PI INTERNATIONAL

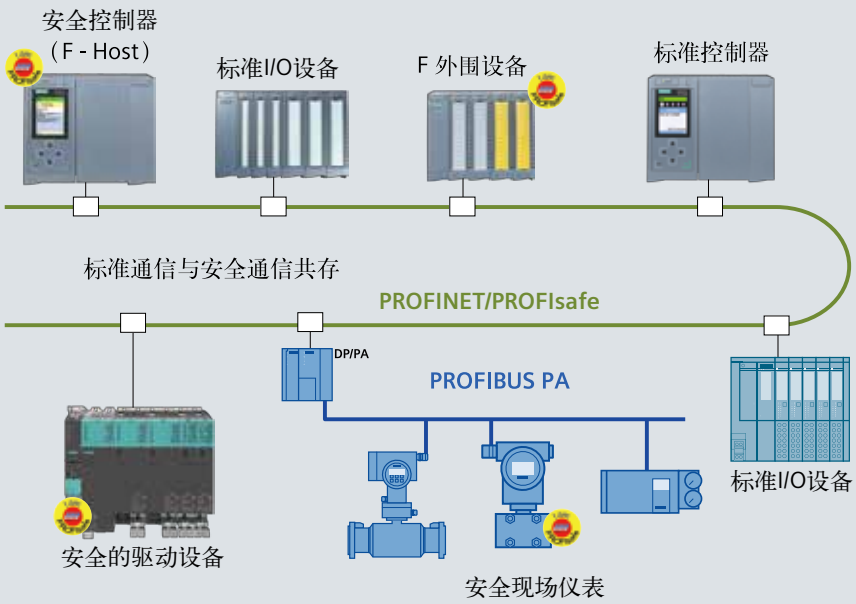
Technologie und Anwendung

技术与应用

PROFIsafe 系统描述

（PROFIsafe Systembeschreibung）

［德］沃尔夫岗 · 斯特里普 （Dr.Wolfgang Stripf ） 著
惠敦炎 译



自动化领域开放的解决方案
(Open Solution for the world of Automation)

PROFIBUS PROCESS FIELD BUS

PROFINET INDUSTRIAL ETHERNET

PROFIsafe-PROFIBUS 和 PROFINET 的安全技术

系统描述

2007 年 11 月 9 日德文版；2008 年 12 月中文版第一次印刷；2011 年 8 月中文第二版第一次印刷；2016年1月中文第三版第一次印刷

订购号：4.341

编者

PROFIBUS Nutzerorganisation e.V. PNO

Haid und Neu-Str.7

76313 Karisruhe

Germany

Tel:+49(0)721/96 58 590

Fax: Tel:+49(0)721/96 58 589

gemany@profibus.com

PORFIBUS Trade Organisation PTO

16101 N 82nd Street, Suite 38

AZ 85260 Scottsdale

USA

Tel:+1 480 483 2456

Fax: Tel:+1 480 483 7202

usa@profibus.com

责任排除声明

PROFIBUS 用户组织（PROFIBUS Nutzerorganisation）非常详细地拟就了这本小册子的内容。但是，不排除文中仍有谬误。PROFIBUS 用户组织或 PROFIBUS 贸易组织（PROFIBUS Trade Organisation）对此一概不负任何法律责任。对本文内容将定期加以审核，以便日后再版时做出必要的更正。对读者提出任何改进的建议，我们深表谢意。

在这本小册子中复述的名称可能是注册商标，第三者利用这些商标达到自己的目的，均可能侵犯其所有者的权利。

这本小册子不能替代 IEC61784-3-3 和 PROFIBUS 标准和行规文件。读者在任何无把握的情况下，都必须注意遵守这一规则。

PI INTERNATIONAL

使命宣言

我们现在是，将来仍然是一个在解决工业通信问题方面位居世界之首的自动化组织。为我们的用户和我们的会员服务，是我们的使命。我们的出版物为广大读者提供理想解决方案，使其受益匪浅，且获悉更多的资讯。

序 言

PROFIBUS 和 PROFINET 是能够为制造业和过程自动化的所有领域提供一种统一的解决方案的现场总线。特别是 PROFINET-基于标准以太网，其需求近年来持续大量增长。这两者的协议均被列入国际标准 IEC 61158 和 IEC 61784-1/-2 的通信行规族 3 中。

自 PROFIBUS 和 PROFINET International 国际组织（PI）成立以来，最为重大的事件之一，是 1999 年功能安全首部规范的颁布。这一步意味着自动化领域中有一个量的飞跃，并开拓了许多新的可能性。

这一技术的名称是 PROFIsafe。PROFIsafe 的标志如下图所示。

从此以后，PROFIsafe 发展成为功能安全通信方面引领全球、最为流行的技术。其间，PROFIsafe 已是 IEC 61784-3-3 名称下的国际标准。

2015 年 12 月 16 日，中国国家标准化委员会正式批准基于 Profibus DP 和 Profinet IO 的功能安全通信行规——PROFIsafe 为推荐性国家标准，标准号为 GB/T20830-2015。这是国内成为国家推荐性标准的功能安全通信行规，安全通信标准的发布将推动我国制造业向更加智能化和全面自动化的方向快速发展。

本系统描述使读者对 PROFIsafe 技术及其相关话题有个全面的了解，而不拘泥于细节。本文无论如何替代不了相关的规范与准则，唯有它们是权威的和有约束力的。

PROFIsafe 获得了 BGIA（Berufsgenossenschaftliches Institut für Arbeitssicherheit-德国工伤保险职业安全研究所）和 TÜV（Technischer Überwachungsverein-德国技术监督联合会）的认可（见下图）。

功能安全是自动化中一个重大的课题。因此，必须谨慎地着手解决 PROFIsafe 技术的推广、实现和应用。所有参与工作的企业和研究机构有义务奉行所谓“PROFIsafe Policy” （PROFIsafe 准则）。

此篇短文可以理解为正式文件的补充和全面的归纳。

本文中缩写“F”表示“fail-safe”（故障安全）、“功能安全”或者“安全相关的”。

PROFIsafe功能安全通信行规成为推荐性国家标准GB/T20830-2015

- 成为推荐性国家标准的功能安全通信行规
- 将进一步推动中国工业功能安全的进程
- 作为PROFIsafe技术的主要推动者，西门子提供了完整的功能安全解决方案

2015年12月16日，中国国家标准化委员会，正式批准基于Profibus DP和Profinet IO的功能安全通信行规——PROFIsafe为推荐性国家标准，标准号为GB/T20830-2015。这是国内成为国家推荐性标准的功能安全通信行规，安全通信标准的发布将推动我国制造业向更智能化，全面自动化的方向快速发展。西门子作为PROFIsafe技术的主要推动者，提供了完整的功能安全解决方案，涵盖安全型PLC、驱动、I/O和传感器等。西门子（中国）有限公司执行副总裁、数字化工厂集团总经理王海滨表示：“制造业的升级需要标准作为支撑，西门子很高兴看到PROFIsafe成为推荐性国家标准，这意味着该标准将在华展开本地化开发、测试与应用，将帮助中国客户提升包括灵活性和效率在内的全面竞争力。”

“PROFIsafe行规获准为推荐性国家标准，对于我国工业功能安全的发展具有里程碑式的意义，将进一步推动我国工业功能安全的进程，为中国在工业功能安全领域向世界先进水平的迈进奠定基础，”机械工业仪器仪表综合技术经济研究所所长欧阳劲松表示。

PROFIsafe是由PI国际组织提出加载在Profibus和Profinet通信协议基础上的故障安全行规，实现了故障安全通信和标准通信共存于同一根电缆上，简化了设备、工程设计并降低了安装成本。PROFIsafe是一种开放性的功能安全通信标准，为研发企业和用户带来诸多便利和保障。PROFIsafe已经获准应用于无线通信技术，如IWLAN、WLAN和蓝牙（Bluetooth）。而且，PROFIsafe带来的系统灵活性也为后续系统改造和升级提供了极大的便利。目前PROFIsafe在国际上已经有超过400万个节点数的应用，其应用范围已经遍布包括汽车、石油化工、煤矿、机械、娱乐设施在内的制造业和过程自动化领域。

功能安全是工业领域的一个重大课题，任何工业过程都或多或少地同风险联系在一起，如人员伤亡、环境破坏和资产损失等，这就对安全自动化提出了更高的要求。国际上功能安全的基本标准是IEC61508（电气/电子/可编程电子安全相关系统的功能安全），而PROFIsafe正是对应该标准的安全通信标准，它覆盖了过程自动化和制造业自动化中的全部安全应用。

目 录

序言 3
目录 5
1. 自动化中的安全 7
1.1 趋势 7
1.2 PI 使 PROFIsafe 得以实现 8
1.3 国际标准 9
2. 目标 10
3. “Black Channels-黑色通道”的设置 12
3.1 基本功能 12
3.2 网络部件 12
3.3 无线通信 & 数据安全 12
3.4 数据类型 12
4. PROFIsafe 解决方案 13
4.1 安全措施 13
4.2 PROFIsafe 报文格式 14
4.3 PROFIsafe 服务 14
4.3.1 安全 Host 服务（安全控制器服务） 14
4.3.2 安全设备服务 15
4.4 安全参数 15
5. 如何实现？ 16
5.1 安全等级 16
5.2 安全设备（F-Device） 16
5.2.1 GSD 的防护 16
5.2.2 I/O 数据的防护 16
5.2.3 i Parameter（i 参数） 16
5.2.4 PROFIdrive（现场总线驱动技术） 17
5.2.5 PA Device（过程自动化设备） 17
5.2.6 I & M-功能（识别 & 维护功能） 18
5.2.7 诊断 18
5.3 安全控制器（F-Host） 18
5.3.1 可能的结构 18
5.3.2 一致性等级（Conformance Classes） 18
6. 认证 19
6.1 PROFIsafe 的测试 19
6.2 安全评估 19
7. PROFIsafe 的应用 20
7.1 电气安全 20
7.2 供电电压 20
7.4 高可用性 20
7.5 安装指南 20
7.5.1 先决条件 21
7.5.2 边界条件 21
7.5.3 布线 21

7.5.4 可用性 21
7.5.5 “紧急停止（E-Stop/Not-Halt）”方案 21
7.6 无线传输 22
7.7 信息安全（Security） 22
7.8 反应时间 23

8. 整体安全考虑 24
8.1 法规 & 标准 24
8.2 风险降低 24
8.3 IEC62061 的应用 24
8.4 风险评估 24
8.5 确定SIL等级 24
8.6 安全功能 24
8.7 已达到的 SIL 等级 25
8.8 电子机械 25
8.9 非电气部件 25
8.10 确认 25

9. 安全（从站）设备家族 26
9.1 远程-I/O 26
9.2 光学传感器 26
9.3 驱动器 26
9.4 机器人 26
9.5 网关 26
9.6 PA-设备 27
9.6.1 液位监控 28
9.6.2 ESD-阀（紧急切断阀） 28
9.6.3 压力变送器 28
9.6.4 瓦斯与火警警报器 28

10. 用户的收益 29
10.1 集成商与用户 29
10.2 设备制造商 29
10.3 未来的投资 29

11. PROFIsafe 应用案例 30
11.1 安全总线协议PROFIsafe在汽车厂总装车间的应用 30
11.2 安全总线协议PROFIsafe在西门子成都SEWC工厂的应用 31
11.3 安全总线协议PROFIsafe为过程行业提供安全保障 32
11.4 安全总线协议PROFIsafe在电梯行业的应用 33

12. PI（PROFIBUS & PROFINET 国际）组织概况 34
12.1 PI 的任务 34
12.2 技术研发 34
12.3 技术支持 34
12.4 认证 35
12.5 培训 35
12.6 因特网平台 35

中、德、英术语对照表 36
参考文献 39

1. 自动化中的安全

任何工业过程都或多或少地同风险联系在一起，从而

- 造成人员伤亡；
- 破坏自然环境；
- 有损投资。

有些工业过程相当简单，无需对自动化系统提出太多的要求即可避免风险。但有些典型应用伴随着很大的风险。这类例子很多，有压力机、工具机床、机器人、传送与包装系统、高压工艺过程、海上石油平台技术、火灾与烟气报警器、燃烧器、索道等等。随着现代工艺技术的复杂，快速和柔性化，对安全的要求日益增加。因此，这些应用需要特别的预防和技术。

市场正在逐渐地使标准自动化系统的可靠性与可用性自行定位在有一定竞争能力的费用高度。虽然标准自动化的故障率或事故率对于一般的应用场合是可接受的，但它对于上述有很大风险的应用，则是不够格的。

这一点可以跟邮政系统相比。一般信件要求的可靠性是可以接受的，因此以普通邮件发送应是十分有利的。重要的邮件则应使用“挂号信的方式”更为安全、可靠。

1.1 趋势

过去微控制器、软件、PC 机和通信网络对于标准自动化产生了巨大的影响，致使费用大幅度降低，使灵活性与可用性都有了较大的提升。但是，新技术的应用最初在安全标准中是被禁止的。在当时，安全自动化还必须采用“固定连线”，且以继电器技术为基础（见图 2）。

在图 1 中你可以找到针对“安全”与“现场总线”课题的 IEC 标准和 ISO 标准及其相互关系。

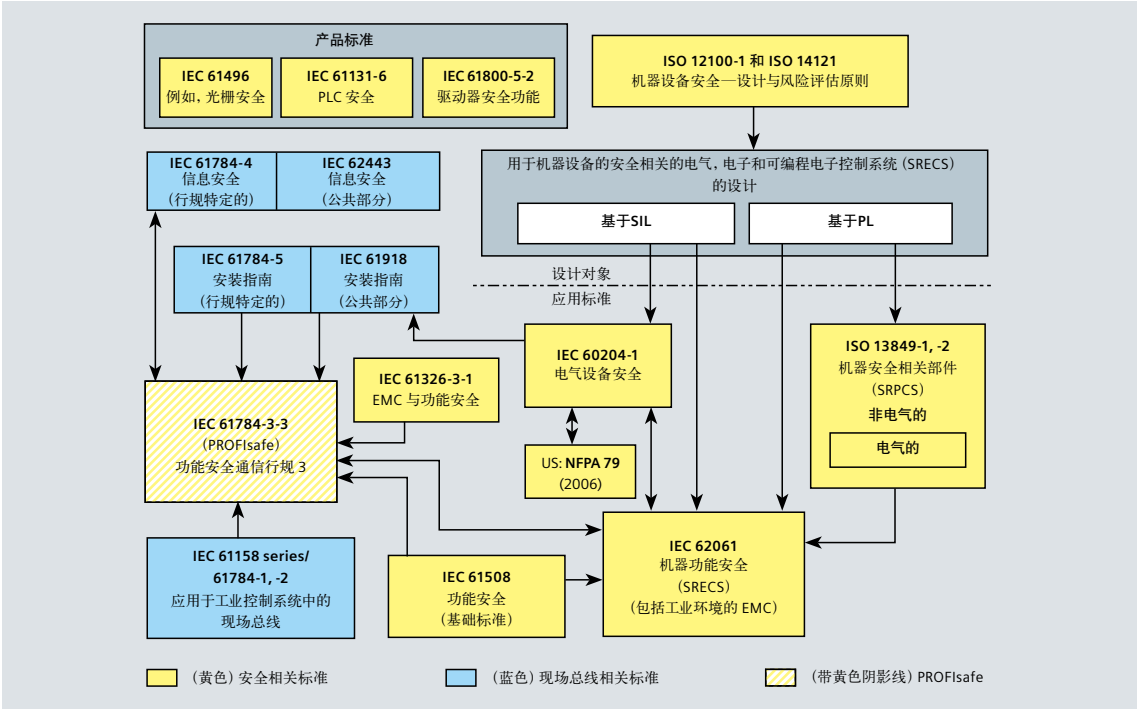


图 1　用于工厂自动化的现场总线与安全标准

功能安全的基本标准是 IEC 61508，它充分考虑了电气装备功能安全的要求，包括了基本原则与方法。它提供一种定量计算所谓安全功能（Safety Integrity Levels-SIL，安全完整性等级）危险失效的残余概率。这对于安全设备和安全主控制器的研发者极有帮助。国际标准 IEC 62061 专门描述应用于制造业自动化中的机械设备的安全要求。该标准考虑了系统、

