



IO-Link 安全系统描述

技术和应用

IO-Link 功能安全系统描述

版本号: 1.1

中文版本 2023 年 6 月

编译: 李钟琦、钱白华 审译: 巴鲁夫自动化(上海) 有限公司

责任编辑: 李钟琦

编译、发布方:

IO-Link 中国委员会

中国 PROFIBUS & PROFINET 协会 (PI-China)

地址: 北京市西城区广安门外大街甲 397 号
(100055)

电话: +86 10 63314939

邮箱: io-link@pi-china.org.cn

网址: www.pi-china.org.cn

出版方:

IO-Link 国际委员会

PROFIBUS & PROFINET 国际组织 (PI)

地址: Haid-und-Neu-Str Karlsruhe
Germany

电话: +49 721 96 58 590

传真: +49 721 96 58 589

电子邮件: info@io-link.com

网址: www.io-link.com

感谢!

本手册版权归 PROFIBUS & PROFINET 国际组织 (PI) 所有, 保留所有权利。PI-China 作为 PI 在中国地区惟一承认和支持的 RPA 组织, 受 PI 委托将此手册翻译为中文版本并在中国发布。

为确保本手册内容准确性, 在编译期间承蒙南京诚达工业互联网有限公司钱白华先生的翻译和巴鲁夫自动化(上海) 有限公司产品管理团队对译文的审校, 并给予了热诚的支持和帮助, 在此谨向他们深表感谢!

免责声明

IO-Link 国际委员会和 PI-China 已仔细检查了本手册的内容, 但仍不排除出现错误或文本翻译错误的可能性。IO-Link 国际委员会和 PI-China 对所出现的错误不承担任何责任, 但会定期检查本手册中的数据。后续版本将会包含所需的更正。欢迎各位读者提出改进意见。

本手册中使用的术语可能为商标。第三方因任何目的使用此类术语可能会侵犯所有者的权利。**

本手册不能取代相应的 IEC 标准、IO-Link 规范和配置文件。如有疑问, 应以这些文件为准。

© 未经出版商书面许可, 不得以任何电子或机械的形式或方式(包括影印和缩微胶片)复制或使
用本出版物的任何部分。

**  IO-Link® 为注册商标。该商标只可被 IO-Link 国际委员会以及在 PI-China 注册的 IO-Link 中国成员以及已获得相应许可证的非成员使用。使用详情, 请参阅 www.io-link.com 网站上关于 IO-Link 国际委员会的规则。

目录

简介	2	8.2 标准化的主站界面	8
1 自动化中的安全	3	8.3 分离器 / 合成器	9
2 为什么需要 IO-Link 安全?	3	8.4 I/O 数据与 FSCP 的映射	9
3 IO-Link 作为 " 黑色通道 "	4	8.5 端口特定钝化	10
3.1 原则	4	9 发展	10
3.2 前提条件	4	9.1 技术组件	10
3.3 OSSDe 和 SIO	4	9.2 功能安全从站	10
4 IO-Link 安全通信	5	9.3 功能安全主站	10
4.1 目标	5	9.4 测试	10
4.2 安全措施	5	10 评估和认证	10
4.3 格式和数据类型	5	10.1 政策	10
4.4 服务	6	10.2 安全评估	11
4.5 协议参数	6	10.3 认证	11
5 配置与验证	7	10.4 EMC 和电气安全	11
6 技术参数	8	11 部署	11
6.1 IODD	8	11.1 FSCP 指南	11
6.2 专用工具	8	11.2 IO-Link 指南	11
6.3 设备工具接口 (DTI)	8	12 优点	11
6.4 非现场参数设定	8	12.1 IO-Link 概述	11
7 OSSDe 操作	8	12.2 集成商和用户	11
8 通往 FSCP 的网关	8	12.3 未来发展	12
8.1 IO-Link 安全的定位	8	13 术语	13

图例列表

图 1: 功能安全通信	3	图 8: SCL 堆栈	6
图 2: 远程 I/O	3	图 9: FS-Device 的启动	7
图 3: FSCP 世界	3	图 10: 非现场参数设定图	8
图 4: 单一平台解决方案	3	图 11: IO-Link 安全的定位	9
图 5: "黑色通道" 原则	4	图 12: 典型映射	9
图 6: 端口扩展	5	图 13: 主要优点	11
图 7: 带有安全 PDU 的信息	5		

简介

本文的目的是提供一个安全 IO-Link 的性能和局限的概述，提供给需要在功能安全设备帮助下防护风险，相关自动化系统的：

- 管理者
- 设计者
- 实施者
- 集成商

IO-Link 安全是基于国际标准 IEC 61131-9 中标准化 的 IO-Link 技术。该标准规定了用于传感器、执行器 或一体化集成模块的数字通信接口技术（SDCI）。它将 IEC61131-2 中定义的传统开关输入和输出接口，扩展到点对点的串口通信链接。这项技术实现了数字量输入和输出过程数据的循环交换，以及 主站和其相关设备之间的参数和诊断数据的非循环交换。一个主站可以通过网关与上层带有可编程逻辑控制器（PLC）的现场总线相连接。

