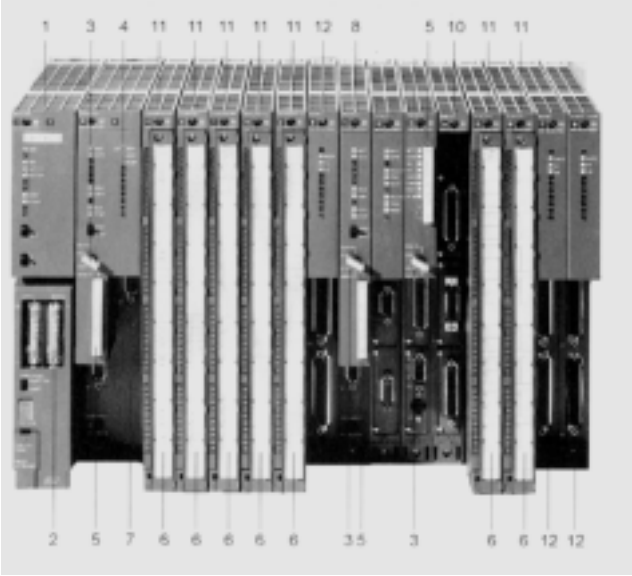
综述

SIMATIC S7-400

概述



1．电源模板
2．后备电池
3．模式开关（钥匙操作）
4．状态和故障 LED
5．存储器卡
6．有标签区的前连接器
7．CPU 1
8．CPU 2
10．I/O 模板
11．IM 接口模板

图 1 使用 CR2 机架的 SIMATIC S7-400 可编程序控制器

- 功能强大的 PLC，适用于中高性能控制领域
- 解决方案满足最复杂的任务要求
- 功能分级的 CPU 以及种类齐全的模板，总能为其自动化任务找到最佳的解决方案
- 实现分布式系统和扩展通讯能力都很简便，组成系统灵活自如
- 用户友好性强，操作简单，免风扇设计
- 随着应用的扩大，系统扩展无任何问题

应用

SIMATIC S7-400 是用于中、高档性能范围的可编程序控制器。

模块化及无风扇的设计，坚固耐用，容易扩展和广泛的通讯能力，容易实现的分布式结构以及用户友好的操作使 SIMATIC S7-400 成为中、高档性能控制领域中首选的理想解决方案。

SIMATIC S7-400 的应用领域包括：

- 通用机械工程
- 汽车工业
- 立体仓库
- 机床与工具
- 过程控制
- 控制技术与仪表
- 纺织机械
- 包装机械
- 控制设备制造
- 专用机械

功能逐步升级的多种级别的 CPU，带有各种用户友好功能的种类齐全的功能模板，使用户能够构成最

佳的解决方案，满足自动化的任务要求。

当控制任务变得更加复杂时，任何时候控制系统都可以逐步升级，而不必过多的添加额外的模板。

SIMATIC S7-400 符合如下国家和国际标准：

- DIN；EN，IEC
- UL 认证
- CAS 认证
- FM1 级，div 2；组 A、B、C 和 D；
  温度组：T4（≤135°C）
- 造船业认证；
  包括
  - 美国船舶制造局
  - Bureau Veritas
  - Des Norske Veritas
  - Germanischer Lloyd
  - Lloyds Register
  - of Shipping
- 允许环境温度 0~60°C
- 抗震性强

设计
综述

S7-400 自动化系统采用模块化设计。它所具有的模板的扩展和配置功能使其能够按照每个不同的需求灵活组合。

一个系统包括：

- 电源模板；
  将 SIMATIC S7-400 连接到120/230 V AC或 24 V DC 电源上。
- 中央处理单元（CPU）
  有多种 CPU 可供用户选择，有些带有内置的 PROFIBUS-DP 接口，用于各种性能范围。一个中央控制器可包括多个 CPU，以加强其性能。
- 各种信号模板（SM）用于数字量输入和输出（DI/DO）以及模拟量的输入和输出（AI/AO）
- 通讯模板（CP）用于总线连接和点到点的连接。
- 功能模板（FM）：专门用于计数、定位、凸轮控制等任务。

根据用户需要还提供以下部件：

- 接口模板（IM），用于连接中央控制单元和扩展单元。
  SIMATIC S7-400 中央控制器最多能连接 21 个扩展单元。
- SIMATIC S5 模板：
  SIMATIC S5-155U，135U和 155U的所有 I/O 模板都可和相应的 SIMATIC S5 扩展单元一起使用。另外，专用的 IP 和 WF 模板可用于 S5 扩展单元，也可直接用于中央控制器（通过适配器盒）。

SIMATIC S7-400 是一种通用控制器

- 由于有很高的电磁兼容性和抗冲击、耐振动性能，因而能最大限度的满足各种工业标准。模板能带电插、拔。

系统安装

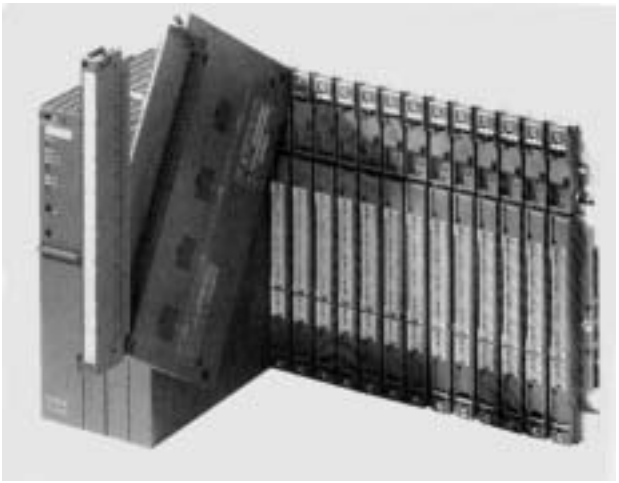


图 2 SIMATIC S7-400 设计系统

简单的设计系统使 S7-400 用途广泛、灵活、适用性强：

- 模板安装非常简便
- 背板总线集成在机架内
- 方便、机械码式的模板更换
- 经过现场考验的连接系统
- TOP 连接
  用螺钉或弹簧端子的1到3 线系统的预装配接线
- 规定的安装深度
  所有端子和接线器都放置在模板凹槽内并有盖板保护
- 没有槽位规则

