

SIEMENS

SIMATIC

工业软件 S7 Distributed Safety — 组态和编程

编程和操作手册

前言

产品概述

1

组态

2

访问保护

3

编程

4

F-I/O 访问

5

执行用户确认

6

标准用户程序和安全程序之
间的数据交换

7

对通讯进行组态和编程

8

F 库

9

编译和调试安全程序

10

系统验收测试

11

操作和维护

12




核对清单

A

法律资讯

警告提示系统

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

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

Siemens 产品

请注意下列说明：

 警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

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，这是出于保护所有权利的目的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。

前言

前言

本文档用途

本文档中的信息使您可以对 **S7 Distributed Safety** 故障安全系统进行组态和编程。

基本知识要求

要理解本文档，需要具备自动化工程方面的基本常识。还需要具备以下基本知识：

- 故障安全自动化系统
- S7-300/S7-400 自动化系统
- PROFIBUS DP/PROFINET IO 上的分布式 I/O 系统
- STEP 7 标准软件包，尤其是：
 - 如何使用 *SIMATIC* 管理器
 - LAD 和 FBD 编程语言
 - 使用 *HW Config* 进行硬件配置
 - CPU 之间的通讯

文档范围

本文档适用于以下选件包：

软件	订货号	版本号和更高版本
<i>S7 Distributed Safety</i> 选件包	6ES7833-1FC02-0YA5	V5.4 SP4

S7 Distributed Safety 选件包用于对 *S7 Distributed Safety* 故障安全系统进行组态和编程。也提到了在 *S7 Distributed Safety* 中集成下面列出的故障安全 I/O：

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

新增内容

本文档反映了以下相对于先前版本的重要变更/新增内容：

- 有关 *S7 Distributed Safety* V5.4 SP1 和 SP3（2007 年 1 月版）的产品信息内容已集成到本手册中。
- 介绍了 *S7 Distributed Safety* V5.4 SP4 中的以下重要创新：
 - *S7 Distributed Safety* 选件包可以在 Windows Vista 中安装
 - 支持 SM 336, F-AI 6 x 0/4-20 mA HART 故障安全信号模块
 - 支持“兼容模式”F-CPU 参数

认证

S7 Distributed Safety、ET 200S、ET 200eco、ET 200pro 故障安全模块和 S7-300 故障安全信号模块可在低于或等于以下等级的安全模式中使用：

- 符合 IEC 61508 规定的 SIL3（安全完整性等级）
- 符合 EN 954-1 规定的类别 4（Cat. 4）

参考文档

使用 *S7 Distributed Safety* 时，根据应用情况您将需要以下补充文档。

本文档在适当的地方参考了补充文档。

文档	相关内容的简短说明
《SIMATIC S7 中的安全工程》系统手册	<ul style="list-style-type: none"> • 提供了有关 S7 Distributed Safety 和 S7 F/FH 故障安全自动化系统的使用、结构及功能的常规信息 • 包含了有关 S7 Distributed Safety 和 S7 F/FH System 的详细技术信息 • 包含 S7 Distributed Safety 和 S7 F/FH 故障安全系统的监视时间和响应时间的计算
对于 S7 Distributed Safety 系统	<p>根据使用的 F-CPU，需要以下文档：</p> <ul style="list-style-type: none"> • S7-300、CPU 31xC 和 CPU 31x： 安装操作指令说明了如何对 S7-300 系统进行装配和接线。 • 《CPU 31xC 和 CPU 31x，技术规范》手册介绍了 CPU 315-2 DP 和 PN/DP、CPU 317-2 DP 和 PN/DP 以及 CPU 319-3 PN/DP。 • 《自动化系统 S7-400 硬件和安装》安装手册介绍了如何对 S7-400 系统进行装配和接线。 • 《自动化系统 S7-400 CPU 规范》参考手册介绍了 CPU 416-2 和 CPU 416-3 PN/DP。 • 《ET 200S IM 151-7 CPU 接口模块》手册介绍了 IM 151-7 CPU。 • 每个可用的 F-CPU 都有自己的产品信息。该产品信息仅说明该产品与相应标准 CPU 的差异。
《ET 200eco 分布式 I/O 站故障安全 I/O 模块》手册	介绍了 ET 200eco 故障安全 I/O 模块硬件（包括安装、接线和技术规范）
《ET 200S 分布式 I/O 系统故障安全模块》操作手册	介绍了 ET 200S 故障安全模块的硬件（包括安装、接线和技术规范）
《自动化系统 S7-300 故障安全信号模块》手册	介绍了 S7-300 故障安全信号模块的硬件（包括安装、接线和技术规范）
《ET 200pro 分布式 I/O 系统 — 故障安全模块》操作手册	介绍了 ET 200pro 故障安全模块的硬件（包括安装、接线和技术规范）

文档	相关内容的简短说明
STEP 7 手册	<ul style="list-style-type: none"> • 《使用 STEP7V5.x 组态硬件和通讯连接》手册介绍了如何操作适用的 STEP 7 标准工具。 • 《S7-300/400 的梯形图 (LAD)》参考手册介绍了 STEP 7 中的 LAD 标准编程语言。 • 《S7-300/400 的功能块图 (FBD)》参考手册介绍了 STEP 7 中的 FBD 标准编程语言。 • 《S7-300/400 系统的系统软件 and 标准功能》参考手册介绍了在分布式 I/O 和 CPU 上访问和执行诊断的功能。 • 《使用 STEP 7 V5.x 编程》手册概述了使用 STEP 7 进行编程（例如安装、启动、创建程序以及用户程序组件）。
STEP 7 在线帮助	<ul style="list-style-type: none"> • 介绍了 STEP 7 标准工具的操作 • 包含有关使用 HW Config 对模块和智能从站进行组态和参数分配的信息 • 包含 FBD 和 LAD 编程语言的介绍

可在 CD-ROM 上获取完整的 SIMATIC S7 文档。

指南

本文档介绍了如何使用 S7 Distributed Safety 选件包。它既包括指导说明材料又包括参考材料（有关故障安全库块的说明）。

对以下主题进行了介绍：

- S7 Distributed Safety 的组态
- S7 Distributed Safety 的访问保护
- 安全程序（安全相关的用户程序）的编写
- 安全相关的通讯
- F 库
- 对系统验收测试的支持
- S7 Distributed Safety 的操作和维护

约定

在本文档中，术语“安全工程”和“故障安全工程”所指内容相同。该约定同样适用于术语“故障安全”和“F-”。

“*S7 Distributed Safety*”显示为斜体时，它是指“S7 Distributed Safety”故障安全系统的选件包。

术语“安全程序”是指用户程序的故障安全部分，用于代替“故障安全用户程序”、“F 程序”等。为了加以对照，非安全相关的用户程序则为“标准用户程序”。

STEP 7 用户界面（例如，在 SIMATIC 管理器中）上的所有故障安全块均以黄色背景表示，以将它们与标准用户程序块进行区分。

其它支持

如果您对本手册中介绍的产品的使用方法还有疑问，且在手册中未找到正确解答，请与当地的 Siemens 销售代表联系。

可从以下网址获取 Siemens 销售代表列表：

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

可从以下网址访问各种 SIMATIC 产品和系统的技术文档：

<http://www.siemens.de/simatic-tech-doku-portal>

培训中心

我们提供了一些课程来帮助您了解 S7 自动化系统。请与当地的培训中心，或位于德意志联邦共和国纽伦堡 (90327) 的培训中心总部联系。

电话：+49 (911) 895-3200

<http://www.sitrain.com>

H/F 研究中心

纽伦堡的 H/F 研究中心提供关于 SIMATIC S7 故障安全和容错自动化系统的专题讨论会。H/F 研究中心还可以提供现场组态、调试和故障排除的帮助。

电话：+49 (911) 895-4759

传真：+49 (911) 895-5193

有关讨论会等的问题，请联系：hf-cc.aud@siemens.com

技术支持

所有 A&D 产品均可寻求技术支持

- 使用 Web 表单提出支持申请 <http://www.siemens.com/automation/support-request>
- 电话: + 49 180 5050 222
- 传真: + 49 180 5050 223

可以从以下网址找到有关技术支持的其它信息:

<http://www.siemens.com/automation/service>。

Internet 上的服务与支持

除了印刷文档外, 我们还在 Internet 上提供了所有的技术信息, 网址为:

<http://www.siemens.com/automation/service&support>

在此, 您可以找到以下信息:

- 新闻快递, 包含您的产品相关的最新信息。
- 搜索引擎, 在“服务与支持”(Service & Support) 中, 用于查找所需的文档。
- 论坛, 可供用户和专家进行全球信息交换。
- 当地 Siemens 销售代表的列表。
- 有关现场服务、维修、备件及其它的信息, 位于“服务”(Services) 下。

维持系统操作安全的重要信息

说明

具有安全相关特性的系统要求操作员遵守特定的操作安全要求。供应商在监视产品时也必须强制遵守特定操作。因此, 我们发布了专门的新闻快递, 其中包含了与(或可能与)安全相关系统的操作相关的产品开发和功能的信息。通过订阅相关的新闻快递, 您可以始终了解最新信息并能根据需要对系统进行更改。要进行在线订阅, 请转到:

<https://www.automation.siemens.com/WW/newsletter/default.aspx?parlasw=1>

并注册以下新闻快递:

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

选中每个新闻快递的“更新”(Updates) 复选框。

目录

前言	3
1 产品概述	15
1.1 概述	15
1.2 硬件组件和软件组件	16
1.3 安装/删除 S7 Distributed Safety V5.4 SP4 选件包	19
2 组态	25
2.1 组态概述	25
2.2 对 F 系统进行组态的特性	26
2.3 组态 F-CPU	28
2.4 对 F-I/O 进行组态	37
2.5 对故障安全 DP 标准从站和故障安全标准 I/O 设备进行组态	42
2.6 分配符号名	47
3 访问保护	49
3.1 访问保护概述	49
3.2 安全程序的访问许可	52
3.3 在没有安全程序密码情况下的读取访问	55
3.4 F-CPU 的访问许可	57
4 编程	59
4.1 编程概述	59
4.1.1 编程概述	59
4.1.2 S7 Distributed Safety 中安全程序的结构	61
4.1.3 故障安全块	63
4.1.4 F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语言之间的区别	66
4.2 创建安全程序	79
4.2.1 创建安全程序的基本步骤	79
4.2.2 定义程序结构	81
4.3 使用 F-FBD/F-LAD 创建 F 块	82
4.3.1 使用 F-FBD/F-LAD 创建 F 块	82
4.3.2 创建和编辑 F-FB/F-FC	83
4.3.3 创建和编辑 F-DB	85
4.3.4 用户创建的 F-FB、F-FC 和 F-DB 的知识保护	87

4.3.5	用户创建的 F-FB、F-FC 和 F-DB 的“检查块的一致性”功能	89
4.3.6	“编译和下载对象”功能	90
4.3.7	用户创建的 F-FB、F-FC 和 F-DB 的“存储写保护”功能.....	90
4.3.8	F-FB 和 F-FC 的“重新接线”功能	90
4.4	定义 F 运行组	91
4.4.1	安全程序的 F 运行组的规则	91
4.4.2	定义 F 运行组的操作步骤	92
4.4.3	安全程序的 F 运行组之间的安全相关通讯	95
4.4.4	删除 F 运行组	98
4.4.5	更改 F 运行组	98
4.5	编写启动保护程序	99
5	F-I/O 访问	101
5.1	F-I/O 访问	101
5.2	过程数据或故障安全值	102
5.3	F-I/O DB	104
5.4	访问 F-I/O DB 变量	110
5.5	启动 F 系统后钝化和重新集成 F-I/O	111
5.6	发生通讯错误后钝化和重新集成 F-I/O	113
5.7	发生 F-I/O 故障和通道故障后钝化和重新集成 F-I/O	115
5.8	组钝化	119
6	执行用户确认	121
6.1	在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认	121
6.2	在智能从站的 F-CPU 的安全程序中执行用户确认	123
7	标准用户程序和安全程序之间的数据交换	127
7.1	数据从安全程序传送到标准用户程序	127
7.2	数据从标准用户程序传送到安全程序	129
8	对通讯进行组态和编程	131
8.1	安全相关通讯概述	131
8.2	安全相关的主站与主站通讯	134
8.2.1	组态地址区（安全相关的主站与主站通讯）	134
8.2.2	组态安全相关的主站与主站通讯	135
8.2.3	通过 F_SENDDP 和 F_RCVDP 的通讯（安全相关的主站与主站通讯）	138
8.2.4	编写安全相关的主站与主站通讯程序	139
8.2.5	数据传输的限制（安全相关的主站与主站通讯）	142

8.3	安全相关的主站与智能从站通讯	143
8.3.1	组态地址区（安全相关的主站与智能从站通讯）	143
8.3.2	组态安全相关的主站与智能从站通讯	145
8.3.3	通过 F_SENDDP 和 F_RCVDP 的通讯（安全相关的主站与智能从站通讯或智能从站 与智能从站通讯）	148
8.3.4	编写安全相关的主站与智能从站通讯和智能从站与智能从站通讯程序	150
8.3.5	数据传输的限制（安全相关的主站与智能从站通讯或智能从站与智能从站通讯）	152
8.4	安全相关的智能从站与智能从站通讯	154
8.4.1	组态地址区（安全相关的智能从站与智能从站通讯）	154
8.4.2	组态安全相关的智能从站与智能从站通讯	156
8.4.3	通过 F_SENDDP 和 F_RCVDP 进行通讯（安全相关的智能从站与智能从站通讯）	159
8.4.4	编写安全相关的智能从站与智能从站通讯的程序	159
8.4.5	数据传输的限制（安全相关的智能从站与智能从站通讯）	159
8.5	安全相关的智能从站与从站通讯	160
8.5.1	组态地址区（安全相关的智能从站与从站通讯）	160
8.5.2	组态安全相关的智能从站与从站通讯	162
8.5.3	对安全相关的智能从站与从站通讯进行 F-I/O 访问	166
8.5.4	数据传输的限制（安全相关的智能从站与从站通讯）	167
8.6	安全相关的 IO 控制器与 IO 控制器通讯	168
8.7	通过 S7 连接进行安全相关的通讯	168
8.7.1	用 S7 连接组态安全相关的通讯	168
8.7.2	通过 F_SENDS7、F_RCVS7 和 F-Communication DB 进行通讯	170
8.7.3	对通过 S7 连接进行的安全相关的通讯编程	171
8.7.4	数据传输的限制（通过 S7 连接的安全相关的通讯）	175
8.8	S7 Distributed Safety 和 S7 F 系统之间的安全相关的通讯	176
9	F 库	177
9.1	Distributed Safety F 库 (V1)	177
9.1.1	Distributed Safety F-Library (V1) 概述	177
9.1.2	F 应用程序块	177
9.1.2.1	F 应用程序块概述	177
9.1.2.2	FB 179 "F_SCA_I": 输入类型 INT 的刻度值	181
9.1.2.3	FB 181 "F_CTU": 增计数	182
9.1.2.4	FB 182 "F_CTD": 减计数	183
9.1.2.5	FB 183 "F_CTUD": 增计数和减计数	184
9.1.2.6	FB 184 "F_TP": 创建脉冲	186
9.1.2.7	FB 185 "F_TON": 创建 ON 延迟	188
9.1.2.8	FB 186 "F_TON": 创建 OFF 延迟	190
9.1.2.9	FB 187 "F_ACK_OP": 故障安全确认	192
9.1.2.10	FB 188 "F_2HAND": 双手操作监视	194
9.1.2.11	FB 189 "F_MUTING": 暂时失效	196
9.1.2.12	FB 190 "F_1oo2DI": 带有误差分析的 1oo2 评估	204

9.1.2.13	FB 211“F_2H_EN”： 具有使能的双手操作监视	209
9.1.2.14	FB 212“F_MUT_P”： 并行暂时失效	212
9.1.2.15	FB 215“F_ESTOP1”： 急停（最高可达停止类别 1）	222
9.1.2.16	FB 216“F_FDBACK”： 反馈监视.....	225
9.1.2.17	FB 217“F_SFDOOR”： 安全门监视	229
9.1.2.18	FB 219“F_ACK_GL”： F 运行组的所有 F-I/O 的全局确认	232
9.1.2.19	FB 223“F_SENDDP”和 FB 224“F_RCVDP”： 通过 PROFIBUS DP 发送和接收数据	233
9.1.2.20	FB 225 “F_SENDS7” 和 FB 226 “F_RCVS7”： 通过 S7 连接通讯.....	240
9.1.2.21	FC 174 “F_SHL_W”： 向左移 16 位.....	246
9.1.2.22	FC 175 “F_SHR_W”： 向右移 16 位	247
9.1.2.23	FC 176 “F_BO_W”： 将 16 位的 BOOL 数据类型值转换为一个 WORD 数据类型值	248
9.1.2.24	FC 177 “F_W_BO”： 将一个 WORD 数据类型值转换为 16 位的 BOOL 数据类型值	248
9.1.2.25	FC 178“F_INT_WR”： 将数据类型 INT 的值间接写入 F-DB	249
9.1.2.26	FC 179“F_INT_RD”： 从 F-DB 间接读取数据类型 INT 的值	250
9.1.3	F 系统块.....	251
9.1.4	F 共享 DB.....	253
9.1.5	自定义 F 库	253
10	编译和调试安全程序	255
10.1	“Safety Program”（安全程序）对话框.....	255
10.2	安全程序状态.....	259
10.3	编译安全程序.....	260
10.4	下载安全程序.....	262
10.5	安全程序的工作存储器要求	267
10.6	通过程序标识对安全程序和保护进行功能测试.....	269
10.7	修改安全程序.....	273
10.7.1	在 RUN 模式下修改安全程序.....	273
10.7.2	比较安全程序.....	275
10.7.3	删除安全程序.....	278
10.7.4	安全程序的记录册	279
10.8	打印输出项目数据	281
10.8.1	打印的硬件配置的项目数据	282
10.8.2	打印的安全程序项目数据.....	284
10.9	测试安全程序.....	288
10.9.1	测试安全程序概述	288
10.9.2	取消激活安全模式	288
10.9.3	测试安全程序.....	291
11	系统验收测试.....	297
11.1	系统验收测试概述	297

11.2	检查打印输出.....	298
11.2.1	对 F-CPU 和 F-I/O 组态进行的验收测试.....	299
11.2.2	安全程序验收测试.....	301
11.3	在将安全程序下载到 F-CPU 之后进行的检查.....	303
11.4	更改的验收测试.....	304
12	操作和维护.....	307
12.1	有关安全程序的安全模式的注意事项.....	307
12.2	更换软件和硬件组件.....	308
12.3	诊断指南.....	310
A	核对清单.....	313
A.1	核对清单.....	313
	词汇表.....	319
	索引.....	331

产品概述

1.1 概述

S7 Distributed Safety 故障安全系统

S7 Distributed Safety 故障安全系统可实现机器和人员保护（例如，用于机床和加工机械的急停设备）以及过程工业（例如，实现对仪表和控制以及燃烧器的保护功能）方面的安全防护概念。

可达到的安全要求

S7 Distributed Safety 故障安全系统可满足以下安全要求：

- 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（Cat.2）至类别 4（Cat.4）

S7 Distributed Safety 中安全功能的原理

功能性安全主要是通过软件中的安全功能实现的。如果发生危险，S7 Distributed Safety 系统将执行安全功能以使系统处于或保持安全状态。安全功能主要包含在以下组件中：

- F-CPU 中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）

故障安全 I/O 可确保现场信息的安全处理（急停按钮、光栅和电机控制）。它们包含进行安全处理所需的所有硬件组件和软件组件（符合要求的安全等级）。用户仅需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过程处理的安全功能。出现错误时，如果 F 系统无法再执行其实际用户安全功能，则它将执行故障响应功能，例如，取消激活关联的输出，以及在必要时将 F-CPU 切换至 STOP 模式。

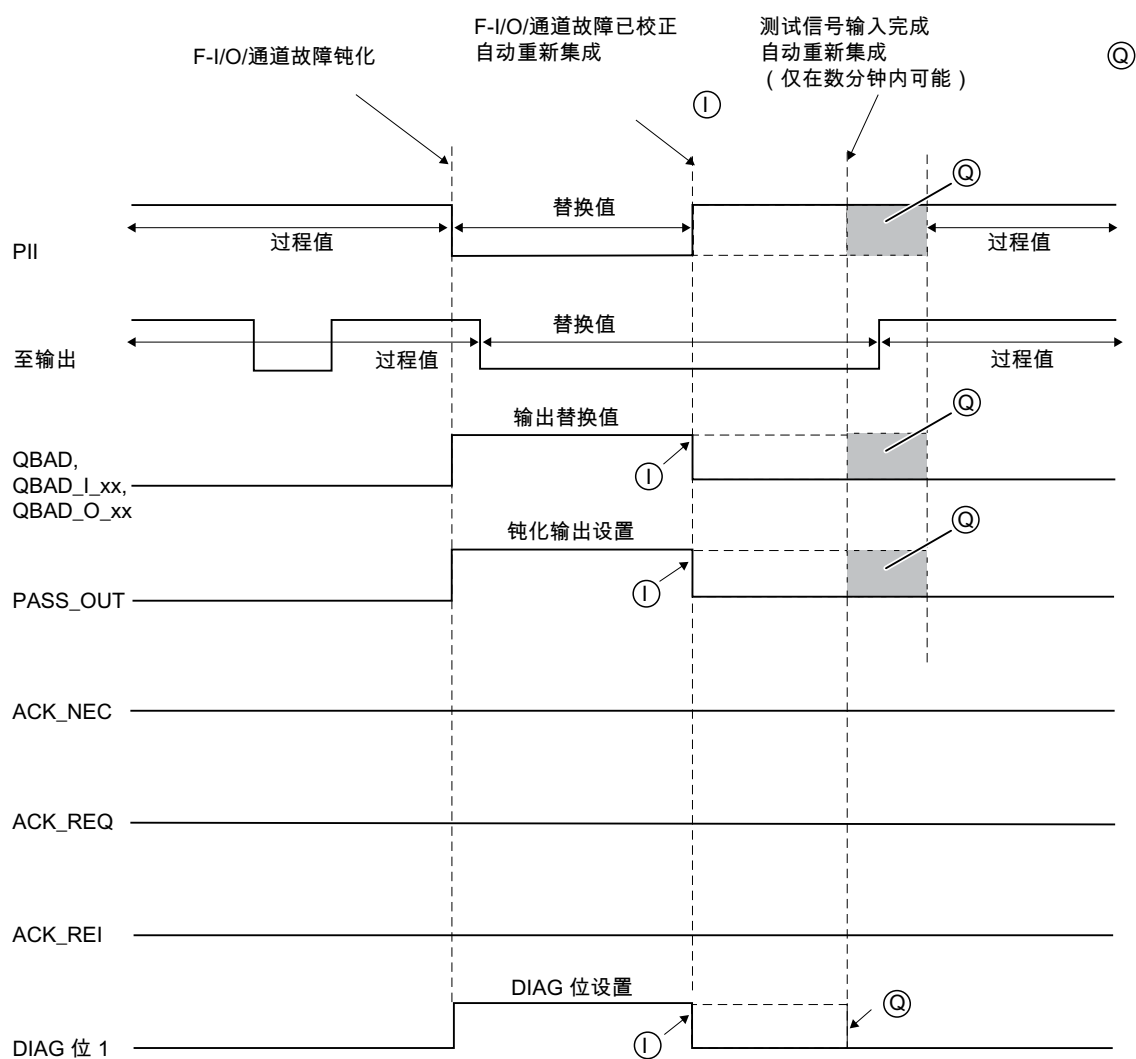
用户安全功能和故障响应功能的实例

如果压力过大，F 系统将打开阀门（用户安全功能）。F-CPU 中发生危险故障时，将取消激活所有输出（故障响应功能），并打开阀门，从而使其它执行器也处于安全状态。如果 F 系统完好无损，则仅打开阀门。

1.2 硬件组件和软件组件

S7 Distributed Safety 的硬件组件和软件组件

下图概述了组态和运行 S7 Distributed Safety 故障安全系统所需的硬件组件和软件组件。



- ① 用于具有输入的 F-I/O
- Ⓚ 用于具有输出的 F-I/O 以及具有输入和输出的 F-I/O (信号模式取决于所使用的 F-I/O)

PROFIBUS DP 的硬件组件

S7 Distributed Safety 包括以下硬件组件：

- F-CPU，例如 315F-2 DP CPU
- 故障安全输入和输出 (F-I/O)，例如：
 - S7 Distributed Safety（集中式组态）中的 S7-300 故障安全信号模块
 - ET 200M（分布式组态）中的 S7-300 故障安全信号模块
 - ET 200S 中的故障安全电源模块和电子模块
 - ET 200eco 故障安全 I/O 模块
 - ET 200pro 中的故障安全模块
 - 故障安全 DP 标准从站

可以使用标准 I/O 扩展组态。

PROFINET IO 的硬件组件

可以在 PROFINET IO 上的 S7 Distributed Safety F 系统中使用以下故障安全组件：

- 具有 PN 接口的 F-CPU，例如 CPU 416F-3 PN/DP
- ET 200S 中的故障安全电子模块
- ET 200pro 中的故障安全电子模块
- 故障安全标准 I/O 设备（光栅、激光扫描仪等）

可以使用标准 I/O 扩展组态。

附加信息

有关硬件组件的详细信息可在《SIMATIC S7 中的安全工程》系统手册中找到。

软件组件

S7 Distributed Safety 包括以下软件组件：

- 编程设备/PC 上用于对 F 系统进行组态和编程的 *S7 Distributed Safety* 选件包
- F-CPU 中的安全程序

此外，编程设备或 PC 上还需要 *STEP 7* 基本软件以对标准 PLC 进行组态和编程。

S7 Distributed Safety 选件包

本文档介绍了 *S7 Distributed Safety V5.4 SP4* 选件包。 *S7 Distributed Safety* 是用于 S7 Distributed Safety 故障安全系统的组态和编程软件。使用 *S7 Distributed Safety*，您可以获得以下功能：

- 支持在 *STEP 7* 中使用 *HW Config* 组态 F-I/O
- 支持创建安全程序并在该安全程序中集成错误检测功能
- 包含可在安全程序中使用的故障安全应用程序块的 F 库

此外，*S7 Distributed Safety* 可提供比较安全程序的功能及协助您进行系统验收测试的功能。

安全程序

可在 *STEP 7* 中使用 *FBD/LAD 编辑器* 创建安全程序。可使用 F-FBD 或 F-LAD 编程语言编写故障安全 FB 和 FC 程序，使用 F-DB 编程语言创建故障安全 DB。随附的 *Distributed Safety F 库 (V1)* 提供了可在安全程序中使用的故障安全应用程序块。

编译安全程序时，将自动执行安全检查，并插入用于错误检测和故障响应的其它故障安全块。这将确保可以检测到故障和错误，并触发适当的响应，以使 F 系统保持在安全状态或进入安全状态。

除安全程序之外，标准用户程序也可以在 F-CPU 上运行。由于安全程序的安全相关数据可免受标准用户程序数据的意外影响，因此标准程序可与安全程序共存于一个 F-CPU 中。


F-CPU 中的安全程序和标准用户程序之间的数据交换可通过位存储器或访问输入和输出过程映像完成。

1.3 安装/删除 S7 Distributed Safety V5.4 SP4 选件包

S7 Distributed Safety V5.4 SP4 的软件要求

至少，在编程设备或 PC 上必须安装以下软件包：

- STEP 7 V5.3 SP 3 或更高版本

 警告
不允许将 <i>S7 Distributed Safety Programming</i> V5.4 SP 4 和更早版本的 STEP 7 一起使用。

- *S7 F Configuration Pack* V5.2 SP 3 或更高版本

使用以下功能需要具备下面指出的软件：

功能	软件要求
S7-300 故障安全信号模块 (ET 200M) 的安全相关的智能从站与从站通讯	<i>STEP 7</i> V5.4 和 <i>S7 F Configuration Pack</i> V5.5 或更高版本
禁用安全模式的取消激活	<i>S7 F Configuration Pack</i> V5.5 SP1
F-iPar_CRC 参数支持故障安全 DP 标准从站/标准 I/O 设备（具有单独的设备参数 [i-参数]）	<i>S7 F Configuration Pack</i> V5.5 SP1
F 块的写保护保存	<i>STEP 7</i> V5.4 SP2
STEP 7 中用于 F 块的“重新接线”功能	<i>STEP 7</i> V5.4 SP2 和 <i>S7 F Configuration Pack</i> V5.5 SP1
故障安全标准 I/O 设备	<i>STEP 7</i> V5.4 SP2 <i>S7 F Configuration Pack</i> V5.4
在 没有 使用 HART 功能的情况下支持 SM 336, F-AI 6 x 0/4-20 mA HART	<i>S7 F Configuration Pack</i> V5.5 SP4
在 使用 HART 功能的情况下使用 SM 336, F-AI 6 x 0/4-20 mA HART	<i>STEP 7</i> V5.4 SP3 和 <i>S7 F Configuration Pack</i> V5.5 SP4

1.3 安装/删除 S7 Distributed Safety V5.4 SP4 选件包

阅读自述文件

自述文件包含有关软件的重要最新信息（例如，支持的 Windows 版本）。可在安装程序中显示该自述文件，也可在稍后通过选择**开始 (Start) > Simatic > 信息 (Information) > 英语 (English)** 菜单命令将其打开。

安装 S7 Distributed Safety

1. 启动已安装 *STEP 7* 标准软件包的编程设备或 PC，并确保所有的 *STEP 7* 应用程序均已关闭。
2. 插入选件包的产品 CD。
3. 启动 CD 上的 *SETUP.EXE* 程序。
4. 牢记自述文件中的信息，按照安装程序的指示操作。

启动 S7 Distributed Safety

S7 Distributed Safety 完全集成在 *STEP 7* 中。这表示无需专门启动 *S7 Distributed Safety*，启动每个 *STEP 7* 应用程序（*SIMATIC 管理器*、*HW Config* 和 *FBD/LAD 编辑器*）即可帮助您对 *S7 Distributed Safety* 进行组态和编程。

显示集成的帮助

S7 Distributed Safety 对话框具有内容相关的帮助。在组态和编程的各个阶段，都可通过按 F1 键或单击“帮助”(Help) 按钮来访问此帮助。要获得高级帮助，请选择**帮助 (Help) > 目录 (Contents) > 访问有关选件包的帮助 (Access Help for Optional Packages) > S7 Distributed Safety 与 F 系统一起使用 (S7 Distributed Safety Work with F-systems)** 菜单命令。

删除 S7 Distributed Safety

S7 Distributed Safety 选件包有如下两个组件：

- “*S7 F Configuration Pack V5.5 SP4*”
- “*S7 Distributed Safety Programming V5.4 SP4*”

可以单独删除这些组件。按照 Windows 的常规操作步骤删除软件：

1. 在 Windows 中，双击“控制面板”(Control Panel) 中的“添加/删除程序”(Add or Remove Programs) 图标打开安装软件的对话框。
2. 在已安装软件的列表中，选择相应的条目。单击“添加/删除...”(Add/Remove...) 删除该软件。
3. 如果显示“删除共享文件”(Remove shared file) 对话框，若您无法确定是否删除，请单击“否”(No)。

转换为 S7 Distributed Safety V5.4 SP4

使用 S7 Distributed Safety V5.4 SP4 读取安全程序

如果要使用 *S7 Distributed Safety V5.4 SP4* 读取（而非更改）使用更早版本的 *S7 Distributed Safety* 创建的安全程序，请使用 V5.4 SP4 打开“安全程序”(Safety Program) 对话框。请勿编译安全程序并且请勿在替换 *HW Config* 中的 *Distributed Safety F* 库 (V1) 的 F 库块时进行保存和编译。

说明

打开使用 *S7 Distributed Safety V5.1* 创建的一致安全程序的“安全程序”(Safety Program) 对话框时，将输出状态“该安全程序是一致的。”(The safety program is consistent.)，尽管显示的签名不同。

原因：签名的长度已从 16 位变为 32 位。

使用 S7 Distributed Safety V5.4 SP4 更改安全程序

可在使用更早版本的 *S7 Distributed Safety* 创建的安全程序中使用 *S7 Distributed Safety V5.4 SP4* 的新功能（请参阅前言中的『新增内容』）。

说明

请注意，F-I/O 的通道级钝化和 F-I/O 到 PROFINET IO 的连接将延长 F 运行组的运行时间，并增加了安全程序的工作存储器要求（请参阅用于计算响应时间的 *Excel* 文件 *s7cotia.xls*）。此外，可用于安全程序的本地数据必须至少为 330 个字节（请参阅『组态 F-CPU』一章）。

1.3 安装/删除 S7 Distributed Safety V5.4 SP4 选件包

如果要使用 *S7 Distributed Safety V5.4 SP4* 更改使用更早版本的 *S7 Distributed Safety* 创建的安全程序，请按照以下步骤进行操作：

1. 使用 *S7 Distributed Safety V5.4 SP4* 编译安全程序，然后再进行更改。

结果： 确认后，在安全程序中使用的、并且在 V5.4 SP4 的 *Distributed Safety F* 库 (V1) 中存在新版本的所有 *Distributed Safety F* 库 (V1) 的 F 块都被自动替换。

所有 F 块的集体签名和单个 F 块的签名由于以下原因而更改：

- 集体签名的长度已从 16 位变为 32 位（仅适用于从 V5.1 转换为 V5.4 SP4）
- *Distributed Safety F* 库 (V1) 的 F 块已被替换
- 自动编译的 F 块已更改

当从 V5.4 SP3 更改为 V5.4 SP4 后，所有 F 块的集体签名都保持不变，尽管 F-CTRL_1 F 系统块被新版本替换（非安全相关的更改）。

2. 根据需要更改安全程序。
3. 重新编译安全程序。
4. 在“比较安全程序”(Compare safety program) 对话框中执行安全程序新旧版本的比较（请参阅『比较安全程序』一章）。
 - 通过 F 块签名的变化可以识别 *Distributed Safety F* 库 (V1) 的 F 块版本的变化。所有 F 应用程序块和 F 系统块的已修改签名及初始值签名均必须与《认证报告》的『附录 1』中的签名相对应。
 - 此外，可以识别是否已在安全程序中进行了更改。如有必要，必须对安全程序再进行一次验收测试。

从 *S7 Distributed Safety V5.4 SP4* 更改为更早版本

如果要更改为早于 V5.4 SP4 的 *S7 Distributed Safety* 版本，则必须先完全删除 *S7 Distributed Safety V5.4 SP4*。

从 S7 Distributed Safety V5.4 SP4 更改为 V5.3

打开使用 S7 Distributed Safety V5.4 SP4 创建的一致安全程序的“安全程序”(Safety Program) 对话框时，将输出状态“该安全程序是一致的。”(The safety program is consistent.)。

如果仅使用在 V5.3 中可用的功能，则可以使用 V5.3 来修改使用 V5.4 SP4 创建的安全程序。

如果要使用 V5.3 来更改使用 S7 Distributed Safety V5.4 SP4 创建的安全程序，请按照以下步骤进行操作：

1. 删除安全程序的离线块文件夹中所有自动生成的和添加的 F 块。
2. 在 *HW Config* 中保存并编译硬件配置。
3. 根据需要更改安全程序。
4. 重新编译安全程序。

从 S7 Distributed Safety V5.4 SP4 更改为 V5.2

打开使用 S7 Distributed Safety V5.4 SP4 创建的一致安全程序的“安全程序”(Safety Program) 对话框时，将输出状态“该安全程序不一致。”(The safety program is not consistent.)，即使该安全程序是一致的。

如果仅使用在 V5.2 中可用的功能，则可以使用 V5.2 来修改使用 V5.4 SP4 创建的安全程序。

从 V5.4 SP4 更改为 V5.3 的操作步骤适用于此处。

F 系统最大响应时间的计算

使用可用于 S7 Distributed Safety V5.4 SP4 的 Microsoft Excel 文件来计算 F 系统的最大响应时间。该文件可从以下网址下载：

<http://support.automation.siemens.com/WW/view/en/11669702/133100>

参见

安全程序验收测试 (页 301)

1.3 安装/删除 *S7 Distributed Safety V5.4 SP4* 选件包

组态

2.1 组态概述

引言

对 S7 Distributed Safety 故障安全系统进行组态的方式与对标准 S7-300、S7-400 或 ET 200S 自动化系统进行组态的方式基本相同。

为此，该部分只介绍组态 S7 Distributed Safety F 系统时与组态标准 PLC 时的本质区别。

必须组态的 F 组件

对 S7 Distributed Safety F 系统，以下硬件组件需组态：

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

可用 F-I/O 的信息

有关可用的 F-I/O 的详细信息，请参考下表中的手册：

主题	参考
组态规则，例如： <ul style="list-style-type: none"> • F-I/O 的集中式组态和分布式组态 • F-I/O 和标准 I/O 共存 	<ul style="list-style-type: none"> • 《SIMATIC S7 中的安全工程》系统手册 • 特定 F-I/O 的手册
F-I/O 的 PROFIsafe 地址分配	特定 F-I/O 的手册和内容相关的在线帮助
F-I/O 在 F-CPU 中的地址区分配	特定 F-I/O 的手册
故障安全 DP 标准从站	特定故障安全 DP 标准从站的文档
故障安全标准 I/O 设备	特定故障安全标准 I/O 设备的文档

可组态的安全相关的通讯选项

必须使用 *HW Config* 来组态以下安全相关的通讯选项：

- 安全相关的主站与主站通讯
- 安全相关的主站与智能从站通讯
- 安全相关的智能从站与智能从站通讯
- 安全相关的智能从站与从站通讯
- 安全相关的 IO 控制器与 IO 控制器通讯
- 通过 S7 连接的安全相关的通讯

2.2 对 F 系统进行组态的特性

F 系统的组态方式与标准系统相同

S7 Distributed Safety 故障安全系统的组态方式与标准 S7 系统的组态方式相同。也就是说，在 *HW Config* 中，可以以集中式组态（F-CPU，如有必要还有 S7-300 F-SM）和/或分布式组态（F-CPU、ET 200M 中的 F-SM、ET 200S 中的 F 模块、ET 200pro、ET 200eco、故障安全 DP 标准从站和故障安全标准 I/O 设备）对硬件进行组态和分配参数。

有关组态选项的详细说明，请参考《SIMATIC S7 中的安全工程》系统手册。

特殊的 F 相关的选项卡

故障安全组件（F-CPU 和 F-I/O）的对象属性中包括一些 F 功能的特殊选项卡。这些选项卡将在后面的章节中进行说明。

为 F-I/O 的故障安全输入/输出分配符号

为方便起见，在对 S7 Distributed Safety 进行编程时，请务必在 *HW Config* 中为 F-I/O 的故障安全输入和输出分配符号。

保存并编译硬件配置

必须在 *HW Config* 中保存并编译 S7 Distributed Safety F 系统的硬件配置。这对于安全程序的后续编程是必需的。

更改安全相关的参数

说明

如果更改 F-I/O、故障安全 DP 标准从站、故障安全标准 I/O 设备或 F-CPU 的安全相关的参数，则必须重新编译安全程序。

这同样适用于安全相关通讯组态中的更改，尤其是用于通过 S7 连接进行安全相关通讯的 S7 连接中的更改。

2.3 组态 F-CPU

引言

对 F-CPU 进行组态的方式与对标准自动化系统进行组态的方式基本相同。对于 *S7 Distributed Safety* F 系统，还必须执行以下操作：

- 组态保护级别 1。
- 组态 F 参数。

组态 F-CPU 的保护级别



在安全模式中，更改标准用户程序时不允许通过 F-CPU 密码进行访问，否则会造成安全程序的更改。要排除这种可能性，必须组态**保护级别 1**。如果仅有一个人经过授权可以对标准用户程序和安全程序进行更改，则应组态保护级别“2”或“3”，从而使其它人员仅能有限地访问或根本无法访问整个用户程序（标准程序和安全程序）。

使用以下步骤组态保护级别 1：

1. 在 *HW Config* 中，选择 F-CPU（例如 CPU 315F-2 DP），然后选择**编辑 (Edit) > 对象属性 (Object Properties)** 菜单命令。
2. 打开“保护” (Protection) 选项卡。
3. 设置保护级别“1: F-CPU 的访问保护” (1: Access protection for F-CPU) 和“使用密码可删除” (Removable with Password)。

在提供的域中为 F-CPU 输入密码，并选择“CPU 包含安全程序” (CPU contains safety program) 选项。请注意，“模式” (Mode) 域与安全模式无关。

有关 F-CPU 密码的信息，请参考『访问保护概述』一章。请特别注意『设置 F-CPU 的访问许可』一章中的警告。

组态 F-CPU 的 F 参数

使用以下操作步骤组态 F 参数：

1. 在 *HW Config* 中，选择 F-CPU，然后选择 **编辑 (Edit) > 对象属性 (Object Properties)** 菜单命令。

2. 打开“F 参数” (F Parameters) 选项卡。打开该选项卡后，将提示您输入安全程序的密码，或者必须在另一个对话框中设定安全程序的密码。有关安全程序密码的信息，请参考『访问保护概述』一章。

在“F 参数” (F parameters) 选项卡中，可以更改或接受以下参数的默认设置：

- 启用或禁用取消激活安全模式功能
- PROFIsafe 地址的基数
- F-CPU 的兼容模式
(仅用于支持 PROFIsafe V2 MODE 的 F-CPU 和仅具有 PROFIBUS DP 接口而不是 PROFINET IO 的 F-CPU)
- F 数据块的编号区
- F 功能块的编号区
- 安全程序的本地数据区大小

说明

更改 F-CPU 的 F 参数会导致安全程序在重新编译时出现变动，因此可能需要进行新的验收测试。

“可以取消安全模式” (Safety Mode Can Be Deactivated) 参数

您可以在“F 参数” (F-Parameters) 选项卡中启用或禁用取消安全模式的功能。在缺省设置中，“可以取消安全模式” (Safety mode can be deactivated) 是启用状态。

如果禁用取消安全模式功能，则通常不能再取消安全模式。也就是说，即使在下列情况中输入安全程序密码也无法取消安全模式：

- 在“安全程序” (Safety Program) 对话框中
- 在测试/调试功能和装载 F 块期间，在用于取消安全模式的对话框中

“PROFIsafe 地址的基数”参数

对 F 系统的 PROFIsafe 地址进行内部管理时需要该信息。

PROFIsafe 地址用于唯一标识源地址和目标地址。

可以为以下模块设置“PROFIsafe 地址的基数” (Base for PROFIsafe addresses)，即自动分配 PROFIsafe 目标地址的范围：

- *HW Config* 中新放置的 ET 200S、ET 200pro 和 ET 200eco F-I/O
- 以下 S7-300 故障安全信号模块：
 - 新放置的且仅可在安全模式下使用的模块（请参阅《S7-300 故障安全信号模块》手册）
 - 首次在 *HW Config* 中设置安全模式但是**没有**用模块起始地址分配 PROFIsafe 地址的模块（请参阅《S7-300 故障安全信号模块》手册）。

此参数对其它所有 F-I/O 均无影响。

设置此参数将定义 PROFIsafe 目标地址的范围。这对同一个网络中运行多个 DP 主站系统和 PROFINET IO 系统时有用。可以进行后续地址更改（但并非必需的），因为已根据参数赋值保留了地址范围。

可按 1000 的增量来设置“PROFIsafe 地址的基数” (Base for PROFIsafe addresses)。PROFIsafe 目标地址根据以下公式自动进行计算得到：PROFIsafe 地址的基数除以 10。可能的最大 PROFIsafe 目标地址为 1022。

实例：将基数设置为“2000”。PROFIsafe 目标地址从 200 开始自动赋值。

“兼容模式” (Compatibility Mode) 参数

该参数仅用于支持 PROFIsafe V2 MODE 的 F-CPU 和仅具有 PROFIBUS DP 接口而不是 PROFINET IO 的 F-CPU。

只有当硬件配置中要用同时支持 PROFIsafe V1 MODE 和 PROFIsafe V2 MODE 的 F-CPU 来替换掉仅支持 PROFIsafe V1 MODE 的 F-CPU 时，才需要更改缺省设置（= 兼容模式已关闭）。

为了防止因更换 CPU 而在后续编译中改变安全程序从而需要新的验证测试，必须启用兼容模式。

如果不执行此操作，在 *HW Config* 中保存并编译硬件配置时所有支持 V2 MODE 的 F-I/O 的 PROFIsafe MODE 将更改为 V2 MODE。

如果项目在 PROFINET IO 上或在基于 IE/PB Link 的 PROFIBUS DP 与 PROFINET IO 的混合组态中使用 F-I/O，则必须禁用兼容模式。

“F 数据块” (F-Data Blocks) 参数

在编译安全程序时，将自动添加 F 块，以从您的安全程序中创建可执行的安全程序。必须为自动添加的 F 数据块保留一个编号区。用户需要定义这个区域的第一个和最后一个编号。

选择编号区大小的规则：

至少应接受缺省设置。此外，以下规则同时适用：

自动添加的 F 数据块的数目 =

已组态 F-I/O 的数目

+ F-DB（不包括“用于 F 运行组通讯的 DB”）的数目

+ 5 x “用于 F 运行组通讯的 DB”的数目

+ FB 类型的 F 块（F-FB/F-PB/F 应用程序块）调用数目

+ FC 类型的 F 块（F-FC/F-PB/F 应用程序块）数目

+ 在两个 F 运行组中使用的 FC 类型的
的 F 块（F-FC/F-PB/F 应用程序块）数目

+ 6 x F 运行组数目

如果组态的编号区不够大，*S7 Distributed Safety* 将提示出错消息。随后，必须相应增加编号区的大小。

提示：为自动添加的 F 数据块分配编号区，从 F-CPU 中最大的可能编号开始依次向下分配。为标准用户程序的 DB，F-FB 的 F-DB 和背景数据块以及安全程序的 F 应用程序块分配编号时从“1”开始。

不得在安全程序或标准用户程序中使用保留的自动添加的 F 数据块。

如果更改了编号区（例如，用编号区较小的 F-CPU 替换原 F-CPU），则在下次编译时不会创建已更改编号区（新 F-CPU 的编号区）中的某些自动添加的 F-DB。而这些 F-DB 将保持它们的旧编号。因此，可能无法将它们下载到 F-CPU。

解决方案：在安全程序的离线块文件夹中删除所有自动生成的 F 块，然后重新编译该安全程序。

“F 功能块” (F-Function Blocks) 参数

编译安全程序时，将自动添加 F 块，以从您的安全程序中创建可执行的安全程序。必须为自动添加的 F 功能块保留一个编号区。用户需要定义这个区域的第一个和最后一个编号。

选择编号区大小的规则：

至少应接受缺省设置。此外，以下规则同时适用：

自动添加的 F 功能块数目 =

F 块 (F-FB/F-FC/F-PB/F 应用程序块) 数目

+ 在两个 F 运行组中调用的 F 块 (F-FB/F-FC) 数目

+ 包含在保留的编号区中的 F 应用程序块数目

+ 5

如果组态的编号区不够大，*S7 Distributed Safety* 将提示出错消息。随后，必须相应增加编号区的大小。

提示：为自动添加的 F 数据块分配编号区，从 F-CPU 中最大的可能编号开始依次向下分配。为标准用户程序的 FB 和安全程序的 F-FB 分配编号时从“1”开始。

不得在安全程序或标准用户程序中使用保留的自动添加的 F 功能块。

Distributed Safety F 库中的 F 应用程序块可能在该编号区中。

“F 本地数据” (F-Local Data) 参数

编译安全程序时，将自动添加 F 块，以从您的安全程序中创建可执行的安全程序。该参数以字节为单位指定整个安全程序本地数据的数量，即安全程序 F 运行组的 F-CALL 块以及 F-CALL 中调用的自动添加的 F 块可用的本地数据。

说明

本地数据设置适用于一个安全程序的所有 F 运行组。

必须为安全程序提供至少 330 个字节的本地数据。但是，自动添加的 F 块对于本地数据的数量要求可能更高，这取决于安全程序的数量要求。

因此，应该为自动添加的 F 块提供尽可能多的本地数据。如果没有足够的本地数据可供自动添加的 F 块使用（330 个字节或更多），仍会编译安全程序。这时将使用自动添加的 F-DB 中的数据，而不是本地数据。但是，这将增加 F 运行组的运行时间。如果自动添加的 F 块需要比组态更多的本地数据，*S7 Distributed Safety* 将通过消息提示。



警告

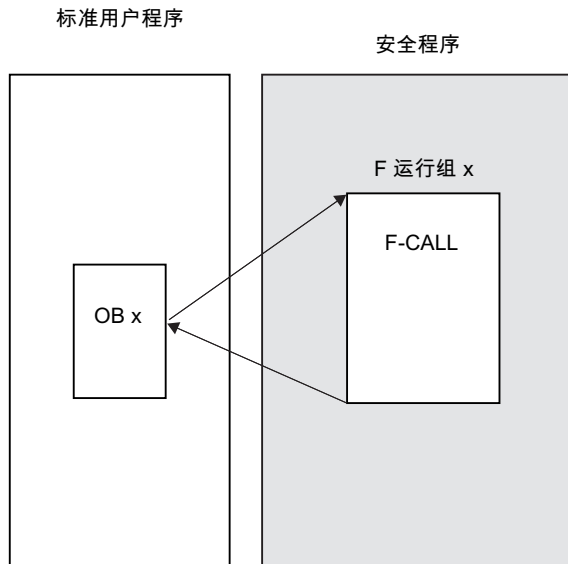
在此情况下，使用 MS Excel 文件 `s7fcotia.xls` 计算得出的 F 运行组最大运行时间将不再正确，因为该计算假定有足够的 F 本地数据可用。

在此情况下，发生错误和使用上述 Excel 文件为标准系统的所有运行时间计算最大响应时间时，可将为 F 运行组的最大周期时间（F 监视时间）组态的值用作 F 运行组的最大运行时间。

说明

请注意，F 本地数据的最大可能数量取决于以下情况：

- 更高级标准用户程序的本地数据要求。因此，应在 OB（只要周期性中断 OB 可用）中直接调用 F-CALL 块，且在這些周期性中断 OB 中不应声明其它本地数据。
- 使用的 F-CPU 的本地数据的最大数量（请参阅所用 F-CPU 的产品信息中的技术规范）。对于 CPU 416F-2，可组态每个优先级等级的本地数据。因此，请为这些将调用安全程序（F-CALL 块）的优先级等级（例如，OB35）分配最大可能的本地数据区。

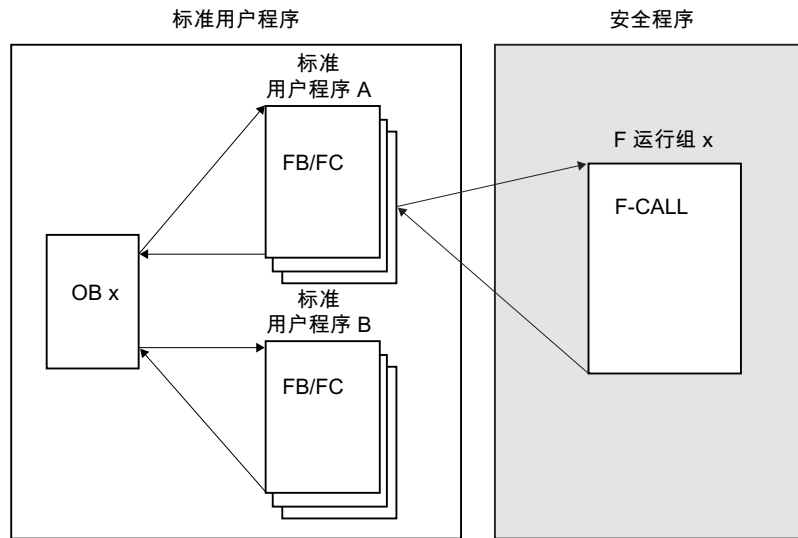
F 本地数据可能的最大数量取决于更高级标准用户程序的本地数据要求数量**第 1 种情况：在 OB 中直接调用 F-CALL 块**

将“F 本地数据” (F local data) 参数设置为以下数量之一：

- 正在使用的 F-CPU 的本地数据最大数量减去 32 个字节
- 如果 OBx（针对具有最大本地数据数量要求的 OBx 的两个 F 运行组）需要的本地数据大于 32 个字节，则用正在使用的 F-CPU 的本地数据的最大数量减去该数量。

注意：可从程序结构得出 OB 的本地数据要求数量。要执行此操作，请在 *SIMATIC 管理器* 中选择 **选项 (Options) > 参考数据 (Reference Data) > 显示 (Display)** 菜单命令（设置：“程序结构” (Program Structure) 已选中）。这将显示路径中或各个块的本地数据要求数量（请参阅 *STEP 7 在线帮助*）。

