

DIN EN 61784-3-18

ICS 35.240.50; 35.160

**Industrielle Kommunikationsnetze –
Profile –****Teil 3-18: Funktional sichere Übertragung bei Feldbussen – Zusätzliche
Festlegungen für die Kommunikationsprofilfamilie 18
(IEC 61784-3-18:2011);
Englische Fassung EN 61784-3-18:2011**

Industrial communication networks –

Profiles –

Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18

(IEC 61784-3-18:2011);

English version EN 61784-3-18:2011

Réseaux de communication industriels –

Profils –

Partie 3-18: Bus de terrain à sécurité fonctionnelle – Spécifications supplémentaires pour
le CPF 18 (CEI 61784-3-18:2011);

Version anglaise EN 61784-3-18:2011

Gesamtumfang 69 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2011-05-25 angenommene Europäische Norm als DIN-Norm ist 2012-07-01.

Nationales Vorwort

Zu diesem Dokument wurde ein Kurzverfahren in den DIN-Mitteilungen veröffentlicht.

Für diese Norm 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.

Die enthaltene IEC-Publikation wurde vom SC 65C „Industrial networks“ erarbeitet.

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

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

Die 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, DIN EN 61784-2 und der Reihe DIN EN 61158 fest. Für diese Kommunikationsnormen ist keine deutsche Sprachfassung verfügbar. Sie alleine 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 der 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.

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.

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 die vorliegende Norm erfüllt.

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die englische Fassung der EN 61784-3-18 veröffentlicht. Zu deren Abschnitt 3, der die Begriffe festlegt, wurde

eine Übersetzung angefertigt und als Nationaler Anhang NA der vorliegenden Norm 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.

Nationaler Anhang NA (informativ)

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 [35], [36]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], [IEC 61158]

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

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

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

Telegrammrahmen (en: frame)

veraltetes Synonym für DLPDU

3.1.1.12

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 [35], [36].

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**Nachrichtensenke (en: message sink)**

Teil eines *Kommunikationssystems*, der für den Empfang von *Nachrichten* gedacht ist

[ISO/IEC 2382-16.02.03]

3.1.1.17**Nachrichtenquelle (en: message source)**

Teil eines *Kommunikationssystems*, der für den Versand von *Nachrichten* gedacht ist

[ISO/IEC 2382-16.02.02]

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**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**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, 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**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.

3.1.1.24

Sicherheitsgerät (en: safety device)

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

3.1.1.25

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]

3.1.1.26

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, 5.2.4, eingeführt und von den in diesem Normteil aufgeführten funktional sicheren Kommunikationsprofilen verwendet.

3.1.1.27

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 IEC 61508-1:2010, Tabelle 2 und 3, 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 potenziell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu „n“ zu unterstützen.

[IEC 61508-4:2010]

3.1.1.28

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.

3.1.1.29

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

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

System, welches *Sicherheitsfunktionen* nach IEC 61508 ausführt

3.1.1.31**unberechtigte Auslösung (en: spurious trip)**

Auslösung in einem Sicherheitssystem ohne Prozessanforderung

3.1.2 CPF 18: Zusätzliche Begriffe**3.1.2.1****Client-Server-Beziehung (en: client/server relationship)**

Beziehung, in welcher der Client Daten an den Server sendet, der wiederum mit den angeforderten Daten antwortet

3.1.2.2**laufende Nummer (en: consecutive number)**

vorzeichenlose ganze Zahl mit Umbruch auf Null bei Überlauf, die als Mittel zur Sicherung der Vollständigkeit und der richtigen Reihenfolge von übertragenen Sicherheits-PDUs verwendet wird

ANMERKUNG Beispiel für eine „fortlaufende Nummer“, wie in IEC 61784-3 beschrieben.