扩展

如果用户需要比中央控制器更多的功能，S7-400 还可以扩展：

- 最多 21 个扩展单元（EU）
  21 个扩展单元（EU）都可以连接到中央控制器（CC）。
- 通过接口模板（IM）连接：
  中央控制器 CC 和扩展单元 EU 通过发送 IM 和接收 IM 连接。中央控制器（CC）可插入最多 6 个发送 IM，每个 EU 可容纳 1 个接收 IM。每个发送 IM 有 2 个接口，每个接口都能连接一条扩展线路。
- 集中式扩展：
  这种扩展方式适用于小型配置或控制柜直接在机器上的场合。每个发送 IM 接口可支持 4 个 EU，如有必要，还可同时提供 5V 电源。

设计
扩展（续）

中央控制器和最后一个 EU 的最大距离是 15 m（带 5 V 电源）；3 m（不带 5 V 电源）。

- 用 EU 进行分布式扩展：这种方式适用于分布范围广，并在一个地方有几个 EU 的场合。发送 IM 的每个接口最多可支持 4 个 EU。可以使用 S7-400 EU，或 SIMATIC S5 EU。中央控制器和最后一个 EU 的最大距离为 100 m（S7 EU）；600 m（S5 EU）。

采用扩展方案时应遵守以下原则：

- 任一中央控制器的扩展单元（EU）数量最多不应超过 21 个。
- 连接到任一中央控制器的发送 IM 不能超过 6 个，并且最多只有 2 个 IM 可提供 5 V 电源。
- 中央控制器器和 S7 EU 的最大距离为 100 m。
- 通过 C 总线的数据交换，仅限于中央控制器和 6 个 EU（EU1~EU6）之间。
- 电源模板总是安装在中央控制器和 EU 的最左边。

- 用 ET 200 进行远程扩展；这种方式适用于分布范围很广的系统。通过 CPU 中的 PROFIBUS – DP 接口最多可连接 125 个总线结点。中央控制器和最后一个结点的最大距离为 23 km（使用光缆）。

