



# 中华人民共和国国家标准化指导性技术文件

GB/Z 37085—2018/IEC 61784-3-8:2016

---

## 工业通信网络 行规 第 3-8 部分:CC-Link 系列功能 安全通信行规

**Industrial communication network—Profiles—  
Part 3-8: Functional safety communication profile of CC-Link family**

(IEC 61784-3-8:2016, Industrial communication networks—Profiles—  
Part 3-8: Functional safety fieldbuses—Additional specifications for CPF 8, IDT)

2018-12-28 发布

2019-07-01 实施

---

国家市场监督管理总局 发布  
中国国家标准化管理委员会

## 目 次

前言 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义、符号、缩略语和约定 .....	2
3.1 术语和定义 .....	2
3.2 符号和缩略语 .....	9
3.3 约定 .....	10
4 概览 .....	10
5 概述 .....	10
6 安全通信层服务 .....	10
7 安全通信层协议 .....	10
8 安全通信层管理 .....	11
9 系统要求 .....	11
10 评估 .....	11
11 FSCP 8/1 .....	11
11.1 范围-FSCP 8/1 .....	11
11.2 规范性引用文件-FSCP 8/1 .....	11
11.3 术语、定义、符号、缩略语和约定-FSCP 8/1 .....	11
11.4 FSCP 8/1 概览 .....	11
11.5 FSCP 8/1 概述 .....	11
11.6 FSCP 8/1 的安全通信层服务 .....	14
11.7 FSCP 8/1 的安全通信层协议 .....	17
11.8 FSCP 8/1 的安全通信层管理 .....	28
11.9 FSCP 8/1 的系统要求 .....	29
11.10 对 FSCP 8/1 的评估 .....	34
12 FSCP 8/2 .....	34
12.1 范围——FSCP 8/2 .....	34
12.2 引用标准——FSCP 8/2 .....	34
12.3 术语、定义、符号、缩略语和约定——FSCP 8/2 .....	34
12.4 概述 .....	34
12.5 概述 .....	34
12.6 FSCP 8/2 的安全通信层服务 .....	40
12.7 FSCP 8/2 安全通信层协议 .....	42
12.8 FSCP 8/2 的安全通信层管理 .....	73

12.9 FSCP 8/2 的系统要求 .....	81
12.10 FSCP 8/2 的评估 .....	85
附录 A (资料性附录) 功能安全通信行规 CPF8 的附加信息 .....	86
附录 B (资料性附录) CPF8 功能安全通信行规的评估信息 .....	87
参考文献 .....	88

## 前 言

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

本指导性技术文件使用翻译法等同采用 IEC 61784-3-8:2016《工业通信网络 行规 第 3-8 部分：功能安全现场总线 用于 CPF 8 的附加规范》。

与本指导性技术文件中规范性引用的国际文件有一致性对应关系的我国文件如下：

- GB 5226.1—2008 机械电气安全 机械电气设备 第 1 部分：通用技术条件(IEC 60204-1:2000, IDT)
- GB/T 15629.3—2014 信息技术标准 系统间的通信和信息交换 局域网和城域网 特定要求 第 3 部分：带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范(IEEE 802.3:2000, IDT)
- GB/T 16657.2—2008 工业通信网络 现场总线规范 第 2 部分：物理层规范和服务定义(IEC 61158-2:2007, IDT)
- GB/T 20438(所有部分) 电气/电子/可编程控制电子安全相关系统的功能安全[IEC 61508(所有部分)]
- GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全[IEC 61511(所有部分)]
- GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全(IEC 62061:2005, IDT)
- GB/T 33537.1—2017 工业通信网络 现场总线规范 类型 23:CC-Link IE 规范 第 1 部分：应用层服务定义(IEC 61158-5-23:2014, IDT)
- GB/T 33537.2—2017 工业通信网络 现场总线规范 类型 23:CC-Link IE 规范 第 2 部分：应用层协议规范(IEC 61158-6-23:2014, IDT)
- GB/T 34040—2017 工业通信网络 功能安全现场总线行规 通用规则和行规定义(IEC 61784-3:2016, IDT)