3.1.2.3**Zyklus (en: cycle)**

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

3.1.2.4**Verzögerung (en: delay)**

Übertragungszeit der PDUs, die dynamisch durch die Netzwerkeigenschaften, wie Verkehr, Schaltgeräte und Topologie, verursacht wird

3.1.2.5**ausfallsicher (en: fail-safe)**

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

3.1.2.6**Gateway (en: gateway)**

Gerät, das als Verbindungselement zwischen verschiedenen Protokollen agiert

3.1.2.7**logische Doppellinie (en: logical double line)**

Reihung des Root-Geräts und sämtlicher üblicher Geräte, die den Kommunikationsrahmen in Vorwärts- und Rückwärtsrichtung verarbeiten

3.1.2.8**Produzent-Verbraucher-Beziehung (en: producer/consumer relationship)**

Beziehung, in welcher der Produzent Daten ohne eine besondere Anforderung an den Verbraucher sendet

3.1.2.9**RTFL (en: real time frame line (RTFL))**

Kommunikationsmodell mit Geräten, die in einer logische Doppellinie kommunizieren (siehe CP 18/2)

3.1.2.10**RTFN (en: real time frame network (RTFN))**

Kommunikationsmodell mit Geräten, die in einem vermittelten Netz kommunizieren (siehe CP 18/1)

3.1.2.11**SCL-Verwaltung (en: SCL management (SALMT))**

Mechanismus zur Steuerung des SCL-Zustands von Sicherheitsgeräten

3.1.2.12

Überwachung der Sicherheitsverzögerung (en: safety delay monitoring (SDM))

Sicherheitsmechanismus zur zyklischen Überwachung der Verzögerung von übertragenen PDUs

3.1.2.13

Sicherheitsherzschlag (en: safety heartbeat (SHB))

Mechanismus zur zyklischen Überwachung des Zustands von Sicherheitsgeräten

3.1.2.14

Sicherheitsprozessdatenobjekt (SPDO) (en: safety process data object (SPDO))

Mechanismus zum zyklischen Austausch von Sicherheitsprozessdaten zwischen Geräten

3.1.2.15

Sender-Empfänger-Beziehung (en: sender/receiver relationship)

Beziehung, in welcher der Sender Daten an den Empfänger sendet

3.1.2.16

1:1-Beziehung (en: 1:1 relationship)

Kommunikationsbeziehung mit genau einem Sender und einem Empfänger

3.1.2.17

1:n-Beziehung (en: 1:n relationship)

Kommunikationsbeziehung mit genau einem Sender und einem oder mehreren Empfängern

**Industrial communication networks -
Profiles -
Part 3-18: Functional safety fieldbuses -
Additional specifications for CPF 18
(IEC 61784-3-18:2011)**

Réseaux de communication industriels -
Profils -
Partie 3-18: Bus de terrain à sécurité
fonctionnelle -
Spécifications supplémentaires pour le
CPF 18
(CEI 61784-3-18:2011)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-18: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen für die
Kommunikationsprofilfamilie 18
(IEC 61784-3-18:2011)

This European Standard was approved by CENELEC on 2011-05-25. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of document 65C/639/FDIS, future edition 1 of IEC 61784-3-18, prepared by SC 65C, Industrial networks, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61784-3-18 on 2011-05-25.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2012-02-25
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2014-05-25

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-18:2011 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60204-1	NOTE Harmonized as EN 60204-1.
IEC 61131-6	NOTE Harmonized as EN 61131-61).
IEC 61158 series	NOTE Harmonized in EN 61158 series.
IEC 61326-3-1	NOTE Harmonized as EN 61326-3-1.
IEC 61326-3-2	NOTE Harmonized as EN 61326-3-2.
IEC 61496 series	NOTE Harmonized in EN 61496 series.
IEC 61508-1:2010	NOTE Harmonized as EN 61508-1:2010.
IEC 61508-4:2010	NOTE Harmonized as EN 61508-4:2010.
IEC 61508-5:2010	NOTE Harmonized as EN 61508-5:2010.
IEC 61511 series	NOTE Harmonized in EN 61511 series.
IEC 61784-1	NOTE Harmonized as EN 61784-1.
IEC 61784-5 series	NOTE Harmonized in EN 61784-5 series.
IEC 61800-5-2	NOTE Harmonized as EN 61800-5-2.
IEC 62061	NOTE Harmonized as EN 62061.
ISO 10218-1	NOTE Harmonized as EN ISO 10218-1.

1) At draft stage.

ISO 12100-1	NOTE Harmonized as EN ISO 12100-1.
ISO 13849-1	NOTE Harmonized as EN ISO 13849-1.
ISO 13849-2	NOTE Harmonized as EN ISO 13849-2.
ISO 14121	NOTE Harmonized as EN ISO 14121.

