SIEMENS

SIMATIC

SIMATIC S7 中的安全工程

系统手册

04/2006

A5E00887402-01

安全技术提示

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

危险

表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

警告

表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

小心

带有警告三角，表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

小心

不带警告三角，表示如果不采取相应的小心措施，可能导致财产损失。

注意

表示如果不注意相应的提示，可能会出现不希望的结果或状态。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

仅允许安装和驱动与本文件相关的附属设备或系统。设备或系统的调试和运行仅允许由**合格的专业人员**进行。本文件安全技术提示中的合格专业人员是指根据安全技术标准具有从事进行设备、系统和电路的运行，接地和标识资格的人员。

按规定使用

请注意下列说明：

警告

设备仅允许用在目录和技术说明中规定的使用情况下，并且仅允许使用西门子股份有限公司推荐的或指定的其他制造商生产的设备和部件。设备的正常和安全运行必须依赖于恰当的运输，合适的存储、安放和安装以及小心的操作和维修。

商标

所有带有标记符号 ® 的都是西门子股份有限公司的注册商标。标签中的其他符号可能是一些其他商标，这是出于保护所有者权利的目地由第三方使用而特别标示的。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

Siemens AG
Automation and Drives
Postfach 48 48
90437 NÜRNBERG

A5E00887402-01
Ⓟ02/2007

前言

系统说明的用途

此系统说明概述了 S7 Distributed Safety 和 S7 F/FH Systems 故障安全自动化系统。它介绍了 S7 Distributed Safety 和 S7 F/FH Systems 之间的异同，并提供了适用于 S7 Distributed Safety 和 S7 F/FH Systems 的详细技术信息。

此系统说明可帮助您确定最适合您的自动化任务的故障安全系统。决策者可以从中了解一些基础信息；服务和调试人员可以将其作为有关 S7 Distributed Safety 和 S7 F/FH Systems 故障安全自动化系统的技术信息来源（例如，可以在附录中找到有关 S7 Distributed Safety 和 S7 F/FH Systems 监视和响应时间的详细信息）。

系统说明的范围

此系统说明适用于 S7 Distributed Safety、S7 F Systems 和 S7 FH Systems 故障安全系统。

此系统说明还介绍了在 S7 Distributed Safety 和 S7 F/FH Systems 中集成以下故障安全 I/O 设备：

- S7-300 故障安全信号模块
- ET 200S 故障安全模块
- ET 200pro 故障安全模块
- ET 200eco 故障安全 I/O 模块
- 故障安全 DP 标准从站/I/O 标准设备

新增功能

下表总结了附加软件包 *S7 Distributed Safety V 5.4* 和 *S7 F Systems V5.2 SP2*（以及更高版本）中最重要的技术更改。此系统说明中已考虑到这些更改。

技术更改	更改将影响：	
	S7 Distributed Safety	S7 F/FH Systems
支持具有以下组件的 PROFINET IO： • CPU 416F-2（6ES7 416-2FK04-0AB0），从固件版本 V4.1 起（带有 CP 443-1 Advanced） • CPU 315F-2 PN/DP • CPU 317F-2 PN/DP • ET 200S 故障安全模块 • ET 200pro 故障安全模块 • 故障安全 I/O 标准设备	x	-
已扩展安全相关的 CPU-CPU 通讯，以包括 I 从站-从站通讯	x	-
通道出错时的特定通道钝化： • S7-300 故障安全信号模块 • ET 200S 故障安全模块 • ET 200pro 故障安全模块 • ET 200eco 故障安全 I/O 模块	x	-
新增 F 库块	-	x
安全数据写入	-	x
ET 200pro 故障安全模块	x	-
故障安全 I/O 标准设备	x	-

前言

系统说明的用途

此系统说明概述了 S7 Distributed Safety 和 S7 F/FH Systems 故障安全自动化系统。它介绍了 S7 Distributed Safety 和 S7 F/FH Systems 之间的异同，并提供了适用于 S7 Distributed Safety 和 S7 F/FH Systems 的详细技术信息。

此系统说明可帮助您确定最适合您的自动化任务的故障安全系统。决策者可以从中了解一些基础信息；服务和调试人员可以将其作为有关 S7 Distributed Safety 和 S7 F/FH Systems 故障安全自动化系统的技术信息来源（例如，可以在附录中找到有关 S7 Distributed Safety 和 S7 F/FH Systems 监视和响应时间的详细信息）。

系统说明的范围

此系统说明适用于 S7 Distributed Safety、S7 F Systems 和 S7 FH Systems 故障安全系统。

此系统说明还介绍了在 S7 Distributed Safety 和 S7 F/FH Systems 中集成以下故障安全 I/O 设备：

- S7-300 故障安全信号模块
- ET 200S 故障安全模块
- ET 200pro 故障安全模块
- ET 200eco 故障安全 I/O 模块
- 故障安全 DP 标准从站/I/O 标准设备

文档	相关内容简介
*《STEP 7》*手册	• *《使用 STEP 7 V5.x 组态硬件和通讯连接》*手册介绍了如何操作 *STEP 7* 标准工具。 • *《S7-300/400 的 LAD》*手册介绍了 *STEP 7* 中的标准梯形图编程语言。 • *《S7-300/400 的 FBD》*手册介绍了 *STEP 7* 中的标准功能块图编程语言。 • *《用于 S7-300/400 系统功能及标准功能的系统软件》*参考手册介绍了分布式 I/O 访问的功能和对分布式 I/O/CPU 的诊断。 • *《使用 STEP 7 V 5.x 进行编程》*手册介绍了使用 *STEP 7* 进行编程的过程。
STEP 7 在线帮助	• 介绍了 *STEP 7* 标准工具的操作。 • 包含有关如何使用 *HW Config* 为模块和智能从站组态和分配参数的信息。 • 包含对 FBD 和 LAD 编程语言的介绍
*《PROFINET 系统说明》*系统手册	• 介绍 PROFINET IO 的基本信息
*《PCS 7》*手册	• 介绍 *PCS 7* 过程控制系统（在更高级别控制系统中集成 F 系统时必需）的操作

可以在 CD-ROM 上找到完整的 SIMATIC S7 文档集。

指南

系统说明中包括以下主题：

- 故障安全自动化系统（尤其是在 SIMATIC S7 中）的概述
- S7 Distributed Safety 和 S7 F/FH Systems 的系统性能比较
- 介绍 S7 Distributed Safety 和 S7 F/FH Systems 的组态变量
- 为您确定满足要求的最佳解决方案的 F 系统的信息
- S7 Distributed Safety 和 S7 F/FH Systems 的通讯选项的异同比较
- S7 Distributed Safety 和 S7 F/FH Systems 中的安全机制（对用户很直观）的概述
- S7 Distributed Safety 和 S7 F/FH Systems F 系统所基于的标准
- 组态 S7 Distributed Safety 和 S7 F/FH Systems 的概述
- 对 S7 Distributed Safety 和 S7 F/FH Systems 进行编程的概述

  在 S7 Distributed Safety 和 S7 F/FH Systems 相应的编程和组态手册中更详细地介绍了编程和组态。
- 组态 F 系统中与 F 相关的监视时间
- 计算 S7 Distributed Safety 和 S7 F/FH Systems 中安全功能的最大响应时间

约定

此系统说明中所使用的术语“安全工程”和“故障安全工程”意义相同。该约定同样适用于术语“故障安全”和“F-”。

“安全程序”是指用户程序的故障安全部分，代替“故障安全用户程序”、“F 程序”等。

斜体“*S7 Distributed Safety*”和“*S7 F System*”是指“S7 Distributed Safety”和“S7 F/FH Systems”的附加软件包。

其它支持

有关对于本手册中所介绍产品的使用存在的未解答的问题，请与本地的西门子代理商联系：

http://www.siemens.com/automation/partner

培训中心

我们提供的课程可以帮助您熟悉使用 S7 自动化系统。请与当地的培训中心或位于纽伦堡（D-90327，德意志联邦共和国）的培训中心总部联系。

电话：+49 (911) 895-3200.

http://www.sitrain.com

H/F 专业中心

纽伦堡的 H/F 专业中心提供了关于 SIMATIC S7 故障安全和容错自动化系统的特殊车间。H/F 专业中心还可提供现场组态、调试和故障排除方面的协助。

电话：+49 (911) 895-4759

传真：+49 (911) 895-5193

有关车间等方面的问题，请联系：mailto:hf-cc@nbgm.siemens.com

技术支持

所有 A&D 产品均可寻求技术支持

- 以 Web 形式提出支持请求
  http://www.siemens.de/automation/support-request
- 电话：+ 49 180 5050 222
- 传真：+ 49 180 5050 223

您可以在以下网址找到有关技术支持的其它信息：
http://www.siemens.de/automation/service

Internet 上的服务与支持

除文档之外，我们还在以下 Internet 网址提供完整的知识库：

`http://www.siemens.com/automation/service&support`

在此处您将找到以下信息：

- 新闻快递为您提供有关产品的最新信息；
- 通过 Service & Support（服务与支持）中的搜索功能，可以找到适用的相关文档；
- 可供全球用户和专家交流经验的论坛；
- 我们的联系数据库，其中可以找到本地的自动化与驱动代理商；
- 在“Services”（服务）下可以找到有关本地服务、维修和更换部件的信息以及其它更多信息。

维护系统操作安全的重要信息

注意

系统（具有安全相关特性）的操作员必须遵守此操作安全要求。供应商在跟踪产品时，也必须强制遵守特定操作。为了确保您可以接收最新信息，将使用一条特殊的新闻快递，此新闻快递中包含的产品开发和属性信息对于安全相关的操作系统很重要（或潜在重要）。通过订阅相应的新闻快递，可以确保您始终看到最新信息，并在需要时对系统进行更改。

请跳转到 Internet 地址

http://my.ad.siemens.de/myAnD/guiThemes2Select.asp?subjectID=2&lang=en

并注册以下新闻快递：

- SIMATIC S7-300
- SIMATIC S7-400
- 分布式 I/O
- SIMATIC 工业软件

并选中每个新闻快递的“Updates”（更新）复选框。

目录

表格

1 故障安全系统概述

1.1 引言

安全工程的目的

安全工程的目的是通过使用以安全为导向的技术安装，尽可能地使对人员和环境的危害最小化，而不必再限制工业生产以及机器和化学产品的使用。

什么是故障安全自动化系统？

故障安全自动化系统（F 系统）用于控制可以在关闭后立即达到安全状态的过程。即在 F 系统控制过程中立即关闭过程不会对人员或环境造成危害。

故障安全系统超越了常规安全工程，启用了全部扩展至电子驱动和测量系统的远程智能系统。

F 系统用于具有高级安全要求的系统。通过详细的诊断信息，F 系统中改进的故障检测和本地化操作允许在生产出现安全相关的中断后快速恢复生产。

概述

本章介绍了 SIMATIC S7 中的安全工程。

同时介绍了 S7 Distributed Safety 和 S7 F/FH Systems 及其应用范围。还介绍了两个故障安全系统之间的重要异同。

在本章的最后一部分，介绍了使用故障安全系统 S7 Distributed Safety 和 S7 F/FH Systems 时，用户需要遵守的基本步骤。

1.2 安全集成 — 西门子提出的集成安全概念

安全集成

安全集成是西门子用于自动化和驱动的集成安全概念。

将自动化工程的成功技术和系统用于安全工程。安全集成覆盖从传感器和执行器下至控制器的整个系列，包括标准现场总线上安全相关的通讯。

除驱动器和控制器的功能任务外，它们还参与安全任务。安全集成的一个特别的功能是，它不仅确保可靠的安全性，还确保了高度灵活性和高生产率。

安全相关的输入和输出信号

安全相关的输入和输出信号形成了到工艺过程的接口。例如，这将允许从设备（例如急停按钮或光栅）中直接连接单通道和双通道 I/O 信号。安全相关的信号冗余地在内部组合在一起。冗余（例如 2 次）读取并比较安全相关的输入信号。统一的读取结果将以故障安全方式传送至中央处理单元，以便进一步处理。基于冗余 ANDing 驱动安全相关的执行器，用户无需执行任何其它操作。极大地简化了输入和输出互连。
这样将无需某些单独安装的硬件开关设备，因此简化了控制柜设计。

故障安全分布式 I/O 系统

故障安全分布式 I/O 系统的实现使 PROFIBUS DP 组件可以替换常规安全工程设计。这包括更换急停、保护门监视器和双手操作等开关设备。

将安全工程集成至标准自动化标准的优点

将安全工程集成至标准自动化系统具有以下重要优点：

- 具有集成故障安全工程的自动化系统比电子机械解决方案更灵活。
- 集成使接线解决方案更简便。
- 由于使用标准工程工具进行组态和编程，因此集成所需的工程量更少。
- 由于可以与 CPU 中的标准部分一起执行程序中的安全相关的部分，因此仅需要一个 CPU。
- 安全相关的组件和标准程序组件之间的通讯十分简单。

1.3 使用 F 系统指南

引言

本节介绍了使用故障安全系统的基本步骤。仅显示 F 系统与标准步骤不同的相关步骤。

此处将不介绍基于过程的计划任务（例如，创建流程图或过程变量列表、定义结构等）。

实例项目

您将在以下内容中找到组态和编程的介绍性实例项目：

- *《S7 Distributed Safety 使用入门》*中的 S7 Distributed Safety
- *《S7 Distributed Safety 组态和编程》*手册中的 S7 Distributed Safety
- *《可编程控制器 S7 F/FH》*手册中的 S7 F/FH Systems
- *step7\Examples* 目录中的 S7 F/FH Systems

系统规划

规划系统时，规划者将根据风险评估为每个所需的安全功能指定适用的安全等级（SIL/类别）。然后，将其用于确定实现安全功能的组件要求（可编程逻辑控制器、传感器和执行器）。这些决定将影响诸如硬件设计、组态和编程之类的其它活动。

注意

标准功能和安全功能的功能区分对于规划十分重要。

步骤顺序的范围为从选择组件到维护 F 系统

下表提供了获取信息的参考手册。相关产品信息表提供了关于 F-CPU 的其它信息。

表格 1-1　步骤顺序的范围为从选择硬件到维护 F 系统

步骤	操作步骤	参考
1.	**规划系统：** • 使用相应的安全等级（SIL/类别）指定安全功能。 • 指定 S7 Distributed Safety、S7 F Systems 或 S7 FH Systems；选择硬件和软件组件。	*《安全工程》*系统说明，*“故障安全系统的概述”*一节 产品目录

步骤	操作步骤	参考
2.	在 **STEP 7** 中组态硬件： • 组态 F-CPU 并为安全程序分配参数。 • 根据安全等级和接线图为故障安全 I/O（F-SM、F 模块）组态和分配参数。 • 为故障安全 DP 标准从站和 I/O 标准设备集成和分配参数。	*《安全工程》*系统说明，*“组态 F 系统”*一节 S7 Distributed Safety：*S7 Distributed Safety，组态和编程* S7 F/FH Systems：*S7 F/FH 自动化系统* ET 200S：*ET 200S，故障安全模块* ET 200pro：*ET 200pro，故障安全模块* ET 200eco：*ET 200eco，故障安全 I/O 模块* F-SM *S7-300，故障安全信号模块*
3.	**安装硬件：** • 通过开关设置 ET 200S、ET 200pro、ET 200eco 和 S7-300 F-SM 上的 PROFIsafe 地址。 • 安装模块。 • 根据所需的接线图连接模块。	ET 200S：*ET 200S，故障安全模块* ET 200pro：*ET 200pro，故障安全模块* ET 200eco：*ET 200eco，故障安全 I/O 模块* F-SM *S7-300，故障安全信号模块*
4.	**在 STEP 7 中创建安全程序：** • 从 F 库创建或选择 F 块；定位、互连 F 块并为其分配参数。 • 编译安全程序，并将其下载至 F-CPU。 • 测试安全程序。 • 如果需要，修改安全程序。 • 归档组态和安全程序。	*《安全工程》*系统说明，*“对 F 系统进行编程”*一节 S7 Distributed Safety：*S7 Distributed Safety，组态和编程* S7 F/FH Systems：*S7 F/FH 自动化系统*
5.	**调试系统：** • 如果需要，请在启动安全模式之前，由相关权威机构对安全相关的部分进行验收测试。 • 调试系统。	S7 Distributed Safety：*S7 Distributed Safety，组态和编程* S7 F/FH Systems：*S7 F/FH 自动化系统*
6.	**执行系统维护：** • 更换硬件和软件组件。 • 更新操作系统。 • 卸载 F 系统。	S7 Distributed Safety：*S7 Distributed Safety，组态和编程* S7 F/FH Systems：*S7 F/FH 自动化系统*

参见

引言 (页 121)

1.4 SIMATIC S7 中的故障安全系统

SIMATIC S7 中可以使用哪些故障安全系统？

可以使用两个故障安全系统以在 SIMATIC S7 自动化系统中集成安全工程：

1. **S7 Distributed Safety** 系统可实现机器和操作员保护（例如，用于机器工具和处理机械操作的急停设备）以及过程工业（例如，用于仪表和控制保护设备以及燃烧器的保护功能）方面的安全防护概念。
2. 故障安全，特别是可选的 **S7 F/FH Systems** 容错自动化系统非常适合过程处理和石油工业应用场合。

故障安全和容错 S7 FH Systems

为了增强自动化系统的可用性以防止由 F 系统中的故障导致过程故障，可以选择配备具有容错功能的故障安全 S7 F Systems（S7 FH Systems）。通过组件冗余（电源、中央处理单元、通讯和 I/O）增强可用性。

可实现的安全要求

S7 Distributed Safety 和 S7 F/FH Systems F 系统可以满足以下安全要求：

- 符合 IEC 61508 规定的安全等级（安全集成等级）SIL1 至 SIL3
- 符合 EN 954-1 规定的类别 2 至类别 4

S7 Distributed Safety 和 S7 F/FH Systems 中的安全功能原理

功能安全主要是通过软件中的安全功能实现的。在发生危险事件时 S7 Distributed Safety 或 S7 F/FH Systems 执行安全功能以恢复或维护系统的安全状态。安全功能主要包含在以下组件中：

- 故障安全 CPU（F-CPU）中的安全相关的用户程序（安全程序）
- 故障安全输入和输出（F-I/O）

F-I/O 确保现场信息的安全处理（急停按钮、光栅和电机控制）。它们具有安全处理所需的所有硬件和软件组件，符合要求的安全等级。用户仅对用户安全功能进行编程。

可以通过用户安全功能或故障响应功能提供该过程的安全功能。出现故障时，如果 F 系统无法再执行其实际用户安全功能，则将执行故障响应功能，例如，取消激活关联输出，以及在必要时将 F-CPU 切换至 STOP 模式。

用户安全功能和故障响应功能的实例

如果压力过大，F 系统将打开阀门（用户安全功能）。如果 F-CPU 中发生危险故障，则取消激活所有输出（故障响应功能），并且打开阀门，于是其它执行器也将处于安全状态。如果 F 系统完好无损，则将仅打开阀门。

具有 PROFIsafe 总线配置文件的 PROFIBUS DP 或 PROFINET IO

F-CPU 中的安全程序和故障安全输入和输出之间的安全通讯可以通过具有重叠 PROFIsafe 安全配置文件的“标准”PROFIBUS DP 或“标准”PROFINET IO 进行。在标准数据帧中发送安全功能的用户数据以及安全措施。

优点：

- 由于标准通讯和与安全相关的通讯均发生在标准 PROFIBUS DP 或标准 PROFINET IO 上，因此无需其它硬件组件。
- 可以解决安全相关的通讯任务而无需借助先前常规的解决方案（例如，急停设备的永久接线）或特殊总线。这样即可将其用于安全相关的分布式应用场合，例如，使用冲压设备和机械手的汽车底盘加工、燃烧器管理、缆车铁道中的乘客运送和过程自动化。
- 可以在 S7 Distributed Safety 和 S7 F/FH Systems F 系统（具有总线功能的传感器/执行器以及 PROFIBUS 合作伙伴公司的安全设备，它们是具有 PROFIsafe 功能的 DP 标准从站）中集成故障安全 DP 标准从站。
- 可以在 S7 Distributed Safety F 系统（具有总线功能的传感器/执行器以及 PROFIBUS 合作伙伴公司的安全设备，它们是具有 PROFIsafe 功能的 I/O 标准设备）中集成故障安全 I/O 标准设备。

1.4.1 S7 Distributed Safety 和 S7 F/FH Systems 的应用领域

S7 Distributed Safety 的使用

S7 Distributed Safety 故障安全系统主要用于机器和操作员保护（例如，用于机器工具和加工机械操作的急停设备)以及过程控制工业（例如，用于仪表和控制保护设备以及燃烧器的保护功能）。

以下显示了处于设备自动化级别的 S7 Distributed Safety 故障安全系统的集成选项。

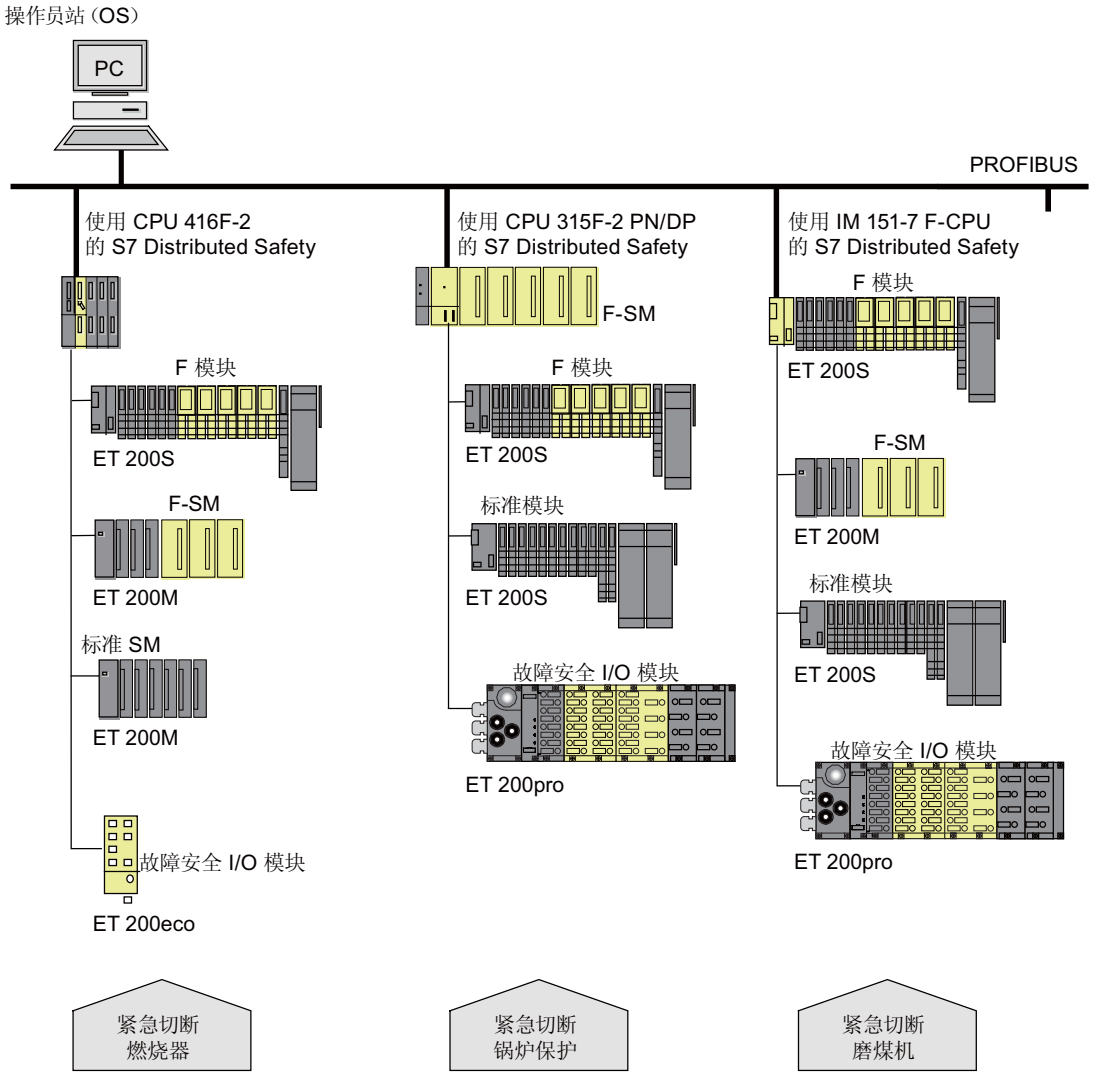
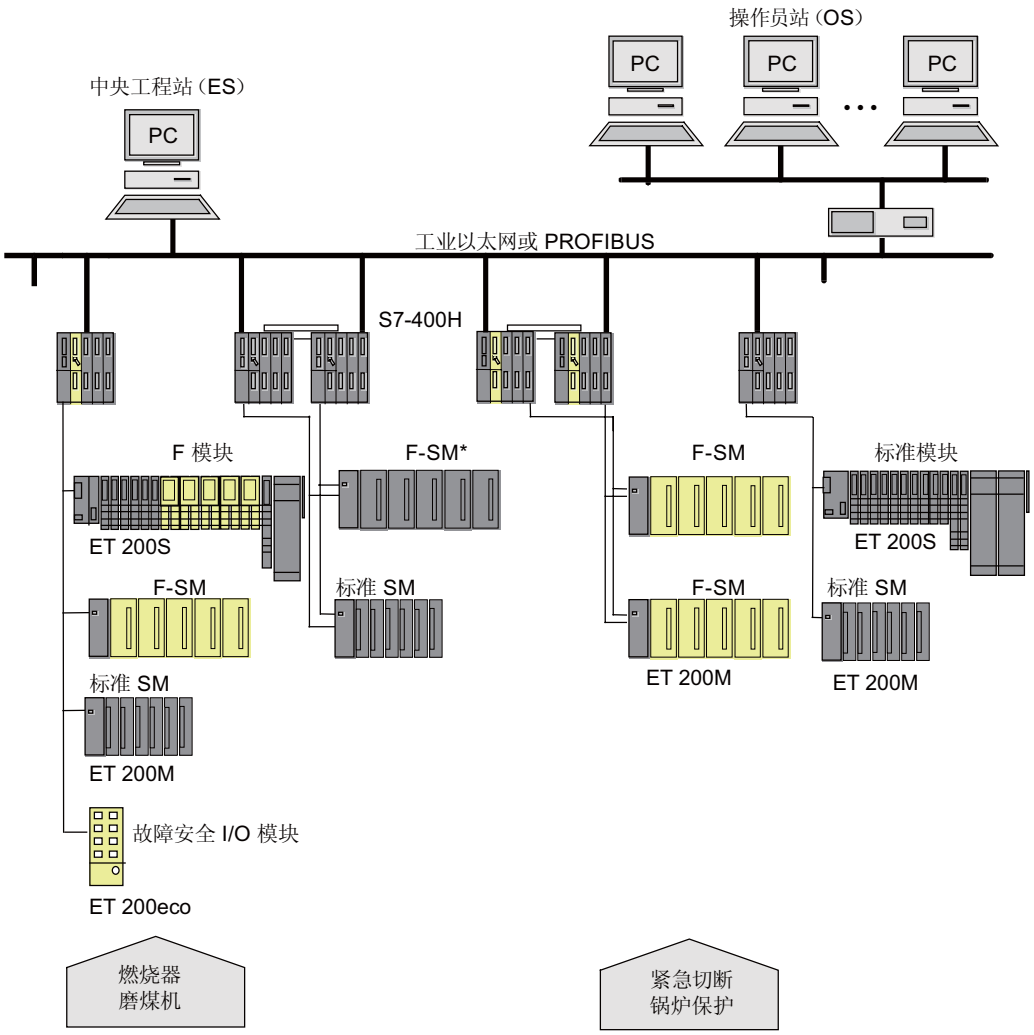


图 1-1 S7 Distributed Safety 的使用

S7 F/FH Systems 的使用

S7 F/FH Systems 故障安全系统主要用于过程工程以及仪表和控制应用中，其中通过禁用故障安全输出可以达到安全状态。

以下显示了在使用 PCS 7 的过程自动化系统中 S7 F Systems 和 S7 FH Systems 的集成选项。



* 在标准模式下

图 1-2　　S7 F/FH Systems 的使用

1.4.2 S7 Distributed Safety 和 S7 F/FH Systems 的性能特征

S7 Distributed Safety 和 S7 F/FH Systems 的共同特性

S7 Distributed Safety 和 S7 F/FH Systems 具有以下共同的重要特性：

- S7-300 或 S7-400 自动化系统中的集成；自动化任务确定系统设计，将故障安全工程集成到系统中
- 可以在相同系统（具有故障安全功能的标准系统，无需专用故障安全解决方案）上执行标准控制功能和保护功能
- 通过具有 PROFIsafe 功能的 PROFIBUS DP 连接分布式 I/O
- 使用标准 PROFIBUS 组件（铜质电缆和光纤电缆技术）
- *STEP 7* 中集成的组态，与标准自动化系统相同
- 使用 *STEP 7* 的标准编程语言创建安全程序
- 通过提供广泛的故障安全 I/O 以灵活适应任务要求

S7 Distributed Safety 和 S7 F/FH Systems 的系统性能比较

下表介绍了故障安全系统之间在重要性能特征方面的区别。

表格 1-2　　F 系统的性能特征

性能特征	S7 Distributed Safety	S7 F/FH Systems
可实现的安全等级	SIL3/类别 4	SIL3/类别 4
可以使用容错特性	否	是
开发阶段	故障安全系统	故障安全系统 故障安全和容错系统
故障安全 I/O 的连接	• 通过 PROFIBUS DP 集中式和分布式连接 • 通过 PROFINET IO（ET 200S 和 ET 200pro F 模块）分布式连接	• 通过 PROFIBUS DP 分布式连接
F 系统（取决于组态）的最小响应时间	50 ms	100 ms
F 系统的典型响应时间	100 ms 至 200 ms	200 ms 至 500 ms
通讯	安全相关的主站-主站通讯 安全相关的主站-I 从站通讯 安全相关的 I 从站-I 从站通讯 安全相关的 I 从站-从站通讯 通过 S7 连接（仅限工业以太网）的安全相关的通讯	通过 S7 连接（通过 PROFIBUS、MPI 和工业以太网等）的安全相关的通讯
创建安全程序	使用 *STEP 7* 中的标准 LAD 或 FBD 语言	在 CFC（*STEP 7* 的可选软件）中通过 safety matrix
在 RUN 模式下修改 F-CPU 中的安全程序	当前可能在取消激活的安全模式下，但是只有将 F-CPU 切换至 STOP 模式，才可能切换到安全模式	当前可能在取消激活的安全模式下或通过安全数据写入；切换到安全模式而无需更改 F-CPU 的工作模式
安全程序中的故障响应	通道或 F-I/O 的钝化 STOP 模式下的 F-CPU	通道或 F-I/O 的钝化 F-CPU 并未跳转到 STOP 而安全程序或故障 F 运行组已关闭
主要的应用领域	操作员和机器保护 燃烧器控制	仪表和控制以及过程工业 （可以在 PCS 7 过程控制系统中进行集成）

表格 1-3　　F-CPU 的存储器配置

F 系统	可用的 F-CPU	存储器配置（RAM）
S7 Distributed Safety	IM 151-7 F-CPU （6ES7 151-7FA01-0AB0）	96 KB（其中 64 KB 用于标准用户程序）
	CPU 315F-2 DP （6ES7 315-6FF01-0AB0）	192 KB
	CPU 315F-2 PN/DP （6ES7 315-2FH10-0AB0）	192 KB
	CPU 317F-2 DP （6ES7 317-6FF00-0AB0）	512 KB
	CPU 317F-2 PN/DP （6ES7 317-2FJ10-0AB0）	512 KB
	CPU 416F-2 （6ES7 416-2FK02-0AB0）	800 KB（用于程序）+ 800 KB（用于数据）
	CPU 416F-2 （6ES7 416-2FK04-0AB0）	1.4 MB（用于程序）+ 1.4 MB（用于数据）
S7 F/FH Systems	CPU 414-4H （6ES7 414-4HJ00-0AB0）	384 KB（用于程序）+ 384 KB（用于数据）
	CPU 414-4H （6ES7 414-4HJ04-0AB0）	700 KB（用于程序）+ 700 KB（用于数据）
	CPU 417-4H （6ES7 417-4HL00-0AB0） （6ES7 417-4HL01-0AB0）	2 MB（用于程序，可扩展至 10 MB）+ 2 MB（用于数据，可扩展至 10 MB）
	CPU 417-4H （6ES7 417-4HL04-0AB0）	10 MB（用于程序）+ 10 MB（用于数据）

支持 PROFINET IO（从 *S7 Distributed Safety V 5.4* 起）：

以下 F-CPU 和 F-I/O 支持 PROFINET IO：

- CPU 315F-2 PN/DP
- CPU 317F-2 PN/DP
- CPU 416F-2（6ES7 416-2FK04-0AB0），从固件版本 V4.1 起（带有 CP 443-1 Advanced）
- ET 200S 故障安全模块
- ET 200pro 故障安全模块
- 故障安全 I/O 标准设备

1.5 S7 Distributed Safety 和 S7 F/FH Systems 的组件

F 系统的硬件和软件组件

以下概述了组态和操作 S7 Distributed Safety 和 S7 F/FH Systems F 系统所需的硬件和软件组件。

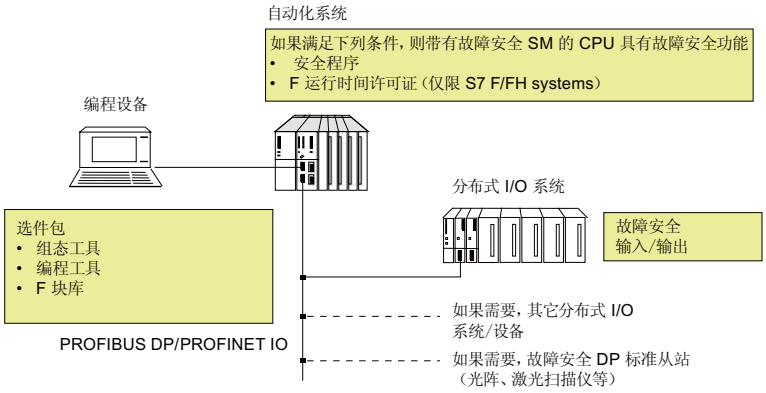


图 1-3 F 系统的硬件和软件组件的概述

组件的交互

要组态故障安全系统，必须组合特定的软件和硬件组件。

连接故障安全 I/O

用户将 F-I/O 连接至传感器和执行器，以便能够达到所需的安全等级。

组态硬件

用户在 *STEP 7 HW Config* 中组态 F-CPU 和 F-I/O。该组态必须与硬件组态匹配；即 F-I/O 的电路图必须反映参数设置。

创建安全程序

用户使用编程语言在 STEP 7 中创建安全程序。

对于 S7 Distributed Safety，用户在 F-FBD 或 F-LAD 中创建故障安全块。关联的 F 块库提供了用户可以在其安全程序中使用的故障安全块。对于大多数部件，F-I/O 在后台进行链接，无需用户参与操作。

