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

中 华 人 民 共 和 国
国家标准化指导性技术文件
基于 PROFIBUS DP 和 PROFINET IO
的功能安全通信行规——PROFIsafe
GB/Z 20830—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 5.5 字数 158 千字
2007 年 8 月第一版 2007 年 8 月第一次印刷
*
书号:155066·1-29735 定价 50.00 元



# 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。

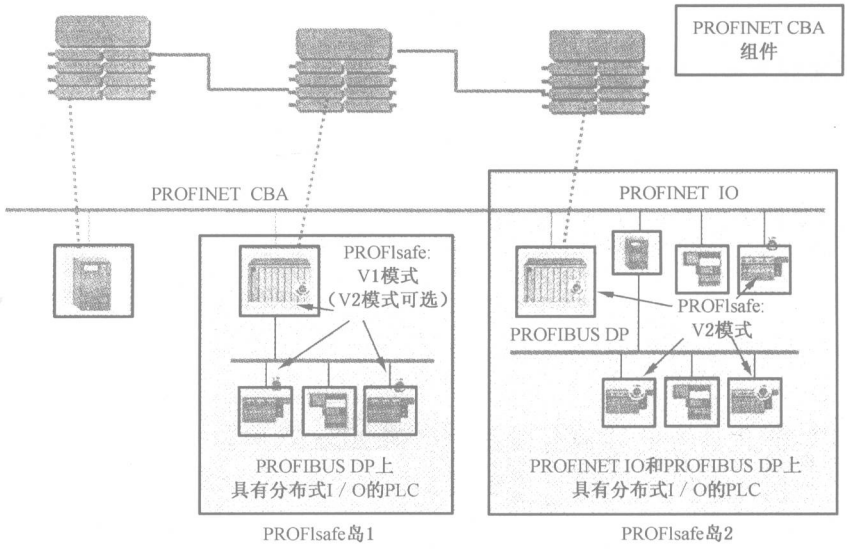


**图1　PROFIBUS DP和PROFINET IO上的PROFIsafe V2**

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。

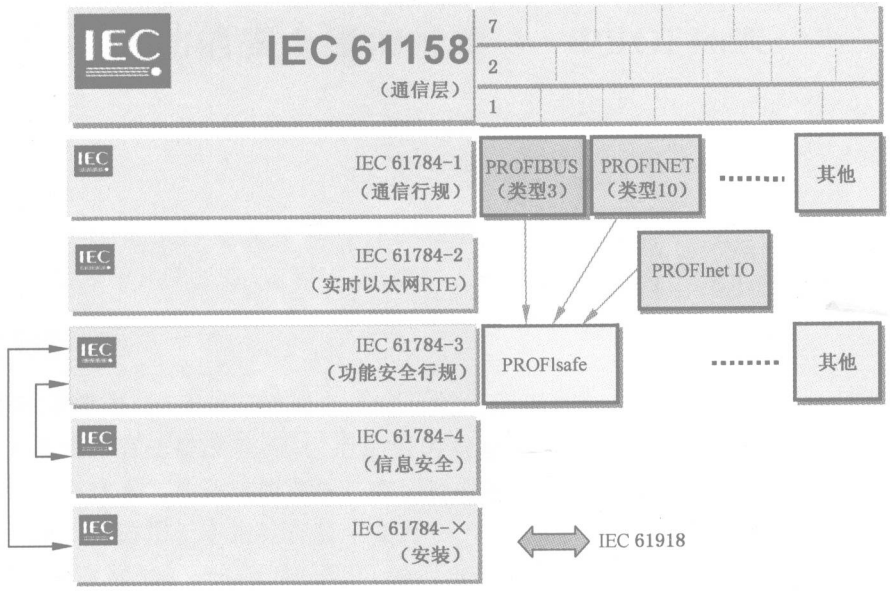


**图 2　IEC 工作状况**

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]。

# 目　次

# 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)。

3.3

**发送方和接收方的代码名称　codename for sender and recipient**

在F通信设备地址空间里，这个代码通常表示明确的源—目的的参数，它被用作F通信对等层之间惟一的“标识”。

3.4

**组态　configuration**

定义单元间的标准通信及具体的设备参数。

3.5

**组态(故障安全)　configuration (Fail-safe)**

定义F-单元间的F-通信及具体的F-设备参数。

3.6

**(虚拟)序列号　(virtual)consecutive number**

V2模式：随触发位的每次改变而递增的连续计数，它根据序列号(递增1)和到下一个值的间隔由接收方进行监控，也称为心跳。V1模式见[30]。和V1模式不同，V2模式下序列号不会在每个单独的PROFIsafe帧内发送。

