ICS 25.040
N 10

中华人民共和国国家标准

GB/T 34040—2017/IEC 61784-3:2016

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

Industrial communication networks—Functional safety fieldbuse profiles—General rules and profile definitions

(IEC 61784-3:2016,Industrial communication networks—Profiles—Part 3: Functional safety fieldbuses—General rules and profile definitions,IDT)

2017-07-31 发布　　2018-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC 61784-3:2016(第 3 版)《工业通信网络　行规　第 3 部分:功能安全现场总线　通用规则和行规定义》。

本标准作了如下编辑性修改:

——修改了标准名称;

——删除了英文标准中关于现场总线各类型商标的脚注。

本标准由中国机械工业联合会提出。

本标准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。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、沈阳中科博微科技股份有限公司、北京机械工业自动化研究所。

本标准主要起草人:谢素芬、赵艳领、刘丹、魏剑嵬、李百煌、王静。

引　言

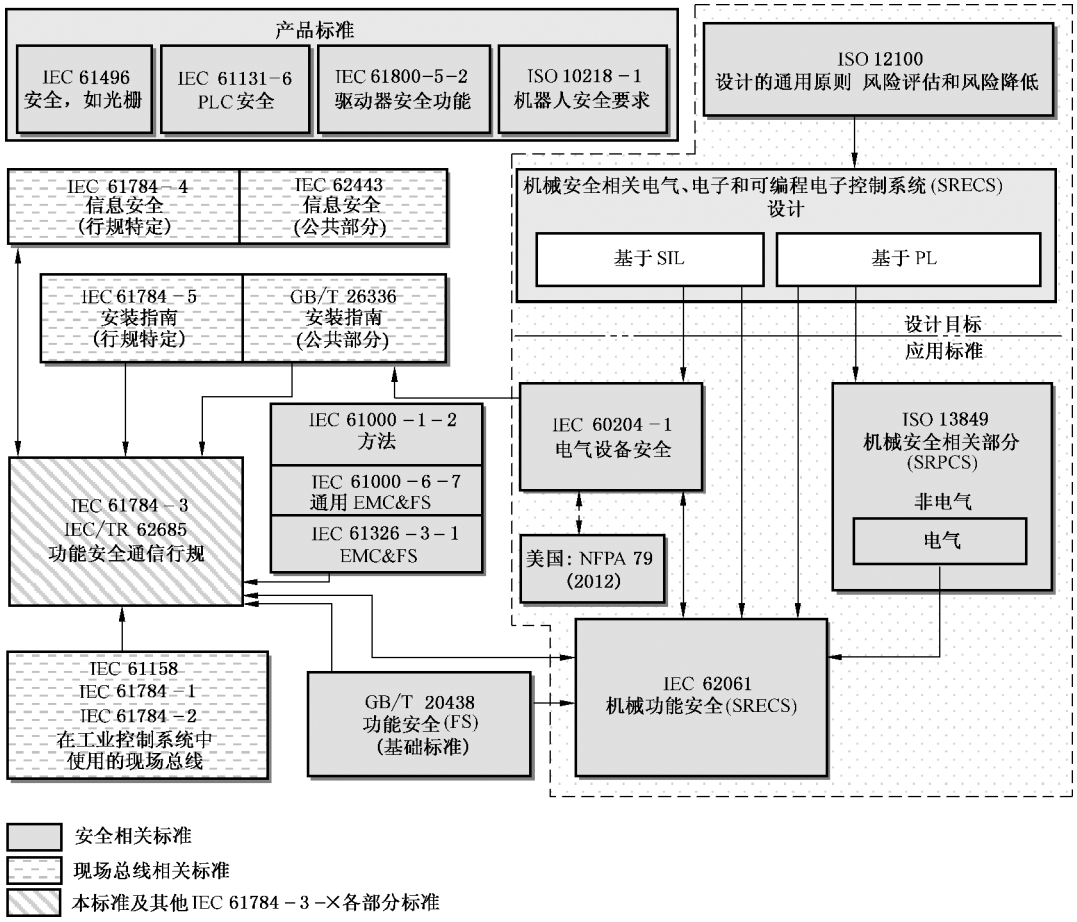
0　简介

0.1　概述

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，现场总线技术不断提升，涉及如实时、功能安全相关和信息安全相关的应用领域。