第 2 种情况：不在 OB 中直接调用 F-CALL 块



将“F 本地数据” (F local data) 参数设置为以下数量之一：

- 正在使用的 F-CPU 的本地数据的最大数量减去 32 个字节
- 如果 OBx（针对具有最大本地数据要求数量的 OBx 的两个 F 运行组）的本地数据要求数量和标准用户程序 A 的本地数据要求数量的和大于 32 个字节，则用正在使用的 F-CPU 的本地数据的最大数量减去它们的和。

注意： 可从程序结构得出 OB 和标准用户程序 A 的本地数据要求数量。要执行此操作，请在 *SIMATIC 管理器* 中选择 **选项 (Options) > 参考数据 (Reference Data) > 显示 (Display)** 菜单命令（设置：“程序结构” (Program Structure) 已选中）。这将显示路径中或各个块的本地数据要求数量（请参阅 *STEP 7 在线帮助*）。

自动添加的 F 块的本地数据要求数量取决于安全程序的本地数据要求数量

仅当可供安全程序使用的本地数据数量不足并从 **S7 Distributed Safety** 收到有关该影响的消息时，才必须考虑以下信息。

可对自动添加的 F 块的可能本地数据要求数量进行估计，如下所述：

对于每个 F 运行组，可确定安全程序每个调用层级（F 运行组中的路径从 F-PB 开始 [包含 F-PB]，通过所有嵌套层向下至最低层）的本地数据要求数量：

调用体系的本地数据要求数量（路径本地数据要求数量 [以字节为单位]）=

2 x 路径中 **BOOL** 数据类型的 F-FB/F-FC 的所有本地数据的数量

+ 4 x 路径中 **INT** 或 **WORD** 数据类型的 F-FB/F-FC 的所有本地数据的数量

+ 6 x 路径中 **TIME** 数据类型的 F-FB/F-FC 的所有本地数据的数量

+ 42 x 调用 F 应用程序块的嵌套层的数量

+ 18 x 嵌套层的数量

+ 14 x 对定点功能或字逻辑指令进行编程的嵌套层的数量。

然后，自动添加的 F 块的本地数据要求的评估数量等于所有 F 运行组的所有路径的最大路径本地数据要求数量。

说明

如果无法为自动添加的 F 块提供足够数量的本地数据，建议您减少安全程序的本地数据要求数量（例如，减小嵌套深度）。

在 F-FB 或 F-FC 中使用本地数据

说明

在编译安全程序时，将自动添加 F 块，以从您的安全程序中创建可执行的安全程序。如果在 F-FB/F-FC 中使用本地数据存储区，请注意以下限制（与 S7-400 F-CPU 无关）：

本地数据要求数量 < 每个块的最大本地数据数量

（请参阅所用 F-CPU 的产品信息中的技术规范）

平均本地数据要求数量（以字节为单位）=

2 x BOOL 数据类型的 F-FB/F-FC 的所有本地数据的数量

+ 4 x INT 或 WORD 数据类型的 F-FB/F-FC 的所有本地数据的数量

+ 6 x TIME 数据类型的 F-FB/F-FC 所有本地数据的数量

+ 12

+ 14（如果对定点功能或字逻辑指令进行编程）

+ 6（如果调用 F-FB、F-FC 或 F 应用程序块）

如果需要更大的本地数据数量，则无法将安全程序下载到 F-CPU。请减少已编程的 F-FB 或 F-FC 的本地数据要求数量。

参见

安装/删除 S7 Distributed Safety V5.4 SP4 选件包 (页 19)

访问保护概述 (页 49)

F-CPU 的访问许可 (页 57)

S7 Distributed Safety 中安全程序的结构 (页 61)

系统验收测试概述 (页 297)

2.4 对 F-I/O 进行组态

F-I/O 的组态方式与标准 I/O 相同

ET 200S、ET 200eco、ET 200pro F 模块和 S7-300 F-SM 的组态方式始终相同：

在 *HW Config* 的站点窗口中插入 F-I/O 后，您可以通过选择 **编辑 (Edit) > 对象属性 (Object Properties)** 或双击 F-I/O 来访问组态对话框。打开该对话框之后，提示您输入安全程序密码，或者必须在另一个对话框中为安全程序分配密码。有关安全程序密码的信息，请参考“访问保护概述”。

F 相关的选项卡中阴影区域中的值是由 *S7 Distributed Safety* 自动分配的。可以更改非阴影区域中的值。

通道故障后的通道级钝化

如果 F-I/O 支持该参数（例如，对于 ET 200S、ET 200pro F 模块），则可组态 F-I/O 对通道故障（例如，短路、过载、误差错误或断线）的响应方式。可在相关 F-I/O 的对象属性中组态该响应（“通道故障后的行为” (Behavior after channel faults) 参数）。该参数用于指定发生通道故障时是钝化整个 F-I/O 还是仅钝化发生故障的通道。

说明

请注意，与钝化整个 F-I/O 相比，通道级钝化将增加 F 运行组的运行时间（请参阅用于计算响应时间的 *Excel* 文件 *s7cotia.xls*）。

其它信息

有关您可以使用（集中式或分布式）哪些 ET 200S、ET 200eco、ET 200pro F 模块和 S7-300 F-SM 的信息，请参考《*SIMATIC S7 中的安全工程*》系统手册。

有关参数的说明，请参考选项卡内容相关的在线帮助和相关的 F-I/O 手册。

有关组态 F-I/O 的监视时间时必须注意的事项，请参考《*SIMATIC S7 中的安全工程*》系统手册。

PROFIsafe 地址

PROFIsafe 地址（“F_source_address”、“F_destination_address”参数）用于唯一标识源地址和目标地址。

F_destination_address

F_destination_address 用于唯一标识（F-I/O 的）PROFIsafe 目标地址。因此，F_destination_address 在网络范围内和站范围内必须是唯一的（请参阅地址分配的以下规则）。

为了防止参数分配不正确，在将 F-I/O 放在 *HW Config* 中之后，系统会自动分配站范围内唯一的 F_destination_address。

当在一个网络上运行多个 DP 主站系统和 PROFINET IO 系统时，为了确保网络范围内唯一的 F_destination_address 分配，必须在网络的各个站中放置 F-I/O 之前，在 S7

Distributed Safety F 系统中各自设置“PROFIsafe 地址的基数” (Basis for PROFIsafe addresses) 参数（在 F-CPU 的对象属性中）。

如果您更改 F_destination_address，系统将自动检查 F_destination_address 在站内的唯一性。您自己必须确保 F_destination_address 在网络范围内是唯一的。

在安装 F-I/O 之前，您必须通过 DIP 开关设置 F-I/O 上的 F_destination_address。

说明

对于以下 S7-300 F-SM，F_destination_address 与 F-SM/8 的起始地址相同：

- SM 326; DI 24 x 24 VDC（订货号 6ES7326-1BK00-0AB0）
- SM 326; DI 8 x Namur（订货号 6ES7326-1RF00-0AB0）
- SM 326 DO 10 x 24 VDC/2 A（订货号 6ES7326-2BF01-0AB0）
- SM 336; AI 6 x 13 Bit（订货号 6ES7336-1HE00-0AB0）

“PROFIsafe 地址的基数”不会影响这些 F-SM 的 F_destination_address 的分配。

如果您还使用其它 F-I/O，请为这些 F-SM 分配低位起始地址。

F_source_address

将在 *S7 Distributed Safety* 中自动分配 F_source_address。

地址分配规则

**警告****PROFIBUS 子网规则:**

F-I/O 的 PROFIsafe 目标地址以及地址开关的开关设置在网络范围*和站范围**（系统范围）内必须是唯一的。对于 S7-300 F-SM 和 ET 200S、ET 200eco、ET 200pro F 模块，最多可以分配 1022 个不同的 PROFIsafe 目标地址。

例外情况：可为不同智能从站中的 F-I/O 分配相同的 PROFIsafe 目标地址，因为仅在站内对它们进行寻址，即通过智能从站中的 F-CPU 寻址。

以太网子网和 PROFIBUS 与以太网子网混合组态的规则:

F-I/O 的 PROFIsafe 目标地址以及地址开关设置只需在以太网子网范围***（包括所有低级别 PROFIBUS 子网）和站范围**（系统范围）内是唯一的。对于 S7-300 F-SM 和 ET 200S、ET 200eco、ET 200pro F 模块，最多可以分配 1022 个不同的 PROFIsafe 目标地址。

例外情况：可为不同智能从站中的 F-I/O 分配相同的 PROFIsafe 目标地址，因为仅在站内对它们进行寻址，即通过智能从站中的 F-CPU 寻址。

一个以太网子网内网络节点的特点是 IP 地址具有相同的子网地址，即，在子网掩码中 IP 地址均使用数字“1”。

实例:

IP 地址: 140.80.0.2.

子网掩码: 255.255.0.0 = 11111111.11111111.00000000.00000000

含义: IP 地址的字节 1 和 2 用于定义子网; 子网地址 = 140.80。

*网络由一个或多个子网组成。“网络范围”表示超出子网边界。

**该地址对于 *HW Config* 中组态的站是唯一的（例如 S7-300 站或智能从站）

***在以太网子网中，周期性 PROFINET IO 通讯（RT 通讯）除外

S7-300 F-SM 的组诊断

“组诊断” (Group diagnostics) 参数用于激活和取消激活将 F-SM 特定通道的诊断消息（例如断线和短路）传送到 F-CPU。为保持可用性，应关闭以下 F-SM 未使用的输入或输出通道上的组诊断：

- SM 326; DI 8 x NAMUR
- SM 326; DO 10 x 24 VDC/2 A
- SM 336; AI 6 x 13 Bit



对于安全模式中的故障安全 F-SM，必须激活所有已连接通道上的“组诊断”。

建议您进行检查，以验证是否仅关闭了未使用的输入和输出的通道组诊断。

可以选择启用诊断中断。

对于 SM 326; DI 24 x 24 VDC（订货号 6ES7326-1BK01-0AB0 或更高）和 SM 326; DO 8 x 24 VDC/2 A PM，以下情况适用：

如果在 *STEP 7 HW Config* 中取消激活某个通道，则该通道的组诊断将被同时取消激活。

2.5 对故障安全 DP 标准从站和故障安全标准 I/O 设备进行组态

要求

为了使用带 S7 Distributed Safety 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 PROFI-safe 总线规约。基于 IE/PB Link 的 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 PROFI-safe 总线规约。

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 PROFI-safe 总线规约。

使用 GSD 文件的组态

与在标准系统中一样，组态故障安全 DP 标准从站的基础是 GSD 文件中的设备规范。

GSD 文件包含 DP 标准从站或标准 I/O 设备的所有属性。对于故障安全 DP 标准从站/标准 I/O 设备，部分规范由 CRC 确保。

GSD 文件由设备制造商提供。

GSD 文件中设备数据结构的保护

自 *PROFI-safe 规范 V2.0* 开始，必须使用 GSD 文件中存储的 CRC (F_IO_StructureDescCRC 的“设定值”)来保护该文件中的设备数据结构。

F_IO_StructureDescCRC

当组态的每个故障安全 DP 标准从站或标准 I/O 设备位于 *HW Config* 中或位于硬件配置项目数据的打印输出中时，将收到下面其中一条信息：

- *S7 Distributed Safety* 计算出来的 F_IO_StructureDescCRC 值与安装的 GSD 文件中的这个“设定值”匹配/不匹配。
- 安装的 GSD 文件中没有提供 F_IO_StructureDescCRC 的“设定值”

说明

如果使用 *S7 Distributed Safety V5.4 SP4* 编译项目，则 F_IO_StructureDescCRC 的信息与系统验收测试无关（请参阅『系统验收测试』一章）。

对于高于 **V5.4 SP4** 版本的 **S7 Distributed Safety**，F_IO_StructureDescCRC 校验必须无错（计算的值与设定值相匹配）。因此，应从设备制造商获取包括 F_IO_StructureDescCRC 设定值的正确的 GSD 文件。

使用 GSD 文件进行组态的操作步骤

将 GSD 导入项目（请参阅 *STEP 7 在线帮助*）。

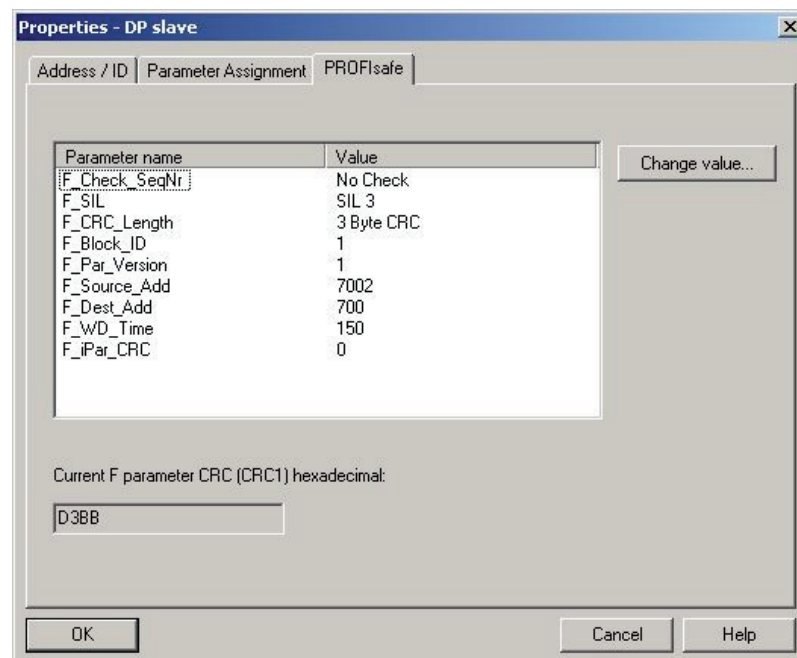
1. 在 *HW Config* 的硬件目录中选择故障安全标准 DP 标准从站/标准 I/O 设备并将其插入 DP 主站系统或 IO 系统。
2. 选择故障安全 DP 标准从站/标准 I/O 设备。
3. 使用 **编辑 (Edit) > 对象属性 (Object Properties)** 菜单命令或双击 F 组件插槽来打开对象属性对话框。打开对话框后，将提示您输入安全程序密码，或者必须在另一个对话框中设定安全程序的密码。有关安全程序密码的信息，请参考『访问保护概述』一章。

不支持故障安全 DP 标准从站/标准 I/O 设备的通道级钝化。

“PROFIsafe”选项卡

GSD 文件中指定的参数文本包含在“PROFIsafe”选项卡中的“参数名称”(Parameter name)下，而每个参数的当前值位于“值”(Value)下面。可使用“更改值...” (Change Value...) 按钮来修改值。

下面将介绍这些参数：



“F_Check_SeqNr”参数

该参数定义了 F 用户数据帧的一致性检查（CRC 计算）中是否包含顺序编号。

在 PROFIsafe V1 MODE 中，需要将“F_Check_SeqNr”参数设置为 "No check"。仅支持具有相应响应的故障安全 DP 标准从站。在 PROFIsafe V2 MODE 中，“F_CHECK_SeqNr”参数不重要。

“F_SIL”参数

该参数定义了故障安全 DP 标准从站或标准 I/O 设备的安全等级。该参数由设备自身决定。根据 GSD 文件，可以将“F_SIL”参数设置为“SIL 1”至“SIL 3”。

“F_CRC_Length”参数

根据 F 用户数据（过程数据）的长度、安全等级和 PROFIsafe MODE，CRC 签名长度必须为 2、3 或 4 个字节。该参数向 F-CPU 提供安全消息帧中 CRC2 键大小的信息。

在 PROFIsafe V1 MODE 中：

对于长度小于或等于 12 个字节的用户数据，为“F_CRC_Length”参数设置 "2-byte CRC"；对于长度在 13 个字节到 122 个字节之间的用户数据，则设置为 "4-byte CRC"。

S7 Distributed Safety 仅支持“2 个字节的 CRC” (2-byte CRC)；故障安全 DP 标准从站必须相应动作。

在 PROFIsafe V2 MODE 中：

对于长度小于或等于 12 个字节的用户数据，为“F_CRC_Length”参数设置 "3-byte CRC"；对于长度在 13 个字节到 123 个字节之间的用户数据，则设置为 "4-byte CRC"。

S7 Distributed Safety 仅支持“3 个字节的 CRC” (3-byte CRC)；故障安全 DP 标准从站/标准 I/O 设备必须相应动作。

“F_Block_ID”参数

如果存在 F_iPar_CRC 参数，则 F_Block_ID 参数的值为 1，否则为 0。

F_Block_ID 参数指示 F_iPar_CRC 值的数据记录已扩展了 4 个字节。不得更改此参数。

“F_Par_Version”参数

该参数用于标识 PROFIsafe 工作模式。可以从提供的这个参数值了解到设备支持的工作模式。对于故障安全标准 IO 设备，该参数设置为“1” (PROFIsafe V2 MODE) 并且不可更改。

对于故障安全 DP 标准从站，可对该参数进行如下设置：

- 如果设备和 F-CPU 都支持，则将同类 PROFIBUS DP 网络的“F_Par_Version”设置为“1”(PROFIsafe V2 MODE)。否则，设置为“0” (PROFIsafe V1 MODE)。
- 对于包含 PROFIBUS DP 和 PROFINET IO 子网的混合网络，必须将“F_Par_Version”设置为“1” (PROFIsafe V2 MODE)。

说明

以下 F-CPU 支持 V2 MODE：

- CPU 416F-2，固件版本 V4.1 及更高版本
- CPU 416F-3 PN/DP
- IM 151-7 F-CPU，固件版本 V2.6 及更高版本
- CPU 315F-2 PN/DP
- CPU 315F-2 DP，固件版本 V2.6 及更高版本
- CPU 317F-2 PN/DP
- CPU 317F-2 DP，固件版本 V2.5 及更高版本
- CPU 319F-3 PN/DP

如果将不支持 V2 MODE 的 F-CPU 的“F_Par_Version”设置为“1”，会导致与设备进行安全相关通讯时出现通讯错误。然后下面其中一条诊断事件进入 F-CPU 诊断缓冲区：

- “F-I/O 已钝化” (F-I/O passivated)： 校验值错误 (CRC)/顺序号错误...
- “F-I/O 已钝化” (F-I/O passivated)： 监视安全消息帧超时...

**警告**

对于包含 PROFIBUS DP 和 PROFINET IO 子网的混合网络，必须将“F_Par_Version”设置为“1” (PROFIsafe V2 MODE)。不支持 PROFIsafe V2 MODE 的设备不得用于 PROFINET IO 或者包含 PROFIBUS DP 与 PROFINET IO 的混合组态中。

“F_Source_Add”和“F_Dest_Add”参数

PROFIsafe 地址 (“F_Source_Add”和“F_Dest_Add”参数) 用于唯一标识源地址和目标地址。

故障安全 DP 标准从站和标准 I/O 设备的“F_Source_Add”和“F_Dest_Add”参数对应于其它 F-I/O 的“F_source_address”和“F_destination_address”参数。例外情况：值范围由 GSD 文件指定，并且不限于 PROFIsafe 目标地址范围 1 到 1022。否则，请参见『对 F-I/O 进行组态』章节中关于 PROFIsafe 地址分配的信息。

“F_WD_Time”参数

该参数定义了故障安全 DP 标准从站/标准 I/O 设备的监视时间。

来自 F-CPU 的当前有效安全消息帧必须在这个监视时间段内到达。这将确保检测到故障和错误，并触发适当的响应，以使 F 系统保持在安全状态或进入安全状态。

选择的监视时间应足够长以容许通讯中的帧延迟，同时应确保当出现连接中断或其它故障时故障响应功能能够及时响应（请参阅『SIMATIC S7 中的安全工程』系统手册）。

可以将“F_WD_Time”参数按 1 ms 递增设置。“F_WD_Time”参数的值范围由 GSD 文件指定。

“F_iPar_CRC”参数

通过各个设备参数 (i-参数) 的 CRC。

故障安全 DP 标准从站/标准 I/O 设备的各个设备参数 (i-参数) 用设备制造商提供的参数分配工具进行设置。

在此处输入由设备制造商提供的参数工具所计算出的 CRC，以保护 i-参数。S7 *Distributed Safety* 在计算 CRC F 参数 (CRC1) 时会考虑该值。

参见

对 F-I/O 进行组态 (页 37)

2.6 分配符号名

F-I/O DB 的符号名

在 *HW Config* 中编译期间，将自动为每个 F-I/O 创建一个 F-I/O DB，并在符号表中输入 F-I/O DB 的符号名。

所有生成的符号名都包含“F”前缀、F-I/O 的起始地址、以及 *HW Config* 的对象属性中为 F-I/O 模块输入的名称（最长 17 个字符），例如 F00005_4_8_F_DI_24VDC。因此，名称中的所有特殊字符都将替换为“_”。

对于通过智能从站与从站通讯访问的 F-I/O，要在 F-I/O 的起始地址后添加 X（例如 F00005_X_4_8_F_DI_DC24V），表示 "Mode: F-DX-Module"，即故障安全智能从站与从站通讯）。

如果不想用 F-I/O 对象属性中输入的默认名称作为符号名，必须首先更改 F-I/O 对象属性中的名称，然后在 *HW Config* 中进行首次编译。请注意，仅将前 17 个字符输入到符号名中。

首次编译之后，只能对符号名进行如下更改：

- 在符号表中直接编辑符号名
(请注意，符号长度最多包括 24 个字符且符号名与 F-I/O 对象属性中的名称不再匹配。)
或
- 删除可用的符号表条目，并在对象属性中更改名称，然后在 *HW Config* 中重新编译。

说明

使用故障安全 DP 标准从站/标准 I/O 设备时，请勿将 *HW Config* 中输入的 "description" 当作名称用来生成相关 F-I/O DB 的符号名。在这种情况下，总是使用前缀“F”、故障安全 DP 标准从站/标准 I/O 设备的起始地址以及一个固定的字符串来生成符号名。只能通过直接在符号表中直接编辑来更改符号名。



始终使用 F-I/O DB 编号（而非符号名中缺省输入的起始地址）将 F-I/O DB 分配给特定的 F-I/O 模块。

因此，不得修改自动分配的 F-I/O DB 编号；否则，安全程序将无法访问为 F-I/O 分配的 F-I/O DB。

2.6 分配符号名

SM 336; AI 6 x 13 Bit 和 SM 336; F-AI 6 x 0/4-20 mA HART 的输入通道的符号名

如果要为 SM 336; AI 6 x 13 Bit 或 SM 336; F-AI 6 x-0/4 20 mA HART 的输入通道分配符号名，请确保这些符号是 INT 数据类型。

参见

F-I/O DB (页 104)

访问保护

3.1 访问保护概述

引言

对 S7 Distributed Safety F 系统的访问受两个密码保护：一个用于 F-CPU，另一个用于安全程序。

安全程序的密码又分为离线密码和在线密码。

- 离线密码是编程设备上离线项目中安全程序的一部分。
- 在线密码是 F-CPU 中安全程序的一部分。

下表概述了 F-CPU 和安全程序的访问许可。

下表介绍了如何分配密码以及如何设置、更改和取消对 F-CPU 和安全程序的访问许可。

3.1 访问保护概述

	F-CPU 的密码	安全程序的密码
分配	<p>在 <i>HW Config</i> 中组态 F-CPU 时，选择 Properties - CPU、"Protection" 选项卡以及需要的保护级别，例如选择 "1: Access protection for F-CPU"、"Removable with Password" 和 "CPU Contains Safety Program" 复选框</p>	<ul style="list-style-type: none"> • 在 <i>SIMATIC 管理器</i> 中，使用 选项 (Options) > 编辑安全程序 (Edit Safety Program) > Permission (许可) 菜单命令 • 首次打开 F-PB 时 • 首次打开 F-FB/F-FC 时 • 首次打开 F-DB 时 • 首次打开“编辑 F 运行组” (Edit F-Runtime Groups) 对话框时 • 首次进行编译时 <p>在 <i>HW Config</i> 中，首次执行保存操作后：</p> <ul style="list-style-type: none"> • 将设置为“安全模式”的 F-I/O 排在组态表中时 • 首次打开 F-CPU 对象属性中的“F 参数” (F parameters) 选项卡时 • 首次打开 F-I/O 的对象属性时 • 首次打开智能从站对象属性对话框中的“F 组态” (F-Configuration) 选项卡时 • 首次打开故障安全 DP 标准从站/标准 I/O 设备的对象属性对话框中的“PROFIsafe”选项卡时 • 上述选项卡和对话框中的参数被更改时 • 从组态表中删除 F-I/O 或 F-CPU 时

	F-CPU 的密码	安全程序的密码
提示	<ul style="list-style-type: none"> • 下载整个安全程序时 • 下载和删除具有 F-Attribute 的 F 块时 	离线密码: <ul style="list-style-type: none"> • 在 <i>SIMATIC 管理器</i> 中下载 F 块时 • 在“安全程序” (Safety Program) 对话框中进行编译时 • 使用“检查块的一致性” (Check block consistency) 功能进行编译时 • 打开 F-PB 时 • 打开 F-FB/F-FC 时 • 打开 F-DB 时 • 为用户创建的 F-FB、F-FC 和 F-DB 设置知识产权保护时 • 打开“编辑 F 运行组” (Edit F-Runtime Groups) 对话框时 • 更改密码时 • 将设置为“安全模式”的 F-I/O 排放在组态表中时 • 打开对象属性中的“F 参数” (F parameters) 选项卡时 • 打开 F-I/O 的对象属性对话框时 • 打开故障安全 DP 标准从站/标准 I/O 设备的对象属性对话框中的“PROFIsafe”选项卡时 • 上述选项卡和对话框中的参数被更改时 • 从组态表中删除 F-I/O 或 F-CPU 时 • 保存和编译硬件配置时 (仅保护安全程序不被更改) • 在安全程序的离线块文件夹中创建/插入/移动 (新的) F 块时* • 保存 F 块时 • 在安全程序的离线块文件夹中重命名 F 块时* • 从安全程序的离线块文件夹中剪切并删除 F 块时* • “重新接线” F 块时 • 保存写保护的 F 块时 • 删除离线块文件夹时* • 删除“S7 程序” (S7 Programs) 文件夹时* • 打开 F 块的对象属性时* • 编辑 F 块的对象属性时*

3.2 安全程序的访问许可

	F-CPU 的密码	安全程序的密码
		离线密码 <ul style="list-style-type: none"> 取消激活安全模式时（尽管对安全程序的访问许可仍有效，但还是必须输入密码） 修改安全程序中的数据时 在安全程序的离线块文件夹中创建新 F 块时
有效性	输入正确的密码后，就可以进行访问，直到关闭 <i>SIMATIC 管理器</i> 或使用 PLC > 访问权限 (Access Rights) > 取消 (Cancel) 菜单命令取消访问许可。	输入正确的密码后，在 1 小时内有权进行访问。 有关其它信息，请参阅『安全程序的访问许可』一章。
*条件：安全程序分配给 F-CPU。		

3.2 安全程序的访问许可

为安全程序分配密码的操作步骤

请按照以下操作步骤分配安全程序的密码：

1. 在 *SIMATIC 管理器* 中，选择 F-CPU 或其 S7 程序。
2. 选择选项 (Options) > 编辑安全程序 (Edit Safety Program) 菜单命令。

将显示“安全程序” (Safety Program) 对话框。

3. 单击“许可...” (Permission...)，然后在“设置安全程序的许可” (Set up permission for safety program) 对话框中的“新建密码” (New password) 和“确认密码” (Confirm password) 区域中输入安全程序的密码。

如果尚未指定安全程序的密码，但是执行某个操作时触发了安全程序的密码提示（请参阅密码指定和提示表格），则将自动显示用于指定安全程序密码的“设置安全程序的许可” (Set up permission for safety program) 对话框。

说明

使用“安全程序” (Safety Program) 对话框下载安全程序到 F-CPU 可以确保安全程序的在线密码和离线密码保持相同，否则无法使用 *SIMATIC 管理器* 和 *LAD/FBD 编辑器* 来下载此安全程序。



警告

为了实现最佳的访问保护，必须为 F-CPU 和安全程序使用不同的密码。



如果没有通过访问保护将编程设备或 PC 的访问权授予那些有权限修改安全程序的人员，则必须采取以下组织措施来确保编程设备或 PC 上的密码保护有效性：

- 只有经过授权的人员才有权使用密码。
- 在离开编程设备或 PC 之前，经授权的人员必须明确取消安全程序的访问许可。如果未严格执行此操作，还必须使用只有授权人员可以使用的密码保护的屏保程序。

更改安全程序的密码

也可以使用“设置安全程序的许可” (Set up permission for safety program) 对话框来更改安全程序的密码。操作步骤与在 Windows 中更改密码的步骤相同：先输入旧密码，再输入两次新密码。

设置安全程序访问许可的操作步骤

要设置安全程序的访问许可：

1. 在 *SIMATIC 管理器* 中，选择 F-CPU 或其 S7 程序。
2. 选择选项 (Options) > 编辑安全程序 (Edit Safety Program) 菜单命令。
将显示“安全程序” (Safety Program) 对话框。
3. 单击“许可...” (Permission...), 然后在“设置安全程序的许可” (Set up permission for safety program) 对话框中的“旧密码” (Old password) 区域中输入安全程序的密码。

如果尚未设置任何访问许可，但是执行某个操作时触发了安全程序的密码提示（请参阅密码指定和提示表格），将自动显示用于设定密码的“安全程序的密码” (Password for safety program) 对话框。

3.2 安全程序的访问许可

安全程序访问许可的有效性

设置安全程序的访问许可可以使进行设置时的当前 **Windows** 用户进行独有的访问。此外，安全程序的访问许可仅在进行设置时安全程序所在项目的环境中发挥作用。输入正确的密码后，可在 1 小时内或取消许可之前进行访问。

在此一小时内，每次在线操作触发密码提示都会将在线密码的有效期复位为 1 小时（请参阅密码指定和提示表格），同样，每次离线操作触发密码提示都会将离线密码的有效期复位为 1 小时。

如果访问许可的有效期到期，而您当时正在执行需要密码的操作（例如编辑 **F-Block**），那么当保存时系统将再次提示您输入当前密码。如果不输入密码，则无法保存此操作的结果。

取消安全程序的访问许可

在“**Set up permission for safety program**”（设置安全程序的许可）对话框中单击“**Cancel**”（取消）按钮可以取消安全程序的访问许可。

在“**Safety Program**”（安全程序）对话框中单击“**Permission...**”（许可...）按钮上的下拉箭头也可以取消安全程序的访问许可。

下次执行需要密码的操作（请参阅密码指定和提示表格）时，系统则将提示用户再次输入安全程序的密码。要在使用修改功能时“取消”访问许可，必须终止到 **F-CPU** 的连接（例如，关闭 **STEP 7** 应用程序）。

当退出所有已打开 **S7 Distributed Safety** 的 **STEP 7** 应用程序（例如 **SIMATIC 管理器**、**FBD/LAD 编辑器**）时，将自动重设安全程序的访问许可。如果在退出这些 **STEP 7** 应用程序后又重新打开 **STEP 7**，并且执行需要密码的操作时，则系统将再次提示您输入安全程序的密码。

3.3 在没有安全程序密码情况下的读取访问

在没有密码情况下的读取访问

使用“安全程序的密码”(Password for Safety Program) 对话框可以设置安全程序的密码。此外，可以选择在没有密码的情况下进行读取访问。

可以在没有密码的情况下使用读取访问来访问 F-CPU、F-I/O、F 块和安全相关通讯的 F 相关选项卡与对象属性对话框、安全程序的 F 块和“编辑 F 运行组”(Edit F-Runtime Groups) 对话框。

“安全程序的密码”(Password for Safety Program) 对话框

“安全程序的密码”(Password for Safety Program) 对话框如下：



所有其它操作的读取访问

如果已为所有其它操作指定读取访问，则系统不会提示用户输入密码以进行其它读取访问，并且允许只读访问。

例外情况： 不允许对请求的操作进行读取访问，此时您可以终止读取访问。

所有其它操作的读取访问都不受时间限制。这仅应用于已激活此权限的安全程序，但不应用于相同编程设备或 PC 上的其它安全程序。

终止所有其它操作的读取访问

当执行以下某一操作时，将终止所有其它操作的读取访问：

- 在“设置安全程序的许可”(Set Up Permission for Safety Program) 对话框中取消访问许可
- 在“安全程序”(Safety Program) 对话框中单击“许可...”(Permission...) 按钮上的下拉箭头取消访问许可。

3.3 在没有安全程序密码情况下的读取访问

- 关闭所有 S7 应用程序，这些程序正处理对所有其它操作具有读取访问权限的安全程序的数据。
- 已为不允许进行读取访问的操作（例如编译安全程序）输入安全程序的密码
- 重新启动编程设备或 PC

该访问的只读访问

如果已指定一次性读取访问，则当进行下一次读取访问和需要密码的所有其它操作时，系统将再次提示用户输入密码。

3.4 F-CPU 的访问许可

为 F-CPU 指定密码的操作步骤

当组态 F-CPU 时为 F-CPU 指定密码（请参阅『组态 F-CPU』一章）。

更改 F-CPU 的密码

只能通过修改组态来更改 F-CPU 的密码。必须将 F-CPU 切换到 STOP 模式来下载已修改的组态。

设置 F-CPU 的访问许可的操作步骤

1. 在 *SIMATIC 管理器* 中，选择 F-CPU 或其 S7 程序。
2. 选择 **PLC > 访问权限 (Access Rights) > 设置 (Setup)**。在随即打开的对话框中，输入在“保护”(Protection) 选项卡中组态 F-CPU 时为其指定的密码。



警告

如果没有通过访问保护将编程设备或 PC 的访问权授予那些有权限修改安全程序的人员，则必须采取以下组织措施来确保 PG/PC 上 F-CPU 的密码保护有效性：

- 只有经过授权的人员才有权使用密码。
- 在离开编程设备或 PC 之前，经授权的人员必须明确取消 F-CPU 的访问许可。如果未严格执行此操作，还必须使用只有授权人员才能访问的密码保护屏保程序。

取消访问许可后，应检查在线块文件夹中具有 F 属性的所有 F 块的集体签名与已验收的安全程序的块文件夹中具有 F 属性的所有 F 块的集体签名是否完全相同。如果两者不同，则必须将正确的安全程序下载到 F-CPU。

F-CPU 的访问许可的有效性/取消

F-CPU 的访问许可将一直有效，直到关闭 *SIMATIC 管理器*，或使用 **PLC > 访问权限 (Access Rights) > 取消 (Cancel)** 菜单命令取消许可或关闭上一个 S7 应用程序。

将安全程序传送到多个 F-CPU



如果一台编程设备或 PC 通过网络（例如 MPI）可以访问多个 F-CPU，则必须采取以下措施以确保将安全程序下载到正确的 F-CPU：

对于每个 F-CPU 都使用特定的密码，例如，F-CPU 的统一密码加上各自的 MPI 地址作为扩展（最多 8 个字符）：“PW_8”。

请注意以下几点：

- 第一次为 F-CPU 分配密码时，必须使用点对点连接（与第一次为 F-CPU 分配 MPI 地址相似）。
- 将安全程序下载到 F-CPU（尚未建立通过 F-CPU 密码获得的访问权限）前，必须首先取消对所有其它 F-CPU 的现有访问许可。

参见

组态 F-CPU (页 28)

编程

4.1 编程概述

4.1.1 编程概述

引言

安全程序包括从 F 库选择或使用 F-FBD 或 F-LAD 编程语言创建的故障安全块，以及在编译安全程序时自动添加的故障安全块。系统会将故障控制措施自动添加到您创建的安全程序，并执行其它安全相关的测试。

概述

本节包含对以下内容的说明：

- S7 Distributed Safety 中安全程序的结构
- 故障安全块
- F-FBD/F-LAD 编程语言与标准 FBD 和 LAD 语言之间的区别

使用标准用户程序和安全程序的项目的基本结构

下图显示了使用标准用户程序 and S7 Distributed Safety 安全程序的编程设备/PC 中的 *STEP 7* 项目的基本结构。

S7 Distributed Safety 选件包随附了用于创建安全程序的 *Distributed Safety* F 块库 (V1)。

F 库位于 *step7/s7libs* 目录中。

有关编程的其他信息将在以下部分中提供。

4.1 编程概述

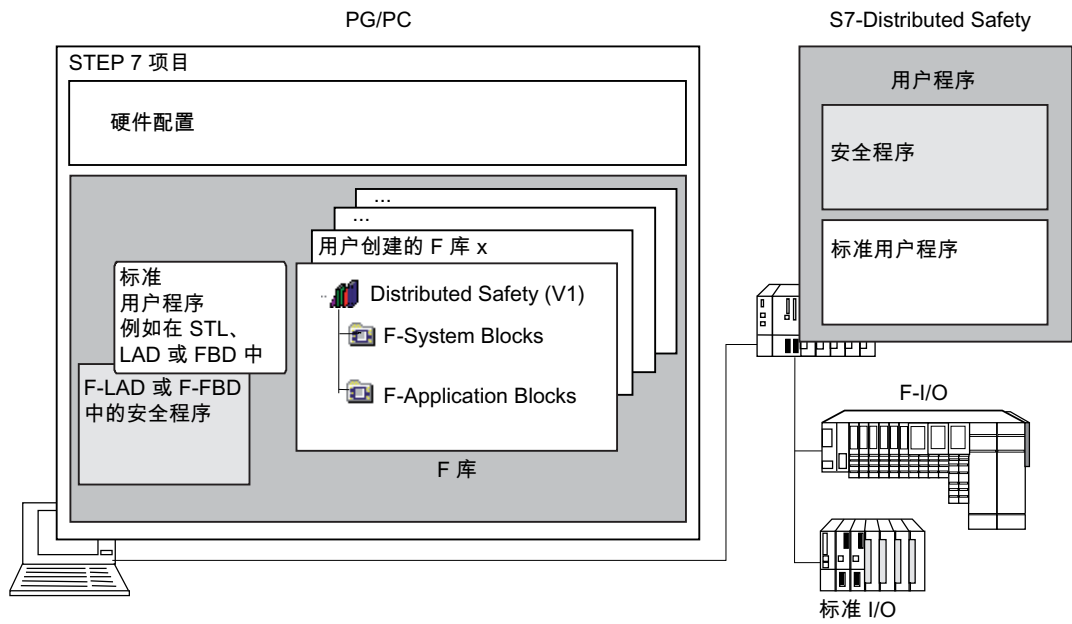


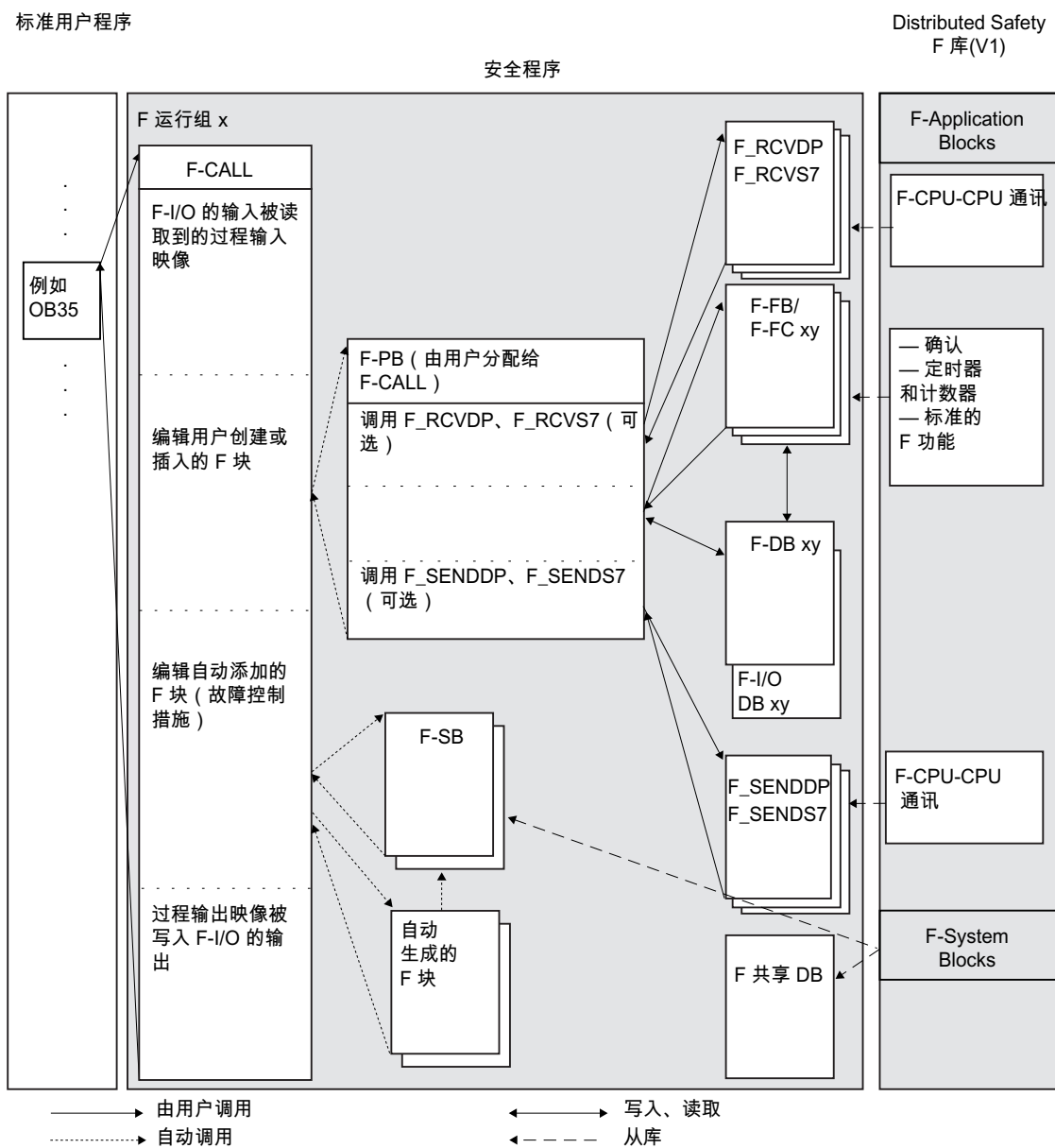
图 4-1 组态

4.1.2 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* 安全程序的基本结构。为了结构化，一个安全程序由一个或两个 F 运行组组成。每个 F 运行组包含：

- 创建的 F 块，或者从 *Distributed Safety* F 库 (V1) 或用户创建的 F 库中选择的 F 块
- 自动添加的 F 块 (F 系统块、自动生成的 F 块和 F 共享 DB)



程序结构说明

通过从标准用户程序中调用 **F-CALL** 来编写安全程序的入口。在 **OB** 中，更应在周期性中断 **OB**（例如，**OB35**）中直接调用 **F-CALL**。

使用周期性中断 **OB** 的优点是它们可以固定的时间间隔中断标准用户程序 **OB1** 中的循环程序的执行；即，在周期性中断 **OB** 中以固定时间间隔调用并执行安全程序。

执行安全程序后，标准用户程序将恢复运行。

F 运行组

为了便于处理，一个安全程序由一个或两个“**F 运行组**”组成。**F 运行组**是由 **F 系统**在内部形成的多个相关的 **F 块**的逻辑结构。

F 运行组包括以下各项：

- 一个 **F 调用块 F-CALL**
- 一个 **F 程序块 F-PB**（分配给 **F-CALL** 的 **F-FB/F-FC**）
- 使用 **F-FBD** 或 **F-LAD** 编程的其他 **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**
- 用户创建的 **F 库**中的 **F 块**
- **F 系统块 F-SB**
- 自动生成的 **F 块**

两个 F 运行组中安全程序的结构

可以将安全程序分为两个 **F 运行组**。通过让部分安全程序（一个 **F 运行组**）以较快的优先级等级运行，实现响应时间较快的安全回路。

参见

安全程序的 **F 运行组**的规则 (页 91)

4.1.3 故障安全块

F 运行组的 F 块

可在 F 运行组中使用下表中的 F 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。 您可以创建 F-CALL，但无法对其进行编辑。可以在 OB 中调用 F-CALL 或在 OB 中调用的 FB/FC 中来调用 F-CALL。	F-CALL
F-FB/F-FC、 F-PB	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。可以在 F-PB 中执行： <ul style="list-style-type: none"> • 使用 F-FBD 或 F-LAD 对安全程序进行编程 • 调用其他已创建的 F-FB/F-FC 以构建安全程序 • 从 <i>Distributed Safety</i> F 库 (V1) 中插入 <i>F 应用程序块</i> 文件夹的 F 块。 • 从“用户创建的 F 库”中插入 F 块 您定义 F-PB 中 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进行读/写访问的可选故障安全数据块	F-DB
F-I/O DB	在 <i>HW Config</i> 中进行编译时，将为每个 F-I/O 自动创建一个 F-I/O DB。您可以或必须访问与 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|块文件夹中的 *F* 应用程序块
- *F* 系统块|块文件夹中的 *F* 系统块和 *F* 共享 DB

下表列出了块文件夹中包括的 *F* 块:

块文件夹	... <i>F</i> 块的用途	功能/ <i>F</i> 块
F 应用程序块		该块文件夹包含用户可以在 <i>F</i> -PB/ <i>F</i> -FB/ <i>F</i> -FC 中调用的 <i>F</i> 应用程序块
	安全相关的 CPU 与 CPU 通讯	用于安全相关的 CPU 与 CPU 通讯的 <i>F</i> 应用程序块: 在安全相关的 CPU 与 CPU 通讯期间, 用于发送和接收数据的 <i>F</i> _SENDDP、 <i>F</i> _RCVDP、 <i>F</i> _SENDS7 和 <i>F</i> _RCVS7
	确认	用于通过操作员监视和控制系统确认故障安全的 <i>F</i> 应用程序块 <i>F</i> _ACK_OP 用于全面确认 <i>F</i> 运行组的所有 <i>F</i> -I/O 的 <i>F</i> 应用程序块 <i>F</i> _ACK_GL
	定时器和计数器	<i>F</i> 应用程序块 <i>F</i> _TP、 <i>F</i> _TON、 <i>F</i> _TOF; <i>F</i> 应用程序块 <i>F</i> _CTU、 <i>F</i> _CTD、 <i>F</i> _CTUD
	预制的 <i>F</i> 功能	用于诸如双手操作监视、暂时失效、急停、安全门监视和反馈回路监视等功能的 <i>F</i> 应用程序块
	数据转换和数据换算	<i>F</i> 应用程序块 <i>F</i> _SCA_I、 <i>F</i> _BO_W、 <i>F</i> _W_BO
	复制	<i>F</i> 应用程序块 <i>F</i> _INT_WR、 <i>F</i> _INT_RD
	移位指令	<i>F</i> 应用程序块 <i>F</i> _SHL_W、 <i>F</i> _SHR_W
F 系统块		该块文件夹包含自动插入安全程序中的 <i>F</i> 系统块 (<i>F</i> -SB) 和 <i>F</i> 共享 DB。

块文件夹	... F 块的用途	功能/F 块
	F 系统块	<p>当编译安全程序以便从用户的安全程序创建可执行安全程序时，F 系统块 (F-SB) 由 <i>S7 Distributed Safety</i> 自动插入。</p> <p>不得从 F-PB/F-FB/F-FC 中的 <i>F 系统块</i> 文件夹插入 F 系统块。同样，不得修改（重命名）或删除 <i>Distributed Safety</i> F 库 (V1) 或用户项目块文件夹中的 F 系统块。</p>
	F 共享 DB	<p>包含安全程序的所有全局数据和 F 系统所需的其他信息的故障安全块。当保存并编译硬件配置时，将自动插入并扩展 F 共享 DB。使用 F 共享 DB 的符号名（即，F_GLOBDB），可以在标准用户程序中评估安全程序的某些数据。</p>

说明

可以在『Distributed Safety F 库 (V1)』一章中找到 F 应用程序块的详细说明。

参见

F-I/O 访问 (页 101)

Distributed Safety F-Library (V1) 概述 (页 177)

自定义 F 库 (页 253)

4.1 编程概述

4.1.4 F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语言之间的区别

引言

通常情况下，F-CPU 中的用户程序由标准用户程序和安全程序组成。标准用户程序是使用标准编程语言（例如，STL、LAD 或 FBD）在 *STEP 7* 中创建的。

S7 Distributed Safety 的安全程序使用 F-FBD 或 F-LAD 进行编程。

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* 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指令集和地址区的限制以及可使用的数据类型的不同。

支持的数据类型和参数类型

F-FBD/F-LAD 支持以下基本数据类型：

- BOOL
- INT
- WORD
- TIME

不允许的数据类型和参数类型

以下为不允许的数据类型和参数类型：

- 以上未列出的基本数据类型（例如，BYTE、DWORD、DINT、REAL）
- 复杂数据类型（例如，STRING、ARRAY、STRUCT、UDT）
- 参数类型（例如，BLOCK_FB、BLOCK_DB、ANY）

支持的地址区

F-CPU 的系统存储器被分为与标准 CPU 的系统存储器相同的地址区。您可以在安全程序中访问下表列出的地址区。

请注意，在 F-FBD 和 F-LAD 中只能访问以下数据：

- BOOL 数据类型的数据（以位为单位）
- INT 数据类型的数据（以字为单位）
- WORD 数据类型的数据（以字为单位）
- TIME 数据类型的数据（以双字为单位）

当通过标准用户程序（标准 I/O 的位存储器或过程映像）对数据进行写访问时，不存在以上限制。

实例：要在 F-I/O 过程输入映像中访问 BOOL 数据类型的输入通道，必须使用“输入（位）”单元。

为了使得程序更加清晰，应该始终使用符号名访问安全程序中的地址区。

地址区	可访问的大小单元：	S7 符号	说明
过程输入映像			
• F-I/O 的			F 运行组 (F-CALL) 开始时，F-CPU 将从 F-I/O 读取输入，并将这些值保存到过程输入映像。输入通道为只读通道。因此，不允许传送到 F-FB 或 F-FC 的 IN_OUT 参数。
数据类型为 BOOL 的通道，例如数字通道	输入（位）	I	数据类型为 BOOL 的输入通道为只读通道，只能使用“输入（位）”单元进行访问。不允许使用其他单元（例如，“输入字”单元）进行访问。
数据类型为 INT (WORD) 的通道，例如模拟通道	输入字	IW	数据类型为 INT (WORD) 的输入通道为只读通道，只能使用“输入字”单元进行访问。不允许使用“输入（位）”单元访问单个位。

地址区	可访问的大小单元:	S7 符号	说明
<ul style="list-style-type: none"> 标准 I/O 的 			每个 OB1 周期开始时, F-CPU 将从标准 I/O 读取输入, 并将这些值保存到过程输入映像。如果使用 S7-400, 请记住使用部分过程映像时的更新次数。
	输入 (位) 输入字	I IW	标准 I/O 的输入通道为只读通道, 只能使用指定的单元进行访问。 因此, 不允许传送到 F-FB 或 F-FC 的 IN_OUT 参数。 此外, 还需要进行过程特定的有效性检查。
过程输出映像			
<ul style="list-style-type: none"> F-I/O 的 			在 F-PB 中, 安全程序将计算 F-I/O 的输出值, 并将其存储在过程输出映像中。F 运行组 (F-CALL) 结束时, F-CPU 将计算的输出值写入 F-I/O 的输出。输出通道为只写通道。 因此, 不允许传送到 F-FB 或 F-FC 的 IN_OUT 参数。
数据类型为 BOOL 的通道, 例如数字通道	输出 (位)	A	数据类型为 BOOL 的输出通道为只写通道, 只能使用“输出 (位)”单元进行访问。不可使用其他单元 (例如, “输出字”单元) 进行访问。
数据类型为 INT (WORD) 的通道, 例如模拟通道	输出字	QW	数据类型为 INT (WORD) 的输出通道为只写通道, 只能使用“输出字”单元进行访问。不允许使用“输出 (位)”单元访问单个位。
<ul style="list-style-type: none"> 标准 I/O 的 			在 F-PB 中, 安全程序还将计算标准 I/O 的输出值 (如果可用), 并将其存储到过程输出映像中。下一个 OB1 周期开始时, F-CPU 将计算的输出值写入标准 I/O 的输出。如果使用 S7-400, 请记住使用部分过程映像时的更新次数。