对于 S7 F/FH Systems，用户为关联的 F 块库的故障安全块分配参数，并将其在 CFC 中互连。特殊的 F 驱动程序块可用于链接 F-I/O。还必须对这些驱动程序块进行参数化和互连。

对于这两种 F 系统，在编译可执行的安全程序时，将自动执行安全检查并自动合并用于故障检测的其它 F 块。

1.5.1 硬件组件

组件

F 系统包含满足特殊安全要求的部分硬件组件：

表格 1-4 硬件组件

F 系统	F-CPU	故障安全 I/O
S7 Distributed Safety	• IM 151-7 F-CPU • CPU 315F-2 DP • CPU 315F-2 PN/DP • CPU 317F-2 DP • CPU 317F-2 PN/DP • CPU 416-2	• ET 200M（分布式组态）中的 F 信号模块 • S7-300 站（具用 CPU 3xxF 的本地组态）的 F 信号模块 • ET 200S（具有 IM 151-7 F-CPU 的 DP 主站或智能 DP 从站）中的 F 电子模块 • ET 200S（具有 IM 151-1 HIGH FEATURE 的 DP 从站）的 F 电子模块 • ET 200S（具有 151-3 PN HIGH FEATURE 的 PROFINET IO 设备）的 F 电子模块 • ET 200pro F 模块 • ET 200eco 故障安全 I/O 模块 • 故障安全 DP 标准从站 • 故障安全 I/O 标准设备
S7 F/FH Systems	• CPU 414-4H • CPU 417-4H （每个都具有 F 运行许可证）	• ET 200M（分布式组态）中的 F 信号模块 • ET 200S（具有 IM 151-1 HIGH FEATURE 的 DP 从站）的 F 电子模块 • ET 200eco 故障安全 I/O 模块 • 故障安全 DP 标准从站

此外，还可以使用 S7-300 和 S7-400 的标准组件扩展 F 系统。

F-CPU

具有故障安全功能的 CPU 是可用于 S7 Distributed Safety 和 S7 F/FH Systems 的中央处理单元。

对于 S7 F/FH Systems，F 运行许可证允许将中央处理单元（CPU）用作 F-CPU。即，可以在其中运行安全程序。

对于 S7 Distributed Safety，不需要 F 运行许可证。

标准用户程序也可在 F-CPU 中运行。
由于可以避免标准用户程序对于安全程序的意外干扰，因此可以同时使用标准程序和安全程序。

必须对用户程序的安全相关的部分进行密码保护，以防止 F-CPU 以及编程设备或 ES 中的未经授权的访问。此外，F-CPU 使用高效措施检测并消除故障。

警告

您可以在 **S7 Distributed Safety** 中使用以下 F-CPU：IM 151-7 F-CPU、CPU 315F-2 DP、CPU 315F-2 PN/DP、CPU 317F-2 DP、CPU 317F-2 PN/DP 和 CPU 416F-2。请注意，这些 F-CPU **不能**用于 S7 F/FH Systems。

您可以在 **S7 F/FH Systems** 中使用以下 F-CPU：CPU 414-4H 和 CPU 417-4H。请注意，这些 F-CPU **不能**用于 S7 Distributed Safety。

故障安全 I/O

可以使用以下故障安全 I/O：

对于 S7 Distributed Safety 和 S7 F/FH Systems：

- S7-300 故障安全信号模块（F-SM）
- ET 200S 故障安全电源和电子模块（ET 200S F 模块）
- ET 200eco 故障安全 I/O 模块（ET 200eco F 模块）
- 故障安全 DP 标准从站

对于 S7 Distributed Safety：

- ET 200pro 故障安全电子模块
- 故障安全 I/O 标准设备

S7-300 故障安全信号模块

可以使用以下故障安全信号模块（F-SM）：

- 故障安全数字输入模块：
  - SM 326；DI 8 × NAMUR（具有诊断中断功能）
  - SM 326；DI 24 × 24 VDC（具有诊断中断功能）
- 故障安全数字输出模块：
  - SM 326；DO 10 × 24 VDC/2 A（使用诊断中断）
  - SM 326；DO 8 × 24 VDC/2 A（使用诊断中断）
- 故障安全模拟输入模块：SM 336；AI 6 × 13 位（使用诊断中断）

在标准应用中，F-SM 还可以用作具有标准 CPU 的标准 SM。从用户的角度来说，由于 F-SM 具有诊断中断功能，因此可以与大多数标准 SM 区别开。

在 S7 Distributed Safety 中，F-SM 可在 ET 200M 中作为分布式模块以及在 S7-300 站中作为集中式模块运行。

在 S7 F/FH Systems 中，F-SM 通常仅可以在 ET 200M 分布式 I/O 系统中运行。

例外：SM 326；DO 8 × DC 24V/2A 仅可以作为故障安全信号模块运行。但是，您完全可以使用以下 CPU 将其与 S7-300 系列的所有 F-CPU 一起集中安装：

- CPU 315F-2 DP（6ES7 315-6FF01-0AB0）（从固件版本 V2.0.9 开始）和
- CPU 315F-2 DP（6ES7 317-6FF00-0AB0）（从固件版本 V2.1.4 开始）。

该模块可以在 S7 Distributed Safety 的分布式组态中运行。

S7-300 标准 SM 的使用限制

在 S7 F/FH Systems 中使用 S7-300 标准 SM 时应该注意容错系统的限制（请参阅《自动化系统 S7-400H 容错系统》手册）。

有关 F-SM 安全模式下 S7-300 标准 SM 的限制，请参考《自动化系统 S7-300 故障安全信号模块》手册。

ET 200S 故障安全电子模块

可以在 ET 200S 中使用以下故障安全电子模块（F 模块）：

- 具有 2 个附加故障安全数据输出的 PM-E F pm 24 VDC PROFIsafe 电源模块
- PM-E F pp 24 VDC PROFIsafe 电源模块
- PM-D F 24 VDC PROFIsafe 电源模块
- 4/8 F-DO 24 VDC PROFIsafe 数字电子模块
- 4 F-DO 24 VDC/2 A PROFIsafe 数字电子模块

在标准应用中，F 模块**无法**与标准 CPU 一起使用。

具有故障安全模块的 ET 200S 的接口模块

每个 ET 200S 需要一个接口模块。F 系统将确定可以使用的接口模块：

表格 1-5　　接口模块与 ET 200S 故障安全模块一起使用

接口模块	订货号（或更高）	ET 200S 中的可用选件包	版本（或更高）
IM 151-1 HIGH FEATURE	6ES7 151-1BA00-0AB0	*S7 Distributed Safety*	V5.1
	6ES7 151-1BA01-0AB0	*S7 F Systems*	V5.2
IM 151-7 F-CPU	6ES7 151-7FA01-0AB0	*S7 Distributed Safety*	V5.2
IM 151-3 PN HIGH FEATURE	6ES7 151-3AB00-0AB0	*S7 Distributed Safety*	V 5.4

注意

与 IM 151-1 HIGH FEATURE 不同，例如，**IM 151-7 F-CPU** 是智能预处理设备（智能 DP 从站），并且还可用作 DP 主站。因此 IM 151-7 F/CPU 可以对技术功能单元进行完全控制（必要时进行完全独立控制），并可用作独立 CPU 或 F-CPU。IM151-7 F-CPU 是对 S7 Distributed Safety 的 F-CPU 系列的补充。

ET 200pro 故障安全模块

可以在 ET 200pro 使用以下故障安全电子模块（简称为 F 模块）：

- 8/16 F-DI DC24V PROFIsafe 数字电子模块
- 4/8 F-DI/4 F-DO DC24V/2A PROFIsafe 数字电子模块

ET 200eco 故障安全 I/O 模块

可以在 ET 200eco 中使用以下故障安全 I/O 模块（F 模块）：

- 4/8 F-DI 24 VDC PROFIsafe

故障安全 DP 标准从站

故障安全 DP 标准从站是使用 DP 协议和 PROFIsafe 总线配置文件在 PROFIBUS 上运行的标准从站。它们的特性必须符合 IEC 61784-1:2002 Ed1 CP 3/1 和 PROFIsafe 总线配置文件。

IE/PB link 后用于 PROFIBUS DP 和 PROFINET IO 混合组态的故障安全 DP 标准从站必须支持 V2 模式下的 PROFIsafe 总线配置文件。

GSD 文件用于组态故障安全 DP 标准从站。

故障安全 IO 标准设备

故障安全 I/O 标准从站是使用 I/O 协议和 PROFIsafe（V2 模式）总线配置文件在 PROFINET 上运行的标准设备。它们的特性必须符合 IEC 61784-1:2002 Ed1 CP 3/3 和 PROFIsafe 总线配置文件（V2 模式）。使用 GSDML 文件对其进行组态。

1.5.2 软件组件

引言

F 系统的软件组件包括以下内容：

- 在编程设备或 ES 上用于对 F 系统进行组态和编程的选件包
- F-CPU 中的安全程序

在编程设备或 ES 上，您还需要 *STEP 7* 基本软件以对标准自动化系统进行组态和编程。

对于 **S7 F/FH Systems**，您还需要用于 *STEP 7* 的 *CFC* 和 *S7-SCL* 附加软件以及 *PCS 7*（如果需要的话）。

用于对 F 系统进行组态和编程的选件包

可以使用两个选件包对 F 系统进行组态和编程（如下表所示）。

表格 1-6　用于组态和编程的选件包

选件包	订货号	F 系统	范围
S7 Distributed Safety	6ES7 833-1FC02-0YX0	**S7 Distributed Safety**	具有 F 块库的组态和编程软件适用于： • IM 151-7 F-CPU、CPU 315F-2 DP、CPU 315F-2 PN/DP、CPU 317F-2 DP、CPU 317F-2 PN/DP、CPU 416F-2 • ET 200S F 模块 • ET 200pro F 模块 • ET 200eco F 模块 • S7-300 F-SM • 故障安全 DP 标准从站 • 故障安全 I/O 标准设备
S7 F Systems	6ES7 833-1CC00-0YX0	**S7 F/FH Systems**	具有 F 块库的组态和编程软件适用于： • CPU 414-4H 和 CPU 417-4H • ET 200S F 模块 • ET 200eco F 模块 • S7-300 F-SM • 故障安全 DP 标准从站

使用这些选件包，用户将获得：

- 支持在 *STEP 7* 中使用 *HW Config* 组态 F-I/O。
- 用于创建安全程序的、具有故障安全块的 F 库
- 支持在安全程序中创建安全程序和集成故障检测功能

编程语言

使用不同的编程语言创建安全程序：

表格 1-7　　编程语言

F 系统	编程语言	说明
S7 Distributed Safety	F-LAD、F-FBD	• 在 *STEP 7* 中，F-LAD 和 F-FBD 编程语言与标准 LAD 和 FBD 语言的主要区别在于指令集和数据类型的限制。 • 可以使用*分布式安全* F 库或自定义 F 库的 F 应用程序块。
S7 F/FH Systems	CFC	• 在 *STEP 7* 中使用可选的 CFC 软件。 • 必须使用*故障安全* F 库中的特殊 F 块。

创建应用于 S7 Distributed Safety 的安全程序

用户在故障安全 FB 和 FC 中使用 F-FBD 或 F-LAD 创建安全程序。提供的 F 库包含用户可以合并至其安全程序的 F 应用程序块。

用户还可以选择为 S7 Distributed Safety（自定义 F 库）创建其自己的 F 库。

创建应用于 S7 F/FH Systems 的安全程序

通过对 F 库（随 *S7 F Systems* 选件包提供）中的故障安全块进行互连，用户可以使用 CFC 创建安全程序。

其它信息

有关组态 S7 Distributed Safety 和 S7 F/FH Systems 的详细信息，请参考*"组态 F 系统"*。在*"对 F 系统进行编程"*中介绍了 F 系统的编程。

组态和帮助选择

2

2.1 引言

概述

本章介绍了 S7 Distributed Safety 和 S7 F/FH Systems 故障安全系统的基本组态。

还根据 F 系统的实际要求提供了关于组态系列变体的信息。

本章的最后一部分介绍了客户用于确定哪个故障安全系统（S7 Distributed Safety、S7 F Systems 或 S7 FH Systems）适用于其自动化任务的主要标准。

其它信息

有关 F-I/O 的详细信息，请参考：

- *《自动化系统 S7-300 故障安全信号模块》*手册
- *《ET 200S 分布式 I/O 系统故障安全模块》*手册
- *《ET 200pro 分布式 I/O 设备、故障安全模块》*手册
- *《ET 200eco 分布式 I/O 站点故障安全 I/O 模块》*手册

2.2 F 系统的组态

基本组态

本章介绍了 F 系统的三种基本组态：

- S7 Distributed Safety 故障安全系统
- S7 F Systems 故障安全系统
- S7 FH Systems 故障安全和容错系统

2.2.1 S7 Distributed Safety 故障安全系统

S7 Distributed Safety 系统的组件

S7 Distributed Safety 指的是故障安全自动化系统，至少包含以下组件：

- 具有故障安全功能的中央处理单元（在其上执行安全程序），例如 CPU 315F-2 DP
- 故障安全 I/O，例如：
  - 带有 CPU 315F-2 DP 的集中式组态中的故障安全信号模块（F-SM）
  - ET 200M 分布式 I/O 系统中的故障安全信号模块（F-SM）
  - ET 200S 分布式 I/O 系统中的故障安全模块
  - ET 200pro 分布式 I/O 设备中的故障安全模块
  - ET 200eco 故障安全 I/O 模块
  - 故障安全 DP 标准从站/标准 I/O 设备

警告

您可以在 **S7 Distributed Safety** 中使用以下 F-CPU：IM 151-7 F-CPU、CPU 315F-2 DP、CPU 315F-2 PN/DP、CPU 317F-2 DP、CPU 317F-2 PN/DP 和 CPU 416F-2。请注意，这些 F-CPU **不能**用于 S7 F/FH Systems。

您可以在 **S7 F/FH Systems** 中使用以下 F-CPU：CPU 414-4H 和 CPU 417-4H。请注意，这些 F-CPU **不能**用于 S7 Distributed Safety。

S7 Distributed Safety F 系统的组态实例

下图说明了 S7 Distributed Safety F 系统的三个实例。

PROFIBUS DP 实例 1：使用 CPU 315F-2 DP 的 S7-300 站是 DP 主站。F-CPU 与集中式组态和 DP 从站中的故障安全 I/O 交换安全相关的数据。

可以通过其它故障安全 I/O、任意数量的“标准”DP 从站和标准模块扩展 F 系统。

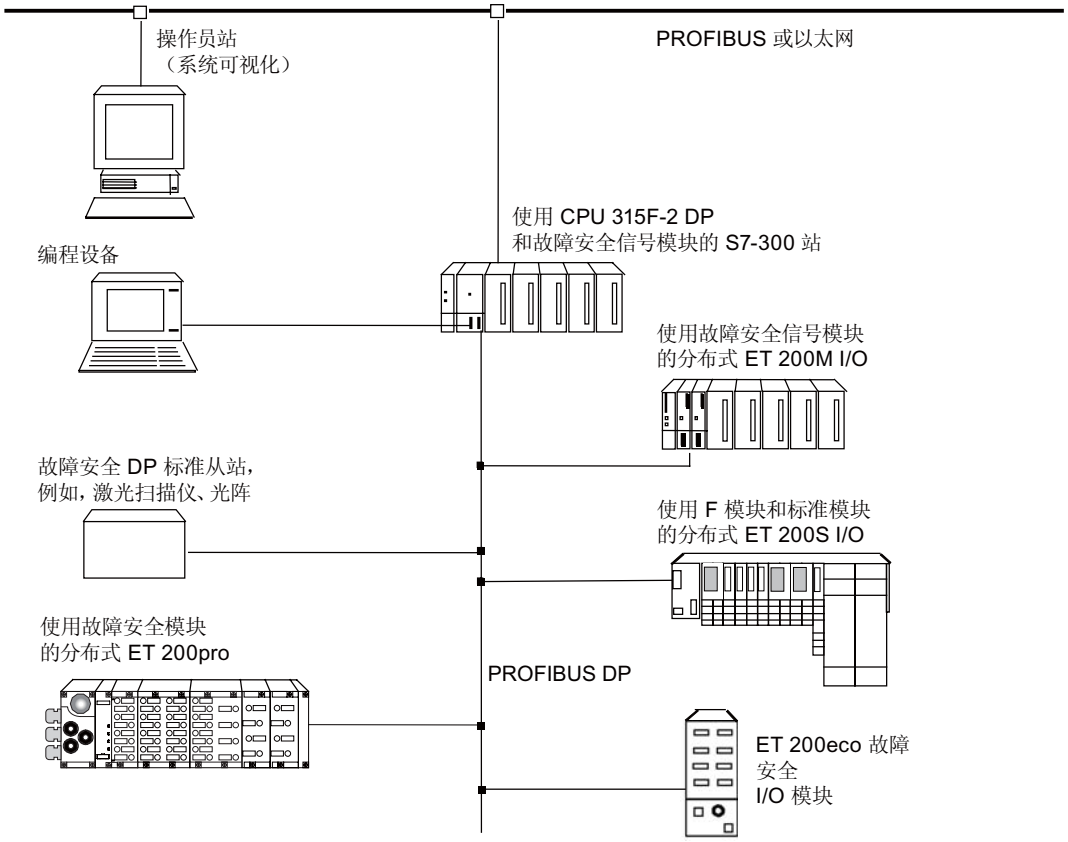


图 2-1　　实例 1：具有 PROFIBUS DP 的 F 系统 S7 Distributed Safety

PROFIBUS DP 实例 2：使用 CPU 416F-2 的 S7-400 站是 DP 主站。F-CPU 与 ET 200S 中的 IM 151-7 F-CPU 交换安全相关的数据。IM 151-7 F-CPU 用作智能预处理设备（I 从站）。

可以通过其它故障安全 I/O、任意数量的“标准”DP 从站和标准模块扩展 F 系统。

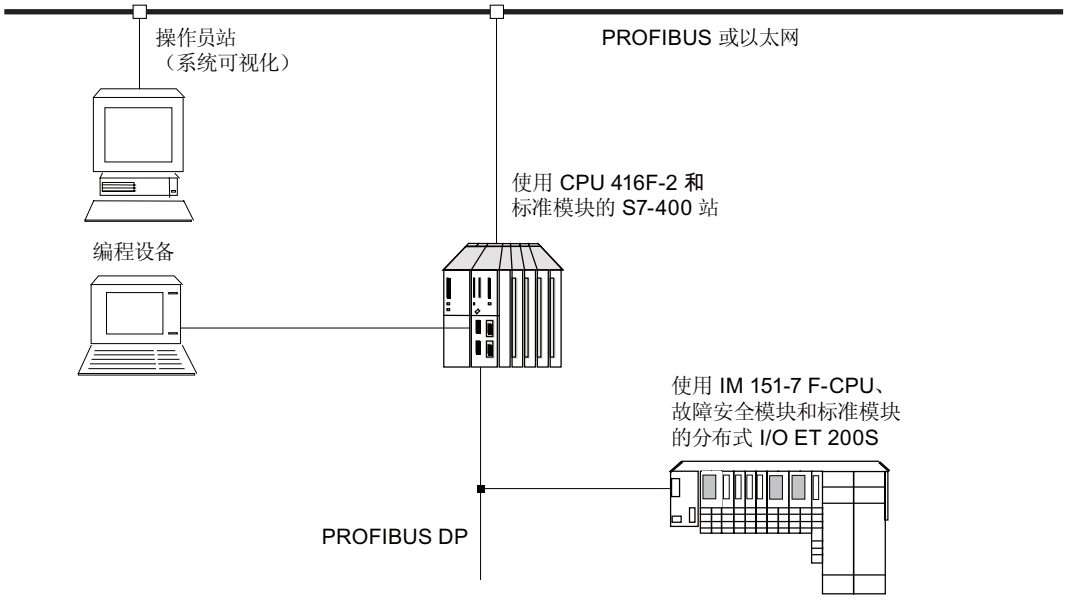


图 2-2　　实例 2：具有 PROFIBUS DP 的 F 系统 S7 Distributed Safety

PROFINET IO 实例 3：使用 CPU 315F-2 PN/DP 的 S7-300 站是 I/O 控制器。F-CPU 与 ET 200pro、ET 200S 和故障安全 I/O 标准设备中的故障安全模块交换安全相关的数据。

可以通过任意数量的“标准”I/O 设备扩展故障安全系统。

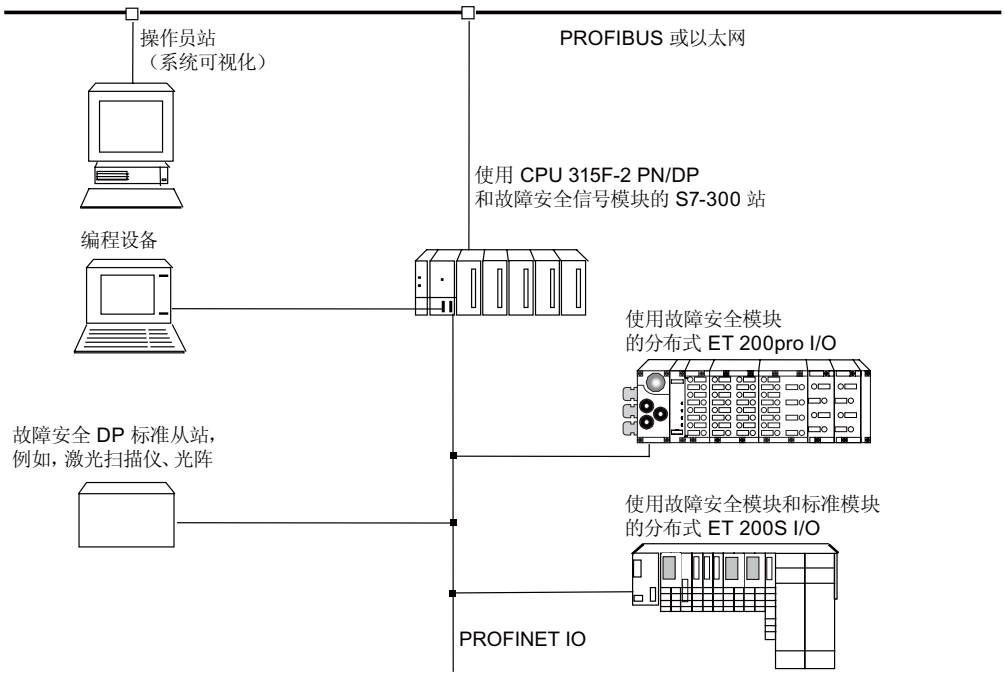


图 2-3　　实例 3：使用 PROFINET IO 的 F 系统 S7 Distributed Safety

2.2.2　S7 F Systems 故障安全系统

S7 F Systems 的组件

S7 F Systems 指的是故障安全自动化系统，至少包含以下组件：

- 具有故障安全功能的中央处理单元（在其上执行安全程序），例如具有 F 运行许可证的 CPU 417-4 H
- 故障安全 I/O，例如：
  - ET 200M 分布式 I/O 系统（具有可选冗余）中的故障安全信号模块（F-SM）
  - ET 200S 分布式 I/O 系统中的故障安全模块
  - ET 200eco 故障安全 I/O 模块
  - 故障安全 DP 标准从站

S7 F Systems F 系统的组态实例

下图说明了 S7 F Systems F 系统的实例。

使用 CPU 417-4H 的 S7-400 站是 DP 主站。F-CPU 与 DP 从站中的故障安全 I/O 交换安全相关的数据。可以通过其它故障安全 I/O、任意数量的“标准”DP 从站和标准模块扩展 F 系统。

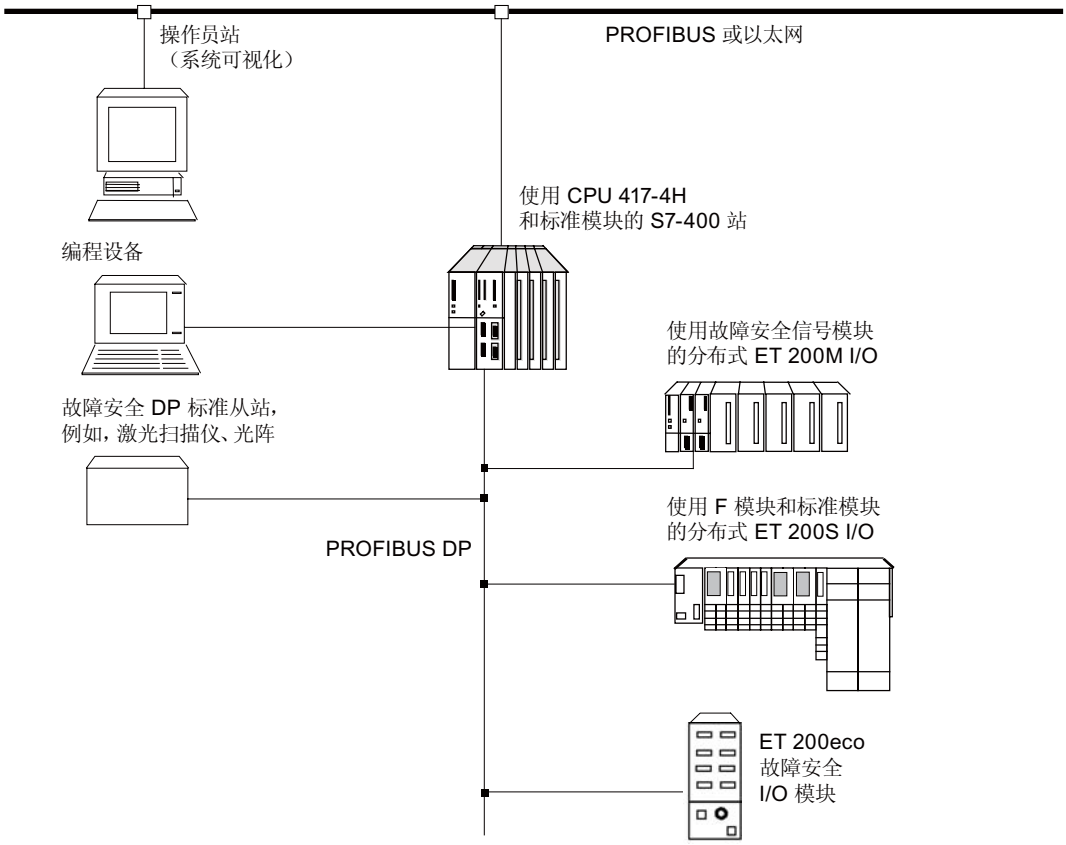


图 2-4　　S7 F Systems 故障安全系统

2.2.3 S7 FH Systems 故障安全和容错系统

S7 FH Systems 的组态

S7 FH Systems 指的是故障安全和容错自动化系统，至少包含以下组件：

- 执行安全程序的 S7-400H 容错系统（主站和备用站）
- 作为切换式 I/O（具有可选冗余）的 ET 200M 分布式 I/O 系统中的故障安全信号模块（F-SM）

S7 F Systems FH 系统的组态实例

下图说明了 S7 FH Systems 系统实例，该系统具有冗余 F-CPU 和共享、切换分布式 I/O 以及至冗余系统总线的连接。

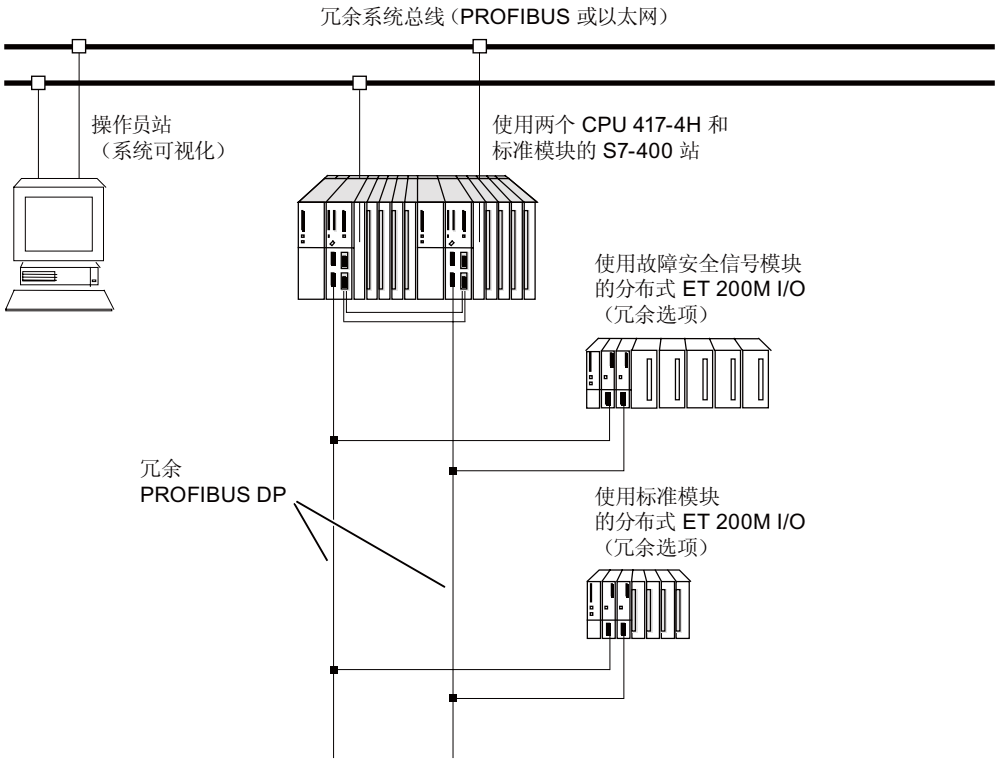


图 2-5 S7 FH Systems 故障安全系统

2.2.4 同时使用标准和故障安全组件

可以共同使用

标准组件、容错（H-）组件和故障安全（F-）组件以及系统可以组合在一起使用，如下所示：

- 标准系统、H 系统、F 系统和 FH 系统可以在一个**系统**中共同使用。
- 在 **F 系统**中：
  - 可以使用标准 I/O 和故障安全 I/O（例如 ET 200S、ET 200pro 和 ET 200eco）运行分布式 I/O 设备和系统。
  - S7-300 标准和故障安全信号模块可以作为集中式模块（仅在 S7 Distributed Safety 中）和分布式模块（在 ET 200M 中）在安全模式中运行。
- 在 F 系统或 FH 系统中，标准用户程序可与安全程序一起执行。

优点

F 组件、H 组件和标准组件共同使用具有以下优点：

- 可以组态利用标准 CPU 创新的全集成自动化系统。同时，可以独立于标准组件（例如，FM 或 CP）执行故障安全组件。使用标准工具（例如，*HW Config*、FBD、LAD 或 CFC）对整个系统进行组态和编程。
- 由于可以将不要求故障安全的程序部分与标准用户程序进行交换，因此可以在一个 F-CPU 中同时使用标准和故障安全程序部分，可以降低验收测试成本。这就缩小了安全程序（即，必须通过验收测试的程序部分）的大小。

  由于标准用户程序可在运行期间进行修改，因此如果将尽可能多的功能移至标准用户程序，也可以降低维护成本。

共同使用的边界条件

警告

对于 **SIL2/类别 3** 以及更低安全等级的应用场合，标准组件的物理接触保护措施已经够用了（请参阅使用的 F-CPU 和 F-I/O 的手册）。

对于安全等级为 **SIL3/类别 4** 的应用场合，还需要除物理接触保护以外的某些措施，以防止经由电源和背板总线的 F 电路的过压危险（即使在出现故障的情况下）。因此，可以采取下列措施系统免受背板总线的影响：

- S7-300 F-SM 的集中式和分布式组态的安全保护装置
- 对于 S7 F/FH Systems，PROFIBUS DP 使用光纤电缆设计
- ET 200S 故障安全模块和 ET 200eco 故障安全 I/O 模块在内部实现 250 VAC 隔离。

为保护免受电源影响，可以使用电源、标准 I/O 和故障安全 I/O 的组态规则（请参阅*故障安全 I/O 手册*）。

使用安全保护装置的规则

此安全保护装置用于保护 F-SM，避免在出现故障时可能发生过压。

警告

此安全保护装置必须用于 **SSIL3/类别 4** 应用场合：

- 通常，在 S7-300 中将 F-SM 用作集中式模块时
- 通常，使用铜质电缆配置 PROFIBUS DP 时
- 在使用光纤电缆配置 PROFIBUS DP，并需要在一个 ET 200M 中组合运行标准和故障安全 SM 时

有关安全保护装置的详细说明，请参考*《自动化系统 S7-300 故障安全信号模块》*手册。

2.3 根据可用性要求的故障安全系统组态变数

增强可用性的选项

为了增强自动化系统的可用性，以防止由 F 系统中的故障导致过程故障，可以选择将 S7 F Systems 故障安全系统组态为容错系统（**S7 FH Systems**）。可以通过组件冗余（F-CPU、通讯连接和 F-I/O）来增强可用性。

对于 S7 F Systems，无需进行容错组态即可增强系统可用性。故障安全信号模块（F-SM）可冗余地应用于一个或多个 ET 200M 中。

以下部分包括如何通过 S7 FH Systems 中 F-CPU 和 F-I/O 的冗余来增强可用性的说明。

注意

无法通过使用“SW Redundancy”（软件冗余）软件包来增强 S7 Distributed Safety 和 S7 F Systems 中故障安全 CPU 的可用性。

安全模式中的组态选项

可使用三种方式组态故障安全系统，如下所示：

表格 2-1　故障安全系统的组态选项（根据可用性）

系统	组态选项	说明	可用性
S7 Distributed Safety S7 F Systems	• 单通道 I/O	单通道和故障安全（F-CPU 和 F-I/O 无冗余）	标准可用性
S7 FH Systems	• 单通道切换式 I/O	单通道切换式和故障安全（F-CPU 有冗余，F-I/O 无冗余；如果出现故障，系统将切换至其它 F-CPU）	增强的可用性
	• 冗余切换式 I/O	多通道和故障安全（F-CPU、PROFIBUS DP 和 F-I/O 有冗余）	最高可用性

