IO-Link safety

# IO-Link Safety Systembeschreibung

## Technologie und Anwendung

# Inhaltsverzeichnis



# Abbildungsverzeichnis

# Einführung

Dieses Dokument soll einen Überblick verschaffen über die Leistungsfähigkeit und die Grenzen von IO-Link Safety. Es richtet sich an

- Manager,
- Designer,
- Entwickler und
- Integratoren

von Automatisierungssystemen, die eine Risikoabsicherung mittels funktional sicherer Einrichtungen benötigen.

IO-Link Safety setzt auf die IO-Link Technologie, standardisiert in der IEC 61131-9. Diese spezifiziert eine digitale Einpunkt-Schnittstelle (SDCI) für Sensoren, Aktuatoren und Mechatronik. Sie erweitert dabei die traditionellen Schaltein- und ausgänge, wie sie in der IEC 61131-2 definiert sind, um eine Punkt-zu-Punkt-Kommunikationsverbindung mittels codiertem Schalten. Diese Technologie erlaubt zyklischen Austausch von digitalen Ein-/Ausgabeprozessdaten wie auch azyklischen Transfer von Parametern und Diagnoseinformationen zwischen einem „Master" und seinen angeschlossenen „Devices". Ein Master kann über Gateway mit übergeordneten Systemen gekoppelt werden, z.B. einem Feldbus mit programmierbaren Steuerungen.

Hauptvorteile von IO-Link als „Black Channel" für sichere Kommunikation sind

- Geringe Kosten und kleinste Abmessungen
- Keine speziellen ASICs
- Jedes Device mit nur einer Schnittstelle
- Robuste digitale Kommunikation
- Gateways zu allen Feldbussen
- Einheitliches Engineering der Devices

IO-Link ist Voraussetzung für Industrie 4.0 und das Internet-der-Dinge. Es ist dabei, die klassische Aufteilung in Sensorik und Aktorik auf der untersten Automatisierungsebene in Richtung Mechatronik-Einheiten mit integrierten Sensoren und Aktuatoren zu ergänzen.

IO-Link Safety ist eine Erweiterung von IO-Link, indem es eine zusätzliche Sicherheitskommunikationsschicht auf der Master- wie auch auf der Deviceseite vorsieht, die dadurch zum „FS-Master" und „FS-Device" werden. Das Konzept wurde durch TÜV-SÜD erfolgreich geprüft.

Die Technologien werden durch die internationale „IO-Link Community" gefördert. Weitere Information und die „IO-Link Safety"-Spezifikation sind auf www.io-link.com verfügbar.

# 1 Sicherheit in der Automation

Funktional sichere Kommunikation in der Automation hat sich nun seit mehr als 20 Jahren bewährt und für Feldbusse wurden mehrere Profile - FSCP genannt - standardisiert in der IEC 61784-3-x-Serie (www.iec.ch).

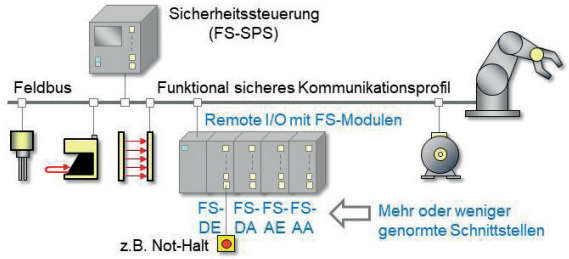


**Abb. 1: FS-Kommunikation**

Sicherheitsfunktionen gemäß IEC 62061 oder ISO 13849-1 (www.iso.ch) werden üblicherweise realisiert durch Sicherheitssensoren wie Lichtgitter, Sicherheitssteuerung FS-SPS und Sicherheitsaktuator wie Antrieb oder Stellglied. Diese Geräte tauschen Sicherheitsdaten unter Nutzung eines FSCP aus.

Abbildung 1 zeigt darüberhinaus funktional sichere Module wie FS-DE in einer „Remote I/O", die den Anschluss elektronischer Sicherheitsgeräte über redundante Signale, sogenannte OSSD („output switching sensing device") ermöglichen. Einfache elektromechanische Geräte wie Not-Halt-Taster können ebenfalls an solchen FS-DE betrieben werden.

Andere Modultypen wie FS-DA ermöglichen zum Beispiel das Abschalten von Relais. Funktional sichere Analogeingangsmodule (FS-AE) werden für den Anschluss von messenden Sensoren genutzt, wie in Abbildung 2 gezeigt.

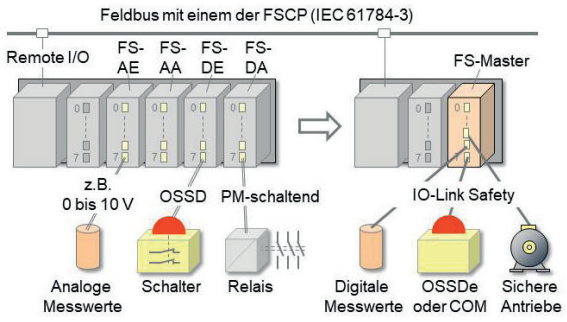


**Abb. 2: Remote I/O**

Es gibt mehrere mehr oder weniger standardisierte Schnittstellen für diese Modultypen und Geräteher-steller können einen Typ eines Sicherheitsgerätes weltweit für den Betrieb an Remote I/O liefern.

# 2 Warum „IO-Link Safety"?

Im Falle einer Innovation ihrer Sicherheitsgeräte überlegen sich die Hersteller unter anderem zwei strategische Aspekte:

- Microcontroller werden laufend günstiger und neue Funktionen könnten in ein Produkt eingebracht werden. Schnittstellen wie OSSD unterstützen dies jedoch nicht.
- Ein FSCP könnte die Lösung sein. Da das Gerät aber weltweit zum Einsatz kommen soll, müssten gemäß Abbildung 3 mehrere FSCP implementiert und betreut werden.

