

DIN EN 61784-3-2

ICS 35.160; 35.240.50

Ersatz für
DIN EN 61784-3-2:2008-11
Siehe Anwendungsbeginn

**Industrielle Kommunikationsnetze - Profile –
Teil 3-2: Funktional sichere Übertragung bei Feldbussen –
Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 2
(IEC 61784-3-2:2010);
Englische Fassung EN 61784-3-2:2010**

Industrial communication networks - Profiles –
Part 3-2: Functional safety fieldbuses –
Additional specifications for CPF 2
(IEC 61784-3-2:2010);
English version EN 61784-3-2:2010

Réseaux de communication industriels –
Partie 3-2: Bus de terrain à sécurité fonctionnelle –
Spécifications complémentaires pour le CPF 2
(CEI 61784-3-2:2010);
Version anglaise EN 61784-3-2:2010

Gesamtumfang 271 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2010-07-01 angenommene Europäische Norm als DIN-Norm ist 2012-03-01.

Für DIN EN 61784-3-2:2008-11 gilt eine Übergangsfrist bis zum 2013-07-01.

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.

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.

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 61784-3-2 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.

Änderungen

Gegenüber DIN EN 61784-3-2:2008-11 wurden folgende Änderungen vorgenommen:

- a) Änderungen, die sich aus der DIN EN 61784-3 (VDE 0803-500):2011-02 ergeben, eingearbeitet;
- b) Hinzufügung oder Änderung der folgenden Unterabschnitte, um das Extended Format zu unterstützen:
6.3.2.1, 6.3.3.4, 6.3.11, 6.6.7.5, 6.8.5.13, 6.8.5.14, 7.1.1, 7.5.5, 7.6.10.10, 7.6.10.12, 8.2, 8.10.2.4.4, 9.5.2;
- c) die gesamten Pseudo Codes in 7.5 so geändert, dass das Extended Format unterstützt wird;
- d) Attribut 15 in 6.7.3.1 hinzugefügt;
- e) die Unterabschnitte 8.11, 8.12 und 8.13 hinzugefügt, um Anforderungen in CP 2/2, CP 2/3 und CP 16/3 klarer formulieren zu können.

Frühere Ausgaben

DIN EN 61784-3-2: 2008-11

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

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]

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

²⁾ Noch zu veröffentlichen.

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]

ANMERKUNG 2 Ein Ausfall kann auf einen *Fehler* zurückzuführen sein (z. B. ein Problem des Hardware-/Software-entwurfs 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 Sicherheitsensors, 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.

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

⁴⁾ In Bearbeitung.

⁵⁾ Noch zu veröffentlichen.

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.

English version

**Industrial communication networks -
Profiles -
Part 3-2: Functional safety fieldbuses -
Additional specifications for CPF 2
(IEC 61784-3-2:2010)**

Réseaux de communication industriels -
Partie 3-2: Bus de terrain à sécurité
fonctionnelle -
Spécifications complémentaires
pour le CPF 2
(CEI 61784-3-2:2010)

Industrielle Kommunikationsnetze -
Profile -
Teil 3-2: Funktional sichere Übertragung
bei Feldbussen -
Zusätzliche Festlegungen
für die Kommunikationsprofilfamilie 2
(IEC 61784-3-2:2010)

This European Standard was approved by CENELEC on 2010-07-01. 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/591A/FDIS, future edition 2 of IEC 61784-3-2, 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 61784-3-2 on 2010-07-01.

This European Standard supersedes EN 61784-3-2:2008.

The main technical changes with respect to EN 61784-3-2:2008 are listed below:

- updates in relation with changes in EN 61784-3;
- addition or modification of the following subclauses to support the Extended Format:
- 6.3.2.1, 6.3.3.4, 6.3.11, 6.6.7.5, 6.8.5.13, 6.8.5.14, 7.1.1, 7.5.5, 7.6.10.10, 7.6.10.12, 8.2, 8.10.2.4.4, 9.5.2;
- modification of all pseudo code in 7.5 to support Extended Format;
- addition of Attribute 15 in 6.7.3.1;
- addition of subclauses 8.11, 8.12 and 8.13 to clarify requirements for CP 2/2, CP 2/3 and CP 16/3 respectively.

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) | 2011-04-01 |
| – latest date by which the national standards conflicting
with the EN have to be withdrawn | (dow) | 2013-07-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61784-3-2:2010 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 61158 series	NOTE	Harmonized in EN 61158 series (not modified).
IEC 61496 series	NOTE	Harmonized in EN 61496 series (partially modified).
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61508-6:2010	NOTE	Harmonized as EN 61508-6:2010 (not modified).
IEC 61511 series	NOTE	Harmonized in EN 61511 series (not modified).
IEC 61784-5 series	NOTE	Harmonized in EN 61784-5 series (not modified).
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.
ISO 12100-1	NOTE	Harmonized as EN ISO 12100-1.
ISO 13849-2	NOTE	Harmonized as EN ISO 13849-2.

CONTENTS

0	Introduction	14
0.1	General	14
0.2	Patent declaration	16
1	Scope	17
2	Normative references	17
3	Terms, definitions, symbols, abbreviated terms and conventions	18
3.1	Terms and definitions	18
3.1.1	Common terms and definitions	19
3.1.2	CPF 2: Additional terms and definitions	23
3.2	Symbols and abbreviated terms	23
3.2.1	Common symbols and abbreviated terms	23
3.2.2	CPF 2: Additional symbols and abbreviated terms	24
3.3	Conventions	25
4	Overview of FSCP 2/1 (CIP Safety™)	25
4.1	General	25
4.2	FSCP 2/1	25
5	General	26
5.1	External documents providing specifications for the profile	26
5.2	Safety functional requirements	27
5.3	Safety measures	27
5.4	Safety communication layer structure	28
5.5	Relationships with FAL (and DLL, PhL)	28
5.5.1	General	28
5.5.2	Data types	28
6	Safety communication layer services	29
6.1	Introduction	29
6.2	Connection object	29
6.2.1	General	29
6.2.2	Class attribute extensions	29
6.2.3	Service extensions	30
6.2.4	Explicit message response format for SafetyOpen and SafetyClose	30
6.3	Connection Manager object	31
6.3.1	General	31
6.3.2	ForwardOpen for safety	31
6.3.3	Safety network segment	33
6.3.4	Originator rules for calculating the connection parameter CRC	36
6.3.5	SafetyOpen processing flowcharts	36
6.3.6	Checks required by Multipoint producers with existing connections	39
6.3.7	Electronic key usage for safety	40
6.3.8	RPI vs. API in safety connections	40
6.3.9	Application path construction for safety	40
6.3.10	Safety Validator connection types	41
6.3.11	Application reply data in a successful SafetyOpen response	43
6.3.12	Unsuccessful SafetyOpen response	45

6.3.13	ForwardClose for safety.....	47
6.4	Identity object.....	48
6.4.1	General.....	48
6.4.2	Changes to common services.....	48
6.5	Link objects.....	48
6.5.1	DeviceNet object changes.....	48
6.5.2	TCP/IP Interface object changes.....	49
6.6	Safety Supervisor object.....	49
6.6.1	General.....	49
6.6.2	Safety Supervisor class attributes.....	50
6.6.3	Subclasses.....	50
6.6.4	Safety Supervisor instance attributes.....	50
6.6.5	Semantics.....	53
6.6.6	Subclasses.....	60
6.6.7	Safety Supervisor common services.....	60
6.6.8	Safety Supervisor behavior.....	71
6.7	Safety Validator object.....	78
6.7.1	General.....	78
6.7.2	Class attributes.....	78
6.7.3	Instance attributes.....	79
6.7.4	Class services.....	84
6.7.5	Instance services.....	85
6.7.6	Object behavior.....	85
6.8	Connection Configuration Object.....	88
6.8.1	General.....	88
6.8.2	Class attribute extensions.....	88
6.8.3	Instance attributes, additions and extensions.....	88
6.8.4	Instance attribute semantics extensions or restrictions for safety.....	90
6.8.5	Special Safety Related Parameters – (Attribute 13).....	95
6.8.6	Object-specific services.....	101
6.8.7	Common service extensions for safety.....	101
6.8.8	Object behavior.....	103
7	Safety communication layer protocol.....	104
7.1	Safety PDU format.....	104
7.1.1	Safety PDU encoding.....	104
7.1.2	Safety CRC.....	116
7.2	Communication protocol behavior.....	117
7.2.1	Sequence of safety checks.....	117
7.2.2	Connection termination.....	117
7.2.3	Cross checking error.....	117
7.3	Time stamp operation.....	118
7.4	Protocol sequence diagrams.....	119
7.4.1	General.....	119
7.4.2	Normal safety transmission.....	119
7.4.3	Lost, corrupted and delayed message transmission.....	120
7.4.4	Lost, corrupted or delayed message transmission with production repeated.....	122
7.4.5	Point-to-point ping.....	124
7.4.6	Multipoint ping on CP 2/3 Safety.....	125

7.4.7	Multipoint ping on CP 2/2 safety networks	127
7.4.8	Multipoint ping – retry with success	127
7.4.9	Multipoint ping – retry with timeout	128
7.5	Safety protocol definition	129
7.5.1	General	129
7.5.2	High level view of a safety device	129
7.5.3	Safety Validator object	129
7.5.4	Relationship between SafetyValidatorServer and SafetyValidatorClient	130
7.5.5	Extended Format time stamp rollover handling	130
7.5.6	SafetyValidatorClient function definition	135
7.5.7	SafetyValidatorServer function definition	143
7.6	Safety message and protocol data specifications	156
7.6.1	Mode octet	156
7.6.2	Time Stamp Section	157
7.6.3	Time Coordination Message	157
7.6.4	Time correction message	157
7.6.5	Safety data production	158
7.6.6	Producer dynamic variables	165
7.6.7	Producer per consumer dynamic variables	167
7.6.8	Consumer data variables	169
7.6.9	Consumer input static variables	171
7.6.10	Consumer dynamic variables	171
8	Safety communication layer management	173
8.1	Overview	173
8.2	Definition of the measures used during connection establishment	174
8.3	Originator-Target relationship validation	177
8.4	Detection of mis-routed connection requests	178
8.5	SafetyOpen processing	178
8.6	Ownership management	179
8.7	Bridging different physical layers	180
8.8	Safety connection establishment	181
8.8.1	Overview	181
8.8.2	Basic facts for connection establishment	181
8.8.3	Configuring safety connections	182
8.8.4	Network time expectation multiplier	183
8.8.5	Establishing connections	185
8.8.6	Recommendations for consumer number allocation	188
8.8.7	Recommendations for connection establishment	189
8.8.8	Ownership establishment	189
8.8.9	Ownership use cases	190
8.8.10	PID/CID usage and establishment	192
8.8.11	Proper PID/CID usage in multipoint and point-to-point connections	193
8.8.12	Network supported services	195
8.8.13	FSCP 2/1 safety device type	196
8.9	Safety configuration process	200
8.9.1	Introduction to safety configuration	200
8.9.2	Configuration goals	200
8.9.3	Configuration overview	201

