

DIN EN IEC 61139-2

ICS 35.240.50

Einsprüche bis 2023-05-03

Entwurf

**Industrielle Netzwerke –
Digitale Single-Drop-Kommunikationsschnittstelle –
Teil 2: Erweiterungen für die funktionale Sicherheit
(IEC 61139-2:2022);
Englische Fassung EN IEC 61139-2:2022**

Industrial networks –
Single-drop digital communication interface –
Part 2: Functional safety extensions
(IEC 61139-2:2022);
English version EN IEC 61139-2:2022

Réseaux industriels –
Interface de communication numérique point à point –
Partie 2: Extensions de sécurité fonctionnelle
(IEC 61139-2:2022);
Version anglaise EN IEC 61139-2:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-03-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Merianstraße 28, 63069 Offenbach am Main.

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

Gesamtumfang 211 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

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

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Die enthaltene IEC-Publikation wurde vom IEC/SC 65C "Industrial networks" erarbeitet und unterliegt dem Copyright der IEC .

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

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

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

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

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten 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 den vorliegenden Norm-Entwurf erfüllt.

Da sich die Benutzer des vorliegenden Norm-Entwurfs der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN IEC 61139-2 veröffentlicht. Zu deren Einleitung, Abschnitt 1, der den Anwendungsbereich festlegt, und Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Norm-Entwurfs hinzugefügt. Für einige der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Norm-Entwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

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

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung

Reihenfolge und Inhalt der folgenden Abschnitte sind identisch mit denen in den jeweiligen Abschnitten der Englischen Fassung.

Einleitung

Die Basistechnologie von IO-Link™¹ ist Gegenstand der Internationalen Norm IEC 61131-9, die zu einer Normenreihe für programmierbare Steuerungen und die zugehörige Peripherie wie Remote I/O (RIO) gehört.

Es legt eine Schnittstelle für die digitale Kommunikation über eine Punkt-zu-Punkt-Verbindung (en: single-drop digital communication interface, SDCI) fest, die die herkömmlichen Schalteingangs- und -ausgangsschnittstellen, wie sie in IEC 61131-2 definiert sind, um eine Punkt-zu-Punkt-Kommunikationsverbindung mit kodiertem Schalten erweitert. Diese Technologie ermöglicht den zyklischen Austausch von digitalen Eingangs- und Ausgangsprozessdaten zwischen einem Master und seinen zugehörigen Geräten (Sensoren, Aktoren, E/A-Klemmen usw.). Der Master kann Teil eines Feldbus-Kommunikationssystems oder eine eigenständige Verarbeitungseinheit sein. Die Technologie ermöglicht auch die azyklische Übertragung von Parametern an Geräte und die Weitergabe von Diagnoseinformationen von den Geräten an das übergeordnete Automatisierungssystem (Steuerung, Host) über den Master.

Die physische Topologie ist eine Punkt-zu-Punkt-Topologie, wobei jedes Gerät über 3 Adern und Entfernungen von bis zu 20 m mit dem Master verbunden ist. Die physische SDCI-Schnittstelle ist abwärtskompatibel mit der üblichen 24-V-E/A-Signalübertragung nach IEC 61131-2 und unterstützt drei Datenübertragungsraten von 4,8 kbit/s, 38,4 kbit/s und 230,4 kbit/s.

Die Hauptvorteile der SDCI-Technologie sind folgende:

- die wahlweise Verwendung sowohl von Schaltsignalen (DI/DO) als auch von Kommunikation mit kodiertem Schalten;
- herkömmlich schaltende Sensoren und Aktoren bieten nun alternativ eine digitale Kommunikation über eine Punkt-zu-Punkt-Verbindung (SDCI) innerhalb desselben Geräts;
- ein einziges dünnes, robustes, sehr flexibles Kabel ohne Abschirmung für Stromversorgung und Signalübertragung;
- kostengünstigste digitale Kommunikation selbst für die einfachsten Sensoren und Aktoren.

Die funktional sichere SDCI-Variante wird „SDCI-FS“ genannt. Figure 1 zeigt ein Beispiel für die Positionierung von SDCI-FS in der funktional sicheren Automatisierung.

¹ IO-Link™ ist ein Handelsname der „IO-Link-Community“. Diese Angabe dient nur der Unterrichtung der Anwender dieser Spezifikation und bedeutet keine Anerkennung des Inhabers des Handelsnamens oder eines seiner Produkte durch die IO-Link-Community. Die Übereinstimmung mit diesem Dokument erfordert nicht die Verwendung der eingetragenen Logos für IO-Link™. Die Verwendung der eingetragenen Logos für IO-Link™ erfordert die Genehmigung der „IO-Link Community“.

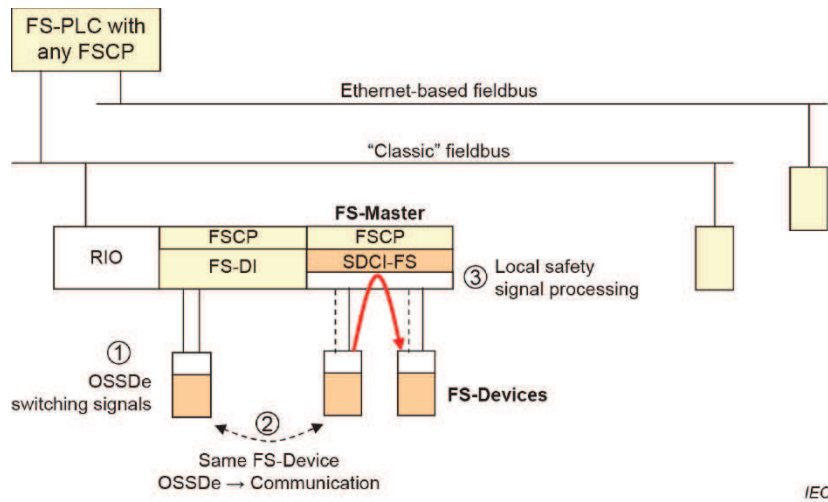


Bild 1 – Positionierung von SDCI-FS in der funktional sicheren Automatisierung

EN	DE
FS-PLC with any FSCP	FS-SPS mit beliebigem FSCP
Ethernet-based fieldbus	Ethernet-basierter Feldbus
"Classic" fieldbus	„Herkömmlicher“ Feldbus
FS-Master	FS-Master
RIO	RIO
FSCP	FSCP
FS-DI	FS-DI
SDCI-FS	SDCI-FS
OSSDe switching signals	OSSDe-Schaltersignale
Same FS-Device OSSDe → Communication	Selbes FS-Device OSSDe → Kommunikation
Local safety signal processing	Lokale sicherheitsbezogene Signalverarbeitung
FS-Devices	FS-Devices

In diesem Beispiel wird ein Remote-I/O-Gerät über eines der funktional sicheren Kommunikationsprofile (en: functional safety communication profile, FSCP) nach der Normenreihe IEC 61784-3 [1]² an eine funktional sichere programmierbare Steuerung angeschlossen, um anhand eines FS-DI-Moduls und eines Gateways mit einem FS-Master mit SDCI-FS zu kommunizieren. FS-Devices mit Schaltausgängen (en: output signal switching device, OSSD) (hier OSSDe nach Dokument „IO-Link Safety System Extensions with SMI“ von IO-Link-Community) können an FS-DIs oder FS-Master angeschlossen werden. Alle FS-Devices können mit jedem FS-Master kommunizieren, der das SDCI-FS-Protokoll verwendet, unabhängig vom übergeordneten FSCP-System. Das Gleiche gilt für sicherheitsbezogene Aktoren (FS-Devices) wie z. B. Antriebe mit integrierter Sicherheit. Dies ist die größte Gemeinsamkeit ① der Komponenten für Sensoren und Aktoren, ähnlich wie bei den in IEC 61131-2 genormten DI- und DO-Schnittstellen.

Sicherheitssensoren mit OSSDe-Schnittstellen mit SDCI-FS-Kommunikation können über Hilfsmittel wie „USB-Master“ parametrisiert und anschließend an einen funktional sicheren Digitaleingang (FS-DI) angeschlossen und im OSSDe-Modus betrieben werden. Sie können auch im OSSDe-Modus an einem FS-Master betrieben werden, der OSSDe unterstützt. Sind diese Sicherheitssensoren zusätzlich mit SDCI-FS-Kommunikation ausgestattet, können sie in beiden Modi ② betrieben werden, entweder OSSDe oder SDCI-FS. Dies entspricht dem SDCI-Standard E/A(SIO)-Paradigma.

Das Konzept von SDCI-FS ermöglicht eine lokale sicherheitsbezogene Signalverarbeitung, wenn das Gateway/der FS-Master eine lokale Sicherheitssteuerung ③ bereitstellt.

² Nummern in eckigen Klammern beziehen sich auf die Literaturhinweise.

Dieses Dokument enthält die notwendigen Erweiterungen zu IEC 61131-9 für die funktional sichere Kommunikation, einschließlich der Standardisierung von OSSDe und der Parametrierung im Bereich der Sicherheit von Maschinen. Figure 2 zeigt die Beziehungen dieses Dokuments zu internationalen Feldbus- und Sicherheitsnormen sowie zu relevanten Spezifikationen (siehe Abschnitt 2 und Literaturhinweise). Funktionale Sicherheit beginnt stets mit der Risikobeurteilung und Risikominderung (ISO 12100). Eine Möglichkeit der Risikominderung ist der Einsatz elektrischer oder elektronischer Steuerungssysteme. Für die Auslegung dieser Systeme können Normen wie IEC 61508, IEC 62061 und ISO 13849 verwendet werden. Umgebungsbedingungen, z. B. hinsichtlich der elektromagnetischen Verträglichkeit (EMV), werden in IEC 61000-6-7 beschrieben. Weitere Aspekte sind die Installation und Sicherheitsfragen. Eine Reihe von Produktnormen wie IEC 60947-5-3 und ISO 14119 ergänzen die allgemeinen Normen oder Branchennormen.

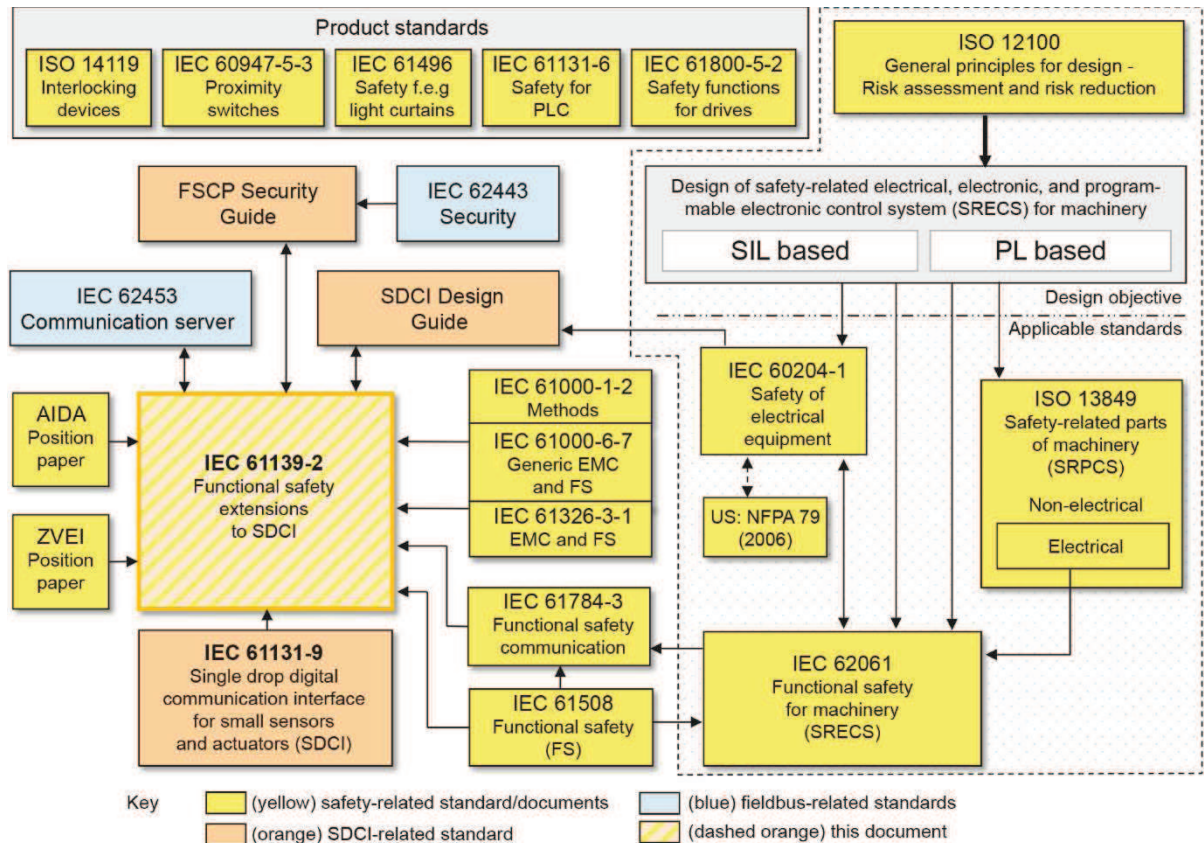


Bild 2 – Beziehung dieses Dokuments zu anderen Normen

EN	DE
Product standards	Produktnormen
ISO 14119	ISO 14119
Interlocking devices	Verriegelungseinrichtungen
IEC 60947-5-3	IEC 60947-5-3
Proximity switches	Näherungsschalter
IEC 61496	IEC 61496
Safety f.e.g light curtains	Sicherheit z. B. für Lichtvorhänge
IEC 61131-6	IEC 61131-6
Safety for PLC	Sicherheit für SPS
IEC 61800-5-2	IEC 61800-5-2
Safety functions for drives	Sicherheitsfunktionen für Antriebe
IEC 62443	IEC 62443
Security	IT-Sicherheit
FSCP Security Guide	Leitfaden für IT-Sicherheit von FSCP
IEC 62453	IEC 62453
Communication server	Kommunikationsserver
SDCI Design Guide	Leitfaden für Auslegung von SDCI
AIDA	AIDA

Position paper	Positionspapier
ZVEI	ZVEI
IEC 61139-2 Functional safety extensions to SDCI	IEC 61139-2 Erweiterungen von SDCI um funktionale Sicherheit
IEC 61131-9 Single drop digital communication interface for small sensors and actuators (SDCI)	IEC 61131-9 Schnittstelle für die Kommunikation mit kleinen Sensoren und Aktoren über eine Punkt-zu-Punkt-Verbindung
IEC 61000-1-2 Methods	IEC 61000-1-2 Verfahren
IEC 61000-6-7 Generic EMC and FS	IEC 61000-6-7 Allgemeines zu EMV und FS
IEC 61326-3-1 EMC and FS	IEC 61326-3-1 EMV und FS
IEC 61784-3 Functional safety communication	IEC 61784-3 Funktional sichere Kommunikation
IEC 61508 Functional safety (FS)	IEC 61508 Funktionale Sicherheit (FS)
ISO 12100 General principles for design - Risk assessment and risk reduction	ISO 12100 Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
Design of safety-related electrical, electronic, and programmable electronic control system (SRECS) for machinery	Auslegung von sicherheitsbezogenen elektrischen, elektronischen und programmierbaren elektronischen Steuerungssystemen (SRE/CS) für Maschinen
SIL based	SIL-basiert
PL based	PL-basiert
Design objective	Auslegungsziel
Applicable standards	Geltende Normen
IEC 60204-1 Safety of electrical equipment	IEC 60204-1 Sicherheit von elektrischer Ausrüstung
US: NFPA 79 (2006)	USA: NFPA 79 (2006)
ISO 13849 Safety-related parts of machinery (SRPCS)	ISO 13849 Sicherheitsbezogene Teile von Steuerungen (SRP/CS)
Non-electrical	Nicht elektrisch
Electrical	Elektrisch
IEC 62061 Functional safety for machinery (SRECS)	IEC 62061 Funktionale Sicherheit von Maschinen (SRE/CS)
Key	Legende
(yellow) safety-related standard/documents	(Gelb) sicherheitsbezogene Normen/Dokumente
(orange) SDCI-related standard	(Orange) SDCI-bezogene Normen
(blue) fieldbus-related standards	(Blau) feldbusbezogene Normen
(dashed orange) this document	(Orange gestrichelt) dieses Dokument

SDCI-FS kann für funktional sichere Anwendungen nach IEC 62061 und IEC 61508 bis zu SIL3 und/oder nach ISO 13849 bis zu PLe verwendet werden.