下面介绍典型的组态实例。为每个组态变体实现不同等级可用性的过程数据。

有关增强可用性的其它信息

该手册的*“安全相关的 CPU-CPU 通讯”*一节介绍了 S7 FH Systems 中 F-CPU 之间的通讯。有关 S7-400H 容错系统的信息，请参考*《自动化系统 S7-400H 容错系统》*手册。

有关 PROFIBUS 和工业以太网的更多信息

SIMATIC NET 硬件手册*《PROFIBUS 网络》*和*《工业双绞线和光纤网络》*中分别介绍了 PROFIBUS 或工业以太网。

2.3.1 单通道 I/O（S7 Distributed Safety）

单通道 I/O 的特性

在单通道组态中，故障安全 I/O 无冗余。故障安全 I/O 由一个 F-CPU 进行寻址。

S7 Distributed Safety 需要的硬件组件

根据将 F 系统组态为集中式系统还是分布式系统，以及使用铜质电缆还是光纤电缆配置 PROFIBUS DP，来确定需要的硬件组件。F-I/O 无冗余。

S7 Distributed Safety 的集中式组态

S7 Distributed Safety 的集中式组态需要以下元件：

- 一个 CPU 31xF-2 DP 或 CPU 31xF-2 PN/DP
- F-SM 和标准 SM（如果需要）
- 安全保护装置（仅 SIL3/类别 4 应用场合需要）

S7 Distributed Safety 的组态实例：单通道 I/O（集中式组态）

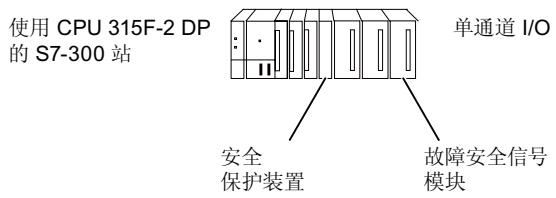


图 2-6 使用单通道 I/O（集中式组态）的 S7 Distributed Safety

使用独立 IM 151-7 F-CPU 的 S7 Distributed Safety

注意

与 IM 151-1 HIGH FEATURE 不同，**IM 151-7 F-CPU** 是智能处理设备（I 从站），并且还可以用作 DP 主站。因此，IM 151-7 F-CPU 可以对技术功能单元进行完全和独立（如果需要）的控制，并可用作独立 CPU 或 F-CPU。IM151-7 F-CPU 表示对 S7 Distributed Safety 的 F-CPU 行的附加。

S7 Distributed Safety 的组态实例：单通道 I/O（独立 IM 151-7 F-CPU）

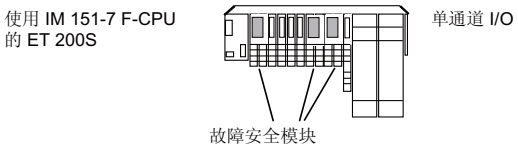


图 2-7　　使用单通道 I/O（独立 IM 151-7 F-CPU）的 S7 Distributed Safety

使用铜质电缆的 S7 Distributed Safety 和 PROFIBUS DP 的分布式组态

使用铜质电缆进行分布式组态时需要下列各项：

- 一个 CPU 416F-2、CPU 31xF-2 DP、CPU 31xF-2 PN/DP 或 IM 151-7 F-CPU
- 一根 PROFIBUS DP 线
- 故障安全 I/O，例如：
  - 一个 ET 200M 具有：
    IM153-2、F-SM、标准 SM（如果需要）
    和安全保护装置（仅 SIL3/类别 4 需要）
  - 一个 ET 200S 具有：
    IM 151-1 HIGH FEATURE 或 IM 151-7 F-CPU、
    故障安全模块和 ET 200S 标准模块（如果需要）
  - 一个 ET 200pro 具有：
    IM 154-2 HIGH FEATURE、
    故障安全模块和 ET 200pro 标准模块（如果需要）
  - ET 200eco 故障安全 I/O 模块
  - 故障安全 DP 标准从站
- 用于将 F-CPU 和故障安全 I/O 连接至 PROFIBUS DP 的总线连接器

S7 Distributed Safety 的组态实例：单通道 I/O（使用铜质电缆进行分布式组态）

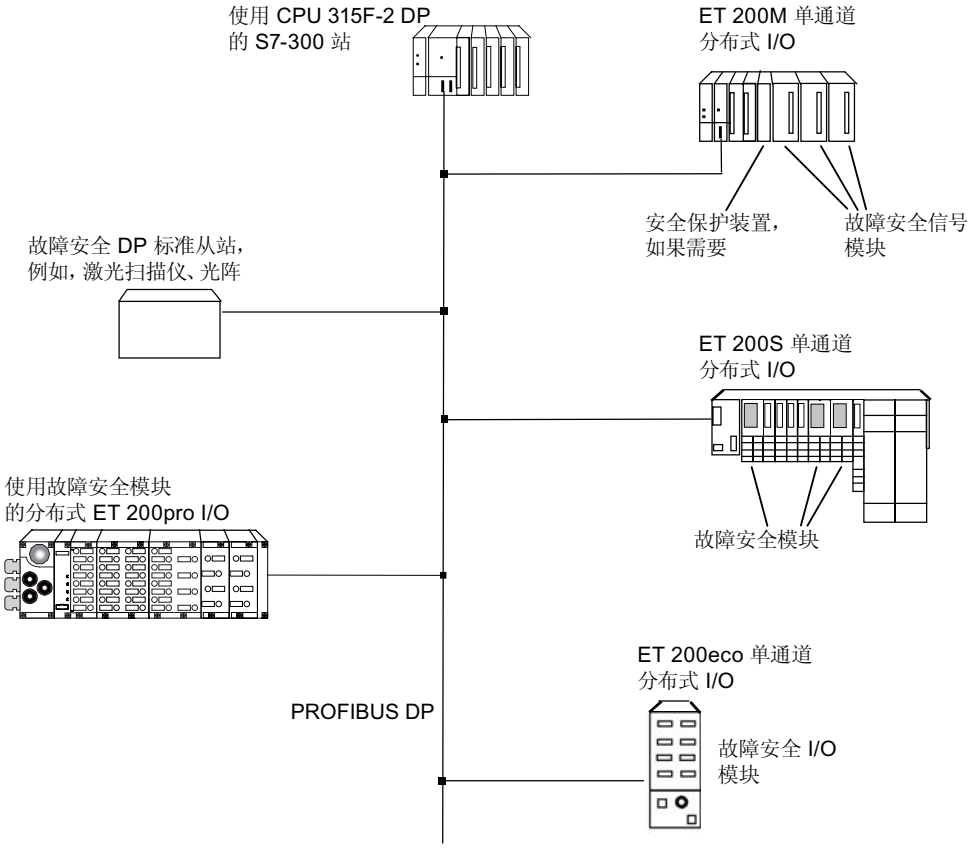


图 2-8　　使用单通道 I/O（PROFIBUS DP、铜质电缆）的 S7 Distributed Safety

使用光纤电缆的 S7 Distributed Safety 和 PROFIBUS DP 的分布式组态

使用光纤电缆配置 PROFIBUS DP 时需要下列各项：

- 一个 CPU 416F-2、CPU 31xF-2 DP、CPU 31xF-2 PN/DP 或 IM 151-7 F-CPU
- 一根 PROFIBUS DP 线
- 故障安全 I/O，例如：
  - 一个 ET 200M 具有：

    IM153-2 FO、F-SMs、标准 SM（如果需要）

    和安全保护装置（仅当在 ET 200M 中同时使用 F-SM 和标准 SM 时，SIL3/类别 4 应用场合需要）
  - 一个 ET 200S 具有：

    IM 151-1 HIGH FEATURE 或 IM 151-7 F-CPU、

    故障安全模块和 ET 200S 标准模块（如果需要）
  - 一个 ET 200pro 具有：

    IM 154-2 HIGH FEATURE、

    故障安全模块和 ET 200pro 标准模块（如果需要）
- 用于将 F-CPU 和故障安全 I/O 连接至光纤电缆的组件，例如 OLM/OBT

S7 Distributed Safety 的组态实例：单通道 I/O（使用光纤电缆进行分布式组态）

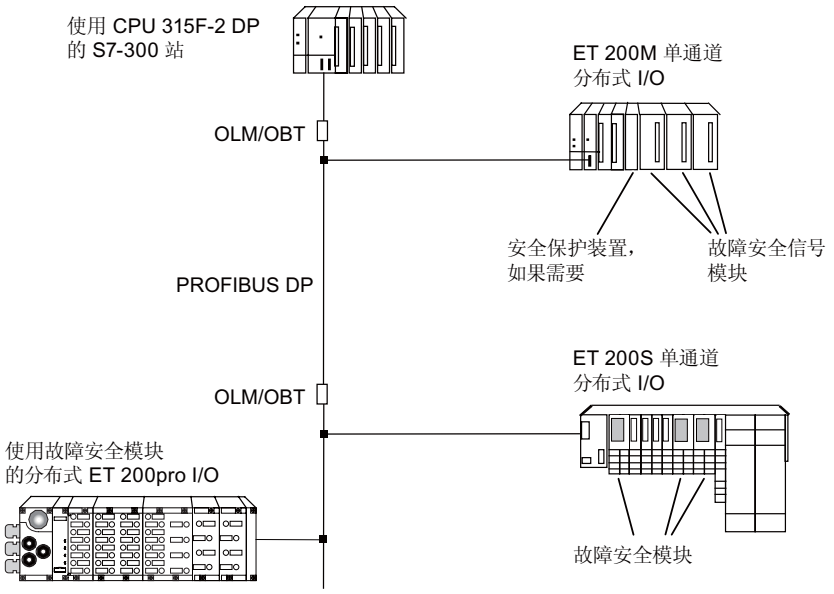


图 2-9　　使用单通道 I/O（PROFIBUS DP、光纤电缆）的 S7 Distributed Safety

S7 Distributed Safety 和 PROFINET IO 的分布式组态

设置 PROFINET IO 时需要下列各项：

- 一个 CPU 31xF-2 PN/DP 或使用 CP 443-1 Advanced 的 CPU 416F-2（从固件版本 V4.1 起）
- 一根 PROFINET IO 线
- PROFINET IO 的故障安全 I/O，例如：
  - 一个 ET 200pro，使用：

    IM 154-4 PN HIGH FEATURE

    故障安全模块和 ET 200pro 标准模块（如果需要）
  - 一个 ET 200S，具有：

    IM 151-3 PN HIGH FEATURE

    故障安全模块和 ET 200S 标准模块（如果需要）
- 故障安全 I/O 标准设备
- 用于组态 PROFINET 的组件
  - 被动式网络组件（电缆、插头）
  - 主动式网络组件（交换机、路由器等）（如果需要）

S7 Distributed Safety 和 PROFINET IO 的组态实例

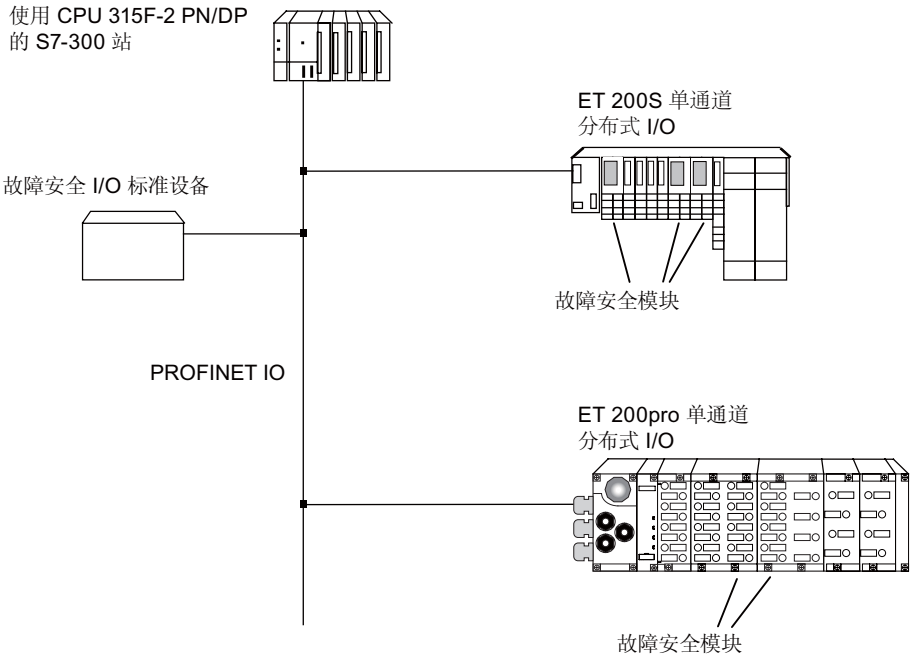


图 2-10　　使用单通道 I/O（PROFINET IO）的 S7 Distributed Safety

单通道 I/O 的可用性限制

如果出现故障，I/O 将不再可用。F-I/O 已钝化。

可能的故障原因：

- F-I/O 故障
- ET 200M、ET 200S 或 ET 200pro 中的接口模块故障
- 整个 ET 200M、ET 200S、ET 200pro 或 ET 200eco 故障
- PROFIBUS DP 或 PROFINET IO 线路故障
- F-CPU 故障

2.3.2 单通道 I/O（S7 F Systems）

什么是单通道 I/O？

在单通道组态中，故障安全 I/O 无冗余。故障安全 I/O 由一个 F-CPU 进行寻址。

S7 F Systems 需要的硬件组件

根据使用铜质电缆还是光纤电缆配置 PROFIBUS DP，来确定需要的硬件组件。F-I/O 无冗余。

使用铜质电缆的 S7 F Systems 和 PROFIBUS DP

使用铜质电缆配置 PROFINET DP 时需要下列各项：

- 一个 CPU 414-4H 或 CPU 417-4H
- 一根 PROFIBUS DP 线
- 故障安全 I/O，例如：
  - 一个 ET 200M 具有：
    IM153-2、
    F-SM、标准 SM（如果需要）和
    安全保护装置（仅 SIL3/类别 4 需要）
  - 一个 ET 200S 具有：
    IM 151-1 HIGH FEATURE、
    故障安全模块和 ET 200S 标准模块（如果需要）
  - ET 200eco 故障安全 I/O 模块
  - 故障安全 DP 标准从站
- 用于将 F-CPU 和故障安全 I/O 连接至 PROFIBUS DP 的总线连接器

S7 F Systems 的组态实例：使用铜质电缆的单通道 I/O

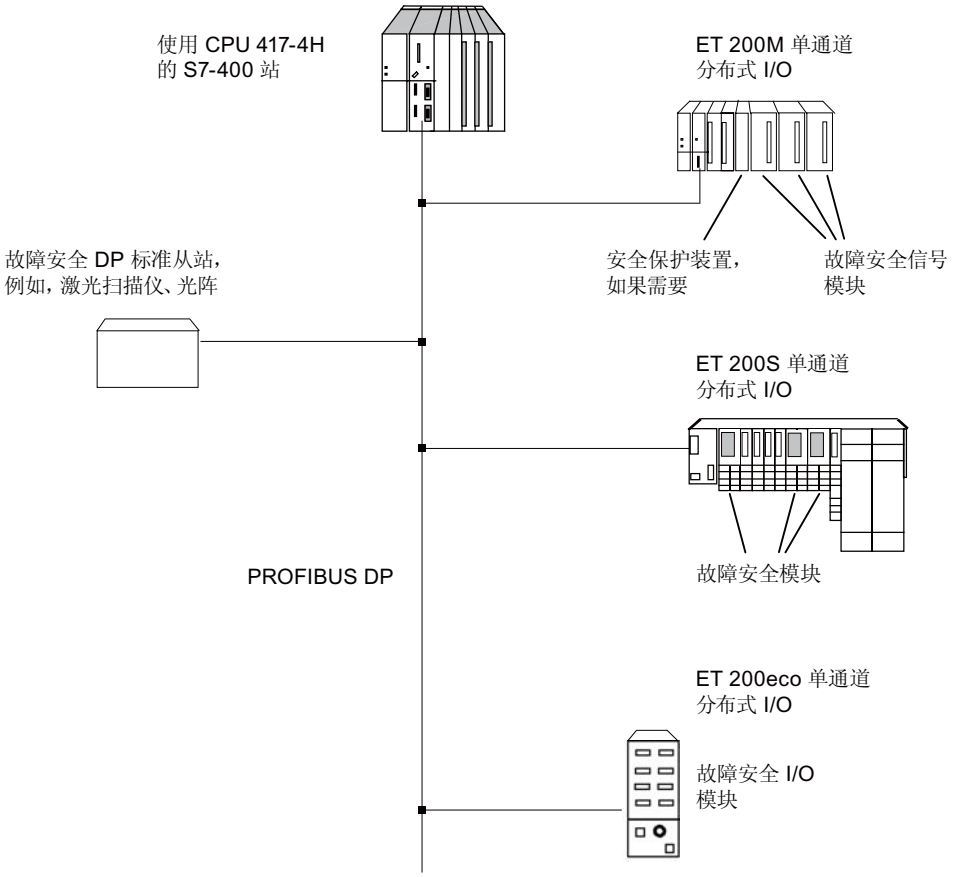


图 2-11　　使用单通道 I/O（铜质电缆）的 S7 F Systems

使用光纤电缆的 S7 F Systems 和 PROFIBUS DP

使用铜质电缆配置 PROFINET DP 时需要下列各项：

- 一个 CPU 414-4H 或 CPU 417-4H
- 一根 PROFIBUS DP 线
- 故障安全 I/O，例如：
  - 一个 ET 200M 具有：

    IM153-2 FO、F-SMs、标准 SM（如果需要）

    和安全保护装置（仅当在 ET 200M 中同时使用 F-SM 和标准 SM 时，SIL3/类别 4 应用场合需要）
  - 一个 ET 200S 具有：

    IM 151-1 HIGH FEATURE、

    故障安全模块和 ET 200S 标准模块（如果需要）
- 用于将 F-CPU 和故障安全 I/O 连接至光纤电缆的组件，例如 OLM/OBT

S7 F Systems 的组态实例：使用光纤电缆的单通道 I/O

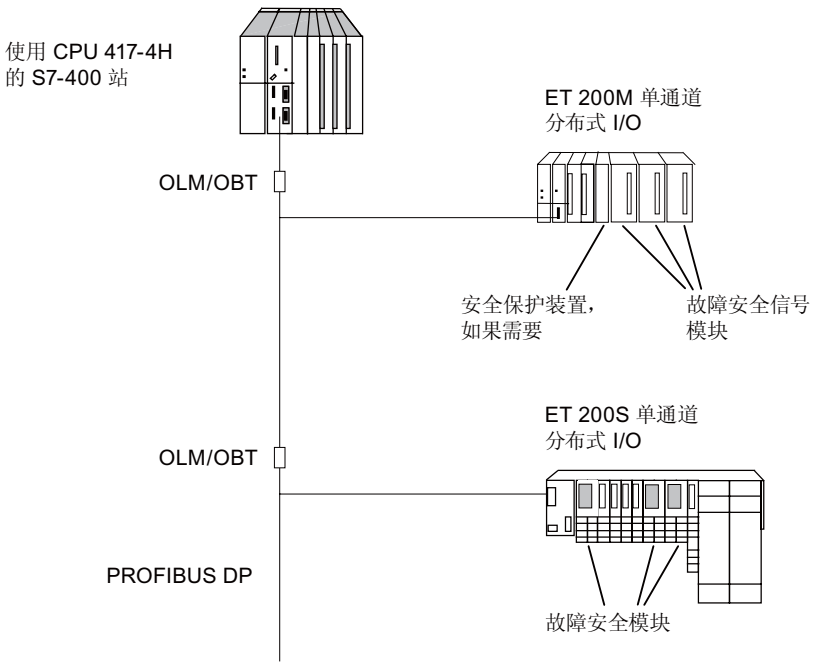


图 2-12　　使用单通道 I/O（光纤电缆）的 S7 F Systems

单通道 I/O 的可用性限制

如果出现故障，I/O 将不再可用。F-I/O 已钝化。

可能的故障原因：

- F-I/O 故障
- ET 200M 或 ET 200S 中的接口模块故障
- 整个 ET 200M、ET 200S 或 ET 200eco 故障
- PROFIBUS DP 线路故障
- F-CPU 故障

2.3.3 单通道切换式 I/O（仅 S7 FH Systems）

单通道切换式 I/O 的特性

在单通道切换式组态中，F-I/O 无冗余。F-I/O 由**两个 F-CPU** 进行寻址。

仅 S7 FH Systems 具有此组态。F-I/O 仅可用于 ET 200M 分布式 I/O 系统。

对于每根冗余 PROFIBUS DP 线路，ET 200M 均有一个 DP 从站接口，因此对两个 F-CPU 均有一个物理连接。

需要的硬件组件

根据使用铜质电缆还是光纤电缆配置 PROFIBUS DP，来确定需要的硬件组件。

F-I/O 无冗余。

使用铜质电缆的 S7 FH Systems 和 PROFIBUS DP

使用铜质电缆配置 PROFINET DP 时需要下列各项：

- 两个 CPU 414-4H 或 CPU 417-4H
- 两根 PROFIBUS DP 线路
- 一个 ET 200M 使用两个（冗余）IM153-2 模块，每个模块均有一个 PROFIBUS DP 接口
- 用于将两个 F-CPU 和两个 IM153-2 或 IM153-3 模块连接至 PROFIBUS DP 的四个总线连接器
- 无冗余的故障安全信号模块和标准信号模块（如果需要）
- 安全保护装置（仅 SIL3/类别 4 应用场合需要）

使用光纤电缆的 S7 FH Systems 和 PROFIBUS DP

以下 CPU 需要使用光纤电缆配置 PROFIBUS DP：

- 两个 CPU 414-4H 或 CPU 417-4H
- 两根 PROFIBUS DP 线路
- 一个 ET 200M 使用两个（冗余）IM153-2 FO 模块，每个模块均有一个 PROFIBUS DP 接口
- 用于将两个 F-CPU 连接至光纤电缆的两个组件，例如 OLM/OBT
- 无冗余的故障安全信号模块和标准信号模块（如果需要）
- 安全保护装置（仅当在 ET 200M 中同时使用 F-SM 和标准 SM 时，

  SIL3/类别 4 应用场合需要）

S7 FH Systems 的组态实例：单通道切换式 I/O

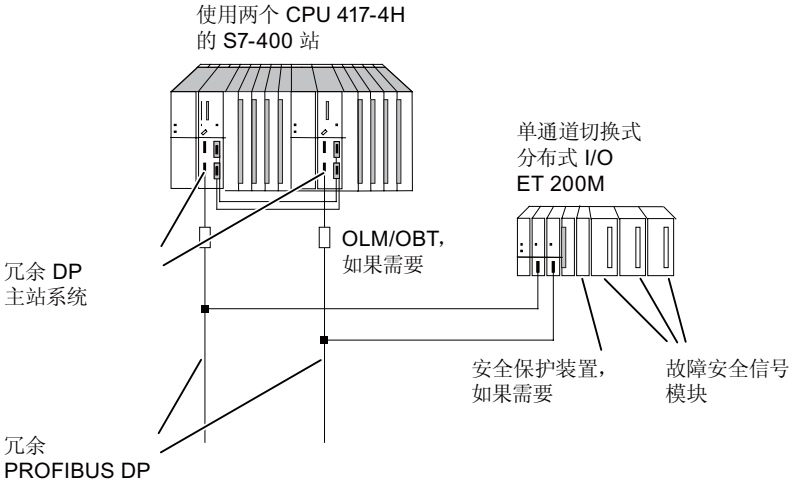


图 2-13　　使用单通道切换式 I/O 的 S7 FH Systems

单通道切换式 I/O 的可用性限制

如果出现以下情况，则过程将无法再使用切换式 I/O：

- 故障安全信号模块出现故障
  （相关的故障安全信号模块已钝化）
- 整个 ET 200M 故障

如果出现以下情况，过程仍可使用切换式 I/O：

- IM153-2/-3/-2 FO 故障
- PROFIBUS DP 线路故障
- F-CPU 故障

2.3.4 冗余切换式 I/O（仅 S7 FH Systems）

冗余切换式 I/O 的特性

由于具有冗余切换式 I/O，F-I/O 有冗余。

仅 S7 FH Systems 具有此组态。F-I/O 仅可用于 ET 200M 分布式 I/O 系统。

两个故障安全信号模块位于不同的 ET 200M 或同一个 ET 200M 中。在以下实例中，冗余信号模块插入在不同的 ET 200M 中。

需要的硬件组件

根据使用铜质电缆还是光纤电缆配置 PROFIBUS DP，来确定需要的硬件组件。

故障安全 I/O 有冗余。

使用铜质电缆的 S7 FH Systems 和 PROFIBUS DP

使用铜质电缆配置 PROFINET DP 时需要下列各项：

- 两个 CPU 414-4H 或 CPU 417-4H
- 两根 PROFIBUS DP 线路
- 两个 ET 200M：每个 ET 200M 使用两个（冗余） IM153-2 或 IM153-3 模块
- 用于将两个 F-CPU 和四个 IM153-2 或 IM 153-3 模块连接至 PROFIBUS DP 的六个总线连接器
- 冗余故障安全信号模块和标准信号模块（如果需要）
- 两个安全保护装置（仅 SIL3/类别 4 应用需求）

使用光纤电缆的 S7 FH Systems 和 PROFIBUS DP

以下 CPU 需要使用光纤电缆配置 PROFIBUS DP：

- 两个 CPU 414-4H 或 CPU 417-4H
- 两根 PROFIBUS DP 线路
- 两个 ET 200M：每个 ET 200M 使用两个 IM153-2 FO
- 用于将两个 F-CPU 连接至光纤电缆的两个组件，例如 OLM/OBT
- 冗余故障安全信号模块和标准信号模块（如果需要）
- 两个安全保护装置（仅当在一个 ET 200M 中同时使用 F-SM 和标准信号模块时，SIL3/类别 4 应用场合需要）

S7 FH Systems 的组态实例：冗余切换式 I/O

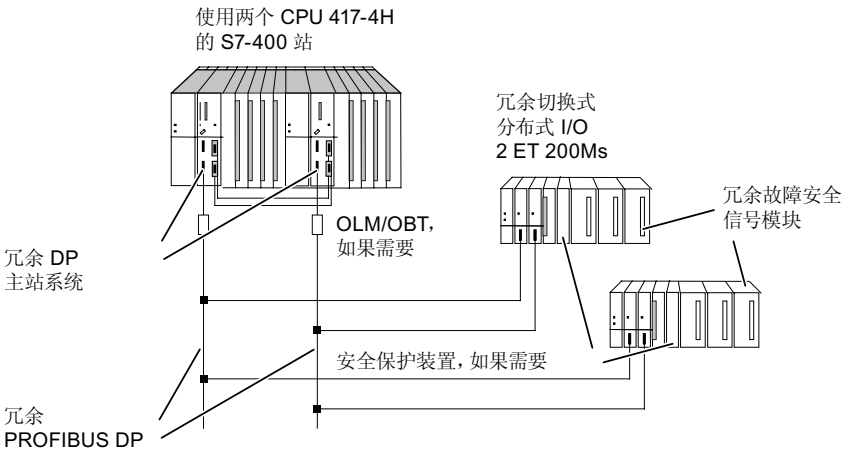


图 2-14　　使用冗余切换式 I/O 的 S7 FH Systems

冗余切换式 I/O 的可用性

如果出现以下情况，过程仍可使用 I/O：

- 故障安全冗余信号模块出现故障
- 两个 ET 200M 中的 IM153-2/-3/-2 FO 均出现故障
- 整个 ET 200M 故障（要求：冗余 F-SM 必须位于不同的 ET 200M 中）
- PROFIBUS DP 线路故障
- F-CPU 故障

2.4 S7 Distributed Safety 或 S7 F/FH Systems – 选择指南

自动化任务

每个自动化任务的正确解决方案，对于用户而言，就是获得最佳性价比。

S7 Distributed Safety 或 S7 F/FH Systems – 选择标准

下表列出了对选择至关重要的原则性 F 系统要求。

该表的最后一行指出哪个故障安全系统（S7 Distributed Safety、S7 F Systems 或 S7 FH Systems）最适合当前的自动化任务。

表格 2-2　　F 系统的选择标准

选择标准			
PROFIBUS DP 上适用的 F-I/O	• ET 200M 中的 F 信号模块 • S7-300 站中的 F 信号模块（例如，使用 CPU 315F-2 DP 的集中式组态） • ET 200S 中的 F 电子模块 • ET 200pro 中的故障安全电子模块 • ET 200eco 故障安全 I/O 模块 • 故障安全 DP 标准从站	• ET 200M 中的 F 信号模块 • ET 200S 中的 F 电子模块 • ET 200eco 故障安全 I/O 模块 • 故障安全 DP 标准从站	
PROFINET IO 上适用的 F-I/O	• ET 200S 中的 F 电子模块 • ET 200pro 中的故障安全电子模块 • 故障安全 I/O 标准设备	-	
F 系统要求的典型响应时间	100 ms 至 200 ms	200 ms 至 500 ms	
在控制系统中集成	不需要集成	需要在 PCS 7 过程控制系统中集成	
编程语言的要求	在 *STEP 7* 中必须使用标准编程语言（LAD、FBD）	必须使用 CFC 进行编程（可以在控制系统中简单集成）	
F 系统的可用性要求	F 系统的常规可用性已经足够	常规的可用性已经足够	需要增强的可用性或需要最高等级可用性
解决方案...	**S7 Distributed Safety**	**S7 F Systems**	**S7 FH Systems**

S7 Distributed Safety 和 S7 F/FH Systems 均可满足的要求

对于以下要求，F 系统在处理时没有区别。即，S7 Distributed Safety 和 S7 F/FH Systems 均可适用：

- 组态使用铜缆或光纤技术均可。

  （如果跨越距离很长或系统会受强电磁干扰，则在标准自动化系统中应使用光纤技术。）

- 可以达到安全等级 SIL2/类别 3 和 SIL3/类别 4。

F 系统的系统组态

故障安全系统的系统组态限制主要取决于使用的 F-CPU。所有可用 F-CPU 的存储器组态位于*"S7 Distributed Safety 和 S7 F/FH Systems 的性能特性"*的*"F-CPU 的存储器组态"*表中。相应 F-CPU 手册的 F-CPU 技术规范中提供了其它值。

您可以在*《自动化系统 S7-400FH 容错系统》*手册和 *S7 H Systems* 可选软件包的自述文件中找到有关 S7 FH Systems 的可能的限制信息。

参见

S7 Distributed Safety 和 S7 F/FH Systems 的性能特征 (页 25)

S7 F Systems 故障安全系统 (页 41)

通讯选项

3

3.1 引言

概述

本章介绍了 S7 Distributed Safety 和 S7 F/FH Systems 中安全相关的通讯选项，以及这两个 F 系统之间的异同。

其它信息

标准用户程序之间可以进行通讯（与标准 S7-300 和 S7-400 自动化系统之间的通讯完全相同），但本章不予介绍。您可以在 *STEP 7* 手册和每个 CPU 的硬件手册中找到相关说明。

在某种程度上，用户可以将故障安全块用于安全相关的通讯。以下参考详细介绍了 F 块及其处理方式：

- 对于 S7 Distributed Safety：*《S7 Distributed Safety 组态和编程》*手册
- 对于 S7 F/FH Systems：*《可编程控制器 S7 F/FH》*手册

3.2 安全相关的通讯概述

通讯概述

下图介绍了 F 系统 S7 Distributed Safety 或 S7 F/FH Systems 的通讯选项。

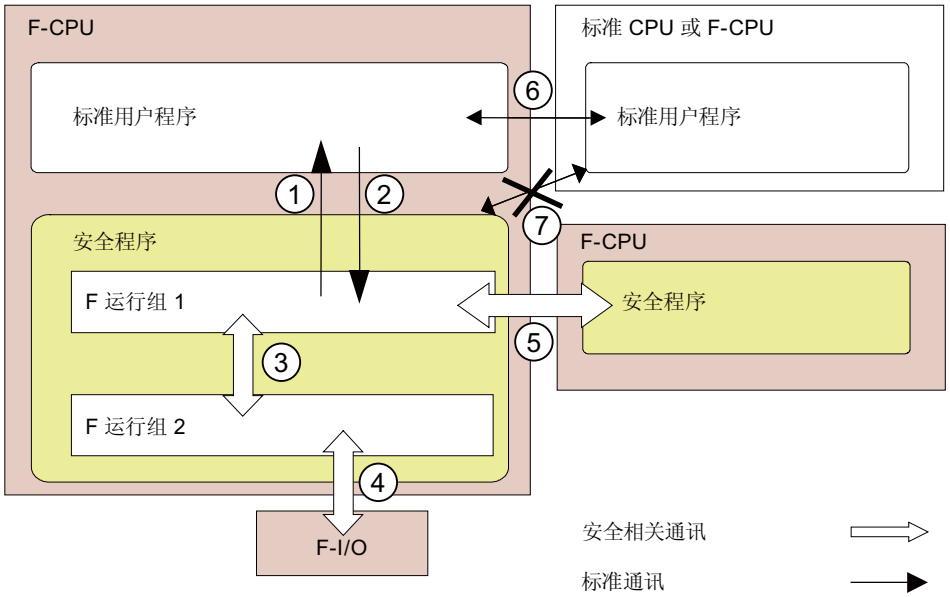


图 3-1 F 系统通讯的概述

表格 3-1 通讯选项

编号	通讯（介于...	和...之间）	安全相关	参阅章节...
1	F-CPU 中的安全程序	F-CPU 中的标准用户程序	否	“标准用户程序和安全程序之间的通讯”
2	F-CPU 中的标准用户程序	F-CPU 中的安全程序	否	“标准用户程序和安全程序之间的通讯”
3	F 运行组	F 运行组	是	“F 运行组之间的通讯”
4	F-CPU 中的安全程序	F-I/O	是	“F-CPU 和 F-I/O 之间的通讯”
5	F-CPU 中的安全程序	F-CPU 中的安全程序	是	“安全相关的 CPU 和 CPU 之间的通讯”
6	在标准 CPU 或 F-CPU 中的标准用户程序	在标准 CPU 或 F-CPU 中的标准用户程序	否	*CPU 手册*
7	F-CPU 中的安全程序	在标准 CPU 或 F-CPU 中的标准用户程序	无法通讯	-

