Table 26 – Safety Supervisor instance attributes		2051
Table 27 – Device status attribute state values		2055
Table 28 – Exception status attribute format		2056
Table 29 – Common exception detail attribute values		2057
Table 30 – Exception detail format summary		2057

— Entwurf —

IEC CDV 61784-3-2 © IEC 2014

– 2007 –

Table 31 – Summary of device behavior for various CFUNID values	2059
Table 32 – Safety Supervisor common services	2061
Table 33 – Safety Supervisor object specific services	2061
Table 34 – Configure_Request message structure	2063
Table 35 – Validate_Configuration message structure	2064
Table 36 – Validate_Configuration success message structure	2064
Table 37 – Validate_Configuration error code	2064
Table 38 – Validate_Configuration extended codes	2064
Table 39 – Set_Password message structure	2067
Table 40 – Reset_Password message structure	2067
Table 41 – Configuration_Lock/Unlock message structure	2067
Table 42 – Mode_Change message structure	2068
Table 43 – Safety_Reset message structure	2068
Table 44 – Safety Supervisor safety reset types	2069
Table 45 – Attribute bit map parameter	2069
Table 46 – Reset processing rules for reset types	2069
Table 47 – Propose_TUNID service	2070
Table 48 – Apply_TUNID service	2070
Table 49 – Safety Supervisor events	2072
Table 50 – State event matrix for Safety Supervisor	2073
Table 51 – Configuration owner control vs. device state	2076
Table 52 – State mapping of Safety Supervisor to Identity object	2077
Table 53 – Safety Supervisor object event mapping	2077
Table 54 – Identity object event mapping	2078
Table 55 – Safety Validator class attributes	2078
Table 56 – Safety Validator instance attributes	2079
Table 57 – Safety Validator state assignments	2081
Table 58 – Safety Validator type, bit field assignments	2081
Table 59 – Multipoint producer SafetyOpen parameter evaluation rules	2083
Table 60 – Safety Validator class services	2084
Table 61 – Safety Validator instance services	2084
Table 62 – Safety Validator Get_Attributes_All service data	2085
Table 63 – Safety Validator state event matrix	2087
Table 64 – State mapping between Safety Supervisor and Safety Validator objects	2087
Table 65 – Connection configuration object class attribute extensions	2088
Table 66 – Connection Configuration Object instance attribute additions/extensions	2088
Table 67 – Connection flag bit definitions	2090
Table 68 – O-to-T connection parameters	2091
Table 69 – T-to-O connection parameters	2092
Table 70 – Data map formats	2093
Table 71 – Data map format 0	2094
Table 72 – Data map format 1	2094
Table 73 – Target device's SCCRC values	2096

Table 74 – Target device's SCTS values.....	2096
Table 75 – Time correction connection parameters for multipoint connection	2097
Table 76 – Format Type attribute meaning	2098
Table 77 – Format Status attribute meaning.....	2099
Table 78 – Connection Configuration Object-specific services	2099
Table 79 – Get_Attributes_All Response service data (added attributes)	2100
Table 80 – Get_Attributes_All Response service data (added parameters)	2100
Table 81 – Set_Attributes_All Request service data (added attributes)	2100
Table 82 – Set_Attributes_All Response service data (added parameters).....	2101
Table 83 – State Mapping between Safety Supervisor and the CCO objects	2101
Table 84 – Connection sections and PDU formats.....	2103
Table 85 – Mode octet variables	2104
Table 86 – Time Stamp variables.....	2107
Table 87 – Time Coordination message variables	2108
Table 88 – Time Correction Message variables.....	2110
Table 89 – CRC polynomials used	2114
Table 90 – Connection sections and message formats.....	2115
Table 91 – Data reception - Link triggered	2143
Table 92 – Time_Correction reception - Link triggered	2143
Table 93 – Data reception - Application triggered.....	2143
Table 94 – Time_Correction reception - Application triggered	2143
Table 95 – Consuming application – Safety data monitoring	2144
Table 96 – Producer connection status determination	2155
Table 97 – Consuming safety connection status	2165
Table 98 – Connection establishment errors and measures to detect errors.....	2169
Table 99 – SNN Date/Time allocations.....	2169
Table 100 – SNN legal range of time values	2170
Table 101 – Safety connection parameters	2177
Table 102 – SafetyOpen summary	2180
Table 103 – Originator/Target service mapping.....	2190
Table 104 – Unsupported originator/target service types.....	2191
Table 105 – Configuration goals	2194
Table 106 – Configuration owner control vs. device state.....	2199
Table 107 – Errors and detection measures	2208
Table 108 – Object Class section keywords	2211
Table 109- Safety Classx entry format	2212
Table 110 – Parameter class keywords.....	2213
Table 111 – New Connection Manager section keywords for safety	2213
Table 112 – Connection Manager field usage for safety	2214
Table 113 – Connection parameter field settings for safety	2216
Table 114 – CP 2/3 ID assignment rules	2217
Table 115 – LED indications for setting UNID	2226
Table 116 – Module Status LED.....	2227