IO-Link 作为“黑色通道”用于安全通信的主要好处是

- 极低的成本和最小的尺寸
- 不需要特殊的 ASIC 芯片
- 一个接口对应任何设备
- 稳健的数字通信
- 支持各种现场总线
- 设备的统一组态方式

IO-Link 是实现工业 4.0 和物联网的一个先决条件。它只是 要改变经典的自动化架构，即在最底层的传感器和执行器的分离，转向具有传感器和执行器的一体化集成模块。

安全 IO-Link 是对 IO-Link 的扩展，它 在主站和设备两端的顶部使用，是一个额外的安全通信层，因此，成为 FS-Master 和 FS-Device。概念 已经得到了 TÜV-SÜD 的批准。

所有技术都得到了国际 IO-Link 委员会的支持。其他信 息和 安全 IO-Link 规范可在 www.io-link.com 查询。

1 自动化中的安全

现场总线中已经被证实使用了 20 多年的自动化功能性安全通信的一些配置文件，称为 FSCP，在 IEC 61784-3-x 系列（见 www.iec.ch）中实现了标准化。

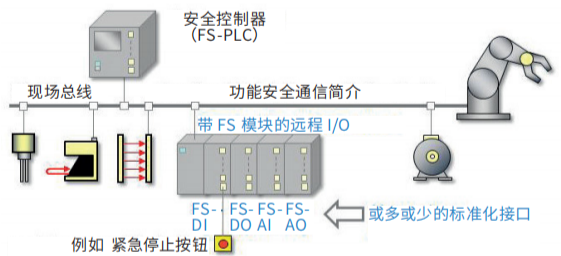


图1：功能安全通信

通常，根据 IEC 62061 或 ISO 13849-1（见 www.iso.ch）的安全功能是使用安全传感器（如安全光幕）、安全逻辑控制器（如 FS-PLC）和安全执行器（如驱动器或其他终端元件）来实现的。这些设备通过使用已选择的任意 FSCP 来交换安全过程数据。

图 1 还显示了功能安全模块，如作为远程 I/O 上的 FS-DI，允许通过冗余信号连接电子安全设备，称为 OSSD（output switching sensing device）。简单的机电设备，例如紧急停止按钮，也可以在此 FS-DI 上操作。

同样，其他模块类型可用于功能安全数字输出至驱动器，或继电器。如图 2 所示，功能安全模拟输入则用于测量仪表。

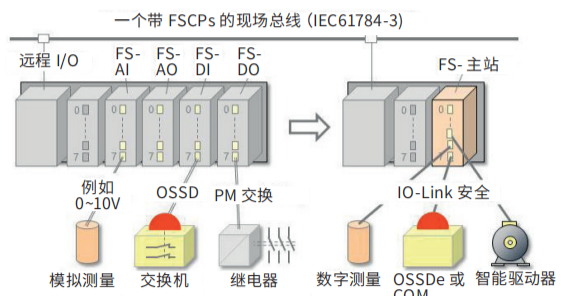


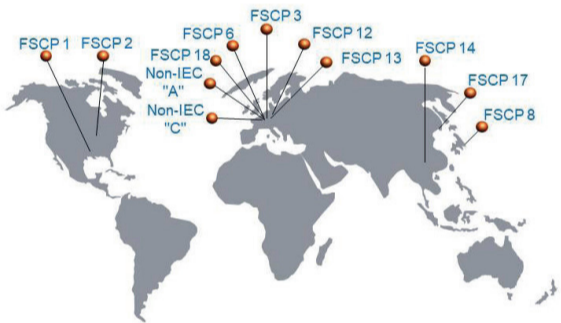
图2：远程 I/O

这些模块类型有许多模块类型和设备制造商的标准化接口，能够为全球范围内每一个安全设备分发一个关于在远程 I/O 上操作的模型。

2 为什么需要 IO-Link 安全？

在对其安全设备进行创新的情况下，制造商正在考虑两个主要的方向：

- 微控制器越来越便宜，新的功能可以整合进已有的产品中。但是，诸如 OSSD 等接口就不支持这些。
- FSCP 可能是一种解决方案。然而，产品需要全球范围内销售，结果就是需要很多 FSCP 来实施和支持，如图 3 所示。



OSSD 接口 (OSSDe), FS-Device 可以部署在经典的 FS-DI 模块上, 从而避免了扩大影响范围。当然, 至少需要一个 FS-Master “x” 包括特定 FSCP 的网关, 才能在该 FSCP “x” 域内部署这种 FS-Device。

安全 IO-Link 对于紧凑型远程 I/O 来说更加重要, 因为 FS-Master 可以在其任何一个通信端口支持任何类型的 FS-Device, 无论是传感器、执行器, 还是复杂的机电类型, 如图 2 右侧所示。