地址区	可访问的大小单元:	S7 符号	说明
	输出 (位) 输出字	A QW	标准 I/O 的输出通道为只写通道, 只能使用指定的单元进行访问。 因此, 不允许传送到 F-FB 或 F-FC 的 IN_OUT 参数。
位存储器	位存储器 (位) 存储器字	M MW	该区域用于与标准用户程序进行数据交换。 只能使用指定的单元访问存储器。 此外, 读取访问需要进行过程特定的有效性检查。 对于存储器位, 可以在安全程序中进行读取访问或写访问。 因此, 不允许传送到 F-FB 或 F-FC 的 IN_OUT 参数。 请注意, 存储器位只能用于连接标准用户程序和安全程序; 不能将其用作 F 数据的缓冲区。
数据块			数据块存储程序信息。可将这些数据块定义为所有 F-FB、F-FC 和 F-PB 均可对其 (F-DB) 进行访问, 也可以将其指定给特定的 F-FB 或 F-PB (背景数据块)。必须使用“F-DB”编程语言或作为 F-FB 或 F-PB 的背景数据块创建数据块。
	数据位 数据字 数据双字	DBX DBW DBD	本地数据只能使用与声明表中的数据类型相对应的单元进行访问。
本地数据			执行该块时, 该存储区接受块或 F 块的临时数据。本地数据栈还提供用于传送块参数和保存中间结果的存储器。
	本地数据位 本地数据字 本地数据双字	L LW LD	本地数据只能使用与声明表中的数据类型相对应的单元进行访问。

不允许的地址区

不允许使用上表未列出的单元进行访问，尤其不允许访问以下地址区：

- 计数器（使用 *Distributed Safety* F 库 (V1) 中的 F 应用程序块： F_CTU、F_CTD、F_CTUD 来实现故障安全计数器的功能）
- 定时器（使用 *Distributed Safety* F 库 (V1) 中的 F 应用程序块： F_TP、F_TON、F_TOF 来实现故障安全定时器的功能）
- 标准用户程序的数据块
- 使用“OPN DI”的数据块 (F-DB)
- 自动添加的数据块
 - 例外情况： 安全程序的 F-I/O DB 和 F 共享 DB 中的某些数据
- I/O 区： 输入
- I/O 区： 输出

布尔常量“0”和“1”

如果在块调用过程中，需要安全程序中的布尔常量“0”和“1”来分配参数，您可使用具有完整资格的 DB 访问（"F_GLOBDB".VKE0 或 "F_GLOBDB".VKE1）来访问 F 共享 DB 中的变量“VKE0”和“VKE1”。

本地数据地址区：特性**说明**

请注意，当使用本地数据地址区时，对 F-PB、F-FB 或 F-FC 中的本地数据元素的首次访问必须始终为写访问。这可对本地数据元素进行初始化。

请确保对本地数据元素的初始化未被 JMP、JMPN 或 RET 指令（分支）略过。

应使用赋值（“=”）指令 (F-FBD) 或输出线圈（“-()”）指令 (F-LAD) 执行“本地数据位”的初始化。为本地数据位赋一个信号状态（布尔常量“0”或“1”）。

不能使用触发器（SR、RS）、置位输出 (S) 或复位输出 (R) 指令来初始化本地数据位。

如果未遵守上述规定，F-CPU 会切换到 STOP。然后下面其中一条诊断事件进入 F-CPU 诊断缓冲区：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

您可以在所使用的 CPU 产品信息中找到可用于 F-CPU 的地址区。

N、P、NEG、POS、S、R、SR 的地址区；RS 指令：特性**说明**

不得将“过程输入映像”、“过程输出映像”和“位存储器”地址区用于 RLO 沿检测（N、P）指令或地址沿检测（NEG、POS）指令的边沿存储器位或用于触发器（SR、RS）指令的地址。

如果要将“本地数据”地址区用于 RLO 沿检测（N、P）或地址沿检测（NEG、POS）指令的边沿存储器位或用于触发器（SR、RS）、置位输出 (S) 或复位输出 (R) 指令的地址，必须首先对本地数据位进行初始化。

支持的指令

您可以在安全程序中使用下表中列出的指令：

指令		功能	说明
F-FBD	F-LAD		
>=1	-	位逻辑指令	OR 逻辑运算
&	-	位逻辑指令	AND 逻辑运算
XOR	-	位逻辑指令	EXCLUSIVE OR 逻辑操作

指令		功能	说明
---	-	位逻辑指令	插入二进制输入
---o	-	位逻辑指令	取反二进制输入
=	-	位逻辑指令	赋值
-	--- ---	位逻辑指令	常开触点
-	--- / ---	位逻辑指令	常闭触点
-	--- NOT ---	位逻辑指令	反转功率流
-	---()	位逻辑指令	输出线圈
#	---(#)--	位逻辑指令	中线输出
S	---(S)	位逻辑指令	置位输出
R	---(R)	位逻辑指令	复位输出
SR	SR	位逻辑指令	置位-复位触发器
RS	RS	位逻辑指令	复位-置位触发器
N	---(N)---	位逻辑指令	负 RLO 沿检测
NEG	NEG	位逻辑指令	地址负沿检测
P	---(P)---	位逻辑指令	正 RLO 沿检测
POS	POS	位逻辑指令	地址正沿检测
WAND_W	WAND_W	字逻辑指令	(字) AND 字
WOR_W	WOR_W	字逻辑指令	(字) OR 字
WXOR_W	WXOR_W	字逻辑指令	(字) Exclusive OR 字
ADD_I	ADD_I	整数函数	整数相加
DIV_I	DIV_I	整数函数	整数相除
MUL_I	MUL_I	整数函数	整数相乘
SUB_I	SUB_I	整数函数	整数相减
CMP ? I	CMP ? I	比较指令	比较整数 (CMP==I、 CMP<>I、CMP>I、 CMP<I、CMP>=I、 CMP<=I)
NEG_I	NEG_I	转换指令	创建二的补码整数 (16 位)
OPN	---(OPN)	DB 指令	打开数据块
MOVE	MOVE	MOVE 指令	分配值

指令		功能	说明
CALL_FC (将 FC 调用为框)	CALL_FC (将 FC 调用为框)	程序控制	无条件调用 F-FC (EN = 1, EN 没有互连!)
CALL_FB (将 FB 调用为框)	CALL_FB (将 FB 调用为框)	程序控制	无条件调用 F-FB (EN = 1, EN 没有互连!)
vRET	---(RET)	程序控制	返回 (退出块)
调用多重背景	调用多重背景	程序控制	调用多重背景
JMP	---(JMP)	跳转指令	在块中无条件跳转 如果是 1 (条件), 则在块中跳转
JMPN	---(JMPN)	跳转指令	如果是 0 (条件), 则在块中跳转
OV	OV --- ---	状态位	评估异常位溢出 (状态字中的 OV 位)

S 指令: 特性

说明

仅在将置位输出 (S) 指令应用于经钝化的 F-I/O 输出时 (例如, 启动 F 系统时), 才执行该指令。因此, 应仅使用赋值 (“=”) (F-FBD) 或输出线圈 (“--()”) (F-LAD) 指令尝试访问 F-I/O 的输出。

您可以在关联 F-I/O DB 中评估 F-I/O 或 F-I/O 的通道是否已被钝化。

S、R、SR、RS、N、NEG、P、POS 指令：特性**说明**

如果要将 F-FB/F-FC 的形参用于 RLO 沿检测 (N、P) 或地址沿检测 (NEG、POS) 指令的边沿存储器位或用于触发器 (SR、RS)、置位输出 (S) 或复位输出 (R) 指令的地址，则必须将其声明为输入/输出参数。

如果未遵守上述警告，F-CPU 会切换到 STOP。然后下面其中一条诊断事件进入 F-CPU 诊断缓冲区：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

ADD_I、SUB_I、MUL_I、NEG、DIV_I、OV 指令：特性**说明**

如果 ADD_I、SUB_I、MUL_I 或 NEG_I 指令的结果或 DIV_I 指令的商在允许的整数范围（16 位）之外，并且此结果/商通过安全相关的 CPU 与 CPU 通讯用于 F-I/O 或伙伴 F-CPU 的输出中，则 F-CPU 将切换到 STOP 模式。然后下面其中一条诊断事件进入 F-CPU 诊断缓冲区：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

因此，应在编程时执行适当的步骤以不超出允许的整数范围（16 位）或评估 OV 位。

如果尚未为 ADD_I、SUB_I、MUL_I、NEG_I 和 DIV_I 指令编写 OV 位扫描程序，则会发出警告。

通过评估 OV 位，您就可以在发生溢出时识别出溢出，而 F-CPU 也不会切换到 STOP 模式。结果/商类似于标准用户程序中的模拟指令。

说明

只允许在具有影响 OV 位的指令的程序段之后的程序段中执行 OV 位扫描。

具有 OV 位扫描的程序段不得是跳转指令的目标；即，它不得包含跳转标志。

如果在影响 OV 位的指令后的程序段中编写 OV 位扫描程序，则会增加影响 OV 位的指令的执行时间（请参阅用于计算响应时间的 Excel 文件 *s7fcotia.xls*）。

说明

如果 DIV_I 指令的除数（输入 IN2）= 0，则除法的商（输出 OUT 处的除法结果）= 0。该结果类似于标准用户程序中的相应指令。F-CPU 不会切换到 STOP 模式。不管是否在下一个程序段中编写 OV 位扫描程序，均会这样响应。

OPN DB 指令：特性

说明

请记住，在使用“OPN DB”指令时，可以在调用 F-FB/F-FC 和“具有完整资格的 DB 访问”之后更改 DB 寄存器的内容，因此不保证您使用“OPN DB”打开的上一个数据块仍处于打开状态。

因此，在访问 DB 寄存器的数据时，您应使用以下寻址数据的方法来避免出错：

- 使用符号寻址。
- 仅使用具有完整资格的 DB 访问。

如果您仍要使用“OPN DB”指令，则必须在调用 F-FB/F-FC 和“具有完整资格的 DB 访问”之后重复“OPN DB”指令以确保恢复 DB 寄存器。否则，将导致出错。

“具有完整资格的 DB 访问”

对 F-FB/F-FC 中的数据块数据的首次访问**必须**始终是“具有完整资格的 DB 访问”或必须在“OPN DB”指令之前执行。这也适用于在跳转标记后对数据块数据的首次访问。

4.1 编程概述

“具有完整资格的 DB 访问”的实例：

FB5: Title

Comment:

Network 1 : Compare VALUE_A with VALUE_B

With fully qualified access and with symbolic names.

You have to assign a symbolic name, for example "F_DATA_1" for the F-DB, and instead of the absolute addresses, use the names assigned in the declaration of the F-DB.

Symbol information

DB2.DBW0	"F_DATA_1" VALUE_A
DB2.DBW2	"F_DATA_1" VALUE_B
DB2.DBX4.0	"F_DATA_1" RESULT

“不具有完整资格的 DB 访问”的实例：

Network 2 : Open F_DB "F_DATA_1"

Without fully qualified access and without symbolic names

Network 3 : Compare VALUE_A with VALUE_B

Without fully qualified access and without symbolic names

访问背景数据块

您还可以使用具有完整资格的访问来访问 F-FB 的背景数据块，例如传送块参数。不可以访问其他 F-FB 的背景数据块中的静态数据。

请确保未选中 *FBD/LAD 编辑器“常规”* (General) 对话框（通过选项 [Options] > 设置 [Settings] 打开）中的“将交叉引用报告为错误”(Report Cross References as Error)。否则，无法访问背景数据块。

请注意，访问未在安全程序中调用的 F-FB 的背景数据块可能会导致 F-CPU 切换到 STOP 模式。

MOVE 指令：特性

说明

如果输入输出处的数据类型相同，或介于具有 INT 和 WORD 数据类型的数据之间，则可以执行 MOVE 操作。

对于来自标准用户程序的数据，输入和输出处的数据类型长度必须匹配。

调用多重背景：特性

说明

请勿将 F_SENDS7 和 R_RCVS7 F 应用程序块声明为多重背景（即使它们具有“多重背景能力”属性）。

不允许访问声明了多重背景的 F-FB 中的多重背景静态数据。

不允许访问声明了多重背景的 F-FB 之外的多重背景输入和输出。

JMP、JMPN、RET 指令：特性

说明

不允许在跳转指令和跳转指令的关联目标之间编写 F_SENDDP 或 F_SENDS7 的调用程序。

不允许在 F_SENDDP 或 F_SENDS7 调用之前编写 RET 指令。

4.1 编程概述

不允许的指令

不允许执行所有未在上表中列出的指令，尤其是：

- 计数器指令（使用 *Distributed Safety* F 库[V1] 中的 F 应用程序块： F_CTU、F_CTD、F_CTUD 来实现故障安全计数器的功能）
- 定时器指令（使用 *Distributed Safety* F 库[V1] 中的 F 应用程序块： F_TP、F_TON、F_TOF 来实现故障安全定时器的功能）
- 移位和循环指令（使用 *Distributed Safety* F 库[V1] 中 F 应用程序块： F_SHL_W、F_SHR_W 来执行移位指令）
- 以下程序控制指令：
 - 调用标准块（FB、FC）
 - CALL： 调用不带参数的 FC/SFC
 - 有条件地调用 F-FB、F-FC（EN 和 EN 的互连 = 0）
 - 调用 SFB、SFC

说明

在进行故障安全编程时，请勿对允许输入 EN 或允许输出 ENO 进行互连、赋“0”值或评估。

参见

F-I/O 访问 (页 101)

数据从安全程序传送到标准用户程序 (页 127)

数据从标准用户程序传送到安全程序 (页 129)

4.2 创建安全程序

4.2.1 创建安全程序的基本步骤

软件要求

『安装/删除 *S7 Distributed Safety* V5.4 SP4 选件包』一章中说明了软件要求。

其他要求

- 必须在 *SIMATIC* 管理器中创建项目结构。
- 必须在编程之前对项目的硬件组件（尤其是 F-CPU 和 F-I/O）进行组态。
- 必须将安全程序分配给 F-CPU，例如 CPU 315F-2 DP。

创建 *S7 Distributed Safety* 程序的步骤

创建安全程序的主要步骤如下：

步骤	操作	参考
1	在 <i>HW Config</i> 中保存并编译硬件配置，并将其下载到 F-CPU（如果需要）。	组态
2	定义程序结构	定义程序结构
3	在 <i>SIMATIC</i> 管理器中，使用 F-FBD 或 F-LAD 编程语言创建 F-FB 和 F-FC	使用 F-FBD/F-LAD 创建 F 块
4	在 <i>FBD/LAD</i> 编辑器中编辑并保存 F-FB 和 F-FC	使用 F-FBD/F-LAD 创建 F 块
5	指定一个或两个 F 运行组： 对于每个 F 运行组： <ul style="list-style-type: none"> • 将先前编写的 F-FB 或 F-FC 分配给 F 运行组的 F-CALL（分配后将使 F-FB 或 F-FC 成为 F-PB） • 如果 F-PB 是功能块，则分配背景数据块 	定义 F 运行组

步骤	操作	参考
	<ul style="list-style-type: none"> 设置 F 运行组的最大周期时间 	《SIMATIC S7 中的安全工程》系统手册
	<ul style="list-style-type: none"> 如果安全程序的一个 F 运行组要为另一个 F 运行组提供评估数据，则为 F 运行组通讯分配一个 DB。 	定义 F 运行组
6	在“安全程序”(Safety Program) 对话框中编译安全程序	编译安全程序
7	在 OB 中（尽可能在周期性中断 OB 中）直接调用 F 调用块	定义 F 运行组
8	在“安全程序”(Safety Program) 对话框中将整个用户程序（标准用户程序和安全程序）下载到 F-CPU	下载安全程序

参见

安装/删除 S7 Distributed Safety V5.4 SP4 选件包 (页 19)

组态概述 (页 25)

定义程序结构 (页 81)

使用 F-FBD/F-LAD 创建 F 块 (页 82)

安全程序的 F 运行组的规则 (页 91)

编译安全程序 (页 260)

下载安全程序 (页 262)

4.2.2 定义程序结构

两个 F 运行组中安全程序的结构

可以将安全程序分为两个 F 运行组。通过安排部分安全程序（一个 F 运行组）以较快的优先级等级运行，从而获得具有短响应时间的较快安全回路。

说明

通过将安全程序分为两个 F 运行组，可以使安全程序的结构更好。但是请注意，不能对单个 F 运行组执行以下操作，只能对整个安全程序执行：

- 为安全程序指定密码
- 编译安全程序
- 下载安全程序
- 取消激活安全模式
- 比较安全程序
- 打印安全程序

使用安全程序的所有 F 块构成集体签名。

程序结构的规则

为 S7 Distributed Safety 设计安全程序时必须记住以下规则：

- 不得在 OB 中直接调用 F 块；而必须将其插入到一个或两个 F 运行组中。
- 安全程序由一个或两个 F 运行组构成，每个组都有一个 F-CALL。每个 F-CALL 最多可分配一个 F 程序块。
- 只能从一个 F 运行组访问 F-I/O 的通道。
- 只能从一个 F 运行组访问 F-I/O 的 F-I/O DB 的变量，而且只能是从其访问该 F-I/O 的通道 F 运行组（如果进行了访问）中进行访问。
- 要最佳使用本地数据，必须在 OB 中（尽可能在周期性中断 OB 中）直接调用 F 调用块（F 运行组）；不应在这些周期性中断 OB 中声明任何其他本地数据。
- 必须为安全程序保留某些特定的资源。在 *HW Config* 中组态 F-CPU 时，在 F-CPU 的对象属性（Object Properties）对话框中进行此操作。如果未明确进行任何设置，则使用有效的默认值。
- 根据常规 *STEP 7* 规则创建程序。例如，考虑数据流量。

4.3 使用 F-FBD/F-LAD 创建 F 块

说明

在标准用户程序中编写安全功能不需要的程序段，可改进性能。

确定标准用户程序中要包括的元素和安全程序中要包括的元素时，应记住标准用户程序可以更容易地修改和下载到 F-CPU。通常，标准用户程序中的更改不需要接受测试。

参见

组态概述 (页 25)

F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语言之间的区别 (页 66)

安全程序的 F 运行组的规则 (页 91)

安全程序验收测试 (页 301)

4.3 使用 F-FBD/F-LAD 创建 F 块

4.3.1 使用 F-FBD/F-LAD 创建 F 块

概述

本节介绍如何通过 F-FBD 或 F-LAD 使用已创建的 F-FB、F-FC 和/或 F-DB 创建安全程序。基本步骤与创建标准用户程序相同；因此，以下仅介绍与编写标准用户程序不同的地方。

可以在“安全程序”(Safety Program) 对话框中查找有关如何在 *SIMATIC 管理器* 中表示 F 块的说明。

创建单个不分配给 F-CPU 的 F 块

说明

可以直接在 S7 程序中创建不分配给任何 F-CPU 的单个 F 块。这使您可以为不同的 F-CPU 创建安全程序而不用考虑使用的硬件。但是请记住，在这种情况下将不检查 F 地址和 F-I/O 访问的有效性。

参见

“Safety Program”（安全程序）对话框 (页 255)

4.3.2 创建和编辑 F-FB/F-FC

创建和编辑 F-FB/F-FC 的步骤

1. 跳转到 *SIMATIC* 管理器的块文件夹，并选择插入 (Insert) > S7 块 (S7 Block) > 功能 (Function) (或功能块) 菜单命令。也可以使用“插入新对象” (Insert New Object) 快捷菜单。

说明

不得使用为自动添加的 F-Function 块 (F-CPU 对象属性中的“F--function blocks”参数) 保留的编号段中的 FB 编号。

2. 在“属性 - 功能” (Properties - Function) 窗口的“常规 - 第 1 部分” (General - Part 1) 选项卡中，输入 F-FB/F-FC 的名称。选择“F-FBD”或“F-LAD”作为编程语言。单击“确定”(OK) 确认。输入安全程序的密码（在下面的操作步骤中将不再述及密码提示）。
块符号在 *SIMATIC* 管理器中将以黄色高亮显示。

然后可以打开创建的 F 块，并使用 *FBD/LAD* 编辑器进行编辑：

3. 在 *SIMATIC* 管理器中双击 F-FB/F-FC。显示 *FBD/LAD* 编辑器。
4. 应在 *FBD/LAD* 编辑器的“LAD/FBD”对话框中选择“地址类型检查” (Type Check of Addresses) (选项 > 设置) (Options > Settings)。

说明

F 程序元素目录中仅显示以下元素：

- 支持的指令
 - S7 程序的块文件夹中的 F-FB 和 F-FC
 - 来自 F 库中的 F 块，例如 *Distributed Safety* F-Library (V1) 的 F 应用程序块
 - 已编辑的 F 块的多重背景
-

5. 编辑 F-FB/F-FC 块。

进行编辑时，将检查数据类型。检测到的所有错误都将输出在 *FBD/LAD* 编辑器中，与创建标准用户程序时的情况一样。

说明

F-CALL 中调用的 F-FB/F-FC（此时已变为 F-PB）不能具有任何参数，因为它们不能进行初始化（请参阅『定义 F 运行组』）。

说明

F-FB/F-FC 不能调用自身。

说明

从 F-FBD 切换为 F-LAD 时，某些 F-FBD 程序段的图形表示可能无法用 F-LAD 表示；但可使用 STL 显示这些程序段。不得更改其中包含的 STL 代码。

规则： STL 程序段不允许用 F-FBD 表示。如果需要切换为 F-FBD，则必须将用 F-LAD 表示的 STL 程序段重新表示为 F-FBD 程序段。

**警告**

不允许在线或离线编辑 F-FB 的背景数据块，这样会导致 F-CPU 切换到 STOP 模式。

说明

不允许访问其他 F-FB 的背景数据块的静态参数。

说明

请注意，使用 F-FC 时，对 F-FC 的输出参数的第一次访问必须是写访问。此操作将初始化输出参数。必须始终初始化 F-FC 的输出参数。

如果未遵守上述规定，F-CPU 会切换到 STOP。然后下面其中一条诊断事件进入 F-CPU 诊断缓冲区：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

说明

如果要和数据区（数据块）中的地址作为实参分配给 F-FC 的形参，必须使用具有完整资格的 DB 访问。

说明

F-FB/F-FC 中的变量名称最多可包含 22 个字符。

说明

请注意，对 F-FB/F-FC 中输入参数的访问为只读访问，而对输出参数的访问为只写访问。

如果要进行读写访问，请使用输入/输出参数。

6. 保存 F-FB/F-FC 块。

说明

在 *FBD/LAD* 编辑器中保存 F-FBD/F-LAD 块时，仅对 F 块执行本地一致性检查。尚未生成安全程序。

说明

有时，尝试保存 F 块时，已使用 F-FBD 编辑的某些程序段将用 STL 表示（例如，边沿存储器位和分支的上游互连）。无法保存此类 F 块。必须删除 STL 程序段并用自己的程序段替换上游互连，可在自己的程序段中直接将上游互连指定给临时变量。然后可将此临时变量用作地址。

说明

要使程序更清晰，请为已创建的 F-FB/F-FC 分配唯一的符号名。这些符号名将显示在 *SIMATIC* 管理器的“详细资料”(Details) 视图、“安全程序”(Safety Program) 对话框和符号表中。分配符号名的方式与进行标准编程时使用的分配方式相同。

参见

组态 F-CPU (页 28)

访问保护概述 (页 49)

F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语言之间的区别 (页 66)

编译安全程序 (页 260)

4.3.3 创建和编辑 F-DB**F-DB**

与 F-FB 或 F-FC 相似，也可以创建和编辑可在安全程序的一个 F 运行组内对其参数进行读/写访问的 F-DB（使用 F-DB 编程语言）。

4.3 使用 F-FBD/F-LAD 创建 F 块

进行编辑时，将检查数据类型。检测到的所有错误都将输出在 *FBD/LAD 编辑器* 中，与创建标准用户程序时的情况一样。

说明

不得使用为自动添加的 F 数据块（F-CPU 对象属性中的“F 数据块”参数；请参阅『组态 F-CPU』一章）保留的编号区中的 DB 编号。

说明

在 *FBD/LAD 编辑器* 中保存 F-DB 时，仅对 F 块执行本地一致性检查。尚未生成安全程序。

说明

要使程序更清晰，请为已创建的 F-DB 分配唯一的符号名。这些符号名将显示在 *SIMATIC 管理器* 的“详细资料”(Details) 视图、“安全程序”(Safety Program) 对话框和符号表中。分配符号名的方式与进行标准编程时使用的分配方式相同。

F-DB 中的变量名称最多可包含 22 个字符。

数据块的选项：“未链接”(Unlinked) 和“DB 在 PLC 中处于写保护状态”(DB is Write-Protected in the PLC)

说明

不得为 F-DB 和 F 块的背景数据块设置 DB 对象属性中的“未链接”(Unlinked) 可用选项。

不得为 F-DB 和 F 块的背景数据块设置 DB 对象属性中的“DB 在 PLC 中处于写保护状态”(DB is write-protected in the PLC) 可用选项。

如果选择了其中任一选项，则将在编译安全程序时校正此选项。

用于通过 S7 连接进行安全相关的 CPU 与 CPU 通讯的 F 通讯 DB

要通过 S7 连接进行安全相关的 CPU 与 CPU 通讯，必须在发送方和接收方分别创建一个 F 通讯 DB。在 *SIMATIC 管理器* 中创建和编辑 F 通讯 DB 的方式与创建和编辑其它 F-DB 的方式相同。

『对通过 S7 连接的安全相关的 CPU 与 CPU 通讯进行编程』一章中说明了 F 通讯 DB 的特殊要求。

F 运行组通讯的 DB

要在安全程序的 F 运行组之间进行安全相关的通讯，必须为每个要为其他 F 运行组提供数据的 F 运行组创建“F 运行组通讯的 DB”。

『定义 F 运行组』一章中说明了为 F 运行组通讯创建 DB 的操作步骤以及这些 DB 的特殊要求。

参见

创建和编辑 F-FB/F-FC (页 83)

4.3.4 用户创建的 F-FB、F-FC 和 F-DB 的知识保护

知识保护

具有知识保护的块是被保护的块，不能编辑。

可为用户创建的 F-FB、F-FC 和 F-DB（背景数据块除外）提供知识保护。

受保护的 F-FB/F-FC/F-DB 将不再能修改。

可以读取受保护的 F-FB/F-FC/F-DB 的块属性，但指令部分仍处于隐藏状态。

使用知识保护

如果要保护 F-FB/F-FC/F-DB 中包含的知识，或要防止对 F-FB、F-FC 和 F-DB（背景数据块除外）进行意外操作，请使用知识保护。

要求

创建要保护其知识产权的 F-FB、F-FC 或 F-DB。不在 *FBD/LAD* 编辑器中打开要保护的 F-FB/F-FC/F-DB。

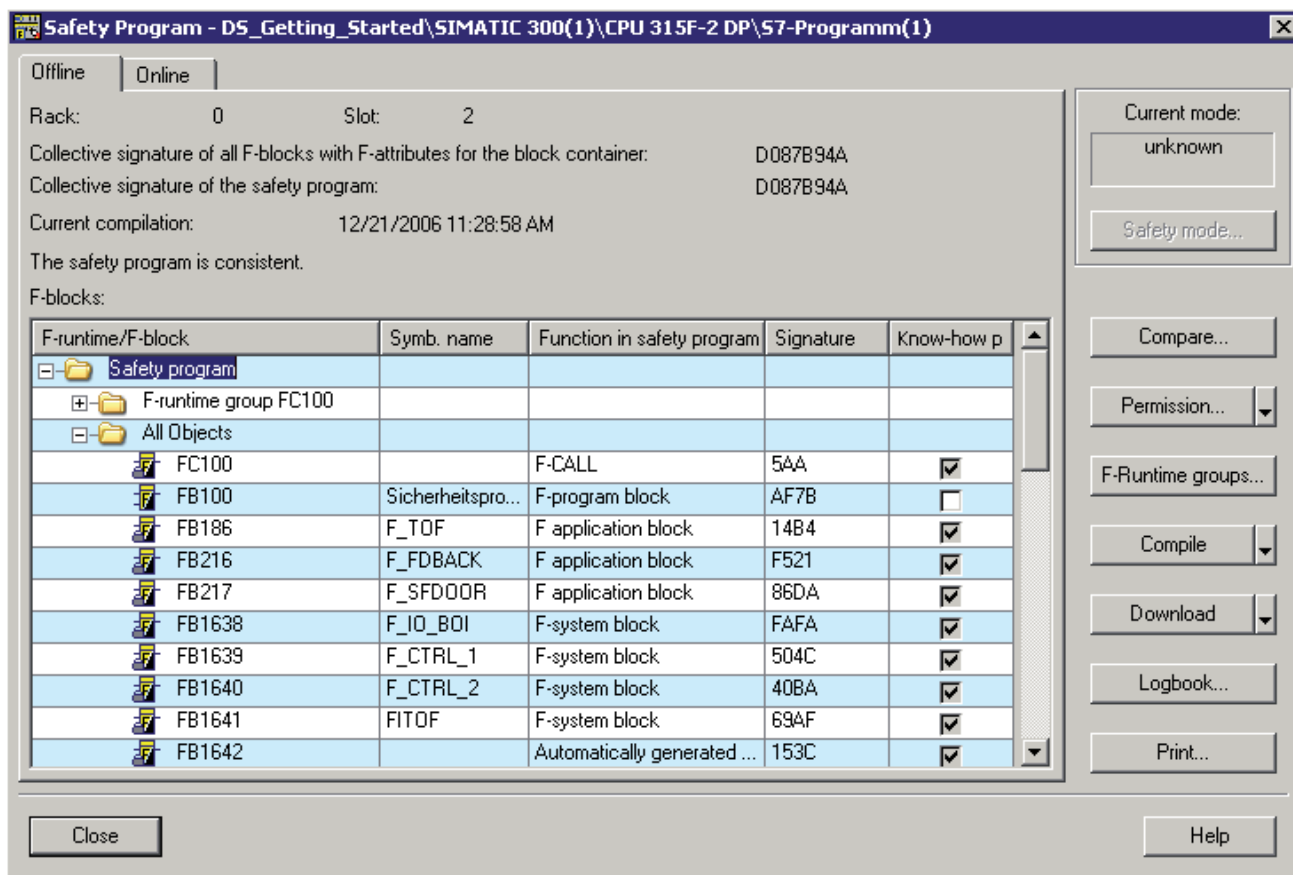
设置知识保护的步骤

请按照下述步骤进行操作：

1. 在 *SIMATIC* 管理器中打开“安全程序”(Safety Program) 对话框。

4.3 使用 F-FBD/F-LAD 创建 F 块

2. 在离线安全程序中为 F-FB/F-FC/F-DB 设置知识保护。要实现此目的，请选择“离线”(Offline) 选项卡。



3. 在“知识保护”(Know-how protection) 列中选中 F-FB、F-FC 和 F-DB 的相关复选框。

结果： 对于要保护的每个 F-FB/F-FC/F-DB，将自动打开一个用于创建备份副本的对话框。

4. 保存备份副本时请记住以下几点：

说明

为备份副本明确分配名称，以便以后可将 F-FB/F-FC/F-DB 与受保护的 F-FB/F-FC/F-DB 相关联（例如，相同名称、有关 F-FB/F-FC/F-DB 的注释）。

请勿将备份副本存储在包含受保护的 F-FB/F-FC/F-DB 的项目中（否则，不受保护的 F-FB/F-FC/F-DB 副本将可用）。

如果要将备份副本存储在 F 库中，请确保此 F 库是 *S7 Distributed Safety* 中的用户创建的 F 库。FBD/LAD 编辑器仅显示 *S7 Distributed Safety* 的 F 库。

5. 保存 F-FB/F-FC/F-DB 的备份副本。

结果：“安全程序”(Safety Program) 对话框中“知识保护”(Know-how protection) 列中的复选框将被选中且不能清除。

“块”(Block) 列中显示的块符号带有一个挂锁。F-FB、F-FC 或 F-DB 受保护。

6. 请执行相同的操作步骤，直到所有要保护的 F-FB/F-FC/F-DB 都受保护。

修改受保护的 F-FB/F-FC/F-DB

说明

不能取消 F-FB/F-FC/F-DB 的知识保护。

如果要修改受保护的 F-FB/F-FC/F-DB，请按照以下步骤进行操作：

1. 从项目中删除受保护的 F-FB/F-FC/F-DB。
2. 将 F-FB/F-FC/F-DB 的备份副本复制到项目中。
3. 在 *FBD/LAD 编辑器* 中编辑不受保护的 F-FB/F-FC/F-DB。
4. 如果需要，请为 F-FB/F-FC/F-DB 设置知识保护（请参阅上文）。

参见

自定义 F 库 (页 253)

4.3.5 用户创建的 F-FB、F-FC 和 F-DB 的“检查块的一致性”功能

“检查块的一致性”功能

如果已选择块文件夹，则可以在 *SIMATIC 管理器* 的“编辑”(Edit) 菜单中找到“检查块的一致性”功能。

“检查块的一致性”功能可修正若干时间戳冲突和块的不一致。可在安全程序中对没有知识保护的 F-FB、F-FC 和 F-DB 使用该功能。操作步骤与进行标准编程时相同。不支持“跳转到”功能。

可以选择 **程序 (Program) > 编译 (Compile)** 和 **程序 (Program) > 全部编译 (Compile All)** 菜单命令来使用“检查块的一致性”功能。

然后，将按照如下方式编译完整的安全程序：

4.3 使用 F-FBD/F-LAD 创建 F 块

- 如果选择程序 (Program) > 编译 (Compile)，则仅当安全程序已被更改时才对其重新编译。
- 如果选择程序 (Program) > 全部编译 (Compile All)，则无论安全程序是否已被修改均对其重新编译。

4.3.6 “编译和下载对象”功能

“编译和下载对象”功能

不能在 *SIMATIC 管理器* 中使用“编译和下载对象”功能来编译安全程序或将其下载到 F-CPU。

4.3.7 用户创建的 F-FB、F-FC 和 F-DB 的“存储写保护”功能

将 F 块存储为写保护的块

可以为 F 块使用“存储写保护”功能。如果为当前在 FBD/LAD 编辑器中打开的 F 块执行文件 (File) > 存储写保护 (Store write-protected) 菜单命令，则在任何块文件夹中均创建 F 块的写保护副本。

4.3.8 F-FB 和 F-FC 的“重新接线”功能

“重新接线”功能

可以在离线安全程序中使用 F-FB 和 F-FC 的 *STEP 7* “重新接线”功能。

成功重新接线后，将在安全程序的记录册中记录相应条目。

不会因为“重新接线”而执行保存 F 块时执行的自动一致性测试。尚未生成一致的安全程序。



警告

F 块的“重新接线”形成安全程序中的一项更改，因此会导致集体签名被更改。因此，安全程序必须再次进行接收测试。


4.4 定义 F 运行组

4.4.1 安全程序的 F 运行组的规则

要求

必须已创建安全程序。

规则

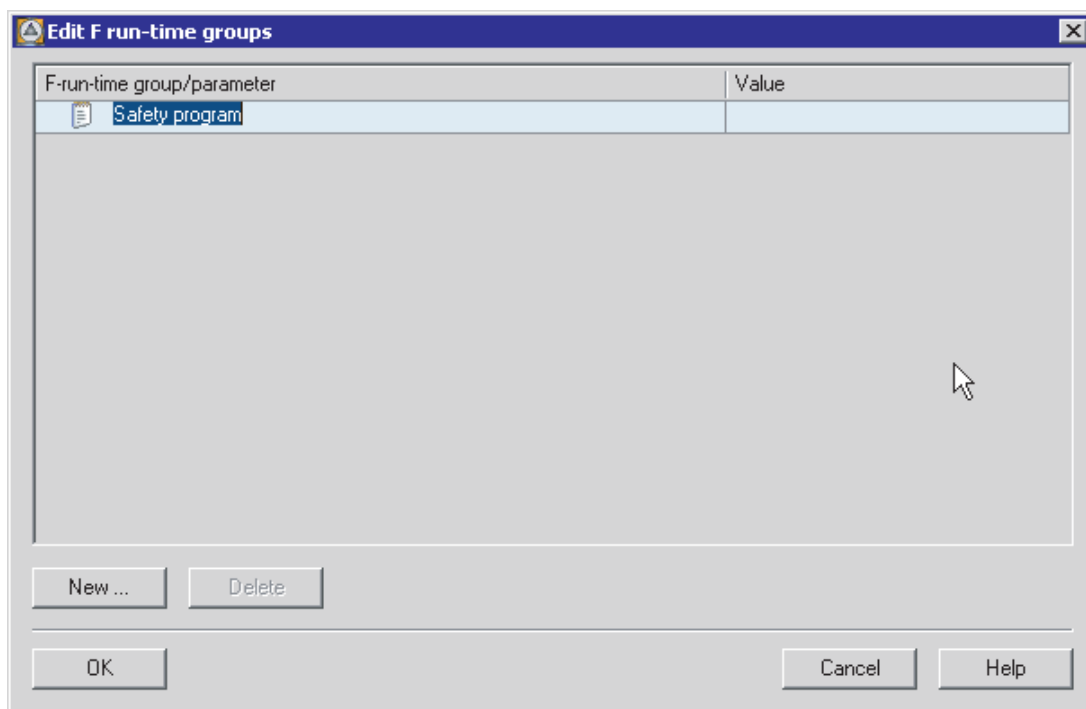
 警告
<p>请注意以下几点：</p> <ul style="list-style-type: none"> • 只能从一个 F 运行组访问 F-I/O 的通道。 • 只能从一个 F 运行组访问 F-I/O 的 F-I/O DB 的变量，而且只能是从其访问该 F-I/O 的通道 F 运行组（如果进行了访问）中进行访问。 • 一个 F 程序块不得在多个 F 运行组中使用。 • F-FB 可在多个 F 运行组中使用，但必须用不同的背景数据块调用。 • 只能从调用关联 F-FB 的 F 运行组访问背景数据块。 • F-DB（F 共享 DB 除外）的每个参数只能在一个 F 运行组中使用（但是，F-DB 可在多个 F 运行组中使用）。 • 通过已被提供 DB 的 F 运行组可对运行组通讯的 DB 进行读访问和写访问，但通过“接收方”F 运行组只能对其进行读访问。 • 只能从一个 F 运行组访问 F 通讯 DB。

- 不得在 OB 中直接调用 F 块；而必须将其插入到一个或两个 F 运行组中。
- 要最佳使用本地数据，必须在 OB 中（尽可能在周期性中断 OB 中）直接调用 F 调用块（F 运行组）；不应在这些周期性中断 OB 中声明任何其他本地数据。
- 在周期性中断 OB 内，F-CALL（F 运行组）应在标准用户程序之前执行；也就是说，F-CALL 应在 OB 的起始处，这样不管处理标准用户程序花费多长时间，始终能以固定的时间间隔调用 F 运行组。
- 每个 F-CALL 只能调用一次。不允许多次调用，因为多次调用将导致 F-CPU 切换到 STOP 模式。
- 可从多个 F 运行组访问标准 I/O 的过程输入和输出映像和存储器位。
- 通常可在多个 F 运行组中调用 F-FC。

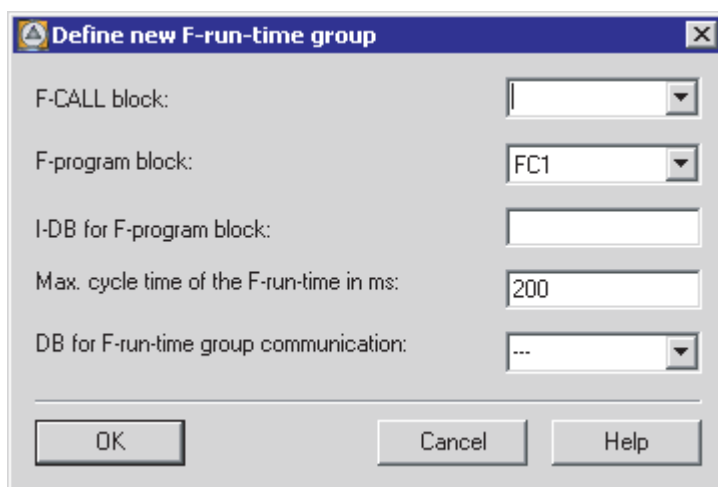
4.4.2 定义 F 运行组的操作步骤

操作步骤

1. 在 *SIMATIC* 管理器中，选择选项 (Options) > 编辑安全程序 (Edit Safety Program) 菜单命令。将显示“安全程序”(Safety Program) 对话框。激活“F-Runtime Groups...” (F 运行组...) 按钮以打开“Edit F-Runtime Groups” (编辑 F 运行组) 对话框。



2. 在“编辑 F 运行组”(Edit F-Runtime Groups) 对话框中，选择“新建...”(New...)。
将显示“定义新的 F 运行组”(Define New F-Runtime Group) 对话框。



3. 从下拉列表中，为新的 F 运行组选择要定义为 F-CALL 的 FC，或指定其他 FC。单击“确定”(OK) 退出“编辑 F 运行组”(Edit F-Runtime Groups) 对话框后，将立即自动创建此 FC。
4. 通过从下拉列表中为新的 F 运行组（可能为符号条目）选择要定义为 F-PB 的 F-FB 或 F-FC，来定义 F 运行组的 F-程序块。只能指定没有参数的 F-FB/F-FC。如果要分配的块为“FB”类型的 F 块，则必须为“F 程序块的 I-DB”(I-DB for F-program block)（可能为符号条目）指定背景数据块（例如，“DB10”）。单击“确定”(OK) 退出“编辑 F 运行组”(Edit F-Runtime Groups) 对话框后，将立即自动创建此 I-DB。I-DB 的编号不能介于 *HW Config* 中保留的范围内。如果指定现有的 I-DB，则该 I-DB 必须适合选定的 F 程序块。
5. F-CPU 将监视 F 运行组中的 F 周期时间。对于“F 运行组的最大周期时间 [以 ms 为单位]”(Max. Cycle Time of F-Runtime Group in ms)，请输入此 F 运行组两次调用之间允许的最大时间（最大为 120,000 ms）；请参阅《*SIMATIC S7 中的安全工程*》系统手册。

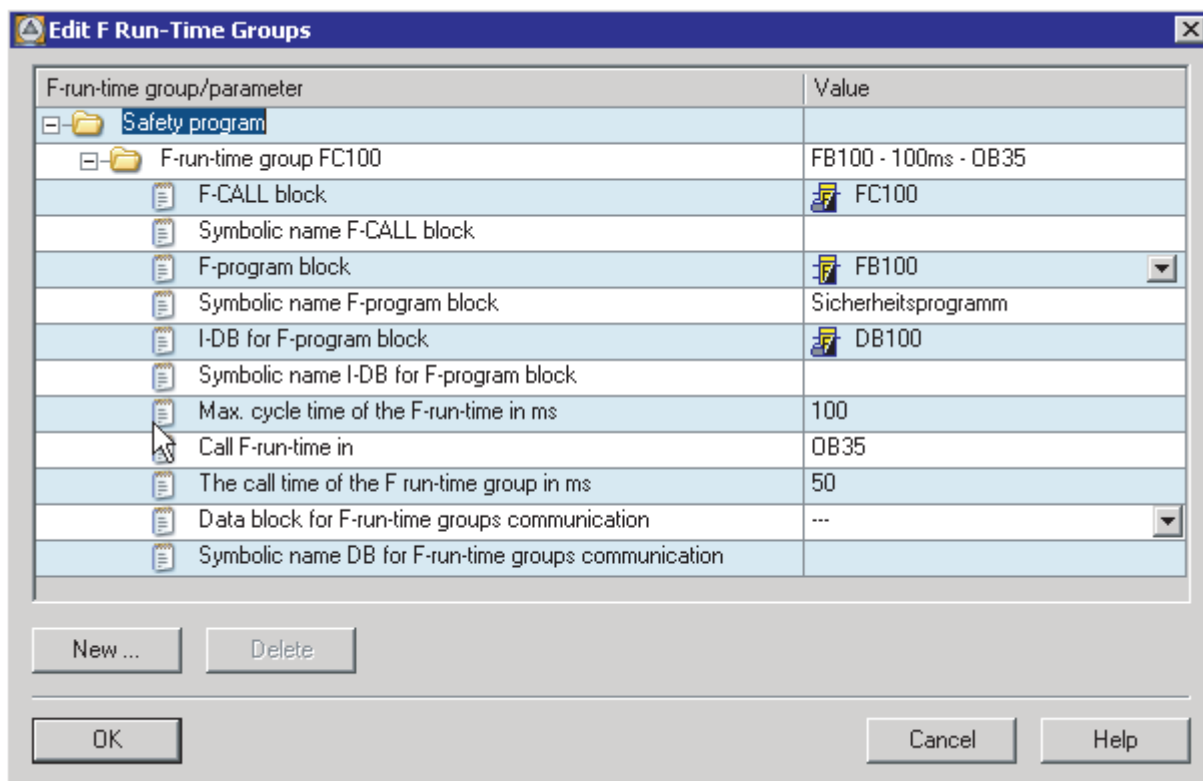
**警告**

F 运行组的调用间隔将根据最大值进行监视；也就是说，执行监视以确定调用的执行次数是否足够多，而不是确定执行次数是否太多。因此，必须使用 *Distributed Safety F* 库 (V1) 中的 F 应用程序块来实现故障安全定时器功能，而非计数器功能（OB 调用）。

4.4 定义 F 运行组

6. 如果该 F 运行组要向其他 F 运行组提供数据，请从下拉列表中为“F 运行组通讯的 DB”(DB for F-runtime group communication) 选择 F-DB，或者指定其他 F-DB（可能为符号条目）。单击“确定”(OK) 退出“编辑 F 运行组”(Edit F-Runtime Groups) 对话框后，将立即自动创建此 F-DB。

激活“确定”(OK) 按钮后，将对“编辑 F 运行组”(Edit F-Runtime Groups) 对话框中的条目进行内部有效性检查，然后再应用。



此对话框还显示：

- 新定义的 F 块的符号名
- 调用 F 运行组的标准用户程序的块
- F 运行组的调用时间

即调用 F-CALL 的周期性中断 OB 的执行时间。已在 *HW Config* 中组态此时间（F-CPU 的对象属性、“周期性中断”[Cyclic interrupts] 选项卡、相应 OB 的“执行时间”参数）。

7. 重复步骤 2 至步骤 6 以创建第二个 F 运行组。
8. 在“编辑 F 运行组”(Edit F-Runtime Groups) 对话框中激活“确定”(OK) 按钮后，将保存这些条目，并且在提示之后自动创建所有尚未创建的 F 块。

4.4.3 安全程序的 F 运行组之间的安全相关通讯

F 运行组之间的安全相关的通讯

可在安全程序的两个 F 运行组之间进行安全相关的通讯。即，F-DB 中一个 F 运行组提供的故障安全数据从另一个 F 运行组中读取。

可通过以下方法创建“F 运行组通讯的 DB” (DB for F-runtime group communication):

- 在“定义新的 F 运行组” (Define New F-Runtime Group) 对话框中
- 在“编辑 F 运行组” (Edit F-Runtime Groups) 对话框中
- 在 *SIMATIC 管理器* 中（请参阅下面的『在 *SIMATIC 管理器* 中为 F 运行组通讯创建 DB』）

说明

通过为其设置该 F-DB 的 F 运行组可对 F 运行组通讯的 DB 进行读访问和写访问，而通过“接收方” (receiver) F 运行组只能对其进行读访问。

提示： 按照使 F 运行组之间交换的数据尽可能少的方式构造安全程序，可提高性能。

在 SIMATIC 管理器中为 F 运行组通讯创建 DB

可在 *SIMATIC 管理器* 中采用与创建其他 F-DB 相同的方式为 F 运行组通讯创建 DB（请参阅『创建和编辑 F-DB』一章）。

在 *SIMATIC 管理器* 中为 F 运行组通讯创建 DB 时，请注意以下几点：

在 F-DB 对象属性的“常规 — 第 2 部分”(General - Part 2) 选项卡中的“系列”(Family) 框中分配“RTG_DB”标识符。此标识符将把 F-DB 标识为 F 运行组通讯的 DB。为 F 运行组通讯的 DB 分配符号名。

从其他 F 运行组读取数据时的最新数据

说明

从其他 F 运行组读取的数据是：在此 F 运行组开始读取数据之前最后一次处理提供数据的 F 运行组时的最新数据。

如果正在处理提供数据的 F 运行组时所提供的数据多次发生变化，则读取数据的 F 运行组始终接收最后一次更改的数据。

4.4 定义 F 运行组

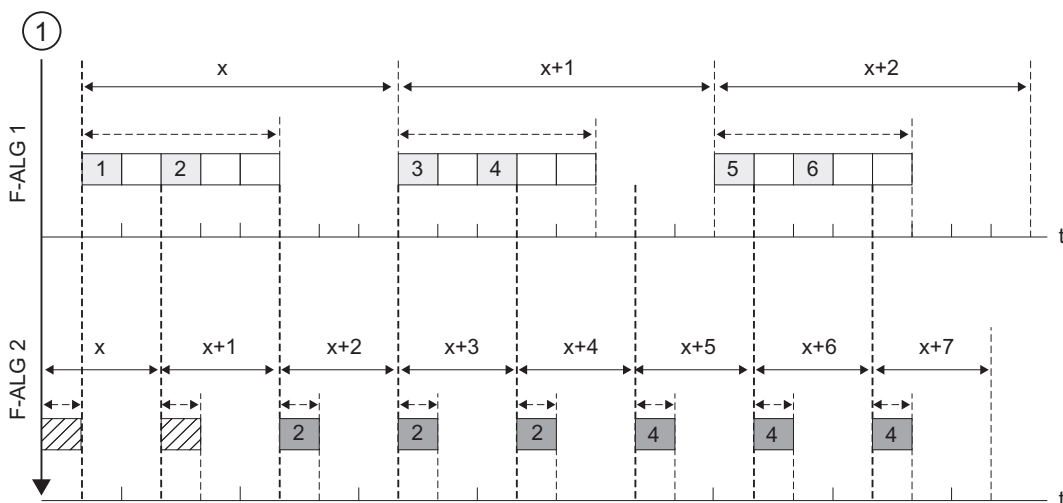
故障安全值的分配

启动 F 系统之后，可以将故障安全值用于对其他 F 运行组（例如，F 运行组 2）的 F 运行组通讯 DB 中的数据具有读访问权限的 F 运行组。在 F 运行组 1 的 F 运行组通讯 DB 中指定的值可用作故障安全值（F 运行组通讯 DB 的预设值）。

F 运行组 2 将在首次被调用时读取故障安全值。F 运行组 2 第二次被调用时，如果在它的两次调用期间已处理完 F 运行组 1，它将读取最新数据。如果未处理完 F 运行组 1，F 运行组 2 将继续读取故障安全值直至完全处理完 F 运行组 1。

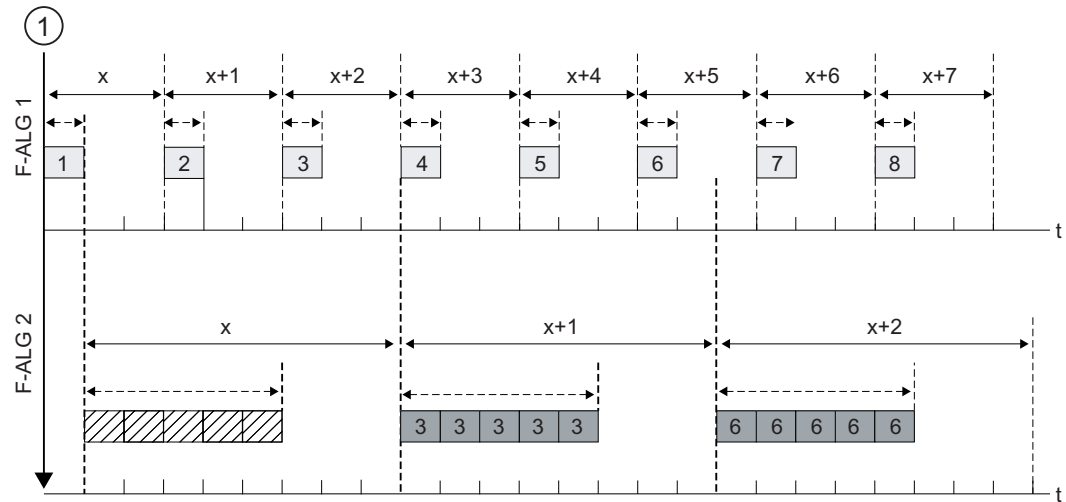
下面两幅图说明了此特性。

从与 F 运行组 2 相比，具有较长 OB 周期和较低优先级的 F 运行组 1 中读取数据



- (1) 启动 F 系统
- ←→ 调用 F 运行组的 OB 的周期时间
- ←- - - -> F 运行组的运行时间
- 1 ... F 运行组 1 的数据，写入到 F 运行组 1 的 F 运行组通讯 DB
- 2 F 运行组 2 的数据，从 F 运行组 1 的 F 运行组通讯 DB 中读取
- ▨ F 运行组通讯 DB 的预设值