8.9.4	User configuration guidelines	202
8.9.5	Configuration process SIL3 justification	203
8.9.6	Device functions for tool configuration	204
8.9.7	Password security	204
8.9.8	SNCT interface services	204
8.9.9	Configuration lock	204
8.9.10	Effect of configuration lock on device behavior	205
8.9.11	Configuration ownership	206
8.9.12	Configuration mode	206
8.9.13	Measures used to ensure integrity of configuration process	206
8.9.14	Download process	208
8.9.15	Verification process	211
8.9.16	Verification process	214
8.9.17	Configuration error analysis	215
8.10	Electronic Data Sheets extensions for safety	218
8.10.1	General rules for EDS based safety devices	218
8.10.2	EDS extensions for safety	219
8.11	Requirements for CP 2/2	223
8.11.1	EPI rules for safety messages that travel over CP 2/2	223
8.11.2	Default safety I/O service	223
8.11.3	Duplicate IP detection	223
8.11.4	Priority for safety connections	224
8.12	Requirements for CP 2/3	224
8.12.1	Allocation of CP 2/3 identifiers	224
8.12.2	Additional requirements	226
8.13	CP 16/3 requirements	227
8.13.1	Transport layer requirements	227
8.13.2	Multicast connections	227
8.13.3	CIP Safety and the CP 16/3 device model	227
8.13.4	UNID assignment on CP 16/3	228
9	System requirements	230
9.1	Indicators and switches	230
9.1.1	General indicator requirements	230
9.1.2	LED indications for setting the device UNID	230
9.1.3	Module Status LED	230
9.1.4	Indicator warning	231
9.1.5	Network Status LED	231
9.1.6	Switches	232
9.2	Installation guidelines	235
9.3	Safety function response time	235
9.3.1	Overview	235
9.3.2	Network time expectation	235
9.3.3	Equations for calculating network reaction times	236
9.4	Duration of demands	238
9.5	Constraints for calculation of system characteristics	238
9.5.1	Number of nodes	238
9.5.2	Network PFH	238
9.5.3	Bit Error Rate (BER)	241

9.6 Maintenance	242
9.7 Safety manual	242
10 Assessment	242
Annex A (informative) Additional information for functional safety communication profiles of CPF 2	243
A.1 Hash function example code	243
A.2	257
Annex B (informative) Information for assessment of the functional safety communication profiles of CPF 2	258
Bibliography	259
Annex ZA (normative) Normative references to international publications with their corresponding European publications	262
Table 1 – Communications errors and detection measures matrix	27
Table 2 – New class attributes	29
Table 3 – Service extensions	30
Table 4 – SafetyOpen and SafetyClose response format	30
Table 5 – Safety network segment identifier	33
Table 6 – Safety network segment definition	33
Table 7 – Safety network segment router format	35
Table 8 – Safety Network Segment Extended Format	35
Table 9 – Multipoint producer parameter evaluation rules	40
Table 10 – ForwardOpen setting options for safety connections	42
Table 11 – Network connection parameters for safety connections	43
Table 12 – CP 2/3 Safety target application reply (size: 10 octets)	44
Table 13 – EF CP 2/3 Safety target application reply (size: 14 octets)	44
Table 14 – SafetyOpen target application reply (size: 18 octets)	45
Table 15 – EF SafetyOpen target application reply (size: 22 octets)	45
Table 16 – New and extended error codes for safety	46
Table 17 – SafetyOpen error event guidance table	46
Table 18 – Identity object common service changes	48
Table 19 – New DeviceNet object instance attribute	48
Table 20 – New TCP/IP Interface object Instance Attribute	49
Table 21 – Safety Supervisor class attributes	50
Table 22 – Safety Supervisor instance attributes	50
Table 23 – Device status attribute state values	54
Table 24 – Exception status attribute format	55
Table 25 – Common exception detail attribute values	56
Table 26 – Exception detail format summary	57
Table 27 – Summary of device behavior for various CFUNID values	59
Table 28 – Safety Supervisor common services	61
Table 29 – Safety Supervisor object specific services	61
Table 30 – Configure_Request message structure	63
Table 31 – Validate_Configuration message structure	63
Table 32 – Validate_Configuration success message structure	63

Table 33 – Validate_Configuration error code.....	64
Table 34 – Validate_Configuration extended codes.....	64
Table 35 – Set_Password message structure.....	66
Table 36 – Reset_Password message structure.....	66
Table 37 – Configuration_Lock/Unlock message structure.....	67
Table 38 – Mode_Change message structure.....	67
Table 39 – Safety_Reset message structure.....	67
Table 40 – Safety Supervisor safety reset types.....	68
Table 41 – Attribute bit map parameter.....	68
Table 42 – Reset processing rules for reset types.....	68
Table 43 – Propose_TUNID service.....	69
Table 44 – Apply_TUNID service.....	70
Table 45 – Safety Supervisor events.....	72
Table 46 – State event matrix for Safety Supervisor.....	73
Table 47 – Configuration owner control vs. device state.....	76
Table 48 – State mapping of Safety Supervisor to Identity object.....	77
Table 49 – Safety Supervisor object event mapping.....	77
Table 50 – Identity object event mapping.....	78
Table 51 – Safety Validator class attributes.....	79
Table 52 – Safety Validator instance attributes.....	79
Table 53 – Safety Validator state assignments.....	81
Table 54 – Safety Validator type, bit field assignments.....	82
Table 55 – Multipoint producer SafetyOpen parameter evaluation rules.....	83
Table 56 – Safety Validator class services.....	84
Table 57 – Safety Validator instance services.....	85
Table 58 – Safety Validator Get_Attributes_All service data.....	85
Table 59 – Safety Validator state event matrix.....	87
Table 60 – State mapping between Safety Supervisor and Safety Validator objects.....	87
Table 61 – Connection configuration object class attribute extensions.....	88
Table 62 – Connection Configuration Object instance attribute additions/extensions.....	88
Table 63 – Connection flag bit definitions.....	90
Table 64 – O-to-T connection parameters.....	92
Table 65 – T-to-O connection parameters.....	93
Table 66 – Data map formats.....	94
Table 67 – Data map format 0.....	95
Table 68 – Data map format 1.....	95
Table 69 – Target device's SCCRC values.....	97
Table 70 – Target device's SCTS values.....	98
Table 71 – Time correction connection parameters for multipoint connection.....	98
Table 72 – Format Type attribute meaning.....	99
Table 73 – Format Status attribute meaning.....	100
Table 74 – Connection Configuration Object-specific services.....	101
Table 75 – Get_Attributes_All Response service data (added attributes).....	101

Table 76 – Get_Attributes_All Response service data (added parameters).....	102
Table 77 – Set_Attributes_All Request service data (added attributes)	102
Table 78 – Set_Attributes_All Response service data (added parameters).....	103
Table 79 – State Mapping between Safety Supervisor and the CCO objects.....	103
Table 80 – Connection sections and PDU formats	105
Table 81 – Mode octet variables.....	106
Table 82 – Time Stamp variables	109
Table 83 – Time Coordination message variables	110
Table 84 – Time Correction Message variables.....	112
Table 85 – CRC polynomials used.....	116
Table 86 – Connection sections and message formats.....	117
Table 87 – Data reception - Link triggered.....	146
Table 88 – Time_Correction reception - Link triggered.....	146
Table 89 – Data reception - Application triggered.....	146
Table 90 – Time_Correction reception - Application triggered.....	147
Table 91 – Consuming application – Safety data monitoring.....	147
Table 92 – Producer connection status determination.....	158
Table 93 – Consuming safety connection status.....	169
Table 94 – Connection establishment errors and measures to detect errors.....	174
Table 95 – SNN Date/Time allocations.....	175
Table 96 – SNN legal range of time values.....	175
Table 97 – Safety connection parameters.....	183
Table 98 – SafetyOpen summary.....	186
Table 99 – Originator/Target service mapping.....	197
Table 100 – Unsupported originator/target service types.....	197
Table 101 – Configuration goals.....	201
Table 102 – Configuration owner control vs. device state.....	206
Table 103 – Errors and detection measures.....	215
Table 104 – Parameter class keywords.....	220
Table 105 – New Connection Manager section keywords for safety.....	220
Table 106 – Connection Manager field usage for safety.....	221
Table 107 – Connection parameter field settings for safety	223
Table 108 – CP 2/3 ID assignment rules	224
Table 109 – LED indications for setting UNID	230
Table 110 – Module Status LED	231
Table 111 – Network status LED states.....	231
Table 112 – Connection reaction time type – producing/consuming applications.....	236
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	14
Figure 2 – Relationships of IEC 61784-3 with other standards (process).....	15
Figure 3 – Relationship of Safety Validators	26
Figure 4 – Communication layers	28

Figure 5 – ForwardOpen with safety network segment.....	32
Figure 6 – Safety network target format	34
Figure 7 – Target Processing SafetyOpen with no configuration data (Form 2 SafetyOpen)..	37
Figure 8 – Target Processing for SafetyOpen with configuration data (Form 1 SafetyOpen)..	38
Figure 9 – Originator logic to determine which format to use	39
Figure 10 – Applying device configuration.....	64
Figure 11 – Configure and Validate processing flowcharts	65
Figure 12 – UNID handling during “Waiting for TUNID”	71
Figure 13 – Safety Supervisor state diagram	72
Figure 14 – Configuration, testing and locked relationships.....	76
Figure 15 – Safety connection types.....	82
Figure 16 – Safety Validator state transition diagram.....	86
Figure 17 – Logic for Auto-detecting format type.....	100
Figure 18 – Connection Configuration Object state diagram	103
Figure 19 – Connection Configuration Object data flow.....	104
Figure 20 – Format of the mode octet	105
Figure 21 – 1 or 2 octet data section, Base Format	106
Figure 22 – 1 or 2 octet data section, Extended Format.....	107
Figure 23 – 3 to 250 octet data section format, Base Format.....	107
Figure 24 – 3 to 250 octet data section format, Extended Format	108
Figure 25 – Time Stamp section format, Base Format	109
Figure 26 – BF Time Coordination message encoding	110
Figure 27 – EF Time Coordination message encoding	110
Figure 28 – BF Time Correction message encoding	111
Figure 29 – EF Time Correction message encoding	111
Figure 30 – 1 or 2 octet point-to-point PDU encoding	113
Figure 31 – 1 or 2 Octet multipoint PDU encoding.....	113
Figure 32 – 1 or 2 Octet, multipoint, Format 2 safety connection format	114
Figure 33 – 3 to 250 Octet Point-to-point PDU encoding	114
Figure 34 – 3 to 248 Octet Multipoint PDU encoding	115
Figure 35 – 3 to 248 Octet, Multipoint, safety connection format.....	115
Figure 36 – CRC Calculation order for Extended Format messages	116
Figure 37 – Time stamp sequence.....	118
Figure 38 – Sequence diagram of a normal producer/consumer safety sequence	119
Figure 39 – Sequence diagram of a normal producer/consumer safety sequence (production repeated).....	120
Figure 40 – Sequence diagram of a corrupted producer to consumer message	121
Figure 41 – Sequence diagram of a lost producer to consumer message.....	121
Figure 42 – Sequence diagram of a delayed message.....	122
Figure 43 – Sequence diagram of a corrupted producer to consumer message with production repeated.....	123
Figure 44 – Sequence diagram of a connection terminated due to delays	123
Figure 45 – Sequence diagram of a failure of safety CRC check.....	124