例如通过 FS-Master 的本地安全逻辑与更高层次的安全功能相结合, 这样的新型安全应用被允许使用。

此外, 允许安全和非安全数据的混合传输, 例如带有急停按钮的控制板。

点对点的 IO-Link 通信减少了客户的工作量 (见第四章)。

3 IO-Link 作为 " 黑色通道 "

3.1 原则

大多数 FSCP 都遵循 “黑色通道” 原则。现有的现场总线被用作包含安全过程数据和附加安全码的特殊类型信息的载体。安全码的目的, 是将数据传输的差错概率降低到相关安全标准 (如 IEC 61784-3 或更好) 所要求的水平或更好。由现场总线上的安全通信层 (SCL) 处理这些信息。

IO-Link 安全遵循这一原则, 如图 5 所示。

IO-Link SCL 位于 FS-Device 和 FS-Master 堆栈的顶部。通过 FS-Master 侧的网关与上层 FSCP 系统交换安全过程数据。通常情况下, IO-Link SCL 对象、FSCP 层和网关可以在多核微控制器的一个内核内通过软件实现。

3.2 前提条件

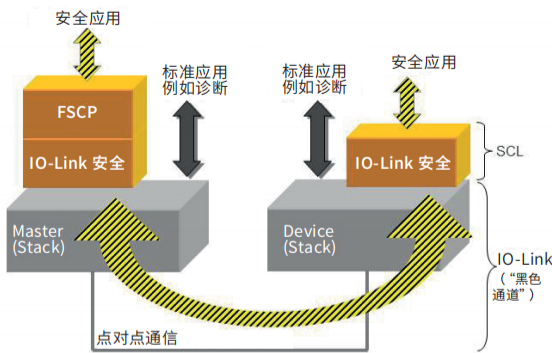


图5：“黑色通道”原则

IO-Link 通过其点对点通信, 满足了周期性过程数据, 以及发送方和接收方之间 1:1 对应关系的要求。在 FS-Master 和 FS-Device 之间不允许网络存储单元也不允许进行无线传输。

由于通电后要进行大量的安全测试, FS-Device 通常需要超过允许的最大唤醒准备时间。因此, 基础 IO-Link 已经稍作修改, FS-Master 会推迟唤醒程序, 直到 FS-Device 准备就绪 (“Ready pulse”)。

在每个端口启动时, FS-Master 发送一 “Verify Record”, 这样 FS-Device 就能够检查存储参数的正确性、真实性 (FSCP、端口号) 和 I/O 数据结构。

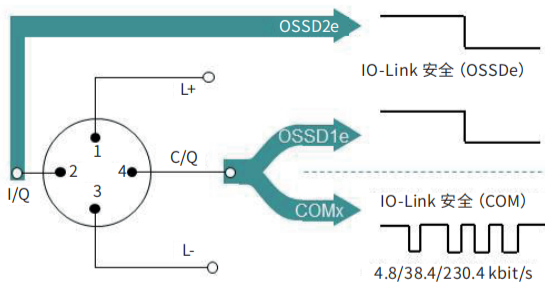
这允许安全 IO-Link 以不变的方式使用 IO-Link 的数据存储机制。有缺陷的 FS-Device 无需工具即可更换。

当涉及到 OSSD 操作时, 端口电源可以由 FS-Master 关闭和开启, 以克服死锁情况。

3.3 OSSDe 和 SIO

安全 IO-Link 协议规定了 IO-Link 的次要信号线 (针脚 2) 与首要信号线 (针脚 4) 一起用于冗余信号操作。这种标准化版本被称为 OSSDe, 并在图 6 中显示。

安全通信只使用主信号线, 并可在所有 3 种传输速率 COM1、COM2 和 COM3 上运行。



4 IO-Link 安全通信

4.1 目标

安全通信对残留误差概率有影响的 3 个主要属性:

- 及时性 (数据及时到达)。
- 真实性 (数据来自正确的发件人)。
- 完整性 (更新和正确的数据到达)。

当消息在 FS-Master 和 FS-Device 之间传输时,可能会发生各种错误如丢失、延迟、损坏等。IEC 61784-3 是有关此类错误的文献资料,以及如何在某些假设下计算残留差错概率。选择了以下安全措施,以便将数据传输的残留误差概率降低到相关安全标准 (如 IEC 61784-3) 要求的水平或更好。这意味着安全 IO-Link 通信分别适用于 SIL3 或 PL e 的安全标准。

4.2 安全措施

安全措施包括:

- FS-Master 和 FS-Device 两者之间信息的编号。FS-Master 使用一个循环的 3 位计数器值。FS-Device 有它自己的计数器,在协议开始时同步,用一个“1”补偿值来响应。
- 通过看门狗定时器确认时间预期,每当有新的后续号码的 IO-Link 安全信息

到达时,总是重新启动。

- 在协议启动时进行认证: FS-Device 与正确的 FS-Master (FSC 的唯一的连接 ID) 和正确的 FS-Master 端口 (“PortNum”) 连接。周期性的,只检查端口号。
- 过程数据和安全代码交叉的循环冗余校验 (CRC) 签名。