子系统和单一零部件以及如何评估它们在安全功能中的组合。ISO 13849-1 是目的类似安全标准 EN954-1 的后续。但是，它使用一个易于修改的计算模型（Performance Levels-PL，性能等级）且也覆盖了非电气设备，例如液压阀。机器设备安全的基础技术与方法已在 ISO 12100-1 中作了规定。ISO 14121 描述了风险评估的原理。IEC 60204-1 规定了机器设备，电气装备的一般要求和应用指南。相关内容有：电源、防电击、紧急断开、导线与电缆等等。产品标准如 IEC 61496，ICE 61800-5-2 和IEC 61131-6 描述了单个设备系列的要求。

在欧洲机器法的附录中，列有依照法规需要通过一个被授权机构（BGIA，TÜV，FM-Factory Mutual，等）认证的机器设备和零部件的表格。在经过各方协调的产品标准（如 IEC 61496）中，有制造商的一份声明就足够了。

对有较高的抗电磁性干扰能力的安全设备和安全主控制器的要求在 IEC 61326-3-1 中作了明确的规定。功能安全（FS）性能判据在电磁干扰特别增强的情况下，允许出现功能偏差。但是，在这类情况下，试验对象（EUT）必须切换到一个安全状态中。

出现这种矛盾是很自然的事。然而，安全是建立在可依赖的技术和适合材料的基础之上。依赖的基础是经验，这需要一定的时间。而将原来的的安全技术引进现代自动化领域，必然会带来一些不适用的负面影响。例如，因增加布线和编程而引起的费用，灵活性和可用性比期望的更低；其他的不足方面，如不确定的机器停止位置和随后在重新启动时所要花费的高额开销。

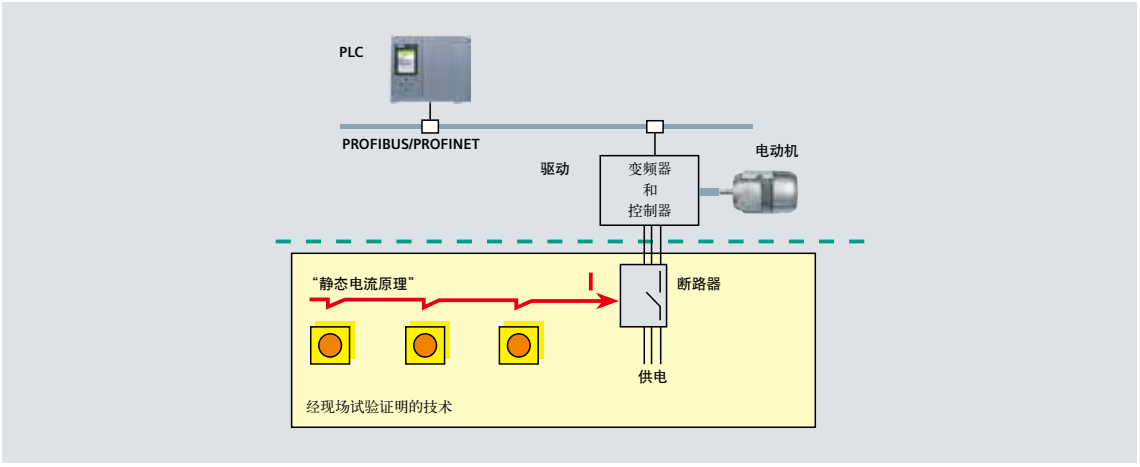


图 2　原来的安全技术

当今，数以百计的微控制器和软件经受了使用的考验。国际标准 IEC 61508 的颁布为其在安全应用领域中的使用创造了先决条件。

人们通过上述标准对许多数字通信系统中的故障识别机制进行了深入细致的研究。有些标准，如 IEC 62280-1 帮助人们为实现此目标铺平道路。

1.2 PI 使 PROFIsafe 得以实现

PI 是研发 PROFIsafe 技术的发起者。该技术是安置在已经存在的 PROFIBUS 和 PROFINET 协议之上的附加层。PROFIsafe 可以使在一个安全主控制器（F-Host）和一个安全设备（F-Device）之间的数据传输中的失效概率降低到标准所要求的范围，甚至低于这个范围。

PROFIsafe 在软件上极易实现，因此在使用 PROFIBUS 和 PROFINET 的条件下，覆盖了过程自动化和制造业自动化中安全应用的整个范围。PROFIsafe 甚至获准应用于无线通信技术，如 WLAN 和蓝牙（Bluetooth）。它将信息安全技术（Security）包括在内，可经由以太网电缆获得更加广泛的应用。

PROFIsafe 在过程自动化中要求高可用性和低能耗，而在制造业自动化中则要求毫秒范围内的瞬时反应时间。

现代的安全设备（F-Device），如激光扫描器或带集成安全装置的驱动器如今可以大显身手。PROFIsafe 的系统支持将其实现，它使单个设备安全参数（i Parameter）的管理变得十分简单。它包括 F-Device-Tools（例如：Tool Calling Interface 调用接口工具）以及选择存储和再装入 i 参数的装置（iPa-Server）。这里应当指出，各类工具的接口和 iPa-Server-Option（i 参数 - 服务器 - 选择）装置也可以应用于非安全相关的设备中。

国际标准 IEC 61508 在抗电磁干扰方面提出了更高的要求，但未规定细节。“PROFIsafe Environment”（PROFIsafe 环境）作为补充准则弥补这一空白和其他的空缺，从而促进了 安全设备（F-Device） 和安全主控制器（F-Host） 的发展与应用。

PI 有一项规定，即在 PROFIBUS 和 PROFINET 网络中只准许使用按照 IEC 61508 认证的安全设备（F-Device） 和安全主控制器（F-Host）。设备同 PROFIsafe 协议的一致性必须在被授权的 PI 测试实验室中通过检验并经 PROFIBUS 用户组织（PNO）认证。“PROFIsafe Test-Spezifikation”（PROFIsafe 测试规范）确定了认证机构（如 TÜV）和 PI 测试实验室的作用与任务。

读者欲查询有关 PROFIsafe 的最新资讯，请登录网站 www.profisafe.net；欲查询有关 PROFIBUS 和 PROFINET 的一般信息，请点击网站 www.profibus.com。

1.3 国际标准

大多数国家都规定了保护人与自然环境的国法。在欧洲，低压法、EMC 法和机器设备法都是这类立法的典型例子。这些法律、法规又都是来源于国际标准。

现场总线标准规定在 IEC 61158 和 IEC 61784-1 中。实时以太网的衍生，例如 PROFINET IO，定义在 IEC 61781-2 中。“安装指南”的一般规定归纳在 IEC 61918 中；行规特定的安装指南见 IEC 61784-5。一般的信息安全指南（Security）见 IEC 62443；行规特定的信息安全指南归入 IEC61784-4 中。

图 3 中可以找到相似的 IEC 标准和 ISO 标准，这些标准适用于过程自动化的现实状况。专业标准 IEC 61511 描述了在已定义的电磁环境下且在极其灵敏的过程测量与控制系统中长期经验积累处境下的功能安全（所谓“经使用验证可信”- Betriebsbewährung）。IEC 61326-3-2 相应地考虑了这种环境的 EMC- 要求。

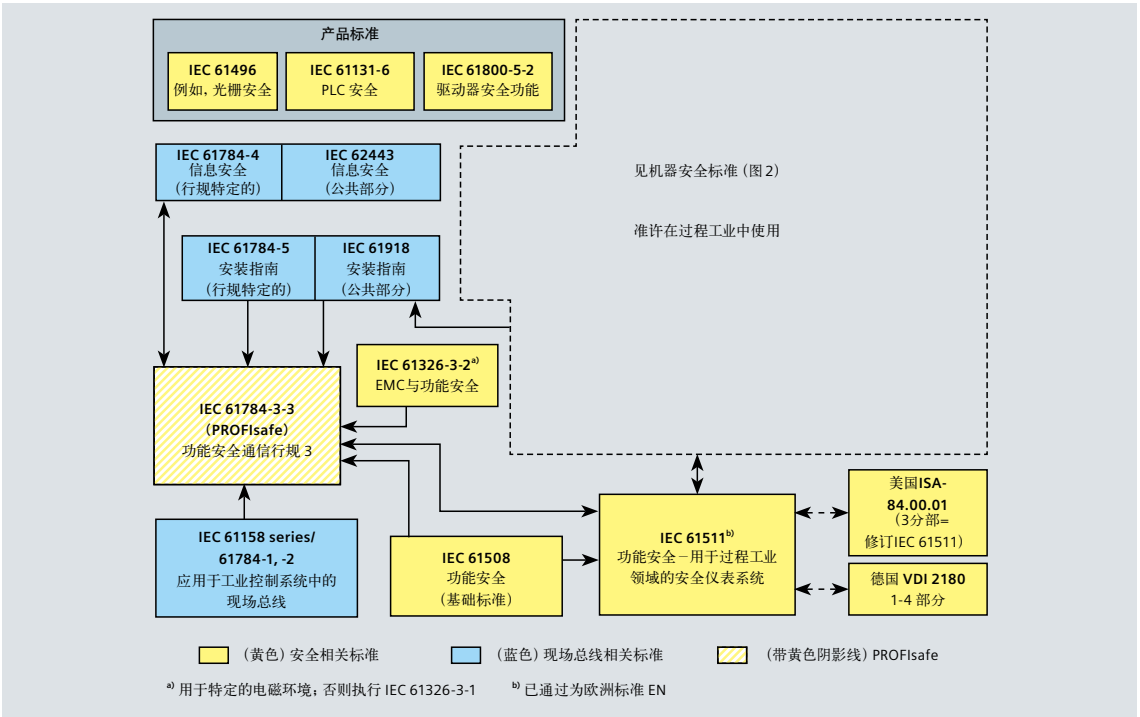


图 3　用于过程自动化的现场总线与安全标准

2. 目标

从一开始 PROFIsafe 的目的就是为了向安全设备的研发者和最终用户提供一种内容丰富和行之有效的解决方案。

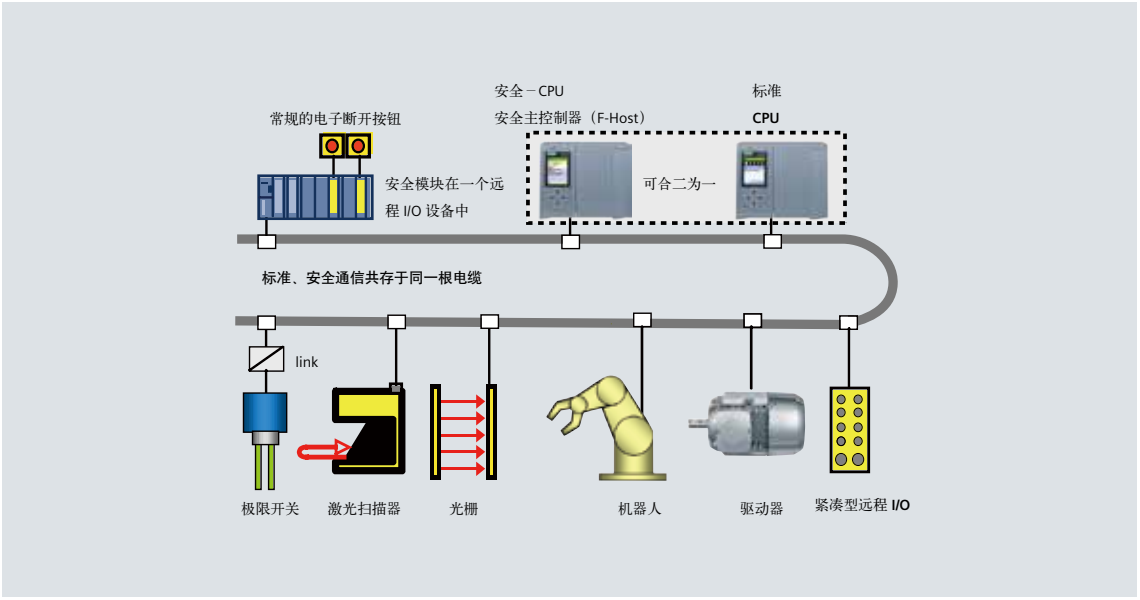


图 4 “单通道（Single Channel）”—方案

PROFIsafe 协议对 PROFIBUS 和 PROFINET 网络的适应达到了理想的程度。安全信息可以同标准信息一道经总线电缆传输（图 4）。

这种“单通道”解决方案也可以使用一台集成的、但逻辑上分离的F-CPU来统一执行标准功能和安全功能，可以有选择地实现高可用性的介质冗余。对于想要在物理上将标准通信和安全通信分隔开来的用户而言，PROFIsafe 同样可以轻松实现。独立的网络的用户也能从集成的 PROFIsafe 技术中获益。

PROFIsafe 协议不会对标准总线协议产生干扰。它也不会受当时的传输通道的影响，无论传输介质是铜缆、光缆，背板总线或无线。传输速率和当时的错误识别也不会影响。对于 PROFIsafe 而言，传输通道是“黑色通道（Black Channels）”原理（图 5）。

PROFIsafe 协议为用户免除了其单个背板总线系统或超越 PROFIBUS 和 PROFINET 的其他通道的安全评估。因此，它将确保整个路径的功能安全，即从一个安全信号的发送器（例如，在一个远离总线终端中的安全模块）至接收器（F-Host），反之亦然（图 7）。

PROFIsafe 协议在安全相关应用方面，按照 IEC 61508/IEC 62061 可达到 SIL3；按照 EN954-1 可达到安全类别 4；按照 ISO 13849-1 可达到 PLe。

PROFIsafe 协议的参数应根据 PROFIBUS 和 PROFINET 的设定处理，例如通过 GSD。但是，这些参数在存储、求值、赋值和从组态工具经 IO-控制器、DP-主站直至安全设备的传输过程中均受到保护。所有安置在远离总线终端的安全设备或安全模块均应使用相同的一组 PROFIsafe 参数，以便实现统一管理。

安全设备的单个安全参数是技术所特有的，例如装有集成安全系统的驱动器，激光扫描器等等。用 GSD 来管理这些参数，会造成资金的极大浪费，且会带来不必要的麻烦。因此，安全设备的开发者们应当能够将其单个组态的、参数化的和诊断的工具（简称为 CPD-工具）经相应的接口集成到工程工具中。这将为各个安全设备或安全模块定位和通信提供方便。

在出现故障的情况下，为了迅速地更换安全设备，系统应当能够集中存储与调用单个设备的安全参数（i Par-Server）。这是由控制器来完成的，该控制器负责启动基于 GSD 的总线参数化进程。

在待补充的指导文件中，应规定使用 PROFIsafe 设备的全部要求，例如：

- 安装；
- 电气安全；
- 电源电压；
- 电磁兼容性；
- 信息安全（Security）。

最后，PROFIsafe 的开发者应通过 PROFIsafe 开发包（PROFIsafe Development-Kits）以及资格中心和测试中心获得对 安全设备或安全模块研发更大可能的支持。