Figure 46 – Sequence diagram of a point-to-point ping - normal response	124
Figure 47 – Sequence diagram of a successful multipoint ping, CP 2/3 safety	126
Figure 48 – Sequence diagram of a successful multipoint ping, CP 2/2 safety	127
Figure 49 – Sequence diagram of a multipoint ping retry	128
Figure 50 – Sequence diagram of a multipoint ping timeout.....	128
Figure 51 – Safety device reference model entity relation diagram.....	129
Figure 52 – Two devices interchanging safety data via a SafetyValidatorClient and a SafetyValidatorServer	130
Figure 53 – Point-to-point, originating consumer. target producer	132
Figure 54 – Point-to-point, originator producer, target consumer.....	133
Figure 55 – Multi-point, originator consumer, target producer	134
Figure 56 – Safety production data flow	135
Figure 57 – Consumer safety data monitoring.....	144
Figure 58 – SafetyValidatorServer - application triggered.....	145
Figure 59 – Target ownership.....	178
Figure 60 – SafetyOpen forms.....	179
Figure 61 – Connection ownership state chart	179
Figure 62 – SafetyOpen UNID mapping.....	180
Figure 63 – Common CPF 2 application layer	180
Figure 64 – End-to-End routing example	181
Figure 65 – Sources for safety related connection parameters.....	184
Figure 66 – Parameter mapping between originator and target	185
Figure 67 – CP 2/3 Safety connection establishment in targets for Form 2a SafetyOpen	187
Figure 68 – General sequence to detect configuration is required	188
Figure 69 – PID/CID exchanges for two originator scenarios	193
Figure 70 – Seed generation for multipoint connections	194
Figure 71 – PID/CID runtime handling.....	195
Figure 72 – Connection categories and supported services.....	198
Figure 73 – Recommended connection types.....	199
Figure 74 – Logic-to-logic supported services.....	199
Figure 75 – Recommended connection types for logic to logic.....	200
Figure 76 – Configuration data transfers	201
Figure 77 – Protection measures in safety devices.....	203
Figure 78 – Configuration, testing and locked relationships.....	205
Figure 79 – Originator's configuration data	207
Figure 80 – SNCT to device download process	209
Figure 81 – SNCT Downloads to originators that perform Form 1 configuration	210
Figure 82 – Protection from locking and ownership.....	212
Figure 83 – Example of read back and comparison of original and printout	213
Figure 84 – Diverse display without full data read back.....	214
Figure 85 – Verification process including all alternatives	214
Figure 86 – CP 16/3 device model.....	227
Figure 87 – Adding a standard module to a modular device.....	229

Figure 88 – Safety device MACID processing logic	234
Figure 89 – Safety function response time.....	235
Figure 90 – Safety function response time components	237
Figure 91 – Network protocol reliability block diagram (RBD)	238
Figure 92 – Network PFH summary	240
Figure 93 – Extended Format PFH summary	241

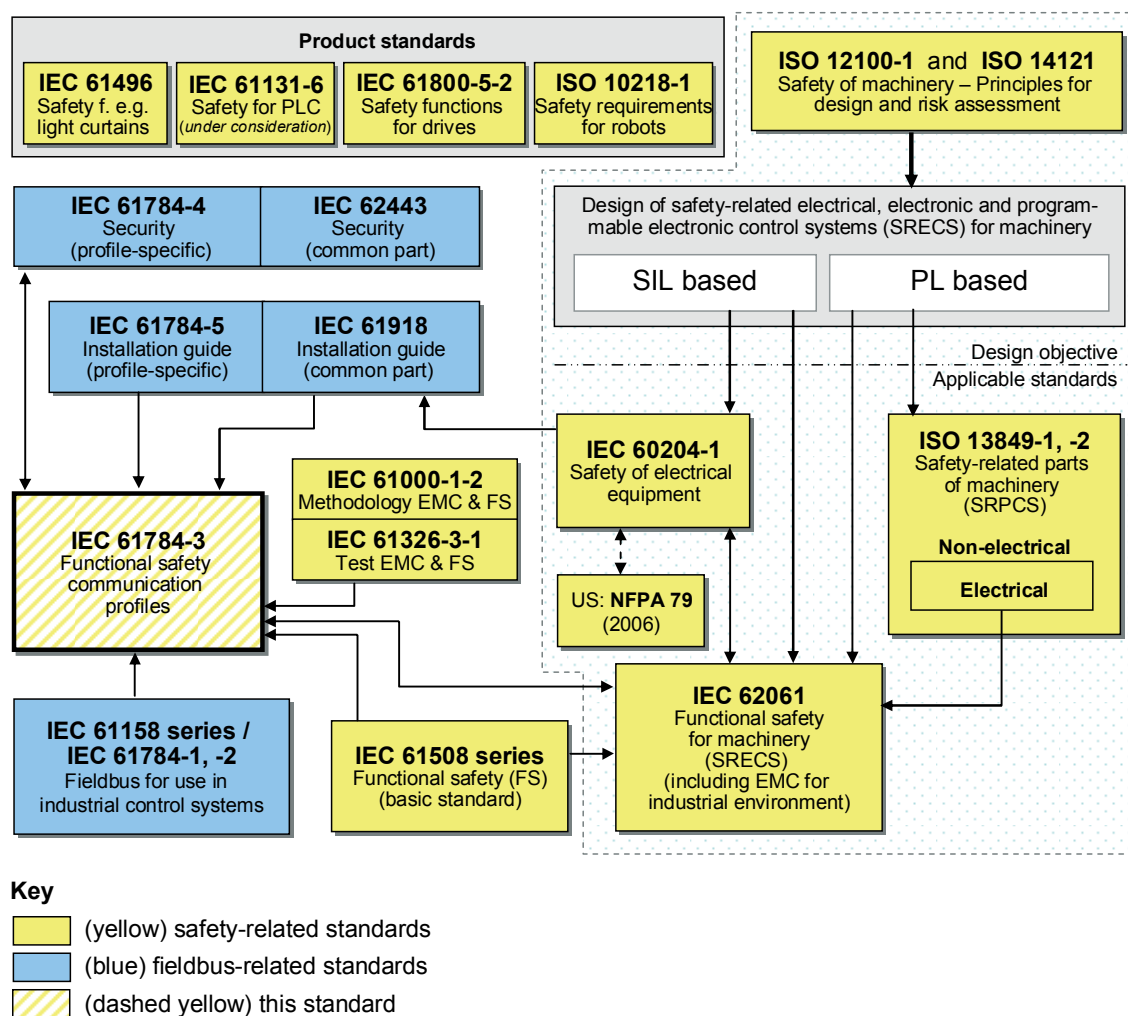
0 Introduction

0.1 General

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

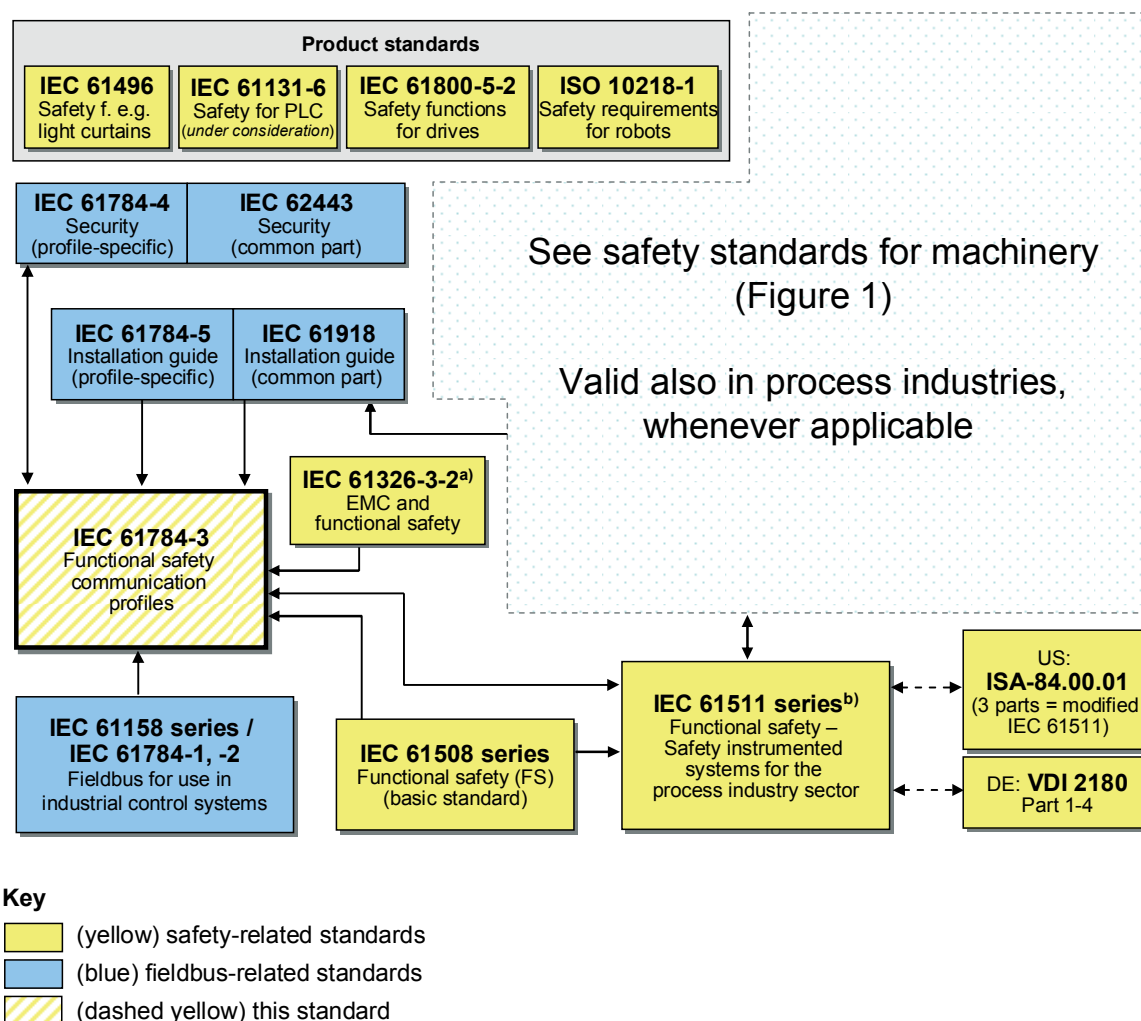
Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of IEC 62061 specify the relationship between PL (Category) and SIL.