安全 IO-Link 协议使用所谓的显式传递安全措施。

4.3 格式和数据类型

来自 FS-Master 的消息和来自 FS-Device 的消息,如图 7 所示。它们由两部分组成。第一部分有 4 个分区,包含安全协议数据单元 (SPDU),最后一个非安全 PDU。

第一个分区存放功能性输入或输出安全过程数据,这取决于传输方向: FS-PDout/FS-PDin。它们可以编码为布尔型 (bit), 整数型 (int16), 或长整型 (int32)。最重要的字组或比特位先发送, 填充位为 “0”。

IO-Link 安全协议有两种格式。一种是专用于短过程数据,如需要高速处理的停机信号的比特数据。这个分区的大小最多为 3 个字节。另一种是为长过程数据设计的如测量或设定值。这个分区的大小最多为 25 个八位字节。

接下来的 3 个分区由所谓的安全代码组成。

这里, 第一个 (1 个八位字节) 是 FS-Master 知

从功能安全主站到功能安全设备。 →

输出过程数据	CRC 签名	控制和主站计数	端口号	功能安全过程数据输出
	根据功能安全输出数据、端口号、控制和计数来产生签名	包含 3bit 计数值	功能安全主站端口号	0~3octets 或者 0~25octets
32~0 octets	2/4octets	1octets	1octets	3/25octets

从功能安全设备到功能安全主站

功能安全过程数据输入	端口号	状态及设备计数	CRC 签名	输入过程数据
0~3octets 或者 0~25octets	端口号取反	包含 3bit 计数取反值	根据功能安全输入数据、端口号、状态和计数镜像来产生签名	
32~0 octets	1octets	1octets	2/4octets	3/25octets

图 7: 带有安全 PDU 的信息

道的端口号，或者是 FS-Device 在调试时收到的一个端口号。

安全代码的第二个分区含有控制和状态信息 (1 个八位字节)，以管理和同步协议的激活以及 3-bit 循环计数器。

安全代码的第三个分区持有一个 CRC 签名。对于短过程数据,16 位 CRC 签名(2 个八位字节)就足够了,对于长过程数据,定义了 32 位 CRC 签名 (4 个八位字节)。

4.4 服务

SPD 的发送方和接收方位于图 5 和图 8 所示的“黑色通道”堆栈的上层。各层的核心部分被指定为状态机,控制 SPDU 的常规的周期性过程工况和特殊工况,如启动、电源关闭 / 开启、CRC 签名错误处理。图 8 说明了安全通信层 (SCL) 如何与 FS-Device 中的技术应用以及 SCL 实例与 FS-Master 中的 FSCP 网关互动。

FS-Master 主要提供的服务是,交换 FS-PDout 和 FS-PDin。在启动过程中,或在出现错误的情况下,实际的过程数据由默认的安全数据 (SDout, SDin) 取代。这些值应全部为“0”,以迫使接收器进入一个安全状态,例如断电。

IO-Link 安全协议通过控制字节中的特征位 (“Activate safe state”) 对安全状态不是断电而是低速的 FS-Device 提供额外支持。作为回报,FS-Device 可以通过状态字中的一个特征位通知接收器,其安全状态已被激活 (“Safe state activated”)。

IO-Link 安全通信错误导致 FS-Master SCL (见图 8) 切换到安全状态。一个安全功能通常不允许在没有人干预的情况下自动从安全状态切换到正常运行。一个附加服务通知 FSCP 关于操作员干预和确认 (“...AckReq...”) 待定。FS-Device 也会通过 LED 指示 (可选),依次收到这个服务。操作员的确认信息可以通过相应的服务 (“...Ack...”) 从 FSCP 传递到 FS-Master SCL。

FS-Device 技术服务包括,交换相应的 FS-PDin 和 FS-PDout 数据,激活和报告安全数据 (SD) 的可行性,以及已经提到的操作员请求指示。

一个 FS-Device 对安全反应的需求时间应足够长,以便通过 IO-Link 安全通信传输 (至少两个计数器的增量)。一个特殊服务将新的计数器值通知技术部分,以便促进和实现这一要求。

来自 FS-Device SCL 的诊断信息可以通过特殊的 “SCL Fault” 服务,传递给技术部分。

4.5 协议参数

安全 IO-Link 中的协议参数带有前缀 “FSP_” 或 “FSCP_”,如果是 FS-Master 的授权。这些参数的目的是根据特定的应用需求调整 SCL 行为,并检查分配的正