3.3 标准用户程序和安全程序之间的通讯

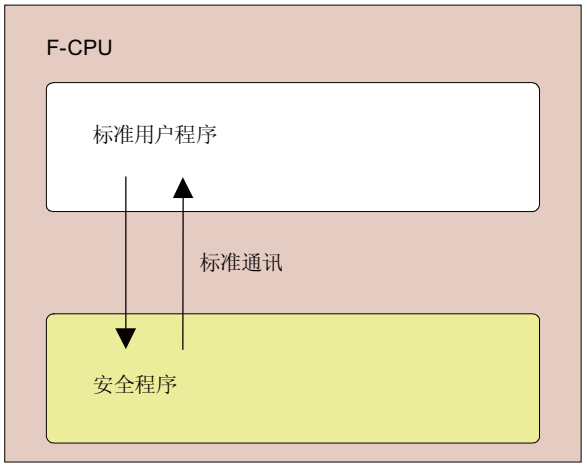


图 3-2 标准用户程序和安全程序之间的通讯

数据

在标准用户程序中，可以对安全程序中的所有数据进行求值。

在安全程序中，由于来自标准程序的数据和信号不安全，仅能处理 F-I/O 和其它安全程序（在其它 F-CPU 中）的故障安全数据或故障安全信号。除非对来自标准用户程序的数据进行似然性检查，否则无法在安全程序中处理这些数据。厂内安全专家负责确保安全并执行似然性检查。如果出现疑问，则必须由安全程序生成这些数据。

S7 Distributed Safety 和 S7 F/FH Systems 之间的区别

在 S7 Distributed Safety 中，使用位存储器或通过访问标准 I/O 的输入和输出过程映像，来交换 F-CPU 中安全程序和标准用户程序之间的数据。

此外，标准用户程序还可以访问安全程序的 F 共享 DB、F-DB 和背景数据块。

在 S7 F/FH systems 中，F-CPU 的安全程序和标准用户程序使用不同的数据格式；因此必须使用特殊的 F 块以转换这些数据格式，以便在安全程序和标准用户程序之间交换数据。

3.3.1 S7 Distributed Safety 中标准用户程序和安全程序之间的通讯

从安全程序向标准用户程序传送数据

由于安全程序中的数据以 F-DB、背景数据块、F 共享 DB 和过程映像的标准格式存在，因此标准用户程序可以直接读取安全程序中的所有数据。

还可以在安全程序中将数值写入位存储器，以使标准用户程序无需通过 F 数据块即可使用此安全程序的中间结果。但是，这些位存储器仅可由标准用户程序进行处理，本身不能在安全程序中读取。

例如，可以为了显示目的而写入标准 I/O 的过程输出映像（PIQ）。也不能在安全程序中读取这些值。

从标准用户程序向安全程序传送数据

要在安全程序中处理来自标准用户程序的数据，则可以使用过程输入映像（PII）读取来自标准用户程序的位存储器或来自标准 I/O 的信号。由于这些数据不安全，用户必须在安全程序中执行其它针对过程的似然性检查，以确保不会发生危险状况。

为了便于进行似然性检查，在打印安全程序时，将包括来自在安全程序中评估的标准用户程序的所有信号。在安全程序中高亮显示来自标准用户程序的地址。

3.3.2 S7 F/FH Systems 中的标准用户程序和安全程序之间的通讯

不同的数据格式

标准用户程序和安全程序使用不同的数据格式。在安全程序中使用安全相关的 F 数据类型。在标准用户程序中使用标准数据类型。

在 S7 F/FH Systems 的 F-CPU 中，用户可以使用特殊的转换块来交换数据。

从安全程序向标准用户程序传送数据

如果要在标准用户程序中进一步处理来自安全程序的数据（例如，监视），则必须在 CFC 的两个程序之间连接一个 F_F *数据类型_数据类型*数据转换块，以将 F 数据类型转换为标准数据类型。可以在*故障安全块* F 库中找到此块。

必须在标准用户程序（CFC、标准运行组）中调用 F_F *数据类型_数据类型*块。

从标准用户程序向安全程序传送数据

除非执行似然性检查，否则无法在安全程序中处理来自标准用户程序的数据。用户必须在安全程序中执行其它针对过程的似然性检查，以确保不会发生危险状况。

要处理来自标准用户程序的数据，必须借助 F_*数据类型*_F *数据类型*数据转换块，从标准数据类型生成安全相关的 F 数据类型。可以在*故障安全块* F 库中找到这些块。

必须在安全程序（CFC、F 运行组）中调用 F_*数据类型*_F *数据类型*数据转换块。

3.4 F 运行组之间的通信

F 运行组

S7 Distributed Safety：F 运行组是由多个相关的 F 块组成的逻辑结构。

S7 F/FH Systems：包含故障安全块的运行组称为 F 运行组。

通讯概述

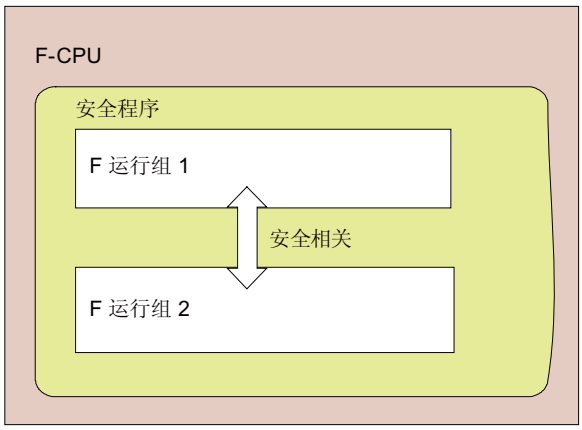


图 3-3 F 运行组之间的通讯

通讯

安全程序的 F 运行组之间的通讯是安全相关的通讯。

S7 Distributed Safety：S7 Distributed Safety 中安全程序的两个 F 运行组之间可以进行 F 运行组通讯。通过“F 运行组通讯的 DB”进行通讯。

S7 F/FH Systems：*故障安全块* F 库中的故障安全块可用于此通讯。这些故障安全块可用于发送同一 F 数据类型的固定数目的参数。

参见

S7 F/FH Systems 中安全程序的结构 (页 134)

3.5 F-CPU 和 F-I/O 之间的通讯

引言

F-CPU 和 F-I/O 之间可以进行安全相关的通讯和标准通讯（取决于使用的 F-I/O）。本节介绍了这两种通讯类型。

3.5.1 安全相关的通讯

通讯概述

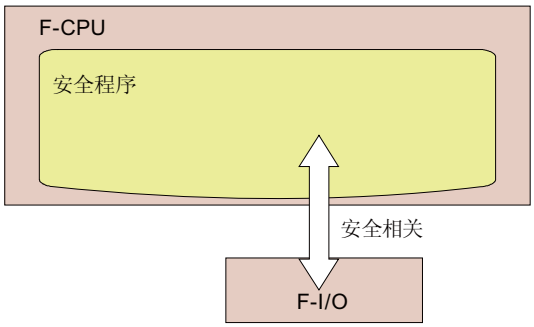


图 3-4 F-CPU 和 F-I/O 之间的安全相关的通讯

S7 Distributed Safety 和 S7 F/FH Systems 之间的 F-I/O 连接的区别

两个 F 系统中的 F-I/O 连接在安全程序集成和关联用户操作上有所不同：

在 S7 Distributed Safety 中，通过过程映像（PII 和 PIQ）进行安全相关的通讯（与标准自动化系统中的通讯相同）。无法直接访问 I/O。

在 F 程序块执行之前，F 运行组开始时更新过程输入映像。在 F 程序块执行之后，F 运行组结束时更新过程输出映像。

使用符合 PROFIsafe 的特殊安全协议，在后台进行 F-CPU（过程映像）和 F-I/O 之间用于更新过程映像的实际通讯。

在 S7 F/FH Systems 中，通过 F 驱动程序块的输入和输出进行安全相关的通讯。用户必须在 F 运行组的 CFC 图表中定位和互连特殊的 F 驱动程序块。

用户可以在**两个 F 系统**中使用**用于 F-I/O 通讯的变量**。其区别在于获得变量的方式。在 S7 Distributed Safety 中，以 F-I/O DB 形式提供变量，而在 S7 F/FH systems 中，则以 F 驱动程序块的输入和输出形式提供变量。

参见

S7 Distributed Safety 中安全程序的结构 (页 130)

3.5.2 在 S7 Distributed Safety 中访问 F-I/O

引言

大多数情况下，将在 S7 Distributed Safety 的后台访问 F-I/O。

用户需要执行的操作步骤

下表介绍了访问 F-I/O 所需的用户动作以及这些动作对 F 系统的影响。

表格 3-2 在 S7 Distributed Safety 中访问 F-I/O

步骤	所需动作	对 F-I/O 连接的影响
1.	在 *HW Config* 中为 F-I/O 组态和分配参数	F-I/O 连接所必需
2.	在 *HW Config* 中保存和编译组态	• *S7 Distributed Safety* 为每个 F-I/O 都生成一个 F-I/O 数据块。 • *S7 Distributed Safety* 在符号表中为每个 F-I/O 数据块生成一个符号。（在安全程序中，用户必须具有对某些变量的符号访问权限，以在 F-I/O DB 中进行 F-I/O 通讯。）
3.	创建 F-CALL（安全程序的调用块）	*S7 Distributed Safety* 在 F-CALL 中提供了 F-I/O 至安全程序的连接。用户无法编辑 F-CALL 块。
4	创建能够访问过程映像的安全程序	*参阅以下部分*
5.	在 *SIMATIC Manager* 中调用“Edit Safety Program”（编辑安全程序）对话框并定义 F 运行组。	该对话框显示了安全程序的所有 F 块，包括 F-I/O 的 F-I/O 数据块。
6.	编译安全程序	检查安全程序与所有有效 F 块的一致性。
7.	将安全程序下载至 F-CPU	将安全程序下载至 F-CPU（包括 F-I/O 数据块）。

F-I/O 的过程数据

可以在 F-CPU 的过程映像（PII 和 PIQ）中找到来自/到 F-I/O 的过程数据。

用户使用 F-I/O 的起始地址访问过程映像（PII、PIQ）中的 F-I/O。起始地址将自动输入到 *HW Config*（输入/输出地址）的组态表中，并且可以更改。

用于 F-I/O 通讯的变量

某些变量**必须**由用户在 F-I/O DB 中的安全程序中进行初始化：

- 用于确认通讯错误和 F-I/O 的变量或 F-I/O 重新集成的通道故障

另外，某些变量**可以**在 F-I/O 数据块中进行初始化和评估：

- 评估输出值表示过程数据还是故障安全值
- 设置过程数据的自动重新集成或手动重新集成
- 其它 F-I/O 或通道的钝化，例如，关联 F-I/O 的组关闭
- 显示 F-I/O 的重新集成是否需要确认
- 显示服务信息（故障类型）

其它信息

有关 F-I/O DB 变量以及如何初始化和评估这些变量的详细说明，请参考*《S7 Distributed Safety 组态和编程》*手册。

参见

S7 Distributed Safety 中安全程序的结构 (页 130)

3.5.3 S7 Distributed Safety 安全相关的 I 从站-I 从站通讯

引言

在 S7 Distributed Safety 中，I 从站的 F-CPU 安全程序和从站的 F-I/O 之间的安全相关的 I 从站-从站通讯采用直接数据交换的方式执行 — 因为它属于标准程序。过程输入映像用于访问 I 从站的 F-CPU 安全程序中的 F-I/O 通道（PII 和 PIO）。

限制

注意

在 *S7 Distributed Safety* V5.4 中，可以使用支持 I 从站-从站通讯的从站（例如，具有 IM 151-1 的 ET 200S HIGH FEATURE 模块，订货号为 6ES7 151-1BA01-0AB0 以及更高）的 F-I/O 进行安全相关的 I 从站-从站通讯。*S7 Distributed Safety* 的任何 F-CPU 均可用作 I 从站中的 F-CPU。

通讯概述

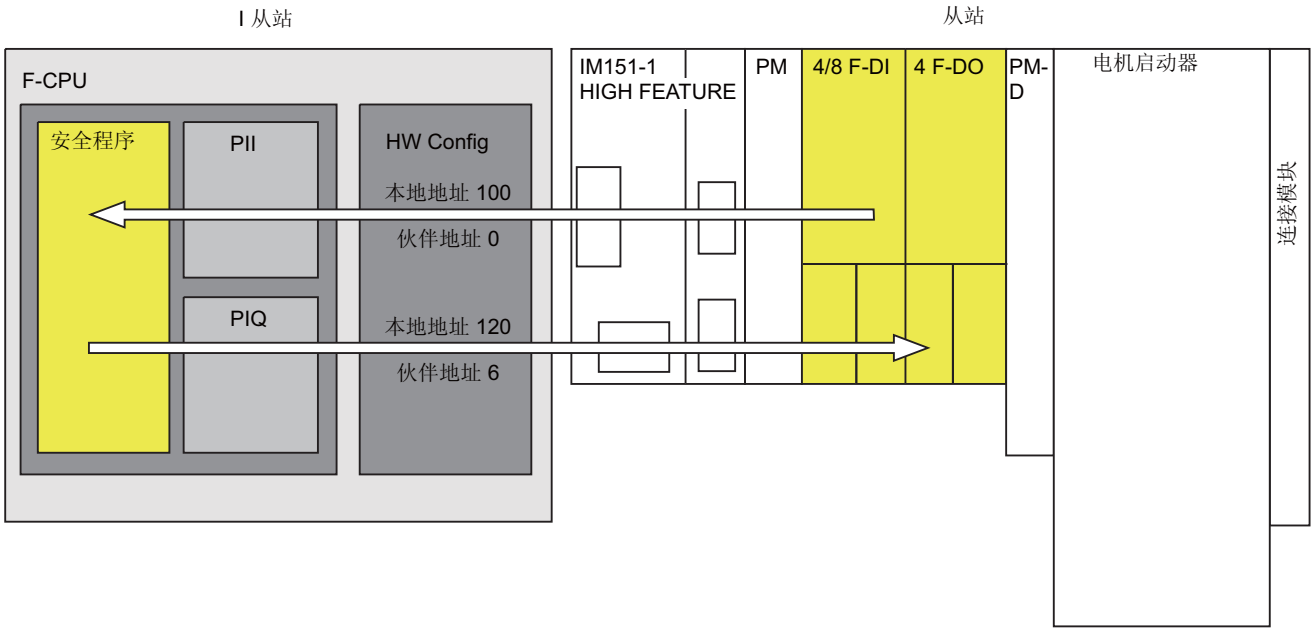


图 3-5 S7 Distributed Safety：安全相关的 I 从站-从站通讯

I 从站-从站通讯

在安全相关的 I 从站-从站通讯中，使用过程映像（PII 和 PIO）访问 F-I/O（与访问标准 I/O 相同）。无法直接访问 I/O。仅可以通过一个 F 运行时组访问 F-I/O 的通道。

用户需要执行的操作步骤

用户执行以下步骤以进行安全相关的 I 从站-从站通讯：

1. 在 *HW Config* 中组态 I 从站和从站。
2. 在 *HW Config* 中组态 DP 主站系统。
3. 将 I 从站连接至从站。
4. 在 I 从站的“Object Properties”（对象属性）对话框中设置用于 *HW Config* 中数据交换的地址区域。
5. 创建安全程序之后，将其生成并下载至 I 从站的 F-CPU。

更多信息

有关组态安全相关的 I 从站-从站通讯的详细信息，请参考*《S7 Distributed Safety 组态和编程》*手册。

3.5.4 在 S7 F/FH Systems 中访问 F-I/O

通过 F 驱动程序块访问

在 S7 F/FH Systems 中，通过 F 驱动程序块（某些情况下，必须由用户进行定位和互连）访问 F-I/O。

要求每个 F-I/O 使用一个 F 模块驱动程序，并且每个 F-I/O 输入和输出通道使用一个 F 通道驱动程序。

F 模块驱动程序

F 模块驱动程序接管安全程序和 F-I/O 之间的 PROFIsafe 通讯。在安全程序中自动对其进行定位和互连。

F 通道驱动程序

F 通道驱动程序提供了安全数据格式的过程数据。用户必须在安全程序中对其进行定位和互连。

用户需要执行的操作步骤

用户必须执行以下步骤以连接 F-I/O：

1. 从*故障安全块* F 库中选择适当的 F 通道驱动程序，并在安全程序中对其进行定位。
2. 对 F 通道驱动程序进行互连。
3. 创建安全程序之后，将其编译并下载至 F-CPU。

F-I/O 的过程数据

可以如下所示找到过程数据：

- 来自 F-I/O（输入通道）的过程数据，作为关联 F 通道驱动程序的输出。
- 来自 F-I/O（输出通道）的过程数据，作为关联 F 通道驱动程序的输入。

用于 F-I/O 通讯的变量

某些变量**必须**由用户在 F 通道驱动程序中进行初始化：

- 用于确认通讯和 F-I/O 故障或 F-I/O 重新集成的通道故障的变量

另外，某些变量**可以**由用户在 F 通道驱动程序中进行初始化和评估：

- 评估输出值表示过程数据还是故障安全值
- 设置过程数据的自动重新集成或手动重新集成
- 其它 F-I/O 或通道的钝化，例如，关联 F-I/O 的组关闭
- 显示 F-I/O 的重新集成是否需要确认
- 显示服务信息（故障类型）

其它信息

有关变量以及如何初始化和评估这些变量的详细说明，请参考*《可编程控制器 S7 F/FH》*手册。

3.5.5 标准通讯

通讯概述

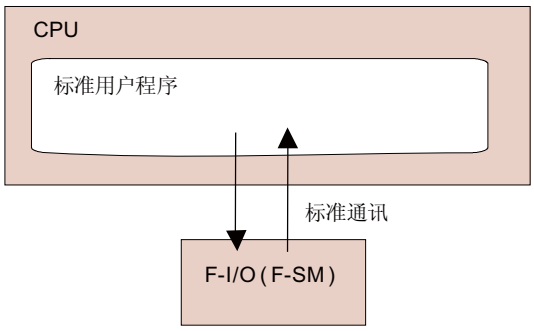


图 3-6 CPU 和 F-I/O 之间的标准通讯

标准通讯（标准模式）

F-I/O 也可用于标准应用场合的标准模式下。例如，F-I/O 提供的诊断功能在标准应用程序中相关或者灵活性具有优先权（在标准系统和故障安全系统中都可以使用 F-I/O）时，这很有用。

是否选择标准模式取决于使用的 F-I/O 的类型。在标准模式中只能使用 S7-300 故障安全信号模块（例外：SM 326; DO 8 × 24 VDC/2 A）。ET 200S、ET 200pro 和 ET 200eco 故障安全模块仅在安全模式中运行，而从不在标准模式中运行。

标准模式中的机制

CPU 和 S7-300 故障安全信号模块之间的标准操作机制可以使用标准自动化系统中普遍使用的机制。这些机制包括：

- 直接访问
- 通过过程映像访问
- 在 CFC 中，通过 *PCS 7 驱动程序*库的通道驱动程序访问（仅 F/FH Systems）
- 读出诊断数据记录

采用与标准模式中相同的方式读出诊断数据

来自故障安全模块 ET 200S 和 ET 200pro 以及 ET 200eco 故障安全 I/O 模块的诊断信息与安全性无关。使用诊断数据记录传送器，采用与标准模式中相同的方式将该信息传送到 F-CPU 并将其非循环输入到 F-CPU 和 F-SM 的诊断缓冲区中。

STEP 7 用户可以如下读出诊断数据：

- 从 F-CPU 和 F-SM 的诊断缓冲区中
- 作为 ET 200S、ET 200pro 和 ET 200eco 故障安全模块的从站诊断
- 在使用 SFC 59 的标准用户程序中（仅 F-SM）

读出 F-SM 安全模式中的诊断数据

当 F-SM 在安全模式中运行时，也可以使用 SFC 59 将 F-SM 的诊断数据记录读出到标准的用户程序中。

因此，其它特殊模块诊断块可用于 S7 F/FH Systems。例如，这些块自动生成到 WinCC 的消息，并主要与 PCS 7 配合使用（请参阅 *《可编程控制器 S7 F/FH》* 手册）。

3.6 安全相关的 CPU-CPU 通讯

引言

S7 Distributed Safety 和 S7 F/FH Systems 均允许在不同 F-CPU 中的安全程序之间进行安全相关的通讯。但是，两者的通讯机制有所不同：

表格 3-3 F-CPU 之间的通讯概述

F 系统	通过 ... 进行通讯	... 之间的通讯
S7 Distributed Safety	PROFIBUS DP	DP 主站/DP 主站
	PROFIBUS DP	DP 主站/I 从站
	PROFIBUS DP	I 从站/I 从站
	PROFINET IO	I/O 控制器/I/O 设备
	工业以太网（已组态的 S7 连接）	不相关
S7 F/FH Systems	通过 PROFIBUS、MPI、工业以太网等： 已组态的标准或容错 S7 连接	不相关

3.6.1 S7 Distributed Safety：安全相关的主站-主站通讯

DP/DP 耦合器

在 S7 Distributed Safety 中，必须使用一个 DP/DP 耦合器（订货号 6ES7 158-0AD01-0XA0） 完成不同 F-CPU（DP 主站）中安全程序之间的安全相关的通讯。

每个 F-CPU 均通过其 PROFIBUS DP 接口连接到 DP/DP 耦合器。

通讯概述

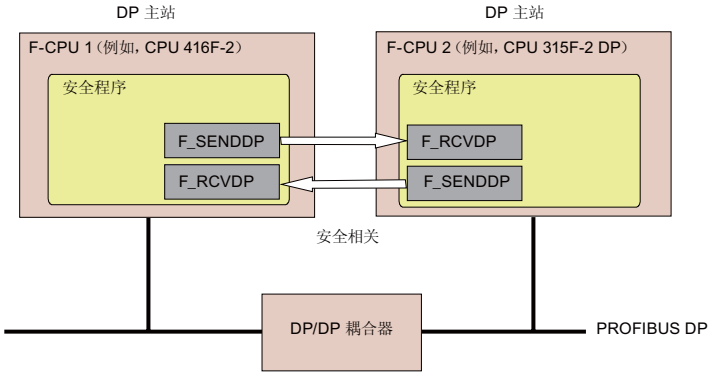


图 3-7 S7 Distributed Safety：安全相关的主站-主站通讯

主站-主站通讯

使用两个故障安全应用程序块进行安全相关的通讯：F_SENDDP 块用于发送数据，而 F_RCVDP 块用于接收数据。这些块由用户从 F-CPU 各自的安全程序中调用。它们可用于以故障安全方式传送数据类型为 BOOL 和 INT 的固定数量的故障安全数据。

用户需要执行的操作步骤

用户执行以下步骤以进行安全相关的主站-主站通讯：

1. 安装带有 DP/DP 耦合器的硬件
2. 在 *HW Config* 中组态 DP/DP 耦合器
3. 分别从各自 F-CPU 的安全程序中的 *Distributed Safety* F 库中调用 F_SENDDP 和 F_RCVDP
4. 为 F_SENDDP 和 F_RCVDP 分配参数
5. 创建安全程序之后，将其编译并下载至适当的 F-CPU

其它信息

有关 DP/DP 耦合器的信息，请参考 DP/DP 耦合器文档和《*SIMATIC NET*、*PROFIBUS 网络*》手册。有关对安全相关的主站-主站通讯进行组态和编程的详细信息，

请参考《*S7 Distributed Safety 组态和编程*》手册。

参见

S7 Distributed Safety 中安全程序的结构 (页 130)

3.6.2 S7 Distributed Safety：安全相关的主站-I 从站通讯

引言

在 S7 Distributed Safety 中，通过主站-从站连接进行 DP 主站 F-CPU 的安全程序和一个或多个 I 从站 F-CPU 的安全程序之间的与安全相关的 CPU-CPU 通讯，与在标准系统中一样。

通讯概述

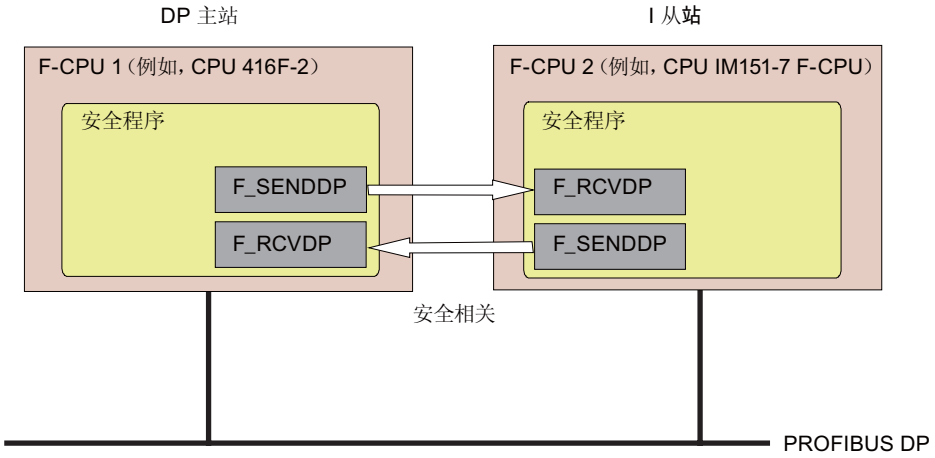


图 3-8 S7 Distributed Safety：安全相关的主站-I 从站通讯

主站-I 从站通讯

安全相关的通讯在两个故障安全应用程序块的辅助下进行：F_SENDDP 块用于发送数据，而 F_RCVDP 块用于接收数据。这些块由用户从 F-CPU 各自的安全程序中调用。它们可用于以故障安全方式传送数据类型为 BOOL 和 INT 的固定数量的故障安全数据。

用户需要执行的操作步骤

用户应执行以下步骤以进行安全相关的主站-I 从站通讯：

1. 在 *HW Config* 中组态 I 从站
2. 在 *HW Config* 中组态 DP 主站系统
3. 将 I 从站连接至 DP 主站
4. 在 *HW Config* 中设置数据交换的地址区域
5. 从 DP 主站和 I 从站 F-CPU 的安全程序中调用 *Distributed Safety* F 库中的 F_SENDDP 和 F_RCVDP
6. 为 F_SENDDP 和 F_RCVDP 分配参数
7. 创建安全程序之后，将其编译并下载至适当的 F-CPU。

其它信息

有关对安全相关的主站-I 从站通讯进行组态和编程的详细信息，请参考*《S7 Distributed Safety 组态和编程》*手册。

参见

对 F-I/O 进行组态 (页 124)

3.6.3 S7 Distributed Safety：安全相关的 I 从站-I 从站通讯

引言

在 S7 Distributed Safety 中，通过数据交换以标准模式进行 I 从站 F-CPU 的安全程序之间的安全相关的 CPU-CPU 通讯。

通讯概述

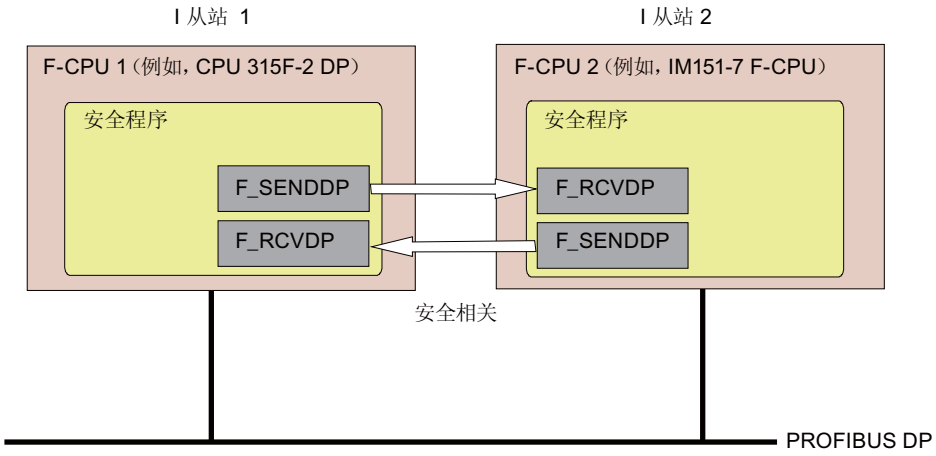


图 3-9 S7 Distributed Safety：安全相关的 I 从站-I 从站通讯

I 从站-I 从站通讯

安全相关的通讯在两个故障安全应用程序块的辅助下进行：F_SENDDP 块用于发送数据，而 F_RCVDP 块用于接收数据。这些块由用户从 F-CPU 各自的安全程序中调用。它们可用于以故障安全方式传送数据类型为 BOOL 和 INT 的固定数量的故障安全数据。

用户需要执行的操作步骤

用户执行以下步骤，进行安全相关的 I 从站-I 从站通讯：

1. 在 *HW Config* 中组态 I 从站
2. 在 *HW Config* 中组态 DP 主站系统
3. 将 I 从站连接至 DP 主站
4. 在 *HW Config* 中设置数据交换的地址区域
5. 从相关的 I 从站 F-CPU 的安全程序中的 *Distributed Safety* F 库中调用 F_SENDDP 和 F_RCVDP
6. 为 F_SENDDP 和 F_RCVDP 分配参数
7. 创建安全程序之后，将其编译并下载至适当的 F-CPU

其它信息

有关对安全相关的 I 从站-I 从站通讯进行组态和编程的详细信息，请参考《*S7 Distributed Safety 组态和编程*》手册。

参见

对 F-I/O 进行组态 (页 124)

3.6.4 S7 Distributed Safety：通过 S7 连接进行安全相关的通讯

引言

在 **S7 Distributed Safety** 中，通过已组态的 S7 连接在两个 F-CPU 的安全程序之间通过 S7 连接进行安全相关的 CPU-CPU 通讯，与在标准模式中一样。

禁止通过公共网络进行安全相关的 CPU-CPU 通讯。

通讯概述

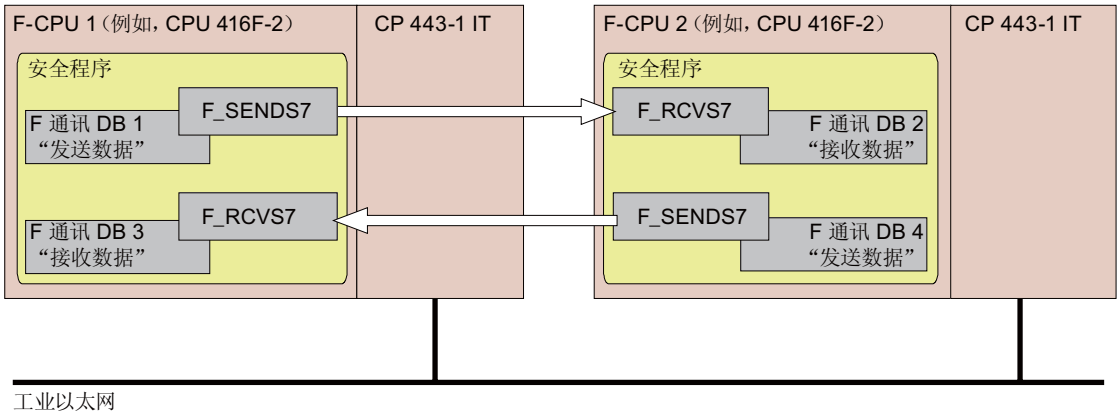


图 3-10 S7 Distributed Safety：F-CPU 之间的通讯

通过 S7 连接进行通讯

安全相关的通讯在两个故障安全应用程序块的辅助下进行：F_SENDS7 块用于发送数据，而 F_RCVS7 块用于接收数据。这些块由用户从 F-CPU 各自的安全程序中调用。使用这些故障安全应用程序块，可以按用户定义的数量以故障安全方式传送数据类型为 BOOL、INT、WORD 或 TIME 的故障安全数据。这些故障安全数据在发送端和接收端添加到 F-DB（“F 通讯 DB”）。

用户需要执行的操作步骤

用户执行以下步骤以通过 S7 连接进行安全相关的通讯：

1. 在 *STEP 7 NetPro* 中，为各个 F-CPU 组态 S7 连接。
2. 创建一个 F 通讯 DB，用于发送和接收数据。
3. 初始化 F 通讯 DB 的变量以发送变量。
4. 在要发送数据的安全程序中调用 F_SENDS7。
5. 在要接收数据的安全程序中调用 F_RCVS7。
6. 为 F_SENDS7 和 F_RCVS7 分配参数。
7. 创建安全程序之后，将其编译并下载至适当的 F-CPU。

S7 Distributed Safety 的限制

注意

在 Distributed Safety 中，通常仅允许通过工业以太网的 S7 连接！

可以在以下 CPU 中/从以下 CPU 中通过 S7 连接进行安全相关的通讯：

- CPU 315F-2 PN/DP（仅通过 CPU 的 PN 接口）
- CPU 317F-2 PN/DP（仅通过 CPU 的 PN 接口）
- CPU 416F-2 **从固件版本 V4.0 起**

其它信息

您可以在 *STEP 7 在线帮助*中找到有关组态 S7 连接的信息。

有关使用 S7 连接对安全相关的通讯进行组态和编程的详细信息，请参考《*S7 Distributed Safety 组态和编程*》手册。

3.6.5 S7 F/FH Systems：通过 S7 连接进行安全相关的通讯

引言

在 **S7 F/FH Systems** 中，通过已组态的 S7 连接或已组态的容错 S7 连接进行两个 F-CPU 的安全程序之间的安全相关的 CPU-CPU 通讯（经由 S7 连接），与在标准模式中一样。

禁止通过公共网络进行安全相关的 CPU-CPU 通讯。

通讯概述

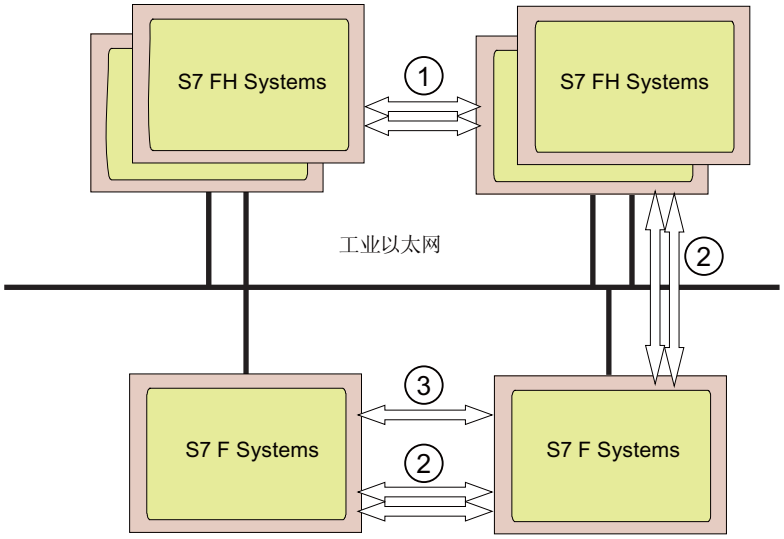


图 3-11 S7 F/FH Systems：F-CPU 之间的通讯

表格 3-4 安全相关的 CPU-CPU 通讯

编号	通讯，从...	至...	连接类型	安全相关的
1	S7 FH Systems	S7 FH Systems	S7 连接，容错	是
2	S7 F/FH Systems	S7 F Systems	S7 连接，容错	是
3	S7 F Systems	S7 F Systems	S7 连接	是