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

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 patents concerning the functional safety communication profiles for family 2 as follows, where the [xx] notation indicates the holder of the patent right:

US 6,631,476	[RA]	Safety network for industrial controller providing redundant connections on single media
US 6,701,198	[RA]	Safety network for industrial controller allowing initialization on standard networks
US 6,721,900	[RA]	Safety network for industrial controller having reduced bandwidth requirements
US 6,891,850	[RA]	Network independent safety protocol for industrial controller
US 6,915,444	[RA]	Network independent safety protocol for industrial controller using data manipulation techniques

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[RA] Rockwell Automation, Inc.
1201 S. Second Street
Milwaukee, WI 53204
USA
Attention: Intellectual Property Dept.

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.

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 2 of IEC 61784-1, IEC 61784-2 and IEC 61158 Type 2. 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 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61158-3-2, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition – Type 2 elements*

IEC 61158-4-2, *Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements*

IEC 61158-5-2, *Industrial communication networks – Fieldbus specifications – Part 5-2: Application layer service definition – Type 2 elements*

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 61158-6-2, *Industrial communication networks – Fieldbus specifications – Part 6-2: Application layer protocol specification – Type 2 elements*

IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – General industrial applications*

IEC 61326-3-2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety related functions (functional safety) – Industrial applications with specified electromagnetic environment*

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

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

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

IEC 61784-3:2010³, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61784-5-2, *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses – Installation profiles for CPF 2*

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

IEC 62026-3, *Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) – Part 3: DeviceNet*

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 15745-2:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 2: Reference description for ISO 11898-based control systems*

ISO 15745-3:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 3: Reference description for IEC 61158-based control systems*

ISO 15745-4:2003, *Industrial automation systems and integration – Open systems application integration framework – Part 4: Reference description for Ethernet-based control systems*

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 To be published.

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

bridge

abstract device that connects multiple network segments along the data link layer

3.1.1.4

communication channel

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

3.1.1.5

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

3.1.1.6

connection

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

3.1.1.7

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 [34], [35]⁴.

3.1.1.8

error

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

[IEC 61508-4:2010⁵], [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*.

3.1.1.9

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

⁴ Figures in square brackets refer to the bibliography.

⁵ To be published.

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)

3.1.1.10

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]

3.1.1.11

fieldbus

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

3.1.1.12

frame

denigrated synonym for DLPDU

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

master

active communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

3.1.1.16

message

ordered series of octets intended to convey information
[ISO/IEC 2382-16.02.01, modified]

3.1.1.17

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.

3.1.1.18

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]

3.1.1.19

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

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

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

3.1.1.20

reliability

probability that an automated system can perform a required function under given conditions for a given time interval (t_1, t_2)

NOTE 1 It is generally assumed that the automated system is in a state to perform this required function at the beginning of the time interval.

NOTE 2 The term "reliability" is also used to denote the reliability performance quantified by this probability.

NOTE 3 Within the MTBF or MTTF period of time, the probability that an automated system will perform a required function under given conditions is decreasing.

NOTE 4 Reliability differs from availability.

[IEC 62059-11, 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 61508-5:2010⁶.

[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 connection

connection that utilizes the safety protocol for communications transactions

3.1.1.24

safety data

data transmitted across a safety network using a safety protocol

NOTE The Safety Communication Layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.1.25

safety device

device designed in accordance with IEC 61508 and which implements the functional safety communication profile

⁶ To be published.

3.1.1.26

safety function

function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

NOTE The definition in IEC 61508-4 is the same, with an additional example and reference.

[IEC 61508-4:2010, modified]

3.1.1.27

safety function response time

worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, before the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function channel

NOTE This concept is introduced in IEC 61784-3:2010⁷, 5.2.4 and addressed by the functional safety communication profiles defined in this part.

3.1.1.28

safety integrity level (SIL)

discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010⁸.

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SILn safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

[IEC 61508-4:2010]

3.1.1.29

safety measure

<this standard> measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

NOTE 1 In practice, several safety measures are combined to achieve the required safety integrity level.

NOTE 2 Communication *errors* and related safety measures are detailed in IEC 61784-3:2010, 5.3 and 5.4.

3.1.1.30

safety-related application

programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.1.31

safety-related system

system performing *safety functions* according to IEC 61508

3.1.1.32

slave

passive communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave

⁷ In preparation.

⁸ To be published.

3.1.1.33

spurious trip

trip caused by the safety system without a process demand

3.1.1.34

time stamp

time information included in a *message*

3.1.2 CPF 2: Additional terms and definitions

3.1.2.1

base format

format used for connection RPIs of less than 100 ms or for applications where dropped connections can be tolerated

3.1.2.2

extended format

format used for connection RPIs of more than 100 ms or for applications where there is a need to avoid dropped connections

3.1.2.3

ping

request for the consumer to acknowledge the reception of a message

3.1.2.4

ping response

response to a ping

3.1.2.5

signature

method of uniquely identifying a set of data

NOTE This could be by revision, checksum or some other method that is agreed upon by the originating and target devices.

3.2 Symbols and abbreviated terms

3.2.1 Common symbols and abbreviated terms

CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5]
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]

PFD	Probability of dangerous Failure on Demand	[IEC 61508-6:2010 ⁹]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-6:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4:2010]

3.2.2 CPF 2: Additional symbols and abbreviated terms

AIRS	Already In Requested Mode/State
BER	Bit Error Rate
BF	Base Format
CCO	Connection Configuration Object
CFUNID	Configuration UNID
CNP	Connection Point
CID	Consumer ID
CIP™ 10	Common Industrial Protocol (application framework shared among CPF 2 communication profiles)
CPCRC	Connection Parameter CRC
CTM	Connection Timeout Multiplier
EDS	Electronic Data Sheet
EF	Extended Format
EPI	Expected Packet Interval
LED	Light Emitting Diode
MACID	Device physical address (CP 2/3) or IP Address (CP 2/2) on network
MOD	Module
NV	Non-Volatile
NVS	Non-Volatile Storage
OCPUNID	Output Connection Owner UNID
OSC	Object State Conflict
O-to-T	Originator to Target
OUNID	Originator UNID
PID	Producer Identifier
PS	Power Supply
Res.	Reserved
RPI	Requested Packet Interval
SCCRC	Safety Configuration Data CRC
SCID	Safety Configuration Identified
SCTS	Safety Configuration Time Stamp
SNCT	Safety Network Configuration Tool
SNN	Safety Network Number
T-to-O	Target to Originator

⁹ To be published.

¹⁰ For trade name declaration, see Clause 4.

TBD	To Be Defined	
TNS	TUNID Not Set	
TUNID	Target UNID	
UML	Universal Modeling Language	[ISO/IEC 19501]
UNID	Unique Network Identifier	

3.3 Conventions

The conventions used for the descriptions of objects services and protocols are described in IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

As appropriate this part uses flow charts, UML Sequence Diagrams and “C” pseudo-code to describe concepts.

4 Overview of FSCP 2/1 (CIP Safety™)

4.1 General

Communication Profile Family 2 (commonly known as CIP™¹¹) defines communication profiles based on IEC 61158-2 Type 2, IEC 61158-3-2, IEC 61158-4-2, IEC 61158-5-2, and IEC 61158-6-2.

The basic profiles CP 2/1, CP 2/2, and CP 2/3 are defined in IEC 61784-1 and IEC 61784-2. The CPF 2 functional safety communication profile FSCP 2/1 (CIP Safety™¹¹) is based on the CPF 2 basic profiles in IEC 61784-1 and IEC 61784-2 and the safety communication layer specifications defined in this part.

4.2 FSCP 2/1

FSCP 2/1 is based on the producer/consumer model of CPF 2. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for safety-related applications.

The FSCP 2/1 safety communication layer is specified using a Safety Validator object. This object is responsible for managing the FSCP 2/1 safety connections and serves as the interface between the safety-related application objects and the link layer connections, as shown in Figure 3. The Safety Validator ensures the integrity of the safety data transfers.

¹¹ CIP™ (Common Industrial Protocol) and CIP Safety™ are trade names of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade names CIP™ or CIP Safety™. Use of the trade names CIP™ or CIP Safety™ requires permission of ODVA.

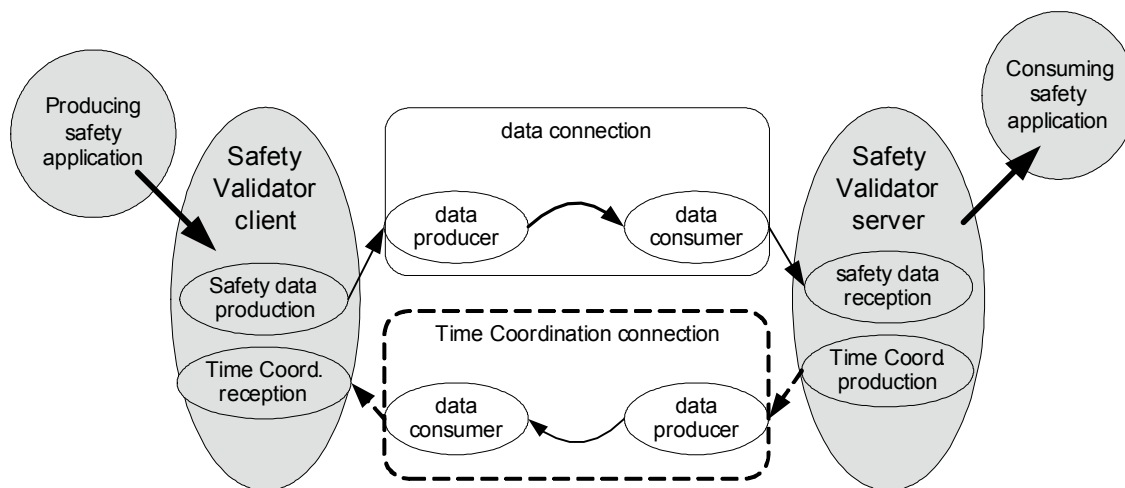


Figure 3 – Relationship of Safety Validators

The integrity of the safety data transfers is ensured as follows:

- the producing safety-related application uses an instance of a client Safety Validator to produce safety data and ensure time coordination;
- the client uses a link data producer to transmit the data and a link consumer to receive time coordination messages;
- the consuming safety-related application uses a server Safety Validator to receive and check data;
- the server uses a link consumer to receive data and a link producer to transmit time coordination messages.