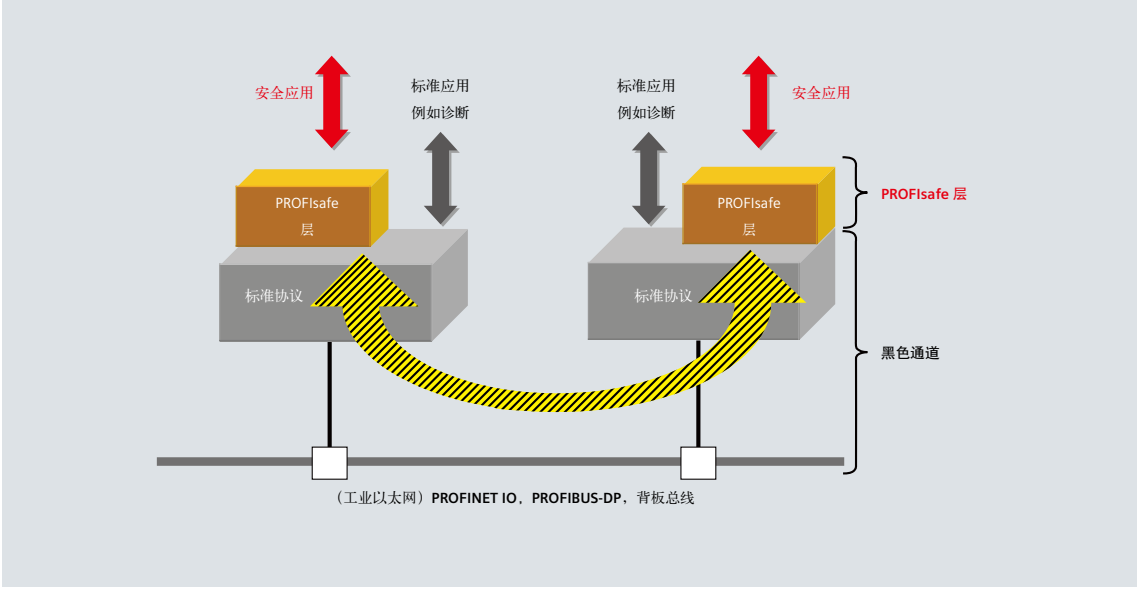


图 5 “Black Channels-黑色通道”原理

在当前的行规版本中，PROFIsafe 实现了所有这些目标。其方案既简单又易懂。

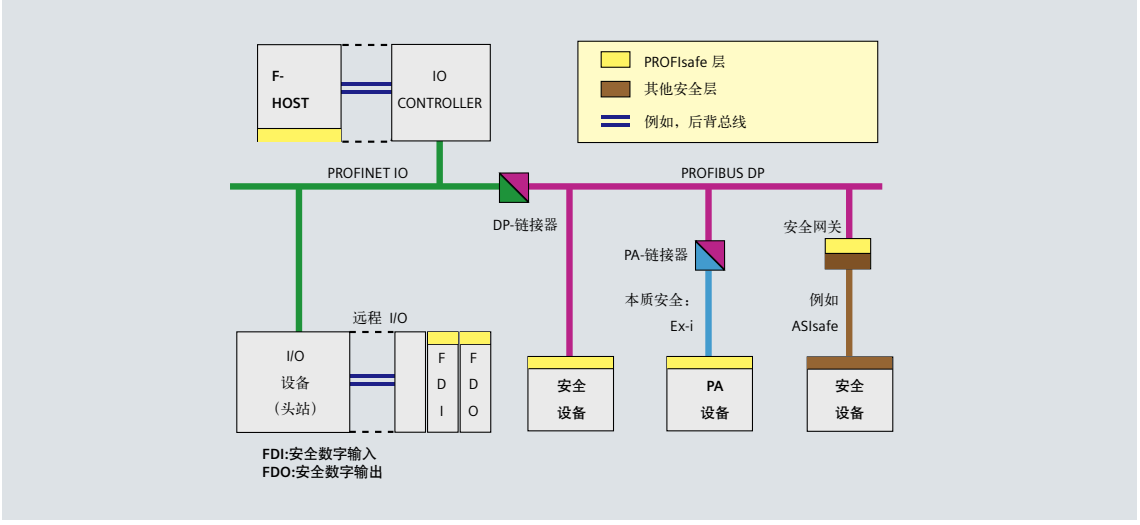


图 6 完整的安全通信路径

在我们深入研讨 PROFIsafe 之前，先将目光投入指定的前提和边界条件。

3. “Black Channels-黑色通道”的设置

尽管 PROFIsafe 使用了“Black Channel”原理，但具备了某些 PROFIBUS 和 PROFINET 的基本性能，在研发 PROFIsafe 的过程中应考虑这些基本性能。

3.1 基本功能

一个总线控制器与其现场设备之间的循环通信（询问与应答原理）是这类基本功能之一。此原理可以直接跟踪找到任何有故障的设备。PROFIsafe 正是建立在此原理的基础之上，因而可以免除自身的音讯应答机制。

另一项功能则是一个总线控制器与其所属现场设备之间的一对一的通信关系。PROFIsafe 建立在此原理的基础之上，以保证信息的真实性。然而，由此产生的结果是，一个单独的安全主控制器（F-Host）只能访问一个模块式现场设备中的一个安全模块（子槽-Subslot）。

3.2 网络部件

一个“Black Channel”可以包括若干个透明的网络部件，例如交换机、路由器、链接器和无线传输区段。

对于 PROFIsafe 而言，为满足 SIL3 要求所采取的限制性措施微不足道。因此，允许使用所有类型的交换机，但只允许串联 100 个交换机。一个 PROFIsafe 岛屿的安全地址空间大小必须有明确的规定。彼此相连且安全地址空间重迭的岛屿必须用多端口路由器将它们彼此分开。除此之外，就再也没有从 PROFINET 经由 PROFIBUS 直至本安版的 MBP-IS 的其他限制（图 6）。

3.3 无线通信 & 数据安全

只要保证足够的可用性（无故障发生）和信息安全性（Secutity），就允许无线通信。

PROFIsafe 详细描述了对无线通信系统以及与工业太网主干线或因特网（所谓开放性网络）相连接的有线网络信息安全所规定的要求。

措施 / 差错	安全报文序列号（活标志）	超时控制（以收据确认）	代码名称（发送方与接收方之间的标志）	数据完整性校验（CRC- 检验）
重复	✓			
丢失	✓	✓		
添加	✓	✓	✓	
错序	✓			
数据搀假				✓
延迟		✓		
寻址出错			✓	
伪装（标准拆报文伪装成故障安全报文）		✓	✓	✓
在交换机中重复出现的存储器失效	✓			

图 7 传输错误类型和安全措施

3.4 数据类型

现场总线通信可以识别许多不同的数据类型，以便进行信息交换（见参考文献）。为减少复杂程度，PROFIsafe 只提供了其中有用的一部分。

4. PROFIsafe 解决方案

两个同等通信系统之间进行的安全通信应保证

- 真实的数据在
- 指定的时间到达
- 指定的接收器。

在以错综复杂的网络拓扑结构进行信息传输的过程中，可能会出现各种各样的错误，有硬件故障、电磁干扰，也有其他的干扰。信息有可能丢失、混入、重复、延迟或出现错序和/或显示虚假的数据。在安全通信的情况下，可能出现“伪装-Maskerade”：标准信息被错误地送达某一个安全设备，且冒充成安全报文。此外，不同的传输速度可能引发总线部件中的存储器失效。PROFIsafe 从文献的许多具体措施中总共采纳了 4 种，如图 7 中所列。

4.1 安全措施

这些相应的措施包括：

- 安全信息（报文）的序列号（“sign-of-life”-活标志）；
- 以收据确认的定时控制（“watchdog”-看门狗；“Time-out with receipt”-以收据确认的超时控制）；
- 发送方与接收方之间的标志（“安全地址”）；
- 数据完整性校验（CRC＝cyclic redundancy check，循环冗余校验）。

接收方根据序列号可以检查其它所收到的报文是否完整，序号是否正确。序列号随同收据重返发送方，以便查验。原本在这里设置一个简单的“触发位”（Toggle-Bit）就足够了。但有些总线部件，如交换机，拥有一个中间存储器，因此，PROFIsafe 选择了一个 24 位计数器。

在安全技术中，传递具体的过程信号和数值固然很重要，在过程容错时间之内这些信号和数值的更新也很关键。因此，一个安全设备在超时的情况下能够自动地释放预定的安全措施，例如停止动作。安全设备为此使用了一个看门狗定时器，当一帧安全报文以新的序列号到达接收方时，该定时器将重新启动。

控制器与现场仪表之间的一对一的通信关系简化了出错的安全报文的识别。为此，发送方和接收方需要在整个网络中有一个无歧义的、用来检验安全报文真实性的标志。在 PROFIsafe 中，此标志就是“安全地址”。

循环冗余校验（CRC）在识别有错的数据位方面起着关键作用。对残余风险概率（Restfehlerwahrscheinlichkeit，Residual error Probability）的研究是十分必要的，为此 IEC 61508 的有关规定都考虑到了。根据这些规定可以估算出安全功能允许的危险失效概率（SIL）。PROFIsafe 遵循该标准的规定（图 8）。

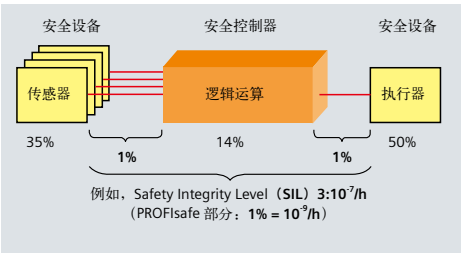


图 8　安全功能与 SIL

F-I/O data	Status/ Control Byte	CRC signature （代码）
		通过 F-I/O data，F-Parameter 和序列号
最大 12 或 123 bytes	1 byte	3 或 4 bytes

图 9　PROFIsafe 报文格式

根据 IEC 61508 标准的规定，一个安全回路包括所有的传感器、执行器、传输元件和逻辑处理单元，它们均含有安全功能。IEC 61508 为不同的安全完整性等级（Safety-Integrity-Level，SIL）定义了失效概率。例如，SIL3 对应的失效概率为 10^{-7}/h。PROFIsafe 为传输只须贡献 1% 就行，所对应的危险失效概率为 10^{-9}/h。利用这些预先给定值可以决定适合安全报文规定长度的 CRC-多项式。由此产生的未知错误的安全报文的剩余差错概率在最大位错误概率为 10^{-2} 的情况下可以保证所要求的值。PROFIsafe 使用一个 24 位和一个 32 位 CRC-生成多项式（Generator-Polynom），以便计算相应的 3 或 4 字节长的 CRC-代码。所选的 CRC-多项式的特性和专用的计算方法使 PROFIsafe 不依赖于“Black Channel”的所有错误识别机制。

4.2 PROFIsafe 报文格式

在一个安全控制器（F-Host）与其安全设备（F-Device）之间的安全报文被当作“有用载物”在 PROFIBUS 和 PROFINET 报文中传输。当一个模块式安全设备拥有若干个安全模块时，此“有用载物”则由若干安全报文所组成，图 9 所示为 PROFIsafe 帧的格式。

考虑到前面提到的数据类型子集，PROFIsafe 帧以安全输入/输出数据（F-Input/output data）开头。一定的安全设备的数据结构在其所属的 GSD-文件（通用站描述-General Station Description）中有规定。制造业自动化与过程自动化对一个安全系统提出不同的要求。前者以短信号（“比特”或“位”）运作，这些短信号必须迅速地加以处理；后者以较长的过程值（“浮点”）运作，对其处理允许速度放缓。为此，PROFIsafe 提供了两种不同长度的数据结构，其中之一限长为 12 字节，为此需要 3 字节长的 CRC-代码；另一个限长为 123 字节，使用一个 4 字节 CRC-代码。

在一个单一的安全控制器报文中，跟在安全输入/输出数据后面的是一个控制字节（Control Byte），要不然就是一个状态字节（Status Byte）。两者都是为 PROFIsafe 协议机的同步化服务的。

一个安全报文的结尾部分是一个 CRC-代码，它取决于安全输入/输出数据。

序列号不用安全报文传递。发送方和接收方各自拥有计数器，它们借助控制与状态字节达到同步。同步化正确与否可通过将计数器的值输入 CRC-代码运算中来进行监控。

“安全地址”也被安全送入 CRC-代码运算中。

4.3 PROFIsafe 服务

安全报文的发送方与接收方的工作层位于“黑色通道-Black Channel”之上（图 4）。实现 PROFIsafe 层的是软件（“驱动”软件）。其核心是用于安全报文正规的循环处理的、以及偶尔操作（例如，系统启动、开与关、CRC-错误处理等）的一台状态机。图 10 所示为 PROFIsafe 层如何同单一的安全设备技术和安全控制器应用程序协作。

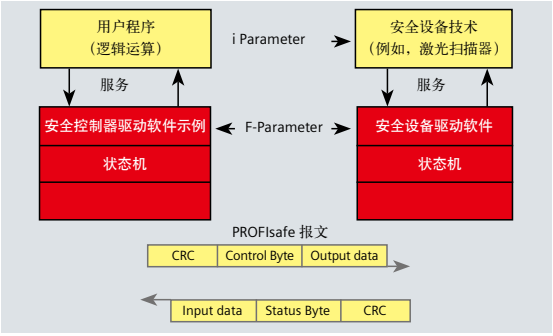


图 10　安全控制器和安全设备中的 PROFIsafe 一层

■ 4.3.1 安全主控制器（F-Host）服务（安全控制器服务）

安全控制器服务首先负责完成安全输入/输出数据的交换。在加速或故障情况下，现实的过程值将被预置的安全值（“0”）所取代，以便将接收方置于一个安全的（无源）状况。

在控制字节中有一个标志（“activate_FV”）是专为那些需要放缓速度进入安全状态以取代“关闭”的安全设备提供的。一个安全设备从它自身通过状态字节中的标志就可以得到其当前的的安全状况（“FV_activated”）。

安全通信故障迫使安全控制器—驱动器被切换到安全状态。一般情况下，安全功能不允许自动地和未经人工干预从安全状态转换为正常工作状态。为了将操作员干预和以收据确认的必要性告知应用程序，PROFIsafe 提供一项额外的服务（“OA-Req”）。此外，PROFIsafe 也使安全设备获悉有关可选用 LED 显示，但尚未做出确认的信息。一旦操作人员确认，便可通过相应的服务把应用程序交给安全控制器驱动器（“OA-C”）。

一个安全设备的技术专用参数称之为 i 参数（i Parameter）。如果一个安全设备在运行中需要更改 i 参数，则 PROFIsafe 在这里也管用。有一项专门的服务允许应用程序释放安全设备去使能新的 i 参数（“iPar-EN”）。另一项服务以信号告知应用程序已准备好恢复安全操作（“iPar-OK”）。

■4.3.2 安全设备服务

PROFIsafe 的安全设备服务可以实现安全输入/输出数据交换，安全状态置位以及有关 i 参数管理和上面已涉及到的向操作员提出确认询问的报告。

除此以外，安全设备可以通过状态字节中的一个标志（“Device_Fault”）向安全控制器报告设备故障。

使用 PROFIsafe 实现数据传输时，所要求的安全设备安全功能持续时间必须足够长（至少为 2 个序列号增量）。为此，有一项特殊服务通过查询序列号给予支持。

PROFIsafe 层的诊断数据被送至安全设备的技术特定的部分。

安全设备将安全参数交给 PROFIsafe 层。安全设备在总线系统提速期间，除了所有其他的参数外，还获得了这些安全参数。剩下来的问题是，这些安全参数究竟包含了什么内容？

4.4 安全参数

安全参数包含了许多旨在使 PROFIsafe 层适应用户给定的要求和以单独的途径（分散的）检验参数化。最主要的安全参数有：

- F_S/D_Address（简称：F-Adresse，安全地址）
- F_WD_Time（安全看门狗时间）
- F_SIL（安全安全完整性等级）
- F_iPar_CRC（F-i 参数-循环冗余校验）
- F_Par_CRC（安全参数-循环冗余校验）

F_S/D_Address 是在一个 PROFIsafe 岛屿之内安全设备的一个无歧义的地址。安全设备的技术部分同现场的地址开关进行数值的比较或者对比所设定的 F-Address，其目的在于检验连接的真实性。

F_WD_Time 将一个看门狗定时器定义在 ms（毫秒）级。定时器监控持续时间，直至接收下一个有效的 PROFIsafe 报文。

F_SIL 给出用户对当时的安全设备所期望的 SIL。此值将同制造厂在本地存储的值相比较。

F_iPar_CRC 是一个由安全设备技术特定部分的所有 i 参数计算出来的校验和。

最后，F_Par_CRC 提供一个 CRC 代码，它是为所有的安全参数而生成的，而且确保安全参数的传输无差错。

有关 PROFIsafe 协议的概述就到此为止。下面我们进一步探讨其他问题。我们来看一看，PI 除此以外还得做些什么，你准备好了吗？

5. 如何实现?