本指导性技术文件作了如下编辑性修改：

- 修改了标准名称。

本指导性技术文件由中国机械工业联合会提出。

本指导性技术文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本指导性技术文件起草单位：机械工业仪器仪表综合技术经济研究所、中国电力工程顾问集团西南电力设计院有限公司、上海自动化仪表股份有限公司、北京奥斯汀科技有限公司、北京和利时系统工程有限公司、北京交通大学、北京机械工业自动化研究所、中科院沈阳自动化研究所、天津大学、东风设计院有限公司、西南大学、中国自动化学会集成自动化技术与专业委员会。

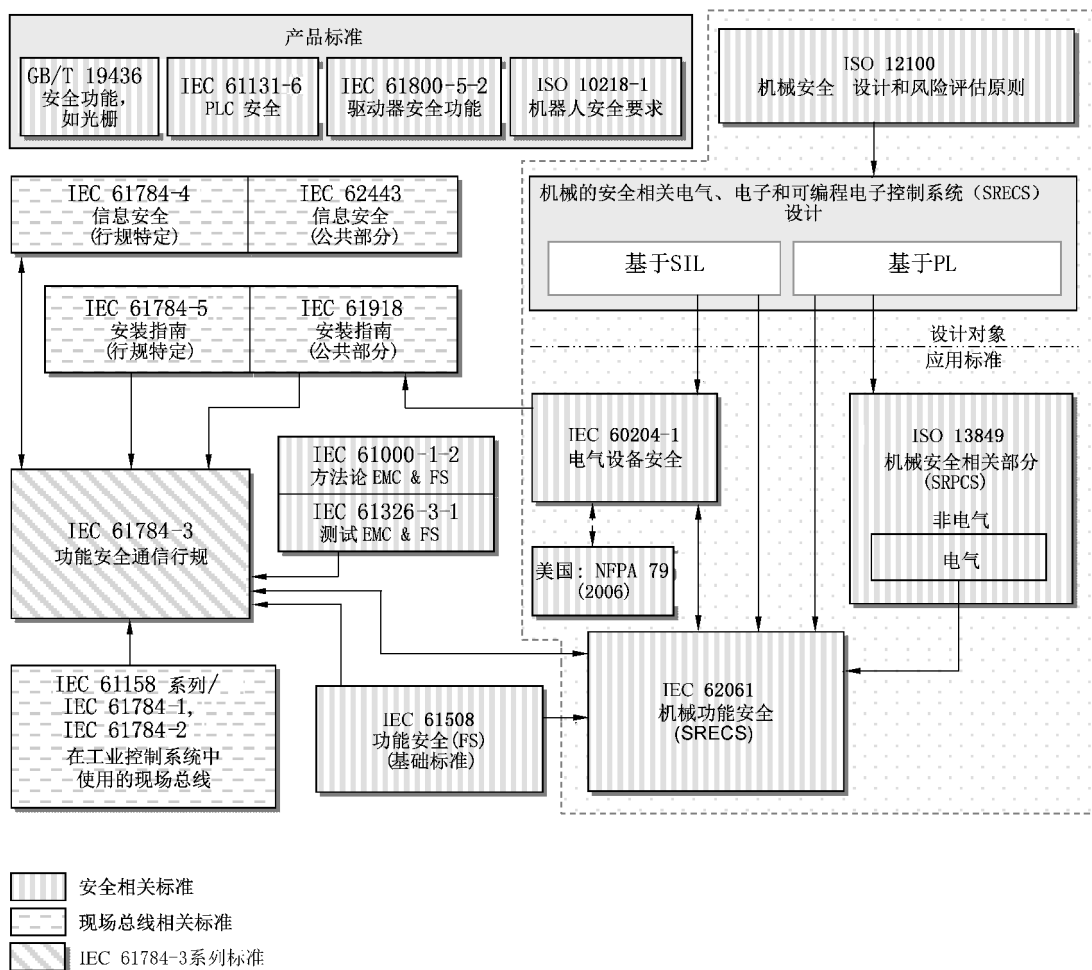
本指导性技术文件主要起草人：高镜媚、丁露、张晋宾、包伟华、陈小枫、罗安、孙昕、李百煌、徐皑冬、董峰、游和平、刘枫、张蓉、甘爽。