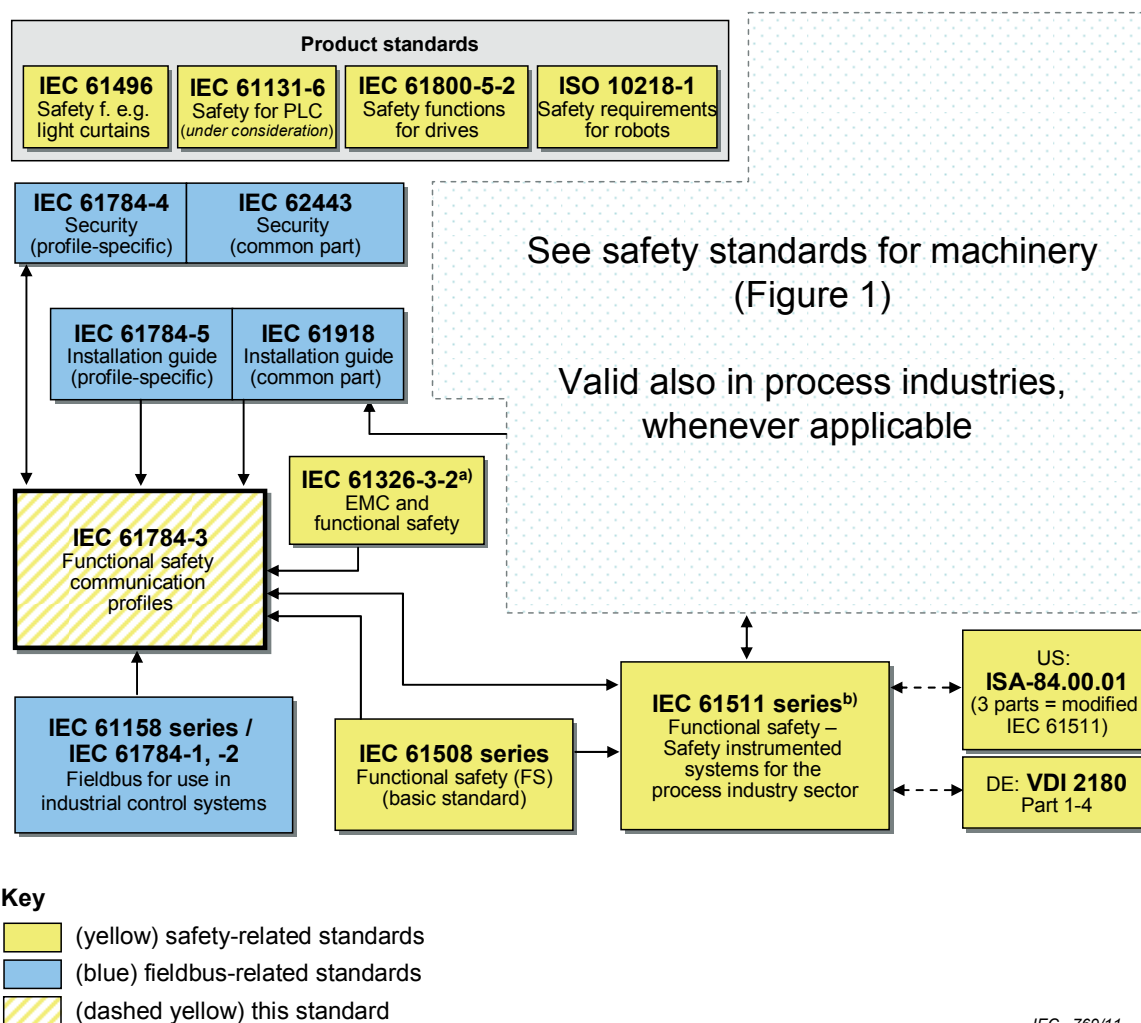
CONTENTS

0	Introduction	7
0.1	General	7
0.2	Patent declaration	9
1	Scope	10
2	Normative references	10
3	Terms, definitions, symbols, abbreviated terms and conventions	11
3.1	Terms and definitions	11
3.1.1	Common terms and definitions	11
3.1.2	CPF 18: Additional terms and definitions	15
3.2	Symbols and abbreviated terms	16
3.2.1	Common symbols and abbreviated terms	16
3.2.2	CPF 18: Additional symbols and abbreviated terms	16
3.3	Conventions	17
4	Overview of FSCP 18/1 (SafetyNET p™)	18
4.1	General	18
4.2	FSCP 18/1	19
5	General	20
5.1	External documents providing specifications for the profile	20
5.2	Safety functional requirements	20
5.3	Safety measures	20
5.4	Safety communication layer structure	21
5.5	Relationships with FAL (and DLL, PhL)	21
5.5.1	General	21
5.5.2	Data Types	21
6	Safety communication layer services	22
6.1	General elements	22
6.1.1	General	22
6.1.2	Safety object dictionary	22
6.1.3	Safety process data object (SPDO)	22
6.1.4	Safety heartbeat (SHB)	22
6.1.5	Safety delay monitoring (SDM)	22
6.2	Communication relation	22
7	Safety communication layer protocol	24
7.1	Safety PDU format	24
7.1.1	General	24
7.1.2	Safety process data objects (SPDO)	24
7.1.3	Safety heartbeat (SHB)	25
7.1.4	Safety PDUs embedded in a Type 22 PDU	27
7.2	Safety communication layer management (SALMT)	28
7.3	Safety process data communication	29
7.4	Safety heartbeat	31
7.5	Delay monitoring	32
8	Safety communication layer management	33
8.1	Parameter handling	33

8.2	Safety object dictionary	33
8.2.1	General	33
8.2.2	Communication profile section	34
8.2.3	Standardized device profile section	50
9	System requirements	50
9.1	Indicators and switches	50
9.1.1	Indicator states and flash rates	50
9.1.2	Indicators	51
9.1.3	Switches	51
9.2	Installation guidelines	51
9.3	Safety function response time	51
9.3.1	General	51
9.3.2	Determination of FSCP 18/1 time expectation behavior	52
9.3.3	Calculation of the worst case safety function response time	52
9.4	Duration of demands	53
9.5	Constraints for calculation of system characteristics	53
9.5.1	Safety related constraints	53
9.5.2	Probabilistic considerations	54
9.6	Maintenance	55
9.7	Safety manual	55
10	Assessment	55
Annex A (informative) Additional information for functional safety communication profiles of CPF 18		56
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 18		57
