ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20830—2015/IEC 61784-3-3:2010
代替 GB/Z 20830—2007

基于 PROFIBUS DP 和 PROFINET IO 的功能安全通信行规——PROFIsafe

PROFIsafe—Profile for safety technology on PROFIBUS DP and PROFINET IO

(IEC 61784-3-3:2010,Industrial communication networks—Profiles—Part 3-3:Functional safety fieldbuses—Additional specifications for CPF 3,IDT)

2015-12-10 发布　　2016-07-01 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。

本标准代替 GB/Z 20830—2007《基于 PROFIBUS DP 和 PROFINET IO 的功能安全通信行规——PROFIsafe》。与 GB/Z 20830—2007 相比，除编辑性修改外主要技术变化如下：

——在引言中增加了“IEC 61784-3 与其他标准(机械)的关系”及“IEC 61784-3 与其他标准(过程)的关系”的图示(见引言中的图 1 和图 2)；

——增加了对 PROFIsafe 的概览内容(见 4)；

——将 2007 版中的第 5 章和第 6 章合并成第 5 章(见 5，2007 年版的 5 和 6)；

——第 6 章的内容替换 2007 年版第 7 章的内容(见 6，2007 年版的 7)；

——第 7 章的内容替换 2007 年版第 8 章的内容(见 7，2007 年版的 8)；

——第 8 章的内容替换 2007 年版第 9 章的内容(见 8，2007 年版的 9)；

——删除了 2007 年版第 10 章的内容；

——将 2007 年版第 11 章和第 12 章合并成第 9 章(见 9，2007 年版的 11 和 12)；

——增加了对“评估”的描述(见 10)；

——增加了对“CPF 3 的功能安全通信行规的附加信息”和“CPF 3 的功能安全行规的评估信息”的描述(见附录 A 和附录 B)。

本标准使用翻译法等同采用 IEC 61784-3-3：2010《工业通信网络　行规　第 3-3 部分：功能安全现场总线　用于 CPF 3 的附加规范》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件见附录 NA。

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、北京机械工业自动化研究所、西南大学、中科院沈阳自动化研究所、上海自动化仪表股份有限公司、天华化工机械及自动化研究设计院、中国石化集团上海工程有限公司、西门子(中国)有限公司。

本标准主要起草人：高镜媚、谢素芬、丁露、刘丹、惠敦炎、李百煌、高欣、杨光、李佳、刘枫、包伟华、魏剑嵬、王春喜、史学玲、姜金锁、李冀颖、倪佳。

本标准所代替标准历次版本发布情况：

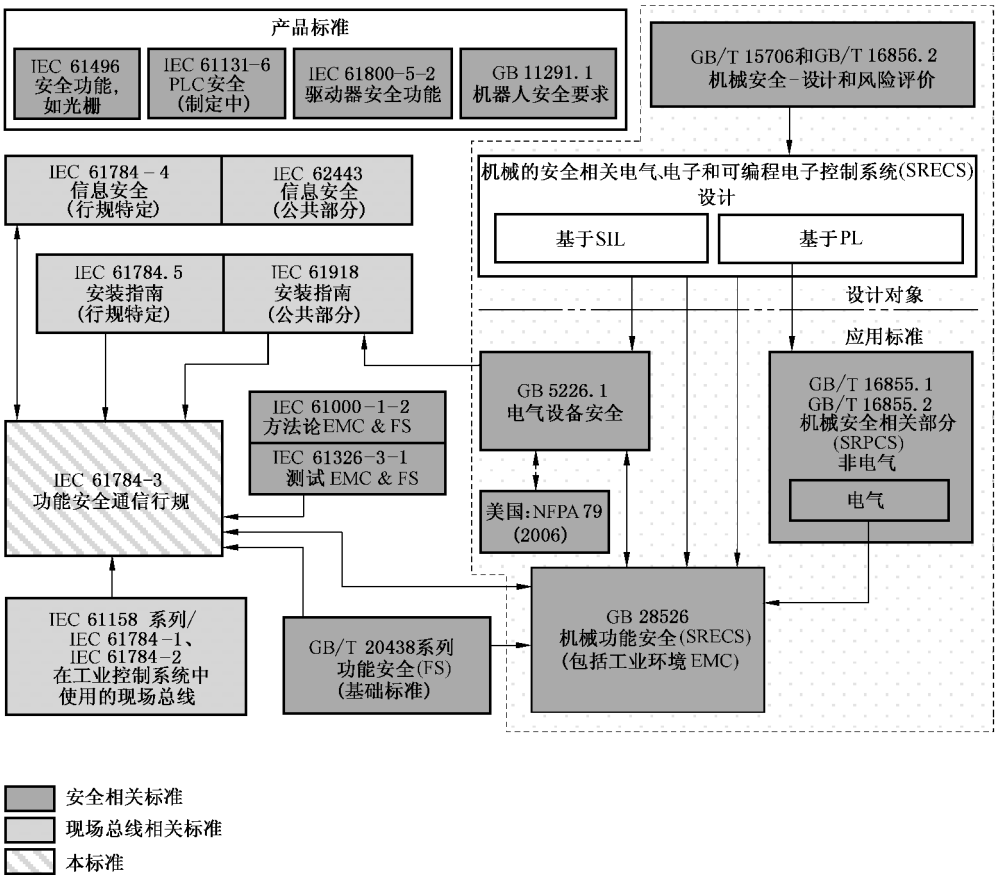
——GB/Z 20830—2007。

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。

本标准依据 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 系列标准的通信行规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。