通过 S7 连接进行通讯

在故障安全应用程序块的辅助下进行安全相关的通讯：F_SENDBO 和 F_SENDR 块用于发送数据，而 F_RCVBO 和 F_RCVR 块用于接收数据。这些块由用户从 F-CPU 相关的安全程序中调用。使用这些故障安全应用程序块，可以按用户定义的数量以故障安全方式传送数据类型为 BOOL 和 REAL 的故障安全数据。

用户需要执行的操作步骤

用户按照以下步骤进行操作，通过 S7 连接进行安全相关的通讯：

1. 在 *STEP 7* 中为各个 F-CPU 组态 S7 连接。
2. 在各自 F-CPU 的安全程序中，从*故障安全块* F 库中选择用于 CPU-CPU 通讯的故障安全块，然后进行互连并为其分配参数。
3. 创建安全程序之后，将其编译并下载至适当的 F-CPU。

其它信息

您可以在 *STEP 7 在线帮助*中找到有关组态可能的连接类型的信息。

有关使用 S7 连接对安全相关的通讯进行组态和编程的详细信息，请参考*《可编程控制器 S7 F/FH》*手册。

参见

S7 F/FH Systems 中安全程序的结构 (页 134)

F 系统中的安全

4

4.1 引言

概述

S7 Distributed Safety 和 S7 F/FH Systems F 系统中的安全机制在本质上是相同的。本章介绍了用户可见的安全机制，包括：

- 安全模式
- 故障响应
- 重新启动 F 系统
- F 系统的密码保护

特别介绍了 S7 Distributed Safety 和 S7 F/FH Systems 之间的区别。

“标准和认证”介绍了 S7 Distributed Safety 和 S7 F/FH Systems 需要满足的标准、认证和安全要求的概述。

其它信息

S7 Distributed Safety 和 S7 F/FH Systems 的组态和编程手册介绍了使用安全机制的信息，并提供了更多详细信息（在用到的地方）。

在 *STEP 7* 手册和硬件手册中介绍了其标准特性，所以本手册并不涉及。

F 系统中的安全

警告

S7 Distributed Safety 和 S7 F/FH Systems F 系统用于控制关闭时可以立即实现安全状态的过程。

S7 Distributed Safety 和 S7 F/FH Systems 只能用于控制那些立即关闭不会引起人身伤害或环境危险的过程。

通过以下方式确保 F 系统中的安全：

- 用于故障检测和故障响应的集成安全功能
- F 系统访问保护

安全功能

用于故障检测和故障响应的集成安全功能主要包含在安全程序和 F-I/O 中。这些功能由合适的故障安全块执行并由 F-CPU 的硬件和操作系统支持。

访问保护

通过为 F-CPU 和安全程序分配密码以对 F 系统访问提供保护。以下手册对访问保护进行了更加详细的说明：

- 对于 S7 Distributed Safety：*《S7 Distributed Safety 组态和编程》*手册
- 对于 S7 F/FH Systems：*《可编程控制器 S7 F/FH》*手册

警告

要阻止未经授权的 F 系统硬件修改，必须采取适当的措施，例如：

- 在锁定的开关柜中安装系统
- 使用粘贴标签保护 F-CPU 的微存储卡或闪存卡

参见

标准和认证 (页 98)

安全要求 (页 102)

4.2 安全模式

安全模式

在安全模式中，在下列部分中激活用于故障检测和故障响应的安全功能：

- 故障安全 I/O
- F-CPU 的安全程序

F-I/O 的安全模式

对于 **S7-300 故障安全信号模块**，*HW Config* 中设置的“Safety mode”（安全模式）参数确定该模块在标准模式（用作 S7-300 标准信号模块，SM 326; DO 8 × 24 VDC/2 A 除外）中运行还是在安全模式中运行。

ET 200S、ET 200pro 和 ET 200eco 故障安全模块仅可在安全模式中使用。

安全程序的安全模式

安全程序在 F-CPU 的安全模式运行这表示故障检测和故障响应的所有安全机制均已激活。安全程序在安全模式中运行期间，无法进行修改。

可以间断性地取消激活和重新激活 F-CPU 中安全程序的安全模式。在所谓“取消激活的安全模式”下，用户可在 F-CPU 处于 RUN 模式时根据需要对安全程序进行在线测试和更改。

对于 S7 Distributed Safety，您仅可以在运行模式由 RUN 切换到 STOP 再切换到 RUN 之后，才能切换回安全模式。

对于 S7 F/FH Systems，无需更改运行模式即可返回安全模式。

安全消息帧

在安全模式中，数据作为安全消息帧在 F-CPU 和 F-I/O 之间进行一致性传输。符合 PROFIsaf 的安全消息帧由以下部分组成：

- 过程数据（用户数据）
- 状态字节/控制字节（安全模式的协调数据）
- 顺序号
- CRC 签名

安全相关的 CPU-CPU 通讯也使用类似于 PROFIsafe 的安全消息帧进行。还用到了下列有关监视时间、顺序号和 CRC 签名的信息。

监视时间和顺序号

F-CPU 为 F-I/O 分配一个顺序号，用于在 PROFIsafe 协议中更新消息框架的时间监视。

F-CPU 和 F-I/O 必须在可分配的监视时间内接收具有有效顺序号且有效的当前安全消息帧。

如果在监视时间内未检测到有效的顺序号，F-I/O 将处于钝化状态。

CRC（循环冗余校验）签名

安全消息帧中的 CRC 签名保护安全消息帧中过程数据的有效性、分配的地址参考的准确性和安全相关的参数。

如果在 F-CPU 和 F-I/O 之间的通讯期间 CRC 签名发生错误（例如由于间歇式电磁干扰），则 F-I/O 处于钝化状态。

参见

引言 (页 79)

故障响应 (页 93)

对监视时间进行组态 (页 138)

4.3 故障响应

安全状态

安全概念基于的基本原理是：对于所有过程变量，均存在一个安全状态。例如，对于数字量 F-I/O，该值为“0”。该原理适用于传感器和执行器。

F-CPU 和操作系统中的故障响应

F-CPU 和操作系统对 S7 Distributed Safety 和 S7 F/FH Systems 中的故障进行响应（以在标准 S7-300 和 S7-400 系统中一样的方式）。另外，在 F 系统的安全程序中触发故障响应。

安全程序中的故障响应

安全程序中的所有故障响应都会导致过程变量跳转到安全状态。特殊情况下，故障响应为：

- **S7 Distributed Safety**：F-CPU 转至 STOP 模式。

  仅可以通过重新启动 F 系统来跳过该状态。

- **S7 F/FH Systems**：完全关闭安全程序，或者使用 F_SHUTDN F 块关闭故障 F 运行组。F-CPU 不跳转到 STOP 模式。关闭不会影响标准用户程序。

  故障消除之后，必须重新启动安全程序或 F 运行时组。用户在 F_SHUTDN 块中确认之后执行重新启动。

- F-I/O 的 F-I/O/通道的钝化。

  I/O 故障或通讯错误导致受影响的 F-I/O 或 F-I/O 通道的钝化；F-CPU 不跳转到 STOP 模式。

  故障消除之后，必须重新集成 F-I/O 或 F-I/O 的通道（消除钝化）。将自动进行重新集成（从故障安全值切换为过程数据），或者由用户强制确认后再进行重新集成。

还可以响应检测到的故障来执行标准诊断和消息功能。

在 S7 FH Systems 中，当主站切换到 STOP 模式时，将触发主站保留切换。

F-I/O 中的故障响应

如果 F-I/O 检测到故障，它会将相关通道或所有通道切换到安全状态。即，该 F-I/O 的通道处于钝化状态。F-I/O 将检测到的故障以信号形式发送至 F-CPU。另外，故障将通过安全消息帧以信号形式发送至 F-CPU 中的安全程序。故障消除之后，必须重新集成 F-I/O（消除钝化）（参阅“安全程序中的故障响应”）。

参见

标准通讯 (页 77)

重新启动 F 系统 (页 95)

4.4 重新启动 F 系统

F 系统运行模式

S7 Distributed Safety 和 S7 F/FH Systems 的运行模式与标准系统的运行模式的不同之处仅在于重新启动特性以及 HOLD 模式中的行为。

重新启动特性

当 F-CPU 从 STOP 模式切换到 RUN 模式时，标准用户程序以正常方式重新启动。当安全程序重新启动时，将使用装载存储器的值初始化以下数据块：

- 对于 S7 Distributed Safety：所有具有 F 属性的数据块
- 对于 S7 F/FH Systems：所有数据块

该操作类似于冷启动。这会导致保存的错误信息丢失。

F 系统自动重新集成 F-I/O。与标准用户程序相比，无法在安全程序中使用重启动 OB（OB 100 至 OB 102）。

重新启动保护

数据处理错误或内部故障也可以使用装载存储器的值来触发安全程序重新启动。如果您的过程不允许此类启动，则必须在安全程序中编写一个重新启动/启动保护程序：必须阻止过程数据输出，直到手动启用为止。只有在安全且已更正故障时，才能释放过程数据输出块。

HOLD 模式

S7 Distributed Safety 和 S7 F/FH Systems 不支持 HOLD 模式。如果 HOLD 请求停止了用户程序的执行，则仅可以通过重新启动（冷启动或暖启动）来跳过该状态。

4.5 F 系统的密码保护

两个密码

除了 F-CPU 或 CPU 的标准密码，F 系统还要求一个安全程序密码。

F-CPU 的密码防止将 F 系统从工程系统（ES）或编程设备（PG）未经授权下载至 F-CPU。

安全程序的密码防止对 F-CPU 和 F-I/O 设置的组态和参数进行未经授权的更改。

分配密码

用户为 F-CPU 分配参数时，在 *HW Config* 中的“Protection”（保护）选项卡中为 F-CPU 分配密码。

用户在对安全程序进行组态和编程时，为安全程序分配密码。因此，第一次编译安全程序时，将自动显示一个对话框。

4.6 系统的验收测试

谁执行验收测试？

一般而言，由独立的专家执行验收测试。

准备验收测试时的支持

当系统进行验收测试时，必须检查是否满足特定应用程序相关的所有标准。

以下特殊的 *STEP 7* 功能在 *SIMATIC Manager* 中可用，可以帮助用户检查 F 系统是否正常使用：

- 比较安全程序
- 打印安全程序

所有与 F 系统的验收测试相关的数据均可以在 *SIMATIC Manager* 中访问，并可根据需要打印。

用户动作

用户为准备验收测试的系统采取的动作取决于使用的 F 系统。因此，在 S7 Distributed Safety 和 S7 F/FH Systems 的相关组态和编程手册中的“系统验收测试”下说明了这些步骤。

4.7 标准和认证

安全证明

S7 Distributed Safety 和 S7 F/FH Systems 故障安全组件的安全证明（TUEV 证明），以及证明报告和证明报告附录 1 的副本

“安全相关的可编程系统 SIMATIC S7 Distributed Safety”和

“安全相关的可编程系统 SIMATIC S7 F/FH Systems（以前是 S7-400F 和 S7-400FH）”可以通过以下途径获取这些证明的副本：

Ms. Petra Bleicher

A&D AS RD ST Type Test，

传真号码：49 9621 80 3146，

电子邮件：mailto:petra.bleicher@siemens.com

注意

证明报告的附录 1 包含 S7 Distributed Safety 和 S7 F/FH Systems（验收测试期间需要对其进行检查）故障安全组件的允许版本号和签名。

证明报告包含当前使用 S7 Distributed Safety 或 S7 F/FH Systems 时必须满足的要求。

有关功能安全的标准和原则

使用下面介绍的标准和原则开发 F 系统 S7 Distributed Safety 和 S7 F/FH Systems。

可以在安全证明报告中找到标准和原则的当前状态和当前版本以及当前要求。

标准/原则	标题	注释
DIN V 19250	控制技术；测量和控制设备涉及到的基本安全方面	2004 年已废除
DIN V VDE 0801 包括修正版本 A1	安全相关的系统中计算机的工作原理	2004 年已废除
IEC 61508 - 1 到 4	电气/电子/可编程电子安全相关的系统的功能安全	-
EN 50159-1	铁路应用 — 通讯、信号和过程系统 — 第 1 部分：封闭传输系统中的安全相关的通讯	-
EN 50159-2	铁路应用 — 通讯、信号和过程系统 — 第 2 部分：开放传输系统中的安全相关的通讯	-
UL 1998	可编程组件中软件的标准	仅适用于 S7 Distributed Safety

过程工程

标准/原则	标题	注释
DIN V 19251	控制技术 — MC 保护设备 — 保护功能的要求和测量	2004 年已废除
VDI / VDE 2180 - 1 到 5	通过过程控制工程保护工业处理设备	对于 S7 F/FH Systems — 仅第 1、2、5 部分
NE 31	NAMUR 建议通过过程控制工程保护设备	-
ISA S 84.01	过程工业中安全测量系统的应用	-

燃烧器管理系统

标准/原则	标题	注释
EN 54	火警系统	仅适用于 S7 F/FH Systems
EN 230，条款 7.3	一体式燃油燃烧器；安全、控制和调节设备以及安全时间	-
EN 298，条款 7、8、9 和 10	自动气体燃烧器控制系统，用于气体燃烧器和具有或不具有鼓风机的气体燃烧器	-
ENV 1954	气体装置的安全相关的电子部分的内部和外部故障特性	已废除
DIN VDE 0116，条款 8.7	用于熔炉的电子设备	-
EN 50156-1	用于熔炉的电气设备，第 1 部分：应用计划和构造的规定	-
NFPA 72	国家火灾报警规范	仅适用于 S7 F/FH Systems
NFPA 85	锅炉与燃烧系统的危险等级标准	-

机器安全

标准/原则	标题	注释
98/37/EC	欧洲机械规范	-
EN 60204-1	机械安全；机器的电气设备；第 1 部分：一般要求	-
EN 954-1 Cat. 2 到 4	控制系统的机械安全相关的部件的安全，第 1 部分：设计的一般原则	-
EN 954-2	控制系统的机械安全相关的部件的安全，第 2 部分：验证	仅适用于 S7 Distributed Safety
NFPA 79	工业机器电气标准	仅适用于 S7 Distributed Safety
IEC 62061	机械安全 — 安全相关的电气、电子和可编程电子控制系统的功能安全	仅适用于 S7 Distributed Safety
IEC 61496	机械安全 — 电敏保护设备	仅适用于 S7 Distributed Safety 有关详细信息，请参考认证报告*《安全相关的可编程系统 SIMATIC S7 Distributed Safety》*。

压力

标准/原则	标题	注释
EN 692	压力机	仅适用于 S7 Distributed Safety
EN 693	Werkzeugmaschinen Pressen （压力机工具）	仅适用于 S7 Distributed Safety
EN 12622	Werkzeugmaschinen von Werkzeugmaschinen Gesenkbiegepressen （折弯机机械工具）	仅适用于 S7 Distributed Safety

关于各种器具的标准和原则

标准/原则	标题	注释
IEC 61131-2	可编程控制器 — 设备要求和测试 89/336/EEC	-
EN 50178	用于电源安装的电子设备	-
EN 60068	环境测试	-
EN 55011	工业、科学和医疗（ISM）射频设备无线电干扰特性的测量方法和限值	已废除
EN 50081-2	电磁兼容性；一般发射标准；第 2 部分：工业环境	已废除
EN 50081-2	电磁兼容性；一般抗扰标准；第 2 部分：工业环境	仅适用于 S7 F/FH Systems
EN 61000-6-2 EN 61000-6-4	EMC 一般标准 — 工业环境抗扰性	-
73/23/EEC	欧洲低电压规范	-
93/68/EEC	欧洲 EMC 规范	-
UL 508	工业控制设备	-

注意

必须遵循 F-CPU 和 F-I/O 环境相关的要求（参阅*适用的手册中的技术规范*）。

4.8 安全要求

标准化安全要求

S7 Distributed Safety 和 S7 F/FH Systems F-System 可以满足以下安全要求：

- 符合 IEC 61508 规定的安全等级（安全完整性等级）SIL1 至 SIL3
- 符合 EN 954-1 规定的类别 2 至类别 4

根据 IEC 61508-5 规定来确定安全完整性等级

使用危险图表的定性方法，可以基于相关危险因素知识来确定安全相关系统的安全完整性等级：

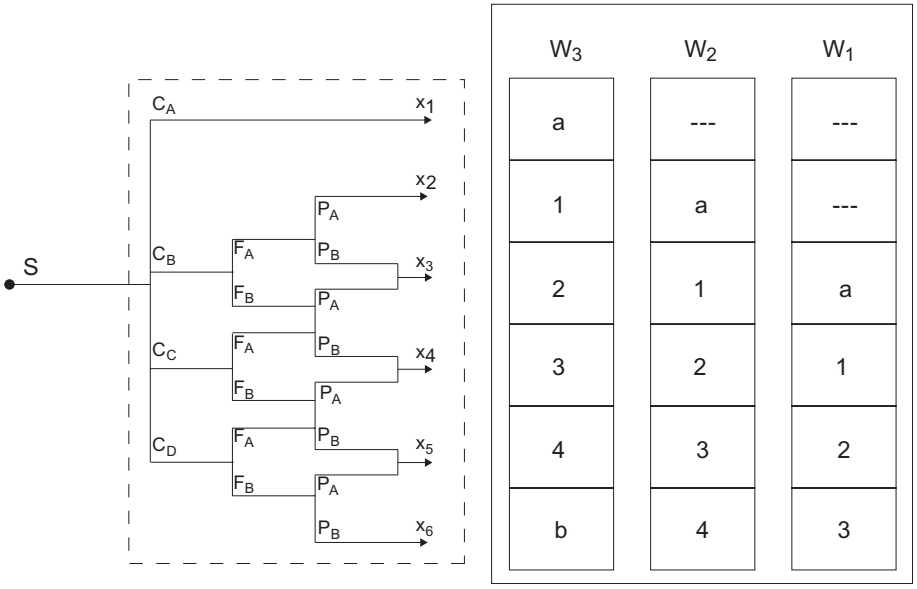


图 4-1 符合 IEC 61508-5 规定的危险图表

S	降低危险分析的起始点
C	危险参数，影响
F	危险参数，频率和暴露时间
P	危险参数，避免危险发生的概率
W	异常事件发生的概率
---	无安全要求
a	无特殊安全要求
b	单个电气/电子/可编程电子系统无法满足要求。
1, 2, 3, 4	安全完整性等级

危险参数

根据 DIN V 61508-5 规定，危险参数具有以下含义：

表格 4-1　　根据 IEC 61508-5 规定的危险参数的含义

参数	含义
影响（C）	
C_A	较小伤害
C_B	对一个或多个人员造成的无法挽回的重大伤害；人员伤亡
C_C	多人死亡
C_D	死亡人数众多
处于危险区中的频率和暴露时间（F）	
F_A	暴露在危险区（很少到经常）
F_B	暴露在危险区（频繁到持续）
避免危险发生的概率（P）	
P_A	在某些情况下可能发生
P_B	几乎不可能发生
异常事件发生的概率（W）	
W_1	很低
W_2	低
W_3	相对较高

符合 IEC 61508 规定的安全完整性等级

对于每一个“安全完整性等级”（SIL），IEC 61508 将目标测量定义为分配给故障安全系统的安全功能发生故障的概率。

表格 4-2　　符合 IEC 61508 规定的安全完整性等级

安全完整性等级	在低需求模式中运行 低需求模式（要求满足的平均故障概率）	在高需求或持续模式中运行 高需求/持续模式（每小时发生危险故障的概率）
4	≥ 10^{-5} 至 < 10^{-4}	≥ 10^{-9} 至 < 10^{-8}
3	≥ 10^{-4} 至 < 10^{-3}	≥ 10^{-8} 至 < 10^{-7}
2	≥ 10^{-3} 至 < 10^{-2}	≥ 10^{-7} 至 < 10^{-6}
1	≥ 10^{-2} 至 < 10^{-1}	≥ 10^{-6} 至 < 10^{-5}

表格说明

通常，执行器和传感器最有可能发生上表中的故障。

在所有情况下，安全功能包含从信息采集到信息处理直至目的动作的整个过程。

相关的设备（例如 S7 F/FH Systems F-System、传感器和执行器）必须共同遵循在危险评估期间确定的 SIL 或类别。

如果在 S7 Distributed Safety 或 S7 F/FH Systems 中共同执行控制功能和关联保护功能，则运行处于高需求模式或持续模式。

符合 IEC 61508 规定的危险分析

如下图所示，F-System 通过适当的组织和技术测量避免发生潜在危险，或将这些危险降低到容许等级。

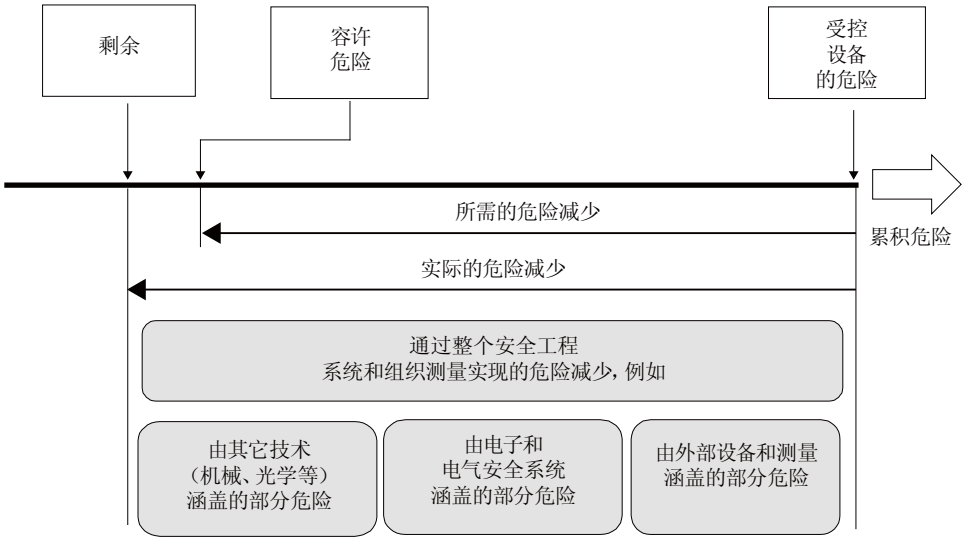


图 4-2　　符合 IEC 61508 规定的危险分析

S7 Distributed Safety 和 S7 F/FH Systems 各个组件的概率值

下表介绍了 S7 Distributed Safety 和 S7 F/FH Systems 各个组件发生故障的概率：

表格 4-3　　S7 Distributed Safety 和 S7 F/FH Systems 各个组件的概率值

	在低需求模式中运行 低需求模式（要求满足的平均故障概率）	**在高需求或持续模式中运行** 高需求/持续模式（每小时发生危险故障的概率）	**检验间隔**
适用于 S7 Distributed Safety 的 **F-CPU**：			
IM 151-7 F-CPU 6ES7 151-7FA01-0AB0	1.59 E-05	3.62 E-10	10 年
CPU 315F-2 DP 6ES7 315-6FF01-0AB0	2.38 E-05	5.43 E-10	10 年
CPU 315F-2 PN/DP 6ES7 315-2FH10-0AB0	4.76 E-05	1.09 E-09	10 年
CPU 317F-2 DP 6ES7 317-6FF00-0AB0	4.76 E-05	1.09 E-09	10 年
CPU 317F-2 PN/DP 6ES7 317-2FJ10-0AB0	4.76 E-05	1.09 E-09	10 年
CPU 416-2 6ES7 416-2FK02-0AB0 6ES7 416-2FK04-0AB0	4.76 E-05	1.09 E-09	10 年
适用于 S7 F/FH Systems 的 ：			
CPU 414-4H 6ES7 414-4HJ00-0AB0 6ES7 414-4HJ04-0AB0	 1.24E-04 1.88E-04	 1.42 E-09 4.29E-09	 10 年 10 年
CPU 417-4H 6ES7 417-4HL00-0AB0 6ES7 417-4HL01-0AB0 6ES7 417-4HL04-0AB0	 1.24E-04 1.24E-04 1.88E-04	 1.42 E-09 1.42 E-09 4.29E-09	 10 年 10 年 10 年
安全相关的通讯	1.00 E-05	1.00 E-09	
故障安全 I/O，例如： S7-300 F-SM	请参阅以下手册中的技术规范： *自动化系统 S7-300 故障安全信号模块*		
ET 200S F-Module	*ET 200S 分布式 I/O 系统故障安全模块*		
ET 200pro 故障安全模块	• *ET 200pro 分布式 I/O 设备，故障安全模块*		
• ET 200eco 故障安全 I/O 模块	• *ET 200eco 分布式 I/O 站故障安全 I/O 模块*		
故障安全 DP 标准从站	• 用于故障安全 DP 标准从站		
故障安全 I/O 标准设备	• 针对故障安全 I/O 标准设备		

确定 F-System 对发生故障的概率的影响

F-System 对安全功能发生故障的概率的影响取决于相关的 F-CPU 和 F-I/O 发生故障的概率之和。这样一来，冗余 F-CPU 计算一次而冗余 F-I/O 则计算两次。

（具有输入的冗余 F-I/O 计算两次，因为通过两个地址重复读取的输入信号在内部执行了 OR 操作，从而两个 F-I/O 都有可能导致出现故障。

具有输出的冗余 F-I/O 计算两次，因为从硬件方面考虑，通过两个地址重复激活的两个 F-I/O 的输出执行了 OR 操作。）

然后，将添加安全相关的通讯的影响。一种安全功能也可以与多个 F-System 相关。

将 F-System 的影响与安全功能相关的传感器和执行器的影响加到一起，来计算安全功能发生故障的概率。

计算实例

使用 S7 FH Systems F-System 执行安全功能。下表中指示的 F-CPU 和 F-SM 与安全功能有关。

F-CPU 和 F-SM 以冗余方式设置。它们的检验间隔为 10 年。对于 SIL3/类别 4，F-SM 在安全模式中运行。运行处于高需求模式：

表格 4-4　　F-System 对安全功能发生故障的概率的影响的计算实例

与安全功能有关的 F-CPU、F-SM 和安全相关的通讯	**编号**	**冗余**	**每小时发生危险故障的概率** （每小时发生危险故障的概率）
CPU 417-4H 6ES7 417-4HL04-0AB0	1	是	4.29E-09
SM 326; DO 10 × DC 24V/2A 6ES7 326-2BF01-0AB0	1	是	2 E-09
SM 326; DI 24 × DC 24V 6ES7 326-1BK01-0AB0	2	是	4 E-09
安全相关的通讯			1.00 E-09
总计			**11.29E-09**

使用 F-I/O 可实现的安全等级

5

5.1 引言

概述

本章列出了使用 S7 Distributed Safety 和 S7 F/FH Systems 中的故障安全 I/O 达到安全等级 SIL2/类别 3 和 SIL3/类别 4 时可以使用的选项。信息涉及到 SIMATIC S7 产品系列的 F-I/O（即 S7-300 F-SM、F 模块 ET 200S、ET 200pro 和 ET 200eco 故障安全 I/O 模块）。

其它信息

所用的 F-I/O 确定了是否可以在您的应用场合下实现说明的选项。有关这方面的信息，请参考以下相应 F-I/O 的手册：

- 对于 S7-300 F-SM：*《自动化系统 S7-300 故障安全信号模块》*手册
- 对于 ET 200S 故障安全模块：*《ET 200S 分布式 I/O 系统故障安全模块》*手册
- 对于 ET 200pro 故障安全模块：*《ET 200pro 分布式 I/O 设备故障安全模块》*手册
- 对于 ET 200eco 故障安全模块：*《ET 200eco 分布式 I/O 站点故障安全 I/O 模块》*手册

达到具有输入的 F-I/O 的安全等级

已达到具有输入的 F-I/O 要求的安全等级，如下：

- 在内部，使用测试线路和自动测试
- 在外部，由传感器评估的类型确定，即**传感器的接线确定安全等级** SIL2/类别 3 或 SIL3/类别 4

达到具有输出的 F-I/O 的安全等级

已达到具有输出的 F-I/O 要求的安全等级，如下：

- 在内部，使用测试线路和自动测试
- 在外部，由执行器规定的互连确定
  此外，可能需要由 F-I/O 读取并由安全程序判断来自过程的测试信号。

5.2 用于达到具有输入的 F-I/O 的安全等级的安全功能

具有数字输入的 F-I/O 的传感器评估

对于具有**数字输入** 的 F-I/O，可以通过传感器评估的类型达到要求的安全等级。

表格 5-1 具有数字输入的 F-I/O 可实现的安全等级

安全等级...		... 要求的传感器评估
符合 IEC 61508	符合 EN 954-1	
SIL2	类别 3	1oo1 评估
SIL3	类别 4	1oo2 评估

具有模拟输入的 F-I/O 的传感器评估

对于具有**模拟输入**的 F-I/O，始终在安全模式中执行 1oo2 传感器评估。使用或不使用传感器冗余达到要求的安全等级。

表格 5-2 具有模拟输入的 F-I/O 可实现的安全等级

安全等级...		... 要求的传感器评估
符合 IEC 61508	符合 EN 954-1	
SIL2	类别 3	1oo2 评估，单通道传感器
SIL3	类别 4	1oo2 评估，冗余传感器

用户需要执行的操作步骤

- 将传感器连线至符合传感器评估要求和供电要求的 F-I/O（1oo1 或 1oo2 评估、单通道或双通道传感器；传感器由 F-I/O 供电或外部供电）
- 使用 *STEP 7* 分配以下参数：
  - 传感器评估（1oo1 或 1oo2）
  - 传感器互连类型（单通道或双通道）
  - 启用短路测试（如果可用）
  - 指定冗余 F-I/O（如果可用）（仅用于 S7 FH Systems）
  - 指定误差时间（如果可用）

传感器质量对安全等级的影响

可实现的安全等级取决于传感器的质量和符合 IEC 61508 的检测间隔（外部功能测试的间隔）的大小。

如果传感器的质量低于要求的安全等级中规定的质量，必须使用通过双通道连接的冗余传感器。

参见

具有输入的 F-I/O 的 1oo2 评估 (页 112)

5.2.1 具有数字输入的 F-I/O 的 1oo1 评估

引言

本节介绍了传感器接线实例，以更好地理解 1oo1 评估。这些实例选自*《自动化系统 S7-300 故障安全信号模块》*手册，在实例中显示了将传感器连线至 F-SM 的多个选项。

1oo1 评估

在 1oo1 评估中，通过一个通道将一个非冗余传感器连接至 F 模块。

符合 VDE 0116 和 EN 298 的燃烧器管理应用程序

如果使用符合 VDE 0116 和 EN 298 并通过一个通道确保安全的传感器，则符合 VDE 0116 和 EN 298 的燃烧器管理应用程序中可能**与 1oo1 传感器评估**一起使用具有数字输入的 S7-300 F-SM、ET 200S 和 ET 200pro F 模块以及 ET 200eco I/O 模块。

实例：通过一个通道将一个单通道传感器连接至一个 F-DI（SIL2/类别 3）

下图介绍了 SM 326、DI 24 x 24 VDC 与 1oo1 传感器评估的接线图。该传感器由 F-I/O 供电。此接线可以达到 SIL2/类别 3。仅在使用适合的传感器时才能达到 SIL2/类别 3。

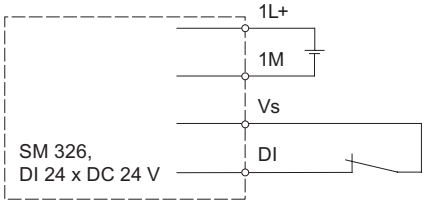


图 5-1 实例：通过一个通道将一个传感器连接至一个 F-DI（1oo1）的接线图

高可用性 1oo1 评估（仅用于 S7 FH Systems）

要达到高可用性，可以在 **S7 FH Systems** 中将一个传感器连接至两个冗余 F-DI 或将两个传感器冗余地连接至两个 F-DI。

实例：通过一个通道将一个传感器连接至两个 F-DI（高可用性；SIL2/类别 3）

下图介绍了一个连接至两个 SM 326、DI 24 x 24 VDC 模块的传感器的 1oo1 传感器评估接线图。该传感器由外部供电。此接线可以达到 SIL2/类别 3 和高可用性。仅在使用合适合格的传感器时才能达到 SIL2/类别 3。

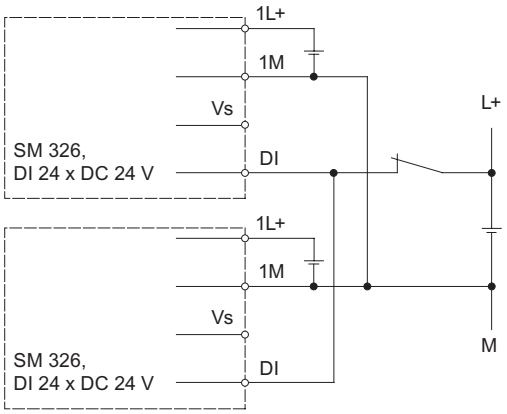


图 5-2　　实例：通过一个通道将一个传感器连接至两个 F-DI（1oo1、高可用性）的接线图

实例：通过一个通道将两个冗余传感器连接至两个 F-DI（高可用性；SIL2/类别 3）

下图介绍了连接至两个 SM 326、DI 24 x 24 VDC 模块的两个冗余传感器的 1oo1 传感器评估接线图。该传感器由 F-I/O 供电。此接线可以达到 SIL2/类别 3 和高可用性。仅在使用合适合格的传感器时才能达到 SIL2/类别 3。

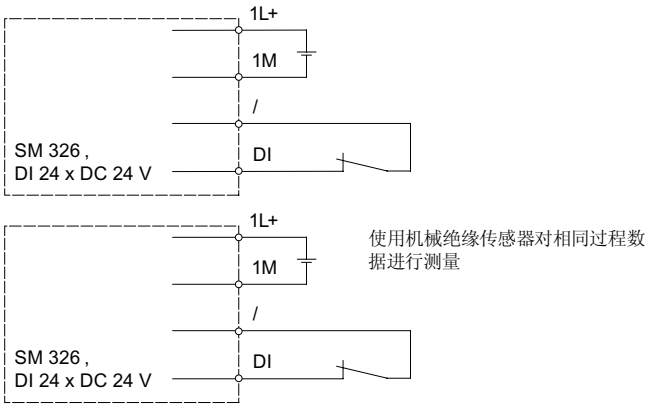


图 5-3　　实例：通过一个通道将两个冗余传感器连接至两个 F-DI（1oo1、高可用性）的接线图

5.2.2 具有输入的 F-I/O 的 1oo2 评估

引言

本节介绍了传感器接线实例，以更好地理解 1oo2 评估。这些实例选自*《自动化系统 S7-300 故障安全信号模块》*手册，显示了将传感器连线至 F-SM 的多个选项。