FSCP 2/1 utilizes the black channel concept. The link producers and consumers have no knowledge of the safety packet and implement no safety function. The responsibility for high-integrity transfer and checking of safety data lies within the Safety Validators.

FSCP 2/1 uses the following measures to ensure the integrity of safety messaging:

- time stamp;
- connection authentication;
- data integrity assurance;
- redundancy with cross checking;
- different data integrity assurance systems.

Messages are produced with a timestamp that allows the consumer to verify the age of data being sent. Identification is encoded into each safety-related message to ensure that the correct consumer is using the message. All safety-related messages use a unique CRC. Safety-related data is sent redundantly. Diverse measures for producing safety-related messages are used to ensure that standard CPF 2 messages are not interpreted as safety messages.

5 General

5.1 External documents providing specifications for the profile

The following document is especially useful in understanding the design of FSCP 2/1 protocols:

- GS-ET-26 [33]

5.2 Safety functional requirements

The following requirements shall apply to the development of devices that implement the FSCP 2/1 protocol. The same requirements were used in the development of FSCP 2/1.

- The FSCP 2/1 protocol is designed to support Safety Integrity Level 3 (SIL3) (see IEC 61508), and PLe/category 4 (see ISO 13849-1).
- The safety state for discrete data is the unenergized state (0). For analog values the unenergized state shall be defined by the safety-related application.
- The basic requirements for the development of the FSCP 2/1 protocol are in IEC 61784-3.
- FSCP 2/1 protocol is implemented using a black channel approach; there is no safety related dependency on the standard CPF 2 communication profiles.
- Implementations of FSCP 2/1 shall comply with IEC 61508.
- Environmental conditions shall be according to IEC 61131-2 for the basic levels and IEC 61326-3-1, IEC 61326-3-2 for the safety margin tests, unless there are specific product standards.
- Safety communication and standard communication shall be independent. However, standard devices and safety devices shall be able to use the same communication channel.
- Unless specified in this part, the CPF 2 requirements shall be unchanged for safety.

5.3 Safety measures

Table 1 contains the measures used to detect communication errors and the coverage provided by each measure as used.

Table 1 – Communications errors and detection measures matrix

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance systems
Corruption						X	X	
Unintended repetition		X				X ^a	(X) ^e	
Incorrect sequence		X				X ^a	(X) ^e	
Loss			X ^c			X ^a	(X) ^e	
Unacceptable delay		(X) ^e	X					
Insertion		X ^d		X		X ^a	(X) ^e	
Masquerade		X ^d		X		X ^b	X ^f	X
Addressing				X		X ^b		
^a The safety related CRC provides additional protection for communication errors in messages. ^b Encoding the unique identifier into the safety related CRC prevent masquerade and addressing errors. ^c A message not received within the time expectation will be detected. ^d Masquerade or inserted messages will not have the expected time stamp. ^e Not claimed for FSCP 2/1. ^f Masquerade will likely not have redundant data and will fail the cross-check.								

5.4 Safety communication layer structure

The safety protocol is layered on top of the standard network protocol (the standard protocol stack is a black channel). Figure 4 shows how the safety communication layer is related to the existing CPF 2 layers.

The safety layers accept safety data from the safety-related application circuit. The safety layers then formulate a safety message, transmit the safety message, receive and decode the safety message. Once the safety message is decoded and verified, the data is presented to the receiving safety-related application circuit.

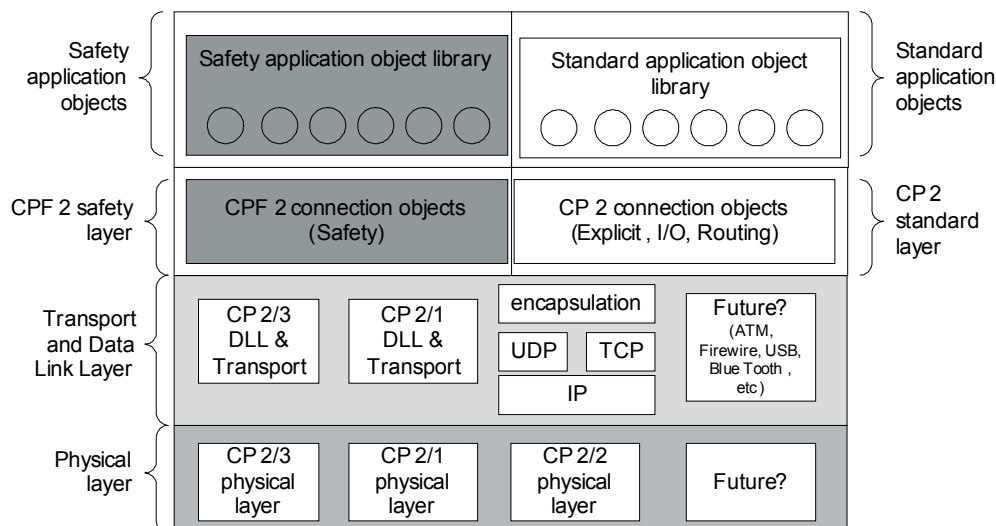


Figure 4 – Communication layers

5.5 Relationships with FAL (and DLL, PhL)

5.5.1 General

This safety communication layer shall only be used in conjunction with CPF 2 communication profiles (CP 2/3 (DeviceNet™¹²), CP 2/2 (EtherNet/IP™¹³)). There are no requirements of CPF 2 communications profiles other than those defined in this part.

5.5.2 Data types

Profiles defined in this part support all the CPF 2 data types as defined in IEC 61158-5-2.

¹² DeviceNet™ is a trade name of the non-profit organization ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade name DeviceNet™. Use of the trade name DeviceNet™ requires permission of ODVA.

¹³ EtherNet/IP™ is a trade name of ODVA, Inc. This information is given for the convenience of users of this International Standard and does not constitute an endorsement by IEC of the trade name holder or any of its products. Compliance to this part does not require use of the trade name EtherNet/IP™. Use of the trade name EtherNet/IP™ requires permission of ODVA.

6 Safety communication layer services

6.1 Introduction

This subclause defines the extensions to existing CPF 2 objects and new objects for Safety. Safety connections use Class 0 connections for I/O messages. Standard Explicit message connections are used for the establishment of Safety I/O connections.

6.2 Connection object

6.2.1 General

Several safety specific class attributes and services are defined to support safety. Safety nodes which reside on FSCP 2/1 shall implement the SafetyOpen and SafetyClose services of the Connection object.

6.2.2 Class attribute extensions

Table 2 defines the class attributes used by safety devices.

Table 2 – New class attributes

Attrib ID	Need in implementation	Access rule	N V	Name	Date type	Description of attribute
8	Optional	Get	V	Connection request error count	UINT	Diagnostic Counter that is a running count of SafetyOpen or SafetyClose faults ^a
9	Optional	Get	V	Safety connection counters	STRUCT of:	Status counters
				SafetyOpen request success count	UINT	Count of successful SafetyOpen requests issued from this node to another target
				SafetyOpen request failure count	UINT	Count of unsuccessful SafetyOpen requests issued from this node to another target
				SafetyClose request success count	UINT	Count of successful SafetyClose requests issued from this node to another target
				SafetyClose request failure count ^b	UINT	Count of unsuccessful SafetyClose requests issued from this node to another target
				SafetyOpen indication success count	UINT	Count of successful SafetyOpen requests issued from an external originator to this node
				SafetyOpen indication failure count ^b	UINT	Count of unsuccessful SafetyOpen requests issued from an external originator to this node
				SafetyClose indication success count	UINT	Count of successful SafetyClose requests issued from an external originator to this node
				SafetyClose indication failure count ^b	UINT	Count of unsuccessful SafetyClose requests issued from an external originator to this node

^a Attribute 8 is the sum of the 4 failure counters in attribute 9. Having this single attribute represent connection errors can be used in monitoring software to efficiently monitor errors without polling the additional attribute 9 structures. Once attribute 8 is non-zero then the monitoring software can examine attribute 9 for more details.

^b Included in class attribute 8.

6.2.3 Service extensions

Table 3 defines services for use by safety devices on FSCP 2/1. These services shall be supported by a target device on FSCP 2/1. The SafetyOpen and SafetyClose services, used in lieu of the ForwardOpen and ForwardClose services of the Connection Manager object, inherit the identical behavior from those Connection Manager services.

Table 3 – Service extensions

Service code	Need in implementation		Service name	Description of service
	Class	Instance		
4D _{hex}	Optional	N/A	Reset Counters	This service resets class attributes 8 and 9 to zero
4E _{hex}	Required	N/A	SafetyClose	Used to close a Safety I/O connection. See the ForwardClose service of the Connection Manager object 6.3.13
54 _{hex}	Required	N/A	SafetyOpen ^a	Used to establish a safety I/O connection. See the ForwardOpen service of the Connection Manager object 6.3.2
^a The SafetyOpen service data shall contain a Safety Network Segment in the Connection_Path field.				

6.2.4 Explicit message response format for SafetyOpen and SafetyClose

The SafetyOpen and SafetyClose service responses have a common response format. This format contains status information for both success and failure. If the service response is a success, response data specific to each service is returned. If the service response is an error, a successful FSCP 2/1 status indicated by the general error code FF_{hex} is returned, along with a variable amount of extended error information.

The response format for the SafetyOpen and SafetyClose object Specific services are defined in Table 4:

Table 4 – SafetyOpen and SafetyClose response format

Parameter name	Data type	Description of response parameter
Reserved	USINT	Reserved
General status	USINT	One of the general status codes listed in IEC 61158-6-2 (status codes)
Size of additional status	USINT	Number of 16 bit words in Additional status array
Additional status	ARRAY of UINT	Additional status
Response data	ARRAY of OCTET	Response data from request or additional error data if general status indicated an error

The Response Data and General/Additional Statuses for the SafetyOpen and SafetyClose services shall match the Response Data and General/Additional Statuses for the ForwardOpen and ForwardClose services of the Connection Manager object, respectively.