1 Anwendungsbereich

Dieser Teil von IEC 61139 legt die Erweiterung der Schnittstelle für die digitale Kommunikation über eine Punkt-zu-Punkt-Verbindung (SDCI, en: single-drop digital communication interface) nach IEC 61131-9 um die funktionale Sicherheit fest. Dies umfasst Folgendes:

- eine standardisierte OSSDe-Schnittstelle für redundante Schaltsignale nach IEC 61131-2;
- geringfügige Änderungen/Erweiterungen der SDCI-Zustandsautomaten zur Unterstützung der Sicherheitsfunktionen;

- ein schlankes funktionales Sicherheitskommunikationsprotokoll, das auf der Standard-SDCI-Kommunikation aufbaut und einen schwarzen Kanal nach IEC 61784-3:2021 darstellt;
- Protokollverwaltungsfunktionen für die Konfiguration, Parametrierung und Inbetriebnahme;
- Erweiterungen der IO-Link-Gerätebeschreibung (IODD, en: IO-Link device description) für die funktionale Sicherheit;
- eine Gerätetool-Schnittstelle (DTI, en: device tool interface) zur Unterstützung von dedizierten Tools nach den Normen für funktionale Sicherheit.

Dieses Dokument gilt nicht für:

- Kommunikationsschnittstellen oder -systeme mit Mehrpunktverbindungen;
- Kommunikationsschnittstellen oder -systeme mit mehrkanaligen oder verschlüsselten Verbindungen;
- drahtlose Kommunikationsschnittstellen oder -systeme;
- die Integration von SDCI-FS in übergeordnete Systeme wie Feldbusse/FSCPs.

3 Begriffe, Symbole, Abkürzungen und Konventionen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 61131-1 und IEC 61131-2. ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

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

3.2 Allgemeine Begriffe

3.2.1

Adresse

Teil der M-Sequenzsteuerung zur Referenzierung von Daten innerhalb von Datenkategorien eines Kommunikationskanals

3.2.2

Anwendungsschicht

AL, en: application layer

<SDCI>³ Teil des Protokolls, der für die Übertragung von Prozessdatenobjekten und Bedarfsdatenobjekten verantwortlich ist

3.2.3

Blockparameter

einheitlicher Zugriff auf Parameter über mehrere Indizes oder Subindizes

3.2.4

Prüfsumme

<SDCI> ergänzender Teil der übergreifenden Maßnahmen zur Datenintegrität in der Sicherungsschicht zusätzlich zum UART-Paritätsbit

3.2.5

kodiertes Schalten

SDCI-Kommunikation auf der Grundlage der in IEC 61131-2 festgelegten standardmäßigen Binärsignalpegel

³ In eckigen Klammern ist die Gültigkeit der Definition für die SDCI-Technologie angegeben.

3.2.6

COM1

SDCI-Kommunikationsmodus mit einer Datenübertragungsrate von 4,8 kbit/s

3.2.7

COM2

SDCI-Kommunikationsmodus mit einer Datenübertragungsrate von 38,4 kbit/s

3.2.8

COM3

SDCI-Kommunikationsmodus mit einer Datenübertragungsrate von 230,4 kbit/s

3.2.9

COMx

einer der drei möglichen SDCI-Kommunikationsmodi „COM1“, „COM2“ oder „COM3“

3.2.10

Kommunikationskanal

logische Verbindung zwischen Master und Device

Anmerkung 1 zum Begriff: Es sind vier Kommunikationskanäle definiert: Prozesskanal, Page- und ISDU-Kanal (für Parameter) und Diagnosekanal.

3.2.11

Kommunikationsfehler

unerwartete Störung des SDCI-Übertragungsprotokolls

3.2.12

Zykluszeit

Zeit zur Übertragung einer M-Sequenz zwischen einem Master und seinem Device einschließlich der anschließenden Leerlaufzeit

3.2.13

Device

einzelner passiver Peer zu einem Master, wie ein Sensor oder ein Aktor

Anmerkung 1 zum Begriff: Wird „Device“ verwendet, so bezieht sich der Begriff auf SDCI-Einrichtungen, während „Gerät“ sich auf Geräte im Allgemeinen bezieht.

3.2.14

Direkt-Parameter

direkt (Page-)adressierte Parameter, die azyklisch ohne Quittierung über den Page-Kommunikationskanal übertragen werden

3.2.15

dynamischer Parameter

zu den statischen Parametern zusätzlicher Teil des Parametersatzes eines Devices, der durch Device-seitige Benutzerschnittstellen, wie Teach-in-Tasten oder Bedienfelder, festgelegt ist

3.2.16

Ereignis

Instanz einer Änderung von Zuständen in einem Device

Anmerkung 1 zum Begriff: Wird „Event“ verwendet, so bezieht sich der Begriff auf SDCI-Ereignisse, während „Ereignis“ allgemein verwendet wird.

Anmerkung 2 zum Begriff: Ein Event wird innerhalb der zyklischen Statusinformationen des Devices über das Event-Flag angezeigt, anschließend erfolgt die azyklische Übertragung von Event-Daten (typischerweise Diagnose-Informationen) über den Diagnose-Kommunikationskanal.

3.2.17

Fallback

Übergang eines Ports vom Modus „Kodiertes Schalten“ in den Schaltsignalmodus

3.2.18

ISDU

indexierte Dienstdateneinheit (en: indexed service data unit) für die bestätigte azyklische Übertragung von Parametern, die in eine Reihe von M-Sequenzen segmentiert werden können

3.2.19

M-Sequenz

Folge von zwei Nachrichten, die eine Master-Nachricht und die darauffolgende Device-Nachricht umfasst

3.2.20

M-Sequenzsteuerung

erstes Oktett in einer Master-Nachricht, das die Lese-/Schreib-Operation, den Typ des Kommunikationskanals und die Adresse angibt, z. B. Offset- oder Flusssteuerung

3.2.21

M-Sequenztyp

ein bestimmtes Format von M-Sequenzen aus einem Satz von festgelegten Formaten für M-Sequenzen

3.2.22

Master

aktiver Peer, der über Ports mit einem Device oder bis zu n Devices verbunden ist und eine Schnittstelle zum Gateway zu den Kommunikationssystemen oder speicherprogrammierbaren Steuerungen der höheren Schicht bereitstellt

Anmerkung 1 zum Begriff: Wird „Master“ verwendet, so bezieht sich der Begriff auf SDCI-Einrichtungen, während „master“ allgemein verwendet wird.

3.2.23

Nachricht

<SDCI> Folge von UART-Rahmen, die entweder von einem Master an das entsprechende Device oder umgekehrt nach den Regeln des SDCI-Protokolls übertragen werden

3.2.24

Bedarfsdaten

OD, en: on-request data

Parameter oder Event-Daten, die auf Anforderung der Master-Applikation azyklisch übertragen werden

3.2.25

Bitübertragungsschicht

erste Schicht des ISO/OSI-Referenzmodells, welche die mechanischen, elektrischen, funktionalen und prozeduralen Mittel zur Aktivierung, Aufrechterhaltung und Deaktivierung physischer Verbindungen für die Bitübertragung zwischen Einheiten der Sicherungsschicht bereitstellt

Anmerkung 1 zum Begriff: Die Bitübertragungsschicht stellt auch Mittel für Wake-Up- und Fallback-Prozeduren bereit.

[QUELLE: ISO/IEC 7498-1, 7.7.2, modifiziert – beschreibender Text aus 7.7.2 entnommen; Anmerkung hinzugefügt.]

3.2.26

Port

<SDCI> Schnittstelle des Masters zum Übertragungsmedium, das mit einem Device verbunden ist

3.2.27

Betriebsmodus des Ports

Status eines Master-Ports, bei dem es sich um „INACTIVE“, „DO“, „DI“, „FIXEDMODE“ oder „SCANMODE“ handeln kann

3.2.28

Prozessdaten

Eingangs- oder Ausgangswerte von oder zu einem diskreten oder kontinuierlichen Automatisierungsprozess, die nach dem Starten des Masters mit hoher Priorität zyklisch und in einem konfigurierten Zeitplan automatisch übertragen werden

3.2.29

SIO

Betriebsmodus des Ports in Übereinstimmung mit den in IEC 61131-2 festgelegten digitalen Ein- und Ausgängen, der nach dem Einschalten oder Fallback oder fehlgeschlagenen Kommunikationsversuchen eingestellt wird

3.2.30

Schaltsignal

Binärsignal von oder zu einem Device, wenn sich dieses im SIO-Modus befindet (im Gegensatz zur SDCI-Kommunikation „Kodiertes Schalten“)

3.2.31

Systemmanagement

SM

<SDCI> Mittel zur Steuerung und Koordinierung der internen Kommunikationsschichten und der Ausnahmen innerhalb des Masters und seiner Ports und innerhalb jedes Devices

3.2.32

UART-Rahmen

<SDCI> Bitfolge, die mit einem Startbit beginnt, gefolgt von acht Bits, die ein Datenoktett bilden, gefolgt von einem geraden Paritätsbit und schließlich einem Stoppbit am Ende

3.2.33

Wake-Up

Prozedur, um ein Device zu veranlassen, vom SIO-Modus in den SDCI-Modus zu wechseln

3.2.34

Wake-Up-Anforderung

WURQ, en: wake-up request

Dienst der Bitübertragungsschicht, der vom Master zum Wake-Up eines Devices verwendet wird, und um es in einen empfangsbereiten Zustand zu versetzen

3.3. Begriffe im Zusammenhang mit SDCI-FS

3.3.1

Abweichung

Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten

Anmerkung 1 zum Begriff: Abweichungen können auf einem Auslegungsirrtum bei Hardware/Software beruhen und/oder auf verfälschten Informationen durch elektromagnetische Einflüsse und/oder anderen Effekten.

Anmerkung 2 zum Begriff: Abweichungen führen nicht notwendigerweise zu einem Ausfall oder einem *Ausfall* oder einem *Fehler*.

[QUELLE: IEC 61508-4:2010, 3.6.11, modifiziert – Die Anmerkungen zum Begriff wurden ergänzt.]

3.3.2

Ausfall

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion bereitzustellen oder Betrieb einer Funktionseinheit in irgendeiner Art anders als gefordert

Anmerkung 1 zum Begriff: Ein Ausfall kann auf eine Abweichung zurückzuführen sein (z. B. ein Problem der Hardware-/Softwareauslegung oder eine Nachrichtenstörung).

[QUELLE: IEC 61508-4:2010, 3.6.4, modifiziert – Die Anmerkungen wurden entfernt und durch eine neue Anmerkung ersetzt, und das Bild entfernt.]

3.3.3

Fehler

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

Anmerkung 1 zum Begriff: IEC 191-05-01 definiert „Fehlzustand“ als den Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Instandhaltung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist.

[Quelle: IEC 61508-4:2010, 3.6.1, modifiziert – Die Verweisung auf IEC 61508-4:2010, Bild 4, wurde aus der Anmerkung entfernt.]

3.3.4

FS-Device

einzelner passiver Peer, wie ein funktional sicherer Sensor oder Aktor, zu einem Master mit Funktionen für funktionale Sicherheit

3.3.5

FS-Master

aktiver Peer mit Funktionen für funktionale Sicherheit, der über Ports mit einem Device oder bis zu n Devices oder FS-Devices verbunden ist und eine Schnittstelle zum Gateway zu den Kommunikationssystemen (nicht sicherheitsbezogen oder sicherheitsbezogen) oder Steuerungen mit Funktionen für funktionale Sicherheit der höheren Schicht bereitstellt

3.3.6

FSP-Parameter

Parametersatz für die Verwaltung und den Betrieb des SDCI-FS-Protokolls

3.3.7

FST-Parameter

Parametersatz für die sicherheitsbezogene Technologie eines FS-Device, z. B. ein Lichtvorhang

3.3.8

Sicherheits-PDU

Sicherheits-Protokolldateneinheit

SPDU, en: safety protocol data unit

durch einen Sicherheitskommunikationskanal übertragene PDU

[Quelle: IEC 61784-3:2021, 3.1.47, modifiziert – Anmerkungen wurden entfernt, und die zulässige Benennung „Sicherheits-Protokolldateneinheit“ wurde hinzugefügt.]