从与 F 运行组 2 相比具有较短 OB 周期和较高优先级的 F 运行组 1 中读取数据



- (1) 启动 F 系统
- ← 调用 F 运行组的 OB 的周期时间
- ← 运行组的运行时间
- 1 ... F 运行组 1 的数据，写入到 F 运行组 1 的 F 运行组通讯 DB
- 2 ... F 运行组 2 的数据，从 F 运行组 1 的 F 运行组通讯 DB 中读取
- ▨ F 运行组通讯 DB 的预设值

未处理提供数据的 F 运行组

说明

如果未处理其 F 运行组通讯 DB 将提供要读取的数据的 F 运行组（未在 OB 或 FB 中调用 F 运行组的 F-CALL），则 F-CPU 将切换到 STOP 模式。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- 安全程序中的错误：周期时间超时
- 相关（未处理的 F 运行组的）F 调用块的编号
- 当前周期时间（以 ms 为单位）："0"

参见

创建和编辑 F-DB (页 85)

定义 F 运行组的操作步骤 (页 92)

4.4 定义 F 运行组

4.4.4 删除 F 运行组

删除 F 运行组

1. 在“编辑 F 运行组”(Edit F-Runtime Groups) 对话框中，选择要删除的 F 运行组文件夹。
2. 激活“删除”(Delete) 按钮。
3. 单击“确定”(OK) 关闭对话框。

分配给 F 运行组的 F 块即会删除。但 F 块仍然存在。

说明

如果要删除安全程序，请在 *SIMATIC 管理器* 中离线删除所有以黄色高亮显示的 F 块。

参见

定义 F 运行组的操作步骤 (页 92)

4.4.5 更改 F 运行组

更改 F 运行组

可在“编辑 F 运行组”(Edit F-RunTime Groups) 对话框中，对安全程序的每个 F 运行组进行以下更改：

- 将其它 FB/FC 定义为 F-Program 块（从下拉列表选择一个 FB/FC）
- 为 F-Program 块输入其它 I-DB 或新的 I-DB
- 更改 F 运行组的最大周期时间值
- 将其它 F-DB 定义为 F 运行组通讯的数据块（从下拉列表选择一个 F-DB 或输入一个新的 F-DB）

激活“确定”(OK) 按钮后，将保存这些更改，提示之后自动创建所有尚未创建的 F-Block。

参见

定义 F 运行组的操作步骤 (页 92)

4.5 编写启动保护程序

引言



当 F-CPU 从 STOP 模式切换到 RUN 模式时，标准用户程序将以正常方式启动。启动安全程序后，将使用装载存储器中的值初始化所有具有 **F-Attribute** 的数据块（与冷重新启动时的情况相同）。这意味着将丢失保存的错误信息。

F 系统将自动重新集成 F-I/O。

数据处理错误或内部错误也可以使用装载存储器中的值来触发安全程序的启动。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。启用输出是安全的且已修正故障后，才能启用这些输出。

重新启动/启动保护的实例

要应用重新启动/启动保护，必须可以检测启动。要检测启动，请在 F-DB 中声明一个数据类型为 **BOOL** 的变量，其初始值/实际值为“1”。

当此变量的值为“1”时阻止过程数据输出，例如，通过使用 F-I/O DB 中的 **PASS_ON** 变量钝化 F-I/O。

要手动启用过程数据输出，请通过用户确认复位该变量。

参见

F-I/O DB (页 104)

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

4.5 编写启动保护程序

F-I/O 访问

5.1 F-I/O 访问

概述

本节将介绍如何访问 F-I/O 及编写此访问程序时必须考虑的特殊特性。

通过过程映像进行访问

与标准 I/O 相同，可通过**过程映像**（PII 和 PIQ）访问 F-I/O（例如，S7-300 F-SM）。不允许直接访问 I/O。只能从一个 F 运行组访问 F-I/O 的通道。

处理 F 程序块之前，在 F 运行组的开始处更新过程输入映像。处理 F 程序块之后，在 F 运行组的结束处更新过程输出映像（请参阅『*S7 Distributed Safety* 中安全程序的结构』一章中的图）。

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



警告

由于此特殊安全协议，F-I/O 占用的过程映像区域比 F-I/O 上实际存在的通道需要的区域大。要找出存储通道（用户数据）的过程映像区域，请参考 F-I/O 的相关手册。在安全程序中访问过程映像时，仅允许访问实际存在的通道。

请注意，对于某些 F-I/O（例如，S7-300 F-SM 和 ET 200S 故障安全模块），可指定“传感器的 1oo2 评估”。要了解可在安全程序中访问哪些由“传感器的 1oo2 评估”组成的通道，请参考 F-I/O 的相关手册。

信号图表

以下部分中的“信号图表……”图中所示的信号图表代表所指特性的典型信号图表。

实际信号图表（特别是单个信号的状态变化的相对位置）可能偏离给定的信号图表，偏离范围是周期程序执行的已知畸变范围，这取决于以下因素：

- 正在使用的 F-I/O
（具有输入的 F-I/O、具有输出的 F-I/O、具有输入和输出的 F-I/O、S7-300 F-SM、ET200S F 模块、ET 200eco F 模块、ET 200pro F 模块或故障安全 DP 标准从站/标准 I/O 设备、F-I/O 和 F-CPU 的 PROFIsafe 总线规约的版本）

- 调用关联的 F 运行组的 OB 的周期时间
- PROFIBUS DP 的目标循环时间或 PROFINET IO 的更新时间

说明

信号图表表示用户安全程序中的信号状态。如果在同一 OB 内调用安全程序之前或之后，在标准用户程序中评估信号，则信号的状态变化可能会移位一个周期。

与信号图表中显示的相反，如果需要的话，过程数据和传送至故障安全输出的故障安全值之间的状态变化（“到输出”信号图表）可以在相关 QBAD 信号的状态变化之前发生。状态变化的时序取决于使用的是具有输出的 F I/O 还是具有输入和输出的 F I/O。

参见

S7 Distributed Safety 中安全程序的结构 (页 61)

对安全相关的智能从站与从站通讯进行 F-I/O 访问 (页 166)

5.2 过程数据或故障安全值

何时使用故障安全值？

在以下情况下，安全功能要求在整个 F-I/O 或 F-I/O 的单个通道发生钝化时使用故障安全值 (0) 代替过程数据。这既适用于数据类型为 BOOL 的（数字）通道，又适用于数据类型为 INT (WORD) 的（模拟）通道，情况如下：

- 当 F 系统启动时
- 当在 F-CPU 和 F-I/O 之间使用符合 PROFIsafe 的安全协议进行安全相关的通讯期间发生出错（通讯错误）时
- 发生 F-I/O 故障和通道故障（例如断线、短路和误差错误）时
- 只要在 F-I/O DB 中使用 PASS_ON = 1 启用 F-I/O 的钝化（请参阅下文）

F-I/O 和 F-I/O 的通道故障安全输出

如果是具有输入的 F-I/O，则发生钝化时，F 系统将向安全程序提供故障安全值 (0) 以代替 PII 中未决的过程数据。

F 系统将 SM 336; AI 6 x 13Bit 或 SM 336; F-AI 6 x 0/4 ... 20 mA HART 通道的上溢或下溢视为 F-I/O 故障或通道故障。将为安全程序提供故障安全值 0 以代替 PII 中的 7FFF_H（对于上溢）或 8000_H（对于下溢）。

如果是具有输入的 F-I/O，且要在安全程序中为数据类型为 INT (WORD) 的模拟通道处理“0”以外的其它故障安全值，则可指定 QBAD/QBAD_I_xx/QBAD_O_xx = 1 时的各个故障安全值。

**警告**

对于具有输入的 F-I/O，必须在安全程序中为数据类型为 BOOL 的（数字）通道进一步处理 PII 中提供的故障安全值“0”。

具有输出的 F-I/O 模块中发生钝化时，F 系统将故障安全值 (0)（而不是 PIQ 中由安全程序提供的输出值）传送给故障安全输出。F 系统将覆盖与故障安全值 (0) 关联的 PIQ。

重新集成 F-I/O 和 F-I/O 的通道

从故障安全值 (0) 到过程数据的切换（F-I/O 的重新集成）将自动进行或在 F-I/O DB 中用户确认后。重新集成的方法取决于以下因素：

- F-I/O 和 F-I/O 的通道的钝化原因
- 必须为 F-I/O DB 分配的参数（请参阅下文）

说明

请注意，如果 F-I/O 中发生通道故障，则故障通道可能发生通道级钝化。如果在 *HW Config* 中进行了相应组态，则将为受影响的通道输出故障安全值 (0)。如果已为 F-I/O 组态通道级钝化，则在修正故障后重新集成相关通道；所有故障通道仍保持钝化状态。

参见

对 F-I/O 进行组态 (页 37)

5.3 F-I/O DB

引言

在 *HW Config* 中进行编译时，将为每个 F-I/O 自动创建一个 F-I/O DB。此 F-I/O DB 包含可在安全程序中评估的变量，或者可以或必须说明的变量（只能在标准用户程序中评估的 DIAG 变量除外）。不能在 F-I/O DB 中直接更改变量的初始值或实际值，因为 F-I/O DB 受知识保护。

使用对 F-I/O DB 的访问

以下是访问 F-I/O DB 的变量的原因：

- 要在发生通讯错误、F-I/O 故障或通道故障后重新集成 F-I/O
- 要将 F-I/O 钝化为安全程序的特殊状态的功能（例如，组钝化）
- 要为故障安全 DP 标准从站/标准 I/O 设备重新分配参数
- 要评估是否应该输出故障安全值或过程数据

F-I/O DB 的变量

下表列出了 F-I/O DB 的变量：

	变量	数据类型	功能	缺省值
可以或必须说明的变量	PASS_ON	BOOL	1 = 启用钝化	0
	ACK_NEC	BOOL	1 = 发生 F-I/O 故障或通道故障时需要确认重新集成	1
	ACK_REI	BOOL	1 = 确认重新集成	0
	IPAR_EN	BOOL	用于故障安全 DP 标准从站/标准 I/O 设备重新分配参数的变量，或用于 SM 336; F-AI 6 x 0/4 ... 20 mA HART 启用 HART 通讯的变量	0
可以评估的变量：	PASS_OUT	BOOL	钝化输出*	1
	QBAD	BOOL	1 = 输出故障安全值*	1
	ACK_REQ	BOOL	1 = 重新集成的确认要求	0

	变量	数据类型	功能	缺省值
	IPAR_OK	BOOL	用于故障安全 DP 标准从站/标准 I/O 设备重新分配参数的变量，或用于 SM 336; F-AI 6 x 0/4 ... 20 mA HART 启用 HART 通讯的变量	0
	DIAG	BYTE	检修信息	
	QBAD_I_x x	BOOL	1 = 将故障安全值输出到输入通道 xx	1
	QBAD_O_ xx	BOOL	1 = 将故障安全值输出到输出通道 xx	1
*有关说明，请参阅“PASS_OUT/QBAD/QBAD_I_xx/QBAD_O_xx”中的信息				

PASS_ON

PASS_ON 变量使您可以启用 F-I/O 的钝化，例如，钝化为安全程序中特殊状态的功能。在 F-I/O DB 中使用 PASS_ON 变量，只能钝化整个 F-I/O，不能进行通道级钝化。只要 PASS_ON 等于 1，就将钝化关联的 F-I/O。

ACK_NEC

如果 F-I/O 检测到 F-I/O 故障，则将钝化相关的 F-I/O。如果检测到通道故障，且已组态通道级钝化，则将钝化相关通道。如果已组态整个 F-I/O 的钝化，则将钝化相关 F-I/O 的所有通道。一旦消除 F-I/O 故障或通道故障，将根据 ACK_NEC 重新集成相关 F-I/O：

- ACK_NEC = 0 时，可以编写自动重新集成程序。
- ACK_NEC = 1 时，可以通过用户确认编写重新集成程序。



警告

从安全角度出发,只有在相关过程允许自动重新集成时才能为 ACK_NEC 分配 0。

说明

缺省情况下，创建 F-I/O DB 后 ACK_NEC = 1。如果不需要自动重新集成，则不需要说明 ACK_NEC。

ACK_REI

当 F 系统检测到通讯错误或 F-I/O 的 F-I/O 故障时，将钝化相关 F-I/O。如果组态了通道级钝化，当检测到通道故障时将钝化相关通道。如果组态了钝化整个 F-I/O，将钝化相应 F-I/O 的所有通道。消除故障后，要**重新集成 F-I/O/F-I/O** 的通道，要求在以下情况下使用 F-I/O DB 的变量 ACK_REI 的上升沿执行**用户确认**：

- 每个通讯错误后
- ACK_NEC = 1 的情况下发生 F-I/O 故障或通道故障后

通道故障后的重新集成将重新集成所有已清除故障的通道。

仅在 ACK_REQ = 1 时才可能确认。

在安全程序中，必须通过 ACK_REI 为每个 F-I/O 提供用户确认。

**警告**

对于用户确认，必须将 F-I/O DB 的 ACK_REI 变量与通过操作员输入生成的信号互连。不允许与自动生成的信号进行互连。

说明

此外，在通讯错误或 F-I/O/通道故障后，可使用 FB 219 “F_ACK_GL” F 应用程序块来执行 F-I/O 的重新集成（请参阅『FB 219“F_ACK_GL”：F 运行组的所有 F-I/O 的全球确认』一章）。

IPAR_EN

IPAR_EN 变量对应于 PROFIsafe 总线规约（PROFIsafe 规范 V1.20 及更高版本）中的 iPar_EN_C 变量。

故障安全 DP 标准从站/标准 I/O 设备

要了解重新分配故障安全 DP 标准从站的参数过程中何时设置或重设此变量，请参阅 PROFIsafe 规范 V1.20 或更高版本或者故障安全 DP 标准从站/标准 I/O 设备的文档。

**警告**

请注意，IPAR_EN = 1 时，**不会**触发相关 F-I/O 的钝化。

如果在 IPAR_EN = 1 时应继续钝化，还必须将变量 PASS_ON 设置为 1。

与 SM 336; F-AI 6 x 0/4 ... 20 mA HART 的 HART 通讯

如果在参数“HART_GATE”=“switchable”时将变量 IPAR_EN 设置为“1”，则将为 SM 336; F-AI 6 x 0/4 ... 20 mA HART 启用 HART 通讯。将该变量设置为“0”将禁用 HART 通讯。F-SM 通过变量 IPAR_OK = 1 还是 0 来确认启用了 HART 通讯还是禁用了 HART 通讯。

直到系统的状态允许对关联的 HART 现场设备的参数进行安全地重新分配，才可启用 HART 通讯。

如果要在安全程序中评估“启用 HART 通讯”状态（例如，为了编写互锁程序），那么必须生成以下实例中所示的信息。即使在通过 IPAR_EN = 1 启用 HART 通讯时发生通讯错误，也要确保该信息正确可用。如果通讯错误或 F-I/O/通道故障 (PASS_OUT = 0) 未导致钝化，那么评估状态时仅更改 IPAR_EN 变量。

启用 HART 通讯的实例

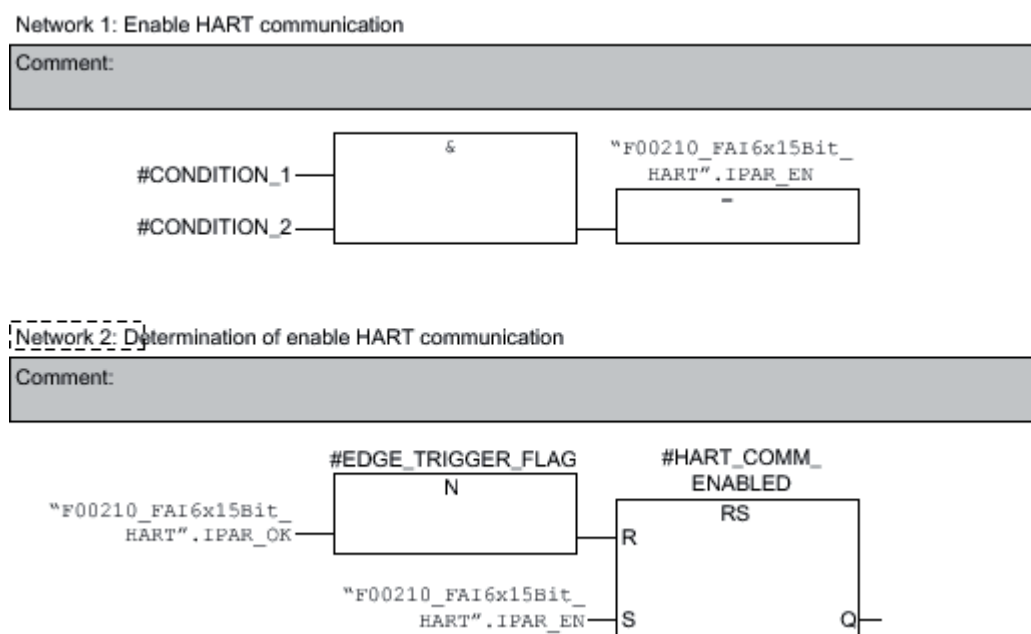


图 5-1 启用 HART 通讯的实例

您可以在《S7-300, 故障安全信号模块》手册中以及 *HW Konfig* 在线帮助中，该 F-SM 的对象属性中找到有关与 SM 336; F-AI 6 x 0/4 ... 20 mA HART 的 HART 通讯的其它信息。

PASS_OUT/QBAD/QBAD_I_xx/QBAD_O_xx

如果已为 F-I/O 组态通道级钝化，则 PASS_OUT = 1 和 QBAD = 1 表示至少已钝化一个通道。QBAD_I_xx 和 QBAD_O_xx 表示被钝化的输入和输出通道。

如果已组态整个 F-I/O 的钝化，则变量 PASS_OUT = 1 和 QBAD = 1 表示已钝化整个 F-I/O。

使用故障安全值 0 代替关联的 F-I/O 或 F-I/O 的单个通道的过程数据后，F 系统将把 PASS_OUT、QBAD、QBAD_I_xx 和 QBAD_O_xx 设置为 1。

但是，如果您通过将 PASS_ON 设置为 1 来启用钝化，则仅将 QBAD、QBAD_I_xx 和 QBAD_O_xx 设置为 1。如果使用 PASS_ON = 1 启用钝化，PASS_OUT 将不更改数值。因此，PASS_OUT 可以用于其它 F-I/O 的组钝化。

ACK_REQ

当 F 系统检测到通讯错误或 F-I/O 的 F-I/O 故障或通道故障时，将钝化相关 F-I/O 或 F-I/O 的单个通道。ACK_REQ = 1 表示重新集成相关 F-I/O 或 F-I/O 的通道需要用户确认。

一旦消除故障后，F 系统将立即把 ACK_REQ 设置为 1，从而可以执行用户确认。对于通道级钝化，一旦修正通道故障，F 系统会立即将 ACK_REQ 设置为 1。可对此故障执行用户确认。确认完成后，F 系统将把 ACK_REQ 复位为 0。

说明

对于具有输出的 F-I/O，由于需要测试信号输入，因此发生 F-I/O 故障或通道故障后，只能在消除故障几分钟之后才可以执行确认（请参阅 *F-I/O 手册*）。

IPAR_OK

IPAR_OK 变量与 PROFIsafe 总线规约（PROFIsafe 规范 V1.20 或更高版本）中的 iPar_OK_S 变量相对应。

故障安全 DP 标准从站/标准 I/O 设备

要了解在重新分配故障安全 DP 标准从站或标准 I/O 设备的参数时如何评估此变量，请参阅 PROFIsafe 规范 V1.20 或更高版本或者故障安全 DP 标准从站/标准 I/O 设备的文档。

与 SM 336; F-AI 6 x 0/4 ... 20 mA HART 的 HART 通讯

请参阅『IPAR_EN』一节

DIAG

DIAG 变量可提供有关已发生的错误或故障的非故障安全信息（1 字节），用于检修目的。可以通过操作员监视和控制系统读取该信息，也可以在标准用户程序中评估该信息（如果适用）。直到您在 ACK_REI 上执行确认或自动重新集成后，才保存 DIAG 位。

说明

禁止在安全程序中访问此变量。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	F-I/O 检测到超时	F-CPU 和 F-I/O 之间的 PROFIBUS/PROFINET 连接发生故障。 <i>HW Config</i> 中 F-I/O 的监视时间设置得太低。 F-I/O 正在接收的参数分配数据无效。 或	<ul style="list-style-type: none"> 检查 PROFIBUS/PROFINET 连接，确保无外部干扰源。 检查 <i>HW Config</i> 中 F-I/O 的参数分配。如果需要，请为监视时间设置一个较高的值。重新编译硬件配置，然后将其下载到 F-CPU。重新编译安全程序。 检查 F-I/O 的诊断缓冲区。 关闭 F-I/O 的电源然后再打开。
		内部 F-I/O 故障 或	更换 F-I/O
		内部 F-CPU 故障	更换 F-CPU
位 1	F-I/O 检测到的 F-I/O 故障或通道故障	请参阅 <i>F-I/O 手册</i>	请参阅 <i>F-I/O 手册</i>
位 2	F-I/O 检测到 CRC 错误或顺序号错误	请参阅位 0 的说明	请参阅位 0 的说明
位 3	保留	-	-
位 4	F 系统检测到超时	请参阅位 0 的说明	请参阅位 0 的说明
位 5	F 系统检测到顺序号错误	请参阅位 0 的说明	请参阅位 0 的说明
位 6	F 系统检测到 CRC 错误	请参阅位 0 的说明	请参阅位 0 的说明
位 7	保留	-	-

参见

对 F-I/O 进行组态 (页 37)

发生 F-I/O 故障和通道故障后钝化和重新集成 F-I/O (页 115)

组钝化 (页 119)

5.4 访问 F-I/O DB 变量

F-I/O DB 的符号名

在 *HW Config* 中进行编译期间，将自动为每个 F-I/O 创建一个 F-I/O DB，并在符号表中为该 F-I/O DB 输入符号名。

符号名由固定前缀“F”、F-I/O 的起始地址和在 *HW Config* 的 F-I/O 对象属性中输入的名称（最多 17 个字符）组合而成（例如：F00005_4_8_F_DI_DC24V）。

对于通过智能从站与从站通讯访问的 F-I/O，在 F-I/O 的起始地址后添加一个 X（例如 F00005_X_4_8_F_DI_DC24V）。

访问 F-I/O DB 的变量的规则

只能从一个 F 运行组访问 F-I/O 的 F-I/O DB 的变量，而且只能是从其访问该 F-I/O 的通道 F 运行组（如果进行了访问）中进行访问。

具有完整资格的 DB 访问

可使用“具有完整资格的 DB 访问”访问 F-I/O DB 的变量（即，通过指定 F-I/O DB 的符号名和变量的名称）。

请确保未选中 *FBD/LAD 编辑器*“常规” (General) 对话框（通过 **选项 [Options] > 设置 [Settings]** 打开）中的“将交叉引用报告为错误” (Report Cross References as Error)。否则，将不能访问 F-I/O DB 的变量。

评估 QBAD 变量的实例

Network 4: Fully qualified access to the variable QBAD

Comment:

"F00005_4_8_F_DI_DC24V".
QBAD



参见

分配符号名 (页 47)

5.5 启动 F 系统后钝化和重新集成 F-I/O

启动后的行为

启动 F 系统后，必须按照 PROFIsafe 安全协议在 F-CPU 和 F-I/O 之间建立通讯。在此期间，将钝化整个 F-I/O。

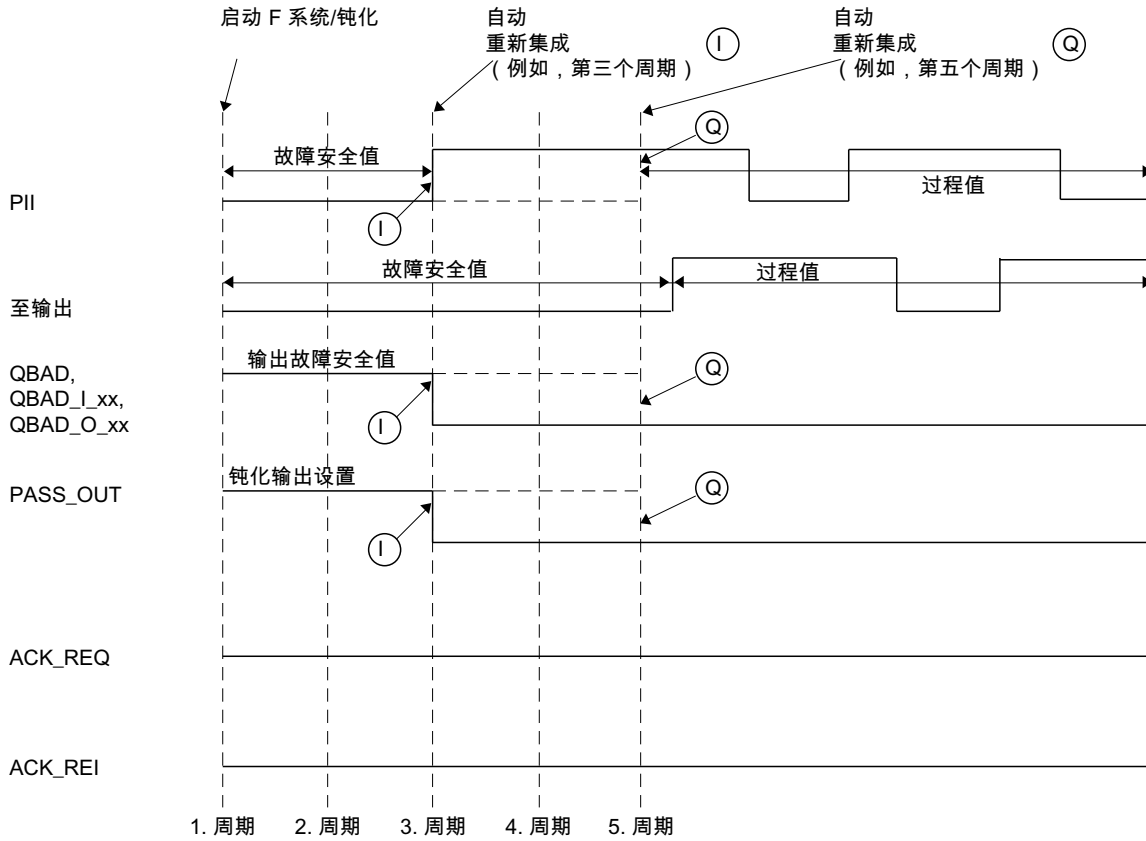
当使用故障安全值 (0) 时，变量 QBAD、PASS_OUT、QBAD_I_xx 和 QBAD_O_xx = 1。

重新集成 F-I/O

启动 F 系统之后，在 F-Run-Time 组的第二个周期开始时，将自动重新集成 F-I/O，即自动在 PII 中提供过程数据或自动将 PIQ 中提供的过程数据传送给故障安全输出；此事件的发生与变量 ACK_NEC 的设置无关。根据使用的 F-I/O 以及 F-Run-Time 组的周期时间和 PROFIBUS DP/PROFINET IO，重新集成可在 F-Run-Time 组的若干周期之后进行。

如果在 F-CPU 和 F-I/O 之间建立通讯的时间比在 *HW Config* 中的 F-I/O 对象属性中设置的监视时间长，将不执行自动重新集成。

在启动 F 系统后钝化和重新集成 F-I/O 的信号图表



- ⓘ 用于具有输入的 F-I/O
- Ⓚ 用于具有输出的 F-I/O 以及具有输入和输出的 F-I/O

警告
 如果不希望在启动 F 系统后自动重新集成，则必须编写启动保护程序。

参见

- 编写启动保护程序 (页 99)
- 发生通讯错误后钝化和重新集成 F-I/O (页 113)

5.6 发生通讯错误后钝化和重新集成 F-I/O

发生通讯错误后的行为

如果在 F-CPU 和 F-I/O 之间按照 PROFIsafe 安全协议进行安全相关的通讯时，F 系统检测到错误（通讯错误），将**钝化**相关 F-I/O。

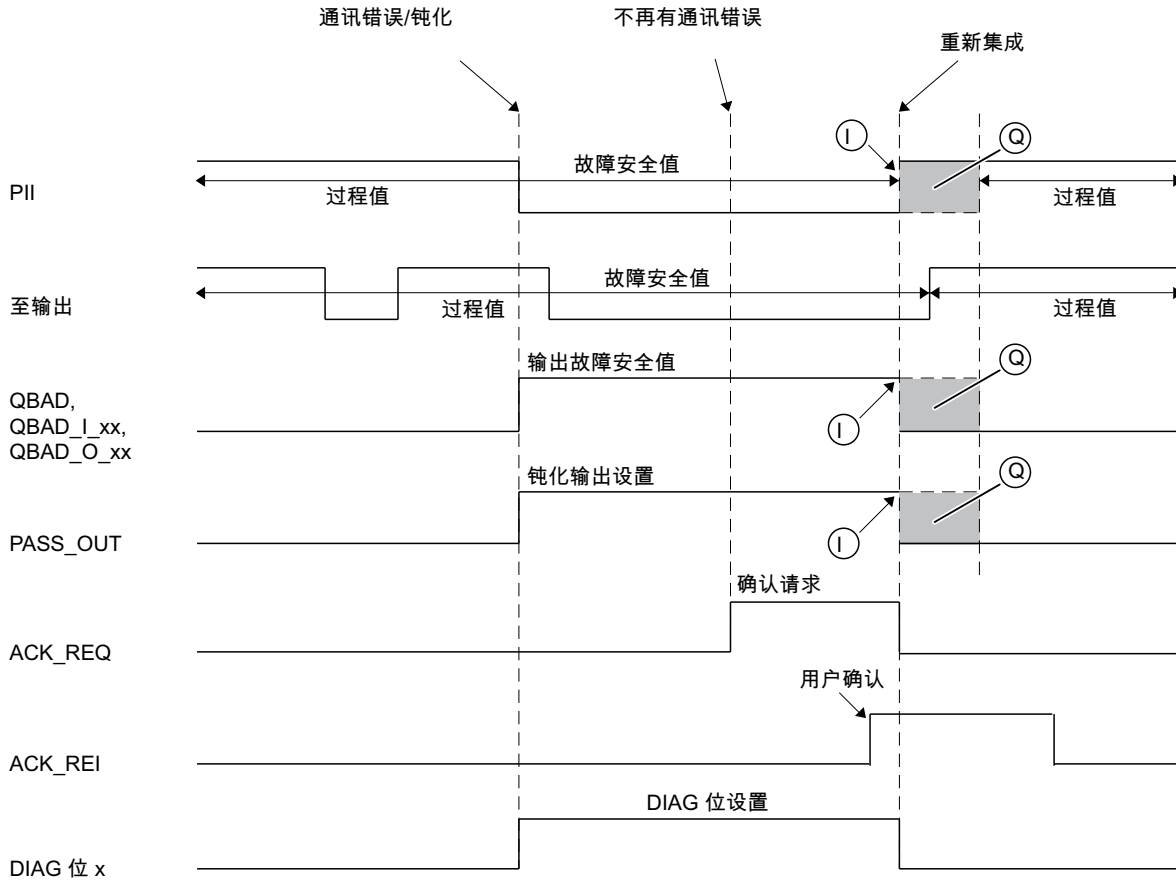
使用故障安全值 (0) 时，变量 QBAD、PASS_OUT、QBAD_I_xx 和 QBAD_O_xx 将被设置为“1”。

重新集成 F-I/O

仅在以下情况下**重新集成**相关 F-I/O，即在 PII 中提供过程数据或将 PIQ 中提供的过程数据传送到故障安全输出：

- 已消除所有通讯错误且 F 系统已将 ACK_REQ 设置为 1
- 已出现了一个具有上升沿的**用户确认**：
 - 在 F-I/O DB 的 ACK_REI 变量上或
 - 在 FB 219 “F_ACK_GL” F 应用程序块的 ACK_REI_GLOB 输入上（请参阅 9.1.2.18 一章）

用于在发生通讯错误后钝化和重新集成 F-I/O 的信号图表



- Ⓘ 用于具有输入的 F-I/O
- Ⓚ 用于具有输出的 F-I/O 以及具有输入和输出的 F-I/O (信号模式取决于所使用的 F-I/O)

参见

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

5.7 发生 F-I/O 故障和通道故障后钝化和重新集成 F-I/O

发生 F-I/O 故障后的特性

如果 F 系统检测到 F-I/O 故障（例如，编程错误、过热），将钝化相应的 F-I/O。

使用故障安全值 (0) 时，变量 QBAD、PASS_OUT、QBAD_I_xx 和 QBAD_O_xx 将被设置为“1”。

发生通道故障后的行为

如果 F 系统检测到通道故障（例如，短路、过载、误差错误或断线），F 系统将根据在 HW Config 中组态的 F-I/O 的“发生通道故障后的行为”(Behavior after Channel Faults) 参数进行响应。

如果已组态通道特定钝化，则将钝化 F-I/O 的相关通道。当使用故障安全值 (0) 时，相关通道的变量 QBAD、PASS_OUT 或 QBAD_I_xx 和 QBAD_O_xx = 1。

如果已组态整个 F-I/O 的钝化，则钝化与发生 F-I/O 错误后的钝化相同（请参阅上文）。

重新集成 F-I/O


仅在以下情况下**重新集成**相关 F-I/O 或 F-I/O 的相关通道，即在 PII 中提供过程数据或将 PIQ 中提供的过程数据传送到故障安全输出：

- 已消除所有 F-I/O 故障或通道故障。

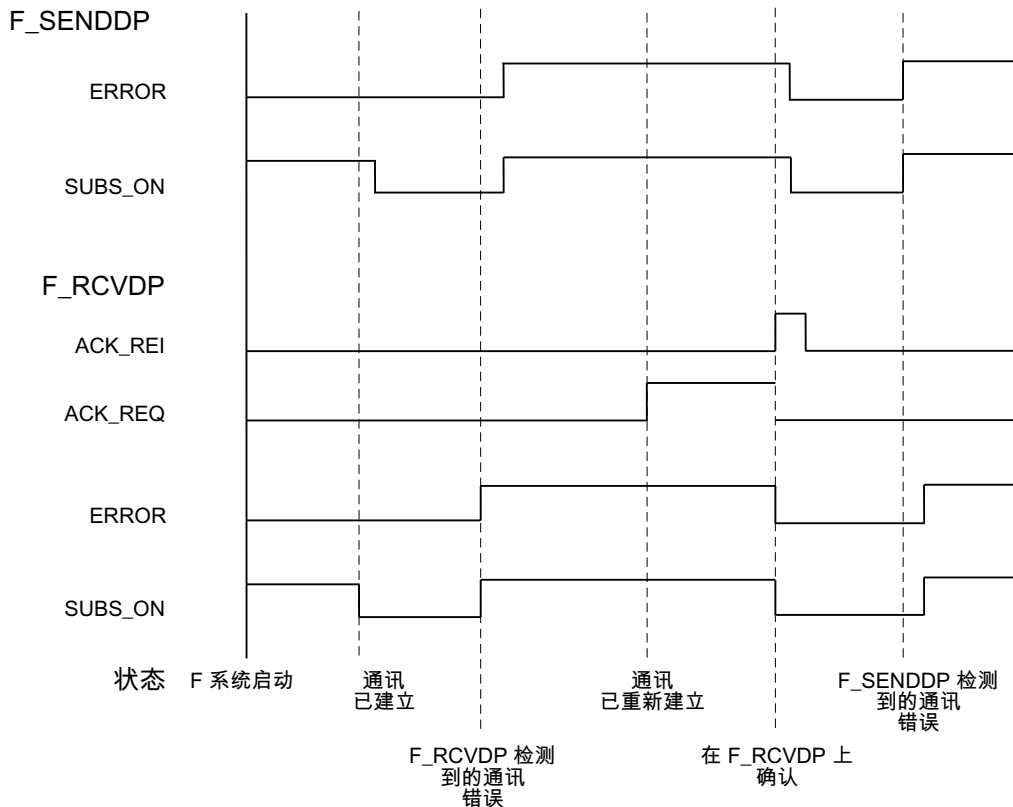
如果已为 F-I/O 组态通道特定钝化，则在修正故障后重新集成相关通道；所有故障通道仍保持钝化状态。

根据 ACK_NEC 的设置，重新集成将按以下方式进行：

- 如果 ACK_NEC = 0，则一旦 F 系统检测到已消除故障，将立即**自动重新集成**。对于具有输入的 F-I/O，将立即重新集成。对于具有输出的 F-I/O 或具有输入和输出的 F-I/O，则根据正在使用的 F-I/O，重新集成可在完成必需的测试信号输入（F-I/O 使用这些测试信号输入确定是否已消除故障）的几分钟之后进行。
- ACK_NEC = 1 时，仅具有上升沿（在 F-I/O DB 的 ACK_REI 变量上或在 FB 219 “F_ACK_GL” F 应用程序块的 ACK_REI_GLOB 输入上）的用户确认才会导致发生重新集成。F 系统检测到已消除故障且已将 ACK_REQ 设置为 1 后，可立即执行确认。

 警告
<p>F-I/O 发生电源故障的时间比在 <i>HW Config</i> 中为 F-I/O 指定的监视时间短时，（请参阅《<i>SIMATIC S7 中的安全工程</i>》系统手册），则无论 ACK_NEC 的设置为何，均会自动重新集成。这与上述当 ACK = 0 时的情况相同。</p> <p>如果在这种情况下，相关过程不允许重新集成，则必须通过评估变量 QBAD 或 QBAD_I_xx 和 QBAD_O_xx 或 PASS_OUT 来编写启动保护程序。</p> <p>如果 F-I/O 发生电源故障的时间比在 HW Config 中为 F-I/O 指定的监视时间长，则 F 系统将检测到通讯错误。</p>

当 ACK_NEC = 0 时，发生 F-I/O 故障和通道故障后钝化和重新集成 F-I/O 的信号序列（用于发生通道故障后钝化整个 F-I/O）

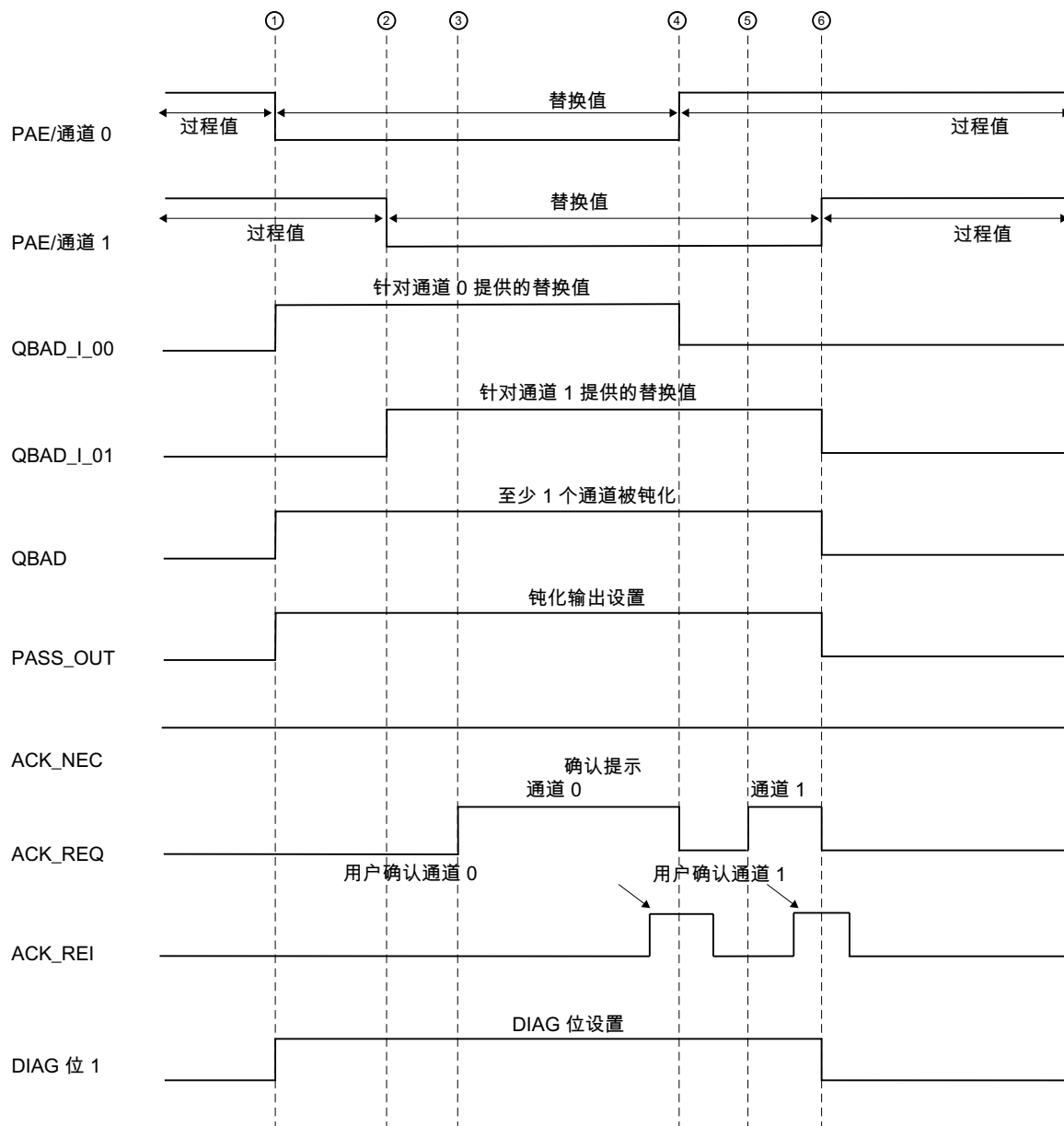


当 ACK_NEC = 1 时，发生 F-I/O 故障和通道故障后钝化和重新集成 F-I/O 的信号序列（用于发生通道故障后钝化整个 F-I/O）

有关 ACK_NEC = 1（缺省值）时，发生 F-I/O 故障或通道故障后钝化和重新集成 F-I/O 的信号序列，请参阅『在发生通讯错误后钝化和重新集成 F-I/O』一章。

当 $ACK_NEC = 1$ 时（用于通道特定钝化），发生通道故障后钝化和重新集成 F-I/O 的信号图表

具有输入的 F 外围设备实例：



- ① 通道 0 的通道故障/钝化通道 0
- ② 通道 1 的通道故障/钝化通道 1
- ③ 已修正通道 0 的通道故障

- ④ 重新集成通道 0
- ⑤ 已修正通道 1 的通道故障
- ⑥ 重新集成通道 1

参见

对 F-I/O 进行组态 (页 37)

编写启动保护程序 (页 99)

发生通讯错误后钝化和重新集成 F-I/O (页 113)

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

5.8 组钝化

编写组钝化程序

如果要在 F 系统钝化 F-I/O 或 F-I/O 的通道时启用其它 F-I/O 的钝化，可使用 PASS_OUT/PASS_ON 变量执行相关 F-I/O 的组钝化。

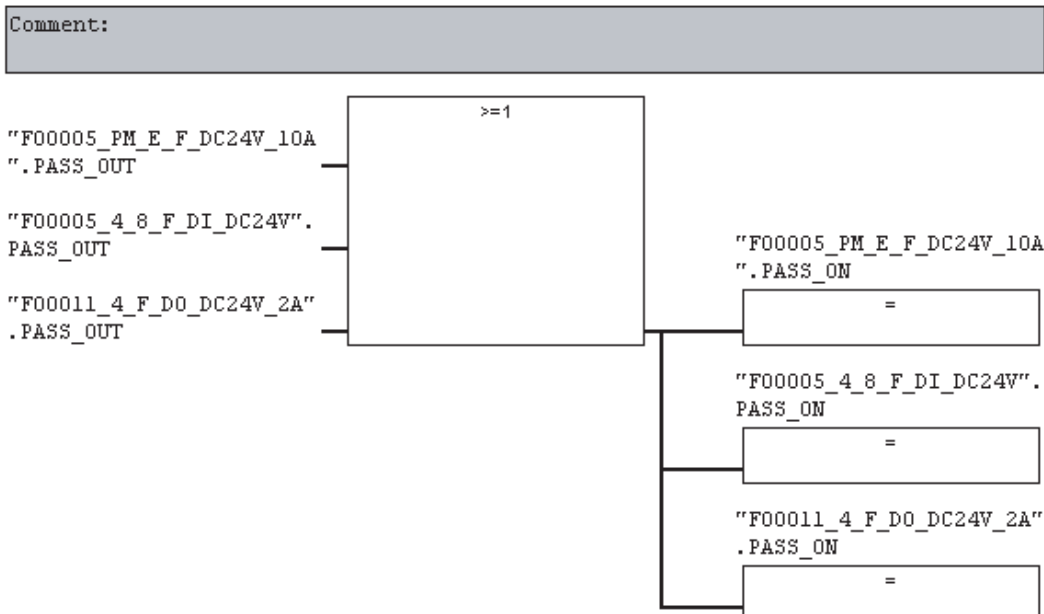
例如，启动 F 系统后，可使用通过 PASS_OUT/PASS_ON 的组钝化强制同时重新集成所有 F-I/O。

要进行组钝化，必须对组中 F-I/O 的所有 PASS_OUT 变量进行 OR 运算，并将结果分配给组中 F-I/O 的所有 PASS_ON 变量。

由于组钝化使用 PASS_ON = 1 而应用故障安全值 (0) 时，组中 F-I/O 的 QBAD、QBAD_I_xx 和 QBAD_O_xx 变量将都设置为 1。

组钝化实例

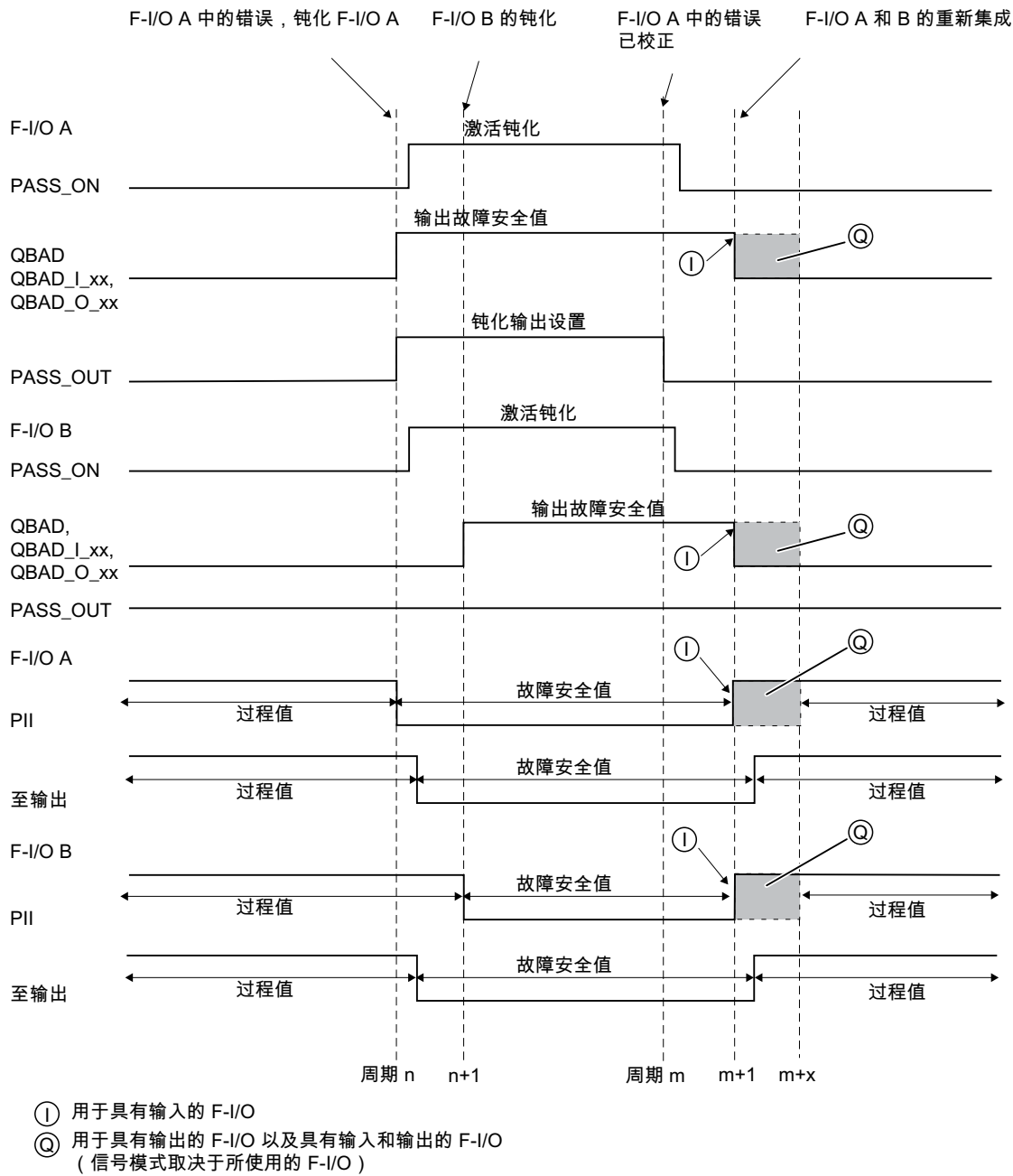
Network 5 : Group passivation



重新集成 F-I/O

如果重新集成了已触发组钝化的 F-I/O（无论是自动重新集成还是通过用户确认重新集成）（PASS_OUT = 0），则自动重新集成被组钝化钝化的 F-I/O。

组钝化的信号图表



执行用户确认

6.1 在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认

用户确认的选项

可通过以下方法之一执行用户确认：

- 通过连接至具有输入的 F-I/O 的确认键
- 通过操作员监视和控制系统

通过确认键执行用户确认

说明

如果使用“通过确认键执行用户确认”选项，且确认键所连接的 F-I/O 上发生通讯错误、F-I/O 故障或通道故障，则将无法确认该 F-I/O 的重新集成。

该“阻塞”只能通过将 F-CPU 从 STOP 切换到 RUN 才能排除。

因此，对于连接了确认键的 F-I/O 的重新集成的确认，建议您还要提供通过操作员监视和控制系统执行的确认。

通过操作员监视和控制系统执行用户确认

通过操作员监视和控制系统执行用户确认需要分布式安全 F 库 (V1) 中的 F_ACK_OP F 应用程序块。

编写通过操作员监视和控制系统执行用户确认程序的步骤

1. 在安全程序中调用“F_ACK_OP” F 应用程序块。用于评估用户确认的确认信号将在 F_ACK_OP 的输出 OUT 处提供。

6.1 在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认

2. 在操作员监视和控制系统上设置一个区域，可使用该区域在 F_ACK_OP 的背景数据块（输入 IN）中手动输入“确认值”“6”（确认的第一步）和“确认值”“9”（确认的第二步）。

或

在 F_ACK_OP 的背景数据块（输入 IN）中，分配功能键 1 以传送“确认值”“6”（确认的第一步），并分配功能键 2 以传送“确认值”“9”（确认的第二步）。

3. 可选：在操作员监视和控制系统上，评估 F_ACK_OP 背景数据块中的输入 Q，以指示必须在其中发生第二步确认的时间帧，或指示第一步确认已发生。

如果只能使用“监视/修改变量” (Monitor/Modify Variabl) 功能通过一个编程设备或 PC 执行用户确认，并且不希望取消激活安全模式，则必须在调用 F_ACK_OP F-Block 时在输入 IN 处传输一个地址（存储器字）。然后可通过修改此存储器字在编程设备或 PC 上传送“确认值”“6”和“9”。不得通过程序说明该存储器字。

说明

如果将输入 IN 与存储器字互联，则该存储器字只能是一个 F 运行组中 F_ACK_OP 上的输入。

 **警告**

不能通过一个操作触发两个确认步骤（例如，通过将两个确认步骤与时间条件自动同时存储在一个程序中并使用一个功能键来触发它们）。
两个单独的确认步骤也可避免非故障安全操作员监视和控制系统误触发确认。

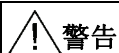
 **警告**

如果操作员监视和控制系统可以访问多个使用 F_ACK_OP 进行故障安全确认的 F-CPU，或如果已将操作员监视和控制系统与 F-CPU（具有 F_ACK_OP F 应用程序块）联网，则执行这两个确认步骤**之前**，必须确保实际上正对正确的 F-CPU 进行寻址：