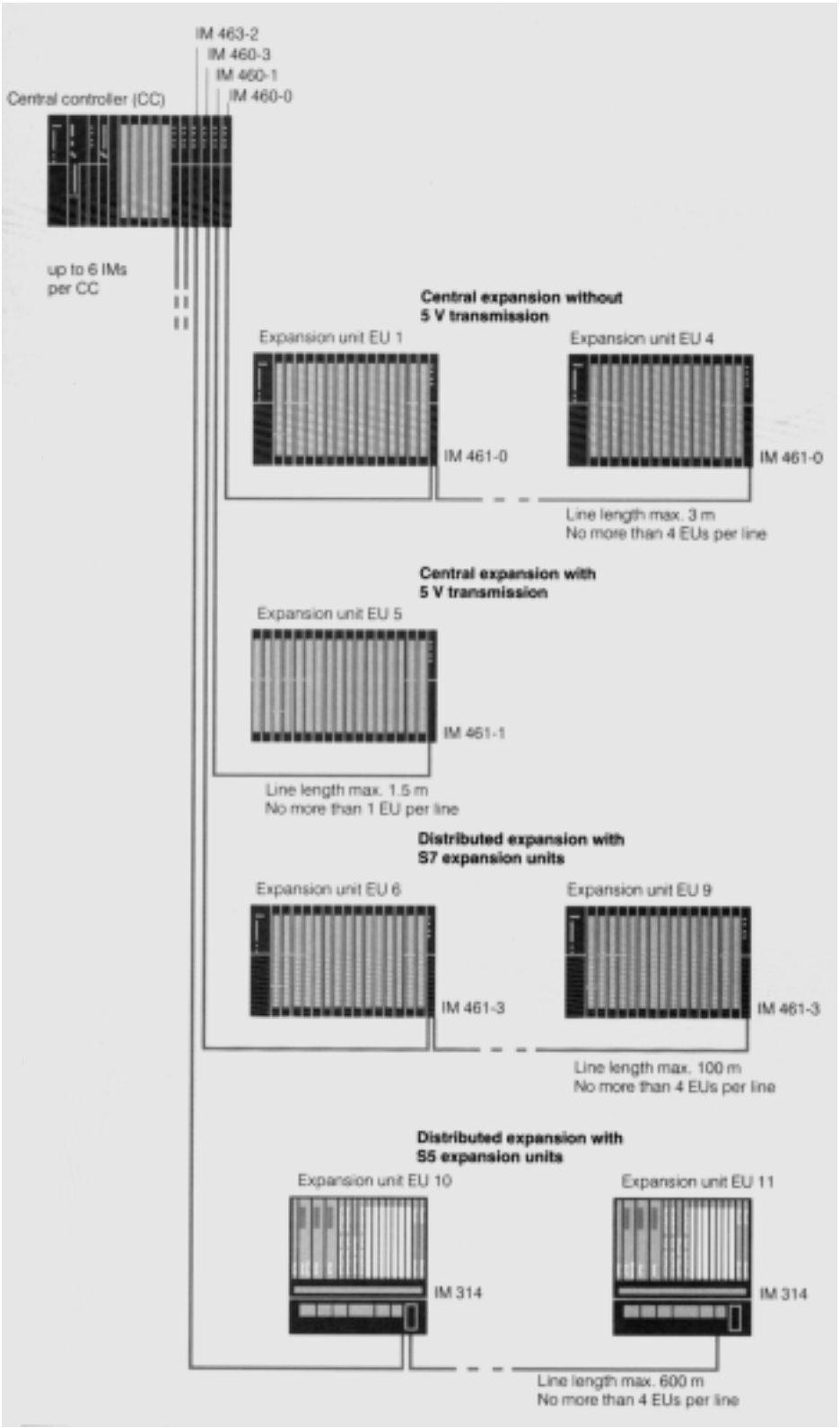


图 3 S7-400 可能的扩展型式

SIMATIC S7-400

功能	S7-400 在编程、启动和服务方面有众多特点： • 高速指令处理 • 用户友好的参数设置	• 用户友好的操作员控制和监视功能（HMI）已集成在 SIMATIC 的操作系统中	• CPU 的诊断功能和自测试智能诊断系统连续地监视系统功能并记录错误和系统的特殊事件。 • 口令保护 • 模式选择开关 • 系统功能
通讯	SIMATIC S7-400 有多种通讯方式： • 组合式多点 MPI 和 DP 主接口，集成在所有 CPU 内，S7-200 和 S7-300 系统以及其它的 S7-400 系统。 • 附加的 PROFIBUS-DP 接口，集成在某些 CPU 内，适用于经济型 ET-200 分布式 I/O 系统。	• 用于连接到 PROFIBUS 和工业以太网的通讯模板 • 用于功能强大的点对点连接的通讯模板 • 过程通讯 :通过总线（AS-I 或 PROFIBUS）周期地寻址 I/O 模板（过程映象数据交换）。从循环执行级调用过程通讯。	• 数据通讯： 自动化系统之间或 HMI 站和若干个自动化系统之间的数据交换。 数据通讯可以周期执行或基于事件驱动由用户程序块调用。
通过 PROFIBUS-DP 的过程通讯	SIMATIC S7-400 作为 DP 主站，可通过集成在 SIMATIC S7-400 CPU 上的 PROFIBUS -DP 接口（选件） 以下设备可作为主站连接到 PROFIBUS-DP 网络： • SIMATIC S7-400（CPU，CP 443-5，IM 467） • SIMATIC S7-300（CPU，CP 342-5DP 或 CP 343-5）	• SIMATIC C7（具有 PROFIBUS-DP 接口或 PROFIBUS-DP CP 的 C7） • SIMATIC S5-115U/H，S5-135U 以及具有 IM308 的 S5-155U/H • 具有 PROFIBUS-DP 接口的 S5-95U • 具有 PROFIBUS-DP 接口的 SIMATIC 505 具有 STEP 7 的编程器（PG）/PC 机或 OP 可作为总线上的主站，但只使用编程器和	OP 功能亦能运行在 PROFIBUS-DP 上。 以下设备可作为从站连接到 PROFIBUS-DP 上： • ET200 分布式 I/O 设备 • 现场设备 • SIMATIC S7-200，S7-300 • C7-633/P DP，C7-633 DP，C7-63P DP，C7-634 DP C7-626 DP • SIMATIC S7-400（只能通过 CP 443-5）。

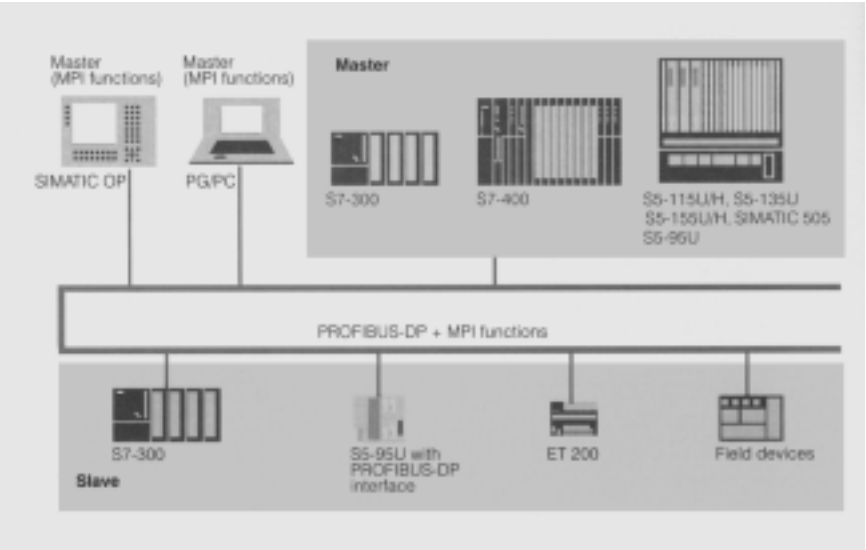


图 4 应用 PROFIBUS-DP 总线系统的联网

数据通讯概述	SIMATIC S7-400 有多种通讯机制：	• 通过全局数据（GD）通讯，网络上的 CPU 之间可周期地交换数据包。	• 应用通讯功能块，网络上各站点之间进行基于事件驱动的通讯。可通过 MPI、PROFIBUS 或工业以太网进行联网。
通过多点接口（MPI）的数据通讯	多点接口（MPI）通讯接口集成在 SIMATIC S7-400 的 CPU 中，它的用途很广泛： • 编程和参数设置 • 控制与监视以及 • 在同等通讯伙伴间建立简单的网络结构 • 多种连接能力：MPI 支持最多 32 个站点的同时连接： - PG/PC， - HMI 系统 - S7-200（作为从站） - S7-300 - S7-400 - C 7	• 通讯连接 S7-400 CPU 可同时建立最多 64 个站的连接： - 至 MPI 节点 - 至相关 C 总线（内部通讯总线，见下述）上的 C 总线节点（例如，通讯模板），以及可以和通讯模板相连接的各节点，例如：工业以太网节点。通讯模板必须是 C 总线节点 • MPI 性能 - 最多 32 个 MPI 节点 - 数据传输率最大为 12M bit/s。	• 灵活的配置选择：经过现场考验的部件用于配置 MPI 通讯：在 PROFIBUS 和分布式 I/O 产品范围内的总线电缆，总线连接器和 RS 485 中继器(12Mbit/s)。这些部件能使配置达到最佳化以充分满足用户的需要。例如，任意两个给定的 MPI 节点之间的长距离桥接可串联 10 个中继器。 • DP 主站：S7-400 的 MPI 也可以配置为 DP 主站，可以连接最多 32 个 DP 从站，通讯速率可达 12Mbit/s，编程和人机接口功能保持不变。

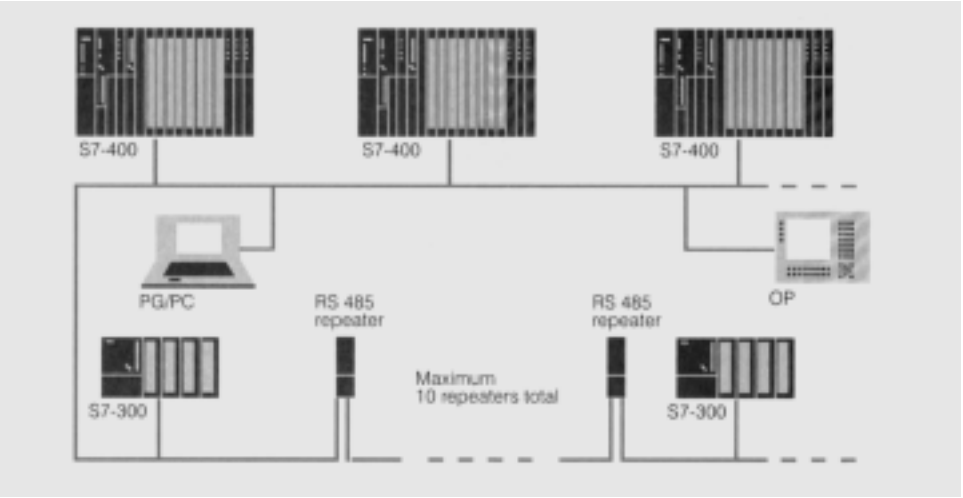


图 5 典型的带 MPI 接口的通讯配置

全局数据（GD）	通过 MPI，连网的 CPU 经全局数据通讯服务（每次程序循环最多 64 个字节的最多 16 个数据包）周期交换数据。	一个 CPU 可访问另一个 CPU 的数据/位存储器/过程映象。 例如，如果系统中包括 S7-300，则数据交换仅限于每个包不超过 22 字节。	全局数据通讯只能使用 MPI 接口，由 STEP 7 中的 GD 表进行组态。 在 CR2 之中，2 个 CPU 可通过 C 总线用 GD 数据包进行通讯。 S7/C7 通讯对象间的通讯服务通过集成在系统中的功能块进行。