1oo2 评估

在 1oo2 评估中，两个输入通道由一个双通道传感器或两个单通道传感器占用。在内部比较输入信号是对等还是非对等。

1oo2 评估的误差分析

为了区分硬件故障与短暂、随机的信号更改，与安全相关的输入信号将进行内部误差分析（作为 1oo2 传感器评估的一部分）。

对于两个关联输入信号，检测到不同级别（对于非对等测试，检测到相同级别）时启动误差分析。在一段可编程的时间（称为误差时间）过去后，将进行检查以确定区别是否消失（对于非对等测试，则检查相同处是否消失）。如果未消失，则说明存在误差错误。

具有数字输入的 F-I/O 的 1oo2 评估

对于 1oo2 评估的情况，在安全程序中只使用与 1oo2 传感器评估相关的两个通道中编号较小的通道。

可以通过一个或两个传感器执行 1oo2 评估。这些传感器通过一个或两个通道连接至 F-I/O。

实例：通过一个通道将一个单通道传感器连接至一个 F-DI（SIL3/类别 3）

下图介绍了 SM 326, DI 24 X 24 VDC 进行 1oo2 传感器评估的接线图。该传感器由 F-I/O 供电。仅在使用合适合格的传感器时才能达到 SIL3/类别 4。

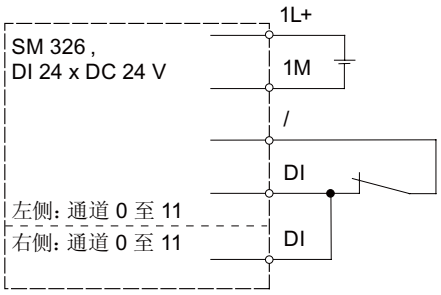


图 5-4　　实例：通过一个通道将一个传感器连接至一个 F-DI（1oo2）的接线图

实例：通过两个通道将一个单通道传感器连接至一个 F-DI（SIL3/类别 4）

下图介绍了 SM 326、DI 24 X 24 VDC 与一个双通道传感器的 1oo2 评估的接线图。此接线可以达到 SIL3/类别 4。仅在使用合适合格的传感器时才能达到 SIL3/类别 4。

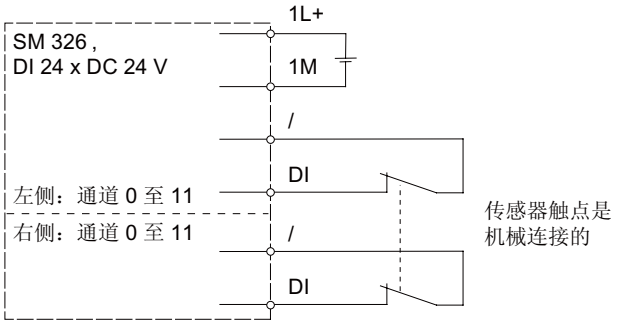


图 5-5　　实例：通过两个通道将一个双通道传感器连接至一个 F-DI（1oo2）的接线图

实例：通过两个通道将一个非对等传感器非对等地连接至一个 F-DI（SIL3/类别 4）

下图介绍了 SM 326、DI 24 x 24 VDC 与非对等传感器（1oo2 评估）的接线图。此接线可以达到 SIL3/类别 4。模块左侧通道将提供有用信号。这意味着如果未检测到故障，则可以在 F-CPU 上的输入 I/O 区域中使用这些信号。仅在使用合适合格的传感器时才能达到 SIL3/类别 4。

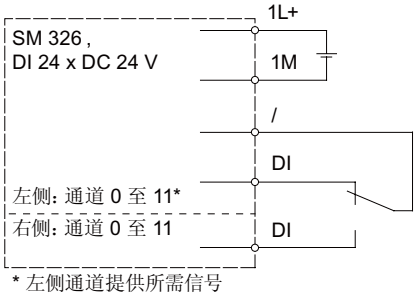


图 5-6　　实例：通过两个通道将一个非对等传感器非对等地连接至一个 F-DI（1oo2）的接线图

高可用性 1oo2 评估（仅用于 S7 FH Systems）

要达到高可用性，可以在 **S7 FH Systems** 中将一个传感器连接至两个 F-DI 或将两个传感器冗余地连接至两个 F-DI。

实例：将一个双通道传感器连接至两个 F-DI（高可用性；SIL3/类别 4）

下图介绍了一个连接至两个 SM 326、DI 24 x 24 VDC 模块的传感器的 1oo2 传感器评估接线图。该传感器由外部供电。此接线可以达到 SIL2/类别 4 和高可用性。仅在使用合适合格的传感器时才能达到 SIL3/类别 4。

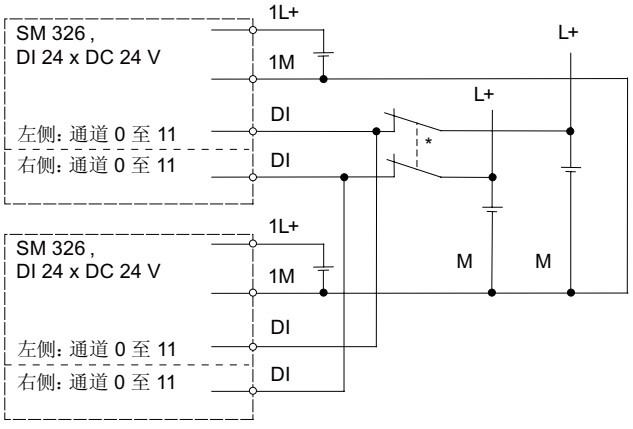


图 5-7　　实例：通过两个通道将一个双通道传感器连接至两个 F-DI（1oo2、高可用性）的接线图

实例：通过一个通道将两个冗余传感器连接至两个 F-DI（高可用性；SIL3/类别 4）

下图介绍了连接至两个 SM 326、DI 24 X 24 VDC 模块的传感器的 1oo2 传感器评估接线图。该传感器由 F-I/O 供电。此接线可以达到 SIL2/类别 4 和高可用性。仅在使用合适合格的传感器时才能达到 SIL3/类别 4。

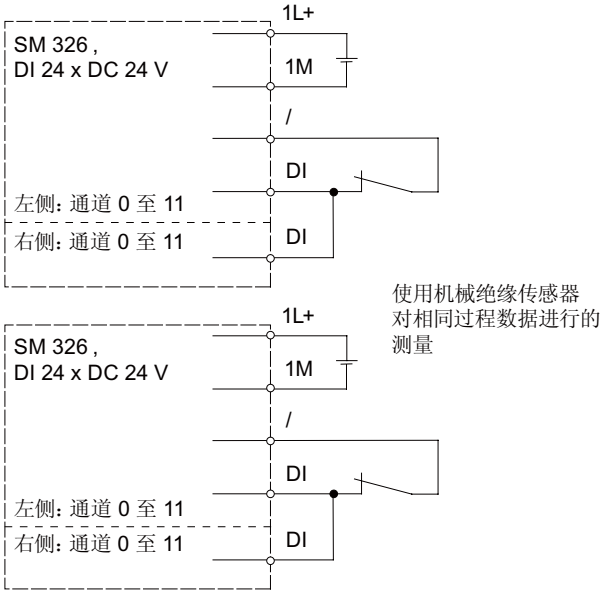


图 5-8　实例：通过一个通道将两个冗余单通道传感器连接至两个 F-DI（1oo2、高可用性）的接线图

具有模拟输入的 F-I/O 的 1oo2 评估

可以使用一个或多个传感器执行具有模拟输入的 F-I/O 的 1oo2 评估。这些传感器通过一个或两个通道连接至 F-I/O。

实例：通过一个通道将一个单通道传感器连接至一个 F-AI（SIL2/类别 3）

下图介绍了 SM 336、AI 6 X 13 位（电流测量范围 4 mA 至 20 mA、2 线变送器输出）的接线图。该传感器由 F-I/O 供电。此接线可以达到 SIL2/类别 3。

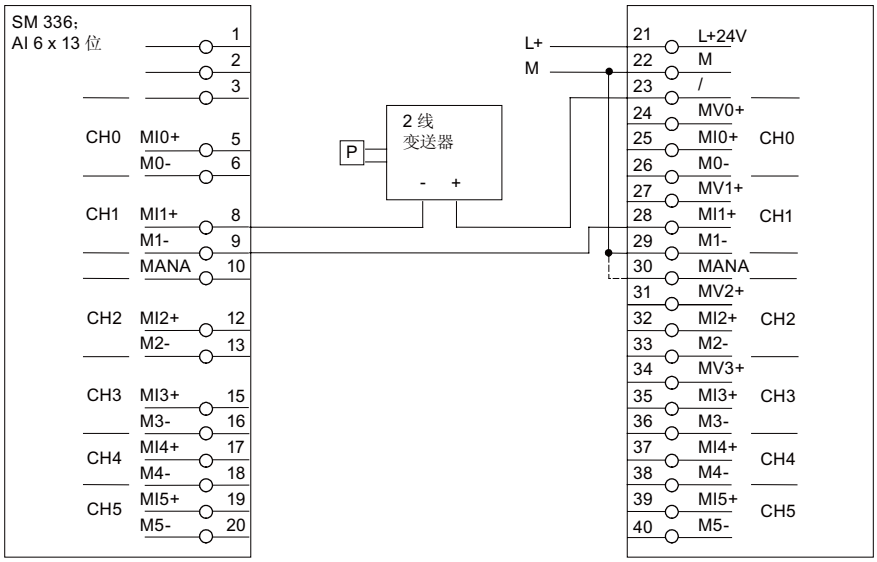


图 5-9　　实例：通过一个通道将一个传感器连接至一个 F-AI（1oo2）的接线图

实例：通过两个通道将两个冗余传感器连接至一个 F-AI（SIL3/类别 4）

下图介绍了 SM 336、AI 6 X 13 位（电流测量范围 4 mA 至 20 mA、2 线变送器输出）的接线图。该传感器由 F-I/O 供电。此接线可以达到 SIL3/类别 4。

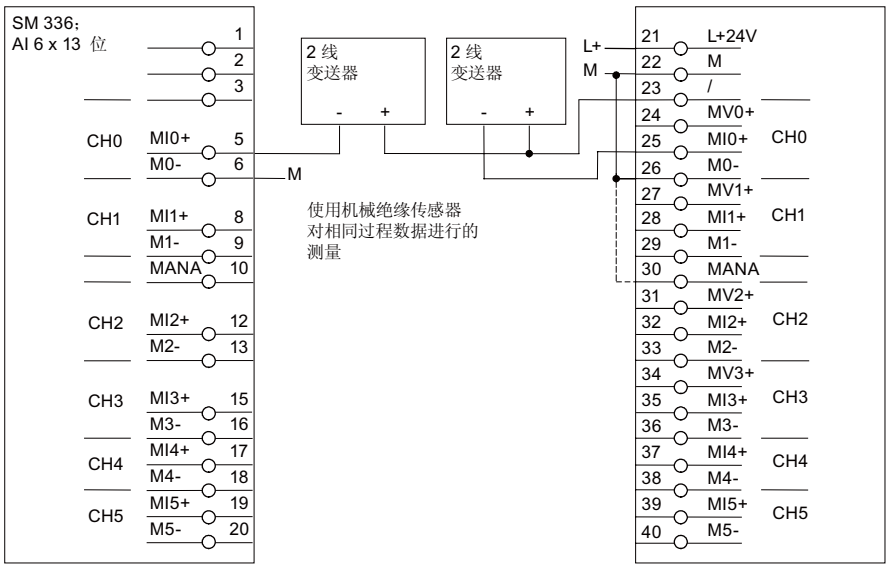


图 5-10　　实例：通过两个通道将两个冗余传感器连接至一个 F-AI（1oo2）的接线图

高可用性 1oo2 评估（仅用于 S7 FH Systems）

要达到高可用性，可以在 **S7 FH Systems** 中将四个冗余传感器连接至两个 F-AI。

实例：通过两个通道将四个冗余传感器连接至两个 F-AI（高可用性；SIL3/类别 4）

下图介绍了两个 SM 336、AI 6 X 13 位（电流测量范围 4 mA 至 20 mA、2 线变送器输出）的接线图。该传感器由 F-I/O 供电。此接线可以达到 SIL2/类别 4 和高可用性。

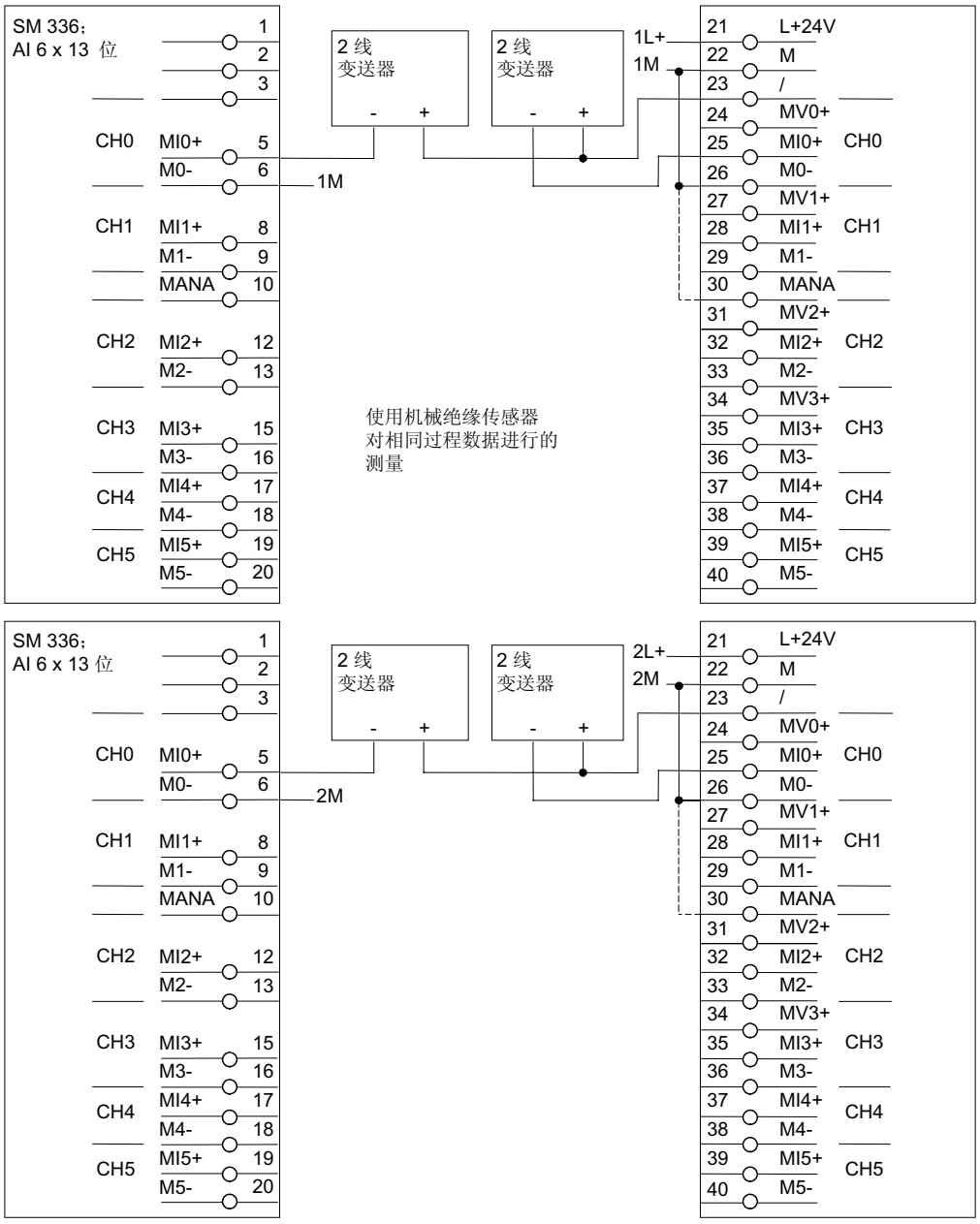


图 5-11　　实例：通过两个通道将四个冗余传感器连接至两个 F-AI（1oo2、高可用性）的接线图

5.3 用于达到具有输出的 F-I/O 的安全等级的安全功能

具有输出的 F-I/O 的测试信号发射

对于具有输出的 F-I/O，通过发射测试信号达到需要的安全等级。

表格 5-3 具有输出的 F-I/O 可实现的安全等级

安全等级...		... 测试信号的发射要求
符合 IEC 61508	符合 EN 954-1	
SIL2	类别 3	• 关闭期
SIL3	类别 4	• 打开期 • 关闭期

关闭期

关闭期发生在关闭测试期间和整个位模式测试期间。它涉及在激活输出时，由具有输出的 F-I/O 提供给输出的与测试相关的“0”信号。然后暂时关闭输出（关闭期）。足够慢的执行器对此无响应，仍处于打开状态。

打开期

打开期发生在整个位模式测试期间。它涉及取消激活输出（输出信号“0”）时，由具有输出的 F-I/O 提供给输出的与测试相关的“1”信号。然后暂时打开输出（打开期）。足够慢的执行器对此无响应，仍处于取消激活状态。

使用双通道、单插头激活的输出时，出现打开期。使用双通道、双插头激活的当前电流源式和电流漏式输出（ET 200S、ET 200pro F 模块和 SM 326；

DO 8 × 24 VDC/2 A PM）时，不出现打开期。

每天（或更频繁地）更改信号

如果每天或更频繁地更改信号，则即使不出现打开期，S7-300 F-SM 也可以达到 SIL3/类别 4。

用户需要执行的操作步骤

对于 S7-300 F-SM，使用 *STEP 7* 进行参数化：

- 以 SIL2/类别 3 或 SIL3/类别 4 运行 F-I/O（隐式指定测试信号发射的类型）
- 每天（或更频繁地）更改信号

对于 ET 200S、ET 200pro 和 ET 200eco **F-DO 模块**，由于通常设计用于安全等级 SIL3/类别 4，因此无需进行设置。

对 F 系统进行组态

6

6.1 引言

F-I/O 的组态和标准系统相同

S7 Distributed Safety 和 S7 F/FH Systems 故障安全系统的组态基本上与标准 S7-300 和 S7-400 站的组态相同。唯一区别是故障安全组件（F-CPU 和 F-I/O）的对象属性包括一些特殊标签。

F 组件需要由用户进行组态

必须对以下硬件组件进行组态：

- F-CPU，例如 CPU 315F-2 DP
- F-I/O，例如：
  - ET 200S 故障安全模块
  - ET 200pro 故障安全模块
  - ET 200eco 故障安全 I/O 模块
  - 故障安全 S7-300 信号模块（F-CPU 旁边的集中式组态或 ET 200M 中的分布式组态）
  - 故障安全 DP 标准从站/标准 I/O 设备

概述

本章概述了对 F 系统组件的组态。S7 Distributed Safety 和 S7 F/FH Systems 之间的较小区别将单独说明。

其它信息

您可以在 *STEP 7 在线帮助*中找到有关对硬件进行组态的详细信息。有关对 F 系统进行组态和编程的特定规则和详细实例项目，请参考：

- 对于 S7 Distributed Safety：*《S7 Distributed Safety 使用入门》*手册
- 对于 S7 Distributed Safety：*《S7 Distributed Safety 组态和编程》*手册
- 对于 S7 F/FH Systems：*《可编程控制器 S7 F/FH》*手册
- 对于 S7 F/FH Systems：*step7\实例*目录

6.2 对 F-CPU 进行组态

组态

在 *HW Config* 的硬件目录中列出了 F-CPU 以及其它 S7-300 和 S7-400 CPU。

使用与组态标准 CPU 相同的步骤对 F-CPU 进行组态。将 F-CPU 放置到组态表中后，您可以通过选择 **Edit（编辑）> Object Properties（对象属性）**菜单命令或双击 F-CPU 来访问组态对话框。

在“Protection”（保护）标签中，您必须对 F-CPU 的保护级别进行组态。

S7 Distributed Safety CPU 还有一个用于 F 属性的特定标签，称为“F 参数”；S7 F/FH systems 不包含此标签。

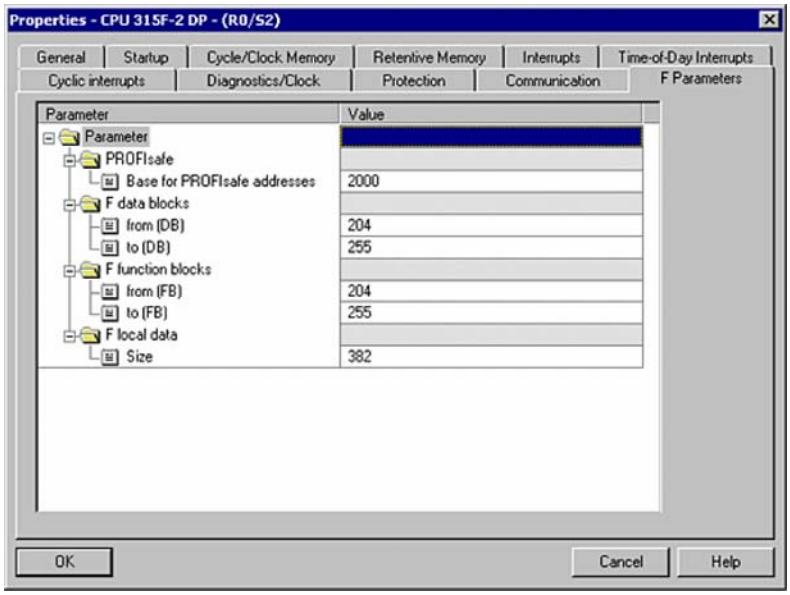
对 S7 Distributed Safety 的 F-CPU 进行组态的实例

以下显示 CPU 315F-2 DP 的“F Parameters”（F 参数）标签。

S7 Distributed Safety 自动分配 PROFIsafe 地址。F 系统 PROFIsafe 地址的内部管理需要“PROFIsafe 地址基址”的信息。PROFIsafe 地址用于唯一标识源和目标。

此外，用户为安全程序保留 CPU 资源（F 数据区域、F 功能块和 F 本地数据）。这些资源无法在安全程序或标准用户程序（已为自动添加的 F 块保留）中使用。

标签的*上下文相关的在线帮助*和*《S7 Distributed Safety 组态和编程》*手册对参数进行了说明。



6.3 对 F-I/O 进行组态

F-I/O 的组态和标准系统相同

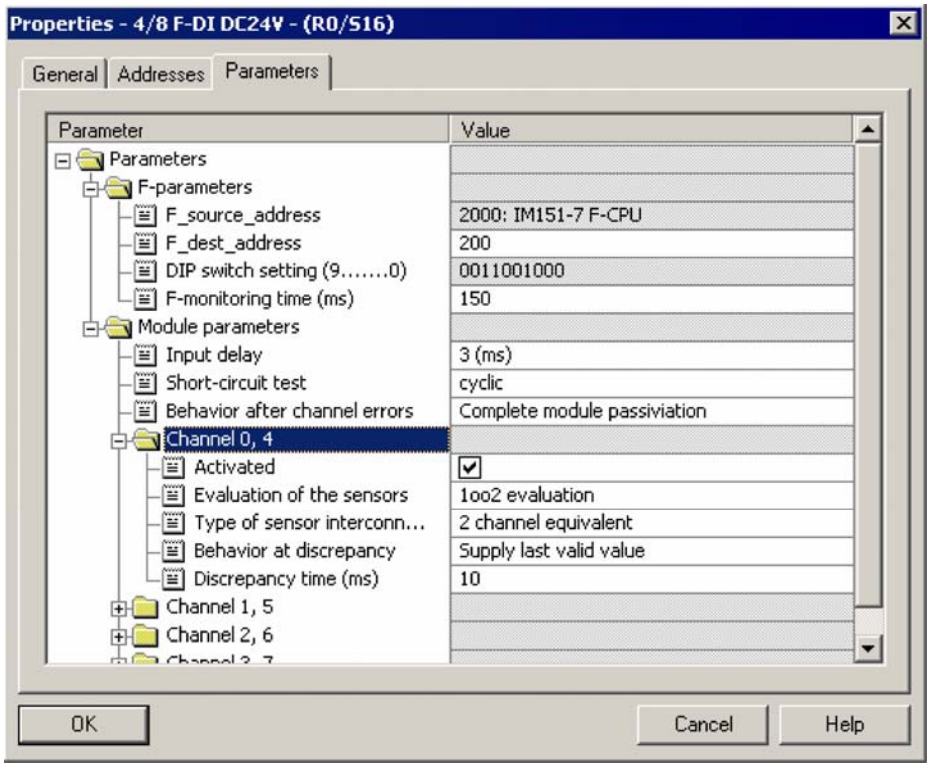
始终按照相同的步骤对 F-I/O 进行组态：

将 F-I/O 放置在 *HW Config* 的站点窗口中后，您可以通过选择 **Edit（编辑）> Object Properties（对象属性）**菜单命令或双击 F-I/O 来访问组态对话框。

对 F-I/O 进行组态的实例

以下显示 4/8 F-DI 24 VDC PROFIsafe 故障安全模块的参数标签。阴影区域中的值是由可选软件自动分配的。用户可以更改非阴影区域中的值。

*标签的上下文相关的在线帮助*和*《ET 200S 分布式 I/O 系统故障安全模块》*手册对参数进行了说明。



6.4 对故障安全 DP 标准从站和故障安全 I/O 标准设备进行组态

要求

为了使用带 S7 Distributed Safety 功能的故障安全 DP 标准从站，该标准从站必须位于 PROFIBUS-DP 上且支持 PROFIsafe 总线配置文件。IE/PB link 后用于 PROFIBUS DP 和 PROFINET IO 的混合组态的故障安全 DP 标准从站，必须支持 V2 模式下的 PROFIsafe 总线配置文件。

为了使用带 S7 Distributed Safety 功能的故障安全 I/O 标准从站，该标准从站必须位于 PROFINET IO 上且支持 V2 模式的 PROFIsafe 总线配置文件。

使用 GSD/GSDML 文件进行组态

就和在标准系统中的情况一样，对故障安全 DP 标准从站/标准 I/O 设备进行组态的基础是 GSD/GSDML 文件（通用站点描述/通用站点描述标识语言 — **G**eneric **S**tation **D**escription/**G**eneric **S**tation **D**escription **M**arkup **L**anguage）中的设备规范。

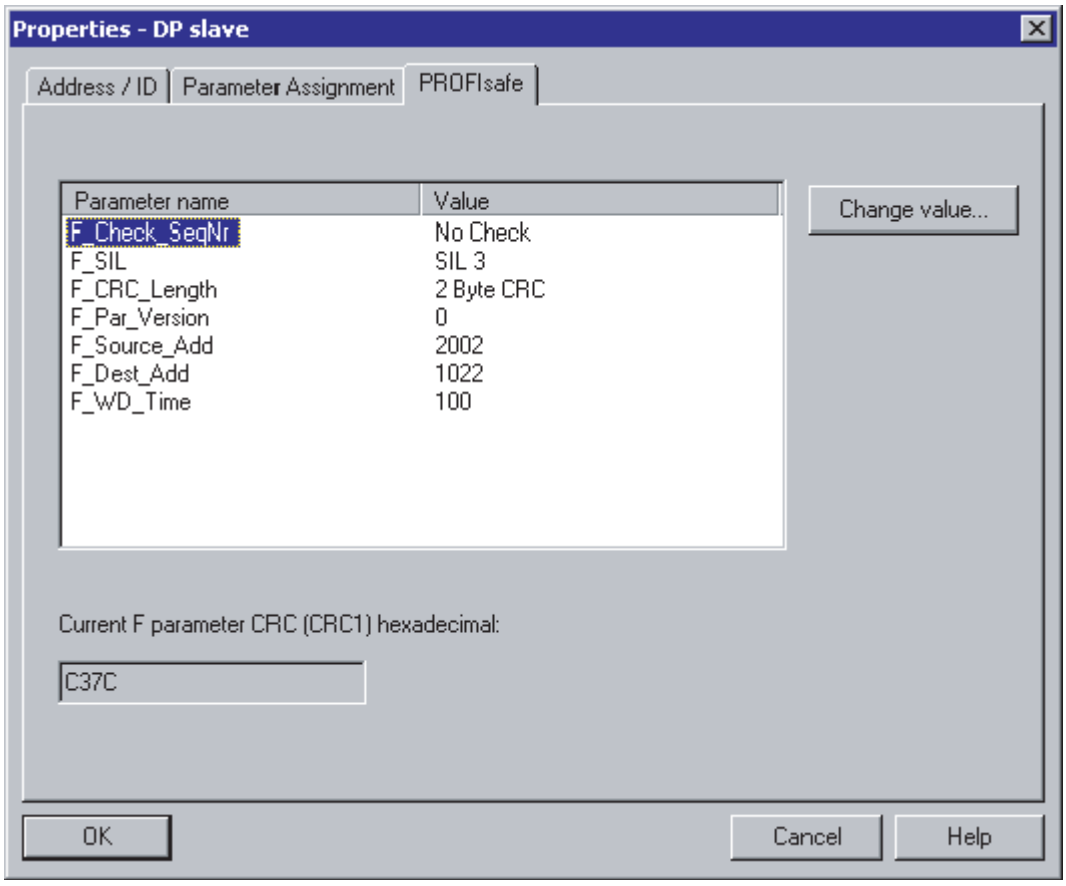
DP 标准从站的所有属性均保存在 GSD 文件中。标准 I/O 设备的属性保存在 GSDML 文件中。CRC 确定故障安全 DP 标准从站/标准 I/O 设备的部分规范。

GSD 和 GSDML 文件由设备生产商提供。用户将 GSD/GSDML 文件导入项目（请参阅 *STEP 7 在线帮助*）。导入了故障安全 DP 标准从站/IO 标准设备后，就可以从 *HW Config* 的硬件目录中选择该设备。

对故障安全 DP 标准从站进行组态的实例

以适用于安全故障 DP 标准从站的故障安全相关标签为例。GSD 文件中指定的参数文本包含在“PROFIsafe”标签中的“Parameter name”（参数名称）下，而每个参数的当前值包含在“Value”（值）下面。单击“Change value....”（更改值...）可以修改该值

标签的*上下文相关的在线帮助*和*《S7 Distributed Safety 组态和编程》*手册对参数进行了说明。



对 F 系统进行编程

7

7.1 引言

使用标准编程语言进行编程

使用 *STEP 7* 的标准编程语言对 S7 Distributed Safety 和 S7 F/FH Systems 故障安全系统进行编程。

概述

本章介绍了安全程序的程序结构和元素。

由于 S7 Distributed Safety 和 S7 F/FH Systems 的编程存在本质区别，因此对它们的安全程序结构分别进行说明。

其它信息

以下手册详细介绍了安全程序的编程步骤：

- 对于 S7 Distributed Safety：*《S7 Distributed Safety 组态和编程》*手册
- 对于 S7 F/FH Systems：*《可编程控制器 S7 F/FH》*手册

具有标准用户程序和安全程序的项目的示意图结构

下图提供了编程设备或工程系统中使用 S7 Distributed Safety 和 S7 F/FH Systems 的标准用户程序和安全程序的 *STEP 7* 项目的示意图结构。

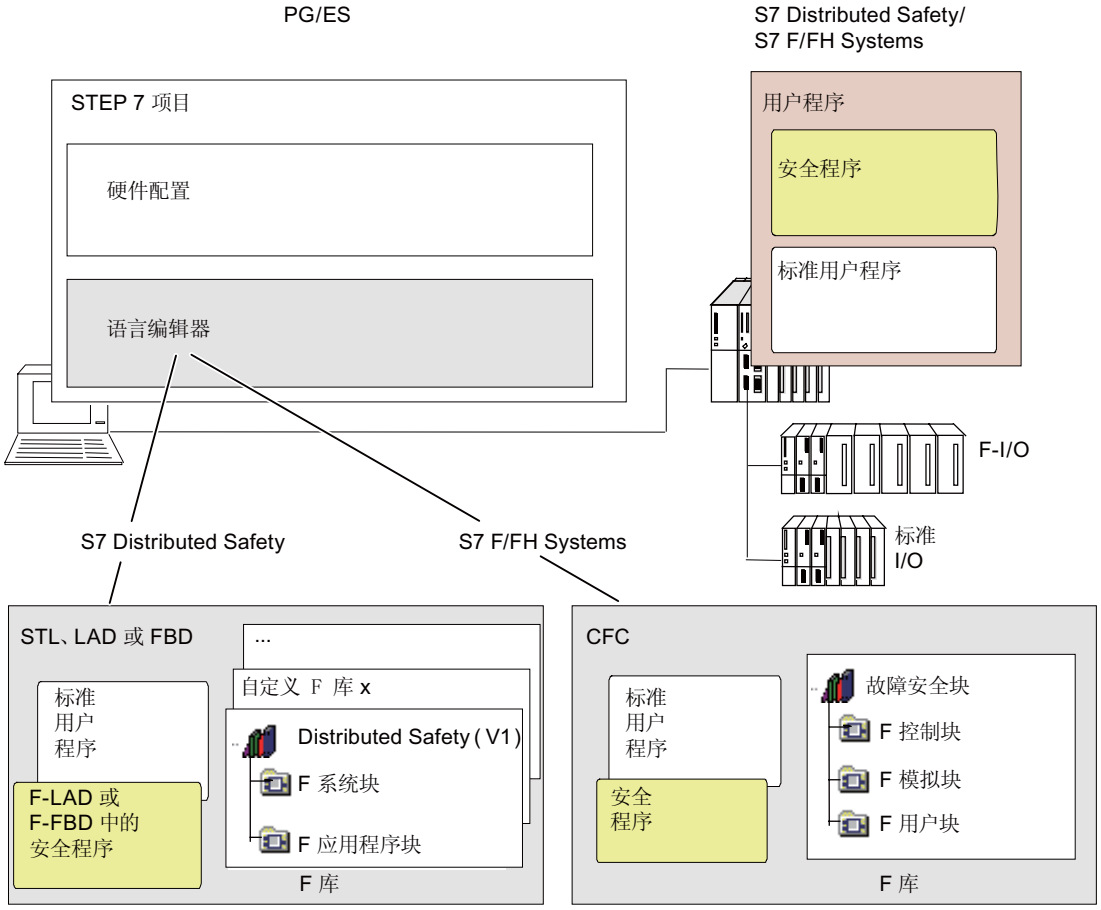


图 7-1　　STEP 7 项目的示意图结构

S7 Distributed Safety 和 S7 F/FH Systems 之间的区别

S7 Distributed Safety 和 S7 F/FH Systems 编程的区别在于：可以使用的编程语言不同以及从安全程序的 F 库中集成故障安全块的方式不同。