## 引 言

IEC 61158 现场总线标准与其配套标准 IEC 61784-1 和 IEC 61784-2 共同定义了一组通信协议以实现自动化应用的分布式控制。现场总线技术目前已被普遍接受并证明可行。因此,很多现场总线技术不断提升,覆盖了尚未标准化的领域,如实时、功能安全相关和信息安全相关的应用。

本指导性技术文件依据 IEC 61508 系列标准,说明了功能安全通信相关原理,规范了基于 IEC 61784-1、IEC 61784-2 和 IEC 61158 系列标准的通行层和协议层的若干安全通信层(行规和对应协议),但不包括电气安全和本质安全方面内容。

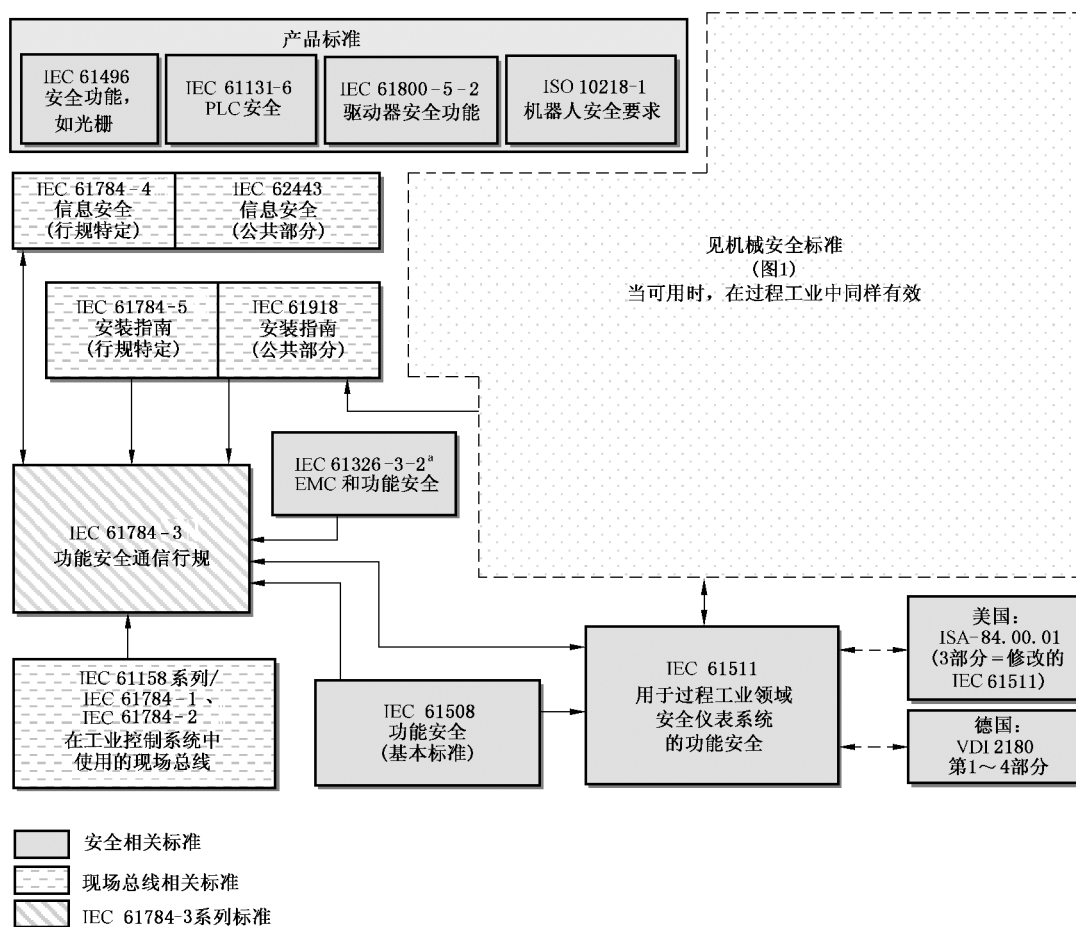
图 1 给出了本指导性技术文件与机械环境中相关安全和现场总线标准之间的关系。



注：IEC 62061 中 6.7.6.4(高复杂性)和 6.7.8.1.6(低复杂性)规定了 PL(类别)和 SIL 的关系。

图 1 IEC 61784-3 与其他标准(机械)的关系

图 2 给出了本指导性技术文件与过程环境中相关安全与现场总线标准间的关系。



<sup>a</sup> 用于规定的电磁环境，否则见 IEC 61326-3-1。

图2 IEC 61784-3 与其他标准(过程)的关系

根据 IEC 61508 系列标准所实现的安全通信层作为安全相关系统的组成部分，为安全相关系统中现场总线上两个或多个参与者之间传输报文(信息)提供了必要的可信度，或为现场总线错误或失效事件中的安全行为提供了足够可信度。

本指导性技术文件规定的安全通信层，使现场总线可以用于要求功能安全达到安全完整性等级(SIL)的应用，该 SIL 等级由其相应的功能安全通信行规来规定。

一个系统最终的 SIL 声明取决于该系统内所选择的功能安全通信行规的实现——在标准设备中实现的功能安全通信行规不足以证明该设备是安全设备。

本指导性技术文件描述了：

- 实现 IEC 61508 系列标准对安全相关数据通信要求的基本原则，包括可能的传输故障、补救措施和对影响数据完整性的考虑；
- IEC 61784-1 和 IEC 61784-2 中多个通信行规族的功能安全通信行规，包括对 IEC 61158 系列标准中通信服务和协议部分的安全层扩展。

# 工业通信网络 行规

## 第 3-8 部分:CC-Link 系列功能 安全通信行规

### 1 范围

本指导性技术文件规定了基于 IEC 61784-1、IEC 61784-2 以及 IEC 61158 类型 18 与类型 23 的 CPF 8 的安全通信层(服务和协议),并标识出在 IEC 61784-3 中定义的功能安全通信原理与本指导性技术文件中的安全通信层是相关的。

注 1: 不包括电气安全和本质安全方面内容。电气安全涉及如电击的危险。本质安全涉及潜在爆炸性环境相关的危险。