首先我们要一一列出所需的和新增的 PROFIsafe 文献资料（参见参考文献）。读者应当只引用这里所指定的或者较新的版本。PROFIsafe 规范 V1.30 是一个较老的版本，仅用作资讯，不可用作开发的依据。

下面要研讨的内容至少涉及安全基本标准 IEC 61508，或者就开发过程中和组织过程中为达到设备必要的安全性必须注意的事项，倾听专家们的建议。一般的原则是：PROFIsafe 的实现不会使一个标准设备变成一个安全设备。“技术”结构，协议和这两者如何实现的方式、方法决定了设备所达到的安全完整性等级（SIL）。

5.1 安全等级

虽然 PROFIsafe 所适用的安全功能可以达到 SIL3，并非必须要开发同样达到 SIL3 的安全设备。所要求的安全等级取决于最终的应用和安全功能的定义。安全等级较低的安全设备可以通过冗余或者其他措施达到较高的 SIL 等级。

5.2 安全设备（F-Device）

实现 PROFIsafe 驱动器软件有两种可能性。软件的开发可依据规范或者使用一个市场上可得的 Starter-Kits(www.profisafe.net)。使用 Starter-Kits 的优点十分明显：驱动软件通过检验，含有额外有价值的信息，提供专用工具和技术支持。

所有可用的芯片（ASICs）和通信层均支持面向 PROFIBUS 和 PROFINET 的接口。PROFIsafe 驱动软件可以与之相适应。

■ 5.2.1 GSD 的防护

在 PROFIBUS 或 PROFINET 网络中，每台设备都有一个 GSD-文件（General Station Description，通用站描述）。在确定 GSD 中一个安全设备的一般参数之后，必须对安全参数进行编码。此安全参数块将通过一个特定的 CRC-代码（“F_ParamDescCRC”）来防止存储器介质上的数据被篡改。有一个组态工具可以根据安全参数块中包含的特定的 CRC-代码来校验安全参数块的真实性。

■ 5.2.2 I/O 数据的防护

GSD 也描述 F-I/O 数描的格式。另有一个 CRC 代码（“F_IO_StructureDescCRC”）用来确保 GSD 这一部分的安全。

■ 5.2.3 i Parameter（i 参数）

安全设备的多种不同的技术造成了大量的单个安全参数（i 参数）。

i 参数的数量从安全模块的几个字节到一个激光扫描器多达若干 10 千字节不等。大多数安全设备都已经有了组态、参数化和诊断的软件工具（CPD-工具）。因此，通过 GSD 来处理 i 参数的意义不大。

PROFIsafe 推荐使用新的所谓 i Par-Server（i 参数服务器）。负责提供 i 参数服务器的是安全控制器制造商。服务器可以安置在安全控制器与安全不相关的部分，即参数化主站中，或者安置在一个下属控制器中，例如在同一网络中的一个 PLC 中或一个工业 PC 中。

图 11 所示为 i Par-Server 机制的各个步骤。安全设备的 i Par-Server 同网络组态和安全参数化一道被初始化（1）。在安全状态（FV）下，安全设备才可以进入循环数据交换阶段。从工程工具可见，某个 CPD 工具经合适的接口（2），例如 TCI（Tool Calling Interface，工具调用接口）或者 FDT（Field Device Tool，现场设备工具）而被启动。

启动时，至少已被组态的设备网络地址一同给出。之后，CPD 工具可以使参数化、投运和测试得以实现（3）。这些过程结束之后，计算出 iPar-CRC-校验和，且以十六进制格式显示。其数值被引入工程工具组态部分中的输入区段“F-iPar-CRC”（4）。一次新的启动也将F参数“F_iPar_CRC”供给安全设备（5）。在通过一次最终验证之后，安全设备有资格要求为其 i Par-Server-Instanz（i 参数服务器实例）加载（Upload）。此时，它利用一个特定的诊断报文。i Par-Server 轮询诊断信息（例如，RDIAG-FB），读取 Upload-询问信息（R），启动 Upload 过程（7）。此时，i 参数在运用非循环服务（Read Record，读记录）的条件下作为实例数据被存储在 i Par-Server 中。

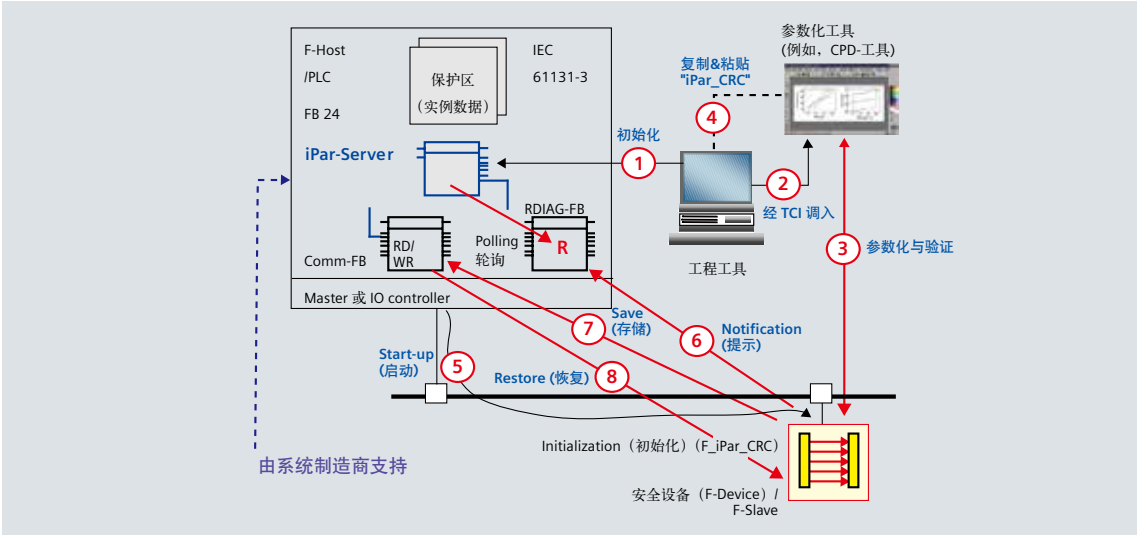


图 11　i Par-Server（i参数服务器）— 方案

如果有一个出错的安全设备被取代，则新的安全设备在系统加速时直接获得它的安全参数，包括“F_iPar_CRC”在内。由于新的安全设备也包括装备了易失性存储器的安全设备在内，并不具备适配的 i 参数，新的安全设备在校准“F_iPar_CRC”校验和时才识别出一个错误。其结果是，它要求从 i 参数服务器实例中下载 i 参数，此时要再次完成标准诊断。i 参数服务器从诊断信息中读取询问值（R），启动下载过程（Write Record，写记录）(8)。安全设备因为有这种传递方式通过简单的途径就能获取原始的功能，而无需 CPD 工具或其他工程开销。

■ 5.2.4 PROFIdrive（现场总线驱动技术）

IEC61800-5-2定义了集成安全驱动器的安全功能。其中有一系列停车功能（Stop），即：

- 安全断开的力矩；
- 安全停车1；（Safety Stop1）
- 安全停车2；（Safety Stop2）
- 安全操作停止（Safety Operation Halt）。

监控功能方面有：

- 安全限制的加速度；
- 安全限制的速度；
- 安全限制的矩/力；
- 安全限制的位置；
- 安全限制的步程；
- 安全的运动方向；
- 安全限制的电动机温度。

图 12 表示常用的电子机械部件如何被电子的、安全停车功能和监视功能所取代。其主要目的就是监视驱动器控制功能且在出现故障时将其断开。PI 的“PROFIdrive”工作组在 PROFIdrive 规范的增扩本中规定了一部分这样的功能（详见参考文献）。

■ 5.2.5 PA Device（过程自动化设备）

过程自动化的安全设备遵循专业标准 IEC 61511 和“经使用验证”（Betriebsbewährtheit/Proven-in-use）的准则。一个PA-设备在一定的情况下，可以达到一个较高 SIL 等级，如果它是经使用验证的话。通常情况下，PA-设备是依据 IEC 61804开发出来的。在这方面，设备描述（EDD）有其重要作用。因此，PI 的“PA-设备”工作组制订了 PA-设备规范的修订本，其中规定了 PA-设备的 PROFIsafe 平台的应用以及参数化方法。

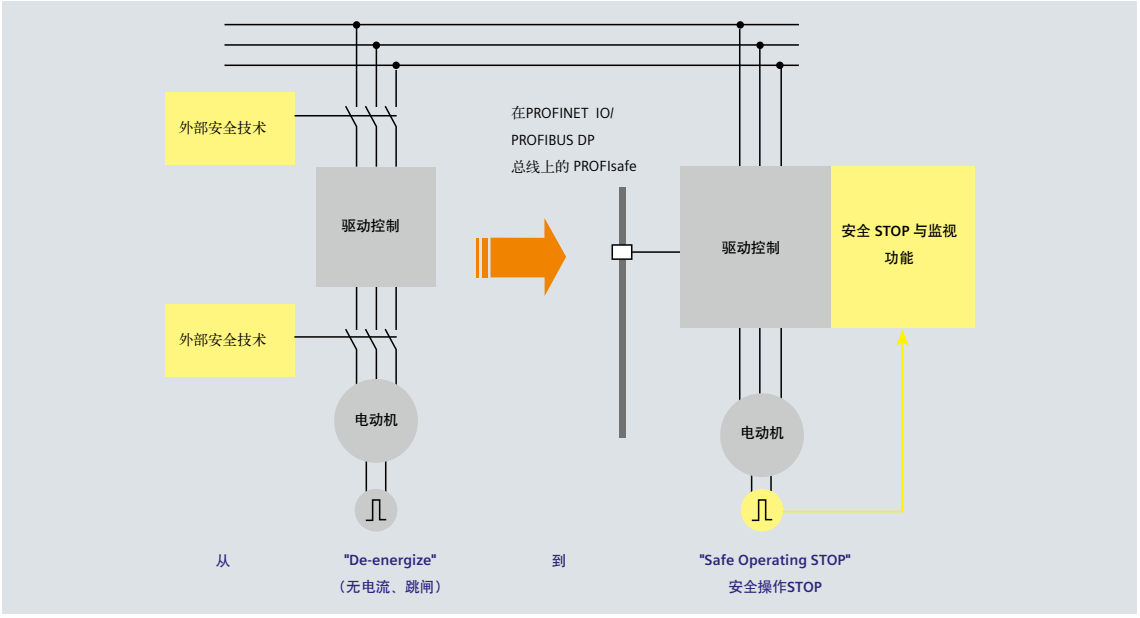


图 12 带集成安全停车（STOP）和监视功能的驱动器

■ 5.2.6 I&M-功能（识别与维护功能）

自 2005 年起，使用非循环服务的所有 PROFIBUS-设备都必须提供 I&M-功能。I&M表示“Identification and Maintenance，识别与维护”。I&M-功能允许以标准的方式读取设备的制造商代码，它的目录号和系列号以及硬、软件的版本。用户依据制造商代码和 PI-网页服务器的附加信息可以被链接到制造商的网页上直接获取最新的产品信息（“Profile Guideline Part 1”）。

■ 5.2.7 诊断

PROFIBUS 和 PROFINET 有一个最主要的优点，就是在出现意外的情况下，如事故或功能失效，依然能够为现场设备、操作人员提供相关信息。利用良好的诊断机制可以缩减生产设备的停机时间，换句话说也就是节省费用。诊断方案除了考虑信息的编码之外，也考虑到使用不同语言和旨在提示遇到特殊情况下的解决方案的（“Profile Guideline Part 3”）。

5.3 安全控制器（F-Host）

使用 PROFIsafe 通信技术的安全控制器有各种各样的结构，这可能与制造商的策略有关，既有独立的 F-CPU，又有集成的，但逻辑上分离的连带标准 CPU 的安全方案。

■ 5.3.1 可能的结构

安全处理可以用多种方式来完成：例如，差分校验的硬件冗余，软件冗余，保护装置，或者现有的分散式硬件平台。由于量很大，开发 Starter-Kits 便毫无意义，主要因为实现 PROFIsafe 驱动软件的开销是微乎其微的。

■ 5.3.2 一致性等级（Conformance Classes）

为了能够保证所有安全设备和所有市场上可得的 PROFIsafe 安全控制器之间的相互配合准确无误，PROFIsafe 规定了所谓安全控制器的一致性等级。满足这些要求是通过 PI 认证的先决条件（图 13）。

6 认证

不同制造商的各种各样的产品在一个 PROFIsafe 岛内进行通信。为了使它们在通信中发挥正确的功能，产品必须按照 PROFIsafe 规范来实现其性能。一般情况下，PI 的业务部门根据它授权的测试实验室的测试报告出具一份证书，以资证明产品的一致性。

6.1 PROFIsafe 的测试

PROFIsafe 协议基于最终的状态机。于是，存在着这样的可能性，即通过一个与协议相符的合法工具，从数学上来验证符合规定的 PROFIsafe 功能，甚至在出现两个彼此毫不相干的差错和故障的情况下进行验证。通过对所有能想得到的功能和负载场景系统地“从头到尾演示一遍”，才达到了上述目的。这些场景曾被用来开发一个全自动的“PROFIsafe 层测试程序”，用来检验安全设备和安全控制器同 PROFIsafe 规范的一致性。它是三级认证过程的一部分，该认证过程根据 IEC 61508 包括了全部的安全认证项目（图 13）。

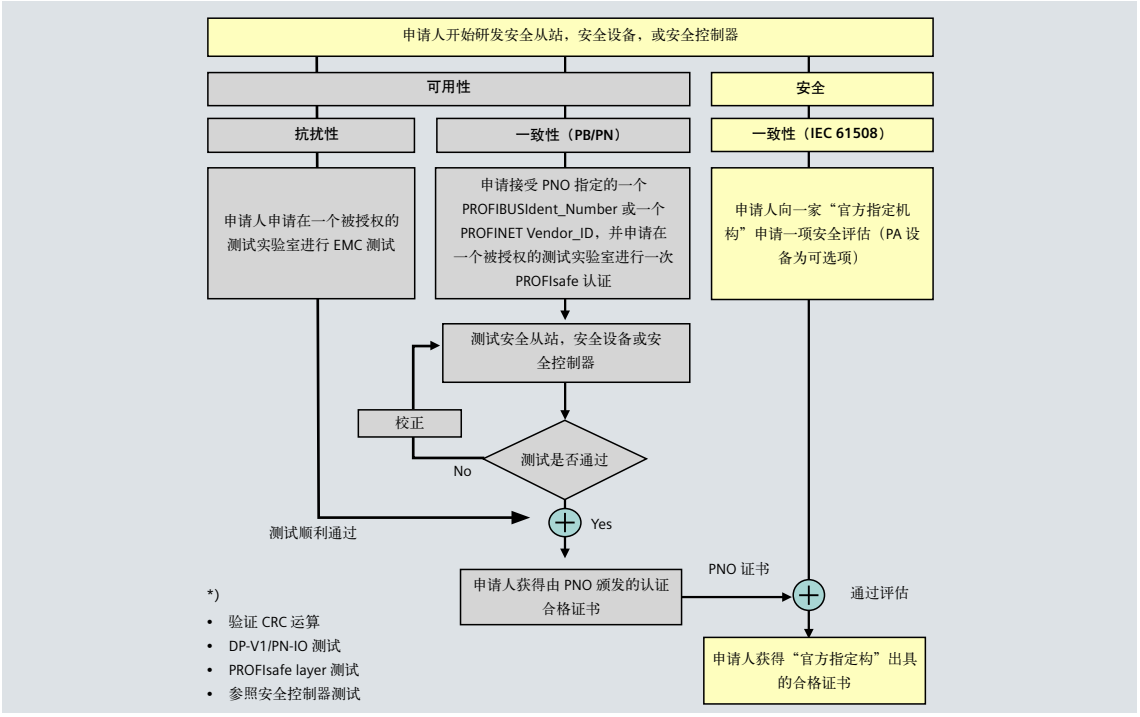


图 13　测试与认证过程

6.2 安全评估

这里应当说明的是，PI 测试实验室在根据 ISO 17025 被授权的检测机构的委托下实施 PROFIsafe 层测试。这些检测机构主要有：

- TÜV（全世界的）
- SP（瑞典）
- INRS（法国）
- HSE（英国）
- BGIA（德国）
- FM（美国）

上述机构是极少数几个被允许按照 IEC 61508 进行安全评估的机构。

对于任何一个安全设备，都按照规定编写了一本手册，其内容必须包括有关 SIL 要求极限 SIL_{CL}（Claim limit）和每小时危险失效概率 PFH_d（Probability of dangerous failure per hour）。