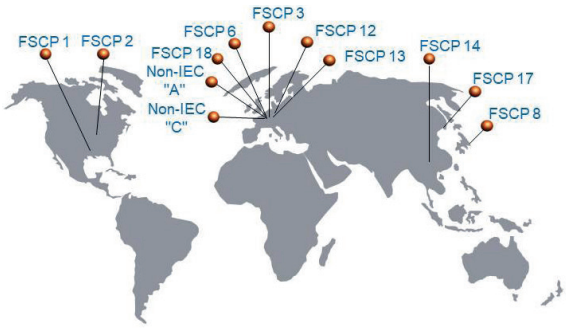


**Abb. 3: FSCP-Welt**

Das „Tunneln" eines der FSCP-Protokolle über IO-Link hilft da auch nicht, weil wiederum mehrere FSCP implementiert und betreut werden müssten.

Eine separate, auf die Bedürfnisse zugeschnittene IO-Link Safety Kommunikation pro FS-Device-Typ, wie in Abbildung 4 dargestellt, ist die Lösung für diese Hersteller.

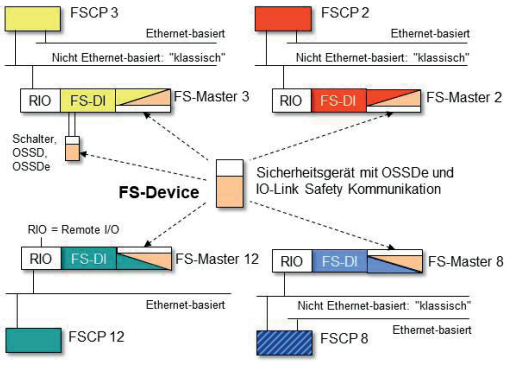


**Abb. 4: Ein-Plattform-Lösung**

Da IO-Link Safety auch eine standardisierte OSSD-Schnittstelle (OSSDe) vorsieht, kann solch ein FS-Device an klassischen FS-DE-Modulen eingesetzt und dadurch Typenvielfalt vermieden werden. Selbstverständlich muss es mindestens einen FS-Master samt Gateway „x" geben, um das FS-Device in der jeweiligen FSCP-Domäne „x" einsetzen zu können.

IO-Link Safety ist wichtig für kompakte Remote I/O, da ein FS-Master den Betrieb von beliebigen FS-Device-Ausprägungen, sei es Sensor, Aktuator oder komplexe Mechatronik, an jedem seiner Ports erlaubt, wie in Abbildung 2 rechts dargestellt.

Dies ermöglicht neue Sicherheitsanwendungen, z.B. lokale Sicherheitslogik im FS-Master in Verbindung mit Sicherheitsfunktionen in übergeordneten Systemen.

Weiterhin vereinfacht die Übertragungsmöglichkeit von sicherheits- und nicht-sicherheitsbezogenen Daten z.B. Bediengeräte mit Not-Halt.

Die Punkt-zu-Punkt-Kommunikation von IO-Link Safety senkt den gesamten Aufwand für den Kunden in erheblichem Maße (siehe Kapitel 4).

# 3 IO-Link als „Black Channel"

## 3.1 Prinzip

Die meisten FSCP folgen dem „Black Channel"-Prinzip. Ein existierender Feldbus wird als Übertragungskanal für einen speziellen Typ von Nachrichten aus Sicherheitsdaten und einem zusätzlichen Sicherungscode genutzt. Zweck des Sicherungscodes ist die Reduzierung der Restfehlerwahrscheinlichkeit für die Datenübertragung auf das von relevanten Sicherheitsnormen wie IEC 61784-3 geforderte Maß oder besser. Die Bearbeitung der Nachrichten erfolgt in einer Sicherheitskommunikationsschicht (SCL) auf dem Feldbus.

IO-Link Safety folgt ebenfalls diesem Prinzip, wie in Abbildung 5 gezeigt.

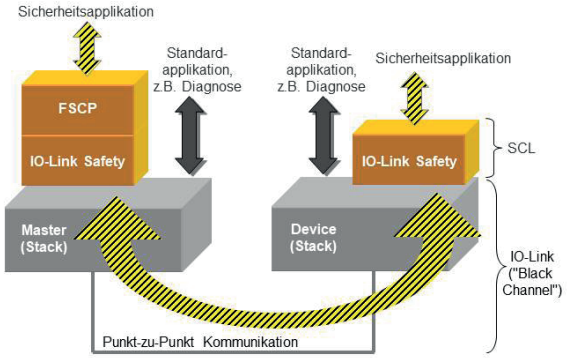


**Abb. 5: „Black Channel"-Prinzip**

Die IO-Link SCL befinden sich oberhalb der FS-Device- und FS-Master-Stacks. Der Austausch von Sicherheitsprozessdaten mit dem übergeordneten FSCP-System findet im Gateway auf FS-Masterseite statt. In der Regel können SCL-Instanzen, Gateway und FSCP-Schicht in einer Einheit mit redundanten Microcontrollern implementiert werden.

## 3.2 Voraussetzungen

IO-Link erfüllt die Anforderung des zyklischen Datenaustauschs und die 1:1-Beziehung zwischen Sender und Empfänger durch die Punkt-zu-Punktverbindung. Speichernde Netzwerkelemente und Funkstrecken zwischen FS-Masterport und FS-Device sind nicht zulässig.

FS-Devices benötigen nach dem Einschalten wegen der Selbsttests meist mehr als die maximale Zeit bis zur „Wake-up"-Bereitschaft. IO-Link wurde daher leicht modifiziert und der FS-Master verzögert die „Wake-up"-Prozedur bis das FS-Device bereit ist. („Ready"-Puls).

Bei jedem Port-Hochlauf sendet der FS-Master einen „Verify Record", damit das FS-Device die Korrektheit der gespeicherten Parameter, die Authentizität (FSCP, Portnummer) und die E/A-Datenstruktur überprüfen kann.

IO-Link Safety ist daher in der Lage, den „Data Storage"-Mechanismus von IO-Link unverändert zu nutzen. Defekte FS-Devices können ohne Tool-Einsatz getauscht werden.

Der FS-Master kann die Portversorgung aus- und einschalten, um eventuelle Blockaden bei OSSD-Betrieb wieder aufzuheben.