Bibliography		58
Annex ZA (normative) Normative references to international publications with their corresponding European publications		61
Table 1 – Object definition		18
Table 2 – Safety PDU element definition		18
Table 3 – Communication errors and detection measures		20
Table 4 – SPDO PDU structure		24
Table 5 – SHB request PDU structure		26
Table 6 – SHB response PDU structure		26
Table 7 – SHB safety communication layer state encoding		27
Table 8 – SALMT commands		28
Table 9 – System states of SALMT state machine		29
Table 10 – State transitions SALMT state machine		29
Table 11 – System states of RxSPDO state machine		30
Table 12 – State transitions RxSPDO state machine		30
Table 13 – Timeouts		31
Table 14 – Safety object dictionary structure		34
Table 15 – Objects of communication section		34
Table 16 – Device type		35
Table 17 – Safety ID		36
Table 18 – Safety consumer heartbeat entry		36
Table 19 – Safety consumer heartbeat		38

Table 20 – Safety producer heartbeat parameter.....	39
Table 21 – Safety bus cycle times	42
Table 22 – SPDO timeout tolerance	43
Table 23 – Receive SPDO communication parameter.....	43
Table 24 – Transmit SPDO communication parameter.....	46
Table 25 – Mapping format.....	49
Table 26 – Receive SPDO mapping parameter	49
Table 27 – Transmit SPDO mapping parameter	50
Table 28 – Indicator states definiton.....	51
Table 29 – STATUS indicator states	51
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	7
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	8
Figure 3 – FSCP 18/1 system.....	19
Figure 4 – FSCP 18/1 software architecture	21
Figure 5 – SPDO interaction model	23
Figure 6 – SHB interaction model.....	23
Figure 7 – Safety process data object structure	24
Figure 8 – Safety heartbeat request structure	25
Figure 9 – Safety heartbeat response structure	26
Figure 10 – Safety PDU for FSCP 18/1 embedded in a Type 22 CDC data section	28
Figure 11 – SALMT state machine	28
Figure 12 – RxSPDO state machine.....	30
Figure 13 – Heartbeat procedure.....	32
Figure 14 – Delay measurement principle.....	32
Figure 15 – Parameter handling	33
Figure 16 – Safety response time components	52
Figure 17 – Considered data fields for message size calculation	54
Figure 18 – Residual error rate.....	55

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



a For specified electromagnetic environments; otherwise IEC 61326-3-1.