3.7

**控制位　control bits**

用于触发控制功能的位。与之相对应的是表示数据项的位(例如数值)。

3.8

**CPD-工具　CPD-tool**

通常运行在个人兼容计算机或便携式电脑上，用于现场总线上特定现场设备的组态、参数化和诊断的专门程序。它可以通过直接、单独的链路(如RS232或USB)，或通过现场总线上与循环数据通信并存的非循环服务与现场设备通信。在PROFIsafe范围内，它应运行在WIN2000或更高级的操作系统上。

3.9

**周期　cycle**

重复并连续执行的一系列命令间的时间间隔。

3.10

**(F-)设备　(F-) device**

通常由控制器为数据交换触发的被动通信对等实体。

3.11

**设备访问点　device access point**

此访问点用于寻址作为实体的IO-设备。

3.12

**驱动程序　driver**

使硬件抽象为驻留软件的软件模块。

3.13

**错误　error**

计算、观测或测量的值或条件，与真实、规定或理论上正确的值或条件间的差异。错误可能是由于硬件/软件内的设计失误，和/或由于电磁干扰和/或其他影响导致信息被破坏而引起的。

3.14

**故障安全　Fail-safe;F-...**

系统通过足够的技术或组织措施，来确定性地防止危险或将其风险降低到可容忍度的能力。

3.15

**故障安全值　Fail-safe values**

如果系统被触发到故障安全状态，它发出故障安全值代替过程 I/O 数据。

3.16

**F-驱动程序　F-driver**

根据 PROFIsafe 规范管理 F-主机和 F-设备中安全报文的软件。

3.17

**失效(状态)　failure(states)**

系统未执行在其性能约束之内的预定功能。失效是在某个时间点导致失效条件(状态)发生的事件。

3.18

**故障　fault**

不符合要求的系统工况。因而，失效状态和错误是不同种类的故障。

3.19

**故障反应　fault reaction**

通过置位 F 状态字节中的故障位来指示一个通信故障，以及

——在 F-输出内：关断输出和/或执行单元的自动安全反应。

——在 F-CPU 内：对应于可能的用户程序响应；将 F-I/O 数据设置为故障安全值。

——在 F-输入内：对于从 F-输入检测到的通信故障，F 状态字节的故障位被置位；
对于从 F-主机检测到的通信故障，F-输入数据被设置为故障安全值。

3.20

**帧(报文)　frame(message)**

在 ISO/OSI 模型第 2 层传输的数据单元，参见参考文献[9]。

3.21

**功能块　function block**

处理特定功能的自包含程序单元。

3.22

**危险　hazard**

系统的一种状态或一组条件，它与系统环境中的其他条件一起，将不可避免地导致事故。

3.23

**(F-)主机　(F-) host**

能够执行安全行规机制并服务于“黑色通道”的信息处理单元。它通常是一个带有适当操作系统的 PLC 或 IPC(工控机)。

3.24

**i 参数　i parameter**

与 F-设备有关的单独的或特定技术参数，例如激光扫描器检测区域的坐标。

3.25

**IO-控制器　IO-controller**

为数据交换用于触发设备的主动 PROFINET IO 通信对等实体。PROFIBUS DP 中，此设备对应 1 类主站。

3.26

**IO-设备　IO-device**

通过 PROFINET IO(远程 I/O、传感器、执行器)连接到 IO-控制器的分布式输入/输出设备。

3.27

**IO-模块　IO-module**

DP 从站或 IO-设备中可寻址的子输入/输出单元。

3.28

**IO-监视器　IO-supervisor**

能够从 IO-设备读数据和向 IO-设备写数据的 PROFINET 工程站或 PC/编程单元。它用于启动、调试或诊断目的。与 IO-控制器不同的是:它并不在 IO-系统运转期间起主动作用。IO-监视器不是 IO-系统的一部分。

3.29

**IO-系统　IO-system**

IO-控制器及其相关 IO-设备。

3.30

**主站(1 类)　master(class 1)**

触发从站进行数据交换的主动 PROFIBUS DP 通信实体。

3.31

**报文(数据包或 TPDU)　message(packet or TPDU)**

由于在 PROFIBUS DP 和 PROFINET IO 中缺少 ISO/OSI 模型较高层(>2),所以带有可能的标准 I/O 数据的一个或多个 PROFIsafe 帧相当于传输报文[9]。