## 3.3 OSSDe und SIO

IO-Link Safety spezifiziert die zweite Signalleitung von IO-Link („Pin 2") für redundanten Signalbetrieb zusammen mit der Hauptsignalleitung („Pin 4"). Diese standardisierte Version wird OSSDe genannt und ist in Abbildung 6 dargestellt.

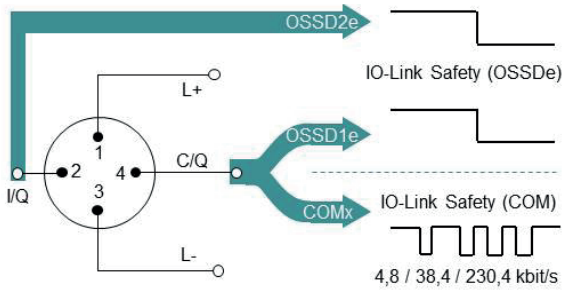


**Abb. 6: „Port"-Erweiterung**

Die sichere Kommunikation nutzt nur die Hauptsignalleitung und läuft mit allen drei Übertragungsraten COM1, COM2 und COM3.

# 4 „IO-Link Safety"-Kommunikation

## 4.1 Sicherheitsziele

Die Restfehlerrate ist für drei Hauptmerkmale der sicheren Kommunikation zu bestimmen:

- Aktualität (Daten kommen rechtzeitig an),
- Authentizität (Daten vom richtigen Sender),
- Integrität (Daten aktuell und korrekt).

Zahlreiche Fehler können auftreten bei der Nachrichtenübertragung zwischen FS-Master und FS-Device wie z.B. Verlust, Verzögerung, Verfälschung, etc. IEC 61784-3 ist eine Informationsquelle hierfür und wie man Restfehlerwahrscheinlichkeiten unter bestimmten Bedingungen berechnet. Die nachfolgenden Sicherheitsmaßnahmen sind so gewählt, dass die Restfehlerwahrscheinlichkeit für die Übertragung auf das von relevanten Normen wie IEC 61784-3 geforderte Maß oder besser verringert wird. IO-Link Safety Kommunikation ist daher einsetzbar für Sicherheitsfunktionen bis SIL 3 oder PL e.

## 4.2 Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen sind u.a.:

- Nummerierung der Nachrichten zwischen FS-Master und FS-Device. Der FS-Master nutzt einen zyklischen 3-bit Zähler. Das FS-Device hat seinen eigenen Zähler, synchronisiert beim Protokollstart. Es antwortet mit einem 1er Komplementwert.
- Zeiterwartung mit Quittung mittels „Watchdog", der bei jedem Eintreffen einer IO-Link Safety Nachricht mit einem neuen Zählwert aufgezogen wird.
- Authentifizierung bei Protokollstart: FS-Device ist mit dem korrekten FS-Master (eindeutige FSCP-Verbindungs-ID) und korrektem FS-Masterport („PortNum") verbunden. Zyklisch wird lediglich „PortNum" geprüft.
- CRC-Signatur (Cyclic Redundancy Check) über Prozessdaten und Sicherungscode.

IO-Link Safety nutzt die sogenannte explizite Übertragung von Sicherungsmaßnahmen.

## 4.3 Formate und Datentypen

Nachrichten vom FS-Master und vom FS-Device sind in Abbildung 7 dargestellt. Sie bestehen aus 2 Teilen. Der erste Teil mit 4 Abschnitten beinhaltet die „Safety-Protocol-Data-Unit" (SPDU) und der letzte die optionalen nicht-sicherheitsbezogenen Prozessdaten.

Im ersten Abschnitt befinden sich je nach Übertragungsrichtung sichere Ein- oder Ausgabedaten: FS-PDaus/FS-PDein. Sie können als BooleanT (Bits), IntegerT(16), oder IntegerT(32) codiert sein. Höchstwertige Octets und/oder Bits werden zuerst gesendet. Füllbits sind „0".

Vom FS-Master zum FS-Device

| Ausgabe PD | CRC-Signatur | Steuer-Byte | PortNum | FS-PDaus |
|---|---|---|---|---|
| | Signatur über FS-PDaus, PortNum, und Steuern & Zählen | enthält 3-Bit-Zähler | FS-Master Port-nummer | 0 bis 3 Octet/ 0 bis 25 Octet |
| 32 bis 0 Octet | 2/4 Octet | 1 Octet | 1 Octet | 3/25 Octet |

Vom FS-Device zum FS-Master

| FS-PDein | PortNum | Status-Byte | CRC-Signatur | Eingangs PD |
|---|---|---|---|---|
| 0 bis 3 Octet/ 0 to 25 Octet | Port-nummer, invertiert | enthält 3-Bit-Zähler, invertiert | Signatur über FS-PDein, PortNum und Status & Zählen | |
| 3/25 Octet | 1 Octet | 1 Octet | 2/4 Octet | 32 bis 0 Octet |

**Abb. 7: Nachrichten mit „Safety-PDU"**

IO-Link Safety kennt zwei Formate. Eines ist gedacht für kurze Prozessdaten wie Bits von Abschaltvorgängen, die schnelle Verarbeitung benötigen. Dafür stehen maximal 3 Octet zur Verfügung. Das andere ist gedacht für längere Prozessdaten wie Mess- und Stellwerte. Dafür stehen maximal 25 Octet zur Verfügung.

Die nächsten drei Abschnitte enthalten den sogenannten Sicherheitscode. Hier steht im ersten (1 Octet) die Portnummer, die der FS-Master kennt bzw. eine, die das FS-Device während der Inbetriebnahme erhielt.

Im zweiten Abschnitt (1 Octet) des Sicherungscodes stehen Steuer- bzw. Statusbits, um die Protokollaktivitäten zu beeinflussen und zu synchronisieren, sowie 3-Bit zyklische Zählerwerte.

Im dritten Abschnitt des Sicherungscodes steht eine CRC-Signatur. Für die kurzen SPDUs reicht eine 16 Bit CRC-Signatur (2 Octets), für längere eine 32 Bit CRC-Signatur (4 Octets).