PI 出台了一项 PROFIsafe 设备测试与认证规范。目前共有两个经 PI 授权专门从事 PROFIsafe 测试与认证的测试实验室。

7. PROFIsafe 的应用

PROFIsafe 单凭一个安全通信协议规范是不会那么完善的。可能会出现下面的问题，例如：

- 我必须为我的安全设备提供由未知电源通过总线电缆馈电的高压保护吗？
- 我可以为我的安全设备使用网络中标准设备所用的同一个 24V 电源吗？
- 我应该如何按照 IEC 61508 的要求对我的安全设备进行“增强的抗干扰性”测试？
- 在安装过程中我必须注意哪些事项？
- 应当保证什么样的信息安全（Security）？

在 PI 规则“PROFIsafe Enviromental Requirements，PROFIsafe 环境要求”中可以找到上面这些问题和其他问题的答案（见参考文献）。

7.1 电气安全

IEC 61158 和 IEC 61784-1/2 要求网络中的所有设备遵守其所在国（例如，以 CE-欧盟委员会标志）的法定要求。因此，在工业应用中必须根据 IEC 61010 或 IEC 61131-2 按照不同的设备类型采取防电击保护措施，它们称之为 PELV（Protected Extra Low Voltage，特低保护电压），在出现故障时将电压限制在允许的、对人无危害的程度上。

由于电气安全要求通常是法定的，花在安全设备和安全控制器方面的安保费用还是“可以忍受的”。

7.2 供电电压

安全设备/安全控制器和标准设备均可以使用同一个 24V 电源。在这两种情况中，都必须根据法规保证 PELV。

7.3 抗干扰性

在安全应用方面，相应的安全要求规范（SRS）必须规定一个抗电磁干扰的极限值，以保持一定的电磁兼容性。此极限值的确定既要考虑 IEC 61000-2-5 的各种现象，又要考虑所要求的 SIL 等级。

IEC 61326-3-1 规定了在一般的工业应用中安全设备的抗干扰要求。

像 IEC 61496-1 这样的产品标准，针对个别的现象规定了另外的、更高的测试水准。

过程工业中的环境条件可能完全不同于一般的工业环境。因此，对于 PA-设备可以引用 IEC 61326-3-2 的特殊要求和特征条件。

针对 PROFIsafe 制订了一项专门的“EMC-测试环境规范”。

7.4 高可用性

功能安全所涉及的是保护人免遭伤害，例如断开有危险的设备。这类安全功能的一个特征量就是安全完整性等级（Safety Integrity Level, SIL）。它表示每小时功能安全的危险失效概率，例如 SIL3 时为 10^{-3}/h。

而高可用性所涉及的却都是在出现故障的情况下，仍应维持自动化设备的运行。高可用性的一个特征量是一个与总运行时间（例如，99.99%）有关的设备运行准备程度。除此以外，冗余决定一个系统的故障容忍度。

	PROFIsafe	Redundancy（冗余）	PROFIsafe 与 Redundancy
Application（应用）	工厂与过程自动化 压力机、机器人，限位开关，切断阀，以及燃烧控制与缆车等	过程自动化； 运输基础实施 化工与制药生产，炼油，海上石油平台，隧道	过程自动化； 运输基础实施 化工与制药生产，炼油，海上石油平台，隧道
High Availability（高可用性）	–	尽可能无故障时间（故障裕度）	尽可能无故障时间（故障裕度）
Safety（安全）	无危险失效（法律或保险业务的要求）	冗余本身并非提供安全保障	无危险失效（法律或保险业务的要求）

7.5 安装指南

PROFIsafe 的目标是将功能安全通信集成到标准的 PI-网络中，且不影响现有的安装规程。为了运行可靠和实施现行的法规，迫切地要求遵守 PROFIsafe 规范和指南，以下就若干重要的议题进行探讨。

■ 7.5.1 先决条件

同在一个网络中的所有标准设备和安全设备必须按照 7.1 确认电气安全。

所有安全设备必须通过依据 IEC 61508 进行的认证，用于过程自动化的安全设备则必须通过依据 IEC 61511 进行的认证。对 PROFIsafe 规范的一致性须经被授权的 PI-测试实验室的测试并确认。

在一个 PROFIsafe 网络中的所有其他的标准设备必须以 PI 的相应证书或同等价值的证明文件来证实其同 PROFIBUS 和 PROFINET 的一致性。

■ 7.5.2 边界条件

在 PROFIBUS DP 中是不允许使用支线的。

对于 PROFINET IO 而言，有下列规定：

- 最多可串联 100 个交换机；
- 每个子模块只有一个安全控制器；
- 所有网络部件都符合工业要求（例如，依据 IEC 61131-2）；
- 不可使用单端口路由器（Single-Port-Router）来分隔 PROFIsafe 岛屿（标注唯一的安全地址）。

■ 7.5.3 布线

PROFIBUS 和 PROFINET 规定使用在插座上带双面屏蔽层的屏蔽电缆，以达到更佳的抗电磁干扰性能。通常情况下，需要实现电位平衡。如果不可能做到，则可使用光纤来达到目的。

在规定的 EMC 和微弱干扰的影响下，用户也可以使用无屏蔽电缆，但须自行承担后果。

■ 7.5.4 可用性

甚至在屏蔽电缆中，数据导线也会因信号噪声而被干扰。例如，当一个变频器的中间电路电压未被足够地过滤时。信号干扰也可能因缺少终端电阻而产生。这并非是安全问题，而是可用性问题。自动化设备拥有足够的可用性，是安全的一个必要的先决条件。不具备足够可用性的生产设备，其安全功能必将导致误脱扣（Nuisance Trips）的发生。而这种情况又会使生产负责人误入放弃使用安全功能的歧途，最终会导致灾难性的后果（例如，“Bhopal-效应”：1984 年，印度 Bhopal 地区某化工厂的厂主，曾因设备可用性不够高而导致“误脱扣”之事干脆取消所有的安全功能，导致该厂在一场重大毒气泄漏事故中毁于一旦）。

PI 的会员企业提供了许多用来研究网络中传输质量的工具、方法和检验程序一览表。

■ 7.5.5 “紧急停止（E-Stop/Not-Halt）”方案

PROFIsafe 是许多安全设备，尤其是集成安全驱动器的开拓者。今天的驱动器可以在不关闭马达的情况下处在安全的状态（Not-Halt）。例如，新的安全功能 SOS（安全运行停止）使马达在掌控下保持在一个确定的位置上。这种新的可能性要求用户改变观念。过去，人们是通过一个“紧急-关闭”按键使马达在物理上与电流断开的。因此，在更换马达时不会产生电流对人的危害。

新的 IEC 60204-1 描述了可关闭的马达保护开关，断路器和带保险的主开关（图 15）。此外，它规定了带有单独的中线“N”和保护导线“PE”以及介于驱动器与马达之间的屏蔽电缆的一个 5-线系统（TN-S）。对于许多安全问题而言，IEC 60204-1 是一个极有价值的“宝库”。在有关的美国标准 NFPA 79 中包含了一些适合北美市场的条款（图 3）。

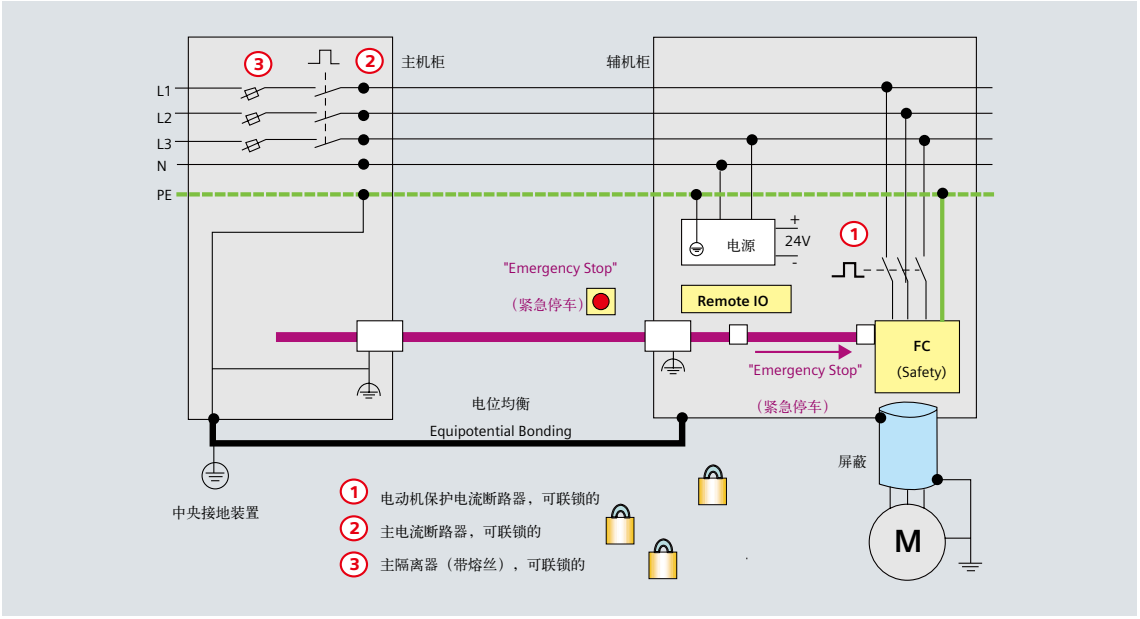


图 15　IEC 60204-1的“E-Stop/Not-Halt”一方案

7.6 无线传输

越来越多的应用，例如无人驾驶的运输系统（AGV），旋转式机械，立式机器人和操作终端，使用无线传输来连接现场总线。PI 支持WLAN和蓝牙解决方案。PROFIsafe 以其对于位错误概率为 10^{-2} 的适用性而被允许用于两个“黑色通道”（Black Channel），但是，下面有关信息安全（Security）的思考也正是我们所关注的。

7.7 信息安全（Security）

基于工业以太网，即一个开放性网络的 PROFINET 在进行无线传输时不得不面临着信息安全（Security）的问题。PI 遵循所谓信息安全区（Security-Zone）的方案，该区可以当作封闭性网络来考虑（图 16）。

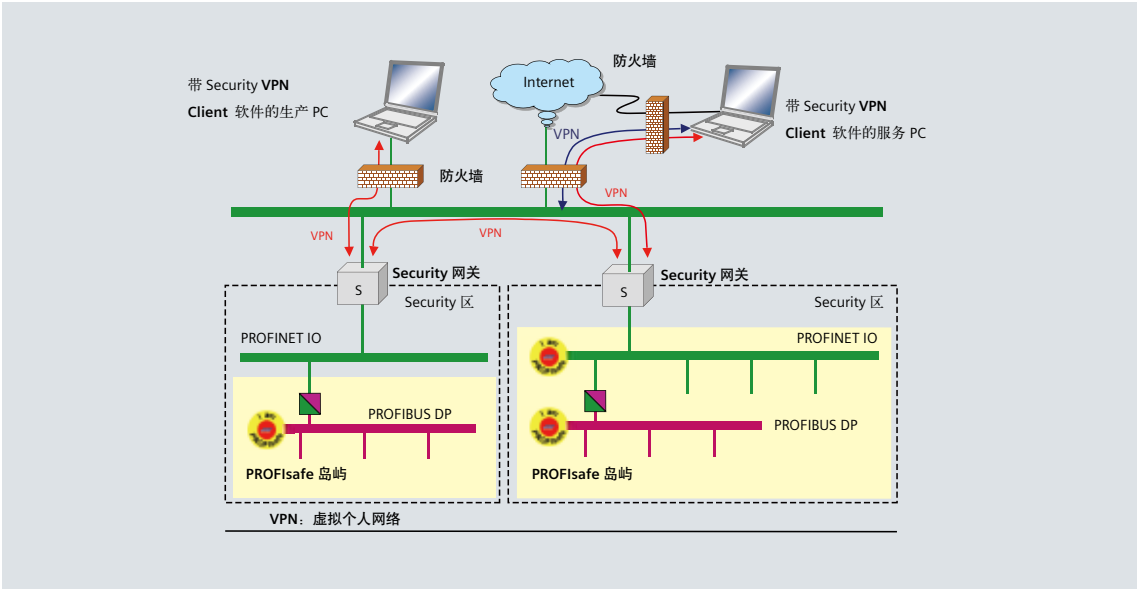


图 16　“封闭性”和“开放性”网络的 Security-方案

经一个开放性网络，如工业以太网，从一个数据安全区到达另一个的惟一可能性是通过所谓数据安全—网关（Security Gate）。这些网关利用可靠的安全技术，如 VPN（Virtual Private Network，虚拟个人网络）和固件，以防止未经许可的访问。当不可避免地连接开放性网络时，PROFIsafe 网络必须始终处于数据安全区之中，且通过数据网关受到保护。

IEEE802.11i 为无线传输规定了 PROFIsafe 网络中必要的数据安全措施。只允许在基础模式（Infrastructure-Modus）中运行，特殊模式（Adhoc-Modus）是不准许存在的。详细情况 PROFIsafe 规范已有描述（见参考文献）。

7.8 反应时间

一般情况下，常见的控制功能应答时间，对于安全功能而言，已足够短暂。然而，安全应用达到了安全功能的临界响应时间（SFRT）。用光栅作为保护装置的压力机就是一个例子。一位机械设计师在最初的研发阶段就必须知道一个光栅至少必须离开危险的压力机多远。普遍适用一条规则是：人手运动的最大速度为 2m/s。如果光栅的分辨力足以识别单个手指（欧标 EN999），则最小间隔可以从公式 S＝2m/s × SFRT 算出。否则需要加上修正数。

SFRT-Safety Function Response Time（安全功能响应时间）的背后到底蕴藏着什么秘密？

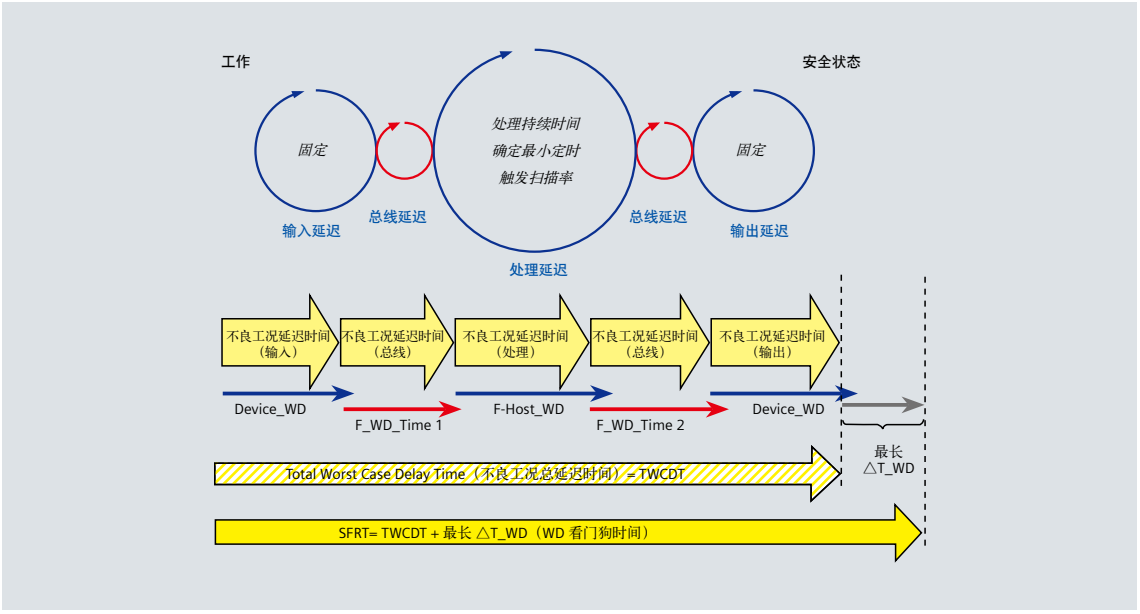


图 17　安全功能响应时间（SFRT）

图 17 所示的模型清楚地说明了 SFRT 的定义。该模型由一个传感器，一个安全传输段，信号处理单元，另一个安全传输段和一个执行器所组成。所有组成部分在信号通过时均有各自的统计变幅。横穿系统最大的运行时间 TWCDT 是在最为不利情况下的延滞时间，即系统的所有元部件均需要最大的时间，在安全情况下，还要外加组成部分之一在信号通过的时刻失效。因此，在出现故障的部分还必须加上一个直到看门狗做出响应的差分时间（在出现一个以上的故障时必定无输出）。于是，SFRT 等于 TWCDT 与上面所提到的差分时间之和。

对于任何单一的安全设备，其符合 PROFIsafe 规范的延滞时间信息必须写进安全手册中，以便能够用工程设计工具估算出 SFRT。

8. 整体安全考虑

以上我们学习了许多有关 PROFIsafe 应用方面的知识。但是，安全应用和安全功能方面的情况又怎样呢?