本指导性技术文件定义了在使用现场总线技术的分布式网络内的参与者之间传输安全相关报文的机制,该机制符合 IEC 61508 系列标准对于功能安全的要求。这些机制可用于各种工业应用,如过程控制、制造自动化和机械。

本指导性技术文件为遵循本指导性技术文件的设备和系统的开发者和评估者提供指导。

注 2: 一个系统最终的 SIL 声明取决于该系统内所选择的功能安全通信行规的实现——在标准设备中依据本指导性技术文件实现功能安全通信行规不足以证明该设备具有安全设备的资格。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 15969.2—2008 可编程序控制器 第 2 部分:设备要求和测试(IEC 61131-2:2007, IDT)

IEC 60204-1 机械电气安全 机械电气设备 第 1 部分:通用技术条件(Safety of machinery—Electrical equipment of machines—Part 1: General requirements)

IEC 61158(所有部分) 工业通信网络 现场总线规范(Industrial communication networks—Fieldbus specifications)

IEC 61158-2 工业通信网络 现场总线规范 第 2 部分:物理层规范和服务定义(Industrial communication networks—Fieldbus specifications—Part 2: Physical layer specification and service definition)

IEC 61158-3-18 工业通信网络 现场总线规范 第 3-18 部分:数据链路层服务定义 类型 18 元素(Industrial communication networks—Fieldbus specifications—Part 3-18: Data-link layer service definition—Type 18 elements)

IEC 61158-4-18 工业通信网络 现场总线规范 第 4-18 部分:数据链路层协议规范 类型 18 元素(Industrial communication networks—Fieldbus specifications—Part 4-18: Data-link layer protocol specification—Type 18 elements)

IEC 61158-5-18 工业通信网络 现场总线规范 第 5-18 部分:应用层服务定义 类型 18 元素(Industrial communication networks—Fieldbus specifications—Part 5-18: Application layer service definition—Type 18 elements)

IEC 61158-5-23 工业通信网络 现场总线规范 第 5-23 部分:应用层服务定义 类型 23 元素