## 4.4 Dienste

Sender und Empfänger von SPDUs befinden sich in Schichten oberhalb des „Black Channel"-Kommunikations-Stacks wie in den Abbildungen 5 und 8 gezeigt. Hauptbestandteile der Schicht sind als Zustandsmaschinen spezifiziert. Sie steuern die reguläre zyklische Bearbeitung von SPDUs und die

Ausnahmefälle wie z.B. Hochlauf, Spannung aus/ein und CRC-Fehler. Abbildung 8 illustriert, wie der SCL mit dem Technologieteil im FS-Device, bzw. die SCL-Instanzen mit dem FSCP-Gateway im FS-Master interagieren.

Die wichtigsten Dienste im FS-Master sorgen für den Austausch von FS-PDaus und FS-PDein. Während des Hochlaufs oder im Fehlerfall werden die aktuellen Prozessdaten durch sichere Daten (SDaus, SDein) ersetzt. Die Ersatzwerte sind alle „0", um den Empfänger in den sicheren Zustand zu versetzen, z.B. Abschalten.

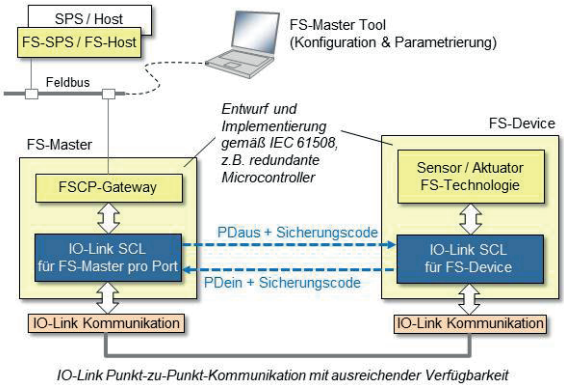


**Abb. 8: SCL-Kommunikationsschicht**

Sollte der sichere Zustand nicht Abschalten sein, sondern z.B. langsame Drehzahl, dann verfügt IO-Link Safety über einen zusätzlichen Dienst in Form eines „Flags" im Control-Byte („Aktiviere sicheren Zustand"). Im Gegenzug kann ein FS-Device den Empfänger über ein „Flag" über den eingenommenen sicheren Zustand informieren („Sicherer Zustand aktiv").

IO-Link Safety Kommunikationsfehler zwingen den SCL im FS-Master (Abbildung 8) in den sicheren Zustand. Eine Sicherheitsfunktion darf in solch einem Fall nicht automatisch ohne menschlichen Eingriff wieder „entriegelt" werden. Ein Dienst informiert den FSCP über ausstehende Eingriffe und Bestätigungen des Personals („…AckReq…"). Das FS-Device erhält diesen Dienst optional ebenfalls zwecks Zustandsanzeige, z.B. LED. Eine Bestätigung gelangt über den FSCP zum FS-Master SCL („…Ack…").

Die Dienste der FS-Device-Technologie beinhalten den Austausch von FS-PDein und FS-PDaus, die Möglichkeit sichere Daten (SD) zu aktivieren bzw. zu melden und die bereits erwähnte Bedienaufforderung zwecks Anzeige.

Die Dauer einer Anforderung eines FS-Devices muss lange genug sein, um auch wirklich durch sämtliche Kommunikationsstrecken durchzukommen (mindestens 2 Zählerinkremente). Ein spezieller Dienst informiert die Technologie über den Zählerwert, um Implementierungen zu erleichtern.

Diagnosen des FS-Device SCL gelangen über den „SCL Fault"-Dienst zur Technologie.

## 4.5 Protokollparameter

Protokollparameter in IO-Link Safety tragen das Präfix „FSP_" oder „FSCP_", wenn es um die FS-Master-Authentifizierung geht. Zweck dieser Parameter ist die Adaption des SCL-Verhaltens an jeweilige Anwendungsanforderungen und um Einstellungen zu prüfen. Sie alle sind auf drei Indizes in Records aufgeteilt.

Der *Authentizitäts-Record* besteht aus:

- FSCP_Authenticity1/2
- FSP_Port
- FSP_AuthentCRC

Der Erste enthält die Verbindungs-ID des FS-Masters als Teilnehmer im FSCP-Netz. Ein FS-Device ist dadurch in der Lage, Fehlverbindungen an einen FS-Master aufzudecken.

Der Zweite trägt die Portnummer und ermöglicht die Prüfung des korrekten FS-Master-Ports.

Der Dritte enthält die CRC-Signatur zur Sicherung korrekter Werte.

Der *Protokoll-Record* besteht aus:

- FSP_ProtVersion
- FSP_ProtMode
- FSP_Watchdog
- FSP_IO_StructCRC
- FSP_TechParCRC
- FSP_ProtParCRC

FSP_ProtVersion führt die eingestellte Protokoll-Version. FSP_ProtMode legt kurze oder lange SPDU fest. FSP_Watchdog liefert die Anzahl von Millisekunden für die Überwachung der Zeit bis zum Eintreffen der nächsten gültigen SPDU.

FSP_IO_StructCRC liefert die Signatur über die Prozessdatenbeschreibung des FS-Device.

FSP_TechParCRC hält die Signatur über die Technologie-Parameter des FS-Device bereit (siehe Kapitel 6).

Die Signatur in FSP_ProtParCRC sichert die Werte im Protokoll-Record.

Die Werte im *Verifikations-Record* (FSP_Verify-Record) dienen als verborgenes diversitäres Verifikationsmittel für alle Parameter während des FS-Device-Anlaufs. Dieser Mechanismus ist unsichtbar für den Anwender (siehe Kapitel 5 und Abbildung 9).

Protokollparameter werden während der Inbetriebnahme mit Hilfe eines FS-Master-Tools und einer IODD mit zusätzlichen Sicherheitsparametern des FS-Devices eingestellt. Einige Parameterwerte wie die der Authentifizierung und des FSP_TechParCRC sind während der Inbetriebnahme zwecks Entsperren und Sperren vorzubesetzen. Bei Inbetriebnahme wird durch Personal überwachter Betrieb vorausgesetzt.