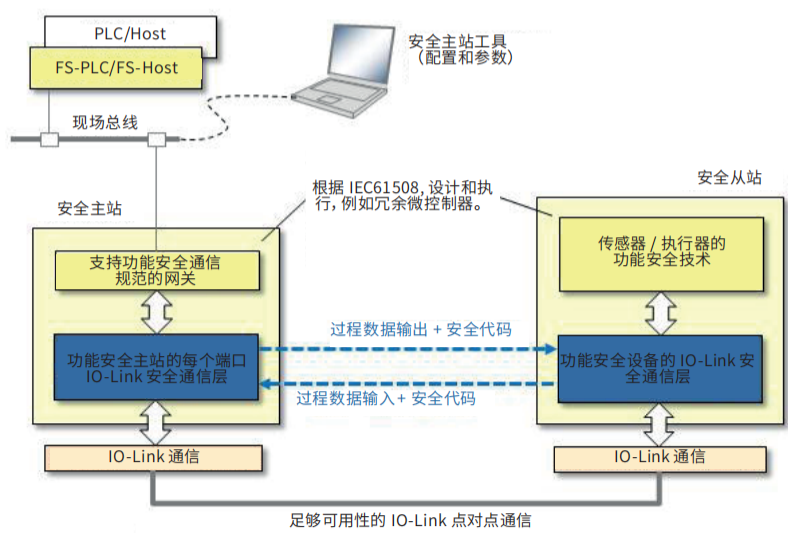


图 8: SCL 堆栈

确性。它们都是被安排在三个记录中的特定标记。

真实性记录由以下部分组成。

- FSCP_Authenticity1/2
- FSP_Port
- FSP_AuthentCRC

第一个包含 FS-Master 的连接 ID，作为 FSCP 网络的参与者。FS-Device 能够检测到与 FS-Master 的连接正确与否。

第二个包含端口号，可以检查与 FS-Master 端口的连接与否。

第三个包含一个 CRC 签名，以确保数值的正确性。

该协议记录由以下内容组成。

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

FSP_ProtVersion 包含使用中的协议版本。FSP_ProtMode 定义了是使用短的还是长的 SPDU。

FSP_Watchdog 定义了一些 ms，为了让看门狗定时器监测下一个有效 SPDU 的接收情况。

FSP_IO_StructCRC 包含一个跨越 FS-Device 的过程数据结构的签名。

FSP_TechParCRC 包含一个与 FS-Device 的技术参数交叉的签名（见第六章）。

FSP_ProtParCRC 中的签名保证了记录数值的准确性。

FSP_VerifyRecord 中的记录作为隐藏的在 FS-Device 启动时的多

样化验证手段。这个机制对用户来说是不可见的（见 5 章和图 9）。

在调试过程中，借助 FS-Master 工具和 IODD，用特定 FS-Device 的安全参数设置协议参数。

例如 Authenticity 和 FSP_TechParCRC 这样的参数在调试过程中需要特定的值来锁定和解锁。调试应该是由人工监控操作。

5 配置与验证

图 9 说明了 FS-Device 启动时的大部分活动。在通电和大量的安全自检之后（通常时间会比标准 IO-Link 的限制长），FS-Device 显示，唤醒已经准备好。在对 FS-Device（数据存储）进行参数检查后，FS-Master 建立通信并发送安全验证的验证记录（见 4.5 章）。

在正确的认证和参数初始化的情况下，FS-Master 和 FS-Device 进入周期性过程数据交换的状态。安全通信层（SCL）将开始自动工作。

除了上述的常规启动，安全 IO-Link 协议还考虑了几种情况，即：

- OSSDe 操作（见第 7 章）

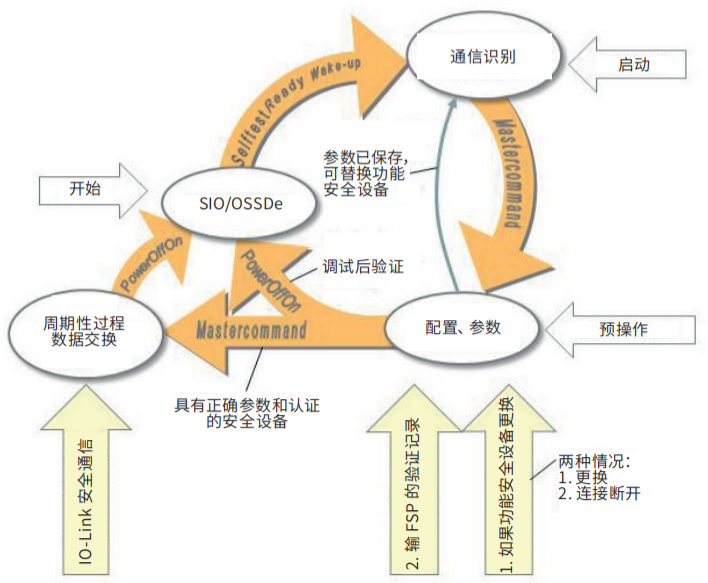


图9：FS-Device 的启动

- 调试 - 测试
- 调试 - 装备
- FS-Device 更换
- 已配置的 FS-Device 错误连接

它们都是在安全 IO-Link 规范中规定的。

6 技术参数

6.1 IODD

IO-Link 的 IO 设备描述是为特定的 FS-Device 工艺如光幕、激光扫描仪、接近开关等参数和量程范围等定义在 IODD 的通用文件里，IODD 定义的参数等应该带有“FST”的前缀。在调试和测试过程中，用户借助于 FS-Master 工具调整 FS-Device 参数值。