- 在每个 F-CPU 中，在标准用户程序的 DB 中存储一个全网唯一的 F-CPU 名称。
- 在操作员监视和控制系统中设置一个区域，可通过该区域在执行两个确认步骤之前从 DB 中在线读出 F-CPU 名称。
- 可选：在操作员监视和控制系统中设置一个区域，用以永久存储 F-CPU 名称。然后，只需比较在线读出的 F-CPU 名称和永久存储的名称，即可确定是否正在对目标 F-CPU 进行寻址。

编写重新集成 F-I/O 的用户确认程序的步骤实例

1. 可选：如果要在发生 F-I/O 故障或通道故障后自动重新集成（无用户确认），请将各个 F-I/O DB 中的 ACK_NEC 变量设置为“0”。



警告

从安全角度出发，只有在相关过程允许自动重新集成时才为 ACK_NEC 分配 0。

2. 可选：发生错误时评估各个 F-I/O DB 中的 QBAD 或 QBAD_I_xx 和 QBAD_O_xx 或 DIAG 变量，以触发指示灯（如果适用），并且/或者在标准用户程序中通过评估 QBAD 或 QBAD_I_xx 和 QBAD_O_xx 或 DIAG，在操作员监视和控制系统上生成错误消息；可在执行确认操作之前评估这些消息。此外，还可以评估 F-CPU 的诊断缓冲区。
3. 可选：评估各个 F-I/O DB 中的 ACK_REQ 变量（例如在标准用户程序中或在操作员监视和控制系统上），以查询或指示是否需要用户确认。
4. 将确认键的输入或 F_ACK_OP 的 OUT 输出分配到相应的 F-I/O DB 中的 ACK_REI 变量或 FB 219 “F_ACK_GL” F 应用程序块的 ACK_REI_GLOB 输入（请参阅上文）。

参见

F-I/O DB (页 104)

FB 187 "F_ACK_OP": 故障安全确认 (页 192)

6.2 在智能从站的 F-CPU 的安全程序中执行用户确认

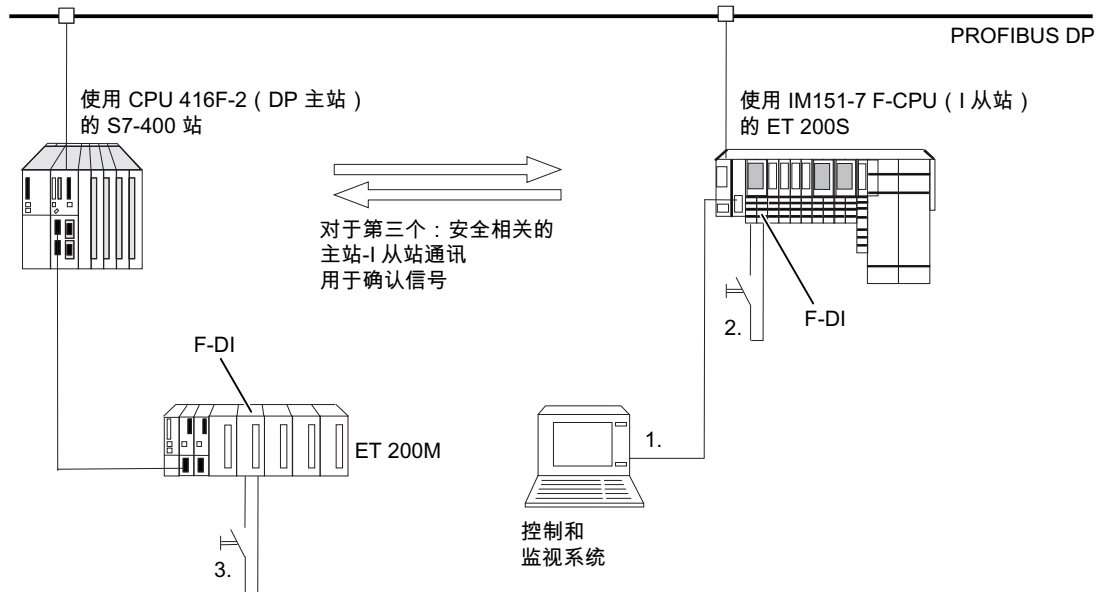
用户确认的选项

可通过以下方法之一执行用户确认：

- 通过可用于访问智能从站的 F-CPU 的操作员监视和控制系统
- 通过连接至输入被分配给智能从站的 F-CPU 的 F-I/O 的确认键
- 通过连接至输入被分配给 DP 主站 F-CPU 的 F-I/O 的确认键

下图说明了以上三个选项。

6.2 在智能从站的 F-CPU 的安全程序中执行用户确认



1. 通过可用于访问智能从站的 F-CPU 的操作员监视和控制系统执行用户确认

要通过可用于访问智能从站的 F-CPU 的操作员监视和控制系统执行用户确认，需要 *Distributed Safety F* 库 (V1) 中的 F_ACK_OP F 应用程序块。

编程步骤

请按照『在 DP 主站的 F-CPU 的安全程序中执行用户确认』下『编写通过操作员监视和控制系统执行用户确认程序的步骤』一章中介绍的步骤进行编程。

然后可通过操作员监视和控制系统直接访问智能从站中 F_ACK_OP 的背景数据块。

2. 通过输入被分配给智能从站的 F-CPU 的 F-I/O 上的确认键执行用户确认

说明

如果确认键所连接的 F-I/O 中发生通讯错误、F-I/O 故障或通道故障，将无法再确认该 F-I/O 的重新集成。

该“块”只能通过将智能从站的 F-CPU 从 STOP 切换到 RUN 才能删除。

因此，对于确认键所连接的 F-I/O 的重新集成的确认，建议还要提供通过可用于访问智能从站的 F-CPU 的操作员监视和控制系统执行的确认（请参阅 1）。

3. 通过输入被分配给 DP 主站的 F-CPU 的 F-I/O 上的确认键执行用户确认

如果要在智能从站的 F-CPU 的安全程序中使用分配给 DP 主站上的 F-CPU 的确认键执行用户确认，必须通过安全相关的主站与智能从站通讯将确认信号从 DP 主站的 F-CPU 的安全程序发送至智能从站的 F-CPU 的安全程序。

编程步骤

1. 在 DP 主站的 F-CPU 的安全程序中调用 F_SENDDP F 应用程序块。
2. 在智能从站的 F-CPU 的安全程序中调用 F_RCVDP F 应用程序块。
3. 为 F_SENDDP 块的输入 SD_BO_xx 提供确认键的输入。
4. 现在可在 F_RCVDP 的相应输出 RD_BO_xx 处获得用于评估用户确认的确认信号。

现在可在对确认信号进行进一步处理的程序段中，通过对相关背景数据块（例如 "Name F_RCVDP1".RD_BO_02）直接进行完整资格的访问来读取确认信号。要启用此功能，必须首先为符号表中 F_RCVDP 的背景数据块分配符号名（该实例中为 "Name F_RCVDP1"）。

5. 为 F_RCVDP 的相应输入 SUBBO_xx 提供故障安全值“RLO0”，以便在启动发送和接收 F 系统之后第一次建立通讯之前，或在发生安全相关的通讯错误时，不会触发意外的用户确认。可在 F 共享 DB 中获得 RLO 0。在输入 SUBBO_xx 处，输入具有完整资格的 "F_GLOBDB".RLO0。

说明

如果确认键所连接的 F-I/O 中发生通讯错误、F-I/O 故障或通道故障，则无法再确认该 F-I/O 的重新集成。

该“块”只能通过将 DP 主站的 F-CPU 从 STOP 切换到 RUN 才能删除。

因此，对于确认键所连接的 F-I/O 的重新集成的确认，建议还要提供通过可用于访问 DP 主站的 F-CPU 的操作员监视和控制系统执行的确认。

如果发生安全相关的主站与智能从站通讯错误，将不能发送确认信号，并且无法再确认安全相关通讯的重新集成。

该“块”只能通过将智能从站的 F-CPU 从 STOP 切换到 RUN 才能删除。

因此，对于安全相关通讯的重新集成的确认，建议还要提供通过可用于访问智能从站的 F-CPU 的操作员监视和控制系统执行的确认，以发送确认信号（请参阅 1）。

6.2 在智能从站的 F-CPU 的安全程序中执行用户确认

参见

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

安全相关通讯概述 (页 131)

FB 187 "F_ACK_OP": 故障安全确认 (页 192)

FB 223 "F_SENDDP" 和 FB 224 "F_RCVDP": 通过 PROFIBUS DP 发送和接收数据 (页 233)

标准用户程序和安全程序之间的数据交换

7.1 数据从安全程序传送到标准用户程序

数据从安全程序传送到标准用户程序

标准用户程序可以读出安全程序的所有数据，例如，通过对以下数据块进行符号（完整资格的）访问：

- F-FB 的背景数据块
- F-DB（例如 "Name F_DB".Signal_1）
- F-I/O 的过程输入映像和过程输出映像（例如，"Emergency_Stop_Button_1"[I 5.0]）

说明

F-I/O 的过程输入映像不仅在执行 F 程序块之前的 F 运行组开始时进行更新，还会被标准操作系统更新。

要了解标准操作系统的更新次数，请参考 *STEP 7 在线帮助* 中的“输入/输出过程映像”。如果使用支持部分过程映像的 F-CPU，请记住使用部分过程映像时的更新次数。因此，在标准用户程序中访问 F-I/O 的过程输入映像时，可获得与在安全程序中获得的值不同的值。可能获得不同值的原因是：

- 更新次数不同
- 安全程序中使用了故障安全值

要使在标准用户程序中获得的值与在安全程序中获得的值相同，则仅在执行 F 运行组之后才能在标准程序中访问过程输入映像。在这种情况下，还可在标准用户程序中评估相关 F-I/O DB 中的 QBAD 或 QBAD_I_xx 变量，以确定过程输入映像是正在接收故障安全值（0）还是正在接收过程数据。使用部分过程映像时，还请确保从执行 F 运行组 (F-CALL) 到在标准用户程序中评估过程输入映像的过程中，标准操作系统或 SFC 26 UPDAT_PI 不更新过程映像。

7.1 数据从安全程序传送到标准用户程序

F 共享 DB

在标准用户程序中或在操作员监视和控制系统上，可读出 F 共享 DB 中的以下信息：

- 运行模式：安全模式或取消激活的安全模式（“MODE”变量）
- 错误信息“执行安全程序时出错”（“ERROR”变量）
- 安全程序的集体签名（“F_PROG_SIG”变量）
- 安全程序的编译日期（“F_PROG_DAT”变量，DATE_AND_TIME 数据类型）

可使用具有完整资格的访问来访问这些变量（例如 "F_GLOBDB".MODE）。F 共享 DB 的编号和符号名及变量的绝对地址在安全程序的打印输出中指明。

位存储器

还可以在安全程序中写入存储器位，以使标准用户程序无需通过 F-Data 块即可使用安全程序的中间结果。但是，不得在安全程序本身中读取这些存储器位。

过程输出映像

可以将标准 I/O 的过程输出映像（PIQ）写入安全程序中，例如，为了显示的目的。同样，不得在安全程序中读取这些值（请参阅『F-FBD/F-LAD 编程语言和标准 FBD/LAD 语言之间的区别』一章中受支持的地址区表）。

参见

F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语言之间的区别 (页 66)

7.2 数据从标准用户程序传送到安全程序

数据从标准用户程序传送到安全程序

作为基本原理，只有故障安全 I/O 和其它安全程序（位于其它 F-CPU 中）的故障安全数据或故障安全信号可在安全程序中处理，因为标准数据和信号不安全。

然而，如果必须在安全程序中处理标准用户程序的数据，则可在安全程序中评估标准用户程序的存储器位或标准 I/O 的过程输入映像（PII）（请参阅『F-FBD/F-LAD 编程语言和标准 FBD/LAD 语言之间的区别』一章中受支持的地址区表）。



由于这些数据不是安全生成的，因此必须在安全程序中执行其它过程特定的有效性检查，以确保不发生危险状况。如果在两个 F 运行组中使用存储器位或标准 I/O 的输入，则必须分别在每个 F 运行组中执行有效性检查。

为了便于进行检查，在打印输出安全程序时，将包括来自标准用户程序、在安全程序中评估的所有信号。

说明

由于标准用户程序的数据是由指令读取和写入的，因此这些数据（位存储器或标准 I/O 的 PII）不能用于 RLO 沿检测（N、P）或地址沿检测（NEG、POS）指令的边沿存储器位，也不能用于触发器（SR、RS）指令的地址。

说明

当在 *FBD/LAD* 编辑器中使用 F-FBD/F-LAD 编辑 F-Block 时，默认情况下，所有非故障安全的地址均以黄色背景显示。

7.2 数据从标准用户程序传送到安全程序

实例：编写有效性检查程序

- 使用比较指令检查来自标准用户程序的非安全数据是否超出允许的上限或低于允许的下限。然后可使用比较的结果影响安全功能。
- 使用来自标准用户程序的非安全信号，例如，使用设置、复位或触发器指令只允许关闭电机，而不允许打开电机。
- 对于来自标准用户程序的启动循环、门控非安全信号，例如，使用带有从故障安全信号中获取的开始条件的 AND 门控。

如果要在安全程序中处理非安全数据，请记住对于所有非安全数据，没有十分简单的有效性检查方法。

在 F 运行组运行期间可更改数据时，从标准用户程序中读取数据

如果要在安全程序中读取标准用户程序的数据（位存储器或标准 I/O 的 PII），并且这些数据可在 F 运行组（从中读取数据）的运行期间通过标准用户程序或操作员监视和控制系统进行更改，则必须使用专用存储器位。例如，因为标准用户程序正被较高优先级的周期性中断执行。调用 F 运行组之前，必须将数据从标准用户程序直接写入这些存储器位。然后，只能在安全程序中访问这些存储器位。

另请注意，由于时钟存储器与 F-CPU 周期异步运行，因此您在组态 F-CPU（在 *HW Config* 中的 F-CPU 对象属性中）时定义的**时钟存储器**在 F 运行组运行期间可以更改。

说明

如果未遵守以上规定，F-CPU 会切换到 STOP。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
 - “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
 - “安全程序：内部 CPU 故障；内部错误信息：404”
-

参见

F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语言之间的区别 (页 66)

编译安全程序 (页 260)

对通讯进行组态和编程

8.1 安全相关通讯概述

引言

本节提供了 *S7 Distributed Safety*F 系统中安全相关通讯的以下选项的概览：

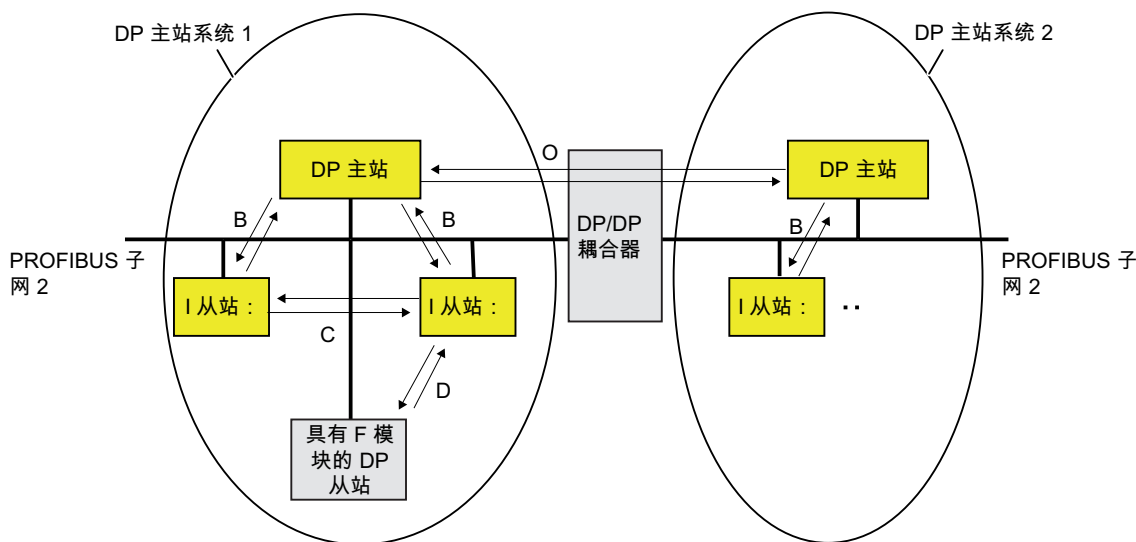
- 安全相关的智能从站与从站通讯（通过 PROFIBUS DP）

安全相关的 CPU 与 CPU 通讯：

- 安全相关的主站与主站通讯（通过 PROFIBUS DP）
- 安全相关的主站与智能从站通讯（通过 PROFIBUS DP）
- 安全相关的智能从站与智能从站通讯（通过 PROFIBUS DP）
- 安全相关的 IO 控制器与 IO 控制器通讯（通过 PROFINET IO）
- 通过 S7 连接的安全相关的通讯（通过工业以太网）
- 安全相关的 *S7 Distributed Safety* 和 *S7 F* 系统之间的通讯

通过 PROFIBUS DP 的安全相关通讯的概述

下图显示了 *S7 Distributed Safety F* 系统中通过 PROFIBUS DP 进行的安全相关通讯的四个选项的概览。



- 安全相关的主站-主站通讯 (通过 DP/DP 耦合器)
- 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 PROFIBUS DP 或 PROFINET IO 的安全相关的 CPU 与 CPU 通讯

在安全相关的 CPU 与 CPU 通讯中，固定数量的数据类型为 **BOOL** 和 **INT** 的故障安全数据将在 DP 主站/智能从站或 IO 控制器的 F-CPU 中的安全程序之间以故障安全方式传输。

数据传送将使用 F 应用程序块 **F_SENDDP** 进行发送，用 **F_RCVDP** 进行接收。数据将存储在 DP/DP 耦合器/DP 主站/智能从站或 PN/PN 耦合器已组态的地址区中。

通过 PROFIBUS DP 的安全相关的智能从站与从站通讯

安全相关的智能从站与从站通讯可以通过 DP 从站（支持安全相关的智能从站与从站通讯）中的 F-I/O 来执行，例如，通过所有 ET 200S F 模块和通过所有 S7-300 故障安全信号模块（具有 IM 153-2，订货号 6ES7 153-2BA01-0XB0 或更高，固件版本高于 V4.0.0）。

在智能从站 F-CPU 和从站 F-I/O 的安全程序之间使用直接数据交换进行安全相关的通讯（与在标准程序中一样）。过程映像（PII 和 PIQ）用于访问智能从站 F-CPU 的安全程序中 F-I/O 的通道。

使用 IE/PB 连接器

也可使用 IE/PB 连接器，在 *S7 Distributed Safety* F 系统中通过 PROFIBUS DP 将安全相关的通讯的四个选项链接到 PROFINET IO（请参阅有关 PROFINET IO 和 IE/PB 连接器的文档）。

说明

如果正在使用 IE/PB 连接器，则必须在组态 F 特定监视时间和计算 F 系统的最大响应时间时将其考虑在内（另请参阅 *S7 Distributed Safety* 的用于计算响应时间的 Excel 文件 *s7cotib.xls*）。

请注意，该 Excel 文件并不支持所有可能的组态。

通过工业以太网的安全相关的 CPU 与 CPU 通讯

可通过已组态的 S7 连接进行通过工业以太网的安全相关的 CPU 与 CPU 通讯可与以下 CPU 进行通讯：

- CPU 315F-2 PN/DP（仅通过 CPU PN 接口）
- CPU 317F-2 PN/DP（仅通过 CPU PN 接口）
- CPU 319F-3 PN/DP（仅通过 CPU PN 接口）
- CPU 416F-2，固件版本 V4.0 及更高版本
- CPU 416F- 3 PN/DP

在通过 S7 连接的安全相关的通讯中，指定数量的数据类型为 BOOL、INT、WORD 或 TIME 的故障安全数据将在通过 S7 连接链接的 F-CPU 的安全程序之间以故障安全方式进行传送。

数据传送将使用 F 应用程序块 F_SENDS7 进行发送，用 F_RCVS7 进行接收。在发送方和接收方分别使用一个 F-DB（“F 通讯 DB”）进行数据交换。

此外，可在 *S7 Distributed Safety* 和 *S7 F System* 之间进行安全相关的通讯。

8.2 安全相关的主站与主站通讯

8.2.1 组态地址区（安全相关的主站与主站通讯）

DP/DP 耦合器

可通过 DP/DP 耦合器（订货号 6ES7158-0AD01-0XA0）在 DP 主站 F-CPU 的安全程序之间进行安全相关的通讯。

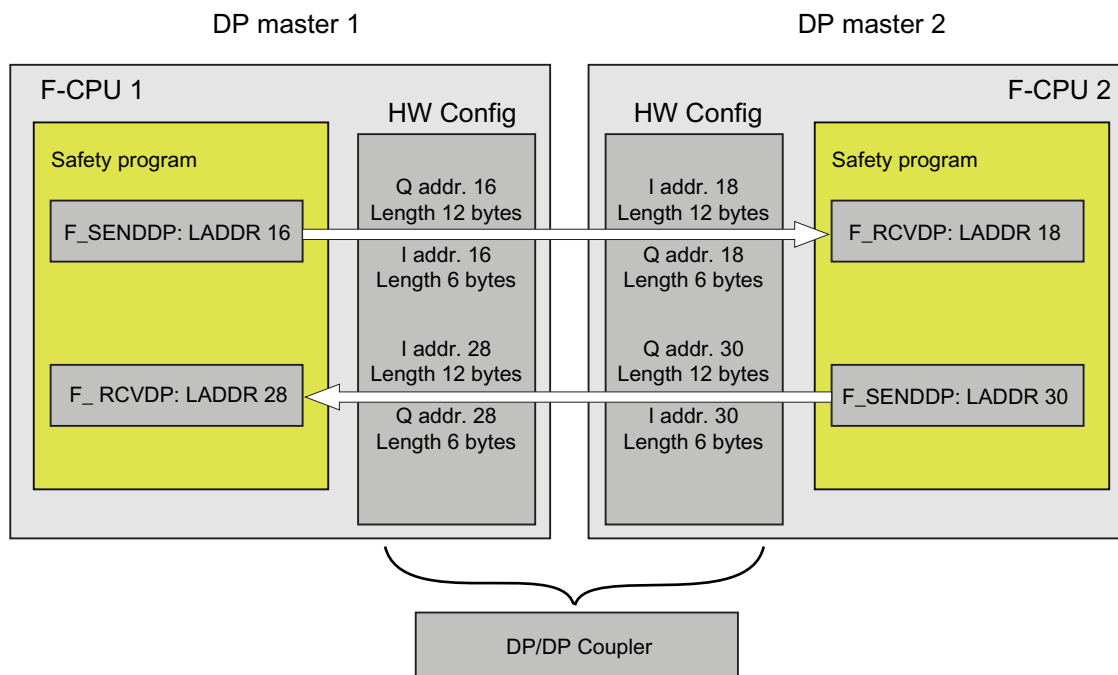
每个 F-CPU 均通过其 PROFIBUS DP 接口链接至 DP/DP 耦合器。

说明

将 DP/DP 耦合器的 DIP 开关上的数据有效性指示灯“DIA”切换到“OFF”。否则，将无法进行安全相关的 CPU 与 CPU 通讯。

组态地址区

对于两个 F-CPU 之间通过 DP/DP 耦合器的每个连接，必须在 *HW Config* 中为 DP/DP 耦合器中的输出数据组态一个地址区，并为输入数据组态另一个地址区。下图中，两个 F-CPU 中的任一个都可以发送和接收数据（双向通讯）。



定义地址区的规则

要发送的数据的输出数据地址区必须以与关联的输入数据地址区相同的起始地址开始。输出数据地址区共需要 12 个字节（一致），而输入数据地址区需要 6 个字节（一致）。

要接收的数据的输入数据地址区必须以与关联的输出数据地址区相同的起始地址开始。输入数据地址区共需要 12 个字节（一致），而输出数据地址区需要 6 个字节（一致）。

8.2.2 组态安全相关的主站与主站通讯

要求

已在 *HW Config* 中创建两个站，每个站都有一个 DP 主站系统。

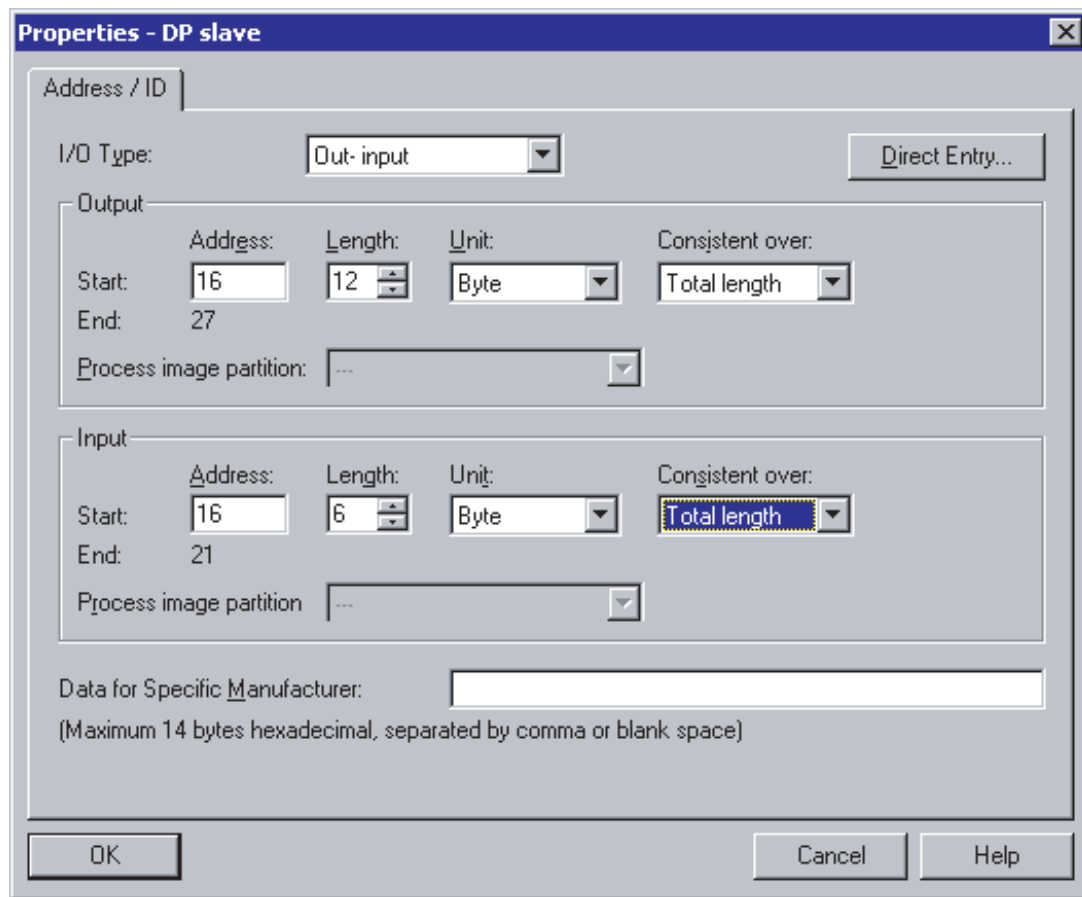
组态主站与主站通讯的操作步骤（以下实例为双向通讯）

1. 通过 F-CPU 1 打开站。
2. 从硬件目录“PROFIBUS DP\其它现场设备 (Additional field devices)\网关 (Gateway)\DP/DP 耦合器 (DP/DP coupler)”中选择“DP/DP 耦合器”(DP/DP coupler)。将 DP/DP 耦合器放置在 F-CPU 的 DP 主站系统上。
3. 将自动在快捷菜单中分配一个可用的 PROFIBUS 地址。可在地址区 1 到 125 中更改该地址。必须通过 DP/DP 耦合器上的开关设置此地址：直接在 DP/DP 耦合器上通过 DIP 开关进行设置或使用 *STEP 7* 进行设置（请参阅《DP/DP 耦合器》手册）。可使用“属性” (Properties) 菜单命令插入子网名称、子网 ID、作者和注释。在“网络设置” (Network Settings) 选项卡中，应将传输率设置为不低于“1.5 Mbps”。必须选择“DP”作为规约。
4. 为了可以在 CPU 之间一致地建立安全相关的通讯，并可使用任意地址和长度设置，必须使用通用模块。在 DP 主站系统上选择“DP/DP”，然后从 DP/DP 耦合器 (DP/DP Coupler) 文件夹插入通用模块。

用于双向连接的每个 F-CPU 将使用两个通用模块，即每个 F-CPU 都将发送和接收数据。

5. 选择第一个通用模块，并选择**编辑 (Edit) > 对象属性 (Object Properties)** 菜单命令。

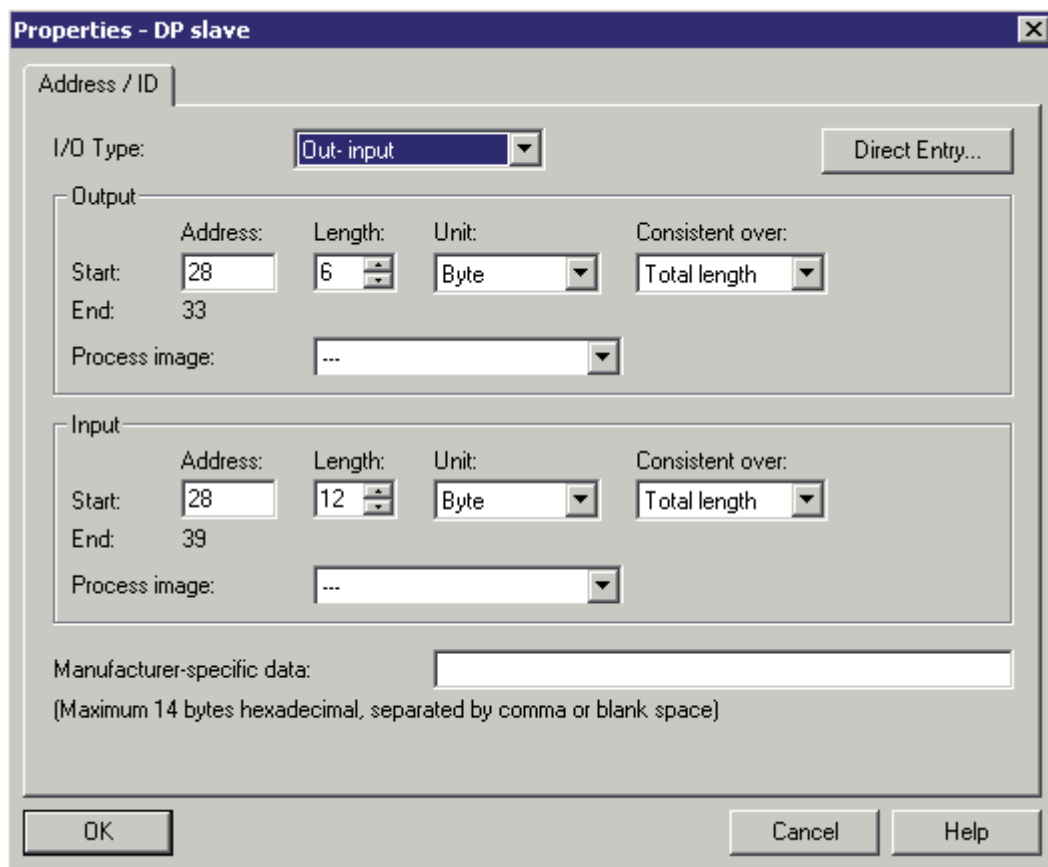
对象属性 (object properties) 对话框出现。



6. 在第一个通用模块的对象属性中，选择“输出输入” (Out input) 作为 I/O 类型。
7. 为输出数据地址区输入关联的值。在我们的实例中，输入“16”作为“起始地址”(Start Address)、“12”作为“长度”(Length)、“字节”(Byte) 作为“单位”(Unit) 以及“总长度”(Total Length) 作为“一致”(Consistent)。
8. 为输入数据地址区输入关联的值。在我们的实例中，输入“16”作为“起始地址”(Start Address)、“6”作为“长度”(Length)、“字节”(Byte) 作为“单位”(Unit) 以及“总长度”(Total Length) 作为“一致”(Consistent)。
9. 单击“确定”(OK) 确认。

10. 选择第二个通用模块，并选择**编辑 (Edit) > 对象属性 (Object Properties)** 菜单命令。

对象属性 (object properties) 对话框出现。



11. 在第二个通用模块的对象属性中，选择“输出输入”(Out input) 作为 I/O 类型。

12. 为输出数据地址区输入关联的值。在我们的实例中，输入“28”作为“起始地址”(Start Address)、“6”作为“长度”(Length)、“字节”(Byte) 作为“单位”(Unit) 以及“总长度”(Total Length) 作为“一致”(Consistent)。

13. 为输入数据地址区输入关联的值。在我们的实例中，输入“28”作为“起始地址”(Start Address)、“12”作为“长度”(Length)、“字节”(Byte) 作为“单位”(Unit) 以及“总长度”(Total Length) 作为“一致”(Consistent)。

14. 单击“确定”(OK) 确认。 这将完成 F-CPU 1 的主站与主站通讯的组态。

为 F-CPU 2 执行第 1 步至第 14 步。请注意，您需要相应地调整地址（请参阅『组态地址区 [安全相关的主站与主站通讯]』一章中的图）。

说明

请确保分配给输出和输入数据地址区的起始地址的值是相同的。

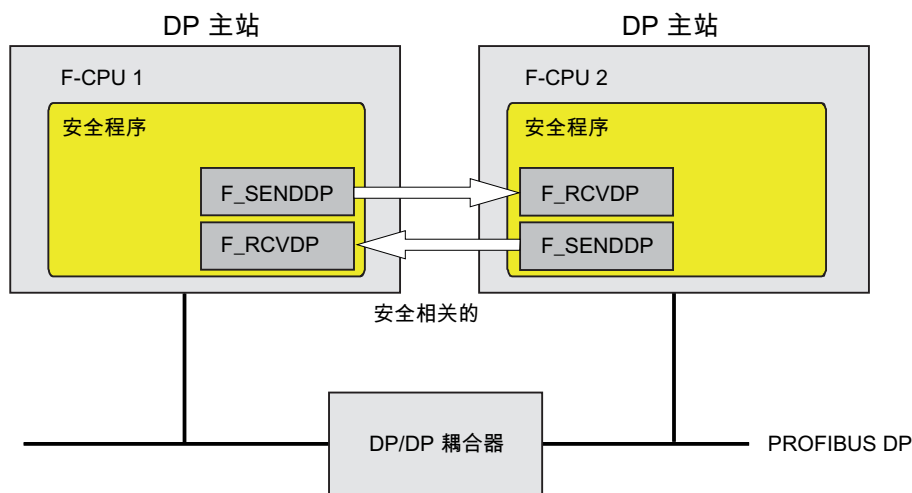
请始终为所有输入和输出数据区选择“在总长度上一致”(Consistent over total length) 选项。

附加信息

《DP/DP 耦合器》手册中介绍了 DP/DP 耦合器。

8.2.3 通过 F_SENDDP 和 F_RCVDP 的通讯（安全相关的主站与主站通讯）

通过 F_SENDDP 和 F_RCVDP 的通讯



安全相关的通讯将使用 F 应用程序块 F_SENDDP 进行发送，用 F_RCVDP 进行接收。可使用它们以故障安全方式传送固定数量的数据类型为 BOOL 和 INT 的故障安全数据。

可以在 *Distributed Safety* F 库 (V1) 中的 *F 应用程序块* 文件夹中找到这些 F 应用程序块。必须在 F-PB 开始时调用 F_RCVDP。必须在 F-PB 结束时调用 F_SENDDP。

请注意，仅当在相应 F 运行组执行结束时调用 F_SENDDP 之后，才会发送这些发送信号。

有关 F_SENDDP 和 F_RCVDP F 应用程序块的详细说明，请参考『FB 223“F_SENDDP”和 FB 224“F_RCVDP”：通过 PROFIBUS DP 发送和接收数据』一章。

参见

FB 223“F_SENDDP”和 FB 224“F_RCVDP”：通过 PROFIBUS DP 发送和接收数据 (页 233)

8.2.4 编写安全相关的主站与主站通讯程序

要求

编程之前必须满足以下要求：

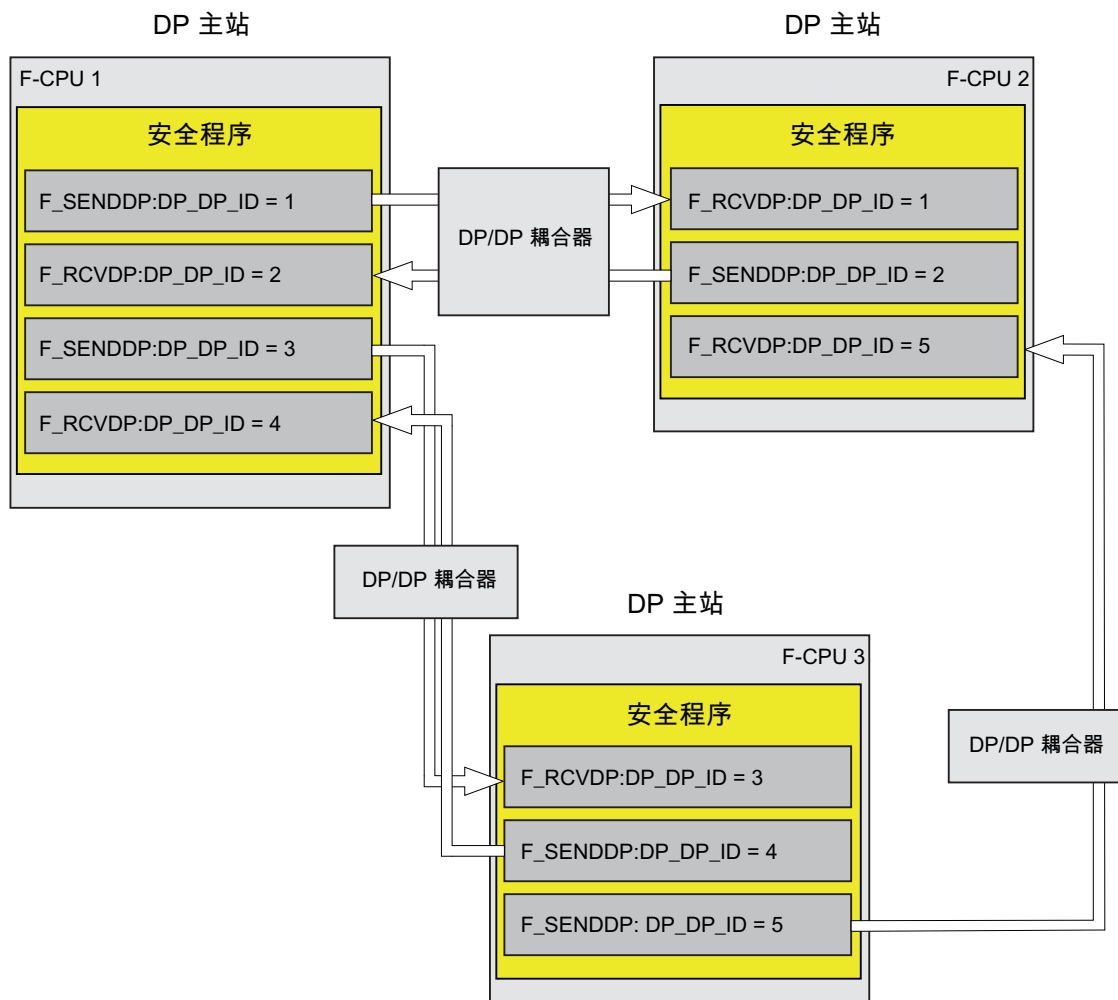
- 必须在 *HW Config* 中组态 DP/DP 耦合器的输入和输出数据的地址区。
- 两个 CPU 都必须组态为 F-CPU：
 - 必须选中“CPU 包含安全程序”（CPU contains safety program）选项
 - 必须输入 F-CPU 的密码

编程步骤

1. 在要发送数据的安全程序中，在 F-PB 结束时调用 F_SENDDP F 应用程序块以进行发送。
2. 在要接收数据的安全程序中，在 F-PB 开始时调用 F_RCVDP F 应用程序块以进行接收。
3. 将在 *HW Config* 中组态的 DP/DP 耦合器的输出和输入数据地址区的起始地址分配给各个 LADDR 输入。
必须为涉及的每个 F-CPU 的每个通讯连接执行该分配。

8.2 安全相关的主站与主站通讯

- 4. 将各个地址关联的值分配给 DP_DP_ID 输入。这将在一个 F-CPU 中的 F_SENDDP 和另一个 F-CPU 中的 F_RCVDP 之间建立起关联。关联的故障安全块将接收相同的 DP_DP_ID 值。



警告

每个地址关联（输入参数 DP_DP_ID；数据类型：INT）的值都是用户定义的；但是，在网络中的所有安全相关的通讯连接中，它必须是唯一的。

说明

每次调用 F_SENDDP 或 F_RCVDP 时必须使用单独的实例 DP。

不得为 F_RCVDP 的输入和输出参数提供 F 程序块的本地数据。

如果已经为相同 F_RCVDP 调用或者其它 F_RCVDP 或 F_RCVS7 调用的输入参数使用了此实参，则不得为 F_RCVDP 的输出参数使用该实参。如果未遵守上述规定，F-CPU 会切换到 STOP。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

5. 为 F_SENDDP 的 SD_BO_xx 输入提供发送信号。为了在传送块参数时减少中间信号，可在调用 F_SENDDP 前使用具有完整资格的符号访问（例如 "Name F_SENDDP1".SD_BO_02）将值直接写入 F_SENDDP 的背景数据块。
6. 为 F_RCVDP 的 RD_BO_xx 输出提供要在其它程序段中进一步处理的信号，或使用具有完整资格的访问在程序段中的关联背景数据块中直接读取接收到的、要进一步处理的信号（例如 "Name F_RCVDP1".RD_BO_02）。
7. 为 F_RCVDP 的 SUBBO_xx 和 SUBI_xx 输入提供 F_RCVDP 要输出的故障安全值以代替过程数据，直到启动发送和接收 F 系统后首次建立起通讯或在安全相关的通讯中发生错误后为止。
 - 常数故障安全值的规范：

对于数据类型为 INT 的数据，可直接输入常数故障安全值作为输入 SUBI_xx 处的常量。如果要为数据类型为 BOOL 的数据指定常数故障安全值，请使用 F 共享 DB 中的变量“RLO0”或“RLO1”。然后，在输入 SUBBO_xx 处，输入具有完整资格访问的 "F_GLOBDB".RLO0（如果要指定故障安全值“0”）和 "F_GLOBDB".RLO1（如果要分配故障安全值“1”）。
 - 动态故障安全值的规范：

如果要指定动态故障安全值，请定义一个可在 F-DB 中通过安全程序动态更改的变量，并在输入 SUBI_xx 或 SUBBO_xx 处使用完整资格访问来声明该变量。

 警告

<p>请注意，用于动态更改动态故障安全值的变量的安全程序只能在调用 F_RCVDP 之后进行处理，因为调用 F_RCVDP 之前 F-PB 中可能没有程序段，最多会有另一个 F_RCVDP。因此，必须为那些在启动 F 系统后的第一个周期中要由 F_RCVDP 输出的变量分配适当的初始值/实际值。</p>
--

8. 使用要求的监视时间组态 F_RCVDP 和 F_SENDDP 的 TIMEOUT 输入。



警告

这样可以确保（从故障安全角度出发）仅当信号待决的时间不小于分配的监视时间 (TIMEOUT) 时，才会在发送方捕获要传送的信号电平并传送给接收方。

有关计算监视时间的信息，请参考《SIMATIC S7 中的安全工程》系统手册。

9. 可选：评估 F_RCVDP 的 ACK_REQ 输出（例如在标准用户程序中或操作员监视和控制系统上）以查询或指示是否需要用户确认。
10. 为 F_RCVDP 的 ACK_REI 输入提供确认重新集成的信号。
11. 可选：评估 F_RCVDP 的 SUBS_ON 输出或 F_SENDDP，以查询 F_RCVDP 是否正在输出在 F_RCVDP 的 SUBBO_xx 和 SUBI_xx 输入处分配的故障安全值。
12. 可选：评估 F_RCVDP 的 ERROR 输出或 F_SENDDP（例如在标准用户程序中或操作员监视和控制系统上），以查询或指示是否发生了通讯错误。
13. 可选：评估 F_RCVDP 的 SENDMODE 输出，以查询带相关 F_SENDDP 的 F-CPU 是否处于取消激活安全模式下。



警告

如果带相关 F_SENDDP 的 F-CPU 处于取消激活安全模式下，则不能再认为从该 F-CPU 接收的数据是安全生成的。然后必须采取组织措施（例如操作监视和手动安全关闭），以确保这部分受接收数据影响的系统的安全。或者，必须通过评估 SENDMODE 来输出故障安全值，而不是输出 F-CPU 中通过 F_RCVDP 接收到的数据。

参见

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

取消激活安全模式 (页 288)

8.2.5 数据传输的限制（安全相关的主站与主站通讯）

说明

如果要传送的数据量超过一对 F_SENDDP/F_RCVDP 块的容量，可调用第二个（或第三个）F_SENDDP/F_RCVDP。这需要组态另一个通过 DP/DP 耦合器进行的连接。使用一个 DP/DP 耦合器是否可行取决于该 DP/DP 耦合器的容量限制。

8.3 安全相关的主站与智能从站通讯

8.3.1 组态地址区（安全相关的主站与智能从站通讯）

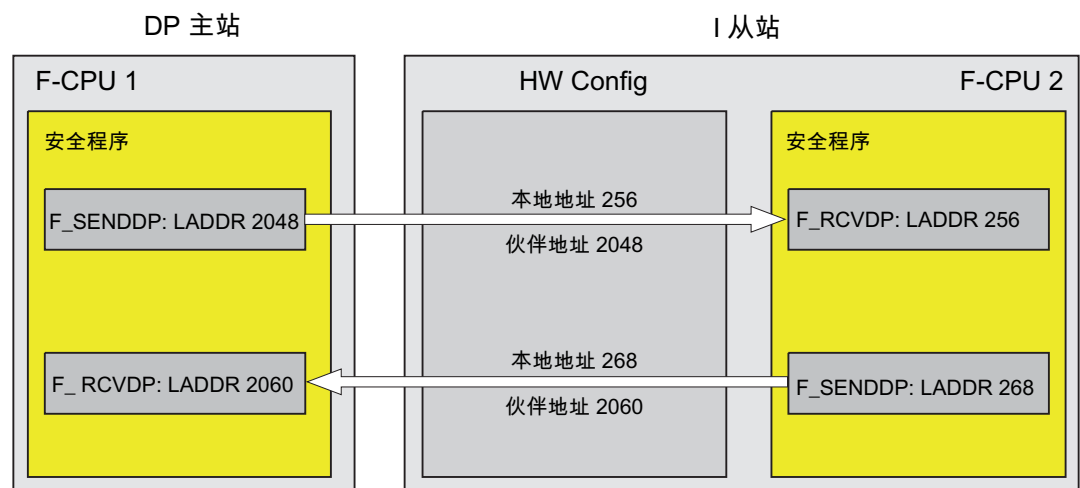
引言

DP 主站 F-CPU 的安全程序和一个或多个智能从站 F-CPU 的安全程序之间通过主站与智能从站连接进行安全相关的通讯（与在标准系统中一样）。

主站与智能从站通讯不需要任何其它硬件。

组态地址区

必须在 *HW Config* 中为两个 F-CPU 之间的每个通讯连接组态地址区。下图中，两个 F-CPU 中的任一个都可以发送和接收数据（双向通讯）。



在智能从站的对象属性中，组态以下地址：

- 用于将数据发送到 DP 主站的本地地址（智能从站）和伙伴地址（DP 主站）
- 用于接收 DP 主站的数据的本地地址（智能从站）和伙伴地址（DP 主站）

在安全程序中将组态的地址分配给相应 F_SENDDP 和 F_RCVDP F 应用程序块的 LADDR 参数。

8.3 安全相关的主站与智能从站通讯

分配的地址区

每个本地地址和伙伴地址均代表输入和输出数据的地址区的起始地址。一旦组态了本地地址和伙伴地址，将自动分配地址区。下表中列出了分配给发送连接和接收连接的地址区：

通讯连接的 F-CPU 中分配的地址区
发送：智能从站发送到 DP 主站	智能从站：12 个字节的输出数据和 6 个字节的输入数据
	DP 主站：12 个字节的输入数据和 6 个字节的输出数据
接收：智能从站从 DP 主站处接收	智能从站：12 个字节的输入数据和 6 个字节的输出数据
	DP 主站：12 个字节的输出数据和 6 个字节的输入数据

说明

由于应为模块的地址区保留过程映像，我们建议使用过程映像以外的地址作为本地地址和伙伴地址。

8.3.2 组态安全相关的主站与智能从站通讯

要求

已在 *STEP 7* 中创建了一个项目。

组态主站与智能从站通讯的操作步骤（以下实例为双向通讯）

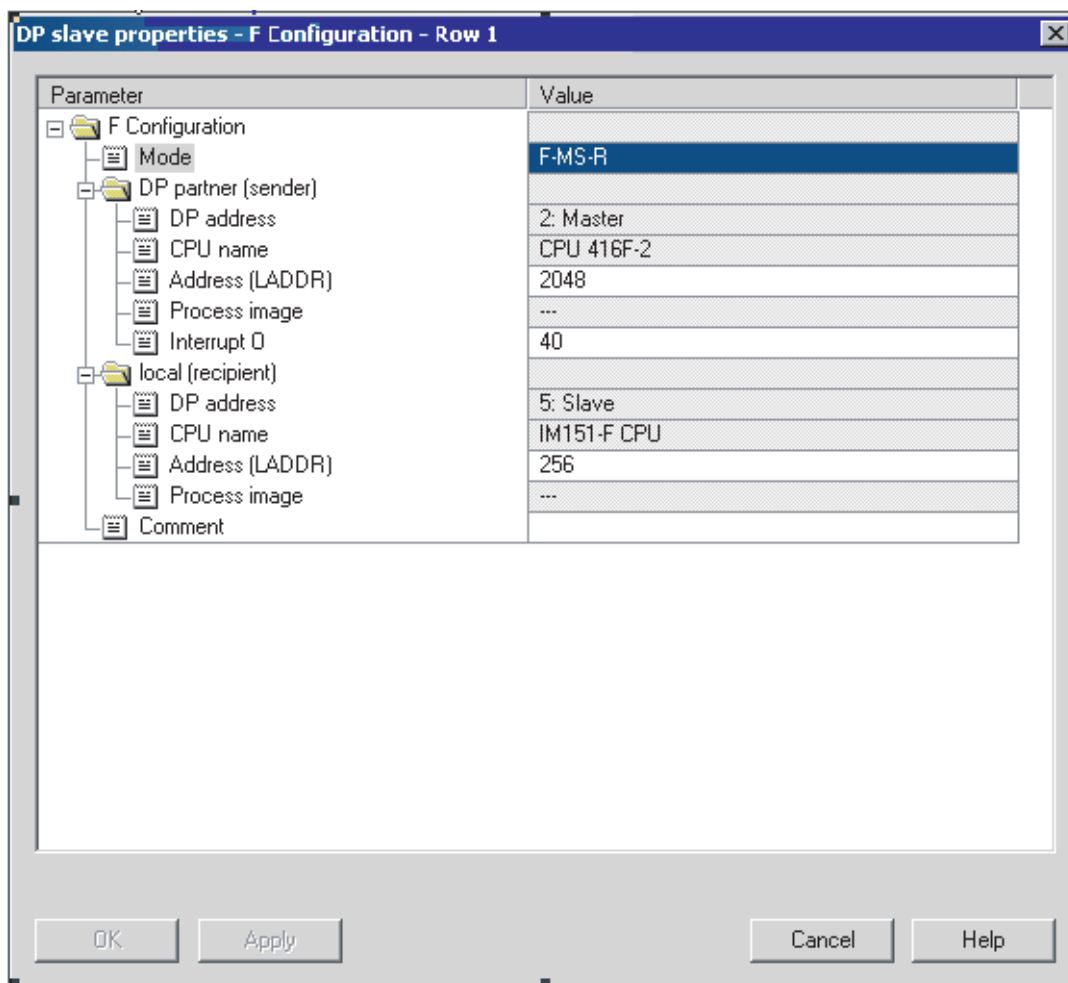
1. 在项目中创建一个站（例如在 *SIMATIC 管理器* 中创建一个 S7-300 站）。
2. 为该站分配一个 F-CPU（从 *HW Config* 中的硬件目录中）。
3. 将该 CPU 组态为 DP 从站（在 *HW Config* 中 CPU 的 DP 接口的对象属性的“工作模式”[Operating Mode] 选项卡中）。
4. 创建另一个站，然后分配一个 F-CPU（请参阅步骤 1 和 2）。
5. 将该 CPU 组态为 DP 主站（在 *HW Config* 中 CPU 的 DP 接口的对象属性的“工作模式”[Operating Mode] 选项卡中）。
6. 在“已组态的站”（Configured stations）下的硬件目录中，选择智能从站的站类型（例如“CPU 31x”）并将其放置在 DP 主站系统上。
7. 在自动打开的“连接”（Connection）对话框中，将智能从站链接至 DP 主站。
现在可以为安全相关的主站与智能从站通讯定义地址区：
8. 在智能从站对象属性的“F 组态” (F-Configuration) 选项卡中，选择“新建”(New)。