# 5 Konfiguration & Verifikation

Abbildung 9 veranschaulicht die meisten Aktivitäten während des FS-Device-Anlaufs. Nach dem Einschalten und den Sicherheits-Selbsttests, die in der Regel länger dauern als das vorgegebene IO-Link-Limit, zeigt das FS-Device seine Bereitschaft zum „Wake-up" durch einen „Ready"-Puls an. Der FS-Master fängt an zu kommunizieren und nach dem Parameter-Check (Data Storage) sendet der FS-Master den Verifikations-Record zwecks Sicherheitsprüfung (siehe Kapitel 4.5).

FS-Master und FS-Device wechseln bei korrekter Authentifizierung und Parametrierung in den Zustand „zyklischer Prozessdatenaustausch" und automatisch fängt die Sicherheitskommunikationsschicht (SCL) an zu arbeiten.

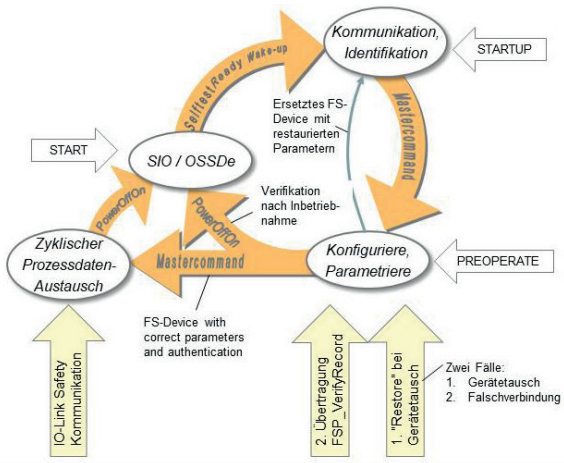


**Abb. 9: Hochlauf des FS-Devices**

IO-Link Safety beschreibt mehrere Szenarien neben dem obigen regulären Anlauf:

- OSSDe-Betrieb (siehe Kapitel 7)
- Inbetriebnahme - testen
- Inbetriebnahme - „scharf" schalten
- FS-Device-Gerätetausch
- Fehlverbindung konfigurierter FS-Devices

Sie alle sind in der IO-Link Safety Spezifikation festgelegt.

# 6 Technologieparameter

## 6.1 IODD

Die Gerätebeschreibung von IO-Link (IODD) ist der übliche Platz, wo Parameter und deren Bereichsgrenzen einer bestimmten FS-Device-Technologie wie z.B. Lichtgitter, Laserscanner, Näherungsschalter etc. beschrieben sind. Sie sollten das Präfix „FST_" tragen. Der Anwender weist mit Hilfe eines FS-Master-Tools während der Inbetriebnahme und des Testens Parameterwerte zu.

## 6.2 „Dedicated Tool"

Ein einfaches PC-Programm - „Dedicated Tool" - kommt mit dem FS-Device und seiner IODD. Seine Aufgabe besteht in der sicheren Berechnung einer CRC-Signatur über alle Technologie-Parameter. Das Ergebnis wird in den FSP_TechParCRC kopiert.

Das FS-Device vergleicht seine lokal berechnete Signatur mit der obigen Referenz-Signatur.

## 6.3 „Device Tool Interface" (DTI)

IO-Link Safety spezifiziert ein einfaches „Device Tool Interface" (DTI) für den Aufruf von Dedicated Tools und die Parameterübergabe.

## 6.4 Extern-Parametrierung

IO-Link kennt „USB-Master" für Extern-Parametrierung (off-site) und Test von Devices. Dies ist für FS-Devices auch möglich, wenn das zugehörige PC-Programm „Master Tool" zum „FS-Master Tool" hochgerüstet ist für IODDs mit Sicherheits-Protokollparametern.

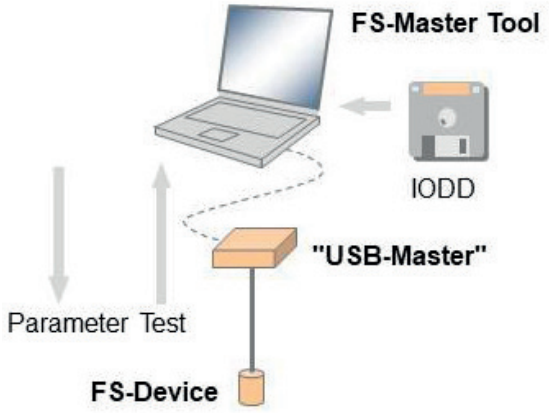


**Abb. 10: Extern-Parametrierung**

# 7 OSSDe-Betrieb

Für das in IO-Link Safety festgelegte und in Kapitel 3.3 gezeigte OSSDe für FS-Devices gelten folgende Annahmen:

- redundante und gleichschaltende Signale,
- erzeugt von elektronischen Ausgängen,
- auf 1000 µs begrenzte Testpulsdauer (Typ „C" und Klasse „1" in ZVEI-CB24I).

Diese Vereinfachungen sorgen für weniger Komplexität in den FS-Master-Ports oder FS-DI-Modulen, z.B. wegen fester Filterzeiten.

Es ist für Sicherheitsgeräte, die für FS-DI-Betrieb vorgesehen sind, möglich, eine eingebaute IO-Link Kommunikation ausschließlich für Parametrierzwecke zu benutzen. Es müssen dabei jedoch die IO-Link Community Regeln in Kapitel 10.1 beachtet werden.

# 8 Gateway zu FSCPs

## 8.1 Position von IO-Link Safety

Abbildung 11 zeigt, wie IO-Link Safety in die Automatisierungs- und IT-Technologie-Hierarchie eingebettet ist. Sicherheits-Gateways schließen „Functional Safety Communication Profiles" (FSCP) mit ein, sind aber nicht darauf begrenzt.

Lokale Steuerungen, wie z.B. in Antrieben, können die IO-Link Safety Technologie ebenfalls nutzen.

## 8.2 Einheitliche Masterschnittstelle

Die einheitliche Masterschnittstelle (SMI) ist eine neue Technologie bei IO-Link. Sie erleichtert Masterimplementierungen und ermöglicht es, Sicherheitskonzepte einfacher zu verstehen und zu begutachten.