通讯功能	S7/C7 通讯对象间的通讯服务通过集成在系统中的功能块进行。 可提供的通讯服务有： • 带 MPI 的 S7 标准通讯 • 带 MPI，C-总线，PROFIBUS 和工业以太网的 S7 通讯。(S7-300 只能用作服务器)	与 S5 通讯对象以及第 3 方设备的通讯服务可用非常驻块建立 这些服务包括： • 通过 PROFIBUS 和工业以太网的 S5 兼容通讯。 • 通过 PROFIBUS 和工业以太网的标准通讯（第三方系统）。	与全局数据通讯相对，必须为通讯功能建立相应的通讯链接。
通过 CP 的数据通讯（点对点）	使用 CP 441 通讯模板可实现功能强大的点到点通讯。	• 各种接口的可能性，包括： - 编程器和个人计算机 - SIMATIC S5/S7 - 工业 PC - 第三方的编程控制器 - 扫描机，条码阅读器，ID 系统 - 机器人控制器 - 打印机	• 不同种类的接口：可互换的接口模板能通过多种传送媒介进行通讯 - 20 mA（TTY） - RS 232C（V.24） - RS 422/485
通过 CP（PROFIBUS 或工业以太网）进行的数据通讯	SIMATIC S7-400 可通过 CP 443-x 通讯模板连接到 PROFIBUS 和工业以太网上。	可以连接以下设备： • SIMATIC S7-200（带 PROFIBUS） • SIMATIC S7-300 • SIMATIC S7-400 • SIMATIC S5-115U/H，S5-135U，S5-155U/H • 编程器	• 个人计算机 • SIMATIC HMI 操作员控制和监视系统 • 数字控制技术 • 机器人控制器 • 工业 PC • 传动控制器 • 其它制造厂的设备

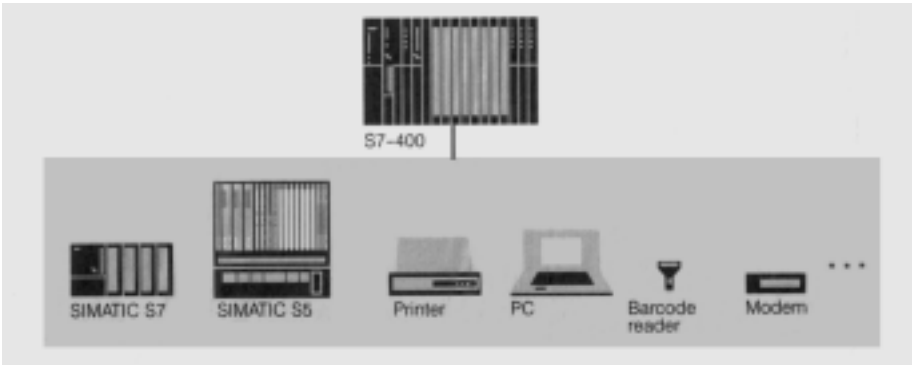


图 6 通过 CP 441 的点对点连接

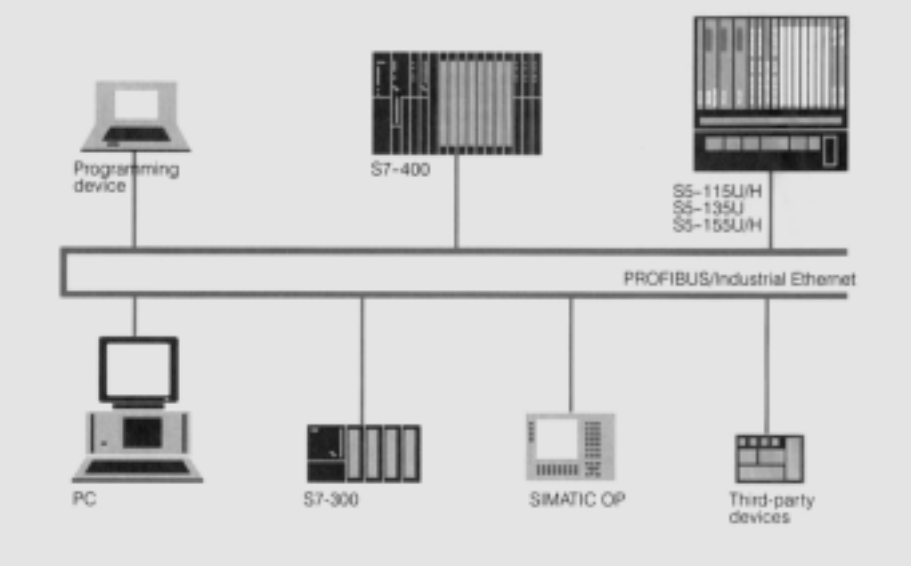


图 7 使用 PROFIBUS 或工业以太网的联网

模板的诊断和过程监视

SIMATIC S7-400 的许多输入/输出模板具有智能性

- 接收信号时的监视（诊断）
- 来自过程（过程中断）的信号监视。

诊断

可以用诊断功能来确定模板信号获取（就数字量模板而言）或模拟量信号处理（模拟量模板）是否正确的按功能进行。在诊断评价中，可参数化和不可参数化的诊断信息是有区别的。

- 可参数化的诊断信息：一个诊断信息只有通过相关参数化功能才能发出。
- 不可参数化的诊断信息：这些信息在任何情况下都能发出而不依赖于参数化功能。

如果一个诊断信息正在进行之中（例如 “ 不提供编码 ”），模板启动一个诊断中断（在可参数化诊断信息的情况下是在相关参数化功能完成之后）。CPU 中断用户程序以及低优先级的程序的执行，而处理相关的诊断中断块（OB 82）根据模板的类型不同，有各种各样的诊断信息：