8.3 安全相关的主站与智能从站通讯

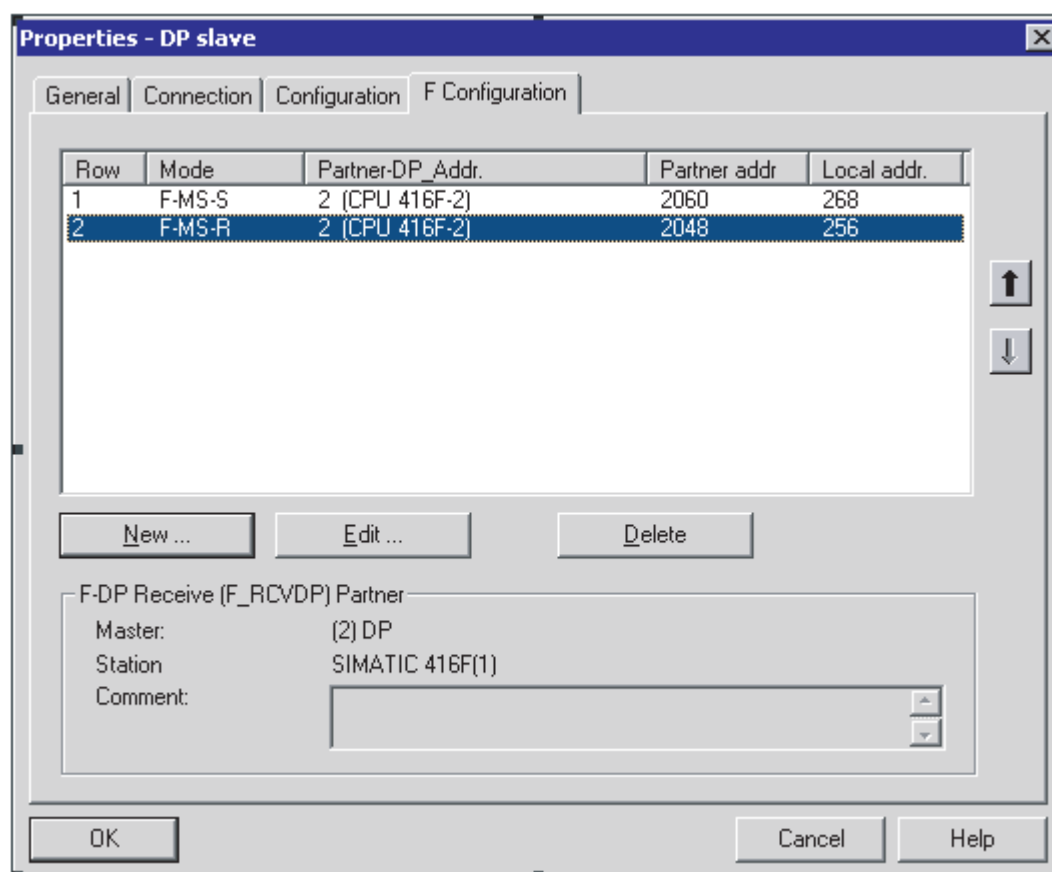
9. 在下一个对话框中，为来自 DP 主站的接收连接输入以下内容（对于我们的实例）：

- 为 Mode 输入 "F-MS-R"（通过故障安全主站与智能从站通讯接收）
- 为 DP partner (sender) 的 Address (LADDR) 输入 "2048"
- 为 Local (receiver) 的 Address (LADDR) 输入 "256"
- 接受对话框中其它参数的缺省值。

对话框将显示如下：



10. 单击“确定”(OK) 确认输入。
11. 在智能从站对象属性的“F 组态”(F-Configuration) 选项卡中，选择“新建”(New)。
12. 在下一个对话框中，针对我们的实例为至 DP 主站的发送连接输入以下内容：
 - 为 Mode 输入 "F-MS-R"（通过故障安全主站与智能从站通讯发送）
 - 为 DP partner (receiver) 的 Address (LADDR) 输入 "2060"
 - 为 Local (sender) 的 Address (LADDR) 输入 "268"
13. 单击“确定”(OK) 确认输入。
本实例中将会产生两条组态行：



说明

基于“F 组态”(F-Configuration) 选项卡中的组态，自动完成智能从站的对象属性中的“组态”(Configuration) 选项卡中的条目。不得修改这些条目。否则，将无法进行安全相关的主站与智能从站通讯。

可在“组态”(Configuration) 选项卡中获得在 DP 主站和智能从站中分配的地址区。

8.3 安全相关的主站与智能从站通讯

禁用智能从站的主动耦合

在禁用智能从站的“主动耦合”之前，必须在“F 组态”选项卡中删除到其它 F-CPU 或 F 模块的所有安全相关的通讯连接。

附加信息

可以在“F 组态”选项卡的内容相关的在线帮助中找到参数的说明。

有关主站与智能从站通讯的更多信息，请参考 *STEP 7 在线帮助*。

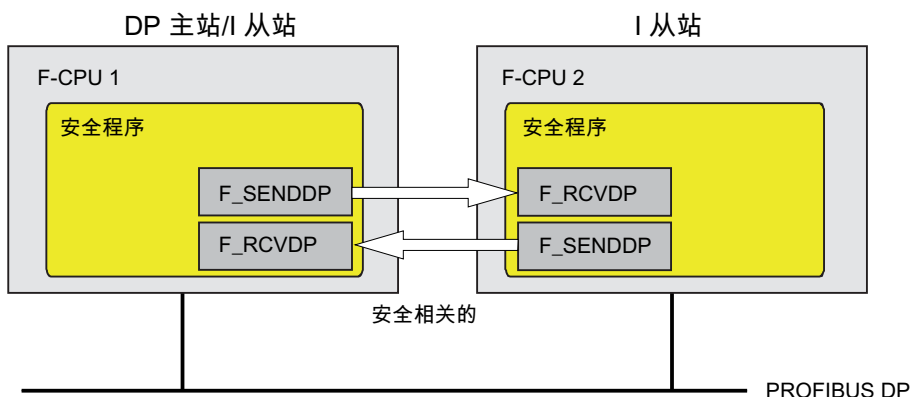
有关地址区、部分过程映像和支持的中断 OB 的信息，请参考所用 F-CPU 的技术规范。

8.3.3 通过 F_SENDDP 和 F_RCVDP 的通讯（安全相关的主站与智能从站通讯或智能从站与智能从站通讯）

引言

编写安全相关的主站与智能从站通讯或安全相关的智能从站与智能从站通讯程序的步骤与编写安全相关的主站与主站通讯程序的步骤相同。因此，以下仅介绍不同的地方。

通过 F_SENDDP 和 F_RCVDP 的通讯



对于 DP 主站和智能从站的 F-CPU 之间或若干智能从站的 F-CPU 之间的安全相关的通讯，可使用 F 应用程序块 F_SENDDP 进行发送，用 F_RCVDP 进行接收。可使用它们以故障安全方式传送固定数量的数据类型为 BOOL 和 INT 的故障安全数据。

可以在 *Distributed Safety F* 库 (V1) 中的 *F 应用程序块* 文件夹中找到这些 F 应用程序块。必须在 F-PB 开始时调用 F_RCVDP。必须在 F-PB 结束时调用 F_SENDDP。

请注意，仅当在相应 F 运行组执行结束时调用 F_SENDDP 之后，才会发送这些发送信号。

有关 F_SENDDP 和 F_RCVDP F 应用程序块的详细说明，请参考『FB 223“F_SENDDP”和 FB 224“F_RCVDP”：通过 PROFIBUS DP 发送和接收数据』一章。

将 F-CPU 分配给 F_SENDDP/F_RCVDP

按照以下说明将 F-CPU 分配给 F_SENDDP/F_RCVDP：

- 在 *HW Config* 中为 DP 主站和智能从站组态地址区（本地地址和伙伴地址）。
- 为 DP 主站 F-CPU 的安全程序中的主站与智能从站通讯指定以下地址：
 - 在输入参数 LADDR 的 F_SENDDP 处，指定发送的伙伴地址（“F 组态”选项卡：“行模式”(row Mode) “F-MS-R”）
 - 在输入参数 LADDR 的 F_RCVDP 处，指定接收的伙伴地址（“F 组态”选项卡：“行模式”(row Mode) “F-MS-S”）
- 为智能从站 F-CPU 的安全程序中的主站与智能从站通讯或智能从站与智能从站通讯指定以下地址：
 - 在输入参数 LADDR 的 F_SENDDP 处，指定发送的本地地址（“F 组态”选项卡：“行模式”(row Mode) “F-MS-S”或“F-DX-S”）
 - 在输入参数 LADDR 的 F_RCVDP 处，指定接收的本地地址（“F 组态”选项卡：“行模式”[row Mode]: “F-MS-R”或“F-DX-R”）

为每个涉及的 F-CPU 进行如上这些分配。

说明

因此，以下操作始终适用于安全相关的主站与智能从站通讯和智能从站与智能从站通讯：

- 在 DP 主站的 F_SENDDP/F_RCVDP 处，始终输入通讯连接的**伙伴地址**（从 *HW Config* 中智能从站的“F 通讯”（F-Communication）选项卡中）。
 - 在 DP 从站的 F_SENDDP/F_RCVDP 处，始终输入通讯连接的**本地地址**（从 *HW Config* 中智能从站的“F 通讯”（F-Communication）选项卡中）。
-

参见

编写安全相关的主站与主站通讯程序 (页 139)

FB 223“F_SENDDP”和 FB 224“F_RCVDP”：通过 PROFIBUS DP 发送和接收数据 (页 233)

8.3 安全相关的主站与智能从站通讯

8.3.4 编写安全相关的主站与智能从站通讯和智能从站与智能从站通讯程序

要求

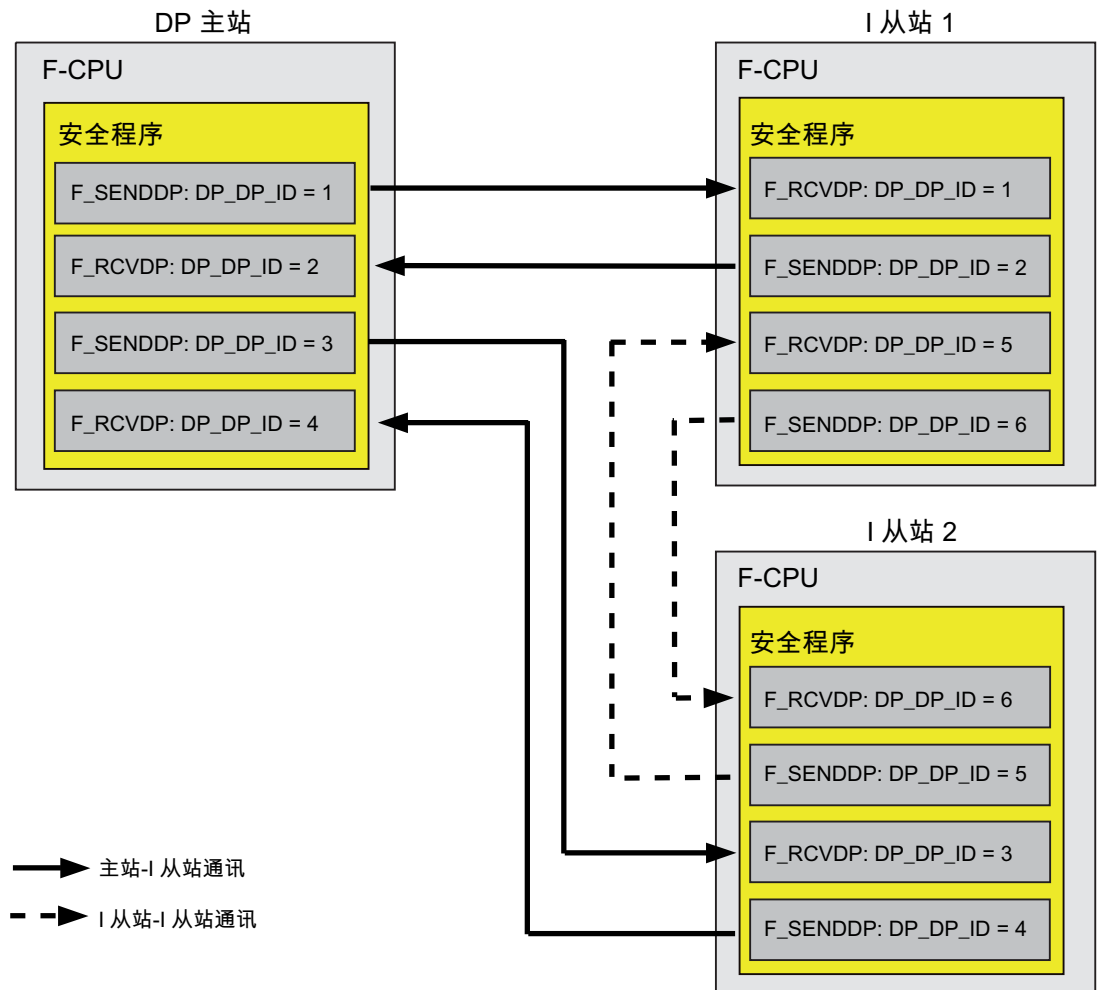
编程之前必须满足以下要求：

- 必须在 *HW Config* 中为 DP 主站和智能从站组态地址区（本地地址和伙伴地址）。
- 两个 CPU 都必须组态为 F-CPU：
 - 必须选中“CPU 包含安全程序”（CPU contains safety program）选项
 - 必须输入 F-CPU 的密码

编程步骤

编写安全相关的主站与智能从站通讯或智能从站与智能从站通讯程序的步骤与编写安全相关的主站与主站通讯程序的步骤相同。

下图包含一个实例，该实例说明了如何为两个安全相关的主站与智能从站通讯连接和一个智能从站与智能从站通讯连接指定 F 应用程序块 F_SENDDP 和 F_RCVDP 的输入处的地址关系。



警告

每个地址关联（输入参数 DP_DP_ID；数据类型：INT）的值都是用户定义的；但是，在网络中的所有安全相关的通讯连接中，它必须是唯一的。

说明


每次调用 F_SENDDP 或 F_RCVDP 时必须使用单独的实例 DP。

不得为 F_RCVDP 的输入和输出参数提供 F 程序块的本地数据。

如果一个实参已用于一个 F_RCVDP 调用或者另一个 F_RCVDP 或 F_RCVS7 调用的输入参数，则不得再将其用于同一 F_RCVDP 的输出参数。如果未遵守上述规定，F-CPU 会切换到 STOP。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

8.3 安全相关的主站与智能从站通讯

 警告
<p>如果与 F_SENDDP 关联的 F-CPU 处于取消激活安全模式下，则不能再假定接收自该 F-CPU 的数据是安全生成的。然后必须采取组织措施（例如操作监视和手动安全关闭），以确保这部分受接收数据影响的系统的安全。或者，必须通过评估 SENDMODE 来输出故障安全值，而不是输出 F-CPU 中通过 F_RCVDP 接收到的数据。</p>

参见

编写安全相关的主站与主站通讯程序 (页 139)

取消激活安全模式 (页 288)

8.3.5 数据传输的限制（安全相关的主站与智能从站通讯或智能从站与智能从站通讯）

数据传输的限制

如果要传送的数据量大于一对 F_SENDDP/F_RCVDP 块的容量，则可使用附加的 F_SENDDP/F_RCVDP 调用。为此还需组态附加通讯连接。请记住，在智能从站和 DP 主站之间传送的输入数据最大限制为 244 个字节，输出数据最大限制为 244 个字节。

下表显示了为安全相关的通讯连接分配的输出数据量和输入数据量：

安全相关的通讯	通讯连接	分配的输入和输出数据			
		在智能从站 1 和 DP 主站之间		在智能从站 2 和 DP 主站之间	
		输出数据	输入数据	输出数据	输入数据
主站与智能从站	发送：智能从站 1 发送到 DP 主站	12 个字节	6 个字节	-	-
	接收：智能从站 1 接收自 DP 主站	6 个字节	12 个字节	-	-
智能从站与智能从站	发送：智能从站 1 发送到智能从站 2	12 个字节	-	6 个字节	-
	接收：智能从站 1 接收自智能从站 2	6 个字节	-	12 个字节	-

如果需要，还应考虑标准用户程序中的故障安全智能从站与智能从站通讯（**F-DX-Module**）、主站与从站连接（**MS**）或用于交换数据的直接数据交换连接（**DX**），它们将是智能从站和 DP 主站之间传输的输入数据和输出数据的最大限制（均为 244 个字节）的一部分。

可以在智能从站对象属性中的“组态”(Configuration) 选项卡中，检查所有已组态的安全相关通讯和标准通讯连接是否位于输入数据和输出数据的最大限制（均为 244 个字节）内。“组态”(Configuration) 选项卡中包含所有“模式”(MODE) 为“MS”的行。但不包含“模式”(MODE) 为“DX”的行。

8.4 安全相关的智能从站与智能从站通讯

8.4.1 组态地址区（安全相关的智能从站与智能从站通讯）

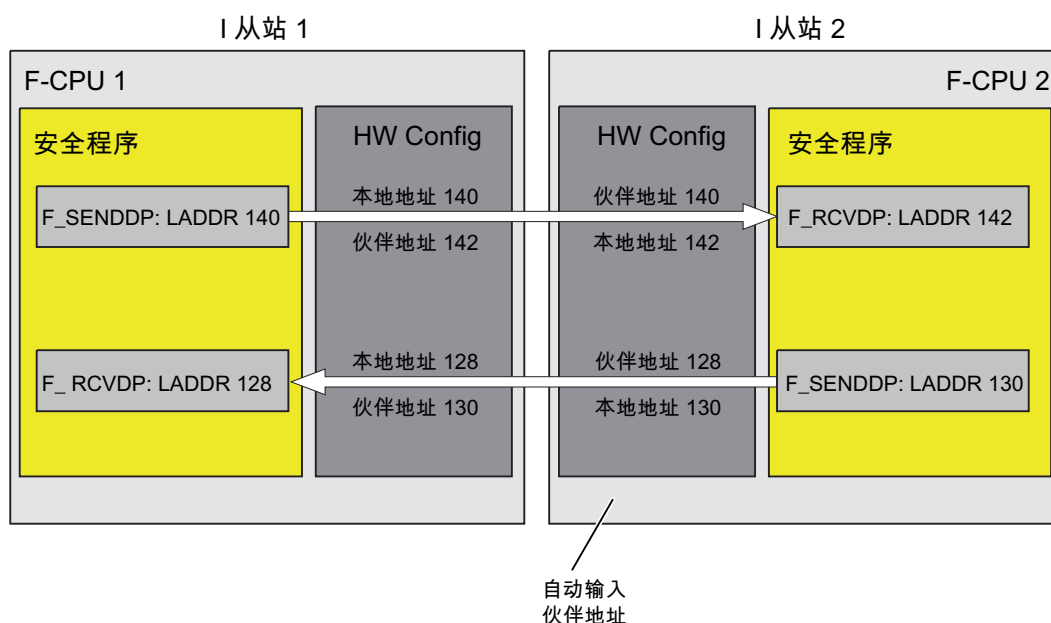
引言

智能从站 F-CPU 的安全程序之间使用直接数据交换进行安全相关的通讯（这与在标准程序中相同）。

智能从站与智能从站通讯不需要任何其它硬件。

组态地址区

必须在 *HW Config* 中为两个 F-CPU 之间的每个通讯连接组态地址区。下图中，两个 F-CPU 中的任何一个都可以发送和接收数据（双向通讯）。



在智能从站 1 的对象属性中组态以下地址：

- 发送到智能从站 2 时，组态本地地址（智能从站 1）和伙伴地址（智能从站 2）
- 自智能从站 2 接收数据时，组态本地地址（智能从站 1）和伙伴地址（智能从站 2）

无需再在智能从站 2 的对象属性中组态通讯。地址将自动输入到智能从站 2 的对象属性中。

在安全程序中将组态的地址分配给相应 F_SENDDP 和 F_RCVDPF 应用程序块的 LADDR 参数。

分配的地址区

每个本地地址和伙伴地址均代表输入和输出数据的地址区的起始地址。一旦组态了本地地址和伙伴地址，将自动分配地址区。下表中列出了分配给发送连接和接收连接的地址区：

通讯连接的 F-CPU* 中分配的地址区
发送： 智能从站 1 发送到智能从站 2	智能从站 1： 12 个字节的输出数据和 6 个字节的输入数据
	智能从站 2： 12 个字节的输入数据和 6 个字节的输出数据
	DP 主站： 12 + 6 个字节的输入数据
接收： 智能从站 1 接收自智能从站 2	智能从站 1： 12 个字节的输入数据和 6 个字节的输出数据
	智能从站 2： 12 个字节的输出数据和 6 个字节的输入数据
	DP 主站： 12 + 6 个字节的输入数据
*DP 主站的 CPU 可以是 F-CPU，也可以是标准 CPU。可以在相关 CPU 的信息文本（在 <i>HW Config</i> 的硬件目录中）中了解标准 CPU 的 PROFIBUS DP 接口是否支持直接数据交换。	

说明

由于应为模块的地址区保留过程映像，我们建议使用过程映像以外的地址作为本地地址和伙伴地址。

8.4.2 组态安全相关的智能从站与智能从站通讯

要求

已在 *STEP 7* 中创建了一个项目。

组态智能从站与智能从站通讯的操作步骤（以下实例为双向通讯）

1. 在项目中创建一个站（例如在 *SIMATIC 管理器* 中创建一个 S7-300 站）。
2. 为该站分配一个 F-CPU（从 *HW Config* 中的硬件目录中）。
3. 将该 CPU 组态为 DP 从站（在 *HW Config* 中 CPU 的 DP 接口的对象属性的“工作模式”[*Operating Mode*] 选项卡中）。
4. 请按照步骤 1 到 3 组态另一个 DP 从站（智能从站）。
5. 创建另一个站，然后分配一个 F-CPU（请参阅步骤 1 和 2）。
6. 将该 CPU 组态为 DP 主站（在 *HW Config* 中 CPU 的 DP 接口的对象属性的“工作模式”[*Operating Mode*] 选项卡中）。

注意：DP 主站的 CPU 可以是 F-CPU，也可以是标准 CPU。

7. 在“已组态的站”（*Configured stations*）下的硬件目录中，为一个智能从站选择站类型（例如“CPU 31x”），然后将其放置在 DP 主站系统上。
8. 在自动打开的“连接”（*Connection*）对话框中，将智能从站链接至 DP 主站。
9. 完成步骤 7 和 8 后，将第二个智能从站链接至 DP 主站。

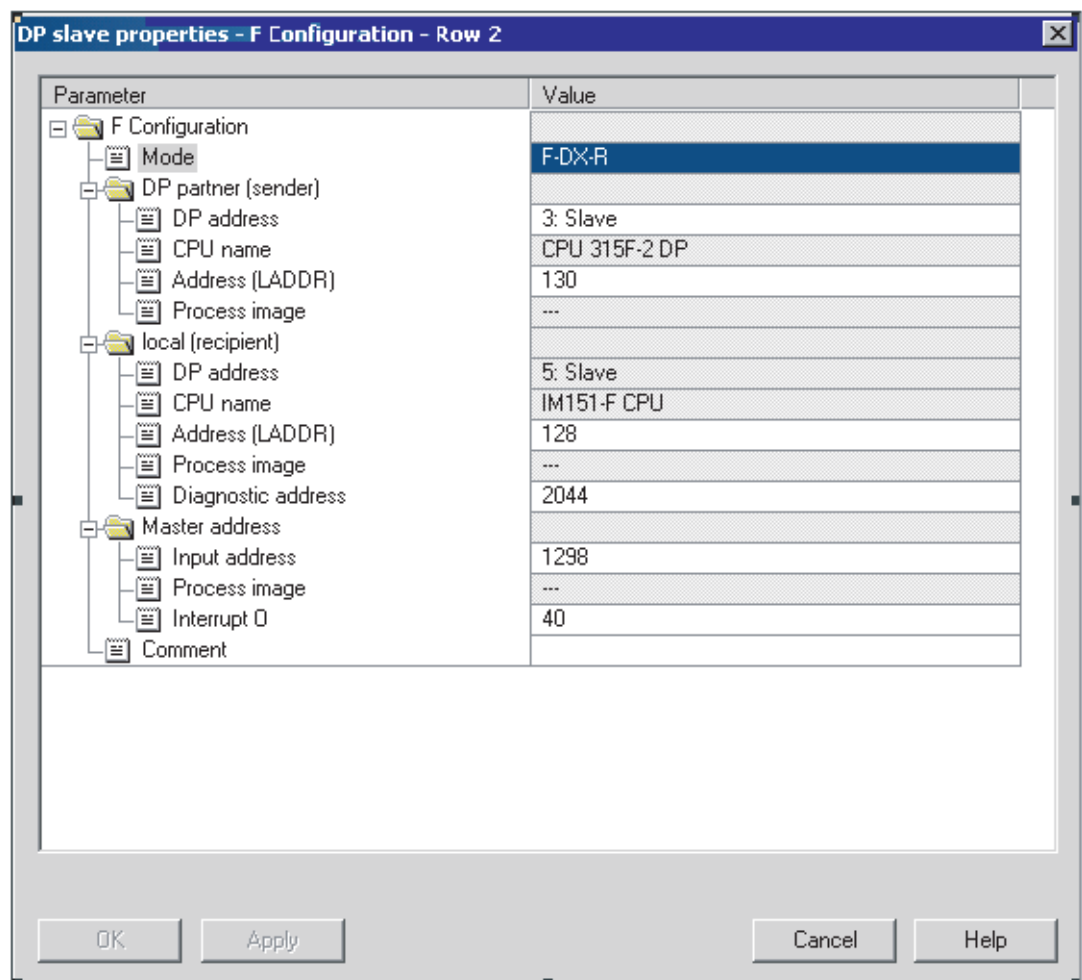
现在可以为安全相关的智能从站与智能从站通讯定义地址区：

10. 在智能从站 1 的对象属性的“F 组态”（*F-Configuration*）选项卡中，选择“新建”（*New*）。

11. 在下一个对话框中，为来自智能从站 2 的接收连接输入以下内容（对于我们的实例）：

- 为 Mode 输入 "F-MS-R"（通过故障安全智能从站与智能从站通讯接收）
- 为 DP partner (sender) 的 DP address 输入 "5: Slave"（PROFIBUS 地址）；为 Address (LADDR) 输入 "130"
- 为 Local (receiver) 的 Address (LADDR) 输入 "128"
- 接受对话框中其它参数的缺省值。

对话框将显示如下：

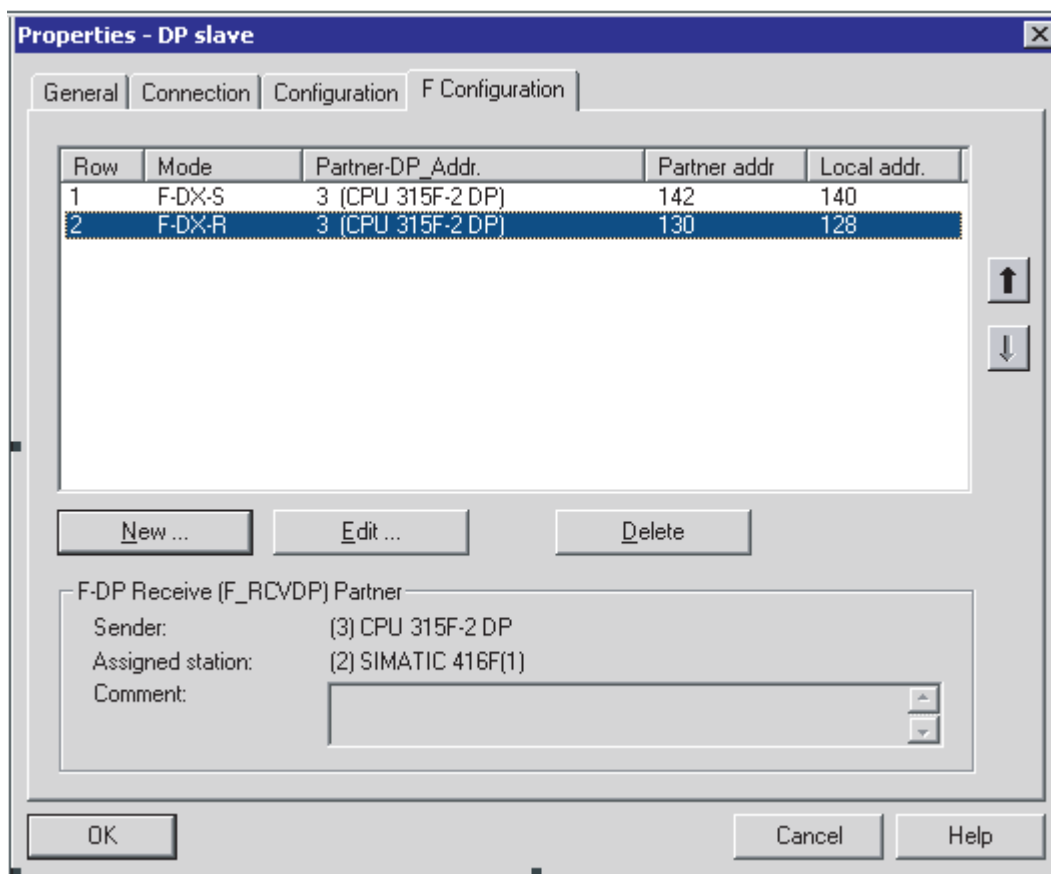


12. 单击“确定”(OK) 确认输入。

13. 在智能从站 1 的对象属性的“F 组态” (F-Configuration) 选项卡中，选择“新建”(New)。

8.4 安全相关的智能从站与智能从站通讯

- 14. 在下一个对话框中，为至智能从站 2 的发送连接输入以下内容（对于我们的实例）：
 - 为 Mode 输入 "F-DX-S"（通过故障安全智能从站与智能从站通讯发送）
 - 为 DP partner (receiver) 的 DP address 输入 "5: Slave"; 为 Address (LADDR) 输入 "142"
 - 为 Local (sender) 的 Address (LADDR) 输入 "140"
 - 接受对话框中其它参数的缺省值。
- 15. 单击“确定”(OK) 确认输入。
本实例中将会产生两条组态行：



说明

基于“F 组态” (F-Configuration) 选项卡中的组态，自动对各个智能从站对象属性中的“组态”(Configuration) 选项卡进行输入。不得修改这些条目。否则，将无法进行安全相关的智能从站与智能从站通讯。

可

在“组态”(Configuration) 选项卡中获得在 DP 主站和智能从站中分配的地址区。

禁用智能从站的主动耦合

在禁用智能从站的“主动耦合”之前，必须在“F 组态” (F-Configuration) 选项卡中删除到其它 F-CPU 或 F 模块的所有安全相关的通讯连接。

附加信息

可以在“F 组态” (F-Configuration) 选项卡的内容相关的在线帮助中找到参数的说明。

有关地址区、部分过程映像和支持的中断 OB 的信息，请参考所用 CPU 的技术规范。

8.4.3 通过 F_SENDDP 和 F_RCVDP 进行通讯（安全相关的智能从站与智能从站通讯）

参考

有关说明，请参考『通过 F_SENDDP 和 F_RCVDP 进行通讯（安全相关的主站与智能从站/智能从站与智能从站通讯）』一章。

8.4.4 编写安全相关的智能从站与智能从站通讯的程序

参考

有关说明，请参考『编写安全相关的主站与智能从站/智能从站与智能从站通讯的程序』一章。

8.4.5 数据传输的限制（安全相关的智能从站与智能从站通讯）

数据传输的限制

有关说明，请参考『数据传输（安全相关的主站与智能从站/智能从站与智能从站通讯）的限制』一章。

8.5 安全相关的智能从站与从站通讯

8.5.1 组态地址区（安全相关的智能从站与从站通讯）

引言

在智能从站的 F-CPU 和 DP 从站中的 F-I/O 的安全程序之间使用直接数据交换进行安全相关的通讯（与在标准程序中一样）。按照『F-I/O 访问』一章所述通过过程映象（PII 和 PAA）访问 F-I/O（在智能从站 F-CPU 的安全程序中）的通道。

对于通过安全相关的智能从站与智能从站通讯进行的 F-I/O 访问，在 *HW Config* 中编译程序时，F-CPU 的安全程序中将自动生成 F-I/O DB。

智能从站与从站通讯不需要任何其它硬件。

限制

说明

安全相关的智能从站与从站通讯可以通过 DP 从站（支持安全相关的智能从站与从站通讯）中的 F-I/O 来执行，例如，通过所有 ET 200S F 模块和通过所有 S7-300 故障安全信号模块（具有 IM 153-2，订货号 6ES7 153-2BA01-0XB0 或更高，固件版本高于 V4.0.0）。

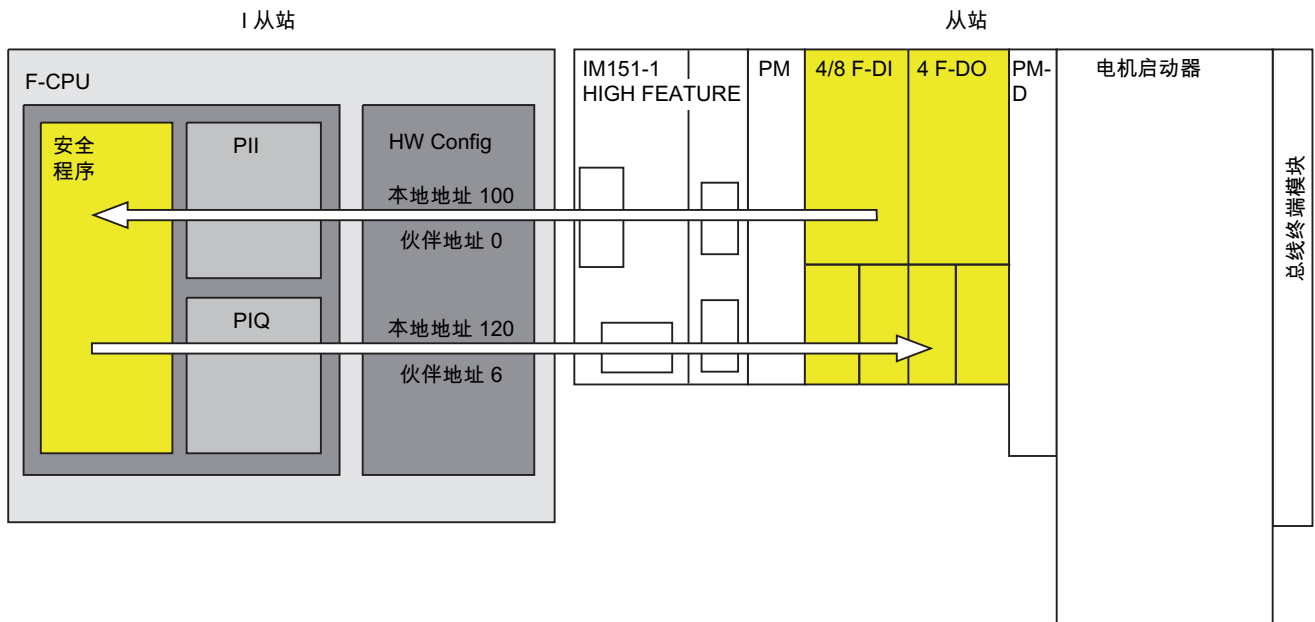
说明

通过安全相关的智能从站与从站通讯，确保先对 DP 主站的 CPU 通电，再对智能从站的 F-CPU 通电。

否则，根据为 F-I/O 指定的 F 监视时间，F 系统可能会在 F-CPU 和分配到智能从站的 F-I/O 之间的安全相关的通讯中检测到错误（通讯错误）。即，在启动 F 系统之后，将不会自动重新集成 F-I/O。确切地说，仅在使用 F-I/O DB 的变量 ACK_REI 上的上升沿执行用户确认后，才可重新集成 F-I/O（请参阅『在发生通讯错误后钝化和重新集成 F-I/O』和『在 F 系统启动后钝化和重新集成 F-I/O』两章）。

组态地址区

对于从智能从站的 F-CPU 到从站中的 F-I/O 的每个通讯连接，必须在 *HW Config* 中组态地址区。下图显示了具有 F-DI 和 F-DO 模块的 ET 200S 的实例。



可在智能从站的对象属性中为每个通过 F-IO 进行的智能从站与从站通讯组态以下内容：

- 可用于访问在智能从站的安全程序中的 F-I/O 的本地地址（安全程序）
- DP 主站中的 F-I/O 的伙伴地址 (F-I/O)

对于 DP 从站和 DP 主站的 F-I/O，不必在对象属性中组态通讯。

分配的地址区

每个本地地址和伙伴地址均代表输入和输出数据的地址区的起始地址。组态了本地地址和伙伴地址之后，将自动分配地址区。针对 ET 200S 的 4/8F-DI 和 4 F-DO，下表显示了为通过 F-I/O 进行的智能从站与智能从站通讯所分配的地址区的实例：

通讯连接	在.....中分配的地址区 *
具有 4/8 F-DI 的智能从站与智能从站通讯	智能从站的 F-CPU： 6 个字节的输入数据和 4 个字节的输出数据
	DP 主站的 F-CPU**： 6 + 4 个字节的输入数据

通讯连接	在.....中分配的地址区 *
具有 4 F-DO 的智能从站 与智能从站通讯	智能从站的 F-CPU: 5 个字节的输出数据和 5 个字节的输入数据
	DP 主站的 F-CPU**: 5 + 5 个字节的输入数据
* 有关 ET 200S 的 4/8 F-DI 和 4 F-DO 的实例（要了解具体地址关系，请参阅 F-I/O 手册）	
** DP 主站的 CPU 可以是 F-CPU，也可以是标准 CPU。可以在相关 CPU 的信息文本（在 <i>HW Config</i> 的硬件目录中）中了解标准 CPU 的 PROFIBUS DP 接口是否支持直接数据交换。	

说明

由于要与真正的 F-I/O 进行通讯，因此必须使用本地地址过程映象中的地址。

8.5.2 组态安全相关的智能从站与从站通讯

要求

已在 *STEP 7* 中创建了一个项目。

组态智能从站与从站通讯的操作步骤

在本节中，我们将示范如何组态上图的地址区。

1. 在项目中创建一个站（例如在 *SIMATIC 管理器* 中创建一个 S7-300 站）。
2. 为该站分配一个 F-CPU（从 *HW Config* 中的硬件目录中）。
3. 将该 CPU 组态为 DP 从站（在 *HW Config* 中 CPU 的 DP 接口的对象属性的“工作模式”[Operating Mode] 选项卡中）。
4. 创建另一个站，并分配一个标准 CPU 或 F-CPU（请参阅第 1 步和第 2 步）。
5. 将该 CPU 组态为 DP 主站（在 *HW Config* 中 CPU 的 DP 接口的对象属性的“工作模式”[Operating Mode] 选项卡中）。
6. 在硬件目录中选择 IM 151 HIGH FEATURE，订货号为 6ES7 151-1BA01-0AB0 或更高，并且将其放置在 DP 主站系统上。
7. 使用拖放操作为 IM 分配电源模块、4/8 F-DI 模块和 4 F-DO 模块。

8. 在“已组态的站”（**Configured stations**）下的硬件目录中，选择智能从站的站类型（例如“**CPU 31x**”）并将其放置在 DP 主站系统上。
9. 在自动打开的“连接”（**Connection**）对话框中，将智能从站链接至 DP 主站。

现在可以为安全相关的智能从站与从站通讯定义 F-I/O:

10. 在智能从站对象属性的“F 组态”（**F-Configuration**）选项卡中，选择“新建”(New)。
11. 对于我们的实例，在下一个对话框中，将以下条目用于至 4/8 F-DI 模块的连接:

- 为 **Mode** 输入 "F-DX-Module"（故障安全智能从站与从站通讯）
- 为 **DP partner (F-I/O)** 的
DP address 输入 "1: Slave"（具有 F-I/O 的从站的 PROFIBUS 地址）；
为 **Address (LADDR)** 输入 "0: 4/8 F-DI"（F-I/O 的起始地址）
- 为 **Local (safety program)** 的 **Address (LADDR)** 输入 "100"（通过 F-I/O 起始地址在智能从站的 F-CPU 的安全程序中进行访问）
- 接受对话框中其它参数的缺省值。

说明

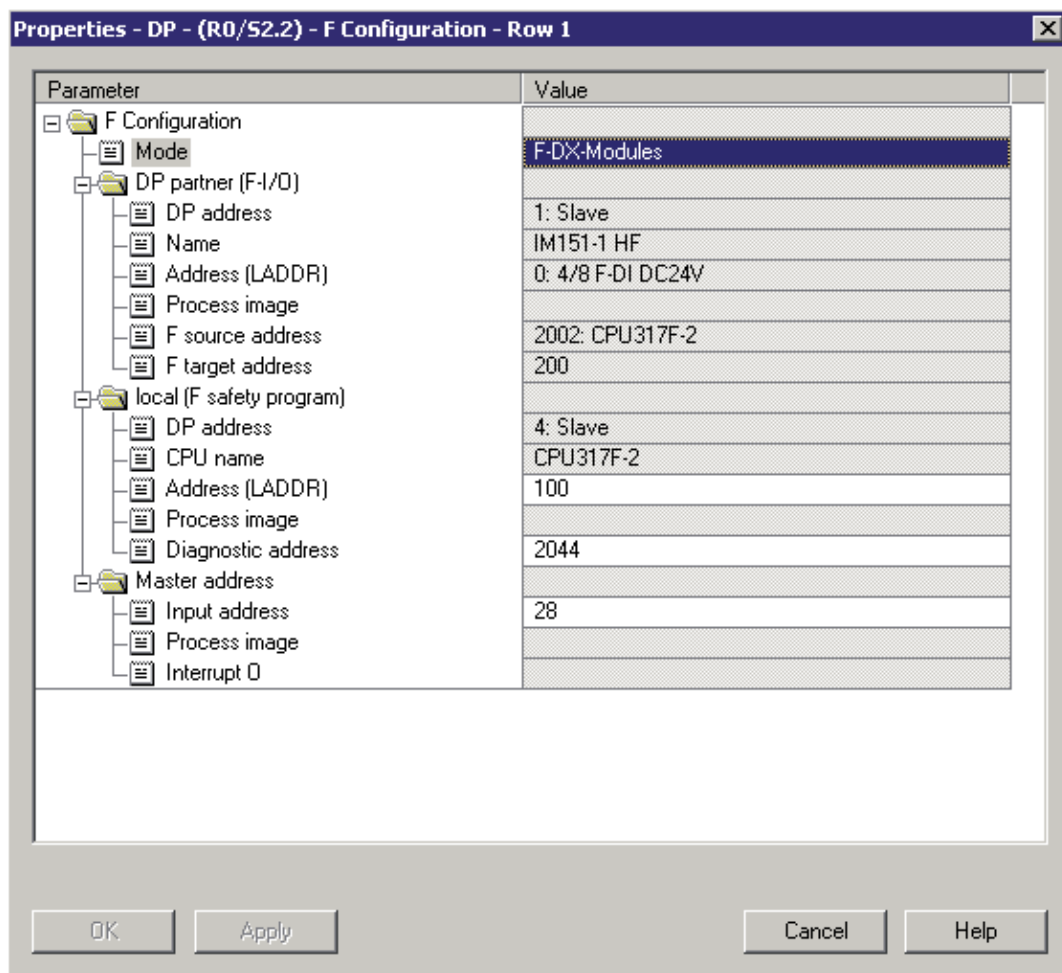
"DP partner (F-I/O)"

对于 "DP address", 列表域将显示可能的 DP 从站（支持安全相关的智能从站与从站通讯）的 PROFIBUS 地址。从该列表中选择所需的 DP 从站。

但是，请注意，该列表可能包括未分配到包含智能从站的 DP 主站系统的 DP 从站。不得选择这些从站。

对于"Address (LADDR)", 列表域将显示选定的 DP 从站的 F-I/O 的起始地址。从该列表中选择所需的 F-I/O。

对话框将显示如下：



12. 单击“确定”(OK) 确认输入。

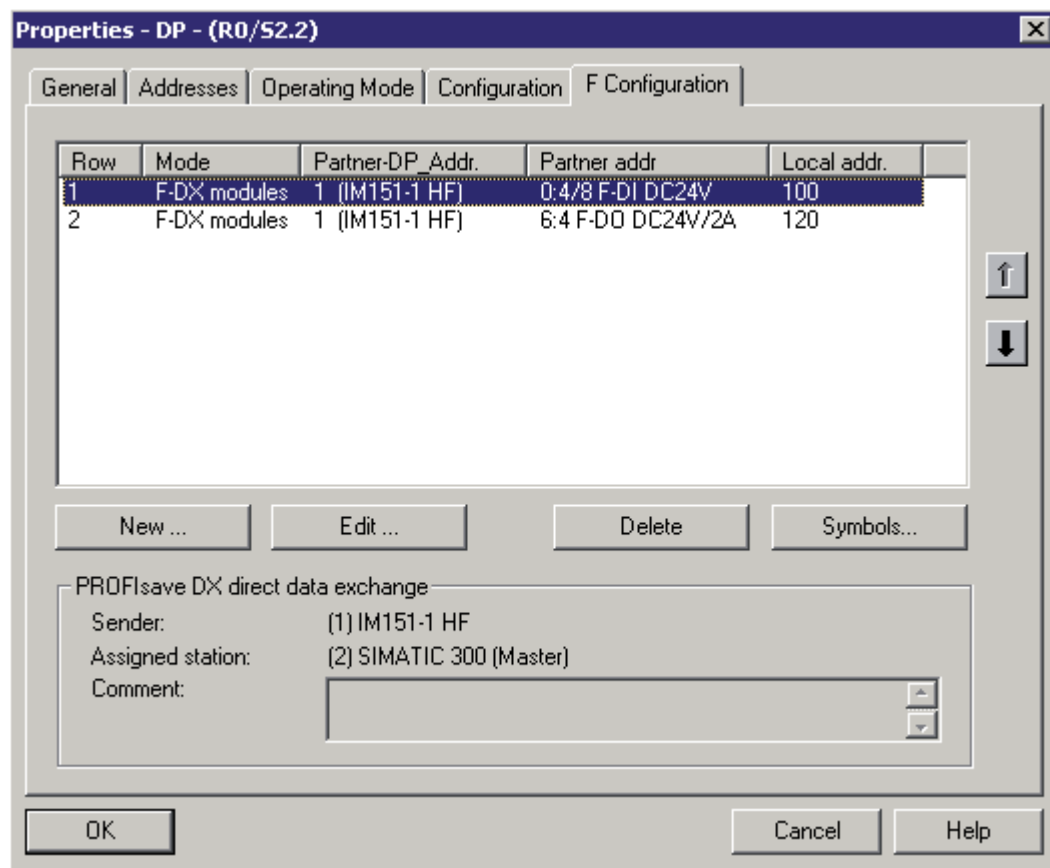
13. 在智能从站对象属性的“F 组态” (F-Configuration)选项卡中，选择“新建”(New)。

14. 对于我们的实例，在下一个对话框中，将以下条目用于至 4 F-DO 模块的连接：

- 为 Mode 输入 "F-DX-Module"（故障安全智能从站与从站通讯）
- 为 DP partner (F-I/O) 的
DP address 输入 "1: Slave"（具有 F-IO 的从站的 PROFIBUS 地址）；
为 Address (LADDR) 输入 "6: 4 F-DO"（F-I/O 的起始地址）
- 为 Local (safety program) 的 Address (LADDR) 输入 "120"（通过 F-I/O 起始地址在智能从站的 F-CPU 的安全程序中进行访问）
- 接受对话框中其它参数的缺省值。

15. 单击“确定”(OK) 确认输入。

本实例中将会产生两条组态行：



说明

基于“F 组态”(F-Configuration) 选项卡中的组态，自动完成智能从站的对象属性中的“组态”(Configuration) 选项卡中的条目。不得修改这些条目。否则，将无法使用安全相关的智能从站与从站通讯。

可在“组态”(Configuration) 选项卡中获得在 DP 主站和智能从站中分配的地址区。

智能从站与从站通讯组态中的更改

警告

如果已为 F-I/O 组态新的智能从站与从站通讯或已删除现有的智能从站与从站通讯，则必须保存并编译 DP 主站的站硬件配置以及智能从站的站硬件配置，并且将其下载到 DP 主站或智能从站的站。

智能从站的 F-CPU 安全程序和 DP 主站的 F-CPU 安全程序（如果也存在安全程序）的集体签名都设置为“0”。然后必须重新编译安全程序。

8.5 安全相关的智能从站与从站通讯

禁用智能从站的主动耦合

在禁用智能从站的“主动耦合”之前，必须在“F 组态” (F-Configuration) 选项卡中删除到其它 F-CPU 或 F 模块的所有安全相关的通讯连接。

附加信息

可以在“F 组态” (F-Configuration) 选项卡的内容相关在线帮助中找到参数说明。

有关地址区、过程映像和支持的中断 OB 的信息，请参考您所使用的 CPU 的技术规范。

8.5.3 对安全相关的智能从站与从站通讯进行 F-I/O 访问

通过过程映像进行访问

在安全相关的智能从站与从站通讯中，使用过程映像 (PII 或 PIQ) 访问智能从站的 F-CPU 安全程序中的 F-I/O。这与到直接分配给智能从站的 F-I/O 的 F-I/O 访问相同。在智能从站中，通过 F-Configuration 选项卡中为 Local (safety program) 的 Address (LADDR) 组态的起始地址来引用 F-I/O。不允许直接访问 I/O。只能从一个 F 运行组访问 F-I/O 的通道。



警告

由于此特殊安全协议，F-I/O 占用的过程映像区域比 F-I/O 上实际存在的通道需要的区域大。要找出存储通道（用户数据）的过程映像区域，请参考 F-I/O 的相关手册。在安全程序中访问过程映像时，仅允许访问实际存在的通道。

请注意，对于某些 F-I/O（例如，S7-300 F-SM 和 ET 200S 故障安全模块），可以指定“传感器的 1oo2 评估”。要了解可在安全程序中访问哪些由“传感器的 1oo2 评估”组成的通道，请参考 F-I/O 的相关手册。

参见

F-I/O 访问 (页 101)

8.5.4 数据传输的限制（安全相关的智能从站与从站通讯）

数据传输的限制

请注意，智能从站和 DP 主站之间传输的最大限制为输入数据 244 个字节和输出数据 244 个字节。

对于 ET 200S 的 4/8 F-DI 和 4 F-DO，为安全相关的通讯分配的输出和输入数据数量的实例显示在下表中：

安全相关的通讯	通讯连接	已分配的输入和输出数据*	
		智能从站和 DP 主站之间	
		智能从站中的输出数据	智能从站中的输入数据
智能从站与从站	具有 4/8 F-DI 的智能从站与从站通讯	4 个字节	6 个字节
	具有 4 F-DO 的智能从站与从站通讯	5 个字节	5 个字节
* ET 200S 的 4/8 F-DI 和 4 F-DO 的实例			

如有必要，也应考虑故障安全主站与智能从站通讯（F-MS-R、F-MS-S）和主站与从站连接（MS）或者

将直接数据交换连接（DX）用于在标准用户程序中交换数据，将这些作为智能从站和 DP 主站之间传输的最大限制（输入数据 244 个字节和输出数据 244 个字节）的一部分。

可以在智能从站对象属性中的“组态”(Configuration) 选项卡中，检查所有已组态的安全相关通讯和标准通讯连接是否位于输入数据和输出数据的最大限制（均为 244 个字节）内。“组态”(Configuration) 选项卡中包含所有“模式”(MODE) 为“MS”的行。但不包含“模式”(MODE) 为“DX”的行。