Darüberhinaus bietet es die Voraussetzungen für den Tool-Zugriff auf Master unterschiedlicher Hersteller.

SMI spezifiziert Dienste für

- Master-Identifikation
- Konfigurationsmanagement (CM)
- Datenspeicherung (DS)
- Azyklische Kommunikation (Read/Write)
- Diagnose (Events)
- Prozess-Datenaustausch

Für IO-Link Safety sind die Dienste erweitert worden.

Dienste für CM sorgen für Zugangs-Autorisierung und den Verifikations-Record.

Dienste für azyklische Kommunikation bieten Portversorgung aus- und einschalten.

Dienste für Prozessdatenaustausch gibt es für SPDUs wie für nicht-sicherheitsbezogene Daten.

## 8.3 „Splitter/Composer"

Teile der Prozessdatenaustausch-Einheit sind der „Splitter" und der „Composer". Aufgabe des Splitters ist es, die SPDU aus der ankommenden Nachricht zu extrahieren.

Aufgabe des Composers ist es, die SPDU und nicht-sicherheitsbezogene Daten zu einer abgehenden Nachricht zusammenzusetzen.

In beiden Fällen wird der Wert-Status (Qualifier) berücksichtigt.

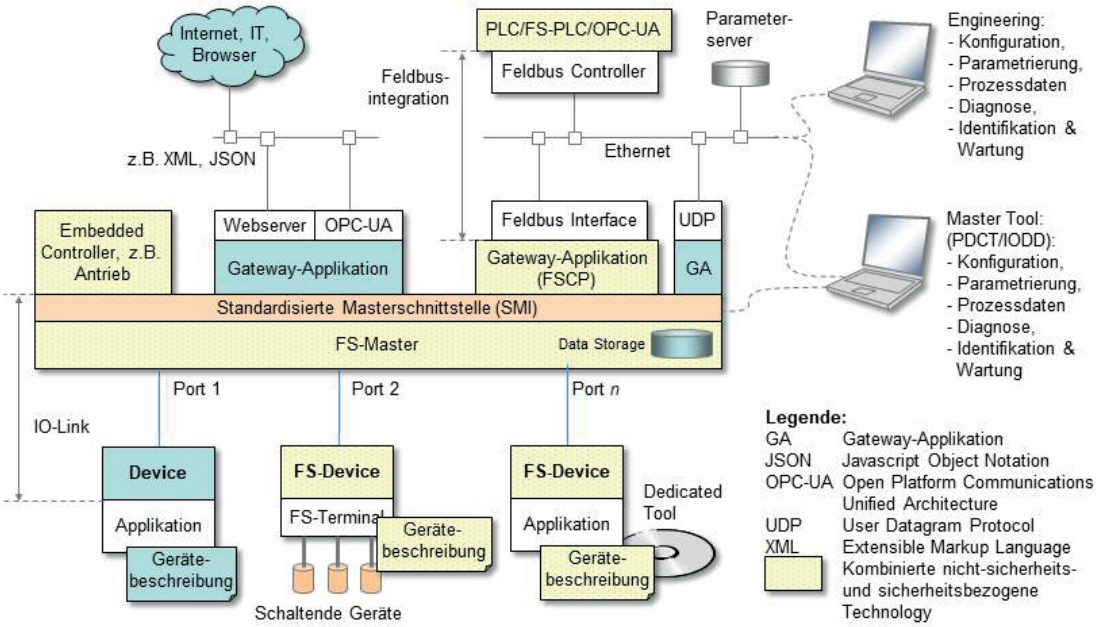


**Abb. 11: Position von IO-Link Safety**

## 8.4 Datenabbildung („Mapping")

Abbildung 12 zeigt vorbildhaft die Darstellung von sicherheits- und nicht-sicherheitsbezogenen Prozessdaten in Richtung FSCP bzw. zum virtuellen Feldbus-Remote I/O.

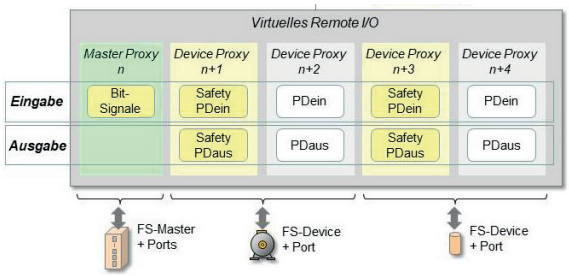


**Abb. 12: Musterbeispiel für Mapping**

Dieses Modell erlaubt die effiziente Abbildung von Bit-orientierten Datenstrukturen in eine FSCP-Nachricht ähnlich wie bei FS-DE-Modulen. Komplexere Datenstrukturen von FS-Devices lassen sich dann direkt auf separate FSCP-Nachrichten abbilden.

Das Modell zeigt auch, wie sich nicht-sicherheitsbezogene Daten und Diagnoseinformationen (Events) abbilden lassen.

## 8.5 Port-spezifische Passivierung

Bietet ein FSCP kanalgranulare Passivierung an, dann ist die port-spezifische Passivierung von IO-Link Safety zu berücksichtigen.

# 9 Geräteentwicklung

## 9.1 Technologiekomponenten

Neben der Möglichkeit, die IO-Link Safety Spezifikation selbst zu implementieren, gibt es auch am Markt erwerbbare Technologie-Komponenten. Die IO-Link Community wird keine universellen Entwicklungskits bereitstellen. Mitgliedsfirmen werden als Technologie-Provider Technologiekomponenten anbieten. Information hierzu ist verfügbar auf www.io-link.com oder in Workshops. Der Vorteil der Technologiekomponenten ist offensichtlich: Vorzertifizierte Software-Module mit Support und zusätzliche wertvolle Information, z.B. IODD-Design und Tools.

## 9.2 FS-Device

Selbst wenn IO-Link Safety für Sicherheitsfunktionen bis SIL 3 oder PL e einsetzbar ist, ist es nicht immer nötig, FS-Devices für diese Klassen zu entwerfen und zu implementieren.