6.3 Connection Manager object

6.3.1 General

Safety devices shall use a ForwardOpen with a Safety Network Segment to establish safety connections. This segment uniquely identifies the ForwardOpen service as a safety ForwardOpen. Throughout this subclause, the term "SafetyOpen" shall refer to both the ForwardOpen service of the Connection Manager object (when containing a Safety Network Segment) and the SafetyOpen service of the Connection object.

6.3.2 ForwardOpen for safety

6.3.2.1 ForwardOpen for safety contents

The contents of the ForwardOpen service of the Connection Manager object, including the safety network segment, are outlined in Figure 5 below. The proper settings for the various parameters in the ForwardOpen are given in Figure 5.

Parameter Name		Data Type / Size	Target Destination and Semantics
Priority/Time_tick		OCTET	Connection manager servicing request
Time-out_ticks		USINT	Connection manager servicing request
O-to-T Network Connection ID		UDINT	Consuming connection instance:: CIP consumed connection ID
T-to-O Network Connection ID		UDINT	Producing connection instance:: CIP producing connection ID
Connection Serial Number		UINT	Value: Unique (to originator) 16-bit number. Destination: Connection manager servicing request
Originator Vendor ID		UINT	Connection manager servicing request
Originator Serial Number		UDINT	Connection manager servicing request
Connection Timeout Multiplier		USINT	Producing and consuming connection instance: Timeout Multiplier
Reserved		3 OCTETS	
O-to-T RPI		UDINT	Consuming connection instance: EPR
O-to-T Network Connection Parameters	Redundant Owner	WORD	Value: 0 (Safety Connections do not support redundancy); Destination: Connection Manager
	Connection Type		Value: Point-to-point; Destination: Connection Manager
	Priority		Value: High Priority; Destination: Connection Manager
	Fixed/Variable		Value: Fixed; Destination: Connection Manager
	Connection Size (in octets)		Value: Size of safety PDU including the Mode Octet, Actual, Complement, and Time stamp sections Destination: Consuming connection instance: Consumed connection size attribute
T-to-O RPI		UDINT	Producing connection instance: EPR
T to O Network Connection Parameters	Redundant Owner	WORD	Value: 0 (Safety connections do not support redundancy); Destination: Connection Manager
	Connection Type		Value: Point-to-point; Destination: Connection Manager
	Priority		Value: High Priority; Destination: Connection Manager
	Fixed/Variable		Value: Fixed; Destination: Connection Manager

Parameter Name		Data Type / Size	Target Destination and Semantics
	Connection Size (in octets)		Value: Size of safety PDU including the Mode Octet, Actual, Complement, and Time stamp sections. Destination: Producing Connection Instance: Produced connection size
Transport Type/Trigger		SWORD	Value: Safety single or multipoint. Destination: Validator instance. Trigger always set to Application. Client/Server: depending on direction
Connection_Path_Size		USINT	Number of 16 bit words in the Connection_Path field – destination is Connection Manager servicing request. NOTE Value included in CRC calculation does not include the words used for Network/Port segments.
Connection_Path (Padded EPATH)	Path		Variable
	Logical Segment: Electronic Key	Vendor ID	UINT
		Prod Type	UINT
		Prod Code	UINT
		Compatible/ Major Rev	SWORD
		Minor Rev	USINT
	Application Path 1	Logical Segment: Class	Variable; 1 word typically
		Logical Segment: Instance	Variable; 1 word typically
	Application Path 2	Logical Segment: Connection Point	Variable; 1 word typically
	Application Path 3	Logical Segment: Connection Point	Variable; 1 word typically
	Config Data	Data Segment: Simple Data	Variable
	Network Segment:	Safety Segment Name	50 _{hex}
		Segment Size	USINT
		Segment Format	USINT
		Network Safety Data	ARRAY of OCTET

Key



= Connection/Safety Validator fields covered by Connection Parameters CRC

= Configuration Data Segment covered by SCCV

Figure 5 – ForwardOpen with safety network segment

6.3.2.2 ForwardOpen for safety for Extended Format

Safety Originators that support the Extended Format may connect to Targets with RPI's of 100 ms or less with either the Extended Format (EF) or the Base Format (BF).

Safety Originators that connect with a CP 2/2 target or a CP 2/3 target with a CP 2/2 hop within the path and have an RPI of greater than 100 ms shall use the Extended Format.

A variety of methods may be used to assure this. EDS files and configuration software can pre-configure the choice, or the originator can use a dynamic algorithm to make the determinations.

The mechanism used by the originator to indicate to a target that the Extended Format is being requested will be with a new Safety Network Segment Format as defined in 6.3.3.

6.3.3 Safety network segment

6.3.3.1 Common format

The Safety Connection Parameters Segment Type has been added to the CPF 2 Network Segment definition as segment type 10_{hex} (resulting in a segment value of 50_{hex}). The updated Network Segment definition is defined in Table 5.

Table 5 – Safety network segment identifier

Network segment type	Network segment name
50 _{hex}	Safety segment

The format of the Safety Network Segment is defined in Table 6. This segment type is in the range of Network Segment types, which contains a data size field. The Safety Segment Format parameter, the first parameter in the data area, indicates which data follows.

Table 6 – Safety network segment definition

Octet offset	Field name	Data type	description
0	Segment Type	SWORD	Indicates Safety Network Segment (50 _{hex})
1	Network Segment data length	SWORD	Length of segment data to follow (in words)
2	Safety Network Segment format	USINT	Indicates type of Safety Network Segment 0 = Target format 1 = Router format 2 – 255 = Reserved
3 - n	Safety Network Segment data	ARRAY of OCTET	Safety Network Segment data, defined by segment format

6.3.3.2 Safety network segment: target format (00_{hex})

The target format is directed at the target of the connection. The value of the Network Segment Data Length parameter shall be 27 (1b_{hex}) which corresponds to 27 WORDS. Figure 6 defines the safety network target format.

Field name	Data type	Description
Reserved	SWORD	Pad
Configuration CRC (SCCRC)	UDINT	CRC-S4 of target Config Data Segment. A value of 0 is an indicator that SCID check can be skipped
Configuration Time Stamp (SCTS)	DATE_AND_TIME	Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction Connection Instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. When not used: 0 (Null). When used: Fixed, High Priority, Multipoint
Target_UNID (TUNID)	STRUCT of: 10 OCTETS	UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Originator UNID (OUNID)	STRUCT of: 10 OCTETS	UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Ping_Interval_EPI_Multiplier	UINT	Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.6.5.10
Time_Coord_Msg_Min_Multiplier	UINT	For Producing Connection Instance. Valid range is 0 to 7 813
Network_Time_Expectation_Multiplier	UINT	For Consuming Connection Instance. Valid range is 0 to 42 969
Timeout_Multiplier	USINT	Used by producer and consumer to timeout connections. Valid range 1 to 4
Max_Consumer_Number	USINT	Value: 1 (Point-to-point), 2-15(Multipoint)
Connection Parameters CRC (CPCRC)	UDINT	CRC-S4 of target connection parameters in this request
Time Correction Connection ID	UDINT	Not Used: FFFFFFFF _{hex} When used: Time Correction Connection Instance:: Connection ID

Key

 = Safety Segment fields covered by Connection Parameters CRC

Figure 6 – Safety network target format

6.3.3.3 Safety network segment: router format (01_{hex})

The router format is directed at an intermediate router along the connection path when that router needs to know this is a Safety ForwardOpen. Currently, only CP 2/3 routers need this network segment directed to them. The Network Segment is applied to the subnet from which the connection request originated. Router Format Safety Network Segments only appear in the Path portion of the Connection_Path of a Safety ForwardOpen. The total segment length is 6 words. The safety network segment router format is defined in Table 7.

Table 7 – Safety network segment router format

Field name	Data type	Description
Reserved	SWORD	Reserved, value = 0
Time Correction Connection ID	UDINT	Not Used: FFFFFFFF _{hex} When used: Time Correction connection instance:: Connection ID
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction connection instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. Not used: 0 (Null). When used: Fixed, High Priority, Multipoint

6.3.3.4 Safety network segment: Extended Format (0x02)

The Extended Format is directed at the target of the connection and shown in Table 8.

All EF safety connections shall be established using the EF safety network segment in a Forward Open (CP 2/2) or a SafetyOpen (CP 2/3).

Table 8 – Safety Network Segment Extended Format

Field Name	Data Type	Description
Reserved	octet	Pad
Configuration CRC (SCCRC)	UDINT	CRC-S32 of target Config Data Segment. A value of 0 is an indicator that SCID check can be skipped
Configuration TimeStamp (SCTS)	DATE_AND_TIME	Time and Date stamp of the configuration. A value of 0 is an indicator that SCID check can be skipped. 6 octet value (Date: 2 octets, Time: 4 octets)
Time Correction EPI	UDINT	Not used: 0 When used: Time Correction Connection Instance:: EPI
Time Correction Network Connection Parameters	WORD	Network Connection Parameters for the Time Correction connection. This field uses the same definition as the Network Connection Parameter within the Connection Manager object. When not used: 0 (Null). When used: Fixed, High Priority, Multipoint
Target_UNID (TUNID)	STRUCT of: UINT 10: octets	UNID of the target device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Originator UNID (OUNID)	STRUCT of: UINT 10: octets	UNID of the Originator device. This value is a 10 octet value consisting of the Safety Network Id (6 octets) and the Node Address (4 octet address)
Ping_Interval_EPI_Multiplier	UINT	Number that defines the Ping_Count_Interval for the connection. Valid range of values is given in 7.6.5.10
Time_Coord_Msg_Min_Multiplier	UINT	For Producing Connection Instance. Valid range is 0 to 7 813

Field Name	Data Type	Description
Network_Time_Expectation_Multiplier	UINT	For Consuming Connection Instance. Valid range is 0 to 42 969
Timeout_Multiplier	USINT	Used by producer and consumer to timeout connections. Valid range of 1 to 255 for HiAvailabilityFormat
Max_Consumer_Number	USINT	Value: 1 (Point to point), 2-15(Multipoint)
Max_Fault_Number	UINT	Used by both producers and consumers to determine how many erroneous packets can be dropped before a connection shall be closed. Default = 5. A value of 0 indicates connections shall be closed on any detected error
Connection Parameters CRC (CPCRC)	UDINT	CRC-S32 of target connection parameters in this request
Time Correction Connection ID1	UDINT	Not Used: 0xFFFFFFFF When used: Time Correction Connection Instance:: Connection ID
Initial Time Stamp1	UINT	Used by Consumer to initialize Last_Time_Stamp_for_Rollover. Consuming Originator sets to 0xFFFF
Initial Rollover Value1	UINT	Used by Consumer to initialize TS_Rollover_Count. Consuming Originator sets to 0xFFFF
^a These fields are NOT included in the CPCRC.		