8.6 安全相关的 IO 控制器与 IO 控制器通讯

要求

IO 控制器的 F-CPU 的安全程序之间的安全相关的通讯，在安装在 F-CPU 之间的 PN/PN 耦合器（订货号 6ES7158-3AD00-0XA0）上进行。

对于该通讯，您将需要 STEP 7 V5.4 SP1 的 HSP 101 或 PN/PN 耦合器的 GSD 文件。

如果 CPU 416F 不具有集成的 PROFINET 接口，则请使用 CP 443-1 Advanced。

说明

在 PN/PN 耦合器（在 *HW Config* 中）的对象属性中禁用“数据有效性指示灯 DIA”(Data validity indicator DIA)（与缺省设置相同）。否则，将无法进行安全相关的 IO 控制器与 IO 控制器通讯。

参考

此外，『安全相关的主站与主站通讯』一章中有关安全相关的主站与主站通讯的信息也适用。

8.7 通过 S7 连接进行安全相关的通讯

8.7.1 用 S7 连接组态安全相关的通讯

引言

与在标准程序中相同，F-CPU 安全程序之间通过 S7 连接的安全相关的通讯是通过 *NetPro* 中的连接表进行的。

限制

说明

在 S7 Distributed Safety 中，通常仅允许在工业以太网上使用 S7 连接！

可与以下 CPU 通过 S7 连接进行安全相关的通讯：

- CPU 315F-2 PN/DP（仅通过 CPU PN 接口）
 - CPU 317F-2 PN/DP（仅通过 CPU PN 接口）
 - CPU 416F-3 PN/DP（仅通过 CPU PN 接口）
 - CPU 416F-2 固件版本 V4.0 及更高版本
-

在连接表中创建 S7 连接

对于两个 F-CPU 之间的每个连接，必须在 *NetPro* 中的连接表中创建一个 S7 连接。

STEP 7 为每个连接端点分配一个本地 ID 和一个伙伴 ID。如有必要，可以在 *NetPro* 中更改本地 ID。为安全程序中相应 F 应用程序块的 ID 参数分配本地 ID。

说明

不能将通过 S7 连接的安全相关的通讯连接至未指定的伙伴。

组态 S7 连接的操作步骤

按照与标准系统组态一样的方式，为安全相关的 CPU 与 CPU 通讯组态 S7 连接。

说明

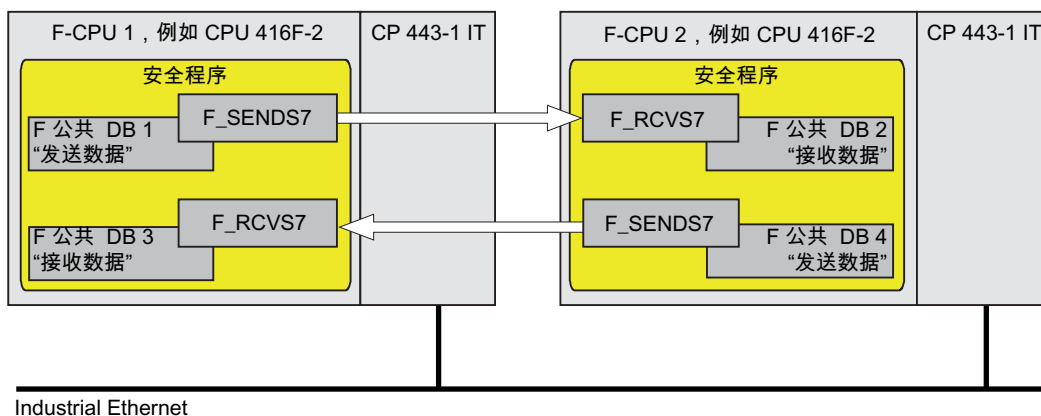
如果更改安全相关的通讯的 S7 连接的组态，则安全程序的集体签名被设置为“0”。然后必须重新编译安全程序。

附加信息

有关组态 S7 连接的说明，请参考『使用 *STEP 7 V5.x* 配置硬件和通讯连接』和 *STEP 7* 在线帮助。

8.7.2 通过 F_SENDS7、F_RCVS7 和 F-Communication DB 进行通讯

通过 F_SENDS7 和 F_RCVS7 进行通讯



使用 **F_SENDS7** 和 **F_RCVS7** F 应用程序块，通过 S7 连接进行故障安全数据的发送和接收。

可以以故障安全方式使用这些 F 应用程序块发送指定数量的 **BOOL**、**INT**、**WORD** 和 **TIME** 数据类型的故障安全数据。故障安全数据存储于创建的 F-DB 中。

可以在 *Distributed Safety* F 库 (V1) 中 *F 应用程序块* 的块文件夹中找到这些 F 应用程序块。必须在 F-PB 开始时调用 **F_RCVS7**。必须在 F-PB 结束时调用 **F_SENDS7**。

请注意，仅当在执行相关的 F 运行组结束时调用 **F_SENDS7** 之后，才会发送这些发送信号。

有关 F 应用程序块的详细说明，请参考『FB 225“F_SENDS7”、FB 226“F_RCVS7”：通过 S7 连接进行通讯』一章。

F 通讯 DB

对于每个连接，发送数据存储于 F-DB (F 通讯 DBx) 中，而每个接收数据存储于 F-DB (F 通讯 DBy) 中。

可以将 F 通讯 DB 编号作为参数用于 **F_SENDS7** 或 **F_RCVS7**。

参见

FB 225 "F_SENDS7" 和 FB 226 "F_RCVS7": 通过 S7 连接通讯 (页 240)

8.7.3 对通过 S7 连接进行的安全相关的通讯编程

引言

本节介绍了如何对通过 S7 连接在 F-CPU 安全程序之间进行的安全相关的通讯进行编程。必须在相关 F-CPU 的安全程序中执行以下操作：

- 创建在其中存储通讯的发送数据或接收数据的 F-DB
- 从安全程序的 *Distributed Safety* F-Library (V1) 中为通讯的 F 应用程序块调用和分配参数。

编程要求

编程之前必须满足以下要求：

- 必须在 *NetPro* 中组态相关 F-CPU 之间的 S7 连接
- 两个 CPU 都必须组态为 F-CPU：
 - 必须选中“CPU 包含安全程序” (CPU contains safety program) 选项
 - 必须输入 F-CPU 的密码

创建并编辑 F 通讯 DB

在 *SIMATIC 管理器* 中创建和编辑 F 通讯 DB 的方式与创建和编辑其它 F-DB 的方式相同。

创建 F 通讯 DB 时请注意以下事项：

创建 F-DB 时，在 F-DB 的对象属性“常规 - 第 2 部分” (General - Part 2) 选项卡中的“系列” (Family) 域中分配“COM_DB_S7”标识符。该标识符将 F-DB 指定为 F 通讯 DB。只有具有该标识符的 F-DB 才可作为 F 通讯 DB 传送至 F_SENDS7 或 F_RCVS7。为 F 通讯 DB 分配符号名。

说明

接收方 F 通讯 DB 的长度和结构必须匹配对应发送方 F 通讯 DB 的长度和结构。

如果 F 通讯 DB 不匹配，则 F-CPU 可能切换到 STOP 模式。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

因此，建议使用以下操作步骤：

1. 在 *SIMATIC 管理器* 中发送方离线安全程序的块文件夹中创建 F 通讯 DB。
 2. 指定合适的 F 通讯 DB 结构，考虑到要发送的数据。
 3. 将此 F 通讯 DB 复制到接收方的离线安全程序块文件夹中，必要的话可以更改 DB 编号。
-

F 通讯 DB 的其它要求

F 通讯 DB 也必须符合以下属性。

- 不允许它们成为背景数据块。
- 它们的长度不允许超出 100 个字节。
- 在 F 通讯 DB 中，只允许声明数据类型 BOOL、INT、WORD 和 TIME。
- 数据类型必须按以下顺序逐块排列：BOOL、INT、WORD 和 TIME。在 F 通讯 DB 中每个数据类型只允许使用一个块。
- 对于数据类型 BOOL，只允许声明不超过 128 个数据元素。
- 数据类型 BOOL 的数据量必须始终为 16 的整数倍（字限制）。如有必要，必须添加保留数据。

如果未满足这些标准，*S7 Distributed Safety* 将输出出错消息。

分配故障安全值

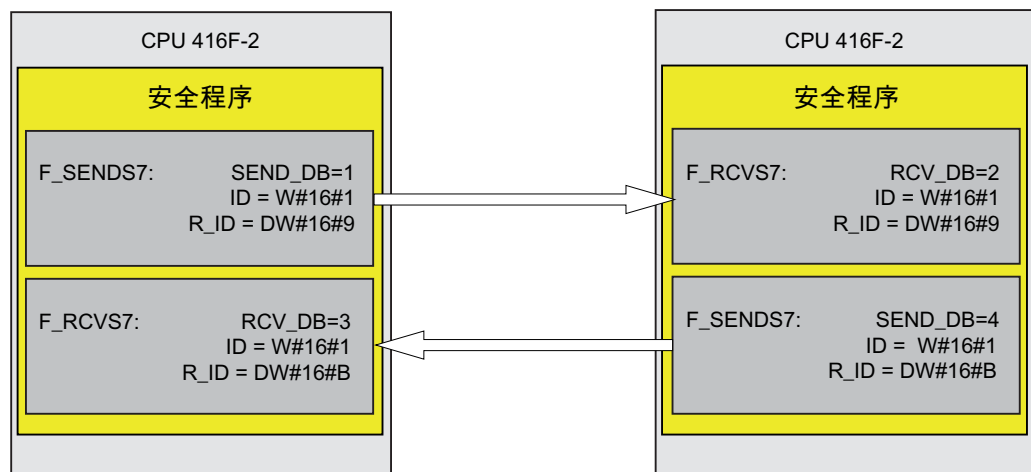
在接收方，下列情况下使用故障安全值：

- 启动 F 系统后首次建立通讯伙伴之间的连接时
- 发生通讯错误时

在接收方 F 通讯 DB 中指定的值可用作故障安全值（F 通讯 DB 的缺省值）。

编程步骤

1. 在发送方的 F 通讯 DB 中提供变量，同时该发送方使用具有完整资格的符号化访问（例如“F 通讯 DB 的名称”、“变量名称”）发送信号。
2. 在接收方（接收信号）的 F 通讯 DB 中读取变量，这是要使用具有完整资格的符号化访问（例如“F 通讯 DB 的名称”、“变量名称”）在程序的其它部分中进行进一步处理的变量。
3. 在要发送数据的安全程序中，在 F-PB 结束时调用 F_SENDS7 F 应用程序块以进行发送。
4. 在要接收数据的安全程序中，在 F-PB 开始时调用 F_RCVS7 F 应用程序块以进行发送。
5. 将适用的 F 通讯 DB 编号分配至 F_SENDS7 的 SEND_DB 输入和 F_RCVS7 的 RCV_DB 输入。
6. 将在 *NetPro* 中组态的 S7 连接的本地 ID（数据类型：WORD）分配至 F_SENDS7 的输入 ID。
7. 将在 *HW Config* 中组态的 S7 连接的本地 ID（数据类型：WORD）分配到 F_RCVS7 的输入 ID。
8. 将一个奇数（数据类型：DWORD）分配到 F_SENDS7 和 F_RCVS7 的 R_ID 输入。这样将指定 F_SENDS7 和 F_RCVS7 合成一个整体。相关的 F 块有相同的 R_ID。



警告

每个地址关联（输入参数 R_ID；数据类型：DWORD）的值都是用户定义的；但是，在网络中的所有安全相关的通讯连接中，它必须是唯一的。值 R_ID + 1 是内部分配的并且不得使用。

说明

每次调用 F_SENDS7 和 F_RCVS7 时必须使用单独的实例 DP。

不得为 F_RCVS7 的输入和输出参数提供 F 程序块的本地数据。

如果已经为 F_RCVS7 或者其它 F_RCVS7 或 F_RCVDP 调用的输入参数使用实参，则不得为相同的 F_RCVS7 的输出参数使用该实参。如果未遵守上述规定，F-CPU 会切换到 STOP。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

9. 使用要求的监视时间组态 F_SENDS7 和 F_RCVS7 的 TIMEOUT 输入。

**警告**

这样可以确保（从故障安全角度出发）仅当信号待决的时间不少于分配的监视时间（TIMEOUT）时，才会在发送方捕获要传送的信号电平并传送给接收方。有关计算监视时间的信息，可在《SIMATIC S7 中的安全工程》系统手册中找到。

10. 为了减少总线负载，可临时关闭 F-CPU 之间的通讯。要执行该操作，请将 F_SENDS7 的输入 EN_SEND 设置为“0”（缺省值 =“1”）。然后，发送数据将不再发送到关联 F_RCVS7 的 F 通讯 DB，并且在此期间接收方 F_RCVS7 将提供故障安全值（缺省的 F 通讯 DB）。如果伙伴之间已建立通讯，则将检测到通讯错误。
11. 可选：评估 F_RCVS7 的 ACK_REQ 输出，例如，在标准用户程序或在操作员监视和控制系统中，以查询或指明是否需要用户确认。
12. 为 F_RCVS7 的 ACK_REI 输入提供信号以对重新集成进行确认。
13. 可选：评估 F_RCVS7 或 F_SENDS7 的输出 SUBS_ON，以查询 F_RCVS7 是否输出在 F 通讯 DB 中指定为缺省值的故障安全值。
14. 可选：评估 F_RCVS7 或 F_SENDS7 的 ERROR 输出（例如，在标准用户程序或在操作员监视和控制系统中），以查询或指明是否出现通讯错误。
15. 可选：评估 F_RCVS7 的 SENDMODE 输出，以查询具有关联的 F_SENDS7 的 F-CPU 是否处于取消激活的安全模式中。

**警告**

如果带有关联 F_SENDS7 的 F-CPU 处于取消激活的安全模式下，则不能再假定接收自该 F-CPU 的数据是安全生成的。然后，必须实施组织措施（例如，操作监视和手动安全关闭），以确保系统中受接收数据影响的那些部分的安全。此外，必须通过评估 SENDMODE，输出故障安全值以代替具有 F_RCVS7 的 F-CPU 中接收的数据。

参见

创建和编辑 F-DB (页 85)

8.7.4 数据传输的限制（通过 S7 连接的安全相关的通讯）

数据传输的限制

说明

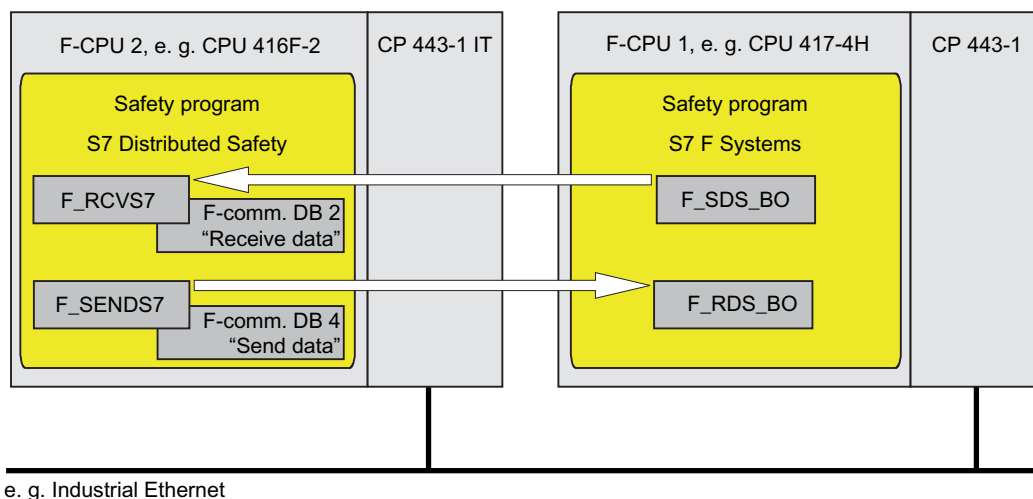
如果传输的数据数量超过 F-Communication DB 允许的长度（100 个字节），则可使用已修改的 R_ID 创建另一个 F-Communication DB，用于传输至其它 F_SENDS7/F_RCVS7 调用。

请注意，每次调用 F_SENDS7 或 F_RCVS7 时 SFB 8 和 SFB 9 已被内部调用，并且使用 F-CPU 中的连接资源。这将影响可用的通讯连接的最大数目。可以在“通讯” (Communication) 选项卡的“模块信息” (Module Information) 对话框中以与标准系统相同的方式获取有关 F-CPU 连接资源的信息。

8.8 S7 Distributed Safety 和 S7 F 系统之间的安全相关的通讯

引言

还可通过在 S7 F 系统中的 F-CPU 的 S7 连接进行安全相关的通讯。最多可交换 32 个数据类型为 BOOL 的数据元素。



S7 Distributed Safety 一方的步骤

在 S7 Distributed Safety 一方，按照『通过 S7 通讯进行安全相关的通讯』一章中介绍的步骤进行操作。

特性：

对于 S7 F 系统和 S7 Distributed Safety 之间的通讯，您必须在 S7 Distributed Safety 一方创建恰好具有 32 个数据类型为 BOOL 的数据元素的 F 通讯 DB。

S7 F Systems 一方的步骤

在 S7 F System 一方，按照《S7 F/FH 系统 - 组态和编程》手册中的『F-CPU 之间的安全相关通讯』一章中介绍的步骤进行操作

(<http://support.automation.siemens.com/WW/view/de/16537972>)。

特性：

S7 F Systems 和 S7 Distributed Safety 之间的通讯仅在具有 F-Block F_SDS_BO/F_RDS_BO 的 S7 F Systems 一方才能进行。

F 库

9.1 Distributed Safety F 库 (V1)

9.1.1 Distributed Safety F-Library (V1) 概述

概述

Distributed Safety F-Library (V1) 包含:

- *F* 应用程序块|块文件夹中的 F 应用程序块
- *F* 系统块|块文件夹中的 F 系统块和 F 共享 DB

说明

不得更改 F 库名称。

Distributed Safety F 库 (V1) 可以仅包含那些使用 *S7 Distributed Safety* 版本安装的 F 块。

9.1.2 F 应用程序块

9.1.2.1 F 应用程序块概述

F 应用程序块概述

块编号	块名称	功能
FB179	F_SCA_I	数据类型 INT 的刻度值
FB181	F_CTU	增计数
FB182	F_CTD	减计数
FB183	F_CTUD	增计数和减计数
FB184	F_TP	创建脉冲

块编号	块名称	功能
FB185	F_TON	创建 ON 延迟
FB186	F_TOF	创建 OFF 延迟
FB187	F_ACK_OP	故障安全确认
FB188	F_2HAND	双手操作监视
FB189	F_MUTING	暂时失效
FB 190	F_1oo2DI	带有误差分析的 1oo2 评估
FB 211	F_2H_EN	具有使能的双手操作监视
FB 212	F_MUT_P	并行暂时失效
FB 215	F_ESTOP1	急停（最高可达停止类别 1）
FB 216	F_FDBACK	反馈监视
FB 217	F_SFDOOR	安全门监视
FB 219	F_ACK_GL	F 运行组的所有 F-I/O 的全局确认
FB223	F_SENDDP	通过 PROFIBUS DP 发送数据（16 BOOL, 2 INT）
FB224	F_RCVDP	通过 PROFIBUS DP 接收数据（16 BOOL, 2 INT）
FB 225	F_SENDS7	对于 CPU 4xxF: 通过 S7 连接发送数据（从 F-DB）
FB 226	F_RCVS7	对于 CPU 4xxF: 通过 S7 连接接收数据（从 F-DB）
FC 174	F_SHL_W	向左移 16 位
FC 175	F_SHR_W	向右移 16 位
FC 176	F_BO_W	将数据类型为 BOOL 的 16 个数据元素转换为数据类型为 WORD 的一个数据元素
FC 177	F_W_BO	将数据类型为 WORD 的一个数据元素转换为数据类型为 BOOL 的 16 个数据元素
FC 178	F_INT_WR	将数据类型 INT 的值间接写入 F-DB
FC 179	F_INT_RD	从 F-DB 间接读取数据类型 INT 的值

说明

可以更改 F 应用程序块的编号。例外情况：使用 F_ESTOP1 和 F_FDBACK F 应用程序块时，F_TOF F 应用程序块必须具有编号 FB 186，且不得重新编号。

如果更改了 F 应用程序块的编号，请注意符号表中的符号名必须仍与块（标题）的对象属性中的名称匹配。

不能将 *Distributed Safety F 库 (V1)* 的 F 应用程序块的符号名用于用户创建的 F-FB、F-FC 和块。

说明

必须确保 F-CPU 中的 F-Block 保持一致。

要执行该操作，必须仅使用单个 *S7 Distribution Safety* 版本的 F 应用程序块，并使用 *S7 Distributed Safety* 设置编译安全程序。

说明

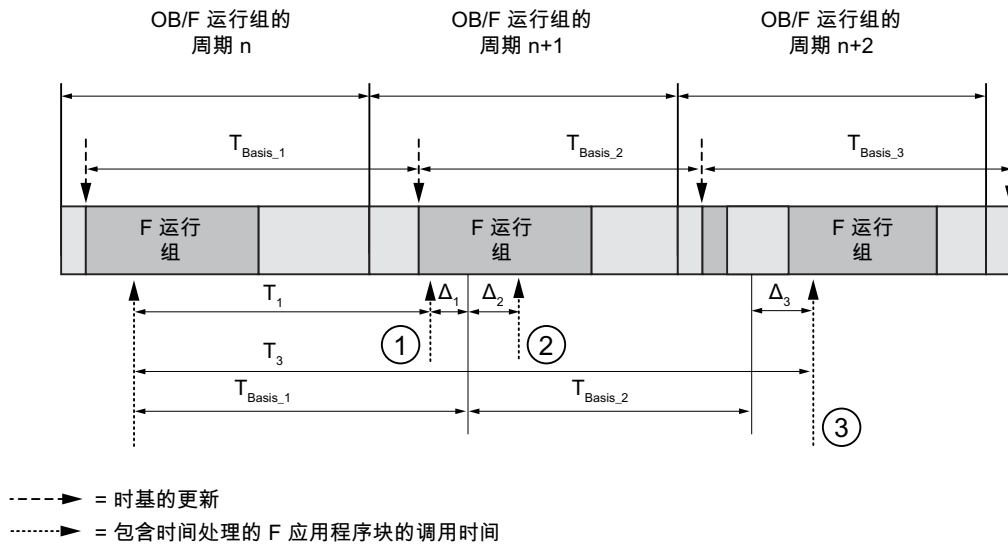
如果调用块，则自动产生使能输入 EN 和使能输出 ENO。不得互连这些连接、为它们提供“0”或评估它们。

具有时间处理的 F 应用程序块的计时不准确**警告**

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新时间引起的计时不准确（请参见下图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%
- 考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。

由 F 应用程序块中使用的时基的更新时间引起的计时不准确



说明

- (1) 对于周期 $n+1$ 中的首次调用，相对于 F 运行组的开始时间，F 应用程序块的调用时间比在周期 n 中的调用时间早 Δ_1 ，例如，因为跳过了周期 $n+1$ 中 F 应用程序块的调用时间之前 F 运行组的安全程序的部分。对于时间更新，F 应用程序块将考虑时间 T_{Basis_1} ，而不是在周期 n 中从调用开始实际已用完的 T_1 时间。
- (2) 在周期 $n+1$ 中第二次调用 F 应用程序块。这不涉及其它时间更新（增量为 Δ_2 ）。
- (3) 对于周期 $n+2$ 中的调用，相对于 F 运行组的开始时间，F 应用程序块的调用时间比在周期 n 中的调用时间晚 Δ_3 ，例如，因为在周期 $n+2$ 中调用 F 应用程序块之前具有更高优先级的中断已中断了 F 运行组。F 应用程序块将考虑时间 $T_{Basis_1} + T_{Basis_2}$ ，而不是在周期 n 中从调用开始实际已用完的时间 T_3 。如果周期 $n+1$ 中没有发生调用也可能出现这种情况。

9.1.2.2 FB 179 "F_SCA_I": 输入类型 INT 的刻度值

输入/输出

	参数	数据类型	说明	缺省值
输入:	IN	INT	以物理单位标定输入值	0
	HI_LIM	INT	物理单位计的上限值	0
	LO_LIM	INT	物理单位计的下限值	0
输出:	OUT	INT	标定的结果	0
	OUT_HI	BOOL	1 = 输入值 > 27648: OUT = HI_LIM	0
	OUT_LO	BOOL	1 = 输入值 < 0: OUT = LO_LIM	0

工作原理

F 应用程序块将输入 IN 处使用物理单位的值标定为输入 LO_LIM 上的下限值和输入 HI_LIM 上的上限值之间的值。假设输入 IN 处的值在 0 和 27,648 之间。在输出 OUT 处提供标定的结果。

F 应用程序块将根据以下等式进行操作:

$$OUT = [IN * (HI_LIM - LO_LIM)] / 27648 + LO_LIM$$

只要输入 IN 处的值大于 27,648, 则输出 OUT 链接至 HI_LIM, 并且 OUT_HI 设置为 1。

只要输入 IN 处的值小于 0, 则输出 OUT 链接至 LO_LIM, 并且 OUT_LO 设置为 1。

要进行反向标定, 必须指定 LO_LIM > HI_LIM。使用反向标定, 输入 IN 处的输入值增加时输出 OUT 处的输出值减小。

模拟值和故障安全值输出的上溢或下溢事件中的性能

说明

如果来自 SM 336 的 PII；AI 6 x 13 位的输入被用作输入值，必须记住 F 系统将检测到的该 F-SM 通道的上溢或下溢作为 F-I/O 故障或通道故障。将为安全程序提供故障安全值 0 以代替 PII 中的 7FFF_H（对于上溢）或 8000_H（对于下溢）。

在这种情况下如果输出其它故障安全值，则必须评估 F-I/O DB 中的 QBAD 变量（到单个故障安全值的输出的分支）。

如果 F-SM 的 PII 中的值在过量或欠量范围内，但是大于 27648 或小于 0，也可以通过分别评估输出 OUT_HI 和 OUT_LO 来为单个故障安全值生成输出分支。

9.1.2.3 FB 181 "F_CTU": 增计数

连接

	参数	数据类型	说明	缺省值
输入:	CU	BOOL	计数器输入	0
	R	BOOL	复位输入 (R 优于 CU)	0
	PV	INT	缺省值, 请参阅用于获得 PV 效果的参数 Q	0
输出:	Q	BOOL	计数器状态: Q = 1 (如果 CV >= PV) Q = 0 (如果 CV < PV)	0
	CV	INT	当前计数值 (可能值: 0 至 32767)	0

工作原理

该 F 应用程序块形成边沿控制的增计数器（具有基于 IEC 计数器 SFB 0“CTU”的功能）。

计数器在输入 CU 处的上升沿（相对于上一次 F 应用程序块调用）进行加 1 增计数。

当计数值达到 32,767 的上限时，不再增计数。对于每个输入 CU 处的其它上升沿，不进行计数器操作。

输入 R 处的信号状态 1 使计数器复位为 0，与输入 CU 处的值无关。输出 Q 显示当前计数值是大于还是等于缺省值 PV。

该 F 应用程序块的功能符合 IEC 61131-3。

启动特性

F 系统启动之后，复位 F_CTD 的实例将引起以下结果：

- CV = 0
- Q = 0

9.1.2.4 FB 182 "F_CTD": 减计数

输入/输出

	参数	数据类型	说明	缺省值
输入:	CD	BOOL	计数器输入	0
	LOAD	BOOL	装载输入 (LOAD 优于 CD)	0
	PV	INT	缺省值; 计数器预设 PV (如果在输入 LOAD 处存在信号状态 1)。	0
输出:	Q	BOOL	计数器状态: Q = 1 (如果 CV ≤ 0) Q = 0 (如果 CV > 0)	0
	CV	INT	当前计数值 (可能值: -32768 至 32767)	0

工作原理

该 F 应用程序块形成边沿控制的减计数器 (具有基于 IEC 计数器 SFB 1“CTD”的功能)。

计数器在输入 CD 处的上升沿 (相对于上一次 F 应用程序块调用) 进行减 1 的减计数。

当计数值达到 -32768 的下限时, 不再减计数。对于每个输入 CD 处的其它上升沿, 不进行计数器操作。

输入 LOAD 处的信号状态 1 使计数器预设到预设值 PV。该情况的发生与输入 CD 处的值无关。输出 Q 显示当前计数值是小于还是等于零。

该 F 应用程序块的功能符合 IEC 61131-3。

启动特性

F 系统启动之后，在第一个循环中复位 F_CTD 的实例将引起以下结果：

- CV = 0
- Q = 0

9.1.2.5 FB 183 "F_CTUD": 增计数和减计数

连接

	参数	数据类型	说明	缺省值
输入:	CU	BOOL	对输入进行增计数	0
	CD	BOOL	对输入进行减计数	0
	R	BOOL	复位输入 (R 优于 LOAD)	0
	LOAD	BOOL	装载输入 (LOAD 优于 CU 和 CD)	0
	PV	INT	缺省值; 计数器预设 PV (如果在输入 LOAD 处存在信号状态 1)。	0
输出:	QU	BOOL	增计数状态: QU = 1 (如果 CV >= PV) QU = 0 (如果 CV < PV)	0
	QD	BOOL	减计数状态: QD = 1 (如果 CV <= 0) QD = 0 (如果 CV > 0)	0
	CV	INT	当前计数值 (可能值: -32768 至 32767)	0

工作原理

该 F 应用程序块将形成边沿控制的增/减计数器（具有基于 IEC 计数器 SFB 2“CTUD”的功能）。

在上升沿处（相对于上一次 F 应用程序块调用），计数器将进行如下操作：

- 计数器在输入 CU 处进行加 1 增计数
当计数值达到上限（32,767）时，不再增计数。
- 计数器在输入 CD 处进行减 1 减计数
当计数值达到下限（-32,768）时，不再减计数。

如果在一个循环中输入 CU 和输入 CD 处都有上升沿，则计数器保持其当前值。



警告

CU 信号和 CD 信号同时出现时，性能与 IEC 61131-3 中规定的性能不同。根据标准，CU 信号和 CD 信号同时出现时 CU 输入优先。

装载 = 1：使用 PV 输入的值对 CV 进行预设。忽略输入 CU 和 CD 处的值。

R = 1：CV 复位为 0。忽略输入 CU、CD 和 LOAD 处的值。

输出 QU 显示当前计数值大于还是等于预设值 PV。输出 QD 显示当前计数值是小于还是等于零。

启动特性

F 系统启动之后，在第一个循环中复位 F_CTUD 的实例将引起以下结果：

- CV = 0
- QU = 0
- QD = 0

9.1.2.6 FB 184 "F_TP": 创建脉冲

连接

	参数	数据类型	说明	缺省值
输入:	IN	BOOL	启动输入	0
	PT	TIME	脉冲宽度 (PT >= 0)	T# 0 ms
输出:	Q	BOOL	时间状态	0
	ET	TIME	已经过的时间	T# 0 ms

工作原理

该 F 应用程序块将在输出 Q 处生成一个长度 PT 的脉冲（该功能基于 IEC TIMER SFB 3“TP”）。

在输入 IN 处的上升沿上启动脉冲。输出 Q 将保持持续时间 PT 的置位状态，与输入信号的任何进一步变化无关（即，即使在时间 PT 用完之前，输入 IN 从 0 切换至 1）。

输出 ET 显示输出 Q 已置位了多长时间。最大值可以等于输入 PT 的值。输入 IN 更改为 0 时复位，但是，在其可以复位之前时间 PT 必须用完。

 警告

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

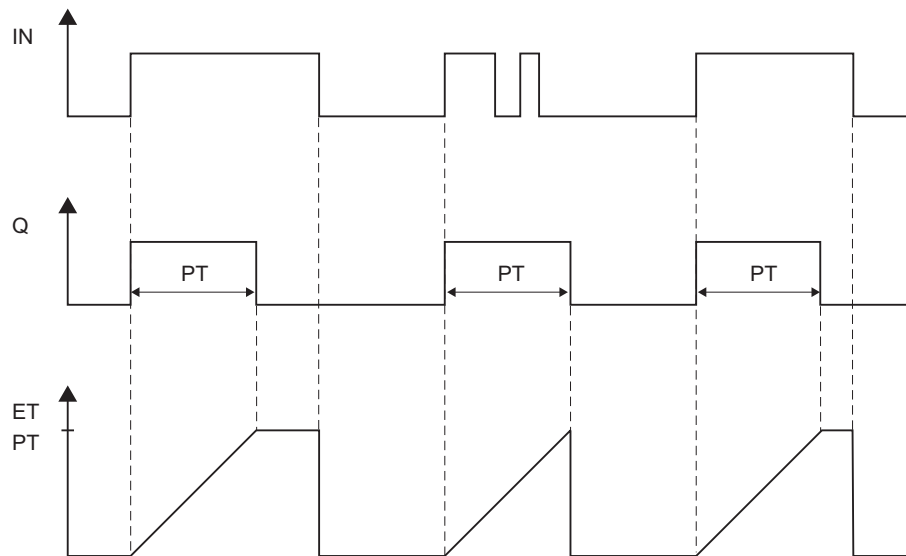
- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新时间引起的计时不准确（请参见“F 应用程序块”中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

考虑到可能发生计时不准确，必须在带有时间处理的 F 应用程序块的两次调用时间之间选择合适的间隔，使得可以获得所需的响应时间。

**警告**

该 F 应用程序块的功能符合 IEC 61131-3，但是它在以下方面与 IEC TIMER SFB 3“TP”不同：

- 使用 $PT = 0\text{ ms}$ 对其进行调用时，F_TP 实例未完全复位（已初始化）。该块的动作符合时序图：仅输出 Q 和 ET 复位。一旦 PT 再次大于 0，就需要输入 IN 处的另一个上升沿来重新启动脉冲。
- $PT < 0\text{ ms}$ 的调用复位输出 Q 和 ET。一旦 PT 再次大于 0，就需要输入 IN 处的另一个上升沿来重新启动脉冲。

F_TP 时序图**启动特性**

F 系统启动之后，在第一个循环中复位 F_TP 的实例将引起以下结果：

- $ET = 0$
- $Q = 0$

参见

F 应用程序块概述 (页 177)

9.1.2.7 FB 185 "F_TON": 创建 ON 延迟

连接

	参数	数据类型	说明	缺省值
输入:	IN	BOOL	启动输入	0
	PT	TIME	输入 IN 处的上升沿被延迟的时间, 需要 $PT \geq 0$	T# 0 ms
输出:	Q	BOOL	时间状态	0
	ET	TIME	已经过的时间	T# 0 ms

工作原理

F 应用程序块将上升沿延迟时间 PT (该功能基于 IEC TIMER SFB 4“TON”)。

一旦时间 PT 已用完, 输入 IN 处的上升沿将引起输出 Q 处的上升沿。Q 将保持置位直到输入 IN 更改为 0。

如果在时间 PT 用完之前输入 IN 更改为 0, 则输出 Q 将保持为 0。

输出 ET 提供自输入 IN 处的上升沿出现之后经过的时间, 不超出输入 PT 处的值。如果输入 IN 更改为 0, 则 ET 复位。

**警告**

使用 F 应用程序块进行时间处理时, 确定响应时间应考虑下列引起计时不准确的源:

- 由周期性处理引起的已知计时不准确 (基于标准系统)
- 由 F 应用程序块中使用的时基的更新时间引起的计时不准确 (请参阅『F 应用程序块』一节中的图)
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值, 容差最大为 (已组态) 时间值的 20%
 - 对于从 100 ms 开始的时间值, 容差最大为 (已组态) 时间值的 2%

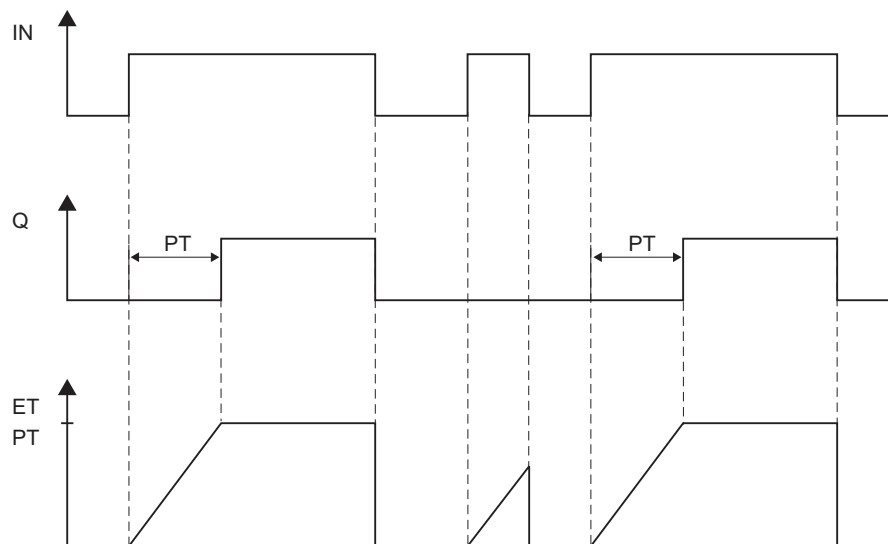
考虑到可能发生计时不准确, 必须在带有时间处理的 F 应用程序块的两次调用时间之间选择合适的间隔, 使得可以获得所需的响应时间。

**警告**

该 F 应用程序块的功能符合 IEC 61131-3，但是它在以下方面与 IEC TIMER SFB 4“TON”不同：

- 使用 $PT = 0\text{ ms}$ 对其进行调用时，F_TON 实例未完全复位（已初始化）。该块的动作符合时序图：仅输出 ET 复位。一旦 PT 再次大于 0，就需要输入 IN 处的另一个上升沿来重新启动 ON 延迟。
- $PT < 0\text{ ms}$ 的调用复位输出 Q 和 ET。一旦 PT 再次大于 0，就需要输入 IN 处的另一个上升沿来重新启动 ON 延迟。

F_TON 时序图



启动特性

F 系统启动之后，在第一个循环中复位 F_TON 的实例将引起以下结果：

- $ET = 0$
- $Q = 0$

参见

F 应用程序块概述 (页 177)

9.1.2.8 FB 186 "F_TON": 创建 OFF 延迟

连接

	参数	数据类型	说明	缺省值
输入:	IN	BOOL	启动输入	0
	PT	TIME	输入 IN 处的下降沿被延迟的时间, 需要 $PT \geq 0$	T# 0 ms
输出:	Q	BOOL	时间状态	0
	ET	TIME	已经过的时间	T# 0 ms

工作原理

F 应用程序块将下降沿延迟时间 PT（该功能基于 IEC TIMER SFB 5“TOF”）。

输入 IN 处的上升沿引起输出 Q 处的上升沿。一旦时间 PT 已用完，输入 IN 处的下降沿将引起输出 Q 处的下降沿。

在时间 PT 用完之前，如果输入 IN 更改为 1，则输出 Q 保持为 1。

输出 ET 提供自输入 IN 处的下降沿出现之后经过的时间，不超出输入 PT 处的值。如果输入 IN 更改为 1，则 ET 复位。

**警告**

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新时间引起的计时不准确（请参阅『F 应用程序块』一节中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

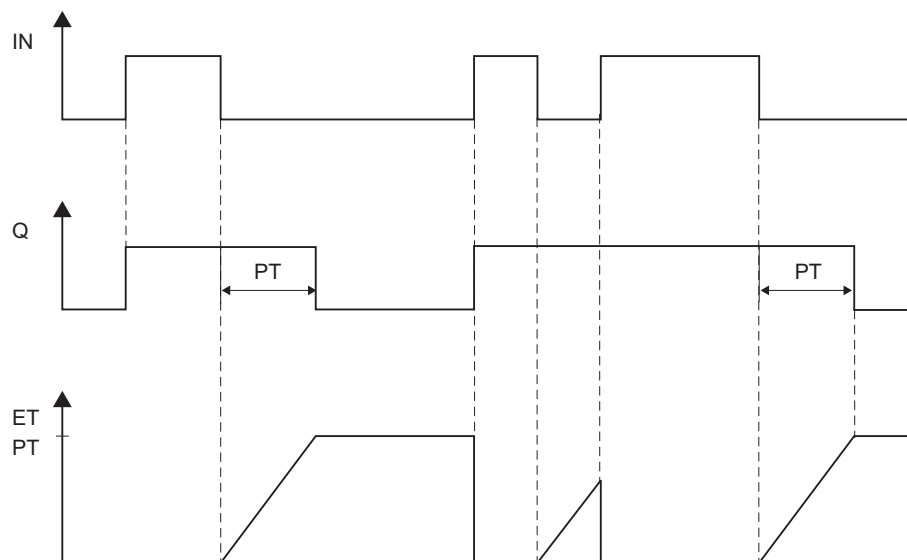
考虑到可能发生计时不准确，必须在带有时间处理的 F 应用程序块的两次调用时间之间选择合适的间隔，使得可以获得所需的响应时间。

**警告**

该 F 应用程序块的功能符合 IEC 61131-3，但是它在以下方面与 IEC TIMER SFB 5“TOF”不同：

- 使用 $PT = 0\text{ ms}$ 对其进行调用时，F_TOF 实例未完全复位（已初始化）。该块的动作符合时序图：仅输出 Q 和 ET 复位。一旦 PT 再次大于 0，就需要输入 IN 处的另一个下降沿来重新启动 OFF 延迟。
- $PT < 0\text{ ms}$ 的调用复位输出 Q 和 ET。一旦 PT 再次大于 0，就需要输入 IN 处的另一个下降沿来重新启动 OFF 延迟。

F_TOF 时序图



启动特性

F 系统启动之后，在第一个循环中复位 F_TOF 的实例将引起以下结果：

- $ET = 0$
- $Q = 0$

参见

F 应用程序块概述 (页 177)

9.1.2.9 FB 187 "F_ACK_OP": 故障安全确认

连接

	参数	数据类型	说明	缺省值
输入/输出参数:	IN	INT	从操作员监视和控制系统输入变量	0
输出:	OUT	BOOL	输出以进行确认	0
	Q	BOOL	时间状态	0

工作原理

该 F 应用程序块从操作员监视和控制系统启用故障安全确认。例如，它允许从操作员监视和控制系统重新集成要控制的 F-I/O。确认分为两步：

1. 输入/输出参数 IN 的值更改为 6。
2. 在 1 min 内将输入/输出参数 IN 的值更改为 9。

一旦输入/输出参数 IN 的值更改为 6，则 F 应用程序块将评估该参数在最早 1 s 或最迟 1 min 后是否更改为值 9。然后将输出 OUT（输出以进行确认）设置为 1 一个周期。

如果输入一个无效值，或者输入/输出参数 IN 的值未在 1 min 内更改为 9 或在 1 s 用完之前发生更改，则输入/输出参数 IN 复位为 0，然后必须重复执行以上列出的两个步骤。

在输入/输出参数 IN 必须从 6 更改为 9 期间，输出 Q 被设置为 1。否则 Q 的值为 0。

 警告

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新时间引起的计时不准确（请参阅『F 应用程序块』一节中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

考虑到可能发生计时不准确，必须在带有时间处理的 F 应用程序块的两次调用时间之间选择合适的间隔，使得可以获得所需的响应时间。

说明

仅可以在标准用户程序中评估输出 Q。不允许在安全程序中访问输出 Q。

仅可以为输入/输出参数 IN 提供一个存储器字或不提供任何存储器字。在安全程序中，不允许在关联的背景数据块中读取和写入访问输入/输出参数 IN!

说明

必须为 F_ACK_OP 的每个调用使用单独的背景数据块。仅可以在 F-Run-Time 组循环中对每个调用处理一次。

如果未遵守以上规定，则 F-CPU 可能切换到 STOP 模式。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
 - “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
 - “安全程序：内部 CPU 故障；内部错误信息：404”
-

附加信息

可以在“参阅”下提供的参考信息中找到有关使用 F_ACK_OP F 应用程序块进行故障安全确认的附加信息。

参见

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

F 应用程序块概述 (页 177)

9.1.2.10 FB 188 "F_2HAND": 双手操作监视

连接

	参数	数据类型	说明	缺省值
输入:	IN1	BOOL	瞬时接触开关 1	0
	IN2	BOOL	瞬时接触开关 2	0
	DISCTIME	TIME	误差时间 (0 至 500 ms)	T# 0 ms
输出:	Q	BOOL	1 = 使能	0

工作原理

此 F 应用程序块实现双手操作监视。如果瞬时接触开关 IN1 和 IN2 在允许的误差时间 $DISCTIME \leq 500 \text{ ms}$ ($IN1/IN2 = 1$) 内被激活（同步激活），则输出信号 Q 被设置为 1。如果瞬时接触开关 IN1 和瞬时接触开关 IN2 激活的时间差大于 DISCTIME，则必须释放瞬时接触开关并重新激活。

释放瞬时接触开关中的一个后，Q 就立即复位为 0 ($IN1/IN2 = 0$)。仅当释放另一个瞬时接触开关后并且两个开关在误差时间内重新激活时，使能信号 Q 才可复位为 1。如果设置的误差时间值小于 0 或大于 500 ms，则使能信号 Q 就永不能设置为 1。

F 应用程序块支持符合 EN 574 的要求。

注：在 F 应用程序块中，每个瞬时接触开关仅可评估一个信号。使用适当的组态（传感器互连的类型：2 通道非等效），由具有输入的 F-I/O 直接执行 IN1 和 IN2 瞬时接触开关的 NC 和 NO 触点的误差监视。NO 触点必须以提供有用信号的方式进行接线（请参阅所使用的 F-I/O 手册）。为了防止误差时间影响响应时间，必须在组态期间为误差特性分配“0 - 提供值”。如果检测到误差，则在过程输入映像 (PII) 中为瞬时接触开关输入故障安全值 0，并且在相关的 F-I/O DB 中设置 QBAD 或 QBAD_I_xx = 1。

**警告**

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新时间引起的计时不准确（请参阅『F 应用程序块』一节中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

考虑到可能发生计时不准确，必须在带有时间处理的 F 应用程序块的两次调用时间之间选择合适的间隔，使得可以获得所需的响应时间。

附加信息

可以在“参阅”下提供的参考信息中找到有关组态和 F-I/O DB 的附加信息。

参见

组态概述 (页 25)

F-I/O DB (页 104)

F 应用程序块概述 (页 177)

9.1.2.11 FB 189 "F_MUTING": 暂时失效

连接

	参数	数据类型	说明	缺省值
输入:	MS_11	BOOL	暂时失效传感器对 1 的传感器 1	0
	MS_12	BOOL	暂时失效传感器对 1 的传感器 2	0
	MS_21	BOOL	暂时失效传感器对 2 的传感器 1	0
	MS_22	BOOL	暂时失效传感器对 2 的传感器 2	0
	STOP	BOOL	1 = 传送带系统停止	0
	FREE	BOOL	1 = 光幕未中断	0
	QBAD_MUT	BOOL	F-I/O 的 QBAD 或 QBAD_O_xx 信号/暂时失效灯的通道 (F-I/O DB)	0
	DISCTIM1	TIME	传感器对 1 的误差时间 (0 至 3 s)	T# 0 ms
	DISCTIM2	TIME	传感器对 2 的误差时间 (0 至 3 s)	T# 0 ms
	TIME_MAX	TIME	最大暂时失效时间 (0 至 10 min)	T# 0 M
	ACK	BOOL	确认重新启动抑制	0
输出:	Q	BOOL	1 = 启用 (未关闭)	0
	MUTING	BOOL	暂时失效的显示处于活动状态	0
	ACK_REQ	BOOL	需要确认	0
	FAULT	BOOL	组错误	0
	DIAG	BYTE	检修信息	0

工作原理

该 F 应用程序块用两个或四个暂时失效传感器执行并行暂时失效。

暂时失效定义为对光幕保护功能的抑制。光幕暂时失效可用于将货物或物体引入由光幕监视的危险区域而不会使机器停止。

要利用暂时失效功能，至少要有两个独立的已接线暂时失效传感器。使用两个或四个暂时失效传感器并正确集成到生产程序，必须确保光幕暂时失效时无人员进入危险区域。

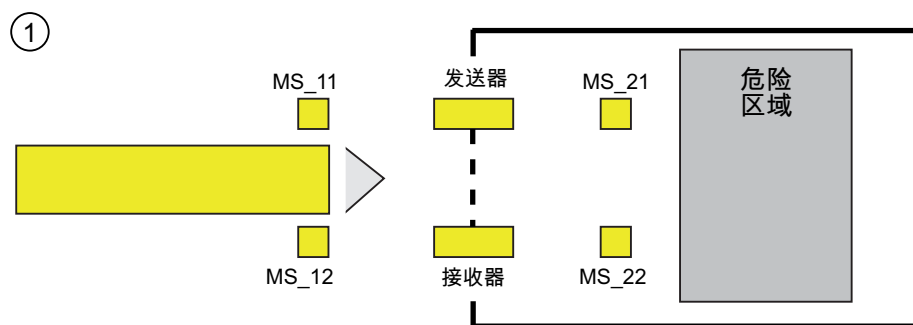
**警告**

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新计时引起的计时不准确（请参阅『F 应用程序块』一章中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。

使用四个暂时失效传感器（MS_11、MS_12、MS_21、MS_22）进行无错暂时失效过程的示意图顺序

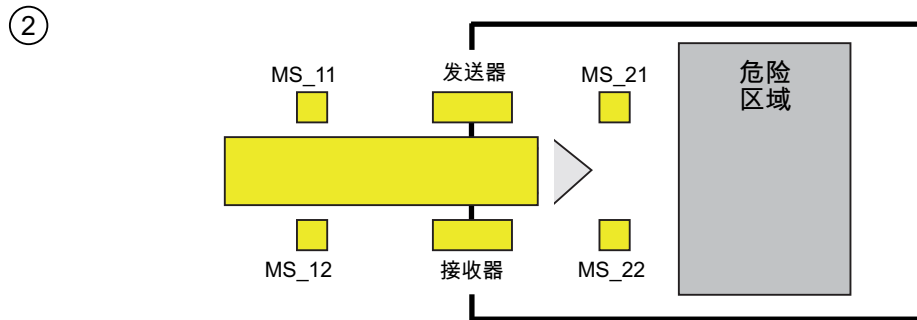


- 如果在 DISCTIM1 内暂时失效传感器 MS_11 和 MS_12 均由产品激活（应用信号状态 = 1），则 F 应用程序块将启动 MUTING 功能。使能信号 Q 保持为 1，即使输入 FREE = 0（由产品中中断光幕）。用于设置暂时失效灯的 MUTING 输出切换为 1。

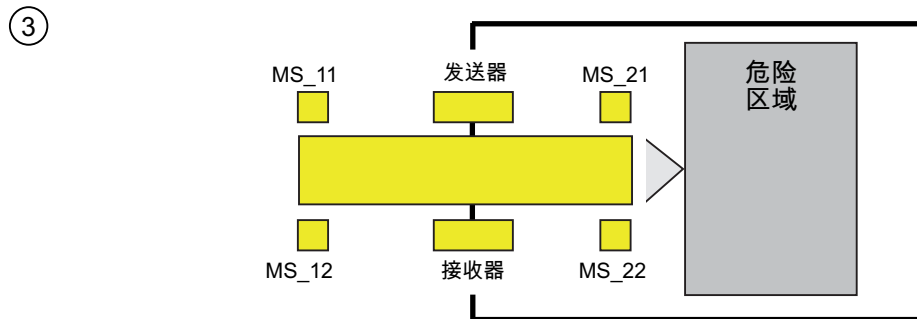
说明

可使用 QBAD_MUT 输入监视暂时失效灯。要进行此操作，必须将暂时失效灯连接至 F-I/O 带有断路监视的输出，并为 QBAD_MUT 输入提供关联的 F-I/O 或通道的 QBAD 或 QBAD_O_xx 信号。如果 QBAD_MUT = 1，将由 F 应用程序块结束暂时失效。如果不需要暂时失效灯的监视，就不必提供输入 QBAD_MUT。

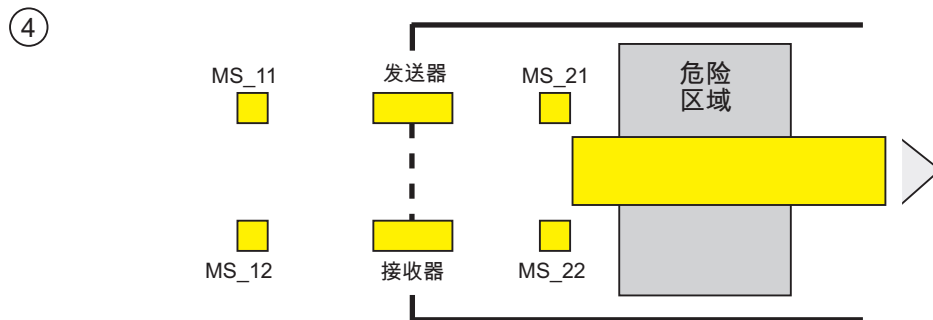
必须使用可在激活暂时失效操作后迅速检测到断路的 F-I/O（请参阅特定的 F-I/O 手册）。



