ICS 25.040
N 10

中华人民共和国国家标准化指导性技术文件

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

2007-01-18 发布

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

GB/Z 20830 修改采用 PNO(PROFIBUS 用户组织)的《PROFIsafe—PROFIBUS DP 和 PROFINET IO 安全技术行规》(V2.0 版),主要差异如下:

a) 原文第 1 章经过修改成为 GB/Z 20830 的引言;增加 GB/Z 20830 的第 1 章;

b) 将原文第 3 章中的缩略语部分修改为 GB/Z 20830 的第 4 章,其后的章节按顺序调整,并修改文中相应的引用条目;

c) 删除原文 4.1,其后的章节按顺序调整,并修改文中相应的引用条目;

d) 删除原文 11.1,其后的章节按顺序调整,并修改文中相应的引用条目;

e) 原文图、表按 GB/T 1.1 重新编号,并修改文中相应的引用条目;

f) 原文的第 12 章修改为 GB/Z 20830 的参考文献;

g) 原文的第 13 章修改为 GB/Z 20830 的附录 A,并修改文中相应的引用条目;

h) 按照 GB/T 1.1 进行了编辑性修改。

本指导性技术文件的附录 A 为资料性附录。

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和控制标准化技术委员会第四分技术委员会归口。

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、西南大学、中国机电一体化技术应用协会、上海自动化仪表股份有限公司、中海石油研究中心、北京交通大学、清华大学、天华化工机械及自动化研究设计院、中石化装备总公司、中国仪器仪表协会、浙江中控科技有限公司、中科院沈阳自动化研究所、西门子(中国)有限公司。

本指导性技术文件主要起草人:王春喜、梅恪、刘枫、李百煌、包伟华、徐伟华、欧阳劲松、王玉敏、孙昕、史学玲、惠敦炎、阳宪惠、董景辰、冯冬芹、谢素芬、姜金锁、唐济扬、陈明海、魏剑嵬、冯秉耘、陈高翔、张渝。

本指导性技术文件为首次发布。

引　言

GB/T 20540《测量和控制数字数据通信　工业控制系统用现场总线　类型3:PROFIBUS规范》(MOD IEC 61158 Type3)中规定的PROFIBUS覆盖了自动化体系各层次中广泛的通信应用范围:从Internet和制造执行系统经控制到现场层。

通过简化和限制在ISO/OSI模型的最下面两层,可以实现工业通信的具体要求(例如短报文、确定性和高性能)。用于分布式I/O的PROFIBUS版本具有特别的重要性。使用主/从式和令牌原理的混合访问规则,PROFIBUS基本功能在这里被用于外围设备和处理器单元间的循环数据交换。

虽然具有分布式I/O的自动化解决方案广泛使用了PROFIBUS DP和新引入的PROFINET IO,但故障安全应用仍然依赖于传统电气技术的另一条或专用的总线,这限制了无缝集成和互操作性。由于缺乏系统支持,不能满足现代故障安全设备(如带有集成安全的扫描器或驱动程序)应用需要。提供相应的安全技术是PROFIsafe规范和相关文档的目的。

特定用户群对通信功能的特定应用被称为行规。行规是在一个用户组或一个现场设备族中有效的一系列规则和定义。本指导性技术文件描述了安全外围设备和安全控制器间的通信。它是对标准PROFIBUS DP和PROFINET IO的补充技术,用于减少安全控制器和安全设备间数据传输的失效率和错误率,以达到或超过相关标准要求的等级。

PROFIsafe提供了两种操作模式:V1模式和V2模式。V1模式的措施对于单独的PROFIBUS DP网络上的安全数据传输是足够的,而Ethernet/PROFINET IO更"大量"的特征(如较广的地址空间和缓存转换元素)要求对PROFIsafe行规做某些扩展,这样形成了V2模式。V1模式限用于PROFIBUS DP,而V2模式要求用于PROFINET IO和/或PROFIBUS DP。PROFINET CBA部件间的安全通信还未被定义。图1提供PROFIBUS DP和PROFINET结构中的PROFIsafe概述。

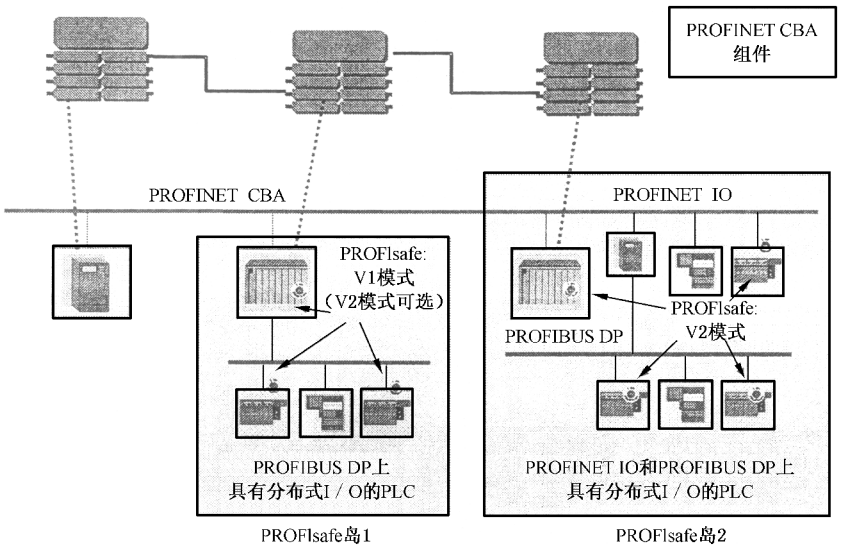

图1　PROFIBUS DP和PROFINET IO上的PROFIsafe V2

本指导性技术文件仅限于安全通信基本机制的描述和它们的参数分配。在终端设备(主机/PLC或现场设备)中为安全所需要的附加措施不在这里描述,因为它们与"开放的"安全通信无关且依赖于单独的结构。