3.4 Symbole und Abkürzungen

AIDA	Automatisierungsinitiative Deutscher Automobilhersteller
AL	Anwendungsschicht (en: application layer)
BEP	Bitfehlerwahrscheinlichkeit (en: bit error probability)
C/Q	Verbindung für Kommunikationssignal (C) oder Schaltsignal (Q) (SIO)
CRC	zyklische Redundanzprüfung (en: cyclic redundancy check)
DDO	Gerätedatenobjekt (en: device data object)
DI	Digitaleingang (en: digital input)
DIP	zweireihiges Gehäuse (en: dual in-line package)
DL	Sicherungsschicht (en: data link layer)
DO	Digitalausgang (en: digital output)
DS	Datenspeicher
DTI	Gerätetool-Schnittstelle (en: device tool interface)
DTM	Gerätetypmanager (en: device type manager)

[IEC 62453 (alle Teile)]

E DIN EN IEC 61139-2:2023-04

FDI	Feldgeräteintegration (en: field device integration)	[IEC 62769 (alle Teile)]
FDT	Feldgerätetool (en: field device tool)	[IEC 62453 (alle Teile)]
FS	funktionale Sicherheit	
FS-AI/AO	funktional sicherer Analogeingang/-ausgang (en: functional safety analog input/output)	
FSCP	funktional sicheres Kommunikationsprofil (en: functional safety communication profile (z. B. Normenreihe IEC 61784-3 [1]))	
FS-DI/DO	funktional sicherer Digitaleingang/-ausgang (en: functional safety digital input/output)	
FSP	funktional sicheres Protokoll (Parameter)	
FST	funktional sichere Technologie (Parameter)	
I/O	Eingang/Ausgang (en: Input/Output)	
I/Q	Anschluss mit mehreren Optionen: DI, OSSD2e oder DO	
IODD	IO-Link-Gerätebeschreibung (en: IO device description)	
IOPD	SDCI-Parametrierungs- und -Diagnosetool	
L-	Stromversorgung (-)	
L+	Stromversorgung (+)	
LSO, MSO	kleinstwertiges Oktett (en: least significant octet), höchstwertiges Oktett (en: most significant octet)	
M12	Rundstecker	[IEC 61076-2-113]
N24	24-V-Zusatzstromversorgung (-); Port Klasse B	
NSR	nicht sicherheitsbezogen (en: non-safety-related)	
OD	Bedarfsdaten (en: on-request data)	
OK	„OK“-Werte oder Zustand richtig	
OSSD	Ausgangsschalelement (en: output signal switching device) (selbstprüfendes Gerät mit integriertem OSSD)	[IEC 61496-1]
OSSD1/2e	Pinbelegung beider OSSDe-Signale	
OSSDe	Ausgangsschalelement (en: output signal switching device) (selbstprüfendes Gerät mit integriertem OSSD nach diesem Dokument)	
OSSDm	Ausgangsschalelement (en: output signal switching device) (Relais- und Halbleiterausgänge)	[IEC 60947-5-5]
P24	24-V-Zusatzstromversorgung (+); Port Klasse B	
PD	Prozessdaten	
PDCT	Port- und Geräte-Konfigurationstool (en: port and device configuration tool)	
PDin	funktional sichere Prozess-Eingangsdaten (aus Sicht eines FS-Masters)	
PDout	funktional sichere Prozess-Ausgangsdaten (aus Sicht eines FS-Masters)	
PDU	Protokolldateneinheit (en: protocol data unit)	
PFH	mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde	[IEC 61508-4]
PID	Programmschnittstellenbeschreibung (en: program interface description)	
PL	Bitübertragungsschicht (en: physical layer)	
PS	Stromversorgung in Volt (en: power supply)	

RIO	Remote-I/O	
rms	Effektivwert (en: root mean square)	
SCL	Sicherheitskommunikationsschicht (en: safety communication layer)	
SDCI	Schnittstelle für die digitale Kommunikation über eine Punkt-zu-Punkt-Verbindung (en: single-drop digital communication interface)	[IEC 61131-9]
SDCI-FS	funktional sichere Schnittstelle für die digitale Kommunikation über eine Punkt-zu-Punkt-Verbindung (en: single-drop digital communication interface for functional safety)	
SIO	Standard-Ein-/Ausgang (en: standard input output) (digitaler Schaltmodus)	[IEC 61131-2]
SLM	Sicherheitsschichtmanager (en: safety layer manager)	
SM	Systemmanagement	
SPDU	Sicherheits-Protokolldateneinheit (en: safety protocol data unit)	
SPS	speicherprogrammierbare Steuerung	
SR	sicherheitsbezogen (en: safety-related)	
SSI	synchrone serielle Schnittstelle (en: synchronous serial interface) (in der Regel für Geber)	
TAF	temporäre Quittierungsdatei (en: temporary acknowledgment file)	
TBF	temporäre Backchannel-Datei (en: temporary backchannel file)	
TPF	temporäre Parameterdatei (en: temporary parameter file)	
UART	universeller asynchroner Empfänger-Sender (en: universal asynchronous receiver transmitter)	
UML 2	vereinheitlichte Modellierungssprache (en: unified modeling language), Version 2	[ISO/IEC 19505-2]
USB	universeller serieller Bus	[www.usb.org]
WURQ	Impuls der Wake-Up-Anforderung (en: wake-up request pulse)	
XML	erweiterbare Auszeichnungssprache (en: extensible markup language)	

3.5 Konventionen

3.5.1 Verhaltensbeschreibungen

Für die Verhaltensbeschreibungen werden die Notationen von UML 2 verwendet (siehe [2], [3], [4]).

Ereignisse, die einen Übergang auslösen, können normalerweise ein Signal, ein Dienstaufwurf oder eine Zeitüberschreitung sein. Logische Bedingungen (wahr/falsch) müssen das Ergebnis eines [Guard] sein. Um die Lesbarkeit und die Pflege der Zustandsautomaten zu erleichtern, enthalten die Diagramme nicht die mit einem Übergang verbundenen Aktionen. Diese Aktionen sind in einer separaten Tabelle nach [5] für den Zustandsübergang aufgeführt.

Die in diesem Dokument dargestellten Zustandsdiagramme sind vollkommen abstrakte Beschreibungen. Sie stellen keine vollständige Spezifikation für die Implementierung dar.

3.5.2 Speicher- und Übertragungsreihenfolge der Oktette

Bild 3 zeigt die Reihenfolge, die für die Übermittlung von Daten vom Typ WORD vom Speicher zum Übertragungsmedium und umgekehrt verwendet werden muss.

ANMERKUNG Bestehende Mikrocontroller können sich darin unterscheiden, wie Daten vom Typ WORD im Speicher abgelegt werden: „Big Endian“ und „Little Endian“. Wird dies bei der Auslegung nicht berücksichtigt, können die Oktette bei der Übertragung fälschlicherweise vertauscht werden.

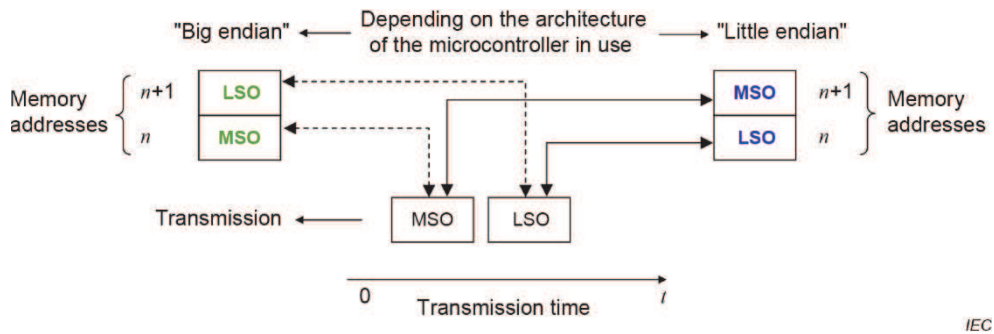


Bild 3 – Speicher- und Übertragungsreihenfolge der Oktette

EN	DE
Depending on the architecture of the microcontroller in use	Abhängig von der Architektur des verwendeten Mikrocontrollers
"Big endian"	„Big Endian“
Memory addresses	Speicheradressen.
$n+1$	$n+1$
n	n
LSO	LSO (kleinstwertiges Oktett)
MSO	MSO (höchstwertiges Oktett)
Transmission	Übertragung
"Little endian"	„Little Endian“
Transmission time	Übertragungszeit
t	t

English version

Industrial networks – Single-drop digital communication
interface – Part 2: Functional safety extensions
(IEC 61139-2:2022)

Réseaux industriels – Interface de communication numérique
point à point – Partie 2: Extensions de sécurité fonctionnelle
(IEC 61139-2:2022)

Industrielle Netzwerke – Digitale Single-
Drop-Kommunikationsschnittstelle – Teil 2:
Erweiterungen für die funktionale Sicherheit
(IEC 61139-2:2022)

This European Standard was approved by CENELEC on 2022-09-23. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre 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, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

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

European Foreword

The text of document 65C/1168/FDIS, future edition 1 of IEC 61139-2, 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 approved by CENELEC as EN IEC 61139-2:2022.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop): 2023-06-23
- latest date by which the national standards conflicting with the document have to be withdrawn (dow): 2025-09-23

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

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 61139-2:2022 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 61784-3 (series)	NOTE	Harmonized as EN IEC 61784-3 (series)
IEC 60947-5-2	NOTE	Harmonized as EN IEC 60947-5-2
IEC 62769 (series)	NOTE	Harmonized as EN IEC 62769 (series)
IEC 60947-5-6	NOTE	Harmonized as EN 60947-5-6
IEC 62453 (series)	NOTE	Harmonized as EN 62453 (series)
IEC 60947-5-3	NOTE	Harmonized as EN 60947-5-3
IEC 61076-2-113	NOTE	Harmonized as EN 61076-2-113
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)

Annex ZA
(normative)**Normative references to international publications with their corresponding European publications**

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60204-1	-	Safety of machinery - Electrical equipment of machines - Part 1: General requirements	EN 60204-1	-
IEC 61010-2-201	-	Safety requirements for electrical equipment for measurement, control, and laboratory use - Part 2-201: Particular requirements for control equipment	EN IEC 61010-2-201	-
IEC 61131-2	-	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests	-	-
IEC 61131-9	2022	Programmable controllers - Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI)	EN IEC 61131-9	2022
IEC 61496-1	-	Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests	EN IEC 61496-1	-
IEC 61508-3	-	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	-
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 62061	-	Safety of machinery - Functional safety of safety-related control systems	EN IEC 62061	-
IEC 62443	Reihe	Security for industrial automation and control systems	EN IEC 62443	Reihe
ISO 639-2	-	Codes for the representation of names of languages - Part-2: Alpha-3 code	-	-
ISO 639-3	-	Codes for the representation of names of languages - Part 3: Alpha-3 code for comprehensive coverage of languages	-	-
ISO 13849-1	-	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design	EN ISO 13849-1	-

CONTENTS

	Page
European Foreword	16
Annex ZA (normative) Normative references to international publications with their corresponding European publications	17
INTRODUCTION	30
1 Scope.....	32
2 Normative references	33
3 Terms, definitions, symbols, abbreviated terms, and conventions	33
3.1 Terms and definitions	33
3.2 Common terms and definitions.....	33
3.3 Terms and definitions related to SDCI-FS.....	37
3.4 Symbols and abbreviated terms	38
3.5 Conventions.....	39
3.5.1 Behavioral descriptions	39
3.5.2 Memory and transmission octet order	40
4 Overview of SDCI-FS	40
4.1 Purpose of the technology and feature levels	40
4.1.1 Base SDCI-FS technology.....	40
4.1.2 From "analog" and "switching" to communication	41
4.1.3 Minimized paradigm shift from FS-DI to FS-Master	42
4.1.4 Following the SDCI paradigm (SIO vs. OSSDe)	43
4.1.5 Port class B	45
4.1.6 "USB-Master" with safety parameterization	46
4.1.7 Interoperability matrix of safety devices	46
4.2 Positioning within the automation hierarchy	47
4.3 Wiring, connectors, and power supply	48
4.4 Relationship to SDCI	48
4.5 Communication features and interfaces.....	49
4.6 Parameterization	49
4.7 Role of FS-Master and FS-Gateway	49
4.8 Mapping to upper-level systems.....	50
4.9 Structure of the document	50
5 Extensions to the Physical Layer (PL).....	50
5.1 Overview.....	50
5.2 Extensions to PL services	51
5.2.1 PL_SetMode	51
5.2.2 PL_Ready	51
5.3 Transmitter/receiver.....	51
5.3.1 Assumptions for the expansion to OSSDe	51

5.3.2	OSSDe specifics	52
5.3.3	Start-up of an FS-Device (Ready pulse)	55
5.3.4	Electric characteristics of a receiver in FS-Device and FS-Master	56
5.4	Electric and dynamic characteristics of an FS-Device	56
5.5	Electric and dynamic characteristics of an FS-Master port (OSSDe)	59
5.6	FS-Master port FS-DI interface	60
5.7	Wake-up coordination	60
5.8	Fast start-up	61
5.9	Power supply	61
5.10	Medium	62
5.10.1	Constraints	62
5.10.2	Connectors	62
5.10.3	Cable characteristics	62
6	Extensions to SIO	62
7	Extensions to the data link layer (DL)	62
7.1	Overview	62
7.2	State machine of the FS-Master DL-mode handler	62
7.3	State machine of the FS-Device DL-mode handler	64
8	Extensions to the Master Configuration Manager (CM)	66
9	Extensions of the FS-Device	67
9.1	Principle architecture and models	67
9.1.1	FS-Device architecture	67
9.1.2	FS-Device model	68
9.2	Parameter Manager (PM)	69
9.3	Process Data Exchange (PDE)	69
9.4	Data Storage (DS)	69
9.4.1	General considerations and extensions including safety	69
9.4.2	Backup levels	70
10	Extensions of the FS-Master	70
10.1	Principle architecture	70
10.2	SMI service extensions	71
10.2.1	Overview	71
10.2.2	SMI_FSMasterAccess	73
10.2.3	SMI_SPDUIn	75
10.2.4	SMI_SPDUOut	75
10.2.5	SMI_FSPDInOut	75
10.3	ArgBlock extensions	76
10.3.1	Overview	76
10.3.2	FSMasterAccess	77

10.3.3	FSCPAuthenticity	77
10.3.4	FSPortConfigList	78
10.3.5	FSPortStatusList.....	80
10.3.6	SPDUIn.....	81
10.3.7	SPDUOut	82
10.3.8	FSPDInOut	82
10.4	Safety Layer Manager (SLM)	83
10.4.1	Purpose	83
10.4.2	FS_PortModes.....	83
10.4.3	FSP parameter	84
10.5	Process Data Exchange (PDE)	87
10.6	Data Storage (DS)	88
11	Safety communication layer (SCL)	88
11.1	Functional requirements	88
11.2	Communication errors and safety measures.....	88
11.3	SCL services	89
11.3.1	Positioning of safety communication layers (SCL)	89
11.3.2	FS-Master SCL services.....	90
11.3.3	FS-Device SCL services.....	92
11.4	SCL protocol	94
11.4.1	Protocol phases to consider	94
11.4.2	FS-Device faults	95
11.4.3	Safety PDU (SPDU)	95
11.4.4	FS-Input and FS-Output data	95
11.4.5	Port number	95
11.4.6	Status and control.....	96
11.4.7	CRC signature	96
11.4.8	TADI safety considerations (informative)	97
11.4.9	Data types for SDCI-FS.....	98
11.5	SCL behavior.....	99
11.5.1	General.....	99
11.5.2	SCL state machine of the FS-Master	99
11.5.3	SCL state machine of the FS-Device	102
11.5.4	Sequence charts for several use cases	106
11.5.5	Monitoring of safety times.....	112
11.5.6	Reaction in the event of a malfunction	113
11.5.7	Start-up (communication)	115
11.6	SCL management.....	115
11.6.1	Parameter overview (FSP and FST)	115