数字量输入/输出模板

诊断信息	可能发生故障/错误的原因	诊断信息	可能发生故障/错误的原因
没提供编码器	编码器超载 编码器到 M 的线路短路	无内部附加电压	模板没有给 L+电压
无外部附加电压	模板没有 L+电压	熔丝烧断	内部熔丝损坏
模板中的参数不对	不正确的参数传送到了模板	RAM 故障	周期性高电磁干扰 模板损坏
监视器断路	周期性的高电磁干扰 模板损坏	硬件中断丢失	硬件中断序列的到达 速度快于 CPU 能够处理的能力
EPROM 故障	周期性的高电磁干扰 模板损坏		

模拟量输入模板

诊断信息	可能发生的故障/错误原因	诊断信息	可能发生的故障/错误原因
无外部负载电压	模板无 L+负载电压	测量范围下溢	输入值超出低限范围，引起故障的原因可能是： • 测量值范围 4~20 mA，1 到 5 V - 传感器连接极性颠倒 - 选择的测量范围有误 • 其它值的测量范围 - 选择的测量范围有误，
配置/参数化错误	不正确的参数传送到了模板		
共模故障	输入（M）和测量回路（M_{ANA}）的参考势点的势差太高	违反测量信号上限范围	
线路中断	编码器的连接电阻太高 模板和传感器之间的线路中断 回路没有连上（开路）		输入超高限

模拟量输出模板

诊断信息	可能发生的故障/错误原因	诊断信息	可能发生的故障/错误原因
无外部负载电压	模板无 L+负载电压	对地短路	输出超负载 从 QV 到 M_{ANA} 的输出短路
配置/参数化错误	不正确的参数传送到了模板	线路中断	执行器电阻太高 模板和执行器之间的线路中断 回路未使用（开路）

硬件中断

硬件中断功能用来监视过程信号以及反应信号变化的断开信号。

数字量输入模板

依据参数化功能，模板可以在任选的每一个通道组的信号上升沿，下降沿或者一个信号变化时的两种跳变沿的任一个上初始化一个过程中断。

CPU 中断用户程序或者具有低优先级的程序的执行，而处理相关的诊断中断块（OB 40）。信号模板的每个通道可暂时存贮一个中断内容。

模拟量输入模板

由参数化的上限值和下限值决定模拟量输入值的工作范围。

此模板用这些极限值与数字化了的测量值相比较。如果测量值违反了其中一个极限值，则给出一个硬件中断。CPU 中断用户程序或具有较低优先级的功能块的执行，去处理相关的诊断中断功能块（OB 40），如果这些极限值不在测量值范围之内，则不进行比较工作。

概述

- 有冗余设计的容错自动化系统
- 在容错技术下用于需要高可靠性的场合：再启动或停机将会造成较大损失的生产领域；需要少量管理和维护的工厂。
- 冗余的中央功能
- 加强 I/O 的可用性：可切换 I/O 的配置
- 也可应用常规的 I/O：单边配置
- 热备：在故障事件发生时自动地切换到备用单元
- 2 个单独的或一个分隔的中央机架配置
- 连接到冗余 PROFIBUS - DP 上的可切换 I/O。

应用

在许多自动化领域中，要求容错和高可靠性的自动化系统的应用越来越多。特别是在某些领域，停机将带来巨大的经济损失。在这种情况下，只有冗余系统才能满足高可靠性的要求。

高可靠性的 SIMATIC S7-400H 能充分满足这些要求。它能连续运行，即使控制器的某些部件由于一个或几个故障而失效也不受影响。由于 SIMATIC S7-400H 具有很高的可用性，它特别适合于以下的应用领域：

- 控制器发生故障后再启动的费用十分昂贵（一般在过程控制工业）
- 如发生停机，将会造成重大的经济损失
- 过程控制中包含有贵重的材料（如制药工业）
- 无人管理的应用场合。
- 需减少维护人员的场合。

SIMATIC S7-400H

设计

SIMATIC S7-400H 包括以下部件：

- 2 个中央控制器（机架）：2 个分立的中央控制器 UR1/UR2，或 1 个分割为 2 个区的中央控制器（UR2-H）。
- 每个中央控制器有 2 个同步模板，通过光纤连接这两个控制器
- 每个中央控制器有一个 CPU 417-4H
- 在中央控制器中架有 S7-400 I/O 模板
- UR1/UR2/ER1/ER2 扩展单元，与/或有 I/O 模板组的 ET 200M 分布式 I/O。