8.1 法规 & 标准

许多国家从法律上制订了危险机器的安全要求。在欧盟通行的机器设备法规是 98/37/EC。它包含一个所谓“调和标准”一览表。对于机器制造商而言，如果相关标准的要求得到满足，便可推测同法规的一致性。

涉及 PROFIsafe 的相关标准有：IEC 62061，ISO 13849-1，ISO 12100-1 和 ISO 14121（见 1.3 和图 2）。

8.2 风险降低

固有安全型机器的发展趋势越来越好，这类机器可以避免危险的发生。在 ISO 12100-1 的第 1 部分举例了所有可能发生的危险。在第 2 部分，它根据风降分析说明了降低自动化风险的一种逐步逼近法。此种方法是由风险分析和风险评估所组成：

- 详述极限和预定的应用；
- 查明危险和整个生命周期的危害状况；
- 估计已查明的每一项危险和危害状况的风险；
- 评价风险和有关风险减少必要性的关键。

利用以下“三步曲”，即

- 固有安全的设计，
- 保护装置和补充的保护措施，
- 对用户残余风险的澄清，

设计师就可以避免危险或者通过保护措施降低危险。

保护装置和补充的保护措施构成了安全功能的基础，如光栅、所属的逻辑连接和电动机保护装置。

8.3 IEC 62061 的应用

IEC 62061 和 ISO 13849-1 提出了处理安全功能的方法。前者（IEC 62061）很好地覆盖了 PROFIsafe 技术和安全控制器，而后者（ISO 13849-1）则额外地涵盖了液压、气动、电气和机械部件。

IEC 62061 要求制订出一台机器生命周期的安全计划—从设计、操作员职责、调试、更换和维护直至拆卸。

8.4 风险评估

基于 ISO 14121 的上述两个标准描述了一种近似的安全功能风险评估方案：

风险（Risiko）＝危害程度 × 发生概率

发生概率由停留时间，其频率和防止危险发生的可能性等参数所组成。

8.5 SIL-确定

这两个标准提供了可以计算的特征参数。其中之一为所要求的 SIL，另一个为所要求的 PL（见 1.3）。二者中的某一个特征参数可以换算为另一个。从长远看，如果风险评估在工程设计工具中被交互地调用，则它们二者之间的差别或许会逐渐地消失。

8.6 安全功能

IEC 62061 定义了所谓安全相关的电气控制系统（SRECS），它包括许多用于检测、处理和输出的子系统。该系统由许多元件所组成（例如，开关）。

实现安全功能的有效途径是使用经过认证的安全设备（传感器、执行器）和安全控制器，它们是经 PROFIsafe 相连在一起的。

8.7 已达到的 SIL

安全设备在其安全手册中提供用以确定由某个安全功能所达到的 SIL 的信息。第一步是求得所有安全设备（安全从设备，安全主设备）的最小 SIL_{CL}。该值确定全部安全功能可以达到的最大 SIL。在某些情况下，制造商提供系统支持，以便通过安全设备和附属系统软件的冗余来达到一个较高的 SIL。

第二步要加上安全设备的 PFH_d 值，而且将它同已确定的允许值相比较。从以上两个计算过程中得出的最小 SIL-值决定安全功能可以达到的最大 SIL。

下面各节内容将叙述如何依照图 5 将远程 I/O 中的安全模块同经典的安全设备，如紧急断路开关，安全门开关，等等进行组合。

8.8 电子机械

IEC 定义了包括计算公式在内的四种子系统结构 A，B，C，D 用于连接经典的安全设备。利用开关的 B_{10} 一值，估计的开关周期数、诊断覆盖率和 CCF-因素（Common Cause Failure，共因失效），且根据计算公式便可求得危险失效概率，以此来确定 SIL 等级。

8.9 非电气部件

ISO 13849-1 定义了所谓 SRP/CS（Safety-Related Parts of Control System，控制系统的安全相关部件），既适用于电气部件，也适用于液压、气动和机械部件。由于有了这个标准也就可以求出非电气部件的 PL-值和 PFH_d-值，然后依据 IEC 62061 利用这两个值来确定某个安全功能的 SIL。

8.10 确认

IEC 62061 要求人们制订一项确认计划，作为整体安全方案的一部分。一台机器设备必须按照此计划来进行测试、认证和建立文档。

9. 安全（从站）设备家族

PROFIsafe 技术为标准设备和安全设备开拓了全新的可能性。本章节简述一些主要的安全从设备和典型的应用。

9.1 远程-I/O

标准的远程-I/O 如今可以包含安全模块，对头站无干扰。这使得安全模块，如数字和模拟输入/输出，断路器模块，电动机起动器或变频器用上了集成安全技术。安全模块可以成组排列，因此也可以成组断开。

“紧急-停止”按键，由于要求单独检验致使年检的费用很高。采用新技术可以对全年的所有操作进行一次简单的记录。因此，必须查验的对象只是剩余未经操作的开关，从而可以节省很多费用。

9.2 光电传感器

光学安全传感器，如光栅或激光扫描器，在 IEC 61496 中作了规定。光学传感器尤其适合出入端口的柔性防护。图 18 中的例子说明 PROFIsafe 是如何工作的，它是对集成安全激光扫描器和驱动器安全功能的补充（9.3）。

9.3 驱动器

驱动器的安全功能在 IEC 61800-5-2 中作了规定。一般情况下在这里需要使用位置发送器来实现安全功能。用户可以通过 PROFIsafe 获取它的数值，从而可以放弃使用物理的终端位置开关或阻尼传感器。如图 18 中所示，在考虑了有关轿车车身轮廓的情况下，电动机的位置决定了安装在生产车间出入端口的激光扫描器的保护区域。

在 5.2.4 中列出了新增加的安全功能，它们在不久的将来会使应用发生革命性的变化。

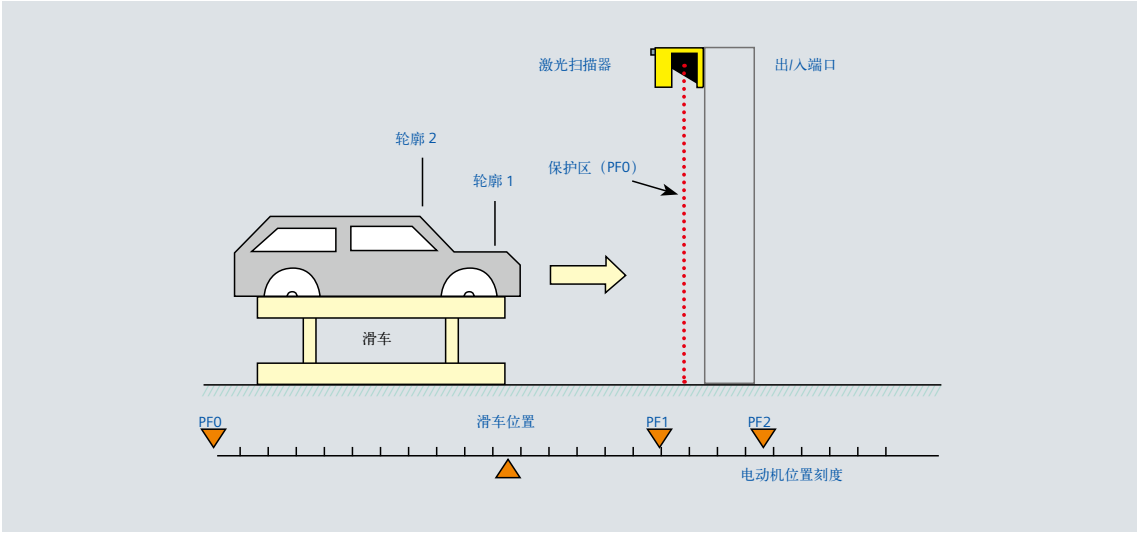


图 18 激光扫描器的柔性低噪声传感器
(Software-“Muting-Sensoren” für Laserscanner)

9.4 机器人

机器人的安全功能在 ISO 10218 中作了规定。驱动器新增的安全功能也可以集成到机器人中，从而产生了像“互动型机器人”这类新功能，可使机器人与人类携手同工。

9.5 安全网关

PROFIsafe 拥有一个连接正在工作的 ASIsafe（AS-Interface Safety-at-work，执行器-传感器接口安全总线）的安全网关。用此安全网关可以将两种安全方案的优点结合在一起。ASIsafe 可以毫无困难地检测到接入电缆端子上的“紧急-停止”按键的信号，而 PROFIsafe 则在运用集成安全设备方面，例如在运用集成安全驱动器方面，显现出独特的优点。

9.6 PA-设备

上面已经提到过，在过程自动化的安全性方面有一个独立的专业标准。NAMUR（Normungs-Ausschuss für Mess- und Regelungstechnik，德国测量与调节技术标准化委员会）作为化学与制药工业的标准化组织颁布了配套标准 NE97。根据该标准，一台“经使用验证”且带一个 PROFIBUS MBP-IS-接口的 PA-设备拥有一个可被激活或者可解除激活的 PROFIsafe 驱动器（软件）。在“关”的操作模式下，它是一台标准的 PA-设备；在“开”的操作模式下，它就是一台安全设备（图 19）。

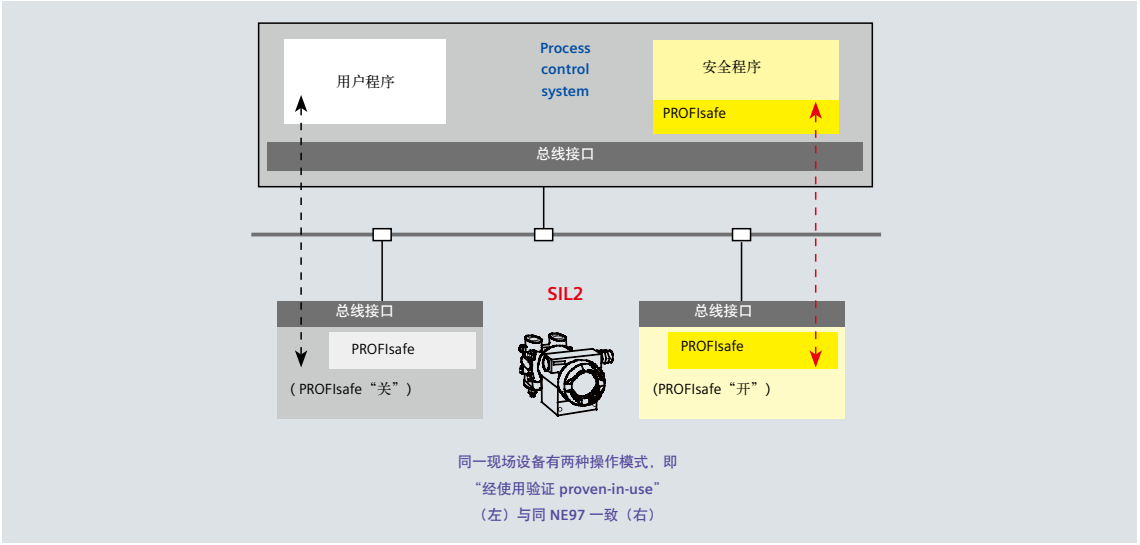


图 19　PROFIsafe 和 PA-设备的 NE97（NAMUR-推荐性标准）

NAMUR 出台了另一个配套标准-VDI 2180，它减轻了 F-PA-设备的研发工作。

目前对于过程自动化中大多数的 PROFIsafe 应用而言，使用的是带安全模块的 Remote I/O，它们用于 4-20mA 或 HART-系统。图 20 所示为面向“经使用验证”的 PA-设备的 PROFIsafe 两种应用可能性。这是一个十分成功的兼容方案，尽管直接连接现场总线的优点，诸如大范围内的测量，参数化和周全的诊断等在这里并不起作用。

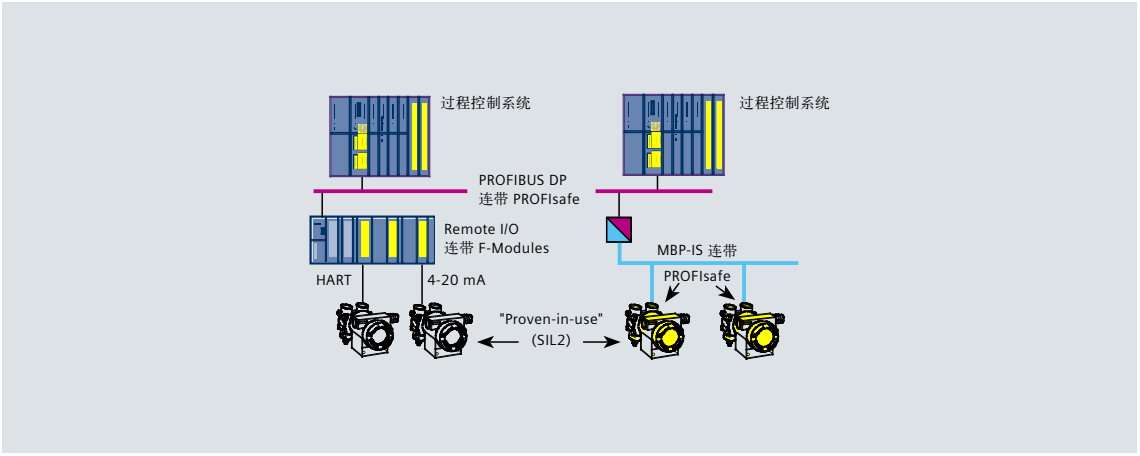


图 20　PROFIsafe 和 PA-设备的两种应用可能性

9.6.1 液位监控

油罐的液位开关也从 PROFIsafe 技术中获益匪浅。运用本质安全传输技术 MBP-IS 和 RS485-IS 的 PROFIBUS PA 尤其适用于这类安全从设备。PROFIsafe 在这里负责断路信号的安全传输，而用户则可以通过标准诊断通道调出传感器的状态。

9.6.2 ESD-阀（紧急切断阀）

运用 PROFIsafe 也可以明显地改善电子紧急切断阀（ESD）的性能。其主要目的是通过“Partial valve Strokes”（局部阀门行程）周期地从检验阀功能，并监视此行程一直到达最终位置，以及监视所需时间的趋势。此目的可以通过安全控制器自动地实现，且可以实现定期维护。RS485-IS-接口可以同防爆栅一道在 Ex-i-环境中使电路快速断开。

9.6.3 压力变送器

安全相关的压力变送器通过对设定值的比较实施一个油罐的液位测量和防止溢流双重功能。

9.6.4 瓦斯与火警警报器

瓦斯与火警警报器，例如用于无人操纵的海上石油平台上。附加的位置信息可以使防火门仅在相关的位置自动关闭。

10. 用户受益

今天，PROFIBUS 的安装节点数已超过 2000 万台设备。进一步扩大其发展宗旨，过去和现在都是实现同市场上使用的设备完全兼容。

由于 PROFIsafe 和“黑色通道原理”功能安全的通信协议是独立的，甚至不必太费心就可以从 PROFIBUS 改用 PROFINET。同一个 PROFIsafe 驱动软件可以用在 PROFINET 和 PROFIBUS 设备中。