11.6.2	Parameterization approaches	117
11.7	Integrity measures	118
11.7.1	IODD integrity	118
11.7.2	Tool integrity	118
11.7.3	Transmission integrity	118
11.7.4	Verification record	118
11.7.5	Authentication	119
11.7.6	Storage integrity	119
11.7.7	FS I/O data structure integrity	120
11.7.8	Technology parameter (FST) based on IODD	120
11.7.9	Technology parameter (FST) based on existing Dedicated Tool (IOPD)	121
11.8	Creation of FSP and FST parameters	122
11.9	Integration of Dedicated Tools (IOPD)	123
11.9.1	IOPD interface	123
11.9.2	Standard interfaces	123
11.9.3	Backward channel	124
11.10	Validation	125
11.11	Passivation	125
11.11.1	Motivation and means	125
11.11.2	Port selective (FS-Master)	125
11.11.3	Signal selective (FS-Terminal)	125
11.11.4	Qualifier settings in case of communication	126
11.11.5	Qualifier handling in case of OSSDe	126
11.12	SCL diagnosis	127
12	Functional safe processing (FS-P)	128
12.1	Recommendations for efficient I/O mappings	128
12.2	Embedded FS controller	128
Annex A	(normative) Extensions to parameters	129
A.1	Indices and parameters for SDCI-FS	129
A.2	Parameters in detail	130
A.2.1	FSP_Authenticity	130
A.2.2	FSP_Port	130
A.2.3	FSP_AuthentCRC	131
A.2.4	FSP_ProtVersion	131
A.2.5	FSP_ProtMode	131
A.2.6	FSP_Watchdog	131
A.2.7	FSP_IO_StructCRC	132
A.2.8	FSP_TechParCRC	133
A.2.9	FSP_ProtParCRC	133

A.2.10	FSP_VerifyRecord	133
A.2.11	FSP_TimeToReady	133
A.2.12	FSP_MinShutDownTime	134
A.2.13	FSP_WCDT	134
A.2.14	FSP_OFDT	134
A.2.15	FSP_ParamDescCRC	134
Annex B (normative) Extensions to EventCodes		135
B.1	Additional FS-Device EventCodes	135
B.2	Additional Port EventCodes	135
Annex C (normative) Extensions to Data Types		137
C.1	Data types for SDCI-FS	137
C.2	BooleanT (bit)	137
C.3	IntegerT (16)	138
C.4	IntegerT (32)	138
C.5	Safety Code	139
Annex D (normative) CRC generator polynomials		140
D.1	Overview of CRC generator polynomials	140
D.2	Residual error probabilities	140
D.3	Implementation considerations	142
D.3.1	Overview	142
D.3.2	Bit shift algorithm (16 bit)	142
D.3.3	Lookup table (16 bit)	143
D.3.4	Bit shift algorithm (32 bit)	144
D.3.5	Lookup table (32 bit)	145
D.3.6	Seed values	146
D.3.7	Octet order for CRC calculation	146
Annex E (normative) IODD extensions		147
E.1	General	147
E.2	Schema	147
E.3	IODD constraints	147
E.3.1	General rules	147
E.3.2	Description of the IODD structure	147
E.3.3	Behavior of "Reset" SystemCommands in SDCI-FS	154
E.3.4	Profile Characteristic	155
E.3.5	ProcessDataInput and ProcessDataOutput	155
E.4	IODD conventions	155
E.4.1	Naming	155
E.4.2	Process Data (PD)	155
E.4.3	IODD conventions for user interface	156

E.4.4	Master Tool features	156
E.5	Securing	156
E.5.1	General.....	156
E.5.2	DefaultValues for FSP.....	157
E.5.3	FSP_Authenticity.....	157
E.5.4	FSP_Protocol	157
E.5.5	FSP_IO_Description	158
E.5.6	Sample serialization for FSP_ParamDescCRC	158
E.5.7	FST and FSP parameters and Data Storage.....	159
E.5.8	Sample IODD of an FS-Device	160
Annex F (normative)	Device Tool Interface (DTI) for SDCI.....	170
F.1	Purpose of DTI	170
F.2	Base model	170
F.3	Invocation interface	171
F.3.1	Overview	171
F.3.2	Detection of Device Tool	172
F.3.2.1	Registry structure	172
F.3.2.2	Device Tool specific registry entries.....	172
F.3.2.3	Processing of the Registry Data.....	174
F.3.3	Program Interface Description – PID	175
F.3.3.1	General.....	175
F.3.3.2	Structure of the PID file	175
F.3.3.3	Example PID file.....	178
F.3.4	Temporary Parameter File – TPF	178
F.3.4.1	General.....	178
F.3.4.2	Structure of a TPF	178
F.3.4.3	Example of a TPF.....	181
F.3.5	Temporary Backchannel File – TBF.....	183
F.3.5.1	General.....	183
F.3.5.2	Structure of the TBF	183
F.3.5.3	Example of a TBF.....	183
F.3.6	Temporary Acknowledgment File – TAF	184
F.3.6.1	General.....	184
F.3.6.2	Structure of the TAF	184
F.3.6.3	Example of a TAF.....	185
F.3.7	Invocation behavior	185
F.3.7.1	Conventions on Device Tool invocation	185
F.3.7.2	Handling of the TPF	185
F.4	Device data objects (DDO)	186

F.4.1	General	186
F.4.2	Structure of DDO package	186
F.5	Communication Interface.....	186
F.5.1	General	186
F.5.2	Principle of DTI communications	187
F.5.3	Gateways	189
F.5.4	Configuration of the Communication Server	189
F.5.5	Definition of the Communication Interface	189
F.5.6	Sequence for establishing a communication relation	189
F.5.7	Usage of the Communication Server in stand-alone mode.....	191
F.5.8	SDCI specifics	191
F.5.9	Changing communication settings	192
F.6	Reaction on incorrect Tool behavior	192
F.7	Compatibility	193
F.7.1	Schema validation	193
F.7.2	Version policy	193
F.8	Scalability.....	193
F.8.1	Scalability of a Device Tool	193
F.8.2	Scalability of a Master Tool	194
F.8.3	Interactions at conformance class combinations	194
F.9	Schema definitions	194
F.9.1	General	194
F.9.2	Schema of the PID	194
F.9.3	Schema of the TPF.....	196
F.9.4	Schema of the TBF.....	199
F.9.5	Schema of the TAF.....	200
F.9.6	Schema of DTI primitives	201
Annex G (normative)	Main scenarios of SDCI-FS.....	203
G.1	Overview.....	203
G.2	Sequence chart of commissioning	204
G.3	Sequence chart of replacement	205
G.4	Sequence chart of misconnection	206
Annex H (normative)	System requirements.....	207
H.1	Indicators	207
H.1.1	General	207
H.1.2	OSSDe.....	207
H.1.3	Safety communication	207
H.1.4	Acknowledgment request	207
H.2	Installation guidelines, electrical safety, and security	207

H.3	Safety function response time	208
H.4	Duration of demands	208
H.5	Maintenance and repair	208
H.6	Safety manual	208
Annex I (informative)	Information for test and assessment of SDCI-FS components.....	209
Bibliography		210

Figures

Figure 1	– Positioning of SDCI-FS in functional safety automation	30
Figure 2	– Relationship of this document to standards	32
Figure 3	– Memory and transmission octet order	40
Figure 4	– SDCI-FS communication layer model	40
Figure 5	– Port interface extensions for SDCI-FS	41
Figure 6	– Migration to SDCI-FS	42
Figure 7	– Minimized paradigm shift from FS-DI to FS-Master	43
Figure 8	– FS-Master types and feature levels	43
Figure 9	– Original pin layout of SDCI (port class A)	44
Figure 10	– Optimized OSSDe commissioning with FS-Master	45
Figure 11	– Level "d" of an FS-Master (Class B)	46
Figure 12	– Off-site configuration and parameterization	46
Figure 13	– SDCI-FS within the automation hierarchy	48
Figure 14	– The SDCI physical layer of an FS-Master (class A)	50
Figure 15	– The physical layer of an FS-Device (class A)	51
Figure 16	– Cross compatibility OSSD and OSSDe	52
Figure 17	– Principle OSSDe function	53
Figure 18	– Test pulses to detect cross connection faults	54
Figure 19	– OSSD timings	55
Figure 20	– Typical start-up of an OSSD sensor	55
Figure 21	– Start-up of an FS-Device	55
Figure 22	– Switching thresholds for FS-Device and FS-Master receivers	56
Figure 23	– Reference schematics (one OSSDe channel)	57
Figure 24	– Voltage level definitions	57
Figure 25	– Charge capability at power-up	60
Figure 26	– OSSDe input filter conflict resolution	60
Figure 27	– Start-up of an FS-Device	61
Figure 28	– Required fast start-up timings	61
Figure 29	– State machine of the FS-Master DL-mode handler	63
Figure 30	– State machine of the FS-Device DL-mode handler	65
Figure 31	– Extension to the Configuration Manager (VerifyRecord)	66

Figure 32 – Principle architecture of the FS-Device	68
Figure 33 – The FS-Device model	69
Figure 34 – Principle architecture of the FS-Master	71
Figure 35 – SMI service extensions	73
Figure 36 – FSP parameter use cases	84
Figure 37 – PDE Splitter	87
Figure 38 – PDE Composer	88
Figure 39 – Positioning of the SDCI-FS Safety Communication Layer (SCL)	90
Figure 40 – FS-Master Safety Communication Layer services	91
Figure 41 – FS-Device Safety Communication Layer services	93
Figure 42 – Protocol phases to consider	94
Figure 43 – Safety PDUs of FS-Master and FS-Device	95
Figure 44 – The 1 % share rule of IEC 61784-3:2021	97
Figure 45 – SCL state machine of the FS-Master	100
Figure 46 – SCL state machine of the FS-Device	103
Figure 47 – FS-Master and FS-Device both with power ON	106
Figure 48 – FS-Master power OFF → ON	107
Figure 49 – FS-Device with delayed SCL start	108
Figure 50 – FS-Device with power OFF and ON	109
Figure 51 – FS-Master detects CRC signature error	110
Figure 52 – FS-Device detects CRC signature error	111
Figure 53 – Monitoring of the SCL cycle time	112
Figure 54 – Parameter types and assignments	116
Figure 55 – FSCP-Host-centric system	117
Figure 56 – Structure of the FSP_VerifyRecord	119
Figure 57 – Start-up of SDCI-FS	120
Figure 58 – Securing of FST parameters via dedicated tool	121
Figure 59 – Modification of FST parameters via Device Tool	122
Figure 60 – Creation of FSP and FST parameters	123
Figure 61 – Example of a communication hierarchy	124
Figure 62 – Motivation for Port selective passivation	125
Figure 63 – Qualifier handler (communication)	126
Figure 64 – Qualifier handler (OSSDe)	126
Figure 65 – Qualifier behavior per FS-Master port	127
Figure 66 – Mapping efficiency issues	128
Figure A.1 – Instance of an FS I/O data description	132
Figure A.2 – Example FS I/O data structure with non-safety data	133
Figure A.3 – Securing of safety parameters	134
Figure C.1 – Example of a BooleanT data structure	138

Figure C.2 – Safety Code of an output message	139
Figure C.3 – Safety Code of an input message	139
Figure D.1 – CRC-16 generator polynomial	141
Figure D.2 – CRC-32 generator polynomial	142
Figure D.3 – Bit shift algorithm in "C" language (16 bit)	142
Figure D.4 – CRC-16 signature calculation using a lookup table	143
Figure D.5 – Bit shift algorithm in "C" language (32 bit)	144
Figure D.6 – CRC-32 signature calculation using a lookup table	145
Figure E.1 – Algorithm to build the FSP parameter CRC signatures	157
Figure F.1 – Principle of DTI invocation interface	171
Figure F.2 – Structure of the registry	172
Figure F.3 – Example of a DTI registry	173
Figure F.4 – Detection of a Device tool in registry	174
Figure F.5 – Menu for Device Tool invocation	175
Figure F.6 – Purpose of Device data objects (DDO)	186
Figure F.7 – Communication routes between Device Tool and Device	187
Figure F.8 – Routing across networks and SDCI	188
Figure F.9 – Communication Server	188
Figure F.10 – Sequence chart for establishing communication	190
Figure F.11 – Create Communication Server instance	190
Figure F.12 – Example of a Connect Request XML document for SDCI	192
Figure F.13 – XML schema of the PID file	195
Figure F.14 – XML schema of the TPF	197
Figure F.15 – XML schema of a TBF	199
Figure G.1 – Commissioning with test and armed operation	205
Figure G.2 – FS-Device replacement	206
Figure G.3 – FS-Device misconnection	206

Tables

Table 1 – Operational modes of feature level "a" to "c" (port class A)	45
Table 2 – Interoperability matrix of safety devices	47
Table 3 – PL_Ready	51
Table 4 – OSSD states and conditions	53
Table 5 – Cross connection faults	54
Table 6 – Electric characteristics of a receiver	56
Table 7 – Electric and dynamic characteristics of the FS-Device (OSSDe)	58
Table 8 – Electric and dynamic characteristics of the Port interface	59
Table 9 – Cable characteristics	62
Table 10 – State transition tables of the FS-Master DL-mode handler	64