7.2 F 系统的编程语言

F-CPU 中的用户程序

F-CPU 中的用户程序通常由标准用户程序和安全程序组成。标准用户程序是在 *STEP 7* 中使用标准编程语言（例如 STL、LAD 或 FBD）或者 CFC 编程语言创建的。

对于 S7 Distributed Safety，在 F-FBD 或 F-LAD 中对安全程序进行编程。**对于 S7 F/FH systems**，F 库的故障安全块在 CFC 中互连。

安全程序还包括用于错误检测和错误响应（由附加软件自动修正）的故障安全块。这将确保可以检测到错误和故障，并触发适当的响应，以使 F 系统停止在安全状态或跳转到安全状态。

S7 Distributed Safety：F-FBD 和 F-LAD 编程语言

F-FBD 和 F-LAD 编程语言原则上相当于标准 FBD/LAD 语言。可以使用 *STEP 7* 中的标准 *FBD/LAD 编辑器*对其进行编程。

F-FBD 和 F-LAD 编程语言与标准 FBD/LAD 语言之间的主要区别在于命令集和数据类型的限制以及可以使用的地址区域不同。

S7 F/FH Systems：编程语言 CFC

在单独的连续功能图（CFC）中，从由 *S7 F 系统*选件包提供的 F 库的故障安全块中创建安全程序。

F 块库

S7 Distributed Safety 和 *S7 F Systems* 选件包包括（用于 F 系统编程）：

- 对于 S7 Distributed Safety：*Distributed Safety* F 库（V1）
- 对于 S7 F/FH Systems：*故障安全块* F 库（V1_2）

F 库位于 *step7/s7libs* 目录中。

7.3 S7 Distributed Safety 中安全程序的结构

程序结构的表示

下图显示了 S7 Distributed Safety 安全程序的示意图结构。为了结构化，一个安全程序由一个或两个 F 运行组组成。安全程序包括以下组件：

- 由用户创建或从 F 库（例如 *Distributed Safety* F 库 [V1]）中选择的 F 块。
- 自动添加的 F 块（F-SB、自动生成的 F 块和 F 共享 DB）

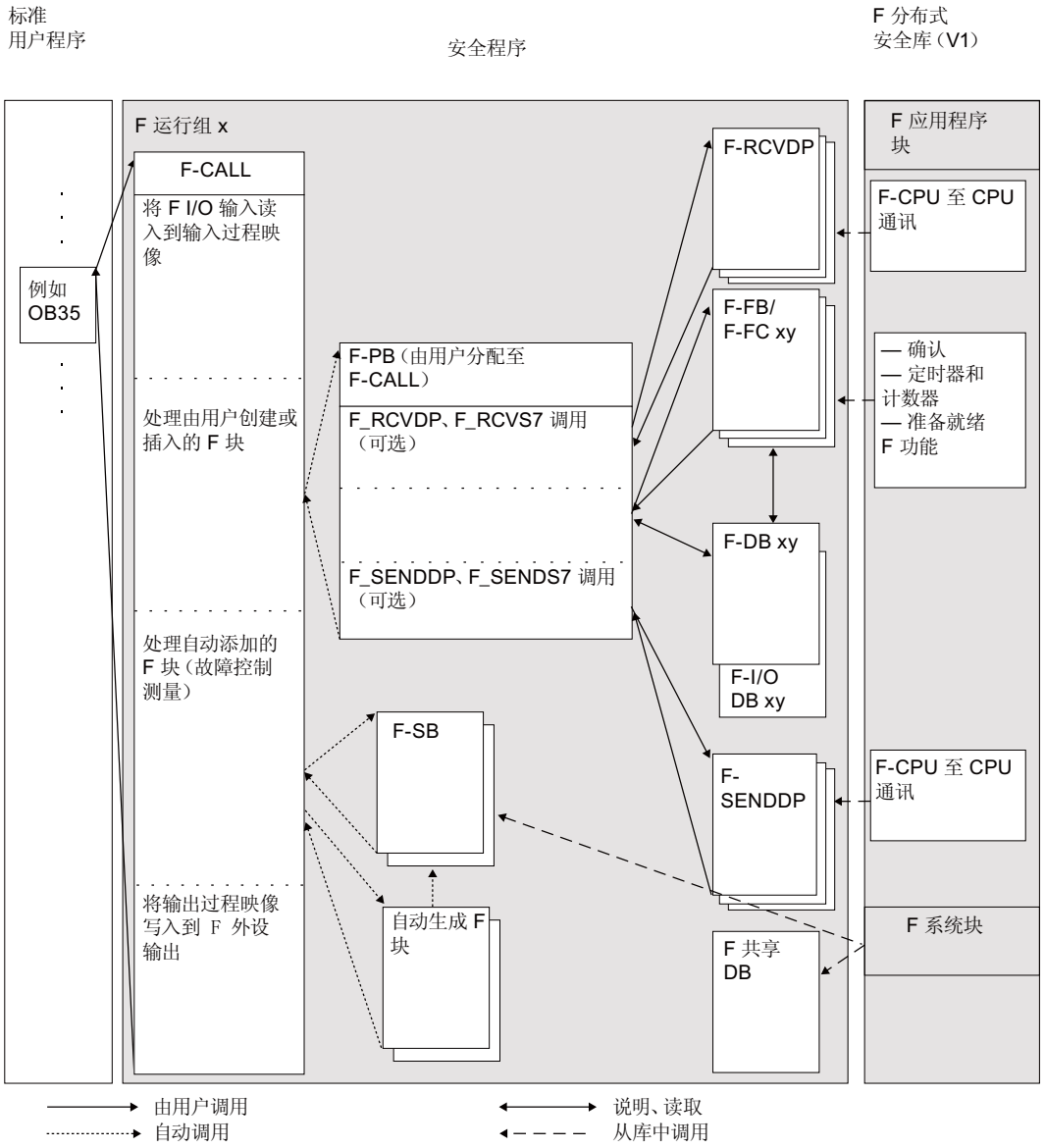


图 7-2 S7 Distributed Safety 中安全程序的组件

程序结构说明

通过从标准用户程序中调用 F-CALL 来访问安全程序。在 OB 中，更应在时间中断 OB（例如 OB35）中调用 F-CALL。

时间中断 OB 的优点是其以固定的时间间隔中断执行标准用户程序的 OB 1 中的循环程序。即，在时间中断 OB 中，以固定的时间间隔调用和运行安全程序。

执行安全程序后，标准用户程序将恢复运行。

F 运行组中安全程序的结构

为了方便操作，安全程序由一个或两个 “F 运行组”构成。F 运行组是由多个相关的 F 块组成的逻辑结构。

S7 Distributed Safety 安全程序中的一个 F 运行组包括：

- 一个 F-CALL F 调用块
- 一个 F 程序块（分配给 F-CALL 的 F-FB/F-FC）
- 使用 F-FBD 或 F-LAD 编程的附加 F-FB 或 F-FC（如果需要）
- 一个或多个 F-DB（如果需要）
- F-I/O DB
- *Distributed Safety* F 库（V1）的 F 块
- 来自自定义 F 库的 F 块
- F 系统块
- 自动生成的 F 块

如果用户将其安全程序分为两个 F 运行组，则可以以更快优先等级执行部分安全程序（一个 F 运行组），从而使用较短的响应时间实现更快的安全回路。

F 运行组的 F 块

下表显示了用户在 F 运行组中使用的 F 块：

表格 7-1　F 运行组的故障安全块

F 块	功能	编程语言
F-CALL	用于从标准用户程序调用 F 运行组的 F 块。F-CALL 包含 F 程序块的调用和 F 运行组中自动添加的 F 块的调用。 F-CALL 由用户创建，无法对其进行编辑。	F-CALL
F-FB/F-FC、 F-PB	用户使用 F-FBD 或 F-LAD 对实际安全功能进行编程。F 编程的起始点是 F 程序块。F-PB 是一个 F-FC 或 F-FB（具有背景数据块），在分配给 F-CALL 时成为 F-PB。用户可以在 F-PB 中执行： • 使用 F-FBD 或 F-LAD 对安全程序进行编程 • 调用其它已创建的 F-FB/F-FC 以构建安全程序 • 从 *Distributed Safety* F 库（V1）插入 *F 应用程序块* 块容器的 F 块。 • 从“自定义 F 库”插入 F 块 用户指定 F-PB 内 F 块的调用顺序。	F-FBD/F-LAD
F-DB	可以从安全程序中的任何地方读/写访问的可选故障安全数据块	F-DB
F-I/O DB	在 *HW Config* 中编译程序时，为每个 F-I/O 自动生成一个 F-I/O DB。用户可以或必须访问与 F-I/O 访问相关的 F-I/O DB 的变量。	-

Distributed Safety F 库（V1）的 F 块

Distributed Safety F 库（V1）包含：

- *F 应用程序块*/*块*块容器中的 F 应用程序块
- *F 系统块*/*块*块容器中的 F 系统块和 F 共享 DB

下表显示了包含在块容器中的 F 块：

表格 7-2　　Distributed Safety F 库（V1）的故障安全块

块容器	... 包含 F 块，用于	功能/F 块
F 应用程序块		块容器包含用户可以在 F-PB/F-FB/F-FC 中调用的 F 应用程序块。
	安全相关的 CPU-CPU 通讯	用于安全相关的 CPU-CPU 通讯的 F 应用程序块： • 在安全相关的 CPU-CPU 通讯中用于接收数据的 F_RCVDP 和 F_RCVS7 • 在安全相关的 CPU-CPU 通讯中用于发送数据的 F_SENDDP 和 F_SENDS7
	确认	用于通过操作员控制和监视系统确认故障安全的 F 应用程序块 F_ACK_OP
	定时器和计数器	F 应用程序块 F_TP、F_TON 和 F_TOF； F 块 F_CTU、F_CTD 和 F_CTUD
	数值线性转换	F 应用程序块 F_SCA_I
	具有误差分析的 1oo2 评估	F 应用程序块 F_1oo2DI
	标准的 F 功能	用于诸如双手操作监视、噪声抑制、急停、保护门监视、反馈回路监视等功能的 F 应用程序块。
	数据转换	F 应用程序块 F_BO_W、F_W_BO
	复制	F 应用程序块 F_INT_WR、F_INT_RD
	移位操作	F 应用程序块 F_SHL_W、F_SHR_W
F 系统块		包含自动插入安全程序的 F 系统块（F-SB）和 F 共享 DB 的块容器
	F 系统块	在编译安全程序以便从用户安全程序创建可执行安全程序时，F 系统块（F-SB）由 *S7 Distributed Safety* 可选软件自动插入。 用户切勿从 *F 系统块*块容器将 F 系统块插入 F-PB/F-FB/F-FC。同样，用户也不能修改（重命名）或删除 *Distributed Safety* F 库（V1）或用户项目块容器中的 F 系统块。
	F 共享 DB	包含安全程序的所有全局数据和 F 系统所需的附件信息的故障安全数据块。在编译安全程序时，自动插入和展开 F 共享 DB。用户可以使用 F 共享 DB（F_GLOBDB）的符号名，在标准用户程序中评估安全程序的某些数据。

参见

在 S7 Distributed Safety 中访问 F-I/O (页 71)

7.4 S7 F/FH Systems 中安全程序的结构

程序结构的表示

下图显示了 S7 F/FH Systems 安全程序的示意图结构。安全程序由 CFC 图表（具有分配给 F 运行组的安全块）组成。

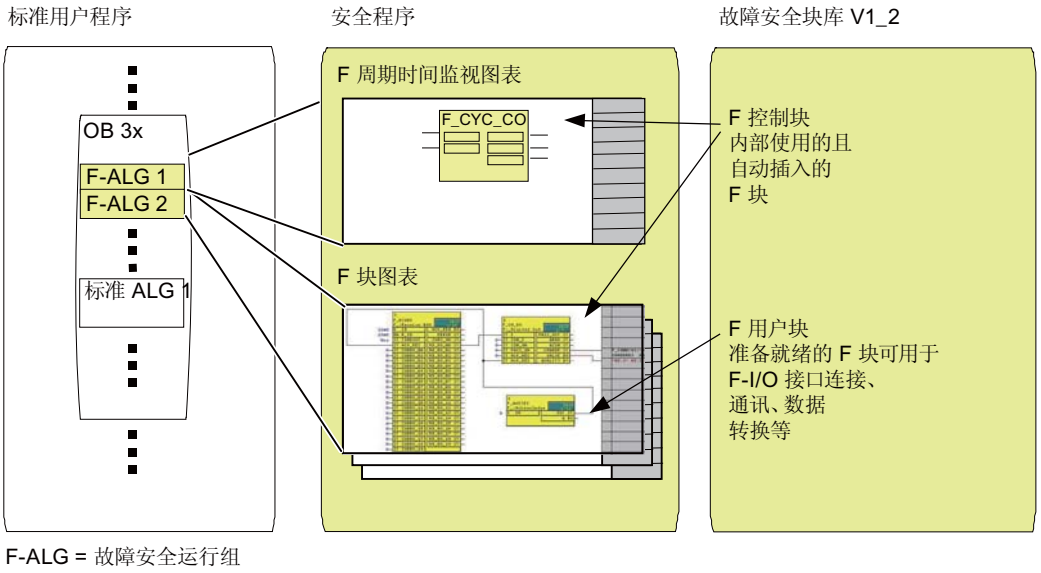


图 7-3 S7 F/FH Systems 中安全程序的组件

程序结构说明

安全程序包含 F 运行组和为其分配的图表。图表包含 F 块（包括其参数分配和互连）。

F 运行组由用户在 OB（最好在时间中断 OB [OB 30 至 OB 38]）的起始处插入。

时间中断 OB 的优点是其以固定的时间间隔中断执行标准用户程序的 OB 1 中的循环程序。即，在时间中断 OB 中，以固定的时间间隔调用和运行安全程序。

时间中断 OB 还可以包含分配其图表的标准运行组。

安全程序的连续功能图（CFC）

此安全程序至少需要两个连续功能图（CFC），如下所示：

- 一个图表用于各个时间中断 OB（带有 F 运行组）的 F 循环时间监视（编译安全程序时，由 *S7 F Systems* 自动插入安全程序中单独的 F 运行组）
- 一个或多个图表用于安全系统的其它 F 块

用户从*故障安全块* F 库的“F 用户块”块容器中选择 F 块，并将其插入图表、为其分配参数以及将其与其它 F 块互连。

故障安全块 F 库（V1_2）的故障安全块

故障安全块 F 库（V1_2）包含以下块容器：

- F 用户块
- F 控制块
- F 模拟块

下表显示了包含在块容器中的 F 块：

表格 7-3　　故障安全块 F 库（V1_2）的故障安全块

块容器	... 包含 F 块	功能
F 用户块		包含用户可以放置在 CFC 中、为其分配参数以及将其互连的 F 块的块容器。
	F 驱动程序	
	• F_CH_DI • F_CH_AI • F_CH_DO	用于 F-I/O 输入和输出信号的通道驱动程序
	转换	用于在标准用户程序和安全程序之间转换数据的 F 块
	• F_BO_FBO • F_I_FI • F_R_FR • F_TI_FTI	将标准数据类型转换为 F 数据类型

块容器	... 包含 F 块	功能
	• F_FBO_BO • F_FI_I • F_FR_R • F_FTI_TI	将 F 数据类型转换为标准数据类型
	• F_FR_FI	将 F 数据类型转换为 F 数据类型
	• F_CHG_R • F_CHG_BO	安全数据写入
	F_QUITES	通过操作员控制和监视系统进行的故障安全确认
F 用户块	**F 系统**块	
	• F_S_BO、F_S_R • F_S_BO、F_S_R	F 运行组之间的通讯
	• F_START	给出冷启动或重新启动（暖重启）的信号
	• F_PSG_M	选择性运行组中的划分
	通讯	
	• F_SENDBO、F_SENDR • F_RCVBO、F_RCVR	用于安全相关 CPU-CPU 通讯的 F 块
	数学标准功能	用于数学标准功能（例如算术、逻辑、多路复用等）的 F 块。
F 控制块	• F_CYC_CO • F_M_AI6 • F_M_DI24 • F_M_DI8 • F_M_DO10 • F_M_DO8 • F_PLK • F_PLK_O • F_SHUTDN • F_CHG_WS • ...	块容器包含在编译安全程序时由 *S7 F Systems* 调用和插入的 F 块，以便从用户安全程序中生成可执行安全程序。 用户切勿将 F 控制块的 F 块插入安全程序。同样地，用户也不能修改（重命名）或删除*故障安全块* F 库（V1_2）或用户项目块容器中的 F 块。
F 模拟块	模拟块	在使用 *PLCSim* 脱机模拟期间，来自*故障安全块* F 库（V1_2）的同名模拟块将覆盖安全程序的 F 块。这些 F 块仅适用于模拟过程，切勿下载到 F-CPU。

F 系统的监视和响应时间

A

A.1 引言

概述

本章提供了关于 S7 Distributed Safety 和 S7 F/FH Systems 的以下信息：

- 必须组态的与 F 相关的监视时间
- 指定监视时间时需遵循的规则
- 在计算 F 特定的最小监视时间和查找必需的时间信息时使用的公式
- 输入 F 相关的监视时间的位置
- 计算安全功能的最大响应时间需遵循的规则

计算的支持信息

为帮助您近似计算 F 系统的 F 特定的最小监视时间和最大响应时间，每个 F 系统均可使用 Microsoft Excel 文件计算该时间，如下所示：

- 对于 S7 Distributed Safety，可以在以下 Internet 地址中找到计算该时间的 Excel 计算文件：
  http://support.automation.siemens.com/WW/view/de/11669702/133100
- 对于 S7 F/FH Systems：在 *...\Siemens\STEP7\S7BIN\S7ftimea.xls* 目录中

其它信息

S7 Distributed Safety 和 S7 F/FH Systems 中，标准部分的监视和响应时间的计算与标准 S7-300 和 S7-400 自动化系统完全相同，在此不再赘述。有关该计算的说明，请参考 CPU 的硬件手册。

A.2 对监视时间进行组态

对 F 系统的监视时间进行组态

在 S7 Distributed Safety 中对安全程序监视时间的组态步骤与其在 S7 F/FH Systems 中的组态步骤相似。即，在某些情况下，您可以在 *STEP 7* 对话框中，将输入的监视时间作为 F 块参数，如以下部分所述。对于 F-CPU 和 F-I/O 之间的监视通讯，您可以在可用 F 模块、F-SM、故障安全 DP 标准从站或故障安全 I/O 标准设备的对象属性对话框的 *HW Config* 中，对响应时间进行组态。

对监视时间进行组态的规则

在对监视时间进行组态时，您必须考虑 F 系统的安全和可用性：

- 可用性：要确保在没有错误时不触发暂时监视，所选的监视时间必须足够长。
- 安全：要确保不超出过程安全时间，所选的监视时间必须足够短。

警告

为了**可靠地**检测脉冲，两次信号更改（脉冲宽度）之间的时间间隔必须大于相应的监视时间。

对监视时间进行组态的一般步骤

使用以下步骤对监视时间进行组态：

1. 对标准或 H 系统进行组态。
   请参考可用硬件手册和在线帮助系统，以获得所需的信息。
2. 对与可用性有关的 F 系统的特定监视时间进行组态。在以下或以下有关监视时间的相应部分中，列出用于计算最小监视时间的近似公式：
   - 对于 S7 Distributed Safety，可以在以下 Internet 地址中找到计算该时间的 Excel 计算文件：
     http://support.automation.siemens.com/WW/view/de/11669702/133100
   - 对于 S7 F/FH Systems：在 *...\Siemens\STEP7\S7BIN\S7ftimea.xls* 目录中
3. 使用这些 MS Excel 文件可以计算最大响应时间并确保不超出过程安全时间。如果需要，可减少 F 系统的特定监视时间。

A.3 S7 Distributed Safety 的 F 相关监视时间

要组态的监视时间

必须为 S7 Distributed Safety 组态以下监视时间：

监视的元素...	F 块/ 在 *STEP 7* 中	参数	参考
包含安全程序的 F 运行组的 F 周期时间	“Edit F-Runtime Groups”（编辑 F 运行组）对话框	最大周期时间	“F 周期时间的最小监视时间”
通过 PROFIsafe（PROFIsafe 监视时间）的 F-CPU 和 F-I/O 之间的安全相关的通讯，也针对安全相关的 I 从站-从站通讯	*HW Config* 中的 Object properties（对象属性）对话框	监视时间	“F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间”
安全相关的主站-主站通讯	F_SENDDP F_RCVDP	TIMEOUT TIMEOUT	“安全相关的主站-主站通讯的最小监视时间”
安全相关的主站-I 从站通讯	F_SENDDP F_RCVDP	TIMEOUT TIMEOUT	“安全相关的主站-I 从站通讯的最小监视时间”
安全相关的 I 从站-I 从站通讯	F_SENDDP F_RCVDP	TIMEOUT TIMEOUT	“安全相关的 I 从站-I 从站通讯的最小监视时间”
通过 S7 连接的安全相关的通讯	F_SENDS7 F_RCVS7	TIMEOUT TIMEOUT	“通过 S7 连接进行安全相关的通讯的最小监视时间”

用户不必组态 F 运行组之间进行安全相关的通讯的监视时间。

参见

F 周期时间的最小监视时间 (页 140)

通过 PROFIBUS DP 的 F-CPU 和 F-I/O 之间的或 I 从站和从站之间进行安全相关的通讯的最小监视时间 (页 141)

安全相关的主站-主站通讯的最小监视时间 (页 142)

安全相关的主站-I 从站通讯的最小监视时间 (页 143)

安全相关的 I 从站-I 从站通讯的最小监视时间 (页 143)

通过 S7 连接进行安全相关的通讯的最小监视时间 (页 144)

A.3.1 F 周期时间的最小监视时间

最大周期时间参数

可以在“Edit F-Runtime Groups”（编辑 F 运行组）对话框中指定 F 周期时间的监视时间。

要确保在没有导致 F-CPU 切换到 STOP 模式的故障时，F 周期时间的监视不响应，则“最大周期时间”参数设置必须大于关联 OB 的最大周期时间。

使用 CiR 扩展最大周期时间：

如果使用的是“在 RUN 模式下组态（CiR）”，则按照以下两个值中**较小**的一个扩展最大周期时间：

- F-CPU 的 CiR 同步时间

  F-CPU 的 CiR 同步时间是所有要同时进行更改的 DP 主站系统的 CiR 同步时间的总和。DP 主站系统的 CiR 同步时间显示在 *HW Config* 中相关 CiR 对象的 Properties（属性）对话框中。

- CiR 同步时间的上限

  上限的默认值为 1 s。您可以根据需要通过调用 SFC 104“CiR”来增大或减小该值。

有关 CiR 和最大周期时间的附加信息

- *STEP 7 在线帮助*：*“在使用 CiR 进行操作期间对系统进行更改”*
- *《用于 S7-300/400 系统功能及标准功能的 SIMATIC 系统软件》*手册
- 有关确定最大周期时间的说明，请参考您正在使用的 F-CPU 的手册

确定安全程序的运行时间

可以借助 Excel 文件计算安全程序的运行时间。可以在 Internet 网址 http://support.automation.siemens.com/WW/view/de/11669702/133100 上获取该 Excel 文件。

A.3.2 通过 PROFIBUS DP 的 F-CPU 和 F-I/O 之间的或 I 从站和从站之间进行安全相关的通讯的最小监视时间

PROFIsafe 监视时间 TPSTO

要确保在没有故障时监视不响应，选定的 PROFIsafe 监视时间 TPSTO 必须足够大：

TPSTO > TCImax + TFPROG + 2 × TDP_DLY + 2 × TTR + 2 × TSlave + TACK

时间定义

时间	定义	参考
TCImax	相关 OB 的最大周期时间	“F 周期时间的最小监视时间”
TFPROG	安全程序的最大运行时间 [1]	-
TDP_DLY	PROFIBUS CP（通讯处理器）的其它 DP 时间延迟	在 *HW Config* 中：CP 的对象属性，“Operating Mode”（工作模式）标签
TTR	DP 主站系统的最大目标转动时间（仅与分布式 F-I/O 相关）	在 *HW Config* 中： DP 主站系统的对象属性，总线参数
TSlave	仅与 ET 200M、ET 200S 和 ET 200pro 中的分布式 F-I/O 相关： 分布式 I/O 系统的最大响应时间，即 IM 及其背板总线的最大延迟	请参考 F-I/O 的手册以了解如何计算这些时间。
TACK	F-I/O 的最大确认时间（适用于 F-SM：在安全模式中）	可以在故障安全模块或 SM 的手册的技术规范中找到该时间。
[1] 仅与具有输入或输出的故障安全 I/O 相关		

检查以确定组态的 PROFIsafe 监视时间是否太短

请参考 S7 F/FH Systems 的“F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间”的相应部分中的信息。

通过 PROFINET IO 的 F-CPU 和 F-I/O 之间的通讯

使用随 S7 Distributed Safety 提供的 Microsoft Excel 文件计算 PROFINET IO 的最小监视时间。可以在 Internet 网址 `http://support.automation.siemens.com/WW/view/de/11669702/133100` 上的文档 `ID 19138505` 下获取该 `Excel` 文件。还请阅读 Excel 文件中的注释。

参见

F 周期时间的最小监视时间 (页 140)

F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间 (页 148)

A.3.3 安全相关的主站-主站通讯的最小监视时间

F_SENDDP 和 F_RCVDP 中的 TIMEOUT 参数

时间监视发生在使用*相同的*监视时间的 F 应用程序块 F_SENDDP 和 F_RCVDP 中，必须在这*两个* F 应用程序块（TIMEOUT 参数）中都为时间监视赋值。

要确保在没有故障时监视不响应，选定的 TIMEOUT 监视时间必须足够大。

TIMEOUT > T CI,F_SENDDP + T CI,F_RCVDP + 2 × TDP_DLY,F_SENDDP + 2 × TDP_DLY,F_RCVDP + 2 × TTR,F_SENDDP+ 2 × TTR,F_RCVDP + 2 × TCOPY

时间定义

时间	定义	参考
TCI,F_SENDDP	调用 F_SENDDP 的 OB 的最大周期时间	“F 周期时间的最小监视时间”
TCI,F_RCVDP	调用 F_RCVDP 的 OB 的最大周期时间	“F 周期时间的最小监视时间”
TDP_DLY,F_SENDDP	位于 F_SENDDP 一侧的 PROFIBUS CP（通讯处理器）的其它 DP 时间延迟	在 *HW Config* 中：CP 的对象属性，“Operating Mode”（工作模式）标签
TDP_DLY,F_RCVDP	位于 F_RCVDP 一侧的 PROFIBUS CP（通讯处理器）的其它 DP 时间延迟	CP 的对象属性，*HW Config* 中的“Operating Mode”（工作模式）标签
TTR,F_SENDDP	位于 F_SENDDP 一侧的 DP 主站系统的最大目标转动时间	在 *HW Config* 中： DP 主站系统的对象属性，总线参数
TTR,F_RCVDP	位于 F_RCVDP 一侧的 DP 主站系统的最大目标转动时间	在 *HW Config* 中： DP 主站系统的对象属性，总线参数
TCOPY	DP/DP 耦合器中的最大复制时间	位于 Internet 网址： http://www4.ad.siemens.de/view/cs/de/8610397

参见

F 周期时间的最小监视时间 (页 140)

A.3.4 安全相关的主站-I 从站通讯的最小监视时间

F_SENDDP 和 F_RCVDP 中的 TIMEOUT 参数

时间监视发生在使用*相同的*监视时间的 F 应用程序块 F_SENDDP 和 F_RCVDP 中，必须在这*两个* F 应用程序块（TIMEOUT 参数）中都为时间监视赋值。

要确保在没有错误时监视不响应，选定的 TIMEOUT 监视时间必须足够大。

TIMEOUT > T CI,F_SENDDP + T CI,F_RCVDP + 2 x TDP_DLY + 2 x TTR

时间定义

时间	定义	参考
TCI,F_SENDDP	调用 F_SENDDP 的 OB 的最大周期时间	“F 周期时间的最小监视时间”
TCI,F_RCVDP	调用 F_RCVDP 的 OB 的最大周期时间	“F 周期时间的最小监视时间”
TDP_DLY	PROFIBUS CP（通讯处理器）的其它 DP 时间延迟	CP 的对象属性，*HW Config* 中的 “Operating Mode”（工作模式）标签
TTR	DP 主站系统的最大目标转动时间	在 *HW Config* 中：DP 主站系统的对象属性，总线参数

A.3.5 安全相关的 I 从站-I 从站通讯的最小监视时间

“安全相关的主站-I 从站通讯的最小监视时间”中提供的信息在此适用。

A.3.6 通过 S7 连接进行安全相关的通讯的最小监视时间

F_SENDS7 和 F_RCVS7 中的 TIMEOUT 参数

时间监视发生在使用*相同的*监视时间的 F 应用程序块 F_SENDS7 和 F_RCVS7 中，必须在这*两个* F 应用程序块（TIMEOUT 参数）中都为时间监视赋值。

要确保在没有错误时监视不响应，选定的 TIMEOUT 监视时间必须足够大。

使用随 S7 Distributed Safety 提供的 Microsoft Excel 文件来确定 PROFINET IO 推荐的 TIMEOUT 监视时间。可以在 Internet 网址 http://support.automation.siemens.com/WW/view/de/11669702/133100 上的文档 ID 19138505 下获取该 Excel 文件。

A.3.7 F 运行组之间进行安全相关的通讯的监视时间

根据“最大周期时间”（“Edit F-Runtime Groups”[编辑 F 运行组] 对话框）的值来自动确定 F 运行组之间进行安全相关的通讯的监视时间。

监视时间 = 第 1 个 F 运行组的最大周期时间 + 第 2 个 F 运行组的最大周期时间

A.4 S7 F/FH Systems 的 F 相关监视时间

要组态的监视时间

必须为 S7 F/FH Systems 组态以下监视时间：

监视的元素...	F 块/ 在 *HW Config* 中	参数	参考...
包含安全程序的时间中断 OB 的 F 周期时间	F_CYC_CO	MAX_CYC	“F 周期时间的最小监视时间”
通过 PROFIsafe（PROFIsafe 监视时间）的 F-CPU 和 F-I/O 之间的安全相关的通讯	*HW Config* 中的 Object properties（对象属性）对话框	“监视时间”	“F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间”
F-CPU 之间的安全相关的通讯	F_RCVR、F_RCVBO F_SENDR、F_SENDBO	TIMEOUT	“F-CPU 之间进行安全相关的通讯的最小监视时间”
F 运行组之间进行安全相关的通讯	F_R_R F_R_BO	TIMEOUT	“F 运行组之间进行安全相关的通讯的最小监视时间”

参见

F 周期时间的最小监视时间 (页 146)

F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间 (页 148)

F-CPU 之间进行安全相关的通讯的最小监视时间 (页 150)

F 运行组之间进行安全相关的通讯的最小监视时间 (页 151)

A.4.1 F 周期时间的最小监视时间

F_CYC_CO 中的 MAX_CYC 参数

在 F 块 F_CYC_CO 的 MAX_CYC 输入参数中为监视时间赋值。编译安全程序时，*S7 F Systems* 将把 F_CYC_CO F 块自动插入安全程序下面一个单独的 F 运行组中。定位 F_CYC_CO 块时，系统将显示一个对话框以便输入 MAX_CYC 参数。

要确保在没有错误时监视不响应，选定的 MAX_CYC 必须大于关联 TCImax 时间中断 OB 的最大周期时间：

MAX_CYC > TCImax

关联 TCImax 时间中断 OB 的最大周期时间至少和 TCI 时间中断 OB 的已组态周期时间一样大。在 S7 FH Systems 中，更新时还必须注意优先级等级的最大禁用时间 > 15（TP15）。

使用 CiR 扩展最大周期时间：

如果使用的是“在 RUN 模式下组态（CiR）”，则按照以下两个值中**较小**的一个扩展最大周期时间：

- F-CPU 的 CiR 同步时间

  F-CPU 的 CiR 同步时间是所有要同时进行更改的 DP 主站系统的 CiR 同步时间的总和。DP 主站系统的 CiR 同步时间显示在 *HW Config* 中相关 CiR 对象的 Properties（属性）对话框中。

- CiR 同步时间的上限

  上限的默认值为 1 s。您可以根据需要通过调用 SFC 104“CiR”来增大或减小该值。

因此，可以应用以下近似公式：

公式	用于何处？
TCImax ≈ TCI + MIN(TCiR; 2500)[2]	S7 F Systems 中
TCImax ≈ MAX (TCI; TP15)[1] + MIN(TCiR; 2500)[2]	在带时间中断 OB（**带**）特别处理功能的 S7 FH Systems 中
TCImax ≈ TCI + TP15 + MIN(TCiR; 2500)[2]	在带时间中断 OB（**不带**特别处理功能）的 S7 FH Systems 中
[1] 使用两个值中较大的一个 [2] 使用两个值中较小的一个	

时间定义

时间	定义	参考
TCI	时间中断 OB 的已组态周期时间	在 *HW Config* 中：CPU 的对象属性，“时间中断，类型”
TP15	优先级等级的最大锁定时间 > 15	在 *HW Config* 中：CPU 的对象属性，“H 参数”
TCiR	F-CPU 的 CiR 同步时间： 所有要同时进行更改的 DP 主站系统的 CiR 同步时间的总和。	在 *HW Config* 中：CiR 对象的对象属性 如果未使用 CiR，则在公式中输入“0”。

进行特别处理的时间中断 OB

进行特别处理的“时间中断 OB”是 S7 FH Systems 中 F-CPU 的 H 参数。该参数包括禁用所有中断后，操作系统更新保留值时特别调用的时间中断 OB 的编号。通常，输入的编号是最高优先级的时间中断 OB（在 CFC 中，将安全程序的 F 块分配给该 OB）。

注意

要确保已启用优先级等级的最大禁用时间 > 15 的监视，必须在 *HW Config* 中的 CPU 的对象属性的“H-Parameters”（H 参数）标签中为该参数赋值。

有关 CiR 的更多信息

- *STEP 7 在线帮助*：“*系统在使用 CiR 进行操作期间更改*”
- *《用于 S7-300/400 系统功能及标准功能的 SIMATIC 系统软件》*手册
- *《可编程控制器 S7 F/FH》*手册