6.2 专用工具

随 FS-Device 及其 IODD 有一个简单的“专用工具”PC 程序。它的任务是以安全的方式计算技术参数的所有实例值的 CRC 签名。计算出的签名结果可以复制到 FSP_TechParCRC 中。

FS-Device 可以将本地的计算出的签名与参考签名进行校验。

6.3 设备工具接口 (DTI)

安全 IO-Link 规定了一个简单的设备工具接

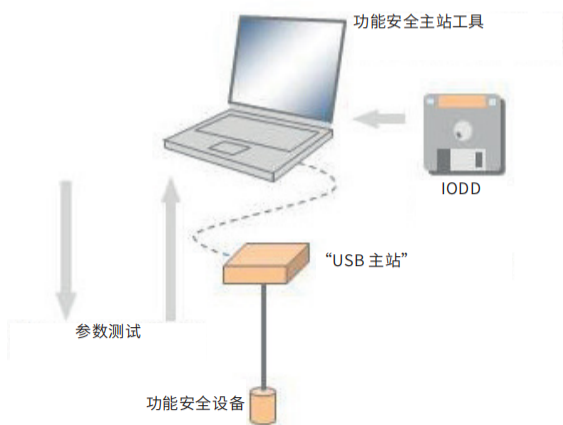


图 10: 非现场参数设定图

口 (DTI)，用于专用工具的调用和参数值传输。

6.4 非现场参数设定

IO-Link 已知的一些工具如“USB-Master”可用于非现场参数设定和设备测试。如果相应的 PC 程序“Master Tool”已升级为“FS-MasterTool”，这对 FS-Device 来说也是可行的，可以用安全协议参数解释 IODD。