6.3.4 Originator rules for calculating the connection parameter CRC

The Connection Parameter CRC (CPCRC) is only calculated when a connection is initially configured or when that connection configuration is changed. This value remains static in the originator otherwise.

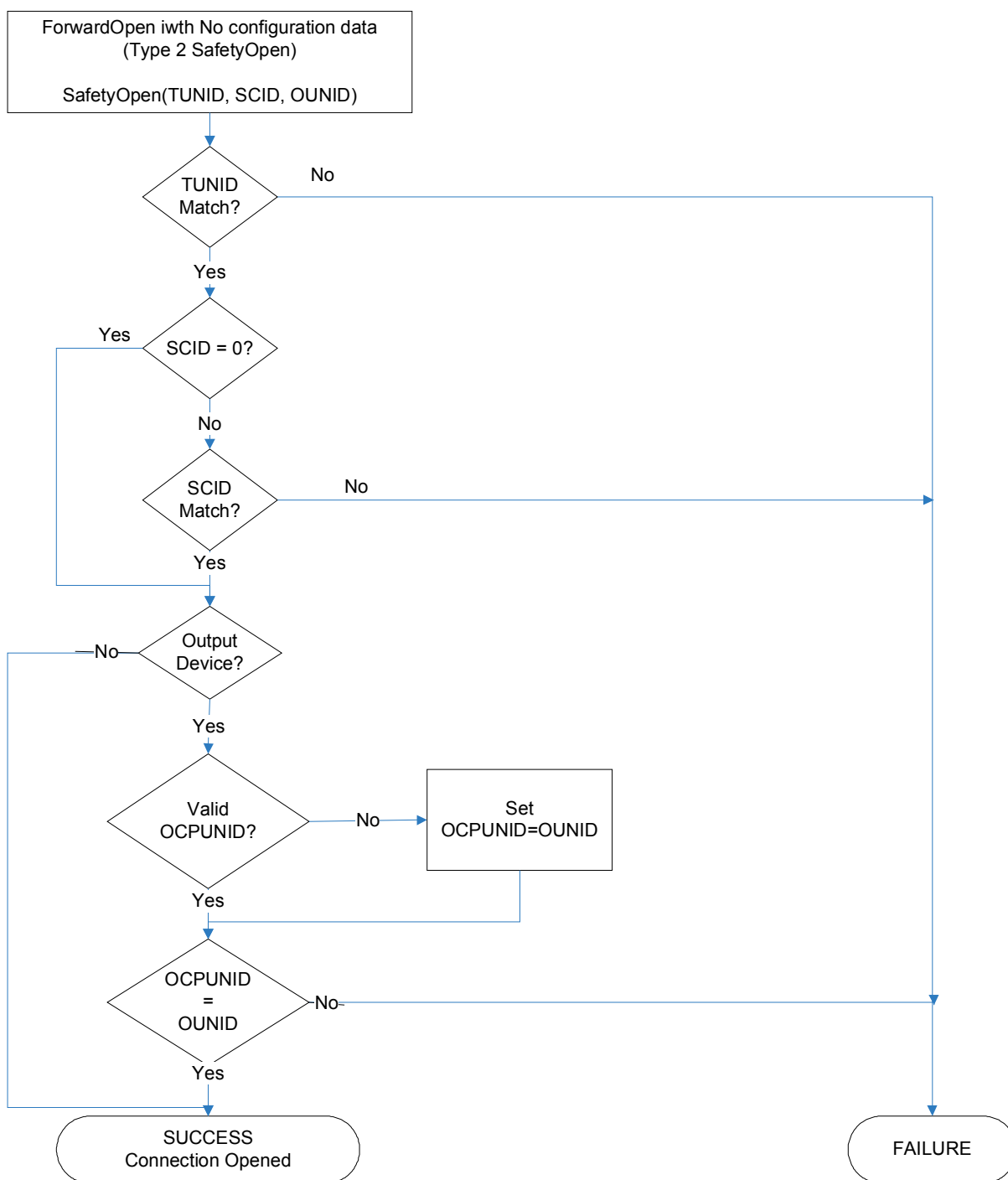
The connection path size in the SafetyOpen changes value depending on whether an originator is sending configuration data or not. Since this field is included in the CPCRC calculation, originators need to calculate and maintain two values when they support the SafetyOpen configuration function. One value is used when configuring a device while opening the connection and the other value is used when just opening the connection (no configuration data is included).

Also, the path size shall be “pre-adjusted” to remove the path entries that get stripped off by routers as the Safety ForwardOpen traverses each sub-net. The requirement is that the originator is responsible for calculating the CPCRC value based on what the SafetyOpen or ForwardOpen will be when the target receives it so that the target can perform a simple calculation in all cases.

6.3.5 SafetyOpen processing flowcharts

The following flowcharts outline the required behavior of a target upon receipt of a SafetyOpen:

- Verify the Connection Parameter CRC. As depicted in Figure 6, the connection parameter CRC covers the SafetyOpen fields that will be used by the target. Routers along the path shall not modify these fields;
- The target checks that the electronic key segment matches (see 6.3.7);
- Depending on the type of safety connection, the logic is defined in Figure 7 or Figure 8 shall be followed.

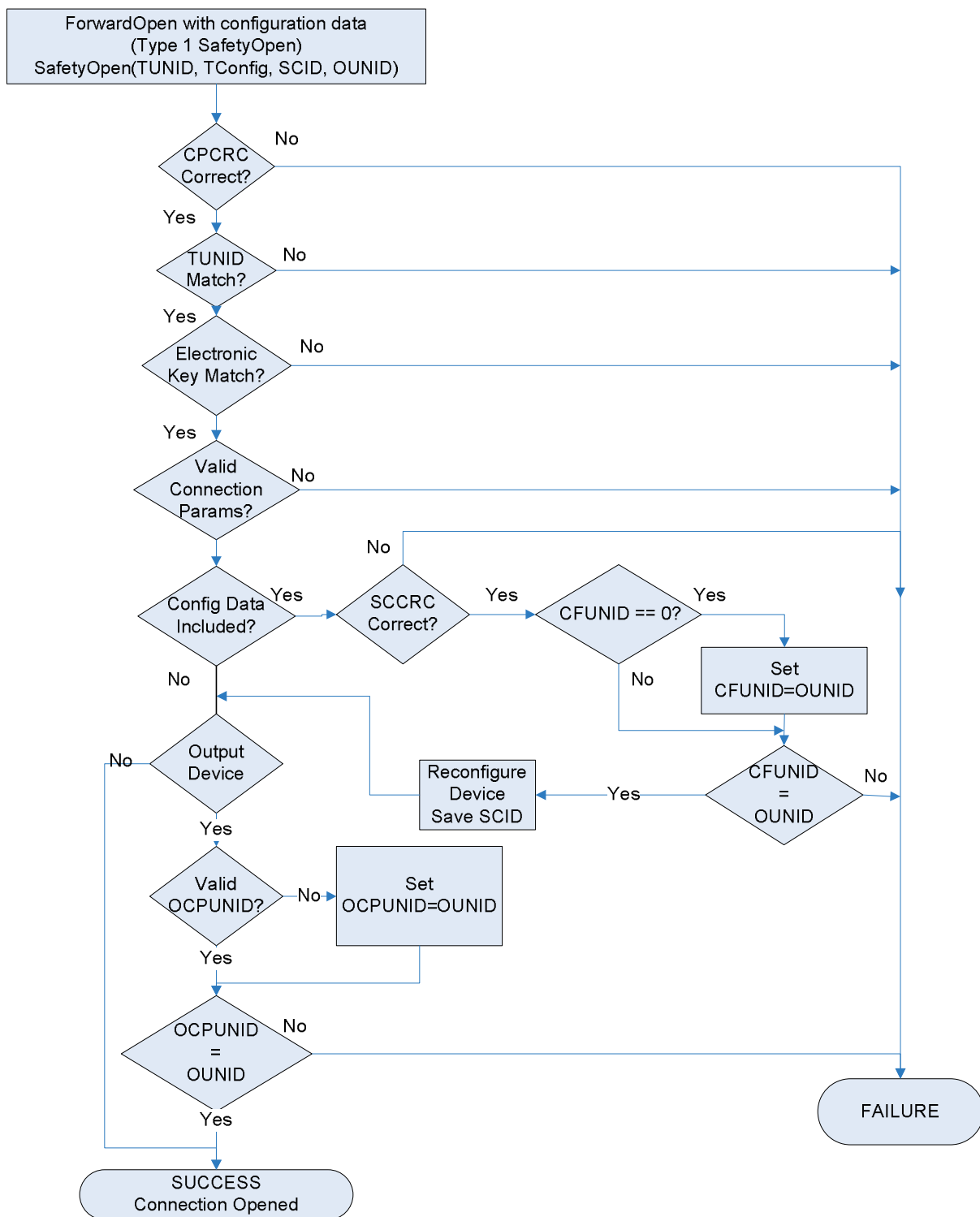


Key:

UNID = Unique Network Identifier
SCID = Target's Safety Configuration ID
OCP = Output Connection Point
CFUNID = Configuration Owning UNID

TUNID = Target's Unique Network Identifier
OUNID = Originator's Unique Network Identifier
OCPUNID = Output Connection Owning UNID

**Figure 7 – Target Processing SafetyOpen with no configuration data
(Form 2 SafetyOpen)**



Key:

UNID = Unique Network Identifier
CPCRC = Connection Parameter CRC
SCCRC = CRC portion of the SCID
OCPUNID = Output Connection Owning UNID

TUNID = Target's Unique Network Identifier
SCID = Target's Safety Configuration ID
OUNID = Originator's Unique Network Identifier
CFUNID = Configuration Owning UNID

**Figure 8 – Target Processing for SafetyOpen with configuration data
(Form 1 SafetyOpen)**

Safety Originators that do not support any other means to determine which format to connect with can implement the logic shown in Figure 9 to dynamically determine the format.