Table 11 – State transition tables of the FS-Device DL-mode handler	65
Table 12 – State transition tables of the Configuration Manager	67
Table 13 – Extension to Data Storage (DS) state machine	70
Table 14 – Data Storage Backup Levels	70
Table 15 – SMI services used for FS-Master	72
Table 16 – SMI_FSMasterAccess	74
Table 17 – SMI_FSPDInOut	75
Table 18 – ArgBlock types and ArgBlockIDs	77
Table 19 – FSMasterAccess	77
Table 20 – FSCPAuthenticity	78
Table 21 – FSPortConfigList	78
Table 22 – FSPortStatusList	80
Table 23 – SPDUIIn	82
Table 24 – SPDUIOut	82
Table 25 – FSPDInOut	82
Table 26 – Use case reference table	84
Table 27 – Communication errors and safety measures	89
Table 28 – SCL services of FS-Master	92
Table 29 – SCL services of FS-Device	93
Table 30 – Protocol phases to consider	94
Table 31 – Control and counting (Control&MCnt)	96
Table 32 – Status and counting mirror (Status&DCnt)	96
Table 33 – MCount and DCount_i values	96
Table 34 – FS process I/O data types	98
Table 35 – Rules for the layout of values and qualifiers	99
Table 36 – Order of values and qualifier	99
Table 37 – Definition of terms used in SCL state machine of the FS-Master	100
Table 38 – FS-Master SCL states and transitions	101
Table 39 – Definition of terms used in SCL state machine of the FS-Device	103
Table 40 – FS-Device SCL states and transitions	104
Table 41 – Timing constraints	112
Table 42 – Qualifier bits "GOOD/BAD"	126
Table 43 – State transition Table for the qualifier behavior	127
Table A.1 – Indices for SDCI-FS	129
Table A.2 – Coding of protocol version	131
Table A.3 – Coding of protocol mode	131
Table A.4 – Generic FS I/O data structure description	132
Table B.1 – FS-Device SCL specific EventCodes	135
Table B.2 – FS-Master SCL specific EventCodes	136

Table C.1 – Data types for SDCI-FS	137
Table C.2 – BooleanT for SDCI-FS	137
Table C.3 – Example of BooleanT within a RecordT	137
Table C.4 – IntegerT(16)	138
Table C.5 – IntegerT(16) coding	138
Table C.6 – IntegerT(32)	138
Table C.7 – IntegerT(32) coding	139
Table D.1 – CRC generator polynomials for SDCI-FS	140
Table D.2 – Definition of variables used in Figure D.3	143
Table D.3 – Definition of variables used in Figure D.4	143
Table D.4 – Lookup Table for CRC-16 signature calculation	143
Table D.5 – Definition of variables used in Figure D.5	145
Table D.6 – Definition of variables used in Figure D.4	145
Table D.7 – Lookup Table for CRC-32 signature calculation	145
Table E.1 – Specific behavior of FS-Device "Reset" SystemCommands	155
Table E.2 – User actions to replace DefaultValues	157
Table E.3 – RecordItems of FSP_Protocol where allowed values shall be serialized	158
Table E.4 – Sample serialization for FSP_ParamDescCRC	158
Table F.1 – Description of PID file elements	176
Table F.2 – Elements of a TPF	179
Table F.3 – Elements of the TBF	183
Table F.4 – Elements of the TAF	184
Table F.5 – Invocation cases and behaviors	185
Table F.6 – Communication Schema mapping	191
Table F.7 – Reaction on incorrect Tool behavior	192
Table F.8 – DTI conformance classes	193
Table F.9 – DTI feature levels of Device Tools	194
Table F.10 – Interactions at conformance class combinations	194
Table G.1 – Main scenarios of SDCI-FS	203

INTRODUCTION

The base technology of IO-Link™⁴ is subject matter of the international standard IEC 61131-9 being part of a series of standards on programmable controllers and the associated peripherals such as remote I/O (RIO).

It specifies a single-drop digital communication interface technology – named SDCI, which extends the traditional switching input and output interfaces as defined in IEC 61131-2 towards a point-to-point communication link using coded switching. This technology enables the cyclic exchange of digital input and output process data between a Master and its associated Devices (sensors, actuators, I/O terminals, etc.). The Master can be part of a fieldbus communication system or any stand-alone processing unit. The technology also enables the acyclic transfer of parameters to Devices and the propagation of diagnosis information from the Devices to the upper-level automation system (controller, host) via the Master.

Physical topology is point-to-point from each Device to the Master using 3 wires over distances up to 20 m. The SDCI physical interface is backward compatible with the usual 24 V I/O signalling specified in IEC 61131-2 and supports three transmission rates of 4,8 kbit/s, 38,4 kbit/s and 230,4 kbit/s are supported.

The main advantages of the SDCI technology are:

- dual use of either switching signals (DI/DO) or coded switching communication respectively,
- traditional switching sensors and actuators now providing alternatively single drop digital communication within the same Device,
- one thin, robust, very flexible cable without shielding for power supply and signalling,
- lowest-cost digital communication down to the lowest end sensors and actuators.

The functional safety variant of SDCI is called SDCI-FS. Figure 1 shows an example positioning of SDCI-FS in functional safety automation.

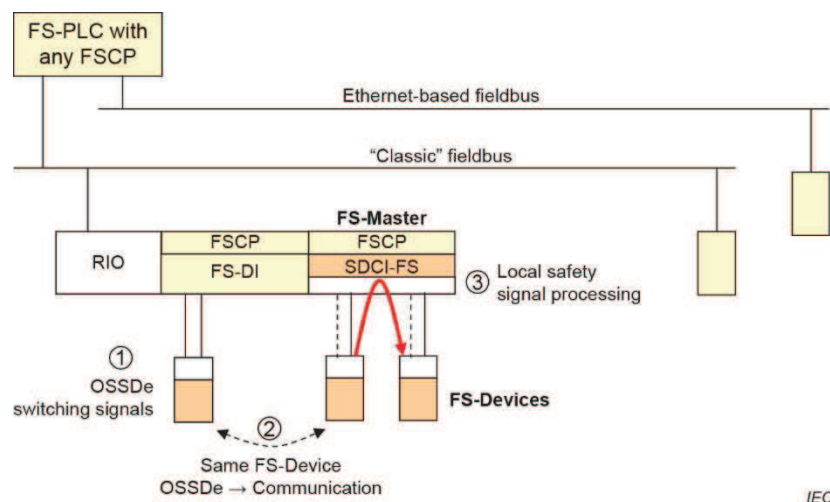


Figure 1 – Positioning of SDCI-FS in functional safety automation

⁴ IO-Link™ is a trade name of the "IO-Link Community". This information is given for the convenience of users of this specification and does not constitute an endorsement by the IO-Link Community of the trade name holder or any of its products. Compliance to this document does not require use of the registered logos for IO-Link™. Use of the registered logos for IO-Link™ requires permission of the "IO-Link Community".

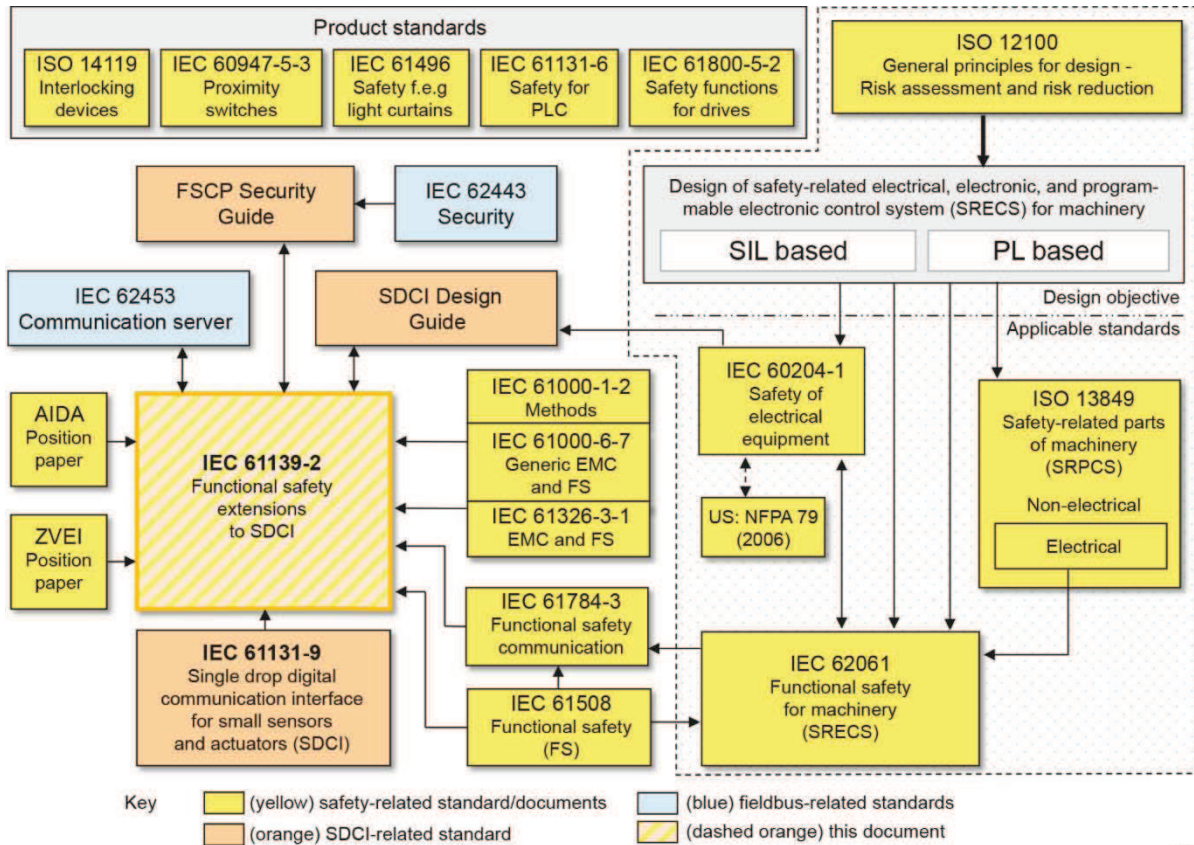
In this example, a remote I/O is connected to a functional safety programmable controller using one of the FSCPs of the IEC 61784-3 series [1]⁵ to communicate with an FS-DI module and a gateway to an SDCI-FS FS-Master. FS-Devices with OSSDe can be connected to FS-DIs or FS-Masters. All FS-Devices can communicate with any FS-Master using the SDCI-FS protocol regardless of the upper-level FSCP-system. The same is true for safety actuators (FS-Devices) such as drives with integrated safety. This means the largest component commonality ① for sensors and actuators similar to the DI and DO interfaces standardized within IEC 61131-2.

Safety sensors with OSSDe interfaces – equipped with SDCI-FS communication – can be parameterized via auxiliary tools such as "USB-Masters", then connected to an FS-DI and operated in OSSDe mode. They also can be operated in OSSDe mode on an FS-Master that supports OSSDe. In case these safety sensors are equipped with SDCI-FS communication in addition, they can be operated in both modes ②, either OSSDe or SDCI-FS. This corresponds to the SDCI SIO paradigm.

The concept of SDCI-FS allows for local safety signal processing if the gateway/FS-Master provides a local safety controller ③.

This document provides the necessary extensions to IEC 61131-9 for functional safety communication including standardization of OSSDe and parameterization within the domain of safety for machinery. Figure 2 shows its relationships to international fieldbus and safety standards as well as to relevant specifications (see Clause 2 and bibliography). Any functional safety starts with risk assessment and risk reduction (ISO 12100). One possibility of risk reduction is the usage of electrical or electronic control systems. For the design of those, standards such as IEC 61508, IEC 62061, and ISO 13849 can be used. Environmental conditions such as EMC are covered by for example IEC 61000-6-7. Further aspects are installations and security issues. A number of product standards such as IEC 60947-5-3 and ISO 14119 complement the generic or sector standards.

⁵ Numbers in square brackets refer to the Bibliography.



IEC

Figure 2 – Relationship of this document to standards

SDCI-FS can be used for functional safety applications according to IEC 62061 and IEC 61508 up to SIL3 and/or according to ISO 13849 up to PLe.

1 Scope

This part of IEC 61139 specifies the extensions to SDCI in IEC 61131-9 for functional safety. This comprises:

- a standardized OSSDe interface for redundant switching signals based on IEC 61131-2,
- minor modifications/extensions to state machines of SDCI to support the safety operations,
- a lean functional safety communication protocol on top of the standard SDCI communication which is a black channel according to IEC 61784-3:2021,
- protocol management functions for configuration, parameterization, and commissioning,
- IODD extensions for functional safety,
- a Device tool interface to support Dedicated Tools according to functional safety standards.

This document does not cover:

- communication interfaces or systems including multi-point or multi-drop linkages,
- communication interfaces or systems including multi-channel or encrypted linkages,
- wireless communication interfaces or systems,
- integration of SDCI-FS into upper-level systems such as fieldbuses/FSCPs.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61010-2-201, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

IEC 61131-2, *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-9:—⁶, *Programmable controllers – Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI)*

IEC 61496-1, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62061, *Safety of machinery – Functional safety of safety-related control systems*

IEC 62443 (all parts), *Security for industrial automation and control systems*

ISO 639-2, *Codes for the representation of names of languages – Part 2: Alpha-3 code*

ISO 639-3, *Codes for the representation of names of languages – Part 3: Part 3: Alpha-3 code for comprehensive coverage of languages*

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

3 Terms, definitions, symbols, abbreviated terms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61131-1 and IEC 61131-2 apply. ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.2 Common terms and definitions

3.2.1

address

part of the M-sequence control to reference data within data categories of a communication channel

⁶ Under preparation. Stage at the time of publication: IEC/CFDIS 61131-9:2022.

3.2.2
application layer
AL

<SDCI>⁷ part of the protocol responsible for the transmission of Process Data objects and On-request Data objects

3.2.3
block parameter
consistent parameter access via multiple Indices or Subindices

3.2.4
checksum
<SDCI> complementary part of the overall data integrity measures in the data link layer in addition to the UART parity bit

3.2.5
coded switching
SDCI communication, based on the standard binary signal levels of IEC 61131-2

3.2.6
COM1
SDCI communication mode with transmission rate of 4,8 kbit/s

3.2.7
COM2
SDCI communication mode with transmission rate of 38,4 kbit/s

3.2.8
COM3
SDCI communication mode with transmission rate of 230,4 kbit/s

3.2.9
COMx
one out of three possible SDCI communication modes COM1, COM2, or COM3

3.2.10
communication channel
logical connection between Master and Device

Note 1 to entry: Four communication channels are defined: process channel, page and ISDU channel (for parameters), and diagnosis channel.

3.2.11
communication error
unexpected disturbance of the SDCI transmission protocol

3.2.12
cycle time
time to transmit an M-sequence between a Master and its Device including the following idle time

3.2.13
Device
single passive peer to a Master such as a sensor or actuator

Note 1 to entry: Uppercase "Device" is used for SDCI equipment, while lowercase "device" is used in a generic manner.