3.32

**过程 I/O 数据　process I/O data**

报文(安全数据或标准数据)中用于控制自动化过程的 I/O 数据。

3.33

**行规　profile**

特定用户群对通信功能的特定应用。

3.34

**PROFIsafe 帧　PROFIsafe container**

通过附加安全代码保护的 PROFIsafe 对等实体(如 F-I/O 模块)的一组过程 I/O 数据。

3.35

**状态指示(位)　qualifier(bits)**

如果 F-从站/设备的过程(I/O)数据由多个输入组成,那么附加的状态指示位可以指示每个单独输入的状态。

3.36

**反应时间　reaction time**

紧急请求的"电气"识别与安全反应的"电气"启动之间的时间。这个响应时间由几个时间段组成,包括总线传输时间。

3.37

**可靠性　reliability**

可靠性规定为给定时间内的平均故障次数(用 $\lambda$ 表示)。对于可修复的故障,定义为平均失效间隔时间(MTBF);对于不可修复的故障,定义为平均失效前时间(MTTF)。对于可修复的故障,经常假定故障以恒定比率发生,在这种情况下失效率 $\lambda=1/\mathrm{MTBF}$。在早期故障排除后和磨损阶段之前的运行阶段,部件可靠性通常以 FIT(每 $10^9$ 小时一次故障)度量("浴盆"故障曲线)。可靠性不同于可用性。

3.38

**风险　risk**

事故可能性及其潜在后果严重性的组合。

3.39

**扫描率　scan rate**

输入信号的任意两个读取过程之间的时间。

3.40

**共享 I/O　shared I/O**

多个主机/PLC 访问的相同的输入和输出。共享输入比共享输出引起的问题更少。

3.41

**从站　slave**

PROFIBUS DP：为交换信息通常由主站触发的被动通信方。

3.42

**专用 F-设备应用程序　specific F-device application**

F-设备/从站中的软件，它负责设备（如激光扫描器、驱动程序和限位开关等）的技术支持。通常其中部分是与安全相关的，并遵循 GB/T 20438 规定的安全设计规则，其他部分（如诊断）应遵循标准设计规则。PROFIsafe 功能通常是安全相关软件的一部分。

3.43

**触发位　toggle bit**

在 V2 模式中，从主站发送到设备的控制字节的比特 5，从设备发送到主站的状态字节的比特 5。

3.44

**V1 模式　V1-mode**

符合 PROFIsafe V1.30 版本[30]的 PROFIsafe 服务和协议。

3.45

**V2 模式　V2-mode**

符合本 PROFIsafe 规范的 PROFIsafe 服务和协议。

3.46

**VLAN 标记　VLAN tag**

使用适当的交换机时，以太网报文中 VLAN 标记扩展，可以使特定的用户群在大网络上通过优先级和 VLAN-Id 来运行他们自己的虚拟网络，与其他用户群互不影响。

## 4　缩略语

| | | |
|---|---|---|
| AP | Application Process | 应用进程 |
| API | Application Process Identifier | 应用进程标识符 |
| AR | Application Relationship | 应用关系 |
| ASE | Application Service Element | 应用服务元素 |
| ASIC | Application Specific Integrated Circuit | 专用集成电路 |
| CBA | Component Based Automation | 基于组件的自动化 |
| CPD | Communication Protocol Data | 通信协议数据 |
| CPU | Central Processing Unit | 中央处理器 |
| CR | Communication Relationship | 通信关系 |
| CRC | Cyclic Redundancy Check [9],[11] | 循环冗余校验[9],[11] |
| DB | Data Block | 数据块 |
| DP | Decentralized Peripherals | 分散式外围设备 |
| EMC | Electromagnetic Compatibility | 电磁兼容 |