中央功能总是冗余配置的。

I/O 模板可以是常规配置或切换型配置。

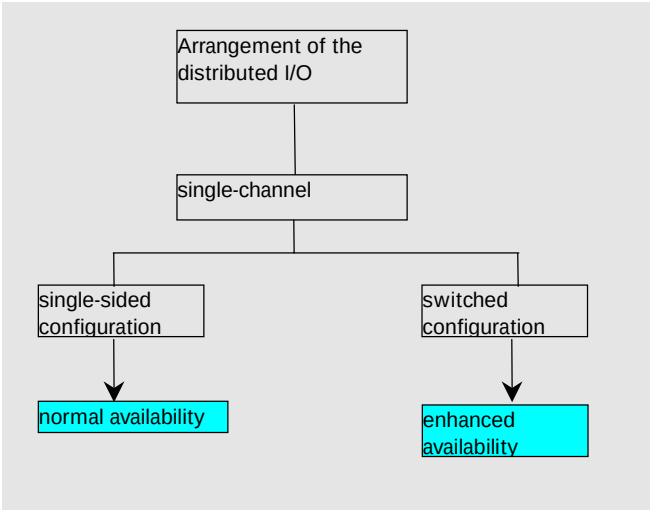


图 8 I/O 系统的可用性等级

常规的 I/O（单边配置）

在单边配置中，I/O 模板是单通道设计的，只能由二个中央控制器中的一个配置地址。单边配置的 I/O 模板可进行：

- 插入到一个中央控制器以及/或
- 插入到扩展机架或分布式 I/O 站

在单边配置中，读到的信息同时提供给 2 个中央控制器，使访问 I/O 的操作正确地运行。如发生故障，属于故障控制器的 I/O 模板退出运行。

单边配置适用于

- 不需要增加可靠性的应用场合
- 连接到以用户程序为基础的冗余 I/O 站。基于此种目的，系统必须对称的配置。

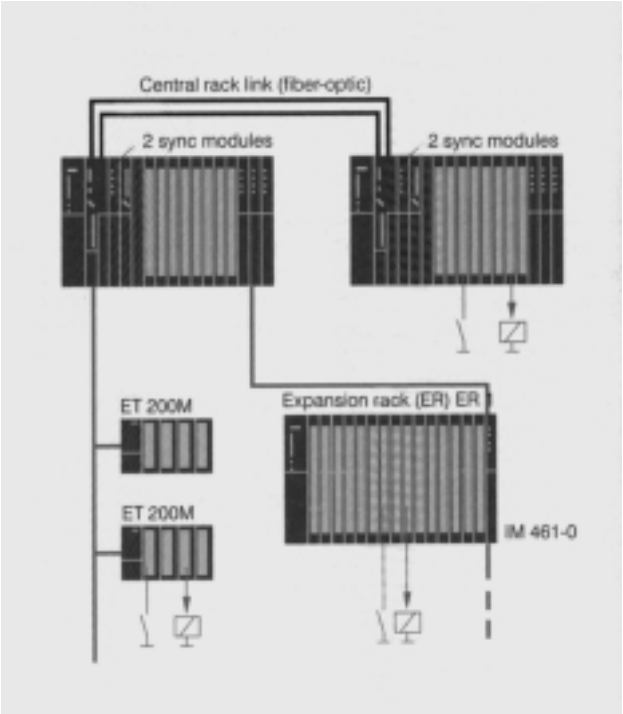


图 9 单边配置（常规的可用性）

设计（续）
增强的可靠性
（切换式配置）

在切换式配置中，I/O 模板虽为单通道设计，但是二个中央控制器均可通过冗余的 PROFIBUS-DP 网络访问 I/O 模板。切换式 I/O 模板只能插入

- ET 200M 远程 I/O 站。

通过 PROFIBUS-DP 连接到中央控制器。可切换的 ET-200M 连接到 2 个子单元中。

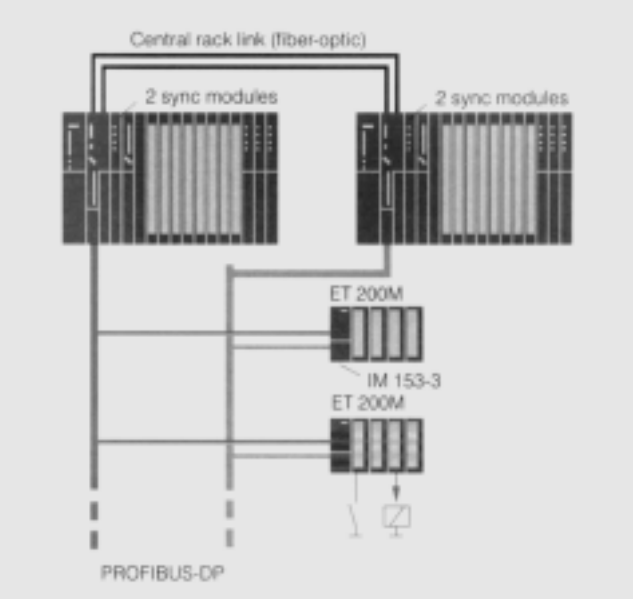


图 10 切换式配置

I/O 模板的冗余

I/O 模板的冗余有两处方式：

- 在两个可切换的 ET 200M 中用两个相同的 I/O 模板。
- 用 2 个相同的模板，每个都可分配给 2 个子单元中的任何一个子单元。

程序处理在用户级中管理，其步骤在有关手册中描述。

FM 和 CP 的冗余

功能模板（FM）和通讯模板有两种冗余配置：

- 可切换的冗余设置：FM/CP 可插到分立的 ET 200M 中，或成对的插入到可切换的 ET 200M 中的一个。
- 双通道冗余配置：FM/CP 可插到两个子单元或者是和这些子单元接口的扩展设备中（参考单边配置）

实现模板的冗余有不同的方法。

- 由用户编程：利用功能模块和 SIMATIC CP 可以由用户编程实现冗余功能。

选择主动模板并检测任何故障以便起动转换机制。所要求的程序和带冗余 FM/CP 的非冗余 CPU 的结构相一致。

- 操作系统直接支持：在 SIMATIC NET-CP（CP-443-1，CP 443-1 TCP，CP 443-5 基本型和 CP 443-5 扩展型）上，操作系统直接支持冗余结构，详细内容见通讯一章。

工作原理

CPU 417-H 操作系统自动地执行所有 S7-400H 需要的附加功能：

- 数据通讯
- 故障响应（切换到备用控制器）
- 2 个子单元的同步功能
- 自检

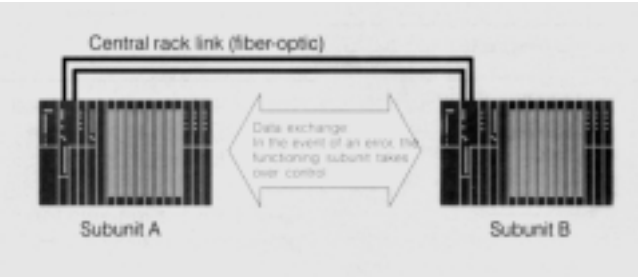
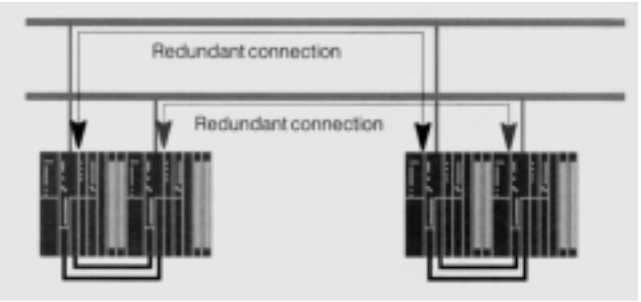