7 OSSDe 操作

OSSDe 在安全 IO-Link 中规定的条款 3.3 中显示的 FS-Device 假设如下。

- 冗余的和等效的开关信号。
- 由固态电子元器件产生的。
- 根据 ZVEI 立场文件 CB24I 的 C 型

class 1 要求，测试脉冲长度限制在最大测试脉冲即 1000 微秒。

这些限制为了使 FS-Master 端口或 FS-DI 模块内的复杂性减少，可能使用了固定的过滤时间。

与 FS-DI 一起使用的安全设备使用单一的内置标准 IO-Link 通信进行参数设定，必须遵守 IO-Link 协会规定的条款 10.1 章节。

8 通往 FSCP 的网关

8.1 IO-Link 安全的定位

图 11 显示了 IO-Link 安全是如何嵌入到自动化和信息技术 (IT) 的层次结构中。安全网关包括但不限于功能安全通信协议 (FSCP)。

嵌入式控制器，如驱动器中的控制器，也可以使用安全 IO-Link 技术。

8.2 标准化的主站界面

标准 IO-Link 中的一项新技术是标准化主

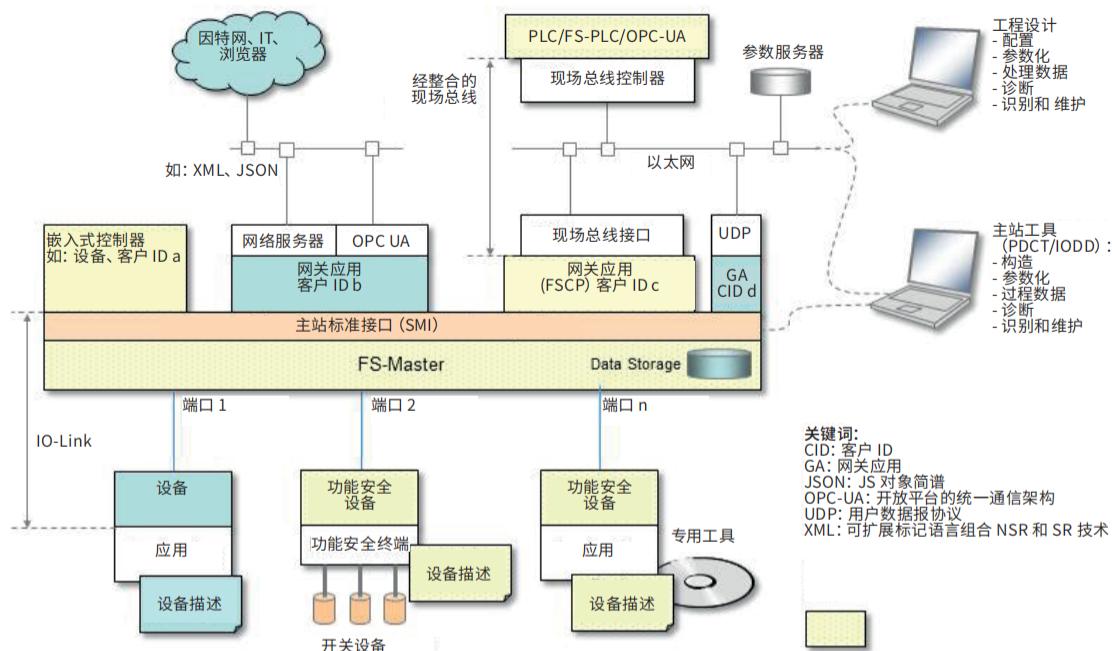


图 11: IO-Link 安全的定位

站接口 (SMI)。它促进了主站的实施, 并允许以一种全面和更容易的方式布置安全内容。

此外, 它还为支持不同品牌主站的工具设置了前提条件。

SMI 规定了以下服务

- 主站识别
- 配置管理 (CM)
- 数据存储 (DS)。
- 非周期性通信 (Read/Write)
- 诊断 (Events)
- 过程数据交换

在安全 IO-Link 的情况下, 一些服务被扩展。

CM 服务也也可以对验证记录进行授权访问。

非循环通信服务提供了电源关闭 / 开启的端口。

过程数据交换服务除了支持非安全过程数据外, 还支持 SPDUs 数据交换。

部分过程数据交换单元是一个所谓的分离器和合成器。分割器的目的是从传入的 IO-Link 消息中提取出 SPDU 数据。

合成器的目的是将 SPDU 和非安全过程数据整合到传出的 IO-Link 消息。

在这两种情况下, 都保留了限定符。

8.4 I/O 数据与 FSCP 的映射

图 12 显示了将 FS-Device 的安全和非安全过程数据映射到 FSCP 和现场总线虚拟远程 I/O 的典型。

这个模型允许将基于比特的数据结构有效地映射到一个 FSCP 消息, 类似于 FS-DI 模块。

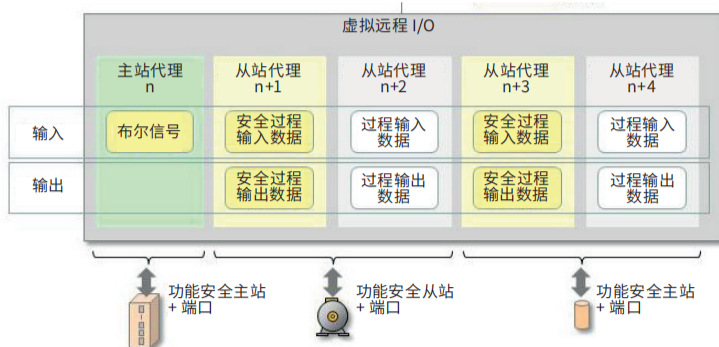


图 12: 典型映射

8.3 分离器 / 合成器

更复杂的 FS-Device 的数据结构, 可以被分别映射到不同的 FSCP 消息中。

该模型还提供了映射非安全过程数据以及诊断 信息 (事件) 的方法。

8.5 端口特定钝化

如果 FSCP 支持通道细化钝化, 映射应考虑安全 IO-Link 的端口特定钝化。

9 发展

9.1 技术组件

除了可以从头开始实施 安全 IO-Link 规范外, 市场上的技术组件也是一种选择。IO-Link 委员会不提供用于 FS-Device、FS-Master 和 FS-Master 工具的通用开发套件。会员公司作为技术供应商提供了技术组件。信息可在协会官网 www.io-link.com 或工作组中获得。

使用技术组件的优势是: 已认证的软件模块, 额外有价值的信息, 例如关于 IODD 设计、工具和支持。

9.2 FS-Device

即使 安全 IO-Link 适用到 SIL 3 或 PL e 的安全功能, 但可能没有必要按照这些安全等级设计和开发 FS-Device。

安全 IO-Link 为 FS-Device 和应用提供了新的可能性。

- 用于接近、应变、扭矩、压力的传感器
- 编码器
- 光幕和激光扫描器
- 数码相机
- 具有自我测试功能的免年检的紧急停止装置图
- 操作员面
- 智能夹钳
- 开关设备

- 电机启动器
- 智能驱动

9.3 FS-Master

同时, 一些公司熟悉现场总线集成。其中许多公司为安全设备提供 FSCP 开发工具包。如果已经建立了安全开发流程, 那么 FS-Master 堆栈的集成是非常容易的。

9.4 测试

测试规范和测试设备目前正在开发中。自动化协议测试仪的测试模式已经准备就绪, 由协议状态机自动生成。

10 评估和认证

10.1 政策

为了防止和保护 IO-Link 协会在与安全相关的开发和应用方面可能出现误导性的理解、错误的期望以及严重的疏忽行为, 任何与安全 IO-Link 有关的人, 无论是培训者、顾问、设计者、实施者或安全 IO-Link 设备的使用者, 都应遵守以下内容:

- 任何非安全设备不会仅仅因为使用 IO-Link 和安全通信层而自动适用于安全相关的应用。
- 为了使产品能够用于与安全有关的应用, 应根据安全标准建立适当的开发流程, 并 / 或取得评估机构的认证。
- 安全产品的制造商, 负责正确实施安全通信层技术 (根据 IEC 61508 或 ISO 13849-1), 产品文档和信息的正确性和完整性。
- 在 IO-Link 规范中提供的信息不包含任何关于正确性和完整性的责任。
- IO-Link 的品牌名称和品牌图片受版权