| | | |
|---|---|---|
| EMI | Electro Magnetic Interference | 电磁干扰 |
| EN, prEN | European Norm, preliminary ... | 欧洲标准,欧洲预标准…… |
| F | Fail-safe | 故障安全 |
| FB | Function Block | 功能块 |
| FV | Fail-safe Values | 故障安全值 |
| GSD(ML) | General Station Description (for PROFINET IO) | 通用站描述(用于 PROFINET IO) |
| GSDML | Generic Station Description Markup Language | 通用站描述标记语言 |
| HD | Hamming Distance | 海明距离 |
| HW | Hardware | 硬件 |
| IEC | International Electrotechnical Commission | 国际电工委员会 |
| I/O | Input/Output | 输入/输出 |
| IOCS | Input Output Consumer Status | 输入输出消费者状态 |
| IOPS | Input Output Producer Status | 输入输出生产者状态 |
| IRT | Isochronous Real Time | 等时模式下的实时 |
| ISO/OSI | International Standards Organization/ Open Systems Interconnection (Reference Model) | 国际标准化组织/开放系统互连(参考模型) |
| LED | Light Emitting Diode | 发光二极管 |
| MBP-IS | Manchester Bus Powered-Intrinsically Safe | 曼彻斯特编码总线供电—本质安全 |
| PA | Process Automation | 过程自动化 |
| PDU | Processing Data Unit | 数据处理单元 |
| PELV | Protective extra low voltage | 特低保护电压 |
| PES | Programmable Electronic (Safety-Related) System | 可编程电子(安全相关)系统 |
| PFD | Probability of Failure on Demand | 要求时的失效概率 |
| PLC | Programmable Logic Controller | 可编程逻辑控制器 |
| PN IO | PROFINET IO | PROFINET IO |
| PV | Process Values | 过程值 |
| RS232 | Recommended Standard 232 | 推荐性标准 232 |
| RS485 | Recommended Standard 485 | 推荐性标准 485 |
| RT | Real Time | 实时 |
| SELV | Safety extra low voltage | 安全特低电压 |
| SIL | Safety Integrity Level | 安全完整性等级 |
| SW | Software | 软件 |
| TPDU | (Transport) Protocol Data Unit[9] | (传输)协议数据单元[9] |
| UML | Unified Modeling Language | 统一建模语言 |
| USB | Universal Serial Bus | 通用串行总线 |
| VLAN | Virtual Local Area Network | 虚拟局域网 |

| | | |
|---|---|---|
| XML | Extendable Markup Language (World Wide Web Consortium) | 可扩展标记语言(World Wide Web 协会) |

## 5 概述

### 5.1 PROFIsafe V2.0 版的主要改进

——随着 PROFINET IO 的使用,使共享设备、每报文的扩展过程(I/O)数据和扩展参数等的改进成为可能。

——缓存在网络部件(如暂时存储全部报文序列的交换机)中的报文错误可以被控制。V1 模式不能完全覆盖这些风险。

——对“黑色通道”下的 CRC 多项式不再加以限制,如禁止使用同样的 CRC 多项式或禁止使用一个可被整除的多项式。

——安全设备的第三方参数化工具可简单调用的接口。

### 5.2 一般要求

——在同样的 PROFINET IO 和/或 PROFIBUS DP 系统中使用标准设备和“安全设备”时,可以保证安全相关通信和标准通信间的独立性;

——适用于安全完整性等级 SIL 3(GB/T 20438)、性能等级“e”(GB/T 16855.1)和控制类别 4(EN 954-1);

——满足单通道通信系统的安全要求→冗余只用于提高可用性;

——安全传输功能的实现应该被限制在通信终端设备(CPU/主机-现场设备和/或 I/O 模块);

——F-设备与其 F-主机之间总是 1 对 1 通信关系;

——传输持续时间被监控;

——环境条件符合通用 PROFIBUS 的要求(主要是 IEC 61131-2 和 IEC 61326-3[29])。有关信息参见参考文献[18]。

——传输设备(如控制器、ASIC、链路、耦合器等)应保持不变(黑色通道)→安全功能位于 OSI 第 7 层之上(即不改变或增加标准协议);