⁷ Angle brackets indicate validity of the definition for the SDCI technology

3.2.14

Direct Parameter

directly (page) addressed parameter transferred acyclically via the page communication channel without acknowledgement

3.2.15

dynamic parameter

part of a Device's parameter set defined by on-board user interfaces such as teach-in buttons or control panels in addition to the static parameters

3.2.16

Event

instance of a change of conditions in a Device

Note 1 to entry: Uppercase "Event" is used for SDCI Events, while lowercase "event" is used in a generic manner.

Note 2 to entry: An Event is indicated via the Event flag within the Device's status cyclic information, then acyclic transfer of Event data (typically diagnosis information) is conveyed through the diagnosis communication channel.

3.2.17

fallback

transition of a port from coded switching to switching signal mode

3.2.18

ISDU

indexed service data unit used for acyclic acknowledged transmission of parameters that can be segmented in a number of M-sequences

3.2.19

M-sequence

sequence of two messages comprising a Master message and its subsequent Device message

3.2.20

M-sequence control

first octet in a Master message indicating the read/write operation, the type of the communication channel, and the address, for example offset or flow control

3.2.21

M-sequence type

one particular M-sequence format out of a set of specified M-sequence formats

3.2.22

Master

active peer connected through ports to one up to n Devices and which provides an interface to the gateway to the upper-level communication systems or PLCs

Note 1 to entry: Uppercase "Master" is used for SDCI equipment, while lowercase "master" is used in a generic manner.

3.2.23

message

<SDCI> sequence of UART frames transferred either from a Master to its Device or vice versa following the rules of the SDCI protocol

3.2.24

On-request Data

acyclically transmitted data upon request of the Master application consisting of parameters or Event data

3.2.25

physical layer

first layer of the ISO-OSI reference model, which provides the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for bit transmission between data-link entities

Note 1 to entry: Physical layer also provides means for wake-up and fallback procedures.

[SOURCE: ISO/IEC 7498-1, 7.7.2, modified – the descriptive text has been extracted from 7.7.2, the note has been added.]

3.2.26

Port

<SDCI> communication medium interface of the Master to one Device

3.2.27

Port operating mode

state of a Master's Port that can be either INACTIVE, DO, DI, FIXEDMODE, or SCANMODE

3.2.28

Process Data

input or output values from or to a discrete or continuous automation process cyclically transferred with high priority and in a configured schedule automatically after start-up of a Master

3.2.29

SIO

Port operation mode in accordance with digital input and output defined in IEC 61131-2 that is established after power-up or fallback or unsuccessful communication attempts

3.2.30

switching signal

binary signal from or to a Device when in SIO mode (as opposed to the "coded switching" SDCI communication)

3.2.31

System Management

SM

<SDCI> means to control and coordinate the internal communication layers and the exceptions within the Master and its ports, and within each Device

3.2.32

UART frame

<SDCI> bit sequence starting with a start bit, followed by eight bits carrying a data octet, followed by an even parity bit and ending with one stop bit

3.2.33

wake-up

procedure for causing a Device to change its mode from SIO to SDCI

3.2.34

wake-up request

WURQ

physical layer service used by the Master to initiate wake-up of a Device, and put it in a receive ready state

3.3 Terms and definitions related to SDCI-FS

3.3.1

error

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

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

Note 2 to entry: Errors do not necessarily result in a *failure* or a *fault*.

SOURCE: [IEC 61508-4:2010, 3.6.11, modified – The notes have been added.]

3.3.2

failure

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

Note 1 to entry: Failure may be due to an error (for example, problem with hardware/software design or message disruption)

SOURCE: [IEC 61508-4:2010, 3.6.4, modified – The notes have been removed and replaced by a new note and the figure has been deleted.]

3.3.3

fault

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

Note 1 to entry: 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.

SOURCE: [IEC 61508-4:2010, 3.6.1, modified – The reference to Figure 4 of IEC 61508-4:2010 in the note has been removed.]

3.3.4

FS-Device

single passive peer such as a functional safety sensor or actuator to a Master with functional safety capabilities

3.3.5

FS-Master

active peer with functional safety capabilities connected through Ports to one up to n Devices or FS-Devices and which provides an interface to the gateway to the upper-level communication systems (NSR or SR) or controllers with functional safety capabilities

3.3.6

FSP parameter

parameter set for the administration and operation of the SDCI-FS protocol

3.3.7

FST parameter

parameter set for the safety-related technology of an FS-Device, for example light curtain

3.3.8

Safety PDU

Safety Protocol Data Unit

SPDU

PDU transferred through the safety communication channel

[SOURCE: IEC 61784-3:2021, 3.1.47, modified – Notes have been removed and admitted term Safety Protocol Data Unit has been added.]

3.4 Symbols and abbreviated terms

AIDA	Automatisierungsinitiative Deutscher Automobilhersteller (Automation initiative of the German automotive manufacturers)	
AL	application layer	
BEP	bit error probability	
C/Q	connection for communication (C) or switching (Q) signal (SIO)	
CRC	cyclic redundancy check	
DDO	Device data object	
DI	digital input	
DIP	dual in-line package	
DL	data link layer	
DO	digital output	
DS	data storage	
DTI	Device Tool Interface	
DTM	Device Type Manager	[IEC 62453 (all parts)]
FDI	Field Device Integration	[IEC 62769 (all parts)]
FDT	Field Device Tool	[IEC 62453 (all parts)]
FS	functional safety	
FSCP	functional safety communication profile (for example IEC 61784-3 series [1])	
FS-AI/AO	functional safety analog input/output	
FS-DI/DO	functional safety digital input/output	
FSP	functional safety protocol (parameter)	
FST	functional safety technology (parameter)	
I/O	input / output	
IODD	IO Device Description	
IOPD	SDCI Parameterization & Diagnostic tool	
I/Q	connection with several options: DI, OSSD2e, or DO	
L-	power supply (-)	
L+	power supply (+)	
LSO, MSO	least significant octet, most significant octet	
M12	circular connector	[IEC 61076-2-113]
N24	24 V extra power supply (-); Port class B	
NSR	non-safety-related	
OD	On-request Data	
OK	"OK", values or state correct	
OSSD	output signal switching device (self-testing electronic device with built-in OSSD)	[IEC 61496-1]
OSSDe	output signal switching device (self-testing electronic device with built-in OSSD according to this document)	
OSSD1/2e	pin assignment of both OSSDe signals	
OSSDm	output signal switching device (relay and solid state outputs)	[IEC 60947-5-5]
P24	24 V extra power supply (+); Port class B	

PD	Process Data	
PDin	functional safety input process data (from an FS-Master's view)	
PDout	functional safety output process data (from an FS-Master's view)	
PDCT	port and Device configuration tool	
PDU	protocol data unit	
PFH	average frequency of a dangerous failure per hour	[IEC 61508-4]
PID	program interface description	
PL	physical layer	
PLC	programmable logic controller	
PS	power supply (measured in V)	
RIO	remote I/O	
rms	root mean square ("effective")	
SCL	safety communication layer	
SDCI	single-drop digital communication interface	[IEC 61131-9]
SDCI-FS	single-drop digital communication interface for functional safety	
SIO	standard input output (digital switching mode)	[IEC 61131-2]
SLM	safety layer manager	
SM	system management	
SPDU	safety protocol data unit	
SR	safety-related	
SSI	synchronous serial interface (usually for encoders)	
TAF	temporary acknowledgment file	
TBF	temporary backchannel file	
TPF	temporary parameter file	
UART	universal asynchronous receiver transmitter	
UML 2	unified modeling language, edition 2	[ISO/IEC 19505-2]
USB	universal serial bus	[www.usb.org]
WURQ	wake-up request pulse	
XML	extensible markup language	

3.5 Conventions

3.5.1 Behavioral descriptions

For the behavioral descriptions, the notations of UML 2 are used, mainly for state and sequence diagrams (see [2], [3], [4]).

Events to trigger a transition usually can be a signal, service call, or timeout. Logic conditions (true/false) shall be the result of a [guard]. To alleviate the readability and the maintenance of the state machines, the diagrams do not provide the actions associated with a transition. These actions are listed within a separate state-transition table according to [5].

The state diagrams shown in this document are entirely abstract descriptions. They do not represent a complete specification for implementation.

3.5.2 Memory and transmission octet order

Figure 3 demonstrates the order that shall be used when transferring WORD based data types from memory to transmission and vice versa.

NOTE Existing microcontrollers can differ in the way WORD based data types are stored in memory: "big endian" and "little endian". If designs are not considering this fact, octets can be erroneously permuted for transmission.

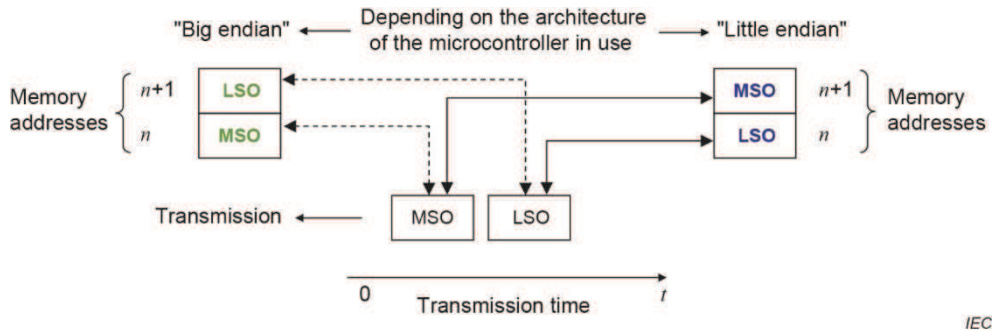


Figure 3 – Memory and transmission octet order

4 Overview of SDCI-FS

4.1 Purpose of the technology and feature levels

4.1.1 Base SDCI-FS technology

This document specifies a new lean functional safety communication protocol on top of the existing SDCI transmission system specified in IEC 61131-9. Figure 4 illustrates how the corresponding SDCI-FS communication layers are located within the architectural models of Master and Device such that they become FS-Master and FS-Device. Most of the original SDCI design remains unchanged for this document.

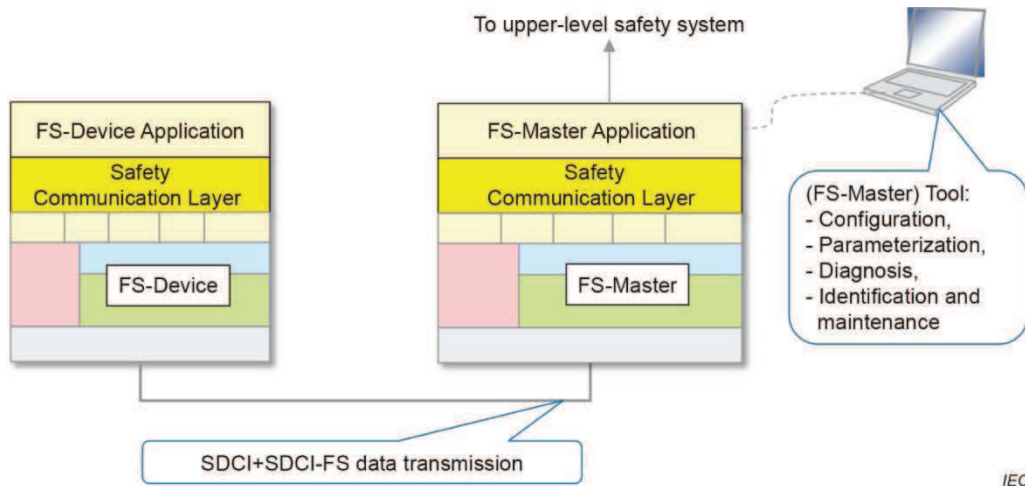


Figure 4 – SDCI-FS communication layer model

The SDCI-FS communication layer accommodates the functional safe transmission protocol. This protocol generates a safety PDU consisting of the FS-I/O data, protocol control or status data, and a CRC signature. The safety PDU together with optionally non-safety-related data is transmitted as SDCI Process Data between an FS-Master and one single FS-Device (point-to-point). It is suitable for functional safety applications up to SIL3 or PLe and the PFH for one connection is less than $10^{-9}/h$.

Full document details: E DIN EN IEC 61139-2:2023-04

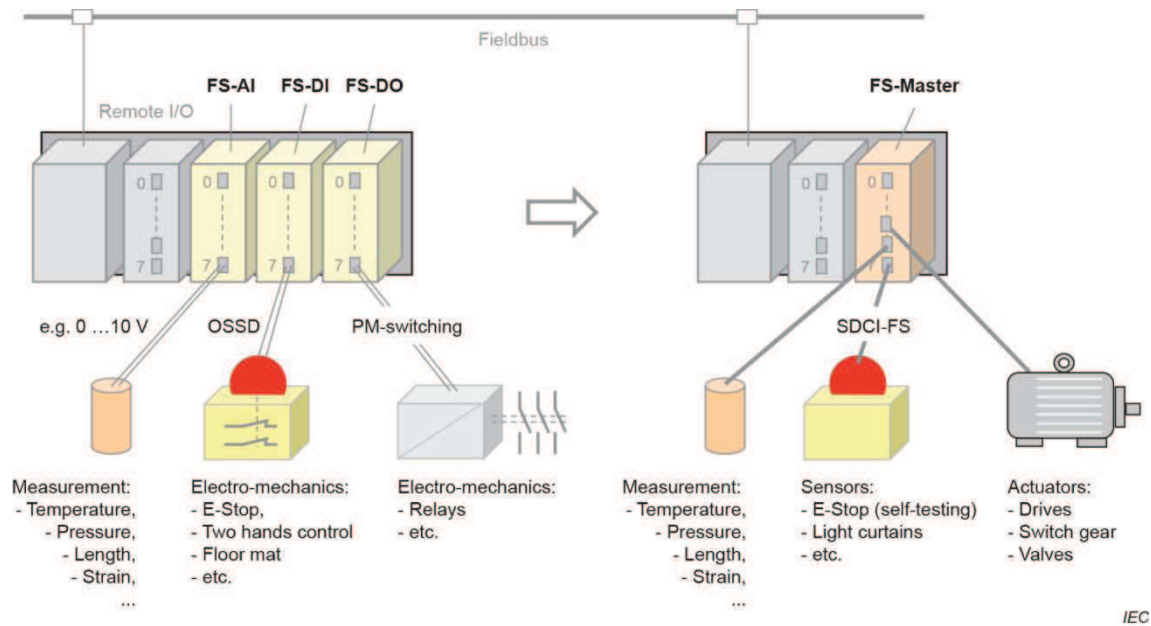


Figure 6 – Migration to SDCI-FS

Without additional interfaces, it was not possible in all cases to configure or parameterize the safety devices or to receive diagnosis information.

SDCI-FS can now provide a functional safe and reliable solution for process data exchange (signal states and measurement values) via single drop digital communication (SDCI), as well as parameterization and diagnosis (see Figure 6, right).