PROFIsafe 的引用从以下“三步曲”表明了一个质的飞跃：

- 从安全相关的继电器逻辑电路到可编程逻辑电路；
- 从并行布线到功能安全串行通信；
- 从孤立运行的到相互协作的安全设备；

下面从不同的视角对 PROFIsafe 的优点作一个确切的总结。

10.1 集成商与用户

- 在节省费用方面，与使用标准-PROFIBUS 的情况相同：减少布线、组态、参数化和诊断十分灵活；
- 系统设计既简单又经济，可选用许多制造商广泛的产品型谱；
- 安装方面，一般情况下没有特殊的限制；
- 高度创新的安全应用只是通过智能化安全设备之间所进的简单通信来实现的；
- 在更换现有的继电器技术以及在扩建与改造现有生产设备时显现出高度的灵活性；
- 适用于制造业自动化和过程自动化的集成技术；
- 只需在总线技术方面进行培训、归档和维护；
- 标准—应用和安全应用的编程仅使用一种工具和通过认证的功能元件；
- 安全组态和安全应用程序的文档简单；
- 由于只使用经过认证的设备，省钱的系统获得了广泛的认同；
- 又因使用符合 IEC 61508 的技术而获得了国际认可；
- BGIA 和 TÜV 对 PROFIsafe 的认证。

10.2 设备制造商

- TÜV 认证的软件使一个 PROFIsafe 解决方案的实现与再现既省心又省钱；
- PROFIsafe 通信适合可编程安全控制器的各类结构；
- PROFIsafe 是崭新的设备功能的开拓者。

10.3 未来的投资

- PROFIBUS 和 PROFINET-设备的安装节点数巨大；
- PROFIBUS/PROFINET 组织机构和支持中心遍布世界各地；
- 由 PI 出版的所有现行的和将来的标准规范均适用于安全应用；
- 未来的软件将伴随着安全应用的生命周期，即从设计、评估、认证直到归档，因而将使开销大幅度地减少。

11. PROFIsafe 应用案例

11.1 安全总线协议PROFIsafe在汽车厂总装车间的应用

■ 11.1.1 客户信息

北京奔驰-戴克汽车厂借助PROFINET 实现 PROFIsafe 的安全通信协议应用。实现了安全通信和标准通信的集成并节省了安装费用，避免了复杂的接线。安全逻辑通过程序来实现，增强了安全系统的灵活性。同时，实现了系统对故障的实时监测。

■ 11.1.2 系统特点

PROFIsafe 安全通信实现了标准数据和安全数据的统一监控：基于 PROFIBUS 和 PROFINET 的 PROFIsafe 安全通信实现了现场 30 个急停和 30 个保护开关及光幕的通信监测，使得系统的安全等级达到 SIL3 客户要求的安全级别。除此之外，它还实现了标准控制网络与安全网络的良好集成。系统采用单总线结构实现了标准和安全数据的传输，操作员可以通过一个界面实现对安全数据和标准数据的监控。

■ 11.1.3 客户获益

汽车制造企业中实现数字化工厂，通信的统一增强了系统的坚固性，高效性并同时降低了工程成本。安全系统与标准系统的整合，简化了网络结构，降低了网络复杂性，方便了系统的实施，使系统维护变得简单。采用 PROFIsafe 增加了系统的灵活性，安全逻辑程序和标准程序在同一个环境中进行编辑，方便了信息共享。

图 21 安全可靠的奔驰车间生产线

图 22 安全控制柜通过PROFIsafe实现安全通信

11.2 安全总线协议PROFIsafe在西门子成都SEWC工厂的应用

■ 11.2.1 基本信息

它是一个完整的数字化企业平台——西门子工业自动化产品成都生产研发基地（以下简称“西门子成都工厂”）。西门子成都工厂全厂内实现了从管理、产品研发、生产到物流配送全过程的数字化，并且通过信息技术，与德国生产基地和美国的研发中心进行数据互联。在西门子成都工厂研发生产一件新产品，它都会拥有自己的数据信息。这些数据信息在研发、生产、物流的各个环节中被不断丰富，实时保存在一个数据平台中。而这座工厂的运行，都是基于这些数据基础，ERP、PLM（产品全生命周期管理系统）、MES（制造执行系统）、控制系统及供应链管理，全部实现了无缝的信息互联，从而造就出了一幅透明工厂的画面。更精彩的是，这个工厂的绝大多数技术来自西门子自身，可谓一座“自己生产自己”的工厂。在这样一个高自动化辅以人工的智能工厂中，一个可靠安全的控制系统的保障不可或缺。

■ 11.2.2 系统特点

其所有的生产线，控制系统均使用西门子安全解决方案，主控由西门子安全型F-PLC构成，通信自动加载PROFIsafe通信，保证数据传输可靠性和安全性。其高速物流存储系统和整个的生产线，通过SIMATIC S7系列安全控制器以及PROFIsafe进行通信，在较少人力的干预下即可实现全工厂的稳定生产。

■ 11.2.3 用户获益

以可编程控制器（PLC）产品为例，在整个生产过程中针对该类产品的自动质量检测节点就超过20个。对比传统制造企业的人工抽检，这显然要可靠又快速得多。

在经过多次装配并接受过多道质量检测后，成品将被送到包装工位。再经过人工包装、装箱等环节，一箱包装好的自动化产品就会通过升降梯和传送带被自动运达物流中心或立体仓库。这样一个完整的生产环节，在传统的制造企业要通过几十甚至上百人的手去完成，而在西门子成都工厂的车间内，却看不见密集的流水线员工，大多数的工序都是自动完成的。而其可靠运行，包括和人工之间可安全交互，都是通过安全的控制系统和PROFIsafe安全网络实现的。

Bukenberger说：“应用了西门子数字化企业平台解决方案的成都工厂与西门子在中国的其他工厂比较，产品的交货时间缩短了50%。”数据显示，通过安全可靠的系统运行和数字化的工厂规划，可以减少产品上市时间至少30%；通过优化规划质量，可以降低制造成本13%。而在新产品上市比例、设备生产效率、产品交付能力及营运利润率等多个方面，数字化工厂的指标均远远高于传统制造企业。

安全性是保证数字化制造的前提，给企业运行带来实实在在的收益，是支撑企业长远发展的竞争力。这将成为未来中国制造可持续发展的根本所在。

图 23 PROFIsafe为西门子成都工厂的智能化柔性生产保驾护航

11.3 安全总线协议PROFIsafe为过程行业提供安全保障
中石油抚顺石化1000万吨/年炼油DCS/SIS项目

■ 11.3.1 基本信息

中国石油天然气总公司抚顺石化公司千万吨炼油、百万吨乙烯项目为特大型炼油化工一体化项目，项目集中原油加工、炼油结构调整技术改造工程、100万吨/年乙烯技术改造工程、热电厂“以大带小”扩能改造工程及配套项目、石油一厂新区和化塑厂搬迁工程，是分别立项又相互联系的炼油和 化工综合项目。在此，功能安全是重中之重。

■ 11.3.2 系统特点

西门子提供了基于TIA技术的DCS和SIS解决方案，其中安全系统S7-400FH即满足安全功能上的独立需求，又可以在DCS的操作界面上显示全部的安全相关的工艺和维护诊断数据，便于统一的数据管理。

为了满足高可用性要求，系统进行了全冗余容错的配置，冗余配置包括：控制器、I/O模块、系统总线和服务器。其中基于柔性模块冗余（FMR）技术的安全系统S7-400FH，其多路容错性能允许系统多个故障发生而不会造成装置的误停车。

其中包括

DCS 冗余控制器AS400H：51对

SIS冗余控制器400FH：10对

OS服务器4对；中央归档服务器1台；资产管理器2台；OPC服务器1台；Web服务器2台；防病毒服务器1台。

DCS操作员站61台，SIS操作员站5台，工程师站12台。

在12个现场控制室中分别配有1台工程师站、1台操作员单站，1台资产管理站

所有的网络都是由PROFIsafe进行安全通信，保障安全信号的可靠性。

■ 11.3.3 用户获益

PCS 7系统和通信中集成了控制功能和安全功能，非安全应用和安全应用在同一平台，避免了由于DCS和SIS属于不同地供应商而产生的接口兼容性问题。

安全型生命周期的组态工具CFC和安全矩阵易于使用，维护工作简单方便。

在各个层级上实现冗余，增加系统的可用性。

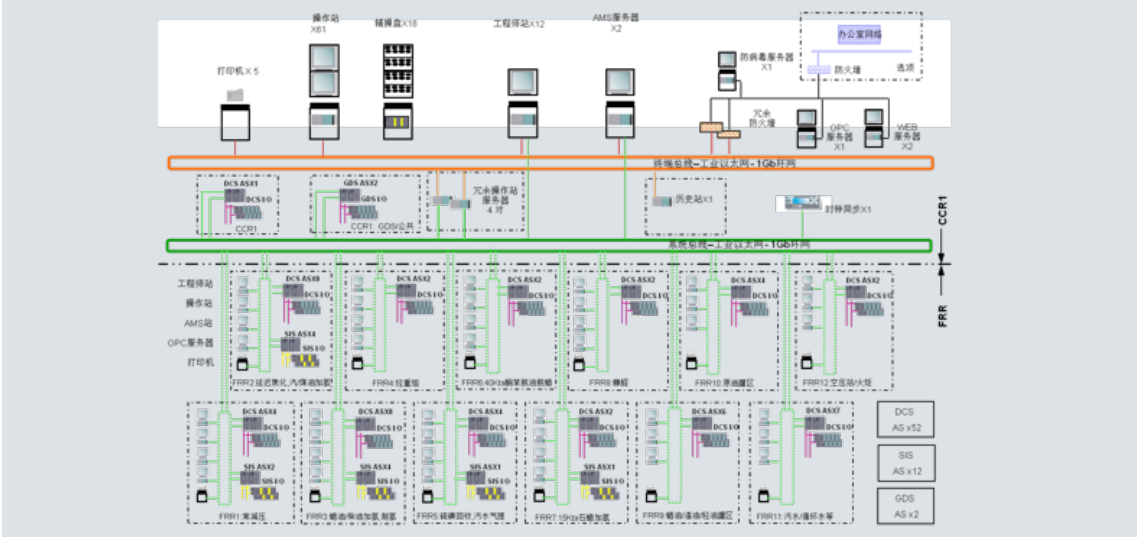


图 24 中石油抚顺石化1000万吨/年炼油DCS/SIS项目系统构架 PROFIsafe贯穿其中

11.4 安全总线协议PROFIsafe在电梯行业的应用
PROFIsafe在美国自由女神像救援电梯中的应用

■ 11.4.1 基本信息

自由女神雕像是纽约市的标志，她已经迎接了数百万来自世界各地的游客。近来，为保证安全，安装了新的消防和安全设备，并对改进参观人流方面采取了一些建筑上的措施。在整修、改建的过程中，也建造了一座全新的救援电梯。“这部专门制造的电梯，绝对是独一无二的。”，TESI电梯系统公司（TESI-Tower Elevator System，Inc）负责人运输电梯系统专家托德·格罗伐特（Todd Grovatt）强调说。

■ 11.4.2 系统特点

在该项目中，由于电梯运载乘客，所以其可靠安全是必须考虑的重要因素。所有部件是首次在运用西门子TIA Portal的情况下开发出来的，并投入运行，缩短调试周期并降低成本。装有故障安全CPU的Simatic ET 200S 构成了TESI电梯控制系统的核心部分。

该项目选用TIA Portal，以实现更少的设计开销，更短的调试时间，更低的成本；

使用故障安全Simatic ET 200S，由TIA Portal对安全任务进行编程；

自动加载PROFIsafe协议在PROFINET和PROFIBUS总线之上，无需额外的总线网络，就可以安全的来监控处于系统的通信状态，执行诊断任务，排除通信过程中的故障与干扰。

项目主任工程师布里安·特拉帕尼（Brian Trapani）说：“安全在我们的工程项目中最具有重要作用。所以，采取故障安全控制器和PROFIsafe安全通信，是我们决定选择西门子作为合作伙伴的主要理由之一，因为安全如今是TIA Portal 的一部分，而且可以简便地从提供的工具中编程。”

除了追踪运行各个方面的冗余系统之外，还开发了一种用于救援的疏散系统，该系统集成于安全机制之中，安全控制系统和PROFIsafe构成了安全控制的中枢和网络，来保证真个系统的功能安全。“控制面版提供了一个用户界面，用来监控处于临界状态的系统，执行诊断任务以及排除故障与干扰，格罗伐特解释说。“PLC获得来自系统的反馈，并借助自行开发的逻辑控制电路将电梯引向预定的安全地点，”他接着说。

■ 11.4.3 用户获益

在救援电梯中使用PROFIsafe和安全系统，一个安全型PLC 可实现所有安全功能并能同时完成标准功能，节省了大量的系统布线和控制柜的空间，电气系统从图纸到接线更加简洁清晰；

PROFIsafe集成的安全理念和基于博途的Safety Advanced V13设计平台使得设计时间减少约 30%，整个工程时间减少约20%；

安全型的PLC之间的F通讯是通过PROFIsafe协议来保证数据安全的，在数据中增加了更多的校验机制，因此可靠性更高。由于应用了PROFIsafe-技术，该使用以来从未发生过意外。

图 25 PROFIsafe为游览胜地提供可靠的安全保障

12. PI（PROFIBUS & PROFINET 国际）组织概况

开放的技术为了在市场上对其进行维护、开拓和推广，需要有一个独立于企业的机构作为工作平台。对于 PROFIBUS 和 PROFINET 技术而言，为达到此目的于 1989 年成立了 PROFIBUS 用户组织（PROFIBUS Nutzerorganisation e.V.，简称 PNO）作为一个无盈利的、代表制造商、用户和研究所利益的机构。PNO 是 1995 年建立的国际联合总会 PI（PROFIBUS & PROFINET International）的会员。PI 拥有 25 个地区代表机构（RPA）和大约 1400 个会员，遍及全球五大洲，在工业通信领域是世界上庞大的利益共同体（图 21）。

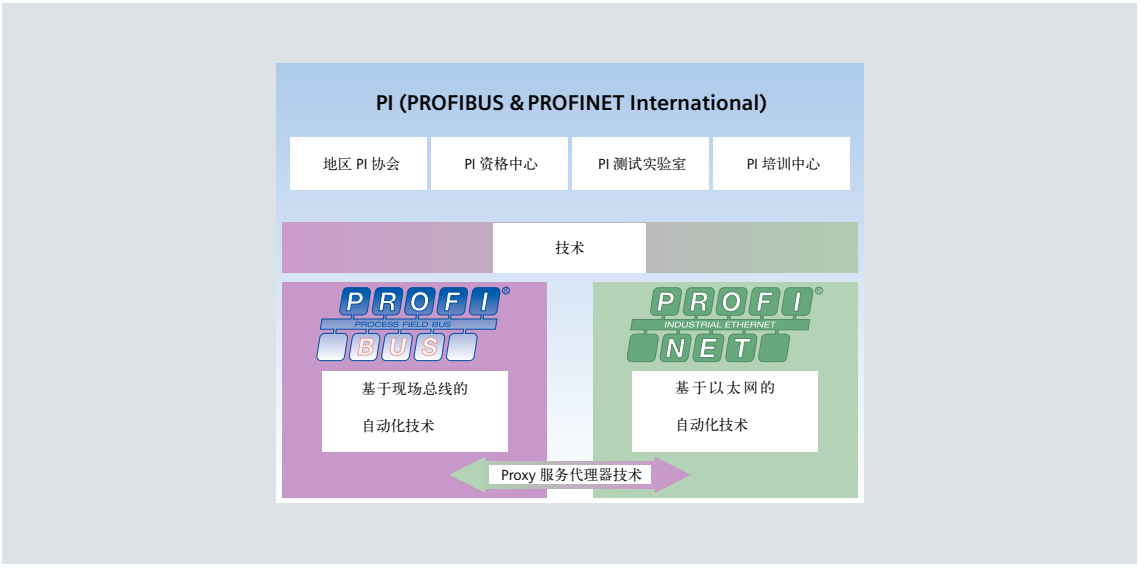


图 26　PROFIBUS & PROFINET International（PI）

12.1 PI 的任务

PI 的主要任务有：

- 维护与继续开拓 PROFIBUS 和 PROFINET；
- 促进 PROFIBUS 与 PROFINET 在全球的推广；
- 通过对标准化和规范化施加影响来实现对用户和制造商的投资保护；
- 在各个标准化委员会和联合会中代表会员企业的利益；
- PI 资格中心（PI Competence Center，PICC）在全球范围内为企业提供技术支持；
- 通过以在 PI 测试实验室（PI Testlabor，PITL）中进行的一致性测试为基础的产品认证来实现质量保证；
- 通过 PI 培训中心（PI Training Center，PITC）来确保全球统一的培训水准。