——本指导性技术文件不应减少所允许的设备数量(在“PROFIBUS PA”应用情况下,由于报文限制,在映射期间可能产生约束)。

### 5.3 安全通信原理(黑色通道)

黑色通道原理见图 3。

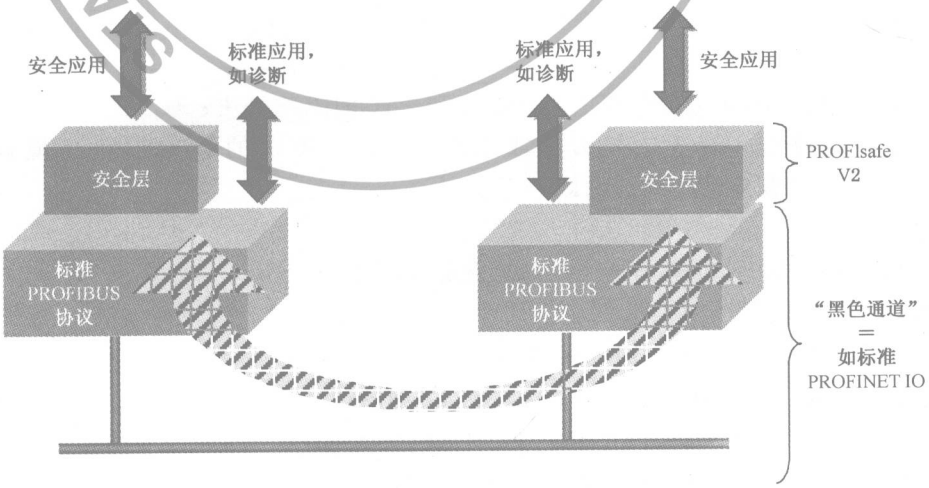


图 3 黑色通道原理

安全通信由下述系统执行：

——标准传输系统(即 PROFINET IO 和/或 PROFIBUS DP)；

——标准传输系统之上附加的安全传输协议。

标准传输系统包括传输系统的全部硬件和相关协议功能(见图 4 中 OSI 模型的第 1 层、第 2 层和第 7 层)。

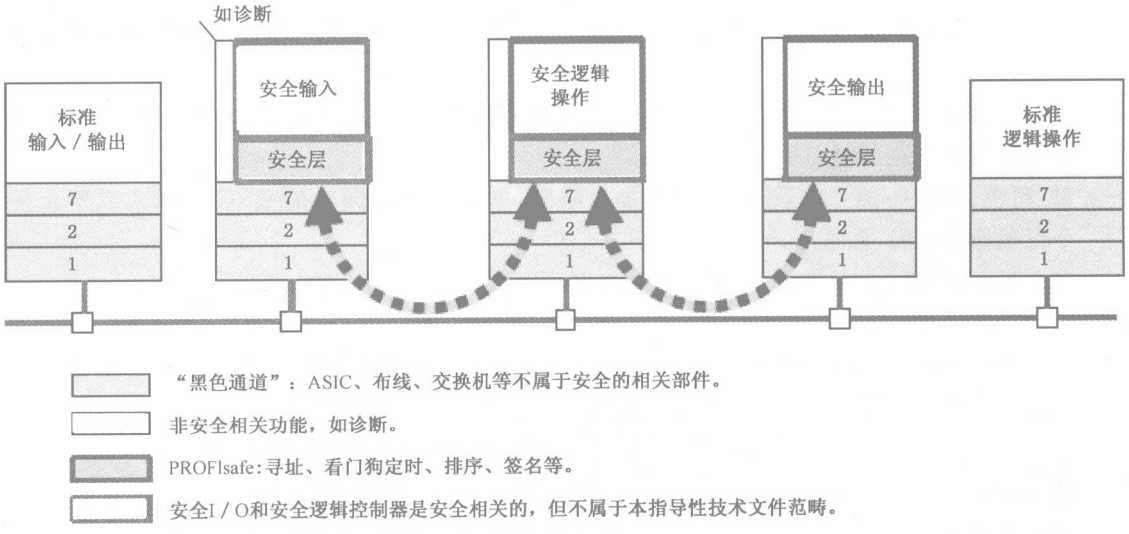


**图 4　安全层体系结构**

安全应用和标准应用同时共享同一个 PROFINET IO 或 PROFIBUS DP 通信系统。

安全传输功能由可以确定性地发现经由标准传输系统渗透的各种可能的故障/危害，或者使残余误差(故障)概率保持在某一限值以下的所有措施组成。可能的故障/危害包括：

——随机故障，例如由于 EMI 对传输通道的影响；

——标准硬件的失效/故障；

——标准硬件和软件的组件的系统故障。

此原理仅限于认证“安全传输功能”，“标准传输系统”不需要任何额外的认证。

通过电缆或光缆实现传输。在 6.4 中规定标准传输系统中允许的拓扑结构、传输特征和“黑色通道”组件。

### 5.4　“黑色通道”的边界条件和约束

对安全评价和残余错误率的计算的边界条件和约束如下所述。

#### 5.4.1　安全相关

通常：

——所有的设备应提供电气安全 SELV/PELV 和 PROFIBUS 证书；

——安全设备应符合 GB/T 17799.2 或 IEC 61131-2 规定的通用工业环境设计，并符合 GB/T 15969.3 规定的增强抗扰性。

V1 模式：

——每种传输技术下每秒的安全相关报文的假定数目为：

- PROFIBUS DP/RS485/FO：100
- PROFIBUS PA/MBP/MBP-IS：10

——每通道类型的重试次数(见 12.5)：

- PROFIBUS DP/RS485/FO：15(IEC 61158：最大 8)
- PROFIBUS PA/MBP/MBP-IS：15(IEC 61158：最大 8)
- 背板总线：8(主机或模块化现场设备内)