A.4.2 F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间

PROFIsafe 监视时间 TPSTO

要确保在没有故障时监视不响应，选定的 PROFIsafe 监视时间 TPSTO 必须足够大：

TPSTO > MAX(TCImax ; TCI + TDP_FD)* + 2 × TDP_DLY + 2 × TTR + 2 × TSlave + TACK + TDP_SO + TSLAVE_SO

* 使用最大值

时间定义

时间	定义	参考
TCImax	相关时间中断 OB 的最大周期时间	“F 周期时间的最小监视时间”
TCI	时间中断 OB 的已组态周期时间	在 *HW Config* 中：CPU 的对象属性，“时间中断，类型”
TDP_FD	最大 DP 错误检测时间	在 *HW Config* 中：DP 主站系统的对象属性，总线参数，“H-parameters”（H 参数）标签
TDP_DLY	PROFIBUS CP（通讯处理器）的其它 DP 时间延迟	在 *HW Config* 中：CP 的对象属性，“Operating Mode”（工作模式）标签
TTR	DP 主站系统的最大目标转动时间	在 *HW Config* 中：DP 主站系统的对象属性，总线参数
TSlave	仅与 ET 200M、ET 200S 和 ET 200pro 中的分布式 F-I/O 相关： 分布式 I/O 系统的最大响应时间，即 IM 及其背板总线的最大延迟	请参考 F-I/O 的手册以了解如何计算这些时间。
TACK	F-I/O 的最大确认时间（适用于 F-SM：在安全模式中）	可以在 *《ET 200S 故障安全模块》*、*《ET 200eco 故障安全 I/O 模块》* 和 *《S7-300 故障安全信号模块》* 手册中的 F 模块或 F-SM 的技术规范中找到该时间。
TDP_SO	最大 DP 切换时间	在 *HW Config* 中：DP 主站系统的对象属性，总线参数，“H-parameters”（H 参数）标签
TSLAVE_SO	切换式 I/O 的激活通讯通道的最大切换时间（仅与 S7 FH Systems 相关）	可以在 *《ET 200M 分布式 I/O 系统》* 手册中的切换式 DP 从站（ET 200M）的技术规范中找到该时间。

检查以确定组态的 PROFIsafe 监视时间是否太短

注意

调试 F 系统时，可在安全模式中执行检查以确定已组态 PROFIsafe 监视时间是否太短。如果您想要确保已组态的监视时间超出最小监视时间很长时间，那么该检查将十分有用。这样，可以避免任何偶尔发生的监视时间错误。

操作步骤：

1. 插入 F-I/O（稍后进行系统操作时不需要的一个）。
2. 为此 F-I/O 赋一个较短的监视时间（与为系统的 F-I/O 赋的监视时间相比）。
3. 如果添加的 F-I/O 故障且发出“超出安全消息帧的监视时间”诊断信号，则表明该时间在最小可能 PROFIsafe 监视时间以下。
4. 将添加的 F-I/O 的监视时间增大到其刚好不再出现故障的时间即可。该监视时间与最小可能监视时间近似符合。

条件：

要插入的 F-I/O 和要检查其 PROFIsafe 监视时间的 F-I/O 必须具有以下共性：

- 它们必须插入同一机架
- 站必须位于同一 DP 子网上
- 它们必须由 F 驱动程序块在同一 F 运行组中进行寻址

提示：

对于进行调试后在操作期间将要修改或扩展的系统，将添加的 F-I/O 保持在适当的位置，可能十分有用。如果时间特性中发生更改，该 F-I/O 随后将提供预警，使您可避免在过程应用中由该 F-I/O 触发的过程停车。

参见

F 周期时间的最小监视时间 (页 146)

A.4.3 F-CPU 之间进行安全相关的通讯的最小监视时间

F_SENDR 和 F_RCVR 或者 F_SENDBO 和 F_RCVBO 中的 TIMEOUT 参数

时间监视发生在使用*相同*监视时间的 F 块 F_SENDR 和 F_RCVR 或者 F_SENDBO 和 F_RCVBO 中，必须在这*两个* F 块（TIMEOUT 参数）中都为时间监视赋值。

要确保在没有错误时 F_SENDR 或 F_SENDBO（或者 F_RCVR 或 F_RCVBO）中的监视不响应，则 TIMEOUT 监视时间设置必须足够大：

TIMEOUT > T CI,F_SEND + T CI,F_RCV + MAX(TDelay,F_SEND; TDelay,F_RCV)[1]
+ 2 × TUSEND + MAX(MIN(TCiR,F_SEND; 2500);MIN(TCiR,F_RCV; 2500))[1]

[1] 使用两个值中较大的一个

时间定义

时间	定义	参考
TCI,F_SEND	调用 F_SENDBO 或 F_SENDR 的时间中断 OB 的已组态周期时间	在 *HW Config* 中：CPU 的对象属性，“时间中断，类型”
TCI,F_RCV	调用 F_RCVBO 或 F_RCVR 的时间中断 OB 的已组态周期时间	在 *HW Config* 中：CPU 的对象属性，“时间中断，类型”
TDelay,F_SEND	在调用 F_SENDBO 或 F_SENDR 的 FH 系统中更新保留值时的最大通讯延迟	在 *HW Config* 中：发送 CPU 的对象属性，“H-parameters”（H 参数）标签
TDelay,F_RCV	在调用 F_RCVBO 或 F_RCVR 的 FH 系统中更新保留值时的最大通讯延迟	在 *HW Config* 中：接收 CPU 的对象属性，“H-parameters”（H 参数）标签
TUSEND	USEND 的最大响应时间 • 为 **F_SENDBO** 提供 48 个字节的用户数据 • 为 **F_SENDR** 提供 88 个字节的用户数据	请访问 Internet 以获取有关信息（请参阅以下内容）
TCiR,F_SEND	调用 F_SENDBO 或 F_SENDR 的 F-CPU 的 CiR 同步时间： 所有要同时进行更改的 DP 主站系统的 CiR 同步时间的总和。	在 *HW Config* 中：CiR 对象的对象属性 如果未使用 CiR，则在公式中输入“0”
TCiR,F_RCV	调用 F_RCVBO 或 F_RCVR 的 F-CPU 的 CiR 同步时间： 所有要同时进行更改的 DP 主站系统的 CiR 同步时间的总和。	在 *HW Config* 中：CiR 对象的对象属性 如果未使用 CiR，则在公式中输入“0”

确定 TUSEND

可在以下 Internet 地址（文档 ID 1651770）在线获取计算 TUSEND 值的工具：

http://www4.ad.siemens.de/view/cs/de/1651770

注意

为了在 S7 FH Systems 中更新保留值时启用最大通讯延迟监视，必须为 *HW Config* 中的此参数（CPU 的对象属性，“H-Parameters”[H 参数] 标签）赋值。

不支持在两个 F-CPU 中同步更新。

A.4.4 F 运行组之间进行安全相关的通讯的最小监视时间

F_R_BO 或 F_R_R 中的 TIMEOUT 参数

在 F 块 F_R_BO 或 F_R_R 中进行时间监视，并且在 TIMEOUT 输入参数中进行赋值。

要确保在没有故障时时间监视不响应，选定的 TIMEOUT 监视时间必须至少和 F_S_R 或 F_S_BO 和 F_R_R 或 F_R_BO 的两个最大时间中断周期时间中较大的时间一样大：

TIMEOUT > MAX (TCImax, F_S; TCImax, F_R)[1]

[1]TIMEOUT > 两个值中较大的一个

时间定义

时间	定义	参考
TCImax,F_S	调用 F_S_BO 或 F_S_R 的时间中断 OB 的最大周期时间	请参阅 *“F 周期时间的最小监视时间”*
TCImax,F_R	调用 F_R_BO 或 F_R_R 的时间中断 OB 的最大周期时间	请参阅 *“F 周期时间的最小监视时间”*

参见

F 周期时间的最小监视时间 (页 146)

A.5 安全功能的响应时间

响应时间的定义

响应时间从检测输入信号开始，到修改选通输出信号时结束。

波动范围

实际响应时间介于最小响应时间和最大响应时间之间。在系统组态中必须始终考虑最大响应时间。

安全功能的最大响应时间规则

安全功能的最大响应时间必须小于该过程的过程安全时间。

过程安全时间的定义

过程安全时间是一段时间间隔，在此期间，可以不管该过程，而不会伤害操作人员或破坏环境。

在过程安全时间内，任何类型的 F 系统过程控制都是可容错的。即在此期间，F 系统可能不正确地控制其过程或者甚至可以不执行任何控制。过程的过程安全时间取决于过程类型，必须视各自情况而定。

计算响应时间的步骤

可从以下地方获取计算安全功能的最大响应时间的公式：

- 对于 S7 Distributed Safety，为 Internet 网址
  http://support.automation.siemens.com/WW/view/de/11669702/133100
- 对于 S7 F/FH Systems，在 *...\Siemens\STEP7\S7BIN\S7ftimea.xls* 目录中

使用这些 MS Excel 文件的其中一个文件来计算安全功能的最大响应时间并确保不超出过程安全时间。
如果需要，减小指定的 F 系统监视时间（请参阅 *"S7 Distributed Safety 的 F 相关监视时间"*和 *"S7 F/FH Systems 的 F 相关监视时间"*）。

词汇表

1oo1 评估

-> 1oo1 评估

1oo1 评估是一种 -> 传感器评估，在其中一个传感器通过一条通道连接到 -> F-I/O。

1oo1 评估

-> 1oo1 评估

1oo1 评估是一种 -> 传感器评估，在其中一个传感器通过一条通道连接到 -> F-I/O。

1oo2 评估

-> 1oo2 评估

1oo2 评估是一种 -> 传感器评估，在其中由一个双通道传感器或两个单通道传感器占用两个输入通道。在内部比较输入信号是对等还是非对等。

1oo2 评估

-> 1oo2 评估

1oo2 评估是一种 -> 传感器评估，在其中由一个双通道传感器或两个单通道传感器占用两个输入通道。在内部比较输入信号是对等还是非对等。

CFC

连续功能图（CFC）

1. CFC 是具有技术功能（块）的图形互连的功能图。
2. CFC 为自动任务的面向技术的、基于图形的组态提供了软件包（CFC 编辑器）。CFC 用于从准备就绪的块创建全面的软件结构（连续功能图）。

CiR

CiR（RUN 模式中的组态）指操作期间进行的系统修改。通过 CiR 在 RUN 模式中进行的系统修改，使得组态更改可以在 RUN 模式中在具有分布式 I/O 的系统的多个部分中进行。因此该过程将为一个短暂的可分配时间段暂停。在此时间段内，该过程输入保持其最后的值。

CRC

周期性冗余检查 -> CRC 签名

CRC 签名

通过包含在安全消息帧中的 CRC 签名保护 -> 安全消息帧中的过程数据的有效性、分配的地址引用的精确性和安全相关的参数。

DP/DP 耦合器

DP/DP 耦合器是一种设备，用于在 S7 Distributed Safety 中耦合不同 -> F-CPU 中安全程序之间的 -> 安全相关的主站-主站通讯所需的两个 PROFIBUS DP 子网。

通过 DP/DP 耦合器，在安全相关的主站-主站通讯中涉及到两个（或更多）F-CPU。每个 F-CPU 均通过其 PROFIBUS DP 接口链接到 DP/DP 耦合器。

ES

工程系统（ES）：工程系统是基于 PC 的组态系统，可以对要处理的任务采取便捷、可视化的过程控制系统自适应。

F 共享 DB

S7 Distributed Safety：包含 -> 安全程序的所有全局数据和 F 系统所需的附加信息的故障安全数据块。编译 -> 安全程序时，F 共享 DB 将自动插入并进行扩展。使用 F 共享 DB 的符号名（F_GLOBDB），用户可以在 -> 标准用户程序中计算 -> 安全程序的某些数据。

F 块

-> 安全程序的故障安全块

F 属性

S7 Distributed Safety：所有与 -> 安全程序关联的 -> F 块都具有 F 属性（在“Safety Program”[安全程序] 对话框中，F 块符号都标有“F”）。成功编译 -> 安全程序后，仅 -> 安全程序的块具有 F 属性。

F 应用程序块

S7 Distributed Safety：在 *Distributed Safety* F 库中，包含 F 应用程序块的块容器。

在 Distributed Safety F 库中，具有准备就绪功能的 F 块（F-FB、F-FC）。在 -> F-PB 中以及在其它 -> F-FB 和 -> F-FC 中，用户可以调用 F 应用程序块。

F 应用程序块

S7 Distributed Safety：在 *Distributed Safety* F 库中，包含 F 应用程序块的块容器。

在 Distributed Safety F 库中，具有准备就绪功能的 F 块（F-FB、F-FC）。在 -> F-PB 中以及在其它 -> F-FB 和 -> F-FC 中，用户可以调用 F 应用程序块。

F 控制块

S7 F/FH Systems：*故障安全块* F 库的块容器包含编译 -> 安全程序时自动调用/添加的 -> F 块以从用户编写的安全程序生成可执行安全程序。

F 数据类型

S7 F/FH Systems：-> 标准用户程序和 -> 安全程序使用不同的数据格式。在安全程序中使用安全相关的 F 数据类型。

F 模块

-> 故障安全模块

F 模块驱动程序

S7 F/FH Systems：F 模块驱动程序可确保 -> 安全程序和 -> F-I/O 之间的 -> PROFIsafe 通讯。在安全程序中，该驱动程序自动进行定位和互连。

F 模拟块

S7 F/FH Systems：包含模拟块的故障安全块库的块容器。-> *PLCSim* 离线模拟期间，-> 安全程序的 -> F 块由 F 库的模拟块使用相同的名称覆盖。

F 用户块

S7 F/FH Systems：*故障安全块*库的块容器包含用户可以在 -> 连续功能图（CFC）中定位、分配参数和互连的 -> F 块。

F 系统

-> 故障安全系统

F 系统块

S7 Distributed Safety：包含 -> F-SB 和 -> F 共享 DB 的 *Distributed Safety* 库的块容器。

-> F-SB

F 系统块

S7 Distributed Safety：包含 -> F-SB 和 -> F 共享 DB 的 *Distributed Safety* 库的块容器。

-> F-SB

F 运行组

创建 -> 安全程序后，无法将 -> F 块
直接插入任务/OB 中，但是必须将它们插入 F 运行组中。安全程序由一个或两个 F 运行组（S7 Distributed Safety）或者若干个 F 运行组（S7 F/FH Systems）组成。

F 运行许可证

-> F-CPU

F 通讯 DB

S7 Distributed Safety：用于通过 S7 连接进行安全相关的 CPU-CPU 通讯的故障安全数据块。

F 通道驱动程序

S7 F/FH Systems：F 通道驱动程序可以提供安全格式的过程数据。用户必须在 -> 安全程序中定位和互连 F 通道驱动程序。

F 驱动程序块

F 驱动程序块用于从 -> F-I/O 输入 AS 值/将 AS 值输出到 -> F-I/O。该块构成了面向该过程的软件接口、将实际值转换为过程数据（反之亦然），并且还提供有关硬件寻址可用性的信息。

在 S7 F/FH Systems 中，使用 F 驱动程序块的输入和输出进行 -> 安全相关的通讯。用户必须在 -> F 运行组的 -> 连续功能图（CFC）中定位和互连特殊 F 驱动程序块。

F-CALL

S7 Distributed Safety：-> 安全程序的“F 调用块”。F-CALL 作为 FC 由用户使用“F-CALL”编程语言进行创建；“F-CALL”无法进行编辑。F-CALL 从 -> 标准用户程序调用 -> F 运行组。它包含对 -> F-PB 的调用和对自动添加的 F 运行组的 F 块（-> F-SB、-> 自动生成的 F 块、-> F 共享 DB）的调用。

F-CPU

F-CPU 是中央处理单元，具有可用于 S7 Distributed Safety/S7 F/FH Systems 的故障安全功能。对于 S7 F/FH Systems，F 运行许可证允许中央处理单元用作 F-CPU。即，它可以执行安全程序。对于 S7 Distributed Safety，不需要 F 运行许可证。-> 标准用户程序也可在 F-CPU 中运行。

F-DB

S7 Distributed Safety：可以在整个 -> 安全程序中读取和写入的可选故障安全数据块。

F-FB

S7 Distributed Safety：用户在其中使用 -> F-FBD 或 -> F-LAD 对 -> 安全程序进行编程的故障安全功能块（具有实例 DB）。

F-FBD

针对 S7 Distributed Safety 中 -> 安全程序的编程语言。*STEP 7* 中的标准 FBD/LAD 编辑器用于进行编程。

F-FC

S7 Distributed Safety：用户在其中使用 -> F-FBD 或 -> F-LAD 对 -> 安全程序进行编程的故障安全 FC。

F-I/O

F-I/O 是 SIMATIC S7 中可用的故障安全输入和输出的组标识，用于在 S7 Distributed Safety 和 S7 F/FH Systems 故障安全系统中进行集成。可以使用以下 F-I/O：

- -> ET 200eco 故障安全 I/O 模块
- S7-300 故障安全信号模块（-> F-SM）
- -> 故障安全模块 ET 200S 和 ET 200pro（仅限于 S7 Distributed Safety 的 ET 200pro）
- -> 故障安全 DP 标准从站（仅限于 S7 Distributed Safety）
- -> 故障安全 IO 标准设备（仅限于 S7 Distributed Safety）

F-I/O DB

S7 Distributed Safety：S7 Distributed Safety 中 -> F-CPU 的 -> F-I/O 的故障安全数据块。在 *HW Config* 中编译程序时，为每个 F-I/O 自动生成一个 F-I/O DB。F-I/O DB 包含用户可以在 -> 安全程序中计算的变量或者可以或必须写入的变量：

- 用于重新集成 F-I/O 跟踪通讯错误、F-I/O 故障或通道故障
- 如果安全程序的特殊状态（例如，组钝化）的结果是必须将 F-I/O 钝化
- 用于重新分配 -> 故障安全 DP 标准从站的参数
- 为了评估故障安全值或过程数据是否为输出

F-LAD

-> F-FBD

F-PB

S7 Distributed Safety：用于 -> 安全程序的故障安全编程的“引导 F 块”。F-PB 是用户分配给
-> F 运行组的 -> F-CALL 的
-> F-FB 或 F-FC。

F-PB 包含 F-FBD 或 F-LAD 安全程序，用于程序结构化的其它 -> F-FB/F-FC 的所有调用以及 *Distributed Safety* F 库的 F 应用程序块的块容器的所有 -> F 应用程序块。

F-SB

S7 Distributed Safety：为了从用户的安全程序创建可执行安全程序，编译 -> 安全程序时自动调用/插入的故障安全系统块。

F-SM

F-SM 是 S7-300 的信号模块，可以用于在 S7 Distributed Safety 或 S7 F/FH Systems 故障安全系统中进行安全相关的操作（在 -> 安全模式中）。这些模块具有集成的 -> 安全功能。

MSR

仪表和控制技术

OBT

光学总线端子（OBT）：用于将无集成光学接口的单个 PROFIBUS DP 设备或 RS 485 段连接至光学 PROFIBUS DP 的设备。

OLM

光连接模块（OLM）：用于光纤接口以将电气信号转换为光学信号（反之亦然）的设备。

OP

操作员面板（OP）：用于操作和监视设备和系统的可编程 HMI 设备。

OS

操作员站（OS）：用于操作和监视设备和系统的可组态操作员站。

PCS 7

PCS 7 是基于选定的 SIMATIC 组件的过程控制系统，这些组件已为用于控制系统而经过优化。此外，还有一些增强功能可以确保在设计到运行期间，某过程和仪表控制系统所需的控制系统特定的系统特性和功能的可用性。

PROFINET IO

在 PROFINET 的框架内，PROFINET IO 是实现模块化、分布式应用程序的通讯原理。

使用 PROFINET IO 可以创建自动化解决方案，就像使用 PROFIBUS 创建一样。

PROFINET IO 是基于自动化设备的 PROFINET 标准和 *STEP 7* 工程工具而实现的。

也就是说，无论是正在组态 PROFINET 设备还是 PROFIBUS 设备，在 *STEP 7* 中的应用程序视图都相同。如果使用 PROFINET IO 的扩展块和系统状态列表，则对 PROFINET IO 和 PROFIBUS DP 来说，编写用户程序基本是相同的。

PROFINET IO 控制器

PROFINET IO 控制器是通过连接的 IO 设备进行寻址的设备。即：IO 控制器与分配的现场设备交换输入和输出信号。IO 控制器通常是运行自动化程序的控制器。

PROFINET IO 管理程序

用于调试和诊断的 PG/PC 或 HMI 设备。

具有已分配 PROFINET IO 设备的 PROFINET IO 控制器。

PROFINET IO 设备

PROFINET IO 设备是分配到其中一个 IO 控制器（例如，远程 IO、阀终端、变频器和交换机）的分散现场设备

PROFIsafe

用于 -> 安全程序和 -> F 系统中的 -> F-I/O 之间通讯的安全相关的 PROFIBUS DP/PA 和 PROFINET IO 总线配置文件。

PROFIsafe 地址

每个 -> F-I/O 都具有一个 PROFIsafe 地址。PROFIsafe 地址必须在 *STEP 7 HW Config* 中进行组态，并通过故障安全 I/O 上的交换机进行设置。

PROFIsafe 监视时间

F-CPU 和 F-I/O 之间进行安全相关的通讯的最小监视时间

S7-PLCSIM

使用 S7-PLCSIM 可以在编程设备或 PC 上的模拟自动化系统中测试和编辑程序。由于模拟完全发生在 STEP 7 中，因此无需任何硬件（CPU、I/O）。

WinCC

WinCC 是工业和技术中立系统，用于生产和过程自动化中的可视化和控制任务。

WinCC 提供行业标准的功能模块用于图形表示、传送消息、存档和记录功能。WinCC 以其强大的过程接口、快速的图像更新和可靠的数据存档来确保高可用性。

专家

通常是一个经过认证的系统，即系统的安全接受测试通常由独立的专家（例如，来自 TueV）来实施。

主站保留切换

在 S7 FH Systems 中，主站跳转到 STOP 模式时，将触发主站保留切换。即，系统从主站 CPU 切换至保留 CPU。

传感器

传感器用于精确测量路径、位置、速度、转动速度、质量等。

传感器评估

有两种类型的传感器评估：

- -> 1oo1 评估 — 读取传感器信号一次
- -> 1oo2 评估 — 由相同 -> F I/O 读取传感器信号两次，并对其进行内部比较。

似然性检查

似然性检查用于检查似然性信号。
必须确保过程数据元素位于用户指定的范围内。

在 -> F 系统中：用户必须在 -> 安全程序中执行似然性检查，以确保将数据从 -> 标准用户程序传送至安全程序时不会发生危险情况。

关闭期

关闭期发生在关闭测试期间和整个位模式测试期间。输出处于活动状态时，测试相关 0 信号将从故障安全输出模块切换至输出位。然后暂时关闭输出（关闭期）。足够慢的执行器对此无响应，仍处于打开状态。

冗余，可用性增强

可用性增强的冗余指确保组件即使在发生硬件故障的情况下也能继续工作的组件冗余。

冗余，安全性增强

安全性增强的冗余指通过比较的方式检测硬件故障的组件冗余，例如，-> F-I/O 中的 -> 1oo2 评估。

冗余切换式 I/O

在 -> 安全模式中，冗余切换式 I/O 是 S7 FH Systems 的组态变量以增加可用性。-> F-CPU、PROFIBUS DP 和 -> F-I/O 是冗余的。如果出现故障，F-I/O 将不可再用。

单通道 I/O

在 -> 安全模式中，单通道 I/O 是 S7 Distributed Safety/S7 F Systems 的组态变量。-> F-CPU 和 -> F-I/O 都不是冗余的。如果出现故障，F-I/O 将不可再用。

单通道切换式 I/O

在 -> 安全模式中，单通道切换式 I/O 是 S7 FH Systems 的组态变量以增加可用性。-> F-CPU 是冗余的而 -> F-I/O 不是冗余的，如果出现故障，则系统将切换至其它 F-CPU。如果出现故障，F-I/O 将不可再用。

取消激活的安全模式

取消激活的安全模式指为进行测试、调试等而临时取消激活 -> 安全模式。

无论何时取消激活安全模式，都必须通过其它有组织的措施（例如，操作监视和手动安全关闭）确保系统的安全。

可用性

可用性是系统在特定的时间点工作的可能性。可以通过冗余（例如，通过在同一测量点使用 -> 冗余 F-I/O 和/或使用多个 -> 传感器）增加可用性。

安全保护装置

安全保护装置用于保护 -> F-SM，以避免发生故障时可能出现的过压。安全保护装置必须用于 SIL3/Cat.4 应用程序：

- 通常，使用铜质电缆配置 PROFIBUS DP 时
- 使用光纤电缆配置 PROFIBUS DP 以及合并 PROFIBUS DP 时，需要运行一个 ET 200M 中的标准信号模块和 -> F-SM。

安全功能

安全功能是内置于 -> F-CPU 和 -> F-I/O 中的机制，允许在 -> S7 Distributed Safety 或 S7 F/FH Systems 故障安全系统中使用这些功能。

符合 IEC 61508：由安全设备实现的功能，以便在发生特殊故障时将系统维持在 -> 安全状态或置于安全状态（-> 用户安全功能）。

安全模式

1. 安全模式是 -> F-I/O 的工作模式，允许使用 -> 安全消息帧进行 -> 安全相关的通讯。-> 故障安全模块 ET 200S、ET 200pro 和 ET 200eco 仅适用于安全模式。-> F-SM S7-300 可用于 -> 标准模式或安全模式（除 SM 326、DO 8 × DC 24V/2A 之外）。
2. -> 安全程序的工作模式。在安全程序的安全模式中，激活故障检测和故障响应的所有安全机制。在安全模式中，运行期间无法修改安全程序。用户可以取消激活安全模式（-> 取消激活的安全模式）。

安全消息帧

在 -> 安全模式中，数据通过安全消息帧在 -> F-CPU 和 -> F-I/O 之间传送，或者通过安全相关的 CPU 到 CPU 通讯在 F-CPU 之间传送。

安全状态

在 -> F 系统中，安全概念的基本原理是存在适用于所有过程变量的安全状态。例如，对于数字 F-I/O，该值为“0”。

安全相关的通讯

安全相关的通讯是用于交换故障安全数据的通讯。

安全程序

安全程序是安全相关的用户程序。

安全等级

安全集成等级（SIL）符合 IEC 61508 和 EN 50129。安全集成等级越高，预防系统故障以及管理系统故障和硬件故障的措施越严格。

可在 -> 安全模式中使用 -> S7 Distributed Safety 和 S7 F/FH Systems 故障安全系统（最高可达 SIL3）。

打开期

打开期发生在整个位模式测试期间。输出处于取消激活状态时（输出信号“0”），测试相关“1”信号将从故障安全输出模块切换至输出位。然后暂时打开输出（打开期）。足够慢的执行器对此无响应，仍处于关闭状态。

执行器

执行器可以是功率继电器或装载时进行切换的接触器，或者本身可以是负载（例如，直接控制的电磁阀）。

控制系统

控制系统是合并和显示单个分布式控制系统的更高级别功能的系统。

故障响应功能

-> 用户安全功能

故障响应时间

F 系统的最大故障响应时间是从发生故障到所有受影响的故障安全输出做出安全响应之间的时间。对于整个 F 系统：最大故障响应时间是从任意 F-I/O 中发生故障到关联的故障安全输出做出安全响应之间的时间。

对于输入：最大故障响应时间是从发生故障到背板总线做出安全响应之间的时间。

对于数字输出：最大故障响应时间是从发生故障到数字输出做出安全响应之间的时间。

故障安全 DP 标准从站

故障安全 DP 标准从站是根据 DP 协议在 PROFIBUS 上进行操作的标准从站。它们的特性必须符合 IEC 61784-1:2002 Ed1 CP 3/1 和 PROFIsafe 总线配置文件。GSD 文件用于组态故障安全 DP 标准从站。

故障安全 I/O 模块

故障安全 I/O 模块是 ET 200eco I/O 模块，可以用于在 S7 Distributed Safety 或 S7 F/FH Systems 故障安全系统中进行安全相关的操作（在 -> 安全模式中）。该 I/O 模块具有集成的 -> 安全功能。

这些模块具有集成的 -> 安全功能。

故障安全 IO 标准设备

故障安全 IO 标准设备是根据 IO 协议在 PROFINET 上进行操作的标准设备。它们根据标准 IEC 61784-1:2002 Ed1 CP 3/3 和 V2 模式中的 PROFIsafe 总线配置文件做出响应。GSDML 文件用于对其进行组态。

故障安全模块

可以用于在 ET 200S 分布式 I/O 系统或 ET 200pro 分布式 I/O 设备中进行安全相关的操作（-> 安全模式）的 ET 200S 和 ET 200pro 模块。这些模块具有集成的 -> 安全功能。

故障安全系统

故障安全系统（F 系统）是在发生某些故障时保持安全状态或立即切换为其它安全状态的系统。

标准模式

在 -> F-I/O 的标准模式中，不可使用 -> 安全消息帧进行 -> 安全相关的通讯，在此工作模式中仅可以进行 -> 标准通讯。

-> S7-300 F-SM 可用于标准模式或 -> 安全模式。-> 故障安全模块 ET 200S、ET 200pro 和 ET 200eco 仅适用于安全模式。

标准用户程序

标准用户程序是非安全相关的用户程序。

标准通讯

标准通讯是用于交换非安全相关的数据的通讯。

检验间隔

检验间隔是一个时间段，在此时间段过后，必须将组件转为故障安全状态。即，由未使用的组件进行替换或证明其完全无故障。

测试信号

对于具有输出的 -> F-I/O，通过注入测试信号获取所需的 -> 安全等级（-> 打开期，-> 关闭期）。

消除钝化

-> 重新集成

用户安全功能

可以通过用户安全功能或故障响应功能提供过程的 -> 安全功能。用户仅对用户安全功能进行编程。如果 -> F 系统无法再执行其实际用户安全功能，则执行故障响应功能，例如，必要时取消激活关联输出且 -> F-CPU 切换为 STOP 模式。

类别

类别符合 EN 954-01

可在 -> 安全模式中使用 -> S7 Distributed Safety 和 S7 F/FH Systems 故障安全系统（最高可达类别 4）。

编程设备（PG）

编程设备：编程设备（PG）是专为用于工业设置而制造的紧凑型个人计算机。编程设备（PG）完全适用于编写 SIMATIC 自动化系统。

自动生成的 F 块

S7 Distributed Safety：这些 -> F 块是在编译和调用 -> 安全程序时自动生成的，如果需要，将从用户的安全程序生成可执行安全程序。

自定义 F 库

由用户创建的 F 库包含 F-FB、F-FC 和应用程序模板（网络模板）。

访问保护

-> 必须对故障安全系统进行保护以阻止危险的、未经授权的访问。通过分配两个密码（分别用于 -> F-CPU 和 -> 安全程序）实现对 -> F 系统的访问保护。

误差分析

对等或非对等的误差分析用于故障安全输入根据具有相同功能的两个信号的定时检测错误。检测到两个相关输入信号的级别（检查非对等：相同级别时）不同时，将启动误差分析。进行检查以确定在指定的时间（称为误差时间）过后，差异（检查非对等：匹配时）是否消失。如果未消失，则说明存在误差错误。

对于故障安全输入模块，有两种类型的误差分析：

- 如果是 -> 1oo2 评估：

  在故障安全输入模块中，在 -> 1oo2 评估的两个输入信号之间执行误差分析。

- 如果是冗余 I/O（仅限 S7 FH Systems）：

通过 *S7 F Systems* 可选软件的故障安全驱动程序块，在冗余输入模块的两个输入信号之间执行误差分析。

误差时间

误差时间是为 -> 误差分析分配的一个时间段。如果误差时间设置得太长，则故障检测时间和 -> 故障响应时间将不必要地延长。如果误差时间设置得太短，则由于在实际没有错误时检测到误差错误，而不必要地降低可用性。

过程安全时间

过程安全时间是一段时间间隔，在此期间，可以不管该过程，而不会伤害操作人员或破坏环境。

在过程安全时间内，任何类型的 F 系统过程控制都是可容错的。即在此期间，-> F 系统可能不正确地控制其过程或者甚至可以不执行任何控制。过程安全时间取决于过程类型，必须视各自情况而定。

连续功能图（CFC）

连续功能图由最多 26 个子图组成，每个子图包含 6 页。连续功能图上的功能（块）是互连的和经过参数化的。

通道故障

通道故障是通道相关故障，例如，断路或短路。

通道选择性钝化

使用该类型的钝化，则发生 -> 通道故障时仅钝化受影响的通道。如果在 -> F-I/O 中发生故障，则钝化 F-I/O 的所有通道。

重新启动 F 系统

-> F-CPU 从 STOP 过渡到 RUN 时，-> 标准用户程序将按照正常方式重新启动。-> 安全程序重新启动时，将使用装载存储器中的值按照以下方式初始化数据块：

- S7 Distributed Safety：所有具有 -> F 属性的数据块
- S7 F/FH Systems：所有数据块
- 该操作类似于冷启动。结果，将丢失保存的故障信息。-> F 系统对 -> F-I/O 执行自动 -> 重新集成。

  与标准用户程序相比，启动 OB（OB 100 至 102）无法在安全程序中使用。

重新集成

故障消除之后，必须重新集成 -> F-I/O（消除钝化）。将自动进行重新集成（从故障安全值切换为过程数据），或者由用户强制确认后再进行重新集成。

对于具有输入的 F-I/O，将在重新集成之后为 -> 安全程序再次提供故障安全输入处未决的过程数据。对于具有输出的 F-I/O，F 系统将安全程序中提供的输出值再次传送给故障安全输出。

钝化

如果 -> F-I/O 检测到故障，则将受影响的通道或所有通道切换至 -> 安全状态，即该 F-I/O 的通道被钝化。F-I/O 通过从站诊断将检测到的故障报告给 -> CPU。

对于具有输入的 F-I/O，如果发生钝化，则 F 系统为 -> 安全程序提供的是故障安全值，而不是故障安全输入处未决的过程数据。

对于具有输出的 I/O，如果发生钝化，则 F 系统将故障安全值（0）传送给故障安全输出，而不是安全程序提供的输出值。

非对等传感器

非对等 -> 传感器是连接（通过两条通道）至 -> 故障安全系统中 -> F-I/O 的两个输入的反向开关（适用于 -> 传感器信号的 1oo2 评估）。

顺序号

通过将顺序号从 -> F-CPU 传送至 -> F-I/O 来执行 PROFIsafe 协议中消息帧更新的时间监视。必须由 F-CPU 和 F-I/O 在可分配的监视时间内接收具有有效顺序号的当前有效安全消息帧。如果在监视时间内未检测到有效的顺序号，F-I/O 将处于钝化状态。

索引

G

H

I

K

O

P

R

S

W

二划

三划

四划

五划

六划

七划

八划

九划

十划

十一划

十二划

十三划

十四划

十六划