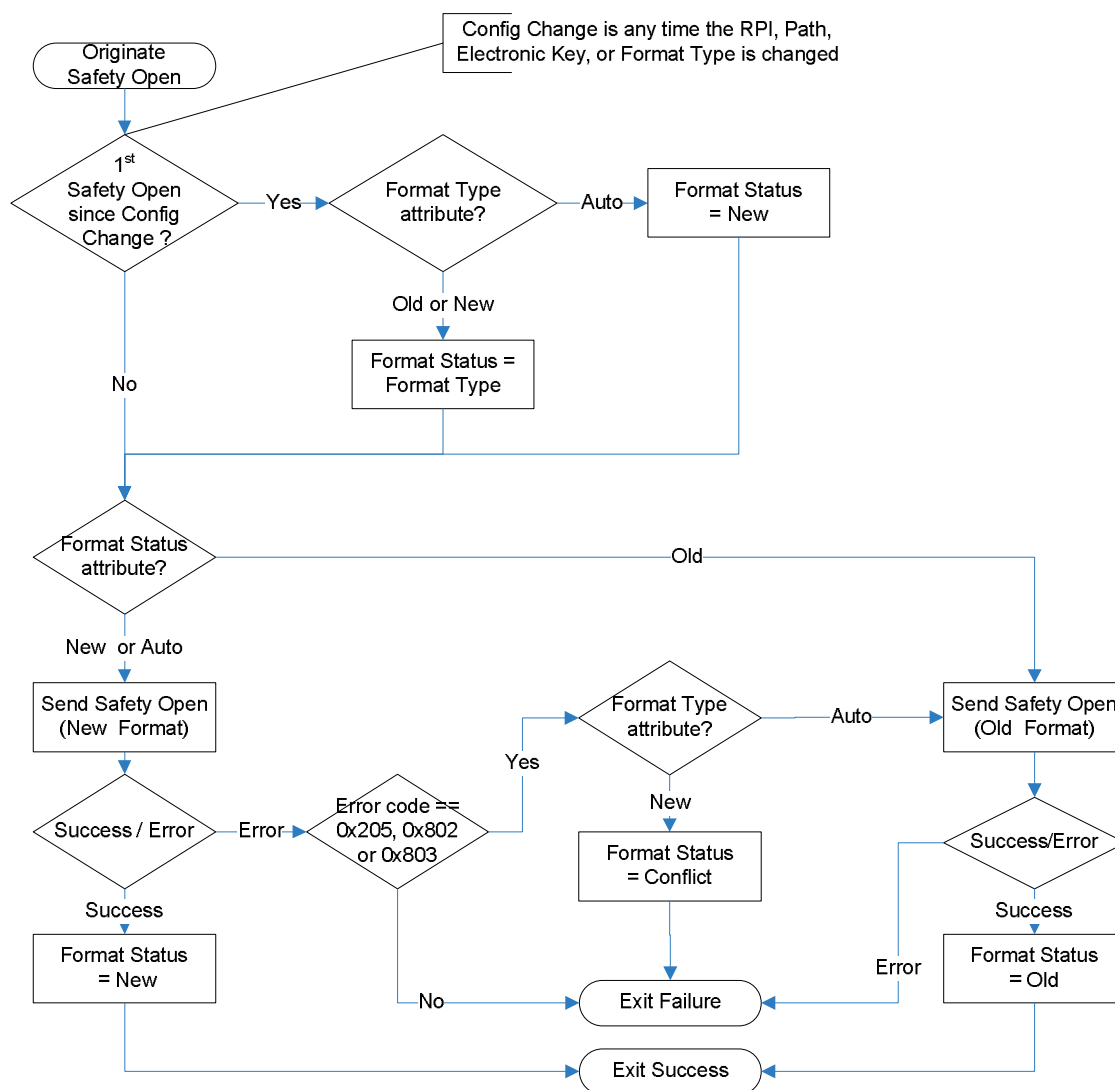


Figure 9 – Originator logic to determine which format to use

6.3.6 Checks required by Multipoint producers with existing connections

There is a distinct possibility that the safety parameters used in a ForwardOpen or SafetyOpen from various consuming originators will not always be the same. A consistent set of rules shall be used for how a Multipoint producing target evaluates these parameters when they conflict with other already established consuming connections. Table 9 defines the multipoint producer parameter evaluation rules.

Table 9 – Multipoint producer parameter evaluation rules

Safety parameter	Producer evaluation rule if connection exists	Error response ^a (if appropriate)	
		General	Extended
Ping_Interval EPI Multiplier	Shall match existing P.I.E.M.	01 _{hex} 00 _{hex}	0801 _{hex} 0012 _{hex}
Time Coord Msg Min Multiplier	Accept any (all can be different)	N/A	
Network Time Expectation Multiplier	Accept any (all can be different)	N/A	
Timeout_Multiplier	Accept any (all can be different)	N/A	
Max_Consumer_Number	Shall match existing Max_Consumer_Number	00 _{hex} 01 _{hex}	0801 _{hex} 002A _{hex}
T-to-O RPI, O-to-T RPI, and Time Correction RPI	Shall match existing connection RPIs	01 _{hex}	0111 _{hex}
Network Segment Type	Shall match existing connection format ^b	0x01	0x803
Max_Fault_Number	Accept any (all can be different)	N/A	
^a At the option of the device developer, another connection could also be opened rather than return an error response.			
^b Subsequent connection requests on an existing multi-point connection shall all be the same format as the existing connection			

6.3.7 Electronic key usage for safety

Safety originators and targets shall meet the following requirements for use of the Electronic Key segment within a SafetyOpen.

The Electronic Key segment shall be present in all SafetyOpen or Safety ForwardOpen service requests.

The Electronic Key shall always be processed by Target devices with integrity (cannot be confirmed externally).

The compatibility bit and behavior in the Electronic Key shall be supported as defined by safety originators and targets. Wildcards (fields set to 0) for individual fields within the Electronic Key shall not be supported.

6.3.8 RPI vs. API in safety connections

Safety devices do not have the ability to negotiate the RPI value. Safety Targets either accept the requested RPI because it can be supported, or it rejects it completely. The tolerance around an acceptable RPI request shall be $\pm 128 \mu\text{s}$.

The T-to-O API, O-to-T API, and Time Correction API in a success response shall always be the same value received in the SafetyOpen.

6.3.9 Application path construction for safety

IEC 61158-6-2 defines a method to construct an application path in a SafetyOpen for 3 references: one for configuration, one for consumed data and one for produced data.

The possible path types are identified as follows:

A. - [Class] [Assembly] [Instance] [Configuration-instance]

- B. - [Class] [Assembly] [Instance] [Producer-instance]
- C. - [Class] [Assembly] [Instance] [Consumer-instance]
- D. - [Class] [Assembly] [Instance] [Device-defined NULL instance)]
- E. - [CNP] [Consumer CNP]
- F. - [CNP] [Producer CNP]
- G. - [CNP] [Device-defined NULL CNP]

When all 3 paths referenced the same class, they are often formatted in a compressed format: (CP stands for Connection Point).

[Class] [Class #] [Instance] [Instance #] [CNP] [Consumer CP] [CNP] [Producer CNP]

Since all three paths shall reference the same class, a NULL instance value shall be reserved in that class (by the device developers) to use the compressed form for safety. The NULL value will be used for the portion of the path that references the Time Coordination connection and configuration connection (in non-configuring originators). If a common class reference is not practical, the long form shall be used.

The following rules apply to SafetyOpen path construction:

- all devices shall support the long form at a minimum;
- a Null path or Null connection point shall be used to represent the Time Coordination connection;
- a Null path or Null connection point shall be used for the configuration path when no configuration data can ever be sent on the connection;
- on any connections, which can accept a Form 1 SafetyOpen, Originators shall always send a valid configuration path even if no configuration data is present (i.e. Form 2a).

The "Null" path or connection point used shall be one of the module's choosing. The method of making this selection in an EDS file will be via the Data Path field in the Connection Manager section. Devices configured by configuration applet also shall provide this path.

Safety device designers can choose the path format to specify in their EDS files from the following options. The possible three-path combinations for Form 1, 2a SafetyOpen on connections, which will accept configuration are:

- [A, D, B] for the input connection;
- [A, G, F] compressed format for input connections;
- [A, C, D] for the output connection;
- [A, E, G] compressed format for output connections.

The possible three-path combinations for Form 2a, 2b SafetyOpen on connections, which will not accept configuration data are:

- [D, D, B] for the input connection;
- [D, G, F] compressed format for input connections;
- [D, C, D] for the output connection;
- [D, E, G] compressed format for output connections.

6.3.10 Safety Validator connection types

The Safety Validator function, depending on the safety connection type provided in the SafetyOpen, will always require between 2-3 connection resources. The SafetyOpen contains the connection

information to allow a target to set up these connections appropriately. This subclause will show how the connection types are determined by how the SafetyOpen shall be filled out.

One basic assumption is that connections for Time Coordination and Time Correction messages do not require a path entry since they have an implied path to the Safety Validator object coordinating the safety connection. The various connection scenarios are described in the Validator object in 6.7.

The Safety Validator function can determine which connection resources will be required by looking at the parameter in the SafetyOpen. The various SafetyOpen parameters as well as the key parameters that the safety function will need to determine the types of connections are defined in Table 10. Connection object instances may not be available due to target identifier capacity or limitations; there may be no unallocated connection identifiers. Or the device may not have the processing throughput to handle the additional connection; etc. Safety Connection objects requires resources similar to standard I/O connections.

Table 10 – ForwardOpen setting options for safety connections

O-to-T connection type	T-to-O connection type	Transport type/ trigger	App path 1	App path 2 ^a	App path 3 ^a	Max consumer number	Safety Validator connection type	Key decision factors	Target role
Point-to-point	Point-to-point	Application, Class 0, Client	Vendor defined Null Path ^b	Vendor defined Null Path	Safety Input App. object	1	Point-to-point Producer (Input)	2-point-to-point + Client	Producing connection: Safety data Consumer connection: Coordination
Point-to-point	Point-to-point	Application, Class 0, Server	Vendor defined Null Path	Safety Output App. object	Vendor defined Null Path	1	Point-to-point Consumer (Output)	2- point-to-point + Server	Consuming connection: Safety data Producing connection: coordination
Point-to-point	Multipoint	Application, Class 0, Client	Vendor defined Null Path	Vendor defined Null Path	Safety Input App. object	2-15	Multipoint Producer CP 2/3	2 – Multipoint + 1 point-to-point + Client	Producing connection: Safety data Producing connection: Correction Consuming connection: coordination
Point-to-point	Multipoint	Application, Class 0, Client	Vendor defined Null Path	Vendor defined Null Path	Safety input app. object	2-15	Multipoint Producer CP 2/2	1 – Multipoint + 1 point-to-point + Client	Producing connection: Safety data + correction Consuming connection: coordination