Table 117 – Network status LED states	2227
Table 118 – Connection reaction time type – producing/consuming applications	2232
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	2014
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	2015
Figure 3 – Relationship of Safety Validators	2026
Figure 4 – Communication layers.....	2028
Figure 5 – ForwardOpen with safety network segment	2032
Figure 6 – Safety network target format	2034
Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)	2037
Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen)	2038
Figure 9 – Originator logic to determine which format to use	2039
Figure 10 – Applying device configuration.....	2065
Figure 11 – Configure and Validate processing flowcharts	2066
Figure 12 – UNID handling during “Waiting for TUNID”	2071
Figure 13 – Safety Supervisor state diagram.....	2072
Figure 14 – Configuration, testing and locked relationships.....	2076
Figure 15 – Safety connection types	2082
Figure 16 – Safety Validator state transition diagram	2086
Figure 17 – Logic for Auto-detecting format type.....	2098
Figure 18 – Connection Configuration Object state diagram.....	2102
Figure 19 – Connection Configuration Object data flow	2102
Figure 20 – Format of the mode octet	2104
Figure 21 – 1 or 2 octet data section, Base Format	2104
Figure 22 – 1 or 2 octet data section, Extended Format	2105
Figure 23 – 3 to 250 octet data section format, Base Format	2105
Figure 24 – 3 to 250 octet data section format, Extended Format.....	2106
Figure 25 – Time Stamp section format, Base Format.....	2107
Figure 26 – BF Time Coordination message encoding	2108
Figure 27 – EF Time Coordination message encoding	2108
Figure 28 – BF Time Correction message encoding	2109
Figure 29 – EF Time Correction message encoding	2109
Figure 30 – 1 or 2 octet point-to-point PDU encoding.....	2111
Figure 31 – 1 or 2 Octet multipoint PDU encoding.....	2111
Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format.....	2112
Figure 33 – 3 to 250 Octet Point-to-point PDU encoding	2112
Figure 34 – 3 to 248 Octet Multipoint PDU encoding	2113
Figure 35 – 3 to 248 Octet, Multipoint, safety connection format	2113
Figure 36 – CRC Calculation order for Extended Format messages	2114
Figure 37 – Time stamp sequence	2116
Figure 38 – Sequence diagram of a normal producer/consumer safety sequence.....	2117

Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated)	2118
Figure 40 – Sequence diagram of a corrupted producer to consumer message	2119
Figure 41 – Sequence diagram of a lost producer to consumer message	2119
Figure 42 – Sequence diagram of a delayed message	2120
Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated	2121
Figure 44 – Sequence diagram of a connection terminated due to delays	2121
Figure 45 – Sequence diagram of a failure of safety CRC check	2122
Figure 46 – Sequence diagram of a point-to-point ping - normal response	2122
Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety	2124
Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety	2125
Figure 49 – Sequence diagram of a multipoint ping retry.....	2125
Figure 50 – Sequence diagram of a multipoint ping timeout	2126
Figure 51 – Safety device reference model entity relation diagram.....	2127
Figure 52 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	2128
Figure 53 – Point-to-point, originating consumer, target producer	2129
Figure 54 – Point-to-point, originator producer, target consumer.....	2130
Figure 55 – Multi-point, originator consumer, target producer	2131
Figure 56 – Safety production data flow	2132
Figure 57 – Consumer safety data monitoring	2141
Figure 58 – SafetyValidatorServer - application triggered	2142
Figure 59 – Target ownership	2172
Figure 60 – SafetyOpen forms	2173
Figure 61 – Connection ownership state chart	2174
Figure 62 – SafetyOpen UNID mapping	2174
Figure 63 – Common CPF 2 application layer	2175
Figure 64 – End-to-End routing example	2175
Figure 65 – Sources for safety related connection parameters	2178
Figure 66 – Parameter mapping between originator and target	2179
Figure 67 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen... ..	2181
Figure 68 – General sequence to detect configuration is required	2182
Figure 69 – PID/CID exchanges for two originator scenarios.....	2187
Figure 70 – Seed generation for multipoint connections	2188
Figure 71 – PID/CID runtime handling.....	2189
Figure 72 – Connection categories and supported services.....	2191
Figure 73 – Recommended connection types.....	2192
Figure 74 – Logic-to-logic supported services	2192
Figure 75 – Recommended connection types for logic to logic	2193
Figure 76 – Configuration data transfers	2194
Figure 77 – Protection measures in safety devices	2196
Figure 78 – Configuration, testing and locked relationships.....	2198
Figure 79 – Originator's configuration data	2199

Figure 80 – SNCT to device download process	2202
Figure 81 – SNCT Downloads to originators that perform Form 1 configuration	2203
Figure 82 – Protection from locking and ownership	2205
Figure 83 – Example of read back and comparison of original and printout	2205
Figure 84 – Diverse display without full data read back	2206
Figure 85 – Verification process including all alternatives	2207
Figure 86 – Baseline FSCP 2/1 on CP 16/3 device	2220
Figure 87 – FSCP 2/1 Adaptation Layer and SMP interaction	2222
Figure 88 – FSCP 2/1 Adaptation	2223
Figure 89 – CP 16/3 device model	2224
Figure 90 – Adding a standard module to a modular device	2225
Figure 91 – Safety device NodeID processing logic	2230
Figure 92 – Safety function response time	2231
Figure 93 – Safety function response time components	2233
Figure 94 – Network protocol reliability block diagram (RBD)	2234
Figure 95 – Network PFH summary	2235
Figure 96 – Extended Format PFH summary	2236

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3-2: Functional safety fieldbuses –
Additional specifications for CPF 2**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
 - 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
 - 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
 - 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
 - 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
 - 6) All users should ensure that they have the latest edition of this publication.
 - 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
 - 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- International Standard IEC 61784-3-2 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.
- This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision. The main changes with respect to the previous edition are listed below (and highlighted in yellow in this document).
- Added detailed requirements for use of FSCP 2/1 in conjunction with CP 16/3 (see 4.1, 6.4.3, 6.5.3, 8.2, 8.13, and miscellaneous references when referencing CPF 2 networks)
 - Defined object class section keywords for safety to EDS file definition in 8.10.2.1
 - New sections on safety CRC overview in 7.1.2.1 and Rollover counts for EF format in 7.4
 - Corrections to PFH calculations in 9.5.2
 - Change from MACID to NodeID as general reference to network identifier
 - Miscellaneous minor corrections made since the last publication