IO-Link Safety schafft neue Möglichkeiten für FS-Devices und Anwendungen:

- Sensoren für Näherung, Dehnung, Moment, Druck, etc.
- Encoder
- Lichtgitter und Laserscanner
- Digitalkameras
- Not-Halt mit Selbsttest, um jährliche Inspektion zu vermeiden

- Bedienpanels
- Intelligente Greifer
- Niederspannungsschaltgeräte
- Motorstarter
- Intelligente Antriebe

### 9.3 FS-Master

Inzwischen sind etliche Firmen vertraut mit der Integration in Feldbusse, für die es FSCP-Entwicklungskits für Sicherheitsgeräte gibt. Damit ist die Integration von FS-Master-SCL-Stacks relativ einfach, wenn Sicherheitsentwicklungsprozesse bereits etabliert sind.

### 9.4 Test

Testspezifikation und Tester sind in Entwicklung. Testmuster für automatisierte Protokolltester wurden bereits aus den Protokollzustandsmaschinen generiert.

## 10 Prüfung und Zertifizierung

### 10.1 Grundsätze („Policy")

Um die IO-Link-Community vor möglichen Irrümern oder falschen Erwartungen und grober Fahrlässigkeit bei sicherheitsbezogenen Entwicklungen und Anwendungen zu schützen, ist Folgendes von jedem zu beachten, der sich mit IO-Link Safety beschäftigt, sei es ein Trainer, Berater, Designer, Implementierter oder Benutzer von IO-Link Safety Geräten:

- Jedes Nicht-Sicherheitsgerät taugt nicht automatisch für sicherheitsbezogene Anwendungen, wenn es IO-Link und eine Sicherheitskommunikationsschicht verwendet.
- Um ein Produkt für sicherheitsbezogene Anwendungen zu entwickeln, sind geeignete Entwicklungsprozesse nach Sicherheitsstandards einzurichten und/oder eine Zertifizierung bei einer entsprechenden Prüfstelle durchzuführen.
- Hersteller eines Sicherheitsproduktes sind verantwortlich für die korrekte Implementierung der Sicherheitskommunikationstechnologie (gemäß IEC 61508 oder ISO 13849-1) und die Richtigkeit und Vollständigkeit der Produktdokumentation und -information.
- Alle Angaben in den IO-Link-Spezifikationen schließen eine Haftung für die Richtigkeit und Vollständigkeit aus.
- Die Verwendung von IO-Link Markennamen und Bildmarken ist urheberrechtlich geschützt und bedarf einer besonderen Vereinbarung.

### 10.2 Sicherheitsprüfung

Sicherheitsprüfungen gemäß IEC 61508 oder ISO 13849-1 müssen durch Prüfstellen ausgeführt werden, wie z.B.:

- TÜV (weltweit)
- IFA (Deutschland)
- SP (Schweden)
- SUVA (Schweiz)
- HSE (Großbritannien)
- FM, UL (USA)

### 10.3 Zertifizierung

Die IO-Link-Testspezifikation bietet Information zu Test und Zertifizierung, sowie zur Erstellung von Herstellererklärungen.

### 10.4 EMV und E-Sicherheit

IEC 61000-6-7 enthält Anforderungen für die EMV-Prüfung von FS-Mastern und FS-Devices, für die keine Produktstandards existieren.

IEC 61010-2-201: 2017 enthält Anforderungen an die elektrische Sicherheit, insbesondere in Bezug auf SELV/PELV.

## 11 Anwendung

### 11.1 FSCP-Richtlinien

In der Regel bieten Feldbusorganisationen Planungs- und Installationsrichtlinien für Peripheriegeräte wie Remote I/O an. Sie enthalten auch IT-Sicherheitsrichtlinien oder beziehen sich auf die IEC 62443-Serie.

Für diese Richtlinien können im Falle von IO-Link Safety Anpassungen notwendig sein.

### 11.2 IO-Link-Richtlinien

Die IO-Link Community bietet eine Planungsrichtlinie, die von der Website www.io-link.com heruntergeladen werden kann.

# 12 Kundennutzen

## 12.1 IO-Link allgemein

Die Vorteile von IO-Link, gelistet in der „Einführung" und in der von www.io-link.com ladbaren „IO-Link Systembeschreibung", treffen auch auf IO-Link Safety zu.

Die Migrationsstrategie ist jedoch von OSSDe zu IO-Link Safety, anstatt von SIO zu IO-Link.

Abbildung 13 zeigt die wesentlichen Vorzüge von IO-Link Safety.

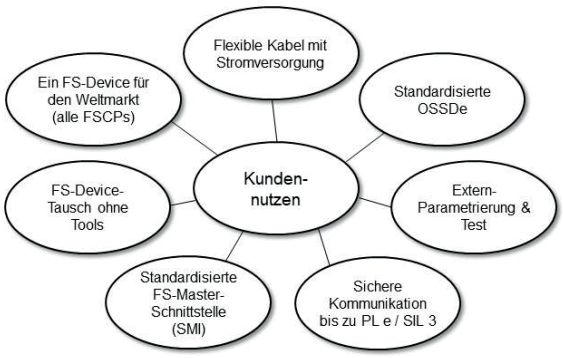


**Abb. 13: Kundennutzen**

Die Vorzüge für Gerätehersteller sind unter anderem:

- Standardtechnologie ohne Lizenzgebühr
- Ein Gerätetyp für FS-DI und FS-Master
- Bidirektionaler Austausch von FS-Daten
- Nicht-Sicherheits- und Sicherheitsdaten
- Vorverdrahtete Mechatronik-Module
- Integrierte Diagnostik unterstützt „Condition Monitoring" und „Predictive Maintenance"
- Verifizierungshilfe durch Authentifizierung
- Vereinfachtes Engineering über IODD und „Dedicated Tool"
- Voraussetzungen für Industrie 4.0, IoT und „Smart Manufacturing"

## 12.2 Integratoren und Anwender

Zu den Vorteilen für Integratoren und Benutzer gehören unter anderem:

- Ein FS-Master Tool für unterschiedliche FS-Master über SMI möglich
- Ganzheitliches Engineering von Sicherheitsfunktionen durch IODD mit Informationen zu
  - › Systematischer Sicherheit (PL/SIL)
  - › Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH)
  - › Ansprechzeit des Geräts

## 12.3 Investition in die Zukunft

IO-Link Safety wurde von der IO-Link Community entwickelt, einer schnell wachsenden, weltweit operierenden Organisation renommierter Unternehmen.