本标准及其他 IEC 61784-3-×各部分标准定义了符合 GB/T 20438 系列标准的功能安全通信相关原理，规范了若干安全通信层(行规和对应协议)，但不包括电气安全和本质安全方面内容。这些安全通信层基于 IEC 61784-1、IEC 61784-2 通信行规和 IEC 61158 系列标准的协议层。

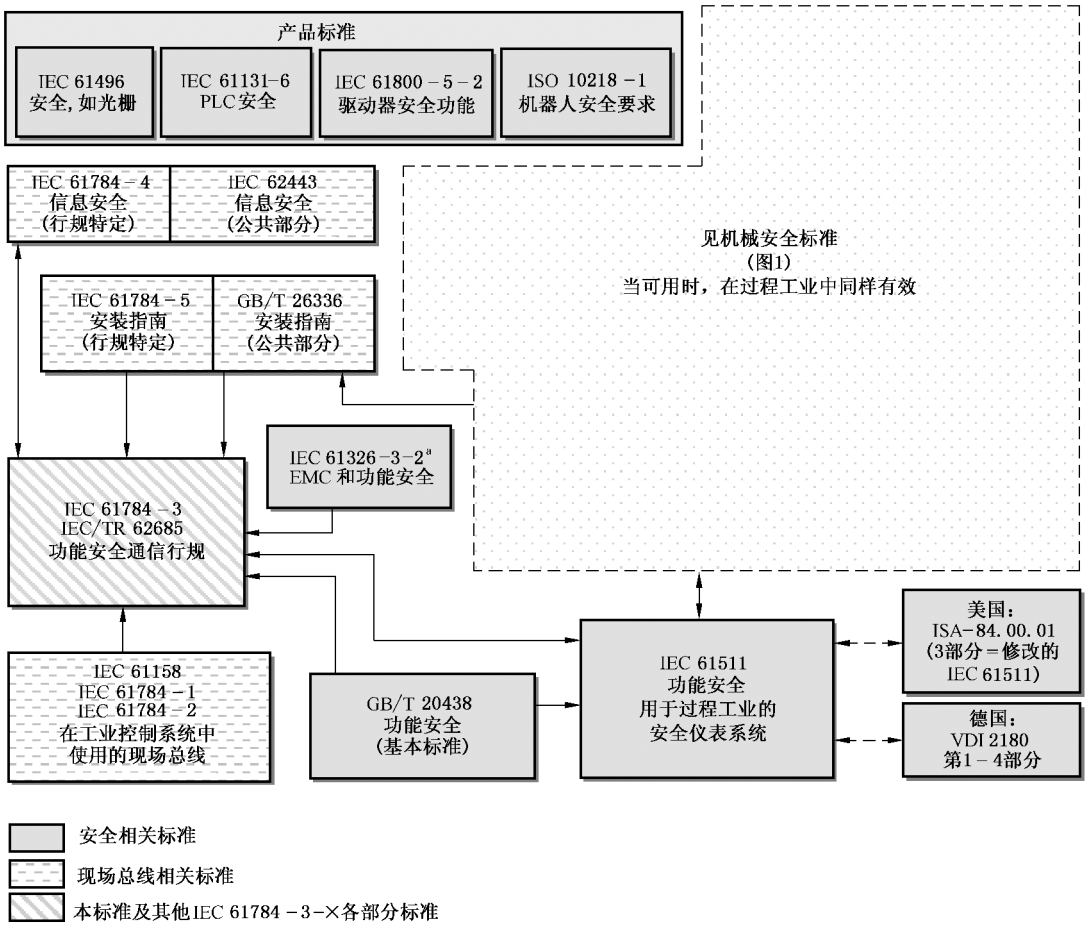
图 1 给出本标准及其他 IEC 61784-3-×各部分标准与机械环境中相关安全和现场总线标准之间的关系。



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　本标准及其他 IEC 61784-3-×各部分标准与其他标准(机械)的关系

图 2 给出本标准及其他 IEC 61784-3-×各部分标准与过程环境中相关安全与现场总线标准间的关系。



[a] 用于确定的电磁环境,否则为 IEC 61326-3-1。

图 2 本标准及其他 IEC 61784-3-×各部分标准与其他标准(过程)的关系

根据 GB/T 20438 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方之间传输报文(信息)提供必要的可信度,或在现场总线发生错误或失效情况下为安全行为提供足够可信度。