4.1.3 Minimized paradigm shift from FS-DI to FS-Master

Similar to nowadays safety devices for FS-DI modules (see Figure 7) and in contrast to FSCP-based safety devices, it is not necessary to

- setup an *authenticity code switch or adequate software solution*,
- assign a *watchdog time*,
- use any software tool in case of *FS-Device replacement*.

Authenticity is guaranteed through checking of the correct FS-Device to the assigned FS-Master Port during commissioning like FS-DI modules. However, SDCI-FS provides means to discover any incorrect plugging.

SDCI-FS uses a watchdog timer for the transmission of safety data in time (Timeliness). The system is able to calculate the required watchdog time automatically due to the point-to-point nature of the transmission.

FS-Device replacement without tools can be achieved using the original SDCI Data Storage mechanism.

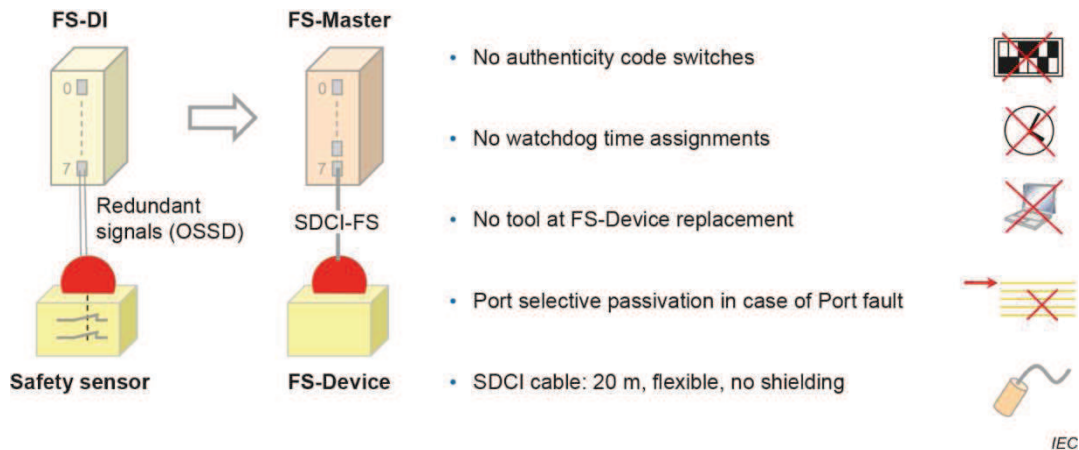


Figure 7 – Minimized paradigm shift from FS-DI to FS-Master

The FS-Master supports *port selective passivation* in case of a port fault and *signal granular passivation* in case of a channel fault within for example a remote I/O terminal ("Hub") connected to an FS-Master Port.

Cables are the same as with SDCI, i.e. unshielded with a maximum of 20 m. However, due to the higher permitted power supply current of 1000 mA per Port, the overall loop resistance RL_{eff} can only be 1,2 Ohm (see Table 9 and IEC 61131-9).

Compliance to AIDA rules requires cable color to be any except yellow. However, the connector color shall be yellow (RAL 1004).

4.1.4 Following the SDCI paradigm (SIO vs. OSSDe)

Standard SDCI-FS supports a port type A (4 pins) without extra power supply and a port type B (5 pins) with extra 24 V power supply (see IEC 61131-9). SDCI-FS takes care of several specification levels "a" to "d" (see Figure 8). The number of pins refers to the possible FS-Master pins.

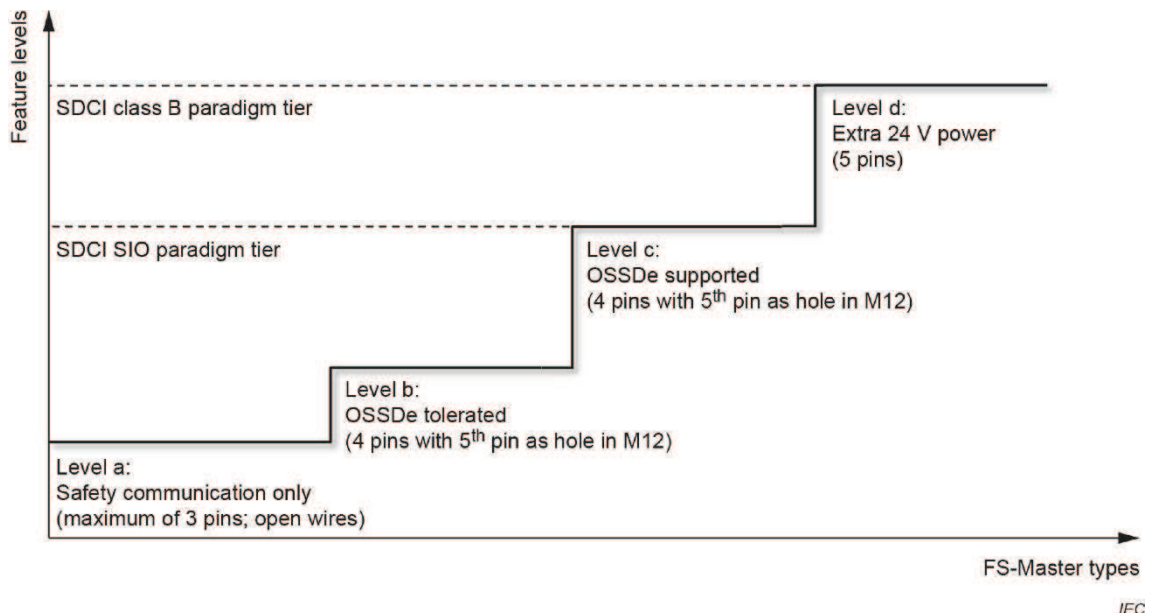


Figure 8 – FS-Master types and feature levels

The original pin layouts of SDCI for port class A are shown in Figure 9 together with the extensions for level "a" through "c". Table 1 shows the details of these levels.

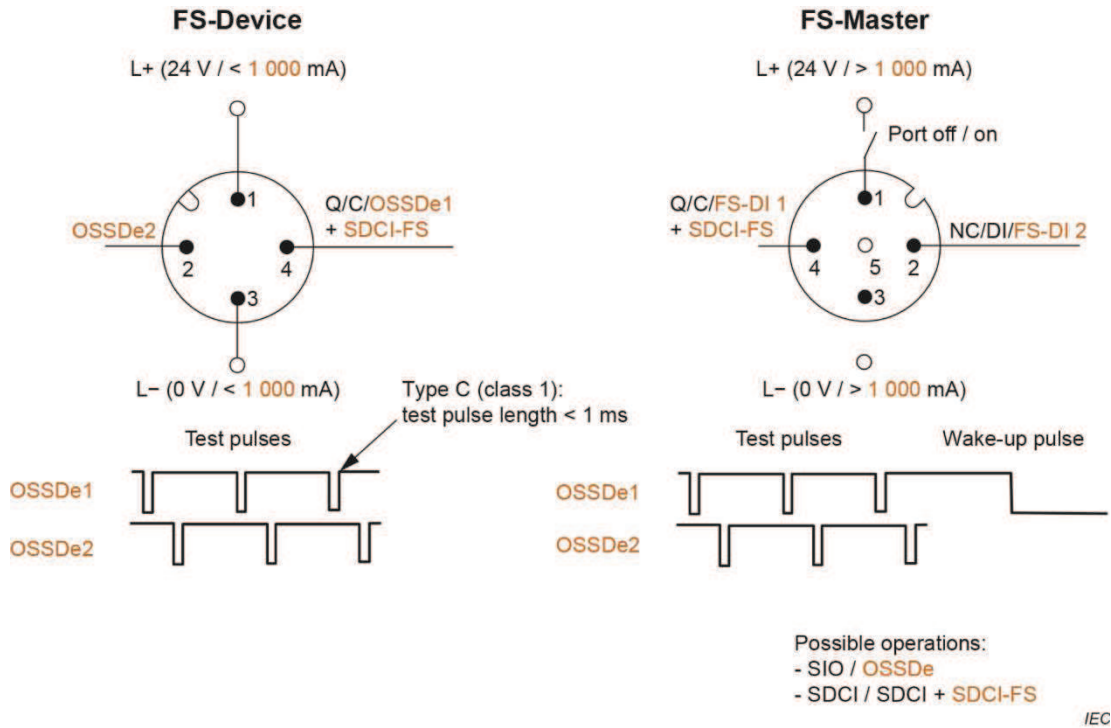


Figure 9 – Original pin layout of SDCI (port class A)

Level "a" provides communication only (Pin 1, 3, and 4). That means support for sensor-type FS-Devices and actuator-type FS-Devices.

Due to the redundant nature of most of the safety device interfaces, SDCI-FS considers pin 2 for the redundant signal path (e.g. OSSDe2) besides pin 4 for the primary signal path (e.g. OSSDe1)⁸. Thus, level "b" allows FS-Devices to provide OSSDe outputs besides the SDCI-FS communication capability. They can be parameterized with the help of a "USB-Master" and be connected to any FS-DI module in switching mode. When connected to an FS-Master, safety and standard non-safety communication is possible.

Level "c" corresponds to the SIO level of standard SDCI Master. In this case, the FS-Master supports an OSSDe mode besides communication (Pin 1, 3, 4 and 2).

Table 1 shows the pin layout and possible operational modes for the feature levels "a" to "c" of the port class A FS-Device and FS-Master.

⁸ FS-Devices are based on electronics and not on relays. Thus, the electronic version OSSDe is considered.

Table 1 – Operational modes of feature level "a" to "c" (port class A)

Feature level	FS-Device		FS-Master	
	Pin 2	Pin 4	Pin 2	Pin 4
"a"	- NC, DI, DO	- DI, DO - SDCI - SDCI + SDCI-FS	- NC, DI, DO	- DI, DO - SDCI - SDCI + SDCI-FS
"b"	- NC, DI, DO - OSSD2e	- DI, DO - OSSD1e - SDCI - SDCI + SDCI-FS	- NC, DI, DO	- DI, DO - SDCI - SDCI + SDCI-FS
"c"	- NC, DI, DO - OSSD2e	- DI, DO - OSSD1e - SDCI - SDCI + SDCI-FS	- NC, DI, DO - FS-DI2	- DI, DO - FS-DI1 - SDCI - SDCI + SDCI-FS

Figure 10 shows the optimized OSSDe commissioning with FS-Masters:

- No filter adjustments due to fixed maximum test pulse length of 1 ms according to type C and class 1 in [7], and
- No discrepancy time adjustments due to fixed maximum discrepancy.

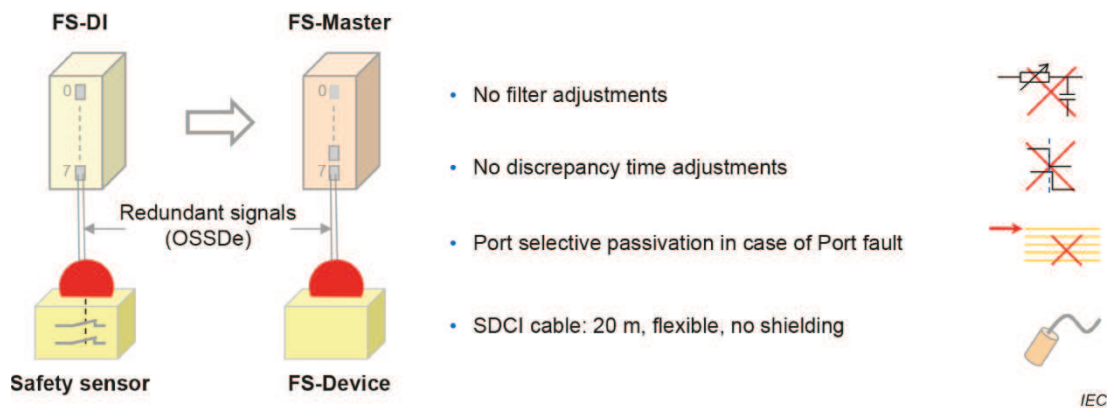


Figure 10 – Optimized OSSDe commissioning with FS-Master

4.1.5 Port class B

A Port class B provides for an extra 24 V power supply for actuators supplementing the main 24 V power supply of SDCI. See IEC 61131-9 for constraints on this extra power supply especially the requirement for electrical isolation of Power 2 from Power 1.

Figure 11 shows the pin layout, signal, and power supply assignment as well as the internal switch for L+.

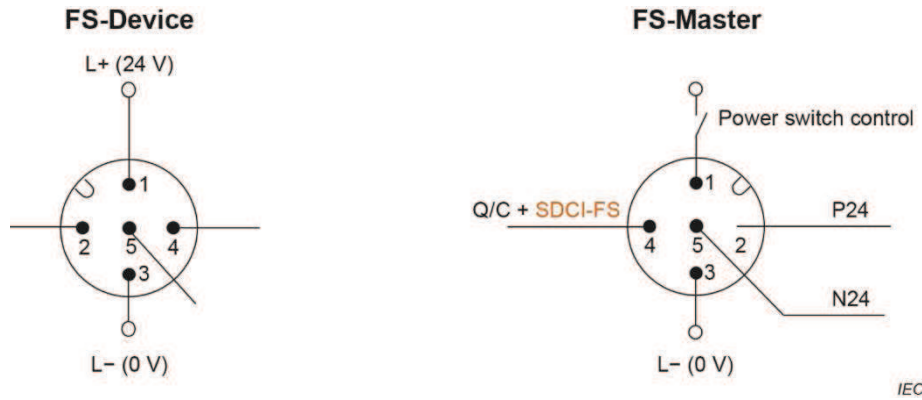


Figure 11 – Level "d" of an FS-Master (Class B)

4.1.6 "USB-Master" with safety parameterization

It is possible to use upgraded "USB-Masters" for off-site configuration, parameterization and test as shown in Figure 12.

Due to functional safety requirements, it will be necessary to extend the Master-Tool software for the functional safe configuration and parameterization of the FS-Device technology (FST-Parameters). See F.4.1 for use case.

Table 2 shows the device types that can be supported by such a "USB-Master".