b EN ratified.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

This standard describes:

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- individual description of functional safety profiles for several communication profile families in IEC 61784-1 and IEC 61784-2;
- safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

0.2 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the functional safety communication profiles for family 18 as follows, where the [xx] notation indicates the holder of the patent right:

DE 10 2008 007 672.4-31	[PI]	Verfahren und Vorrichtung zum Übertragen von Daten in einem Netzwerk
-------------------------	------	---

IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from:

Information may be obtained from:

[PI]	Pilz GmbH & Co. KG Felix-Wankel-Str. 2 73760 Ostfildern GERMANY
------	--

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://www.iec.ch/tctools/patent_decl.htm) maintain on-line data bases of patents relevant to their standards. Users are encouraged to consult the data bases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 18 of IEC 61784-2 and IEC 61158 Type 22. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series² for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61158-3-22, *Industrial communication networks – Fieldbus specifications – Part 3-22: Data-link layer service definition – Type 22 elements*

IEC 61158-4-22, *Industrial communication networks – Fieldbus specifications – Part 4-22: Data-link layer protocol specification – Type 22 elements*

IEC 61158-5-22, *Industrial communication networks – Fieldbus specifications – Part 5-22: Application layer service definition – Type 22 elements*

IEC 61158-6-22, *Industrial communication networks – Fieldbus specifications – Part 6-22: Application layer protocol specification – Type 22 elements*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

¹ In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

² In the following pages of this standard, “IEC 61508” will be used for “IEC 61508 series”.

IEC 61784-2:2010, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises*

ISO/IEC 10731, *Information technology – Open system interconnection – Basic reference model – Conventions for the definition of OSI services*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 Common terms and definitions

3.1.1.1 availability

probability for an automated system that for a given period of time there are no unsatisfactory system conditions such as loss of production

3.1.1.2 black channel

communication channel without available evidence of design or validation according to IEC 61508

3.1.1.3 communication channel

logical connection between two end-points within a *communication system*

3.1.1.4 communication system

arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498 application layer) from one application to another

3.1.1.5 connection

logical binding between two application objects within the same or different devices

3.1.1.6 Cyclic Redundancy Check (CRC)

<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

NOTE 1 Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this standard to refer to the redundant data.

NOTE 2 See also [35], [36]3.

³ Figures in square brackets refer to the Bibliography.

3.1.1.7

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

[IEC 61508-4:2010], [IEC 61158]

NOTE 1 Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

NOTE 2 Errors do not necessarily result in a *failure* or a *fault*.

3.1.1.8

failure

termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

NOTE 1 The definition in IEC 61508-4 is the same, with additional notes.

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

NOTE 2 Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

3.1.1.9

fault

abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEC 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

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

3.1.1.10

fieldbus

communication system based on serial data transfer and used in industrial automation or process control applications

3.1.1.11

frame

denigrated synonym for DLPDU

3.1.1.12

Frame Check Sequence (FCS)

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

NOTE 1 An FCS can be derived using for example a CRC or other hash function.

NOTE 2 See also [35], [36].

3.1.1.13

hash function

(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

NOTE 1 Hash functions can be used to detect data corruption.

NOTE 2 Common hash functions include parity, checksum or CRC.

[IEC/TR 62210, modified]

3.1.1.14

hazard

state or set of conditions of a system that, together with other related conditions will inevitably lead to harm to persons, property or environment

3.1.1.15

message

ordered series of octets intended to convey information

[ISO/IEC 2382-16.02.01, modified]

3.1.1.16

message sink

part of a *communication system* in which *messages* are considered to be received

[ISO/IEC 2382-16.02.03]

3.1.1.17

message source

part of a *communication system* from which *messages* are considered to originate

[ISO/IEC 2382-16.02.02]

3.1.1.18

nuisance trip

spurious trip with no harmful effect

NOTE Internal abnormal errors can be caused in communication systems such as wireless transmission, for example by too many retries in the presence of interferences.

3.1.1.19

performance level (PL)

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[ISO 13849-1]

3.1.1.20

redundancy

existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information

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

3.1.1.21

risk

combination of the probability of occurrence of harm and the severity of that harm

NOTE For more discussion on this concept see Annex A of IEC 61508-5:2010.

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

3.1.1.22

safety communication layer (SCL)

communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.1.23

safety data

data transmitted across a safety network using a safety protocol