本标准及其他 IEC 61784-3-×各部分标准规定的安全通信层,使现场总线可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对所选功能安全通信行规(FSCP)的实现——在标准设备中实现功能安全通信行规不足以证明该设备是安全设备。

IEC 61784-3 是一个系列标准,各部分标准编号及内容如下:

——IEC 61784-3(本标准)为通用部分,定义了实现 GB/T 20438 系列标准关于安全相关数据通信要求的基本原则,包括可能的传输故障、补救措施和影响数据完整性的考虑;

——IEC 61784-3-×各部分标准为技术相关部分,为 IEC 61784-1 和 IEC 61784-2 中各通信行规族分别定义了功能安全通信行规(其中×为通信行规族编号),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。

因此,在本文件中"本标准"仅指 IEC 61784-3 系列标准中的通用部分。

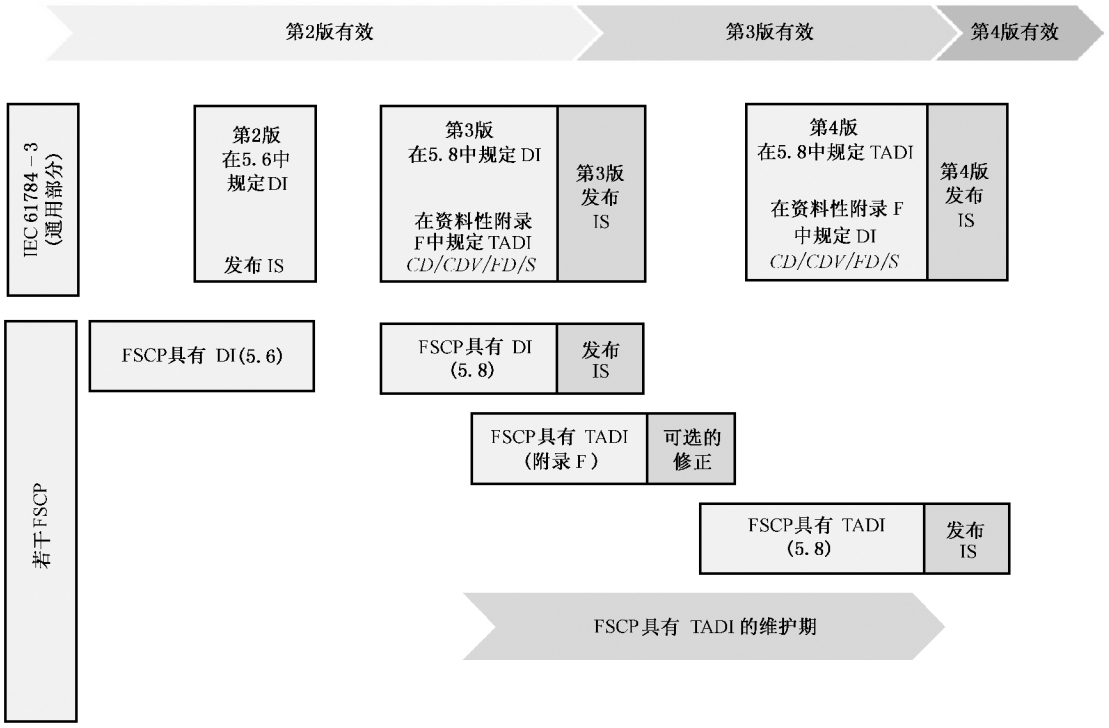
0.2 IEC 61784-3 第 3 版对第 2 版扩展的评估方法

本标准对应 IEC 61784-3(第 3 版)系列标准的通用部分,包含了若干附加的扩展模型。以后,将使用这些模型来评估一个 FSCP 的总残余错误率。其值可用于确定该 FSCP 是否满足给定 SIL 的功能安全应用需求。附录 E 和附录 F 详细描述了这些用于定性和定量安全确定方法的扩展模型。

此外,由于评估过程的典型持续时间,仅本新版(第 3 版)通用部分之前或同时发布的 FSCP,才可使用先前版本(第 2 版)的方法进行评估,即基于本标准 5.8 中规定的数据完整性考虑。

图 3 中的有效期框架给出从第 2 版原始评估方法(在 5.8 中规定)到第 3 版扩展方法(当前在附录 F 中规定)的过渡方法。根据该框架,不依据附录 F 对 FSCP 进行新的评估,直到 IEC 61784-3(第 4 版)中用当前附录 F 取代 5.8。