当前 IEC 的几个工作组正在制定现场总线技术标准，如 PROFIBUS、PROFINET、PROFINET IO 以及安全层行规、信息安全(security)和安装指南(编号还未确定)，见图 2。

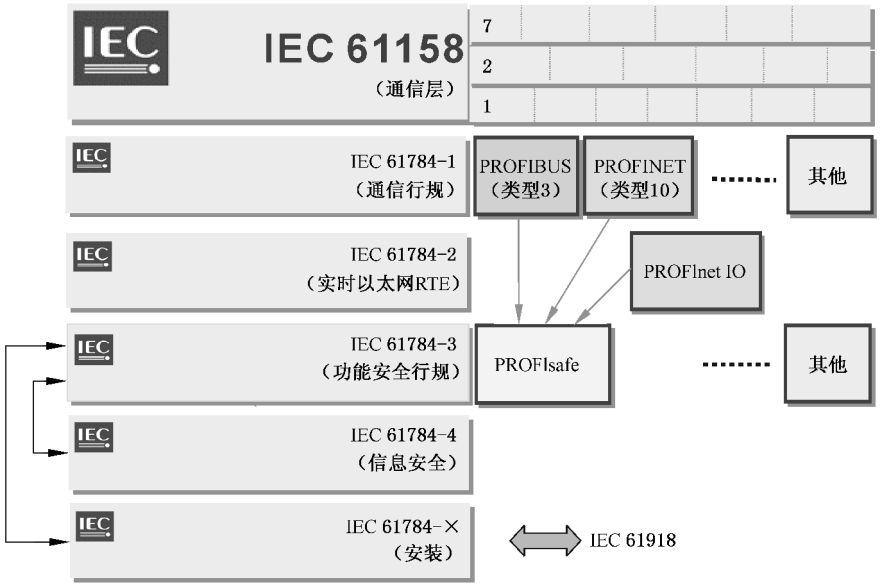

图 2　IEC 工作状况

本指导性技术文件的结构为：第 1 章范围，第 2 章规范性引用文件，第 3 章术语和定义，第 4 章缩略语，第 5 章介绍单通道安全通信概念，第 6 章介绍 PROFIsafe 层细节，第 7 章介绍所传输的 PROFIsafe 帧(container)内容以及 F-主机和 F-设备服务，第 8 章通过描述一个序列图来讨论安全层动态机制，第 9 章安全层管理介绍用于安全层和 F-设备的安全参数，第 10 章介绍 F-I/O 数据格式，第 11 章介绍残余错误率的概率考虑，第 12 章介绍 PROFIsafe 应用，最后是关于 CRC 计算的附录和参考文献。

另外两个电气安全和认证的 PROFIsafe 指南参见参考文献[18]、[19]。

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

1 范围

本标准化指导性技术文件定义了基于 PROFIBUS DP 和 PROFINET IO 的功能安全通信行规——PROFIsafe，适用于加工工业、流程工业、燃料工程和公共运输等领域的通信功能安全应用。

2 规范性引用文件

下列文件中的条款通过 GB/Z 20830 的本部分的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

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(GB/T 20438.1—2006，IEC 61508-1:1998，IDT；GB/T 20438.2—2006，IEC 61508-2:2000，IDT；GB/T 20438.3—2006，IEC 61508-3:1998，IDT；GB/T 20438.4—2006，IEC 61508-4:1998，IDT；GB/T 20438.5—2006，IEC 61508-5:1998，IDT；GB/T 20438.6—2006，IEC 61508-6:2000，IDT；GB/T 20438.7—2006，IEC 61508-7:2000，IDT)

GB/T 15969.3 可编程序控制器 第3部分：编程语言(GB/T 15969.3—2005，IEC 61131-3:2002，IDT)

GB/T 16855.1 机械安全 控制系统有关安全部件 第1部分：设计通则(GB/T 16855.1—1997，eqv PRE N 954-1:1994)

GB/T 17799.2 电磁兼容 通用标准 工业环境中的抗扰度试验(GB/T 17799.2—2003，IEC 61000-6-2:1999，IDT)

IEC 61131-2 可编程序控制器 第2部分：设备要求和试验

IEC 61784 测量和控制用数字数据通信

IEC 61918 测量和控制的数字数据通信 自动化岛内部及岛间现场总线通信媒介安装行规

IEC 62061 机械安全 与安全有关的电气、电子和可编程序电子控制系统的功能安全

EN 954-1 机械安全 控制系统的安全相关部分 设计通用原理

3 术语和定义

下列术语和定义适用于本指导性技术文件。

在下面的文本中，术语“面向安全的”、“安全相关”和“故障安全”将同等使用，并缩写为字母“F”。

3.1

可用性 availability

自动化系统在给定时间内未出现不满足系统条件(如停产)的概率。它取决于 MTBF(平均失效间隔时间)和 MDT(平均不可用时间)：A＝MTBF/(MTBF＋MDT)。

3.2

位信息 bit information

无量纲的二进制编码信息(二进制数字)。