保护, 其使用需要签订特别协议。

10.2 安全评估

根据 IEC 61508 或 ISO 13849-1 的安全评估必须在以下的评估机构的协助下进行:

- TÜV(全球)
- IFA(德国)
- SP(瑞典)
- SUVA(瑞士)
- HSE(英国)
- FM, UL(美国)

10.3 认证

IO-Link 测试规范提供了关于测试和认证以及如何使用制造商声明的信息。

10.4 EMC 和电气安全

IEC 61000-6-7 规定了 FS-Master 和那些没有产品标准的 FS-Device 的 EMC 测试要求。

IEC 61010-2-201:2017 规定了电气安全的要求, 特别是关于 SELV/PELV 方面。

11 部署

11.1 FSCP 指南

通常情况下, 现场总线组织提供设计和安装指南, 涵盖外围设备, 如远程 I/O。他们还提供安全指南, 或分别参考 IEC62443 系列。

在 IO-Link 安全特性的情况下, 这些准则可能需要更新。

11.2 IO-Link 指南

IO-Link 委员会提供了一份设计指南, 可以从网站 www.io-link.com 下载。

12 优点

12.1 IO-Link 概述

从 www.io-link.com 官网下载的 "IO-Link System Description" 简介一章所述的 IO-Link 的优点也适用于 IO-Link 安全。

然而, 从 OSSDe 到 IO-Link 安全的迁移策略不同于从 SIO 到 IO-Link。

图 13 显示了安全 IO-Link 的主要优点。

对设备制造商的好处包括但不限于:

- 一种无需许可费标准技术
- 同时支持 FS-DI 和 FS-Master 的设备
- 安全数据的双向通信
- 混合安全和非安全过程数据
- 预接线的复杂的一体化模块
- 内置诊断功能以支持状态监测和预测性维护
- 通过认证的验证支持
- 通过 IODD 和专用工具以简化工程
- 工业 4.0、物联网和智能制造的先决条件

12.2 集成商和用户

对集成商和用户的好处包括但不限于:



- 通过 SMI, 一个 FS-Master 工具适用于多个品牌的 FS-Master。
- 通过 IODD 提供以下信息, 安全功能整体集成为可能：
 - › 设备响应时间
 - › 系统性安全 (PL/SIL)
 - › 每小时发生危险故障的概率 (PFH)

12.3 未来发展

安全 IO-Link 是由 IO-Link 协会开发的, 该协会是一家由知名公司组成, 并快速增长的全球运营组织。

13 术语

黑色通	道根据 IEC 61508 [IEC 61784-3] 标准,没有可用的设计或验证证据的通信渠道。
状态监测	预测性维修的主要组成部分,以监测机械状况中的参数(如振动、温度等)。
DTI	Device Tool Interface; 设备工具接口; 用于导航和调用包括参数传输的专用工具软件接口。
FS-AI / AO	远程 I/O 中的功能安全模拟输入 / 输出模块。
FSCP x	在 IEC61784-3 系列中详细说明了用于特定现场总线 x 的功能安全通信规范。
FS-Device	单个被动与具有功能安全能力的主站匹配使用的设备,如功能安全传感器或执行器。
FS-DI / DO	远程 I/O 中的功能安全数字输入 / 输出模块
FS-Master	具有功能性安全能力的主动设备,其通过端口连接到最多 n 个设备或 FS-Device,并提供一个标准化的主接口到上层通信系统(NSR 或 SR)的网关或具有功能安全能力的控制器。
网关	为与另一通信系统对接而配备的使用不同的协议的网络节点
工业 4.0/ 物联网	当前制造业技术的自动化和数据通信的趋势,它包括网络物理系统、物联网和云计算。
IODD	电子设备描述 (IO Device Description)
安全 IO-Link	用于 IO-Link 的功能安全通信扩展
NSR	非安全相关 (Non safety-related)
OSSDe	根据 ZVEI 的建议,在安全 IO-Link 标准中输出开关感应设备接口
Port	主站 /FS-Master 上 IO-Link 通信通道的端口。
预测性维护技术	帮助确定在用设备状况的技术,以便预测何时应进行维护。
远程 I/O	(现场总线 -) 网关到带有 (DI/DO) 模块的开关设备或带有 (AI/AO) 用于测量 / 模拟控制设备的
模块安全功能	关于特定的危险事件,实现或保持受控设备的安全状态的最后要素,与安全输入元素、安全处理和安全相关的系统。
SCL	代表安全协议引擎的 SCL 安全通信层。
SMI	Standardized Master Interface, 在 (FS-) 主站和上层网关之间的标准化主站接口,协调主站的行为并为主站工具提供统一的访问。
SPDU	Safety Processing Data Unit, 由安全输入 / 输出过程数据和相关安全代码组成的安全处理数据单元。
SR	Safety-related, 安全相关。



更多 IO-Link 信息请访问：
www.io-link.com
www.pi-china.org.cn



IO-Link 中国委员会
地址：北京市西城区广安门外大街甲 397 号
电话：010-63314939
E-mail: io-link@pi-china.org.cn
网站: www.pi-china.org.cn