注:然而,特定 FSCP 可能较早完成评估并发布一个适当的修正。



说明:

DI ——数据完整性(Data Integrity);

TADI ——时效性(Timeliness)、真实性(Authenticity)、数据完整性(Data Integrity);

IS ——国际标准(International Standard);

CD ——委员会草案(Committee Draft);

CDV ——投票委员会草案(Committee Draft for Vote)。

图 3 第 2 版到第 3 版评估方法的过渡

0.3 专利声明

本文件的发布机构提请注意,声明符合本文件时,可能涉及与功能安全通信行规族 FSCP 1(IEC 61784-3-1 规定)、FSCP 2(IEC 61784-3-2 规定)、FSCP 3(IEC 61784-3-3 规定)、FSCP 6(IEC 61784-3-6 规定)、FSCP 8(IEC 61784-3-8 规定)、FSCP 12(IEC 61784-3-12 规定)、FSCP 13

(IEC 61784-3-13 规定)、FSCP 14(IEC 61784-3-14 规定)、FSCP 17(IEC 61784-3-17 规定)和 FSCP 18(IEC 61784-3-18 规定)相关的专利的使用。

注：在 IEC 61784-3-1、IEC 61784-3-2、IEC 61784-3-3、IEC 61784-3-6、IEC 61784-3-8、IEC 61784-3-12、IEC 61784-3-13、IEC 61784-3-14、IEC 61784-3-17 和 IEC 61784-3-18 中提供这些专利细节和相应联系方式。

本文件的发布机构对于这些专利的真实性、有效性和范围无任何立场。

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

1　范围

本标准对应 IEC 61784-3 系列标准的通用部分描述了一些共性原理。这些原理按照 GB/T 20438 功能安全系列[1)]标准的要求，可用于在分布式网络上使用现场总线技术的各参与方之间传输安全相关的报文。这些原理基于黑色通道方法，可适用于各种工业应用，如过程控制、制造自动化和机械设备。

本标准及其他 IEC 61784-3-×各部分标准规定了若干功能安全通信行规。这些功能安全通信行规基于现场总线技术的通信行规和协议层(在 IEC 61784-1、IEC 61784-2 和 IEC 61158 系列标准中规定)，使用 GB/T 20438 中定义的黑色通道方法。在功能安全设备中专门实现这些功能安全行规。

注 1：还可能存在不包含在本标准及其他 IEC 61784-3-×各部分标准范围内的满足 GB/T 20438 系列标准要求的其他安全相关通信系统。

注 2：不包括电气安全和本质安全方面内容。电气安全与如电击这样的危险有关。本质安全与具有潜在爆炸环境的危险有关。

所有系统在生命周期的某个时间都会面临未经授权的访问。因此，在任何安全相关的应用中需要考虑额外的措施以保护现场总线系统不受未经授权的访问。IEC 62443 系列标准将处理这些问题，本标准在特定章节详细描述与 IEC 62443 的关系。

注 3：在 IEC 61784-4 中也可能规定额外的行规特定的信息安全要求。

注 4：根据本标准在设备上实现一个功能安全通信行规不足以证明其是一个符合 GB/T 20438 系列标准规定的安全设备。

注 5：系统最终声明的 SIL 取决于该系统内所选择的功能安全通信行规的实现。

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 20438(所有部分)　电气/电子/可编程电子安全相关系统的功能安全(IEC 61508(所有部分)，IDT)

GB/T 20438.2—2006　电气/电子/可编程电子安全相关系统的功能安全　第 2 部分：电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2000，IDT)

GB/T 26336—2010　工业通信网络　工业环境中的通信网络安装(IEC 61918:2007，IDT)

GB/T 20830—2015　基于 PROFIBUS DP 和 PROFINET IO 的功能安全通信行规——PROFIsafe(IEC 61784-3-3:2010 Industrial communication networks—Profiles—Part 3-3：Functional safety fieldbuses—Additional specification for CPF 3，IDT)

IEC 61000-6-7:2014　电磁兼容(EMC)　第 6-7 部分：通用标准　工业环境下对在安全相关系统中执行功能(功能安全)的设备的抗扰要求 [Electromagnetic compatibility (EMC)—Part 6-7：Generic standards—Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial environments]

1)　本标准后续部分中，GB/T 20438 是指 GB/T 20438 系列标准。