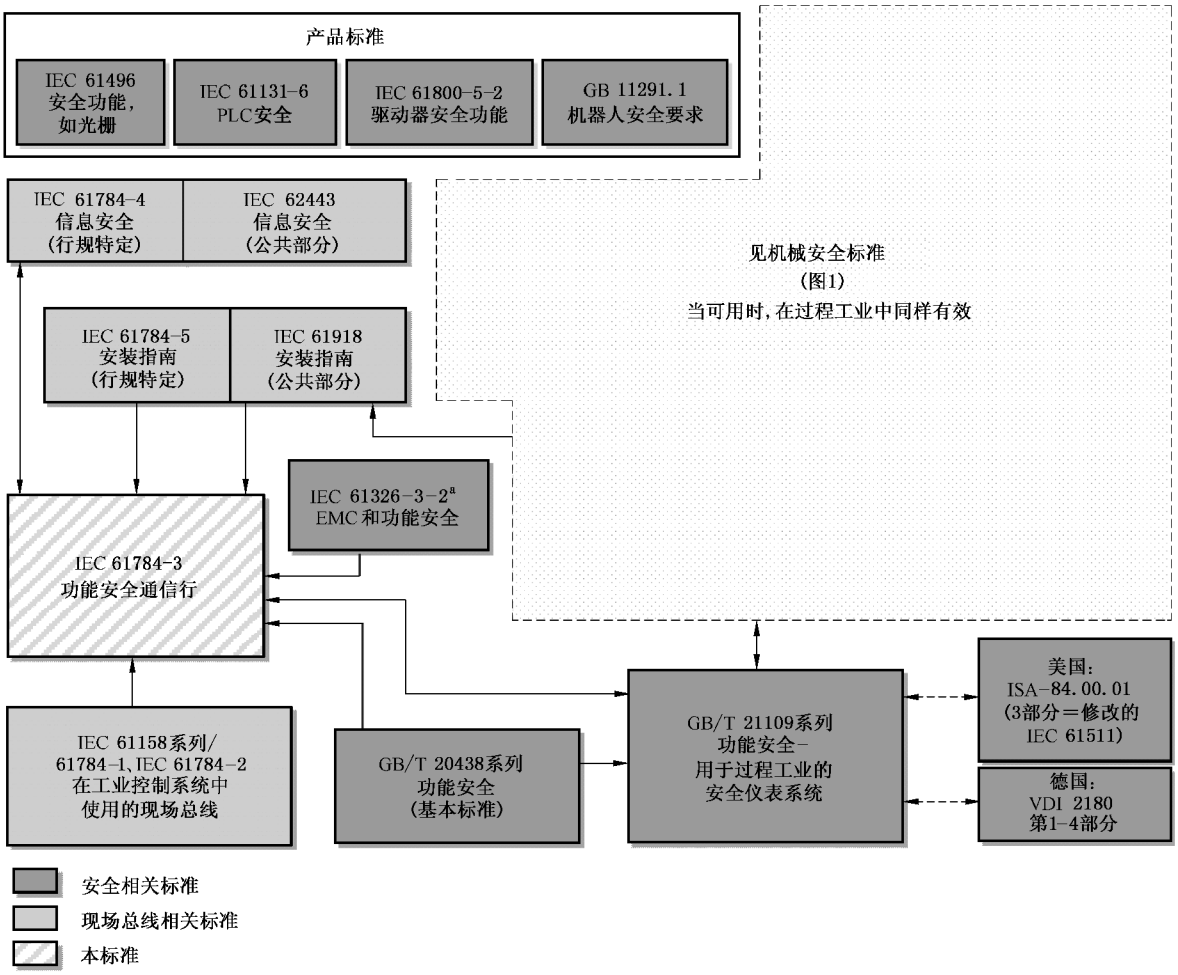
图 1 给出了本标准与机械环境中相关安全和现场总线标准之间的关系。



注：GB 28526 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 给出了本标准与过程环境中相关安全和现场总线标准之间的关系。



[a] 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。

本标准规定的安全通信层，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。

本标准描述了：

——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；

——对 IEC 61784-1 和 IEC 61784-2 中多个通信行规族的功能安全行规的分别描述；

——对 IEC 61158 系列标准中通信服务和协议部分的安全层扩展。

基于 PROFIBUS DP 和 PROFINET IO 的功能安全通信行规——PROFIsafe

1 范围

本标准规定了基于 IEC 61784-1、IEC 61784-2(CP 3/1、CP 3/2、CP 3/4、CP 3/5 和 CP 3/6)以及 IEC 61158 类型 3 与类型 10 的 CPF 3 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标准中的安全通信层是相关的。

注:不包括电气安全和本质安全方面内容。电气安全与危险(如电击)有关。本质安全与关系到潜在爆炸性环境的危险有关。

本标准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。

本标准为符合本标准的设备和系统的开发者和评估者提供指导。

注: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标准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。

ISO 13849-1 机械安全 控制系统有关安全部件 第 1 部分:设计通则(Safety of machinery-Safety-related parts of control systems—Part 1: General principles for design)

IEC 61000-6-2 电磁兼容 第 6-2 部分:通用标准 工业环境中的抗扰度(Electromagnetic compatibility(EMC)—Part 6-2:Generic standards-Immunity for industrial environments)

IEC 61010-1 测量、控制和实验室用电气设备的安全要求 第 1 部分:通用要求(Safety requirements for electrical equipment for measurement,control,and laboratory use—Part 1: General requirements)

IEC 61131-2 可编程序控制器 第 2 部分:设备要求和测试(Programmable controllers—Part 2: Equipment requirements and tests)

IEC 61131-3 可编程序控制器 第 3 部分:编程语言(Programmable controllers—Part 3:Programming languages)

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

IEC 61158-4-3 工业通信网络 现场总线规范 第 4-3 部分:数据链路层协议规范 类型 3 元素