# 13 Glossar

| | |
|---|---|
| Black Channel | Kommunikationskanal ohne verfügbaren Nachweis von Design oder Validierung nach IEC 61508 [IEC 61784-3] |
| Condition Monitoring | Teil der vorausschauenden Wartung, die einen Parameter des Zustands von Maschinen überwacht (Vibration, Temperatur, usw.) |
| DTI | *Device Tool Interface*; Software-Schnittstelle für das Navigieren zum und Aufrufen des „Dedicated Tools" inklusive Parameterübertragung |
| FS-AE / AA | *Functional Safety Analog Input/Output*; FS-AE/AA-Modul in einem dezentralen (remote) I/O Knoten |
| FSCP x | *Functional Safety Communication Profile*; *FS-Kommunikationsprofil* für einen bestimmten Feldbus „x", spezifiziert in IEC 61784-3-x |
| FS-Device | Einzelner passiver Partner, wie ein funktional sicherer Sensor oder Aktuator, zu einem Master mit funktional sicheren Eigenschaften |
| FS-DE / DA | *Functional Safety Digital Input/Output*; FS-DE/DA-Modul in einem dezentralen (remote) I/O Knoten |
| FS-Master | Aktiver Partner mit funktional sicheren Eigenschaften, der über Ports mit einem bis zu *n* Devices oder FS-Devices verbunden ist und eine standardisierte Master-Schnittstelle für das Gateway zum Kommunikationssystem der übergeordneten Ebene (NSR oder SR) bietet, oder eine Steuerung mit funktional sicheren Eigenschaften |
| Gateway | Netzwerkknoten, der für die Verbindung mit einem anderen Kommunikationssystem mit anderem Protokoll ausgerüstet ist |
| Industry 4.0 /IoT | Aktueller Trend der Automatisierung und des Datenaustauschs in Produktionstechnologien. Es umfasst „Cyber-Physical"-Systeme, das „Internet der Dinge" und „Cloud Computing" |
| IODD | *IO Device Description*; elektronische Gerätebeschreibung |
| IO-Link Safety | Kommunikationserweiterung für funktionale Sicherheit in IO-Link |
| NSR | *Non safety-related*; nicht sicherheitsbezogen |
| OSSDe | *Output Switching Sensing Device*; Ausgangsschaltende und prüfende Geräteschnittstelle; in IO-Link Safety standardisiert gemäß ZVEI-Empfehlungen |
| Port | IO-Link Kommunikationskanal an einem Master/FS-Master |
| Predictive Maintenance | Techniken zur Bestimmung des Zustands von in Betrieb befindlichen Maschinen zwecks Voraussage von fälligen Wartungsarbeiten |
| Remote I/O | (Feldbus)-Gateway mit (DE/DA)-Modulen für Schaltgeräte oder mit (AE/AA)-Modulen zum Erfassen oder Steuern von analogen Geräten |
| Safety function | Sicherheitsbezogenes System von Sicherheitseingangselementen, Sicherheitsverarbeitung und Sicherheitsstellgliedern, um einen sicheren Zustand von gesteuerten Einrichtungen in Bezug auf ein bestimmtes gefährliches Ereignis zu erzielen oder zu erhalten |
| SCL | *Safety Communication Layer*; sichere Protokollmaschinen-Schicht |
| SMI | *Standardized Master Interface*; einheitliche Master-Schnittstelle zum Gateway zwecks Harmonisierung des Masterverhaltens und einheitlichem Zugriff von Master-Tools |
| SPDU | *Safety Processing Data Unit*; Protokolldateneinheit, bestehend aus Sicherheits-E/A-Prozessdaten und zugehörigem Sicherheitscode |
| SR | *Safety-related*; sicherheitsbezogen |

# IO-Link Safety Systembeschreibung – Technologie und Anwendung

Version März 2018

Bestellnummer 10.171

## Herausgeber

IO-Link Firmengemeinschaft
c/o PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Str. 7
76131 Karlsruhe
Deutschland

Telefon: +49 721 96 58 590
Fax: +49 721 96 58 589
E-Mail: info@io-link.com
Internet: www.io-link.com

## Haftungsausschluss

Die IO-Link Firmengemeinschaft hat den Inhalt dieser Broschüre mit großer Sorgfalt erarbeitet. Dennoch können Fehler nicht ausgeschlossen werden. Eine Haftung der IO-Link Firmengemeinschaft, gleich aus welchem Rechtsgrund, ist ausgeschlossen. Die Angaben in dieser Broschüre werden jedoch regelmäßig überprüft. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten. Für Verbesserungsvorschläge sind wir dankbar.

Die in dieser Broschüre wiedergegebenen Bezeichnungen können Warenzeichen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann**.

Diese Broschüre ist nicht als Ersatz der einschlägigen IEC-Standards und der IO-Link Spezifikationen und Profile gedacht, die in allen Zweifelsfällen unbedingt beachtet werden müssen.



** IO-Link ® ist ein eingetragenes Warenzeichen. In Verbindung mit Produkten und Dienstleistungen darf es grundsätzlich von Mitgliedern der IO-Link-Firmengemeinschaft und von Nicht-Mitgliedern, die eine entsprechende Linzenz erworben haben, verwendet werden. Genauere Hinweise zur Nutzung finden Sie in den Regeln der IO-Link Community Regeln unter: www.io-link.com.

**Weitere Informationen über IO-Link:**
**www.io-link.com**

IO-Link Firmengemeinschaft
c/o PROFIBUS Nutzerorganisation e.V. (PNO)
Haid-und-Neu-Str. 7 · 76131 Karlsruhe · Deutschland
Tel.: +49 721 96 58 590 · Fax: +49 721 96 58 589
E-Mail: info@io-link.com
www.io-link.com