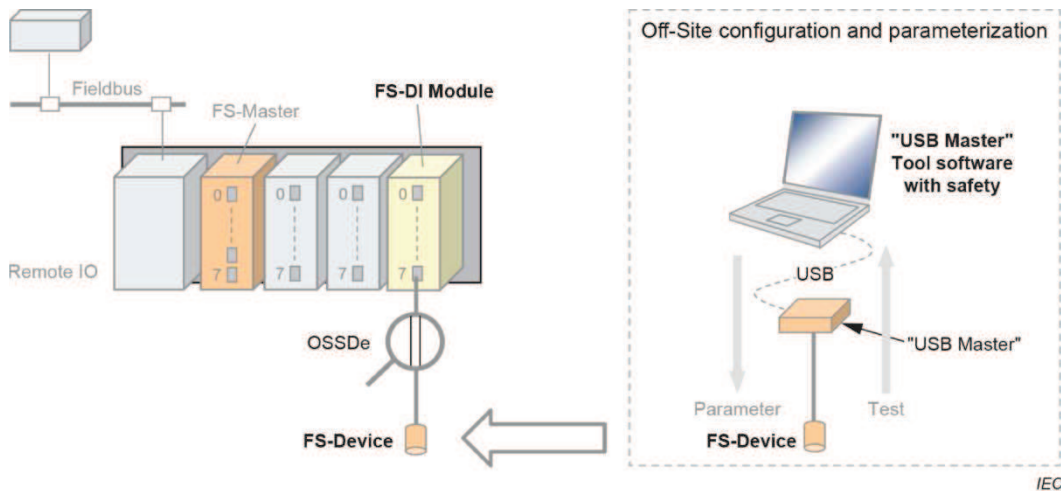


Figure 12 – Off-site configuration and parameterization

4.1.7 Interoperability matrix of safety devices

Table 2 provides an overview of typical safety sensors and actuators and their interoperability with FS-Masters of different feature levels, a "USB-Master" upgraded to safety parameterization, and conventional FS-DI modules connected to FSCPs.

Table 2 – Interoperability matrix of safety devices

Device type	FS-Master			"USB-Master" with safety parameteri- zation	FS-DI module (FSCP)
	Communi- cation	OSSDe tolerated	OSSDe supported		
	"a"	"b"	"c"		
Sensor with OSSDe ^a	-	-	OSSDe	-	OSSDe
Sensor with OSSDe and SDCI	-	-	OSSDe	SDCI ^b	OSSDe
Sensor with OSSDe and SDCI-FS	SDCI-FS	SDCI-FS	OSSDe or SDCI-FS	SDCI	OSSDe
Sensor with SDCI-FS communication only, e.g. light curtain	SDCI-FS	SDCI-FS	SDCI-FS	SDCI	-
Sensor with OSSDm, e.g. E-Stop	-	-	-	-	OSSDm
Actuator with SDCI-FS, e.g. 400 V power drive, low voltage switch gear	SDCI-FS	SDCI-FS	SDCI-FS	SDCI	-
Key SDCI-FS = SR and NSR data exchange ^a Pin layout according to [8]. ^b Pin layout may differ		USB = Universal Serial Bus, currently the most common interface amongst possible others for offsite parameterization tools due to fast communication combined with power supply			

4.2 Positioning within the automation hierarchy

Figure 13 shows the positioning of SDCI-FS within the automation hierarchy.

Classic safety is relay based and thus seemed to be straightforward, easily manageable, and reliable. However, the same criteria that led to the success of fieldbuses, led to the success of functional safety communication profiles (FSCP) on top of the fieldbuses also: reduced wiring, variable parameterization, detailed diagnosis, and more flexibility. SDCI is the perfect complement to the fieldbus communication and bridges the gap to the lowest cost sensors and actuators. It not only provides communication, but power supply on the same flexible and unshielded cable. One type of sensor can be used in the traditional switching mode or in the coded switching mode (communication).

SDCI-FS follows exactly this paradigm with its OSSDe.

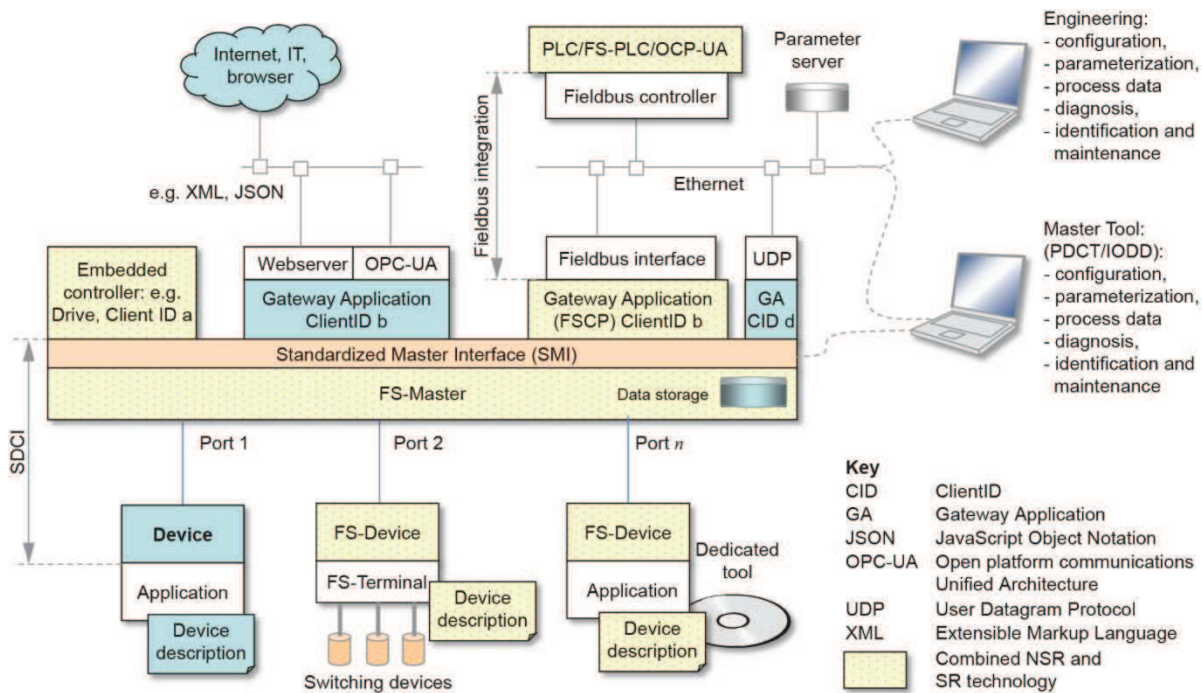


Figure 13 – SDCI-FS within the automation hierarchy

It aims for two main application areas. One is building up safety functions across the SDCI-FS communications and the functional safety communications across fieldbuses. The other builds up safety functions "locally" between an "embedded" safety controller and safety sensors/actuators using SDCI-FS communication.

SDCI-FS allows for building up power saving FS-Devices ("green-line"), for self-testing safety sensors in order to avoid yearly testing, for the reduction of interface types (e.g. 0 V to 10 V, 4 mA to 20 mA, etc.), and for robust and reliable transmission of safety information.

Finally, it is a precondition for new automation concepts such as Industry 4.0 or the Internet-of-Things (IoT).

4.3 Wiring, connectors, and power supply

Port class A types (3 to 4 wires): Cables and connectors as specified in IEC 61131-9 for Class A can be used for SDCI-FS also. However, due to the higher permitted power supply current of up to 1000 mA per Port, the overall loop resistance RL_{eff} can only be 1,2 Ohm. No shielding is required.

Port class B types (5 wires): Cable, wire gauges, shielding, maximum switched currents, interference, signal levels, etc. are not specified within this document.

4.4 Relationship to SDCI

The SDCI communication and its SIO mode are used as the base vehicle ("black channel") for SDCI-FS. Besides SDCI-FS, any FS-Master Port can also be configured for standard SDCI operation.

The independent signal inputs of the SIO mode on Pin 2 and Pin 4 are scanned by an FS-Master simultaneously to achieve an OSSDe interface. The result is propagated to the upper-level safety system as one safety signal. A new Safety Layer Manager supports this feature.

Another new Port configuration mode enables the SDCI-FS communication. Standard state machines are slightly extended to support

- detection of a Ready pulse from the FS-Device on Pin 4;

- power supply (Pin 1) switching OFF/ON in case an FS-Device missed the Wake-up sequence and started its OSSDe operation;
- transmission of functional safety protocol parameters (FSP) during PREOPERATE from FS-Master to the FS-Device;
- activation of the SDCI-FS communication layer (SCL);
- activation of the FS Process Data Exchange within the Safety Layer Manager.

4.5 Communication features and interfaces

FS Process Data from and to an FS-Device are always packed into a safety code envelop consisting of the port number, a safety PDU counter, protocol Control/Status information, and a 16/32-bit CRC signature. The minimum safety PDU size is 4 octets in case of no FS Process Data. SDCI-FS uses M-Sequence TYPE_2_V.

Only a subset of the SDCI data types is permitted: Boolean (packed as record), IntegerT(16), and IntegerT(32).

Parameterization within the domain of safety for machinery requires a "Dedicated Tool" per FS-Device or FS-Device family. The Device Tool Interface (DTI) based on proven technology has been chosen for the links between FS-Master Tool, FS-Device, and its "Dedicated Tool". The FS-Master Tool shall provide communication means for a "Dedicated Tool" to allow for the transmission of safety technology parameters (FST parameters) to and from an FS-Device. The "Dedicated Tool" and the FS-Device are both responsible for sufficient means to secure the transmitted data, for example via CRC signature or read-back.

4.6 Parameterization

SDCI-FS comprises a three-tier concept. The first tier is IODD based and contains all basic non-safety parameters for a Device or FS-Device.

The second tier requires an extension of the IODD for the fixed set of protocol parameters (FSP). These parameters are safety-related and secured via CRC signature against unintended changes of the IODD file. The interpreter of the FS-Master Tool provides a safety-related extension for the handling of the FSP parameters. Usually, the FS-Master Tool is able to determine and suggest the FSP parameter assignments (instance values) automatically and thus relieves the user from assigning these values initially. He can check the plausibility of the values and modify them if required.

The third tier deals with technology specific safety parameters (FST) of an FS-Device. SDCI-FS classifies two types of FS-Devices. Type "basic" requires only a few orthogonal FST parameters, whereas type "complex" can have a number of FST parameters requiring business rules and verification or validation wizards. Usually, the latter comes already with existing PC software ("Dedicated Tool") used for several functional safety communication profiles for fieldbuses.

The FST parameters for type "basic" are coded as any non-safety parameter within the IODD. They can be modified and downloaded to the FS-Device as usual. However, a diverse second path allows for checking these assignments for correctness. At the end of a parameterization session, the user launches a safety-related "Dedicated Tool" (FS-IOPD) for the calculation of a CRC signature across all FST instance values provided by the FS-Master Tool.

For both types of FS-Devices, the "Dedicated Tool" presents a CRC signature, which the user can copy into one of the FSP parameters. Upon reception of the FSP parameters at start-up, the FS-Device calculates a CRC signature across the locally stored instance values and compares it with the received CRC signature.

This method is used also for the check after using the SDCI Data Storage mechanism.

4.7 Role of FS-Master and FS-Gateway

The role of the FS-Master is extended to safe monitoring of Process Data, transferred to and from FS-Devices with respect to timeliness, authenticity, and data integrity according to IEC 61784-3:2021. Concerning authenticity, it uses the authenticity code assigned to the FS-Master by the upper-level FSCP system and the

port number. This prevents from local port related misconnections and misconnections whenever several FS-Masters are located side by side.

An FS-Master can be equipped by a safety controller, for example according to IEC 61131-6, or vice versa, and thus build-up a stand-alone safety system with its own complete safety functions.

With the help of an FS-Gateway in conjunction with the FS-Master, safety functions can be build-up across the upper-level FSCP system using the safety sensors and actuators connected to the FS-Master.

4.8 Mapping to upper-level systems

Specification of the mapping to an upper-level FSCP system is the responsibility of the fieldbus organization. SDCI-FS made provisions to meet the majority of FSCPs for example via reduced number of data types, descriptions of safety IO data, port selective passivation, and operator acknowledgment signals to prevent from automatic restart of machines.

4.9 Structure of the document

The structure of this document complies mostly with the structure of IEC 61131-9. Clause 5 specifies the extensions to the Physical Layer (PL), mainly the OSSDe issues, the wake-up behavior, and the additional Port modes. Extensions to SIO are specified in Clause 6, those to data link layer (DL) in Clause 7, those to system management (SM) in Clause 8, those to the FS-Device in Clause 9, and those to the FS-Master in Clause 10.

The core part of this document is the safety communication layer (SCL) in Clause 11. It comprises the SCL services, protocol, state machines, and management. In addition, it deals with integrity measures, with protocol (FSP) and technology (FST) parameters, with the integration of "Dedicated Tools" via Device Tool Interface (DTI) technology, with port selective passivation, and with SCL diagnosis. Clause 12 complements the core part by functional safety processing either through mapping to the upper-level system or local.

Extensions to parameters and commands are specified in Annex A, those to EventCodes in Annex B, and those to data types in Annex C. CRC polynomial issues are presented in Annex D, the IODD aspects in Annex E, the Device Tool Interface technology in Annex F, main scenarios in Annex G, and the system requirements in Annex H. Annex I provides information on test and assessment. Annexes A, C, D, and E are safety related.

5 Extensions to the Physical Layer (PL)

5.1 Overview

Figure 14 shows the adapted physical layer of an FS-Master (class A).

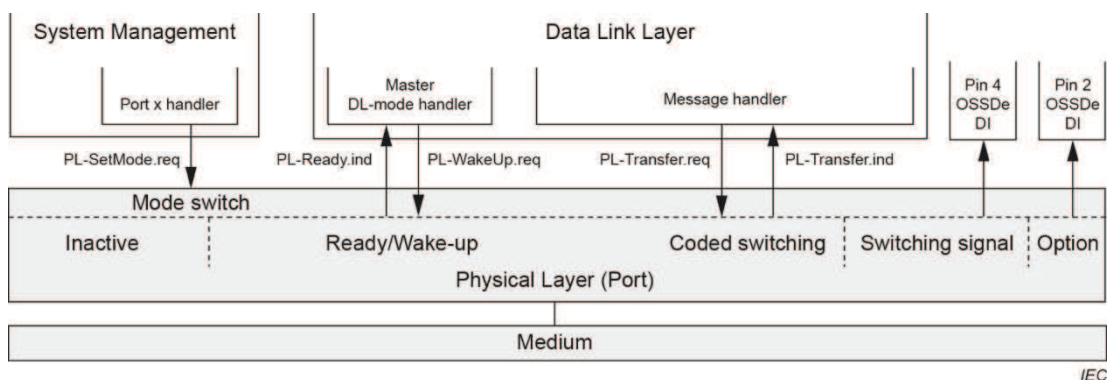


Figure 14 – The SDCI physical layer of an FS-Master (class A)

Pins 2 and 4 shall be scanned simultaneously to achieve OSSDe functionality. The FS-Master shall scan the C/Q line for the Ready signal of the FS-Device (see A.2.11).