图 11 S7-400H 的工作原理

SIMATIC S7-400H

工作原理（续） 见余原理	“ 热备 ” 模式的 S7-400H 的运行是根据主动冗余原理（在发生故障时，无扰动地自动切换）。根据这个原理，无故障时两个子单元都在运行状态。如果发生故障，正常工作的子单元能独立地完成整个过程的控制。	为了保证无扰动地切换，必须做到中央控制器链路之间快速、可靠的数据交换。 为此控制器必须自动的接收 • 相同的用户程序 • 相同的数据块 • 过程映象内容	• 相同的内部数据，如计时器、计数器、位存储器等。 这样确保两个子控制器要随时更新内容，并在任何时间只要一个有故障，另一个可承担全部控制任务。
同步	为了无扰动地切换，两个单元必须保持同步。 S7-400H 运行于 “ 事件驱动同步 ”。	这就是说两个子单元有不同的内部状态时，就会进行同步操作。例如在下列情况： • 直接 I/O 访问 • 中断，报警 • 刷新用户时间	• 通过通讯功能修改数据 由操作系统自动地执行同步功能，编程时不需要考虑。
自检	S7-400H 执行扩展的自检。包括如下内容： • 中央控制器间的链接 • CPU 模板 • 处理器/ASIC • 存储器	检测到的每一个故障都给出报告。 运行后的自检， 当再起动时，每个子单元完整地执行所有的测试功能。	周期运行时的自检： 全部自测试被分配到几个周期中进行。每个周期只执行自检中的一部分，以减轻控制器的负担。
通讯 （高可用性的通讯）	SIMATIC 的高可用性的通讯，为用户提供了一种新型的通讯类型，它具有以下特点： • 增强了可用性： 发生故障时，通过最多达 4 个冗余连接，使通讯仍能继续进行。对用户来说，需要的切换过程是看不到的。 • 用户友好特点 从用户观点来看，高可用性是看不到的，可使用含标准通讯的用户程序，不需要做修改。冗余功能只在参数化阶段建立。	 图 12 S7-400H 的容错通讯 目前 S7-400H（冗余和非冗余配置）和 PC 支持容错通讯。PC 冗余需要有连接程序软件包。（见 “ SIMATIC NET 工业通讯 ” 一章）	配置 由于对容错的要求不同，其配置也是各种各样的： • 非冗余或冗余总线 • 总线型或环形结构
编程参数化	S7-400H 的编程和 S7-400 相同，可使用所有 SIMATIC S7 的编程语言。 编程 S7-400H 需使用 STEP 7 V 5.1 版本。	用于 S7-400H 的可选软件包 组态 S7-400H 的基本步骤和组态 S7-400 的基本步骤相同，例如 • 建立项目和站 • 配置硬件和网络 • 装载系统数据到目标系统	S7-400H 的可选软件包用来配置 S7-400H 的结构，和 S7-400 的配置不同。安装时，需要 STEP 7 标准软件包 V5.1 版或更高版本。

概述		• 安全型自动化系统适合于需要高安全性要求的设备 • 遵守 SIL3 至 IEC 61508，AK6 至 DIN V19250 和 Cat 4 到 EN 954-1 的安全要求。 • 如果需要，可通过冗余设计达到容错功能。	• 安全式 I/O 没有附加的连线： 通过带 PROFIS 安全曲线的 PROFIBUS-DP 的安全通讯 • 以 S7-400H 和 ET 200M 为基础，包括安全型模板。 • 标准模板可在非安全型的自动化系统中应用
应用	SIMATIC S7-400F/FH 安全型自动化系统可用在有着安全性要求的工厂。它的控制过程（如果直接关闭）不会对人或环境产生损坏。S7-400F/FH 有 2 种基本型： • S7-400F 安全型自动化系统 在控制系统中，如果发生故障，过程步骤转为安全状态，并执行中断。	• S7-400FH 安全及容错型自动化系统 如果在控制系统中发生故障，冗余的控制内容可以继续执行过程控制步骤。 S7-400F/FH 适应于具有下列安全型要求的场合： • 安全要求级别符合 AK1 至 AK 6 至 DIN V 19250/ DIN V VDE 0801。	• 安全要求级别符合 SIL 1 至 SIL 3 至 IEC 61508 • 待级 1 至 4 至 EN 954-1 另外，S7-400F/FH 可以使用标准模板，以及安全型模板，这样可以配置一个完全型集成控制系统。用在无安全性要求以及部分安全性要求的工厂中。整个工厂可以用相同的标准工具进行配置和编程。
工作原理	S7-400F/FH 的安全性功能已包含在 CPU 的 F 程序中，以及安全型的信号模板中。信号模板利用偏差分析和测试信号注入的方法来监视输出和输入的信号。	CPU 通过常规自检，结构检查以及逻辑和顺序程序流程控制来检查 PLC 的相关操作。另外，通过实际使用中的相关符号检查 I/O 模板的功能。如果在系统中发现了故障，后者转为安全状态，	F 运行时间许可证 必须将 F 运行时间许可证安装到 S7-400F/FH 的 CPU 417-4H 上。每一个 S7-400F/FH 系统需要一个许可证。
编程	S7-400F/FH 的编程方法和其它 SIMATIC S7 系统的编程方法相同。无安全性要求的部分设备的用户程序可以通过已被实践证明的编程工具编写，例如 STEP 7。 S7 F 系统的可选软件包 在编写有安全性要求的程序时需要“S7 F 系统”的可选软件包，软件包已包括用于生成 F 程序的所有功能和功能块。	下列软件包必须安装在 S7 F 系统的编程器或个人计算机上，以便运行。 • STEP 7 V5.1 或更高版本 • CFC V5.0+Service Pack 3 或更高版本 • S7-SCL v.5.0 或更高版本 • S7H 系统 v.5.1（对于 S7-400FH 为可选项）	从带 CFC 的 F 库中调用特殊功能块，并从内部连接到含有安全性功能的 F 程序中。由于交叉设备的标准显示需要，CFC 的使用，简化了对设备的配置和编程工作是可行的。编程者可以将精力全部集中在安全性要求的应用场合，而不必使用什么附加的工具。
通讯	中央控制器和 ET 200M 之间的安全型和标准通讯在 PROFIBUS-DP 上进行。特别是由于 PRFISafe PROFIBUS 规范的发展，允许安全	型功能的有用数据可以和标准数据信息框架一起传送。另外，不需要附加硬件设备。所必要的软件既可以是集成在硬件设备中的软件，	如操作系统的扩展部分，也可以是在 CPU 中经过检定的软件功能块。

设计	可以用不同的方法配置 S7-400F/FH 安全型自动化系统，以满足各种不同的要求。		
S7-400F 的单通道、单边 I/O 设计	设备需要带安全性保护的 PLC 控制，而又不必是容错式的，需要如下配置：	• 带 F 运行时间许可证的 1 个 CPU 417-4H • 1 条 PROFIBUS-DP 线 • 带 IM 153-2 FO 的 ET 200M • 无冗余设计的安全型信息模板	发生故障时 I/O 停止工作，安全型信号模板被钝化。