12.2 技术研发

PI 将技术研发工作交给了 PNO（德国）。PNO（德国）的顾问委员会（Advisory Board）掌控研究与发展工作。技术研发在 50 多个工作团组中进行，参与研发的专家超过 500 人。

12.3 技术支持

PI 在全球拥有 35 个以上的经授权的 PICC。这些机构以各种方式为用户和制造商提供咨询和技术支持。它们作为 PI 的机构对企业保持中立，在约定的规章框架内提供其服务。PICC 将在一个专为它们安排的授权程序中，定期地接受对其资格的审核，其当前地址可从网页上查找。

12.4 认证

PI 在世界各地拥有 8 个认证带有 PROFIBUS 和 PROFINET 接口的产品的机构 PITL。作为 PI 的机构，它们对企业保持中立，在约定的规章框架内提供其服务。PITL 的测试服务质量将定期地在一个极其严格的授权程序中经受考核。其当前地址可从网页上查找。

12.5 培训

为确保全球统一的工程师与技术人员的培训标准，建立了 PI 培训中心（PI Training Center）。对培训中心及其专家的授权保证了培训质量，从而也保证了 PRIFIBUS 和 PROFINET 工程设计与施工建设的服务能力。最新地址可在网页上寻找。

12.6 因特网平台

有关 PI 和 PROFIBUS 与 PROFINET 技术的最新信息可登录 PI-网页 www.profibus.com，此外，网页信息还包括在线产品指南（Online-Product-Guide），词汇表（Glossary），网上培训（Web-Based-Trainings）和规范、行规、安装规则及其它文档下载专区（Downloads）。

中、德、英术语对照表

1 对 1 关系 /1:1Beziehung/1 to 1 relationship

“三步曲”/3-Schritt-Methode/3-step-method

执行器 — 传感器 — 接口安全总线/ASIsafe/ASIsafe

B_{10}-值/B_{10}-Wert /B_{10} value

经使用验证/Betriebsbewährt/Proven-in-use

德国工伤保险职业安全研究所/BGIA/BGIA

位错误概率/Bitfehlerwahrscheinlichkeit/Bit error probability

黑色通道/Black Channel/Black Channel

共因失效因素/Common Cause Factor/Common cause factor

性能类别/Conformance Classes/Conformance classes

组态 — 参数化 — 与诊断工具/CPD-Tool/CPD-Tool

循环冗余校验代码/CRC-Signature/CRC-signature

数据安全/Datensicherheit/Data Security

数据类型/Datatypen/Data types

要求的持续时间/Dauer der Anforderung/Duration of demand

诊断覆盖/Diagnoseabdeckung/Diagnostic Coverage

无线传输/drahtlose Übertragung/Wireless

本质安全/Eigensicherheit/Intrinsic Safety

电气安全/Elektrische Sicherheit/Electrical Safety

抗电磁干扰性/elektromagnetische Störfestigkeit/Electro magnetic immunity

欧洲标准EN954-1/EN954-1/EN954-1

出入端口/Entry/Exit-Portal/Entry/exit portal

本安防爆/Ex-i/Ex-i

安全地址/F-Adresse/F-Address

安全（从站）设备/安全设备（F-Device）/安全设备（F-Device）

故障容忍度/Fehlertoleranz/Fault tolerance

制造业自动化/Fertigungsautomation/Factory automation

安全控制器/安全主控制器（F-Host）/安全主控制器（F-Host）

现场设备工具/Field Device Tool (FDT)/Field Device Tool (FDT)

安全模块/F-Module/F-Module

顺序号/fortlaufende Nummer/Consecutive Number

安全参数/F-Parameter/F-Parameter

功能安全性能判据/FS Verhaltenskriterien/FS Performance Criteria

高可用性/Hochverfügbarkeit/High availability

国际电工技术委员会/IEC/IEC

IEC 61508/IEC 61508/IEC 61508

IEC 61784-3-3/IEC 61784-3-3/IEC 61784-3-3

IEC 62061/IEC 62061/IEC 62061

基础模式/Infrastruktur-Modus/Infrastructure mode

固有安全/inhärente Sicherheit/Inherent safety

安装/Installation/Installation

i 参数/i Parameter/i Parameter

i 参数—服务器/i Par-Server/i Par-Server

国际标准化组织/ISO/ISO

ISO 1200-1/ISO 1200-1/ISO 1200-1

ISO 13849-1/ISO 13849-1/ISO 13849-1

ISO 14121/ISO 14121/ISO 14121

类别 4/Kategorie 4/Category 4

通信错误/Kommunikationsfehler/Communication error

机器设备法、指令/Maschinenrichtlinie/Machinery Directive

MBP-IS曼彻斯编码总线供电—本质安全/MBP-IS/MBP-IS

德国（化工与制药业）测量与调节技术标准化委员会/NAMUR/NAMUR

NAMUR之推荐标准97/NE 97/NE 97

非电气部件/nichtelektrische Teile/Non-electrical Parts

误脱扣（引发事故）/Nuisance Trip/Nuisance Trip

过程自动化—设备/PA-Gerät/PA-Device

特低保护电压/PELV/PELV

性能等级/Performance Level (PL)/Performance Level (PL)

准则、政策/Policy/Policy

PROFIBUS & PROFINET国际/PROFIBUS & PROFINET International/PROFIBUS & PROFINET International

PROFIBUS 之驱动技术专用行规/PROFI drive/PROFI drive

PROFIsafe 岛屿/PROFIsafe-Insel/ PROFIsafe island

PROFIsafe 层测试/PROFIsafe-Layer-Test/PROFIsafe layer test

PROFIsafe 报文格式/PROFIsafe-Nachrichtenformat/PROFIsafe message format

过程自动化/Prozessautomation/Process automation

剩余差错概率/Restfehlerwahrscheinlichkeit/Residual error probability

风险评估/Risikobewertung/Risk assessment

RS485-本安/RS485-IS/RS485-IS

安全功能响应时间（SFRT）/Safety Function Response Time (SFRT）/Safety Function Response Time (SFRT）

安全完整性等级（SIL）/Safety Integrity Level (SIL)/Safety Integrity Level (SIL)

屏蔽/Schirmung/Shielding

保护装置/Schutzeinrichtung/safeguarding

信息安全网关/Security-Gate/Security Gate

故障安全值/Sichere Werte/Fail-safe values

安全评估/Sicherheitsbeurteilung/Safety assessment

安全功能/Sicherheitsfunktion/Safety Function

安全手册/Sicherheitshandbuch/Safety manual

安全措施/Sicherheitsmassnahmen/Safety measures

安全系统/Sicherheitssystem/Safety system

输入/输出数据的防护/Sichern der E/A-Daten/Securing I/O data configurations

GSD 的防护/Sichern der GSD/Securing GSD files

SIL 要求极限/SIL Claim limit/SIL claim limit

单通道/Single-Channel/Single Channel

供电、电源/Spanungsversorgung/Power supply

开发软件包/Starter-Kit/Development Kit

状态字节/Status-Byte/Status Bytes

控制字节/Steuer-Byte/Control Byte

支线/Stichleitungen/Spur/branch lines

交换机（以太网）/Switches (ETHERNET) /Switches (ETHERNET)

工具调用接口/Tool calling Interface (TCI)/Tool calling Interface (TCI)

德国技术监督联合会 TÜV/TÜV/TÜV

德国工程师协会/VDI/VDI

VDI 2180/VD I2180/VDI 2180

可用性/Verfügbarkeit/Availability

（危险）失效概率/Versagenswahrscheinlichkeit/Probability of dangerous failure

无线（通信）/Wireless/Wireless

认证/Zertifizierung/Certification

参考文献

- PROFIsafe Policy V1.3; Order No. 2.282
- PROFIsafe Profile for Safety Technology on PROFIBUS DP and PROFINET IO, V2.4; Order No. 3.192b
- PROFIsafe . Environmental Requirements, V2.5; Order No. 2.232
- PROFIsafe . Test Specification for F-Slaves, F-Devices, and FHosts, V2.1; Order No. 2.242
- PROFIsafe for PA-Devices, V1.0; Order No. 3.042
- PROFIdrive on PROFIsafe, V1.0; Order No. 3.272
- Rapid way to PROFIBUS DP; Order No. 4.072
- Industrial Communications with PROFINET; Order No. 4.182
- Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD, V5.04; Order No. 2.122
- GSDML Specification for PROFINET IO, V2.2; Order No. 2.352
- Profile Guideline, Part 1: Identification & Maintenance Functions, V1.1; Order No. 3.502
- Profile Guideline, Part 2: Data Types, Programming Languages, and Platforms, V1.0; Order No. 3.512
- Profile Guideline, Part 3: Diagnosis, Alarms and Time Stamping, V1.0; Order No. 3.522
- Communication Function Blocks on PROFIBUS DP and PROFINET IO, V2.0; Order No. 2.182

Australla & New Zealand
PROFIBUS User Group
Mr. John Immelman
PO Box 797
North Ryde Business Centre
NSW 1670 North Ryde
Phone: +61 2 88 77 70 07
Fax: +61 2 88 77 70 99
australia@profibus.com
PROFIBUS Belgium
Mr. Herman Looghe
August Reyerslaan 80
1030 Brussels
Phone: +32 27 06 80 00
Fax: +32 27 06 80 09
belgium@profibus.com
Ass. PROFIBUS Brazil
c/o SMAR Equip. Inds. Ltda.
Mr. Cesar Cassiolato
Av. Antonio Paschoal, 1945 Centro
14160-500 Sert„ozinho - SP
Phone: +55 16 3946 3519
Fax: +55 16 3946 3595
brazil@profibus.com
China PROFIBUS & PROFINET Association
Mrs. Dr. Liu Dan
397A Guanganmenwai Street
100055 Beijing
Phone:+86 10 63 32 20 89
Fax:+86 10 63 49 04 89
china@profibus.com
www.pi-china.org
PROFIBUS Association Czech Republic
Mr. Zdenek Hanzalek
Karlovo nam. 13
12135 Prague
Phone: +420 2 24 35 76 10
Fax: +420 2 24 35 76 10
czechrepublic@profibus.com
PROFIBUS Denmark
Mr. Kim Husmer
Jydebjergvej 12A
3230 Graested
Phone: +45 40 78 96 36
Fax: +45 44 97 77 36
denmark@profibus.com
PROFIBUS Finland
c/o AEL Automaatio
Mr. Taisto Kaijanen
Kaarnatie 4
00410 Helsinki
Phone: +35 8 95 30 72 59
Fax: +35 8 95 30 73 60
finland@profibus.com
France PROFIBUS
Mrs. Christiane Bigot
4, rue des Colonels Renard
75017 Paris
Phone: +33 1 42 83 79 13
Fax: +33 1 42 83 79 1
3france@profibus.com
PROFIBUS Nutzerorganisation
Mr. Peter Wenzel
Haid-und-Neu-Str. 7
76131 Karlsruhe, Germany
Phone: +49 721 96 58 590
Fax: +49 721 96 58 589
germany@profibus.com
PROFIBUS Ireland
University of Limerick
Mr. Hassan Kaghazchi
Automation Research Centre
National Technology Park - Plassey
Limerick
Tel.: +353 61 20 21 07
Fax: +353 61 20 25 82
ireland@profibus.com
PROFIBUS Network Italia
Mr. Maurizio Ghizzoni
Via Branze, 38
25123 Brescia
Phone: +39 030 3 38 40 30
Fax: +39 030 39 69 99
pni@profibus.com
Japanese PROFIBUS Organisation
Mr. Shinichi Motoyoshi
Takanawa Park Tower
3-20-14 Higashi-Gotanda, Shinagawa-ku
Tokyo 141-8641
Phone: +81 3 54 23 86 28
Fax: +81 3 54 23 87 34
japan@profibus.com
Korea PROFIBUS Association
Mr. Cha Young-Sik
#812, Seocho Platinum
1445-13 Seocho-dong, Seocho-gu
Seoul 137-866, Korea
Phone: +82 25 23 51 43
Fax: +82 25 23 51 49
korea@profibus.com
PROFIBUS User Organisation U.A.E.
Mr. S.C. Sanu
P.O. Box. 123759
Unit No. 424, Al Diyafah Building
Al-Diyafah Street, Satwa
Dubai , United Arab Emirates
Tel.: +971 4 398 2760
Fax: +971 4 398 2761
middle.east@profibus.com
PROFIBUS Nederland
c/o FHI
Mr. Dolf van Eendenburg
P.O. Box 2099
3800 CB Amersfoort
Phone: +31 33 4 69 05 07
Fax: +31 33 4 61 66 38
netherlands@profibus.com
PROFIBUS User Organisation Norway
c/o Festo AB
Mr. Ivar Sorlie
Østensjøveien 27
0661 Oslo
NORWAY
Phone: +47 90 98 86 40
Fax: +47 90 40 55 09
norway@profibus.com
PROFIBUS Polska
Mr. Dariusz Germanek
ul. Konarskiego 18
44-100 Gliwice
Phone: +48 32 37 13 65
Fax: +48 32 37 26 80
poland@profibus.com
PROFIBUS User Org. Russia
c/o Vera + Association
Mrs. Olga Sinenko
Nikitinskaya str, 3
105037 Moscow, Russia
Phone: +7 09 57 42 68 28
Fax: +7 09 57 42 68 29
russia@profibus.com
PROFIBUS Slovakia
Mr. Igor Belai
Slovak Technical University
Dept. of Autom. KAR FEI STU
Ilkovièova 3
812 19 Bratislava
Phone: +421 2 60 29 14 11
Fax: +421 2 65 42 90 51
slovakia@profibus.com
PROFIBUS Association South East Asia
Mr. Volker Schulz
60 MacPherson Road, 4th Floor
Singapore 348615
Tel: +65 64 90 64 00
Fax: +65 64 90 64 01
southeastasia@profibus.com
PROFIBUS User Organisation Southern Africa
Mr. Dieter Dilchert
51 Brunton Circle
1645 Modderfontein
Phone: +27 11 2 01 32 03
Fax: +27 11 6 09 32 04
southernafrica@profibus.com
PROFIBUS i Sverige
Mr. Peter Bengtsson
Kommandörsgatan 3
28135 Hässleholm
Phone: +46 45 14 94 40
Fax: +46 45 18 98 33
sweden@profibus.com
PROFIBUS Schweiz
Mrs. Karin Beyeler
Kreuzfeldweg 9
4562 Biberist
Phone: +41 32 6 72 03 25
Fax: +41 32 6 72 03 26
switzerland@profibus.com
The PROFIBUS Group
Mr. Bob Squirrell
The New House
1 Grove Road
Epsom, Surrey, KT17 4DE
Phone: +44 20 78 71 74 13
Fax: +44 870 1 41 73 78
uk@profibus.com
PTO
Mr. Michael J. Bryant
16101 N. 82nd Street, Suite 3B
Scottsdale, AZ 85260 USA
Phone: +1 48 04 83 24 56
Fax: +1 48 04 83 7 02
2usa@profibus.com

西门子（中国）有限公司
数字化工厂集团

如有变动，恕不事先通知
订货号：E20001-A0008-C400-V3-5D00
4071-SH903052-04220

欲知更多信息可登录以下网站：
www.profibus.com
www.profinet.com
PROFIBUS Nutzerorganisation e.V.
PROFIBUS & PROFINET International Support Center
Haid-und-Neu-Str. 7, D-76131 Karlsruhe/Germany
Fon +49 721 96 58 590, Fax +49 721 96 58 589
info@profibus.com