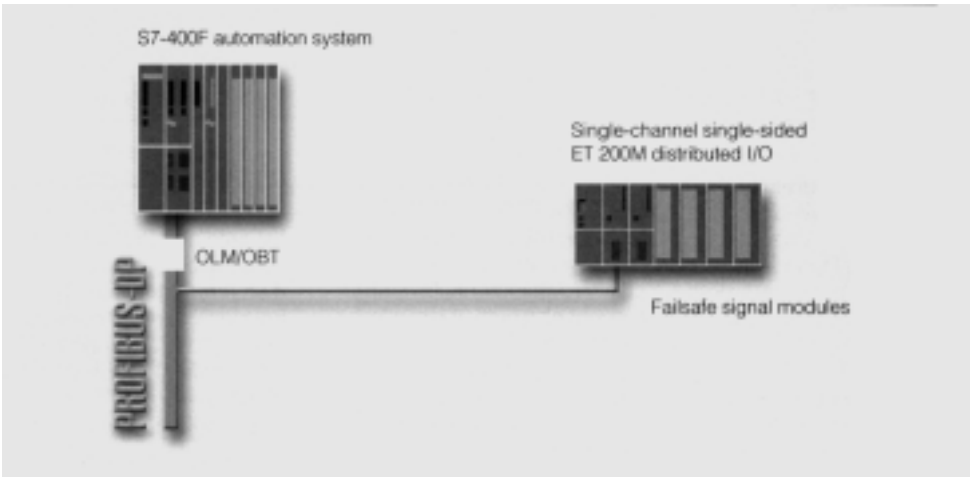


图 13 单通道单边 I/O 的配置

S7-400F 的单通道、切换式 I/O	设备需要带安全性保护的 PLC 控制，CPU 一侧采用容错技术，配置如下：	• 带 F 运行时间许可证的 2 个 CPU 417-4H • 2 条 PROFIBUS-DP 线 • 带 2 个 IM 153-2 FO（冗余）的一个 ET 200M • 无冗余设计的安全型信号模板	一个 CPU 1 个 IM 153-2 FO 或 1 条 PROFIBUS-DP 线发生故障后 PLC 还能继续使用。 如果安全型信号模板或 ET 200M 出现故障，I/O 则不能再工作，安全型信号模板处于钝化状态。

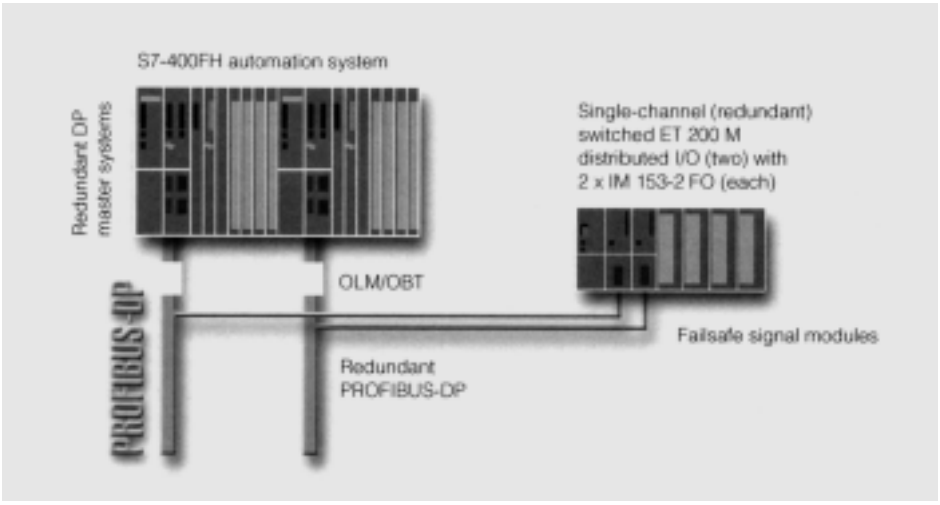


图 14 单通道、切换式 I/O 的配置

S7-400FH 的冗余切换式 I/O	设备需要带安全性保护的 PLC 控制，CPU 一侧需要采用容错技术，配置如下：	• 带 F 运行时间许可证可证的 2 个 CPU 417-4H • 2 条 PROFIBUS-DP 线 • 带 2 个 IM 153-2 FO（冗余式）的 2 个 ET 200M • 冗余设计的安全型信号模板	如果 CPU、IM153-2FO、PROFIBUS-DP，安全型信号模板或 ET 200M 出现故障，PLC 可以继续运行。 在 S7-400F/FH 自动化系统中也可以使用标准模板，但它们不能和 ET 200M 一起使用。

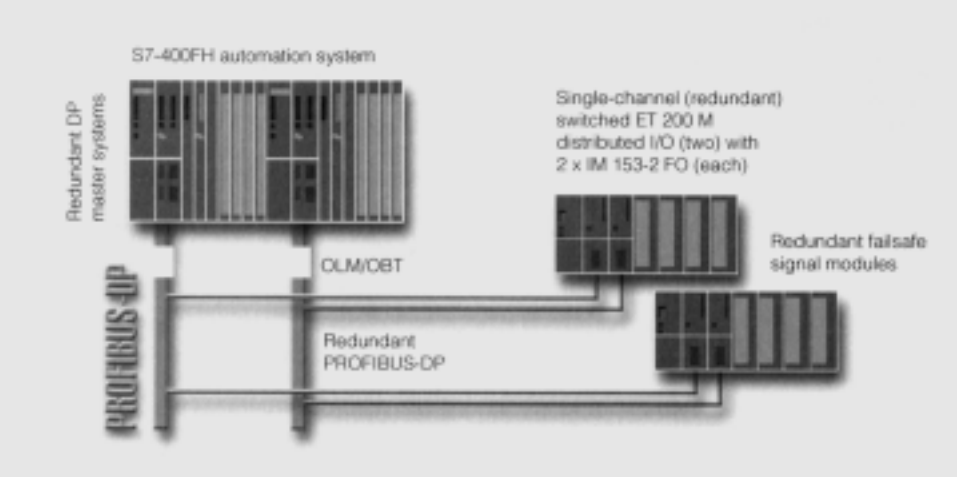


图 15 冗余切换式 I/O 的配置

总体技术规范	
保护等级	IP 20
环境温度	0 - 60°C
相对湿度	5 – 95%，无凝结
大气压	860 – 1080 hPa
电磁兼容	EG Directive 89/336/EWG；
	• Per EN 50082-2(噪声抑制)， Testing per：IEC 61000-4-2， IEC61000-4-4，IEC61000-4-3 IEC61000-4-6，IEC61000-4-5
	抑制干扰符合 EN 50081-2，极限制符合 EN 55011，A 级，第 1 组

机械公差	
• 震动测试	IEC 68，Part2-6/10-58Hz；连续振幅 0.075mm； 58-150Hz；恒定加速度 1g；
• 碰撞测试	IEC 68，Part 2-27/半正弦 碰撞 15g(峰值)，持续 11ms