- 只要继续激活暂时失效传感器 MS_11 和 MS_12, F 应用程序块的 MUTING 功能将使 Q 保持为 1 并使 MUTING 保持为 1 (因此产品就可以通过光幕而不会导致机器停止)。



- 必须在暂时失效传感器 MS_11 和 MS_12 切换为不活动状态 (应用信号状态 0) 之前, 激活两个暂时失效传感器 MS_21 和 MS_22 (在 DISCTIM2 内)。这样, F 应用程序块将保持 MUTING 功能。(Q = 1, MUTING = 1)。

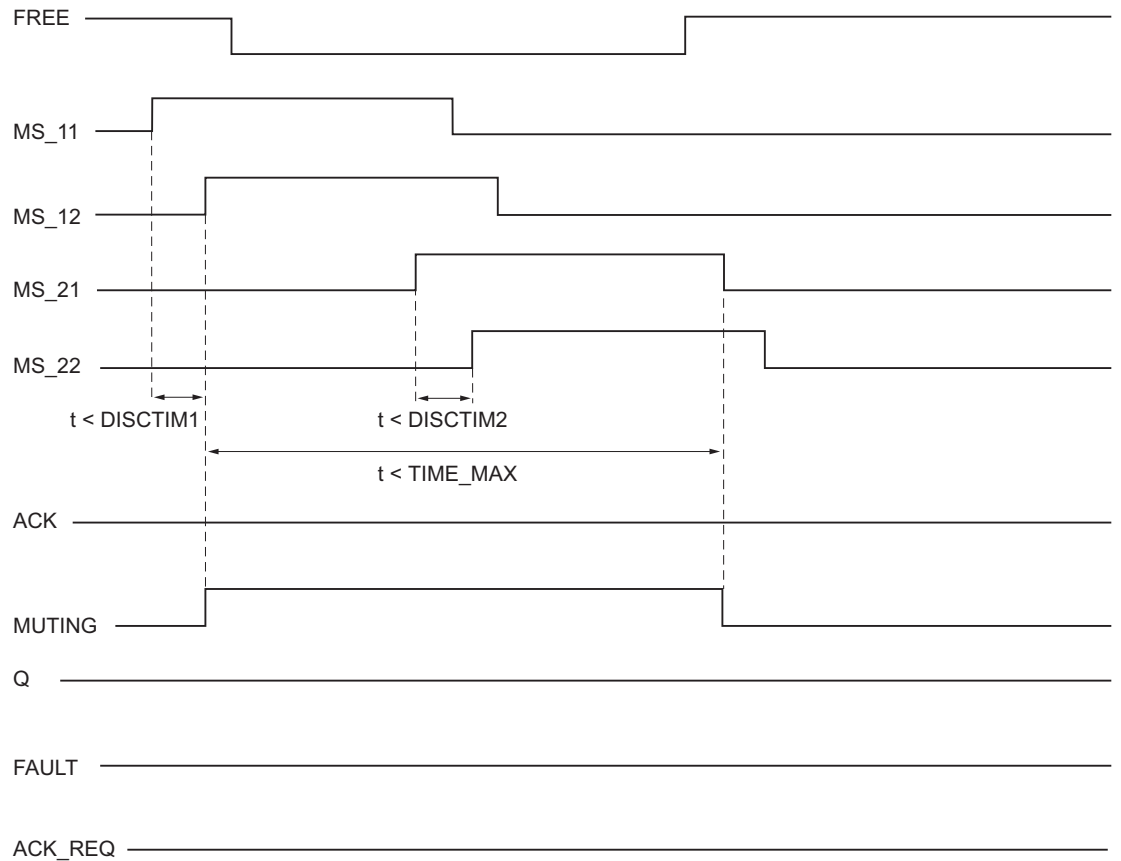


- 仅当两个暂时失效传感器 MS_21 和 MS_22 其中之一切换至不活动状态 (产品启用传感器), 才能终止 MUTING 功能 (Q = 1, MUTING = 0)。MUTING 功能最大激活时间是在输入 TIME_MAX 处设置的时间。

说明

如果产品反向通过光幕, 并且因此产品以相反顺序激活暂时失效传感器, 则也将启动 MUTING 功能。

使用四个暂时失效传感器的无错暂时失效过程的时序图

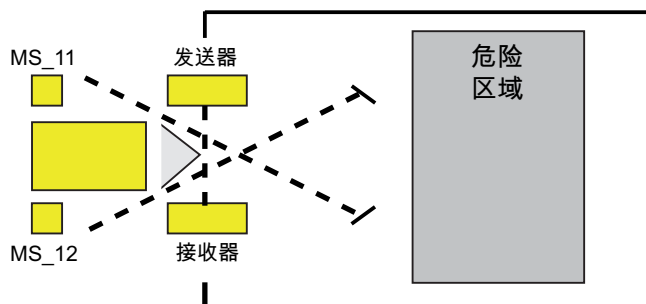


使用反射挡光板的暂时失效过程的示意图顺序

如果反射挡光板用作暂时失效传感器，则它们通常沿对角线排列。

通常，反射挡光板用作暂时失效传感器的这种排列仅需要两个挡光板，并且仅将 MS_11 和 MS_12 互连。

该顺序与使用四个多传感器的暂时失效过程顺序类似。忽略第 3 步。在第 4 步中，请用 MS_11 和 MS_12 分别替换 MS_21 和 MS_22。



在出现错误以及在 F 系统启动期间，在光幕中断（如果 MUTING 未被激活）时重新启动抑制

不能将使能信号 Q 设置为 1 或变成 0，如果：

- MUTING 功能未被激活时光幕中断（例如，被人员或材料运输中断）
- 暂时失效灯监视功能在输入 QBAD_MUT 处响应
- 在误差时间 DISCTIM1 或 DISCTIM2 期间，传感器对 1（MS_11 和 MS_12）或传感器对 2（MS_21 和 MS_22）分别未被激活或被取消激活
- MUTING 功能活动时间长于最大暂时失效时间 TIME_MAX
- 误差时间 DISCTIM1 和 DISCTIM2 的值已设置为 < 0 或 $> 3\text{ s}$
- 最大暂时失效时间 TIME_MAX 的值已设置为 < 0 或 $> 10\text{ min}$

在标识的示例中，输出 FAULT（组错误）设置为 1（重新启动抑制）。如果启动 MUTING 功能，则它将被终止并且暂时失效输出变为 0。



警告

如果在 F 系统启动时立即检测到暂时失效传感器的有效组合（例如，因为暂时失效传感器与标准 I/O 的输入互连，该标准 I/O 在 F-系统启动时立即提供过程值），MUTING 功能将立即启动并且将 MUTING 输出和使能信号 Q 设置为 1。FAULT 输出（组错误）则不设置为 1（无重新启动抑制！）。

确认重新启动抑制

使能信号 Q 再次变成 1，如果：

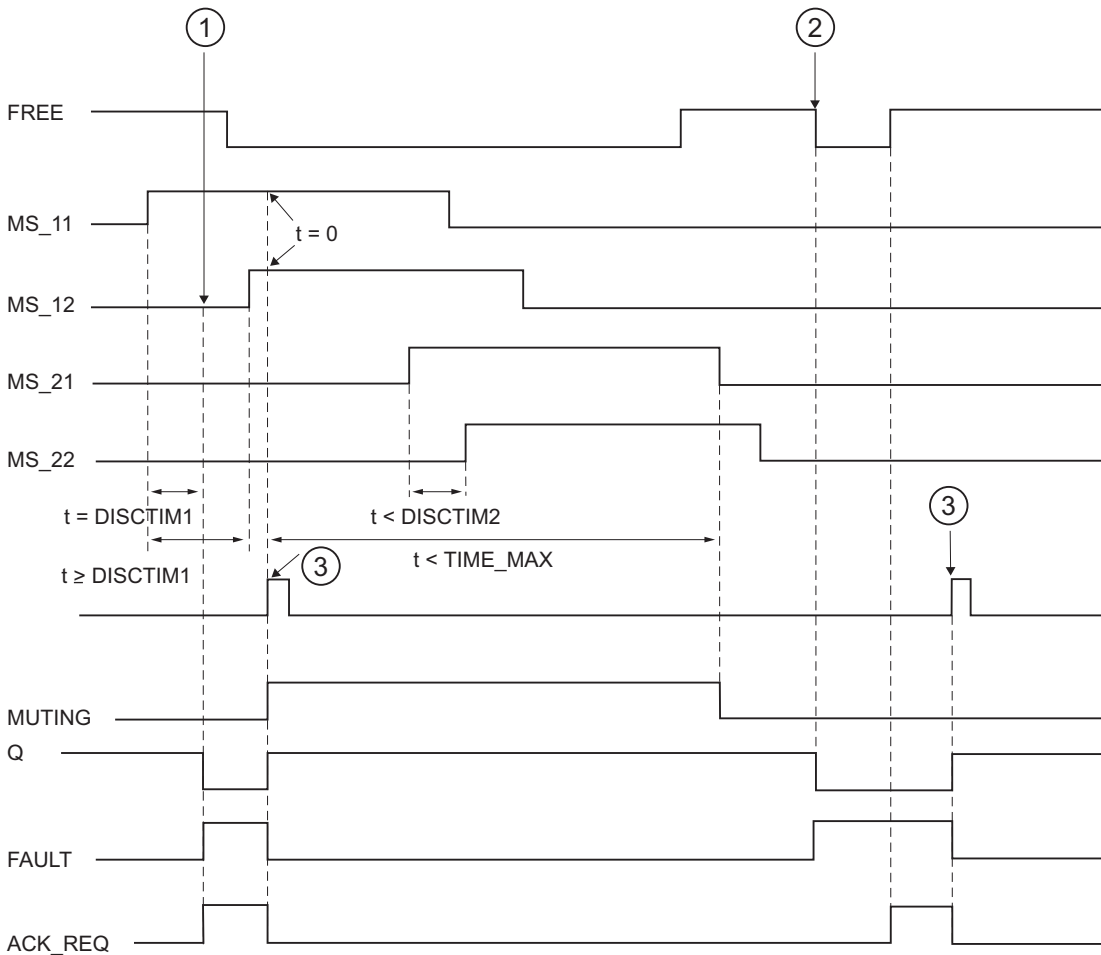
- 光幕不再被中断
- 错误（如果存在）被消除（请参阅输出 DIAG）
和
- 在输入 ACK 处通过上升沿进行用户确认（请参阅『执行用户确认』一章）。

FAULT 输出设置为 0。输出 ACK_REQ = 1 指示要求输入 ACK 处的用户确认以消除重新启动抑制。只要光幕不再中断或错误已经消除后，块就立即设置为 ACK-REQ = 1。进行确认后，块将 ACK_REQ 复位为 0。

说明

发生误差错误后并且一旦超出最大暂时失效时间，ACK_REQ 将立即设置为 1。在输入 ACK 处进行用户确认后，误差时间 DISCTIM1 和 DISCTIM2 以及最大暂时失效时间 TIME_MAX 都将立即复位。

传感器对 1 处的误差错误或光幕中断（如果 MUTING 未被激活）的时序图



- (1) 传感器对 1 (MS_11 和 MS_12) 在误差时间 DISCTIM1 内未被激活。
- (2) 即使 MUTING 功能未被激活，光幕也将被中断。
- (3) 确认

停止传送带设备时的行为

如果在传送带设备停止时取消激活监视，可能由于以下原因之一：

- 为了符合误差时间 DISCTIM1 或 DISCTIM2
- 为了符合最大暂时失效时间 TIME_MAX

传送带设备停止后，必须立即为输入 STOP 提供“1”信号。传送带设备再次运行 (STOP = 0) 后，误差时间 DISCTIM1 和 DISCTIM2 以及最大暂时失效时间 TIME_MAX 都将立即复位。



警告

当 STOP = 1 时，将关闭误差监视。在此期间，如果由于未知错误（例如，因为两个暂时失效传感器无法设置为 1）而使传感器对的输入 MSx1/MSx2 均采用信号状态 1，则将不能检测到该错误并且 MUTING 功能可能会被无意启动。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，也可以在标准用户程序中评估该信息（如果适用）。直到在输入 ACK 处进行确认后，DIAG 位才被保存。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	传感器对 1 的误差错误或为其设置了不正确的误差时间 DISCTIM 1	生产顺序中的故障	生产顺序中的故障已消除
		传感器故障	检查传感器
		接线故障	检查传感器接线
		传感器连接至不同的 F-I/O，以及 F-I/O 故障、通道故障、通讯错误或通过 F-I/O 的 PASS_ON 的钝化	有关解决方案，请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
		误差时间设置过低	设置较高的误差时间（如有必要）
		误差时间设置为 < 0 s 或 > 3 s	设置误差时间的范围在 0 s 和 3 s 之间
位 1	传感器对 2 的误差错误或为其设置了不正确的误差时间 DISCTIM 2	与位 0 相同	与位 0 相同

位号	分配	问题的可能原因	补救措施
位 2	超出最大暂时失效时间或暂时失效时间 TIME_MAX 设置不正确	生产顺序中的故障	生产顺序中的故障已消除
		最大暂时失效时间设置过低	设置较高的最大暂时失效时间 (如有必要)
		暂时失效时间设置为 < 0 s 或 > 10 min	设置暂时失效时间的范围在 0 s 和 10 min 之间
位 3	光幕中断并且暂时失效未激活	光幕有故障	检查光幕
		接线故障	检查光幕的接线 (FREE 输入)
		F-I/O 故障、通道故障、通讯错误或通过 F-I/O 的 PASS_ON 对光幕的钝化 (FREE 输入)	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
		请参阅其它 DIAG 位	
位 4	暂时失效灯故障或无法设置	暂时失效灯有故障	更换暂时失效灯
		接线故障	检查暂时失效灯的接线
		F-I/O 故障、通道故障、通讯错误或通过暂时失效灯的 F-I/O 的 PASS_On 进行的钝化	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
位 5	保留	-	-
位 6	保留	-	-
位 7	保留	-	-

说明

不允许在安全程序中访问 DIAG 输出!

参见

F-I/O DB (页 104)

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

F 应用程序块概述 (页 177)

9.1.2.12 FB 190“F_1oo2DI”： 带有误差分析的 1oo2 评估

连接

	参数	数据类型	说明	缺省值
输入：	IN1	BOOL	传感器 1	0
	IN2	BOOL	传感器 2	0
	DISCTIME	TIME	误差时间 (0 至 60 s)	T# 0 ms
	ACK_NEED	BOOL	1 = 需要对误差错误进行确认	1
	ACK	BOOL	误差错误的确认	0
输出：	Q	BOOL	输出	0
	ACK_REQ	BOOL	1 = 需要确认	0
	DISC_FLT	BOOL	1 = 误差错误	0
	DIAG	BYTE	检修信息	0

工作原理

该 F 应用程序块将执行结合误差分析的两个单通道传感器的 1oo2 评估。

如果输入 IN1 和 IN2 的信号状态均为 1 并且未存储误差错误 DISC_FLT，则输出 Q 设置为 1。如果其中一个或两个输入的信号状态为 0，则输出 Q 设置为 0。

一旦输入 IN1 和 IN2 的信号状态不同，就会立即启动误差时间 DISCTIME。一旦误差时间结束，如果两个输入的信号状态仍不同，则将检测到误差错误并且 DISC_FLT 设置为 1（重新启动抑制）。

如果不再检测到输入 IN1 和 IN2 之间有误差，则根据 ACK_NEC 的参数分配确认误差错误：

- 如果 ACK_NEC = 0，则将自动进行确认。
- 如果 ACK_NEC = 1，则必须使用输入 ACK 处的上升沿来对误差错误进行确认。

ACK_REQ = 1 发出信号指示在输入 ACK 处对误差错误进行必要的用户确认（取消重新启动抑制）。一旦不再检测到误差，F 应用程序块将立即设置 ACK_REQ = 1。确认后或如果在确认之前，输入 IN1 和 IN2 之间再次存在误差，F 应用程序块将 ACK_REQ 复位为 0。

如果误差时间设置 < 0 或 > 60 s，则输出 Q 不能设置为 1。在这种情况下，输出 DISC_FLT 也设置为 1（重新启动抑制）。安全程序的调用间隔（例如，OB35）必须小于误差时间设置。



警告

不得为变量 ACK_NEC 分配值 0，除非排除受影响的过程的自动重启。



警告

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新计时引起的计时不准确（请参阅『F 应用程序块』一章中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

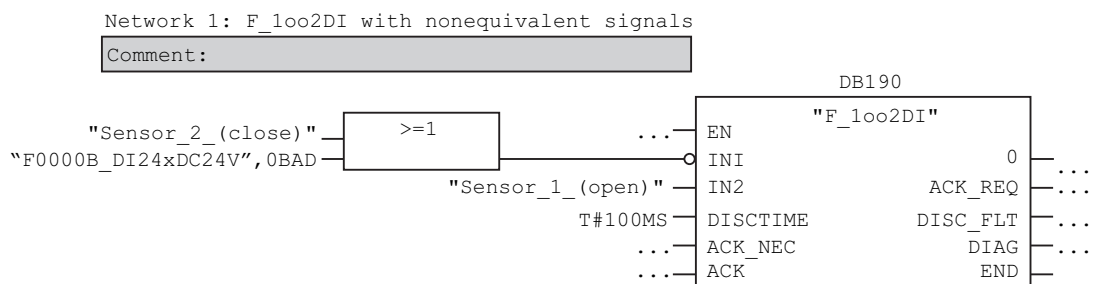
考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。

激活输入 IN1 和 IN2

输入 IN1 和 IN2 的激活方式必须保证使它们的安全状态为 0。

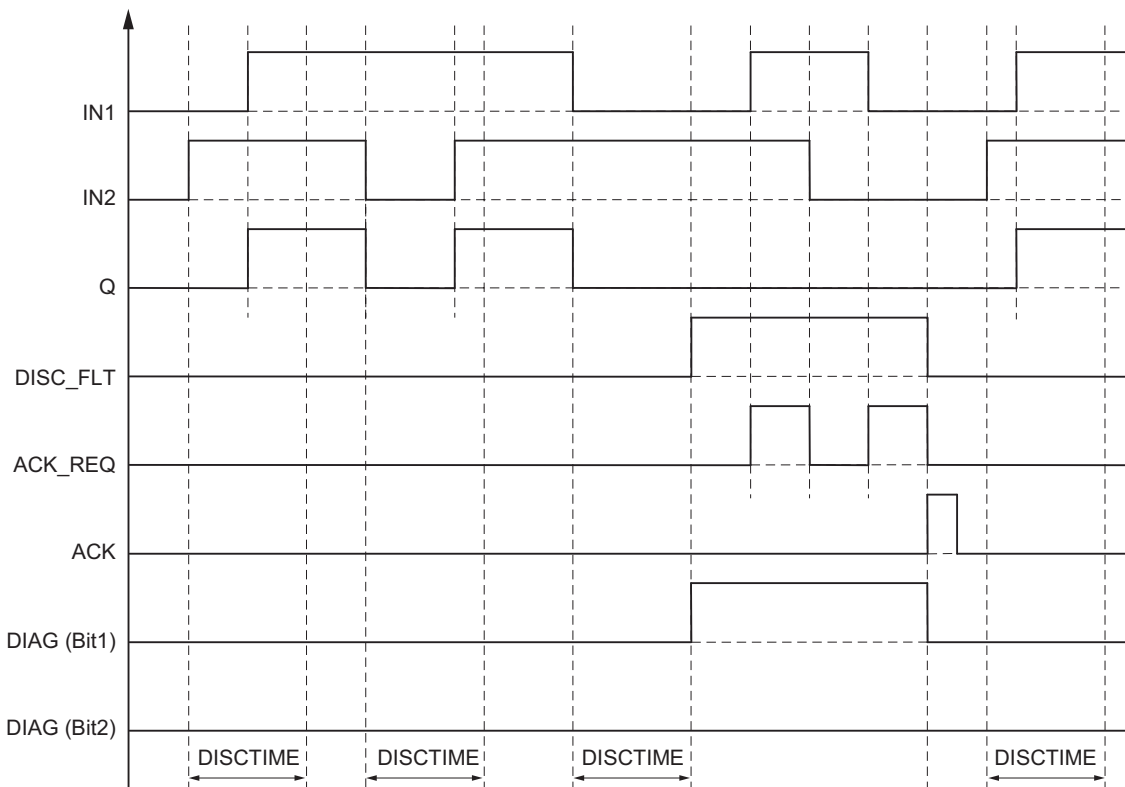
实例

对于非等效信号，必须转换为其分配了具有安全状态 1 的传感器信号的输入（IN1 或 IN2）。还必须使用关联的 F-I/O DB 或通道的 QBAD 或 QBAD_I_xx 变量对传感器信号进行 OR 运算，这样如果输出了故障安全值，则在输入 IN1 或 IN2（转换之后）处的信号状态显示为 0。



F_1oo2DI 的时序图

如果 ACK_NEC = 1:



启动特性

说明

如果将输入 IN1 和 IN2 处的传感器分配到不同的 F-I/O，由于 F-I/O 不同的启动特性，在 F 系统启动后安全故障值可能输出不同的时间长度。如果误差时间 DISCTIME 结束后，输入 IN1 和 IN2 的信号状态仍保持不同，则 F 系统启动后将检测到误差错误。

如果 ACK_NEC = 1，则必须使用输入 ACK 处的上升沿来确认误差错误。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，也可以在标准用户程序中评估该信息（如果适用）。直到在输入 ACK 处进行确认后，DIAG 位才被保存。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	误差错误或误差时间设置不正确 (= DISC_FLT 状态)	传感器故障	检查传感器
		接线故障	检查传感器接线
		传感器连接到不同的 F-I/O，以及 F-I/O 故障、通道故障、通讯错误或通过 F-I/O 的 PASS_ON 的钝化	有关解决方案，请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
		误差时间设置过低	设置较高的误差时间（如有必要）
		误差时间设置为 < 0 s 或 > 60 s	设置误差时间的范围在 0 s 和 60 s 之间
位 1	对于误差错误：上次信号状态更改发生在输入 IN1 处	-	-

位号	分配	问题的可能原因	补救措施
位 2	对于误差错误：上次信号状态更改发生在输入 IN2 处	-	-
位 3	保留	-	-
位 4	保留	-	-
位 5	对于误差错误：输入 ACK 的信号状态将永久为 1	确认按钮故障	更换确认按钮
		接线故障	检查确认按钮的接线
位 6	需要确认	-	-
位 7	输出 Q 的状态	-	-

说明

不允许在安全程序中访问 DIAG 输出！

参见

F-I/O DB (页 104)

F 应用程序块概述 (页 177)

9.1.2.13 FB 211“F_2H_EN”：具有使能的双手操作监视

连接

	参数	数据类型	说明	缺省值
输入：	IN1	BOOL	瞬时接触开关 1	FALSE
	IN2	BOOL	瞬时接触开关 2	FALSE
	ENABLE	BOOL	使能输入	FALSE
	DISCTIME	TIME	误差时间（0 至 500 ms）	T# 0 ms
输出：	Q	BOOL	1 = 使能	FALSE
	DIAG	BYTE	检修信息	B#16#0

工作原理

该 F 应用程序块将执行双手操作监视。如果瞬时接触开关 IN1 和 IN2 在允许的误差时间 $DISCTIME \leq 500 \text{ ms}$ ($IN1/IN2 = 1$) 内被激活（同步激活），则当存在使能 $ENABLE = 1$ 时，输出信号 Q 将设置为 1。如果瞬时接触开关 IN1 和瞬时接触开关 IN2 激活的时间差大于 DISCTIME，则必须释放瞬时接触开关并重新激活。

其中一个瞬时接触开关被释放 ($IN1/IN2 = 0$) 或 $ENABLE = 0$ 后，Q 将立即复位为 0。仅当另一个瞬时接触开关被释放并且当存在使能 $ENABLE = 1$ 时两个开关在误差时间内重新激活，使能信号 Q 才可以复位为 1。

F 应用程序块支持符合 EN 574 的要求。

注意： 在 F 应用程序块中，每个瞬时接触开关仅可评估一个信号。使用适当的组态（传感器互连的类型：双通道非对等型），由具有输入的 F-I/O 直接执行 IN1 和 IN2 瞬时接触开关的 NC 和 NO 触点的误差监视。NO 触点必须以提供有用信号的方式进行接线（请参阅所使用 F-I/O 的手册）。为了防止误差时间影响响应时间，必须在组态期间为误差特性分配“提供 0 值”。

如果检测到误差，则在过程输入映像 (PII) 中为瞬时接触开关输入故障安全值 0，并且在相关的 F-I/O DB 中设置 QBAD 或 QBAD_I_xx = 1。

 **警告**

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新计时引起的计时不准确（请参阅『F 应用程序块』一章中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，或者，可以的话在标准用户程序中评估该信息。直到消除错误原因后，才保存 DIAG 位 0 至 5。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	误差时间 DISCTIME 设置不正确	误差时间设置为 < 0 或 > 500 ms	设置误差时间在范围 0 至 500 ms 内
位 1	误差时间已用完	误差时间设置过低	设置较高的误差时间 (如有必要)
		在误差时间内未激活瞬时接触开关	释放瞬时接触开关并在误差时间内将其激活
		接线故障	检查瞬时接触开关的接线
		瞬时接触开关故障	检查瞬时接触开关
		瞬时接触开关连接至不同的 F-I/O, 以及 F-I/O 故障、通道故障、通讯错误或通过 F-I/O 的 PASS_ON 的钝化	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
位 2	保留	-	-
位 3	保留	-	-
位 4	激活顺序不正确	一个瞬时接触开关未被释放	释放瞬时接触开关并在误差时间内将其激活
		瞬时接触开关故障	检查瞬时接触开关
位 5	使能 ENABLE 不存在	使能 ENABLE = 0	设置 ENABLE = 1, 释放瞬时接触开关并在误差时间内将其激活
位 6	保留	-	-
位 7	输出 Q 的状态	-	-

说明

不允许在安全程序中访问 DIAG 输出!

参见

F-I/O DB (页 104)

F 应用程序块概述 (页 177)

9.1.2.14 FB 212“F_MUT_P”： 并行暂时失效

连接


	参数	数据类型	说明	缺省值
输入:	MS_11	BOOL	暂时失效传感器 11	0
	MS_12	BOOL	暂时失效传感器 12	0
	MS_21	BOOL	暂时失效传感器 21	0
	MS_22	BOOL	暂时失效传感器 22	0
	STOP	BOOL	1 = 传送带系统停止	0
	FREE	BOOL	1 = 光幕未中断	0
	ENABLE	BOOL	1 = 使能 MUTING	0
	QBAD_MUT	BOOL	F-I/O 的 QBAD 或 QBAD_O_xx 信号/暂时失效灯的通道 (F-I/O DB)	0
	ACK	BOOL	确认重新启动抑制	0
	DISCTIM1	TIME	传感器对 1 的误差时间 (0 至 3 s)	T# 0 ms
	DISCTIM2	TIME	传感器对 2 的误差时间 (0 至 3 s)	T# 0 ms
	TIME_MAX	TIME	最大暂时失效时间 (0 至 10 min)	T# 0 ms
	输出:	Q	BOOL	1: 启用 (未关闭)
MUTING		BOOL	暂时失效的显示处于活动状态	0
ACK_REQ		BOOL	需要确认	0
FAULT		BOOL	组错误	0
DIAG		WORD	检修信息	W#16#0

工作原理

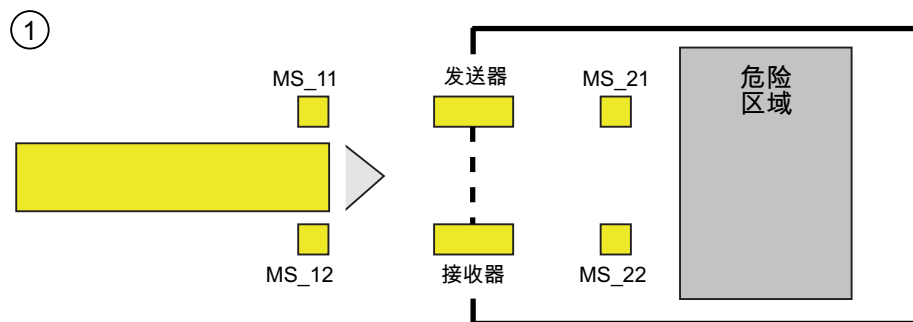
该 F 应用程序块用两个或四个暂时失效传感器执行并行暂时失效。

暂时失效定义为对光幕保护功能的抑制。光幕暂时失效可用于将货物或物体引入由光幕监视的危险区域而不会使机器停止。

要利用暂时失效功能，至少要有两个独立的已接线暂时失效传感器。使用两个或四个暂时失效传感器并正确集成到生产程序，必须确保光幕暂时失效时无人员进入危险区域。

 警告
<p>使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：</p> <ul style="list-style-type: none"> ● 由周期性处理引起的已知计时不准确（基于标准系统） ● 由 F 应用程序块中使用的时基的更新计时引起的计时不准确（请参阅『F 应用程序块』一章中的图） ● F-CPU 中内部时间监视的容差 <ul style="list-style-type: none"> – 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20% – 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2% <p>考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。</p>

使用四个暂时失效传感器（MS_11、MS_12、MS_21、MS_22）进行无错暂时失效过程的示意图顺序

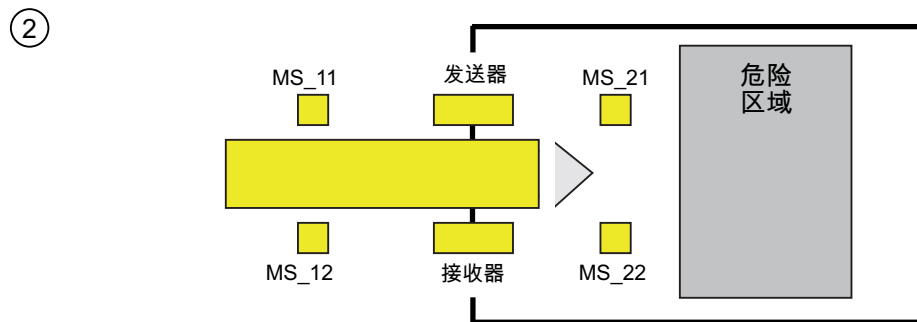


- 如果在 DISCTIM1 内暂时失效传感器 MS_11 和 MS_12 均由产品激活（应用信号状态 = 1），并且通过将 ENABLE 输入设置为 1 启用 MUTING，则 F 应用程序块将启动 MUTING 功能。使能信号 Q 保持为 1，即使输入 FREE = 0（由产品中中断光幕）。用于设置暂时失效灯的 MUTING 输出切换为 1。

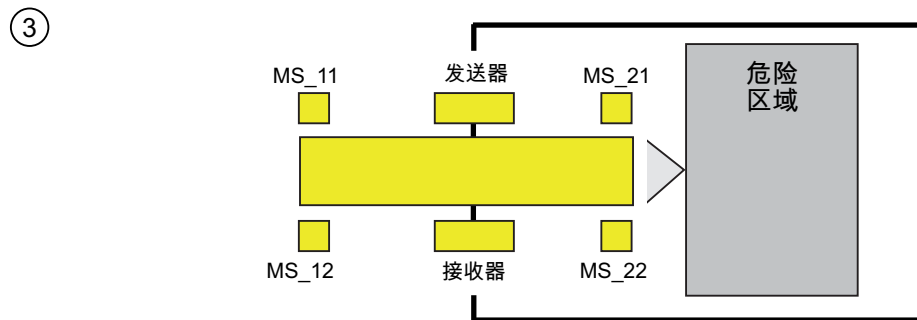
说明

可使用 QBAD_MUT 输入监视暂时失效灯。要进行此操作，必须将暂时失效灯连接至 F-I/O 带有断路监视的输出，并为 QBAD_MUT 输入提供关联的 F-I/O 或通道的 QBAD 或 QBAD_O_xx 信号。如果 QBAD_MUT = 1，将由 F 应用程序块结束暂时失效。如果不需要暂时失效灯的监视，就不必提供输入 QBAD_MUT。

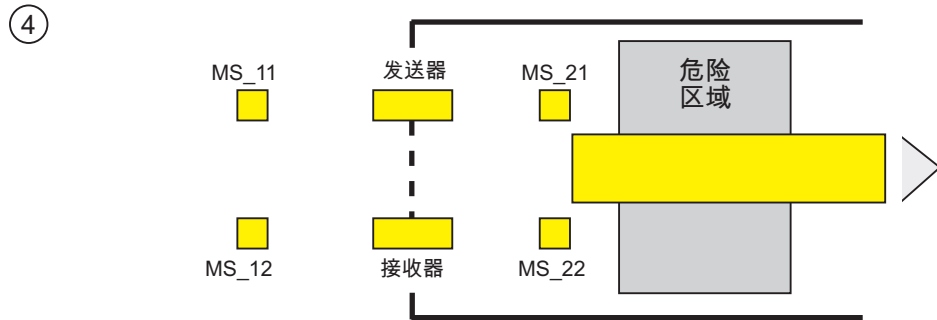
必须使用可在激活暂时失效操作后迅速检测到断路的 F-I/O（请参阅特定的 F-I/O 手册）。



- 继续激活暂时失效传感器 MS_11 和 MS_12 时，F 应用程序块的 MUTING 功能将使 Q 保持为 1 并使 MUTING 保持为 1（因此产品就可以通过光幕而不会导致机器停止）。两个暂时失效传感器 MS_11 和 MS_12 中的每一个都可能会在短时间内切换至不活动 ($t < DISCTIM1$) 状态（应用信号状态 0）。



- 必须在暂时失效传感器 MS_11 和 MS_12 同时切换为不活动（应用信号状态 0）状态之前激活暂时失效传感器 MS_21 和 MS_22（在 DISCTIM2 内）。这样，F 应用程序块将保持 MUTING 功能。（ $Q = 1, MUTING = 1$ ）。

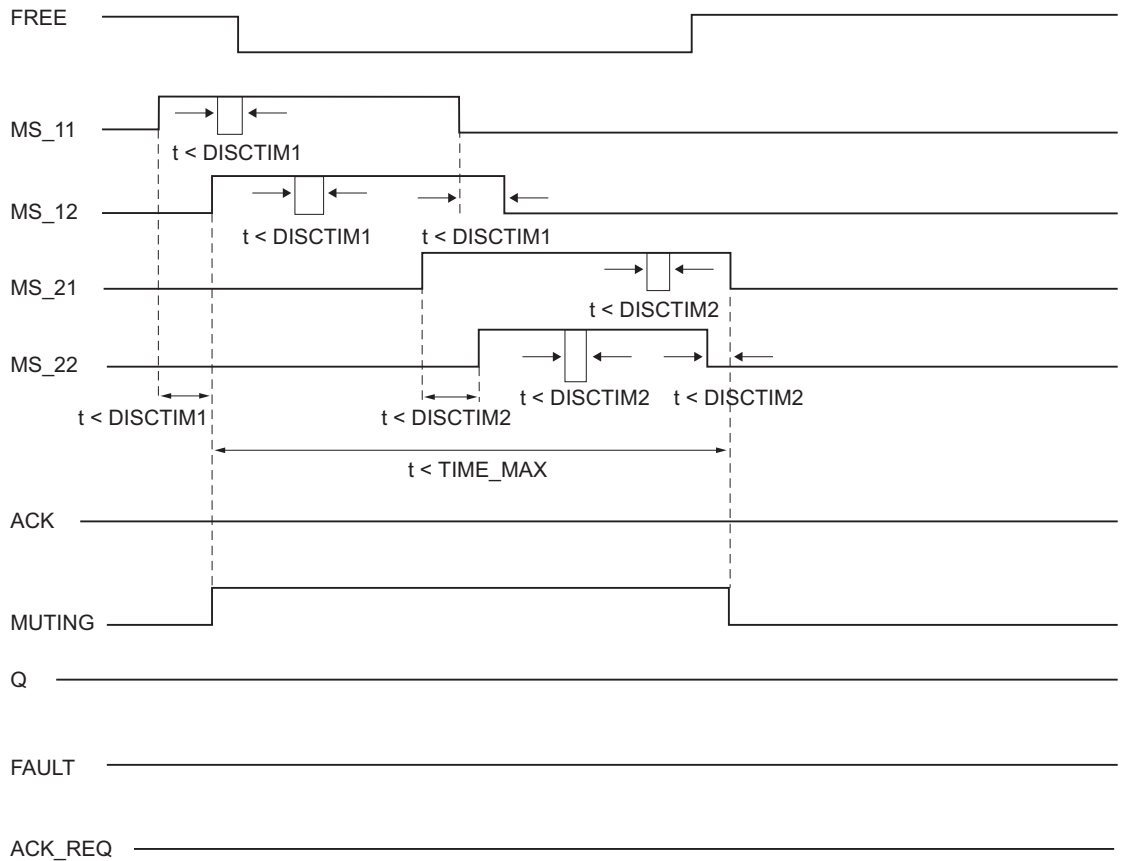


仅当两个暂时失效传感器 MS_21 和 MS_22 均切换至不活动状态（产品启用传感器）才能终止 MUTING 功能（ $Q = 1$, $MUTING = 0$ ）。MUTING 功能最大激活时间是在输入 TIME_MAX 处设置的时间。

说明

如果产品反向通过光幕，并且因此产品以相反顺序激活暂时失效传感器，则也将启动 MUTING 功能。

使用四个暂时失效传感器的无错暂时失效过程的时序图

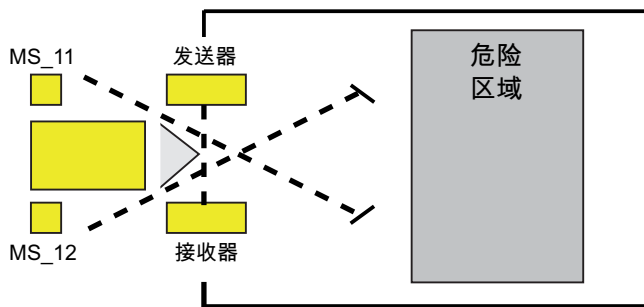


使用反射挡光板的暂时失效过程的示意图顺序

如果反射挡光板用作暂时失效传感器，则它们通常沿对角线排列。

通常，反射挡光板用作暂时失效传感器的这种排列仅需要两个挡光板，并且仅将 MS_11 和 MS_12 互连。

该顺序与使用四个多传感器的暂时失效过程顺序类似。忽略第 3 步。在第 4 步中，请用 MS_11 和 MS_12 分别替换 MS_21 和 MS_22。



在光幕中断（MUTING 未被激活）时以及出现错误和在 F 系统启动期间，重新启动抑制。

不能将使能信号 Q 设置为 1 或变成 0，如果：

- MUTING 功能未被激活时光幕中断（例如，被人员或材料运输中断）
- 光幕被（正在被）中断，暂时失效灯监视在输入 QBAD_MUT 处响应
- 光幕被（正在被）中断，通过将输入 ENABLE 设置为 1 不启用 MUTING 功能
- 在误差时间 DISCTIM1 或 DISCTIM2 期间，传感器对 1（MS_11 和 MS_12）或传感器对 2（MS_21 和 MS_22）分别未被激活或被取消激活
- MUTING 功能活动时间长于最大暂时失效时间 TIME_MAX
- 误差时间 DISCTIM1 和 DISCTIM2 的值已设置为 < 0 或 > 3 s
- 最大暂时失效时间 TIME_MAX 的值已设置为 < 0 或 > 10 min
- F 系统启动（与光幕是否中断无关，因为在 F 系统启动后 F-I/O 被钝化，因此最初为 FREE 输入提供的值为 0）

在标识的示例中，输出 FAULT（组错误）设置为 1（重新启动抑制）。如果启动 MUTING 功能，则它将被终止并且暂时失效输出变为 0。

重新启动抑制的用户确认（暂时失效传感器未被激活或者 ENABLE = 0）

使能信号 Q 再次变成 1，如果：

- 光幕不再被中断
- 错误（如果存在）被消除（请参阅输出 DIAG）
和
- 在输入 ACK 处通过上升沿进行用户确认（请参阅『执行用户确认』一章）。

FAULT 输出设置为 0。输出 ACK_REQ = 1 指示要求输入 ACK 处的用户确认以消除重新启动抑制。只要光幕不再中断或错误已消除，块就立即设置为 ACK_REQ = 1。进行确认后，块将 ACK_REQ 复位为 0。

重新启动抑制的用户确认（至少一个暂时失效传感器被激活并且 ENABLE = 1）

使能信号 Q 再次变成 1，如果：

- 错误（如果存在）被消除（请参阅输出 DIAG）
- 直到检测到暂时失效传感器的有效组合后，才发生 FREE

FAULT 输出被设置为 0。重新启动 MUTING 功能（如有必要），并且如果检测到暂时失效传感器的有效组合，则 MUTING 输出变为 1。当 ENABLE = 1 时，输出 ACK_REQ = 1 发出信号指明为了消除错误和移除重新启动抑制需要 FREE。成功 FREE 后，块将 ACK_REQ 复位为 0。

说明

一旦超出最大暂时失效时间，重新启动 MUTING 功能后，就可立即重新设置 TIME_MAX。

FREE 功能

如果无法立即校正错误，FREE 功能可用于清空暂时失效范围。使能信号 Q 和输出 MUTING = 1（临时）。可以使用 FREE 功能，如果：

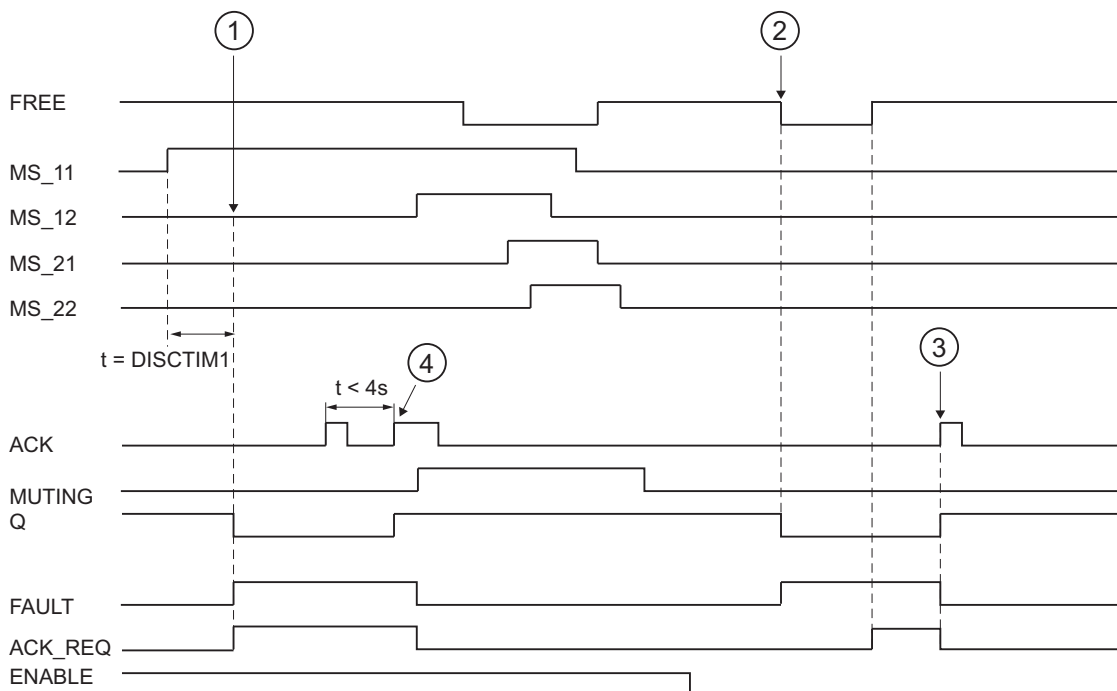
- ENABLE = 1
- 至少一个暂时失效传感器被激活
- 在输入 ACK 处使用上升沿的用户确认在 4 s 内发生两次，并且在输入 ACK 处的第二次用户确认保持在信号状态 1（确认按钮保持活动状态）



警告

使用 FREE 功能时，必须观察操作。必须随时可以通过释放确认按钮来中断危险情况。确认按钮的安装，必须可以管理整个危险区域。

传感器对 1 处的误差错误或光幕中断（MUTING 未被激活）的时序图



- (1) 传感器对 1（MS_11 和 MS_22）在误差时间 DISCTIM1 内未被激活。
- (2) 即使不存在使能（ENABLE = 0），光幕也被中断。
- (3) FREE 功能
- (4) 确认

停止传送带设备时的行为

如果在传送带设备停止时取消激活监视，可能由于以下原因之一：

- 为了符合误差时间 DISCTIM1 或 DISCTIM2
- 为了符合最大暂时失效时间 TIME_MAX

传送带设备停止后，必须立即为输入 STOP 提供“1”信号。传送带设备再次运行 (STOP = 0) 后，误差时间 DISCTIM1 和 DISCTIM2 以及最大暂时失效时间 TIME_MAX 都将立即复位。



当 STOP = 1 或 ENABLE = 0 时，将关闭误差监视。在此期间，如果由于未知错误（例如，因为两个暂时失效传感器无法设置为 1）传感器对的输入 MSx1/MSx2 均采用信号状态 1，则将未检测到该故障并且 MUTING 功能可能会被无意启动（ENABLE = 1 时）。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，或者，可以的话在标准用户程序中评估该信息。直到在输入 ACK 处确认后，DIAG 位 0 到 6 才被保存。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	传感器对 1 的误差错误或为其设置了不正确的误差时间 DISCTIM 1	生产顺序中的故障	生产顺序中的故障已消除
		传感器故障	检查传感器
		接线故障	检查传感器接线
		传感器连接到不同的 F-I/O, 以及 F-I/O 故障、通道故障、通讯错误或通过 F-I/O 的 PASS_ON 的钝化	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
		误差时间设置过低	设置较高的误差时间 (如有必要)
		误差时间设置为 < 0 s 或 > 3 s	设置误差时间的范围在 0 s 和 3 s 之间
位 1	传感器对 2 的误差错误或为其设置了不正确的误差时间 DISCTIM 2	与位 0 相同	与位 0 相同
位 2	超出最大暂时失效时间或暂时失效时间 TIME_MAX 设置不正确	生产顺序中的故障	生产顺序中的故障已消除
		最大暂时失效时间设置过低	设置较高的最大暂时失效时间 (如有必要)
		暂时失效时间设置为 < 0 s 或 > 10 min	设置暂时失效时间的范围在 0 s 和 10 min 之间

位号	分配	问题的可能原因	补救措施
位 3	光幕中断并且暂时失效未激活	ENABLE = 0	设置 ENABLE = 1
		光幕有故障	检查光幕
		接线故障	检查光幕的接线 (FREE 输入)
		I/O 故障、通道故障、通讯错误或通过光幕的 F-I/O 的 PASS_On 进行的钝化 (FREE 输入)	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
		启动 F 系统	有关 FREE, 请参阅 DIAG 变量, 位 5
		请参阅其它 DIAG 位	
位 4	暂时失效灯故障或无法设置	暂时失效灯有故障	更换暂时失效灯
		接线故障	检查暂时失效灯的接线
		F-I/O 故障、通道故障、通讯错误或通过暂时失效灯的 F-I/O 的 PASS_On 进行的钝化	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
位 5	FREE 是必要的	请参阅其它 DIAG 位	ACK 处在 4 s 内出现两个上升沿, 并且激活确认按钮直到 ACK_REQ = 0。
位 6	需要确认	-	-
位 7	输出 Q 的状态	-	-
位 8	输出 MUTING 的状态	-	-
位 9	FREE 激活	-	-
位 10	保留		
...			
位 15	保留		

说明

不允许在安全程序中访问 DIAG 输出!

参见

F-I/O DB (页 104)

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

F 应用程序块概述 (页 177)

9.1.2.15 FB 215“F_ESTOP1”：急停（最高可达停止类别 1）

连接

	参数	数据类型	说明	缺省值
输入：	E_STOP	BOOL	急停	0
	ACK_NEC	BOOL	1 = 需要确认	1
	ACK	BOOL	1 = 确认	0
	TIME_DE L	TIME	延时	T# 0 ms
输出：	Q	BOOL	1 = 使能	0
	Q_DELAY	BOOL	使能为 OFF 延迟	0
	ACK_REQ	BOOL	1 = 确认请求	0
	DIAG	BYTE	检修信息	B#16#0

工作原理

此 F 应用程序块将执行急停关闭，同时带有停止类别 0 和 1 的确认。

只要 E_STOP 输入采用信号状态 0，使能信号 Q 就立即复位为 0（停止类别 0）。在经过输入 TIME_DE L 上设置的延迟时间之后，使能信号 Q_DELAY 复位为 0（停止类别 1）。

仅当输入 E_STOP 采用信号状态 1 且进行确认后，使能信号 Q 才复位为 1。按照在输入 ACK_NEC 处的参数分配对使能进行确认：

- 如果 ACK_NEC = 0，则将自动进行确认。
- 如果 ACK_NEC = 1，则必须使用输入 ACK 处的上升沿来对使能进行确认。

输出 **ACK_REQ** 用于发送信号，指示需要为确认在输入 **ACK** 上输入一个用户确认。只要输入 **E_STOP = 1**，F 应用程序块就立即将输出 **ACK_REQ** 设置为 1。

确认后，F 应用程序块将 **ACK_REQ** 复位为 0。



警告

不得为变量 **ACK_NEC** 分配值 0，除非排除受影响的过程的自动重启。

说明

如果 F 应用程序块 **F_TOF** 尚不存在，则必须先将其从 *Distributed Safety F 库 (V1)* 的 F 应用程序块的块文件夹中复制到 S7 程序的块文件夹，然后才能插入 F 应用程序块 **F_ESTOP**。



警告

使用 F 应用程序块 **F_ESTOP1** 时，F 应用程序块 **F_TOF** 必须具有编号 **FB 186**，且不得重新编号！



警告

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新计时引起的计时不准确（请参阅『F 应用程序块』一章中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 100 ms 的时间值，容差最大为（已组态）时间值的 20%
 - 对于从 100 ms 开始的时间值，容差最大为（已组态）时间值的 2%

考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。

F 应用程序块支持 EN 418、EN 292-2 和 EN 60204-1 的要求。

注意： 在 F 应用程序块上，只能评估一个急停信号 (**E_STOP**)。使用适当的组态（传感器互连的类型：2 通道等效型），由具有输入的 F-I/O 直接执行符合 EN 954-1 中定义类别 3 和 4 的两个 NC 触点（涉及到两个通道时）的误差监视。为了防止误差时间影响响应时间，必须在组态期间为误差特性分配“提供 0 值”。

启动特性

F 系统启动后，当 **ACK_NEC = 1** 时，必须使用输入 **ACK** 处的上升沿来确认 F 应用程序块。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，或者，可以的话在标准用户程序中评估该信息。直到在输入 ACK 处确认后，DIAG 位 1 到 5 才被保存。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	TIM_DEL 设置不正确	延时设置 < 0	设置延时 > 0
位 1	保留	-	-
位 2	保留	-	-
位 3	保留	-	-
位 4	因为急停仍处于活动状态，所以不能进行确认	急停开关被互锁	释放急停开关的互锁
		F-I/O 故障、通道故障、通讯错误或通过急停开关的 F-I/O 的 PASS_ON 进行的钝化	有关解决方案，请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
		急停开关有故障	检查急停开关
		接线故障	检查急停开关的接线
位 5	如果缺少使能：输入 ACK 的信号状态将永久为 1	确认按钮故障	检查确认按钮
		接线故障	检查确认的接线按钮
位 6	需要确认 (= ACK_REQ 的状态)	-	-
位 7	输出 Q 的状态	-	-

说明

不允许在安全程序中访问 DIAG 输出！

参见

F-I/O DB (页 104)

9.1.2.16 FB 216“F_FDBACK”： 反馈监视

连接

	参数	数据类型	说明	缺省值
输入:	ON	BOOL	1 = 使能输出	0
	FEEDBACK	BOOL	反馈输入	0
	QBAD_FIO	BOOL	F-I/O 的 QBAD 或 QBAD_O_xx 信号/输出 Q 的通道 (F-I/O DB)	0
	ACK_NEC	BOOL	1 = 需要确认	1
	ACK	BOOL	确认	0
	FDB_TIME	TIME	反馈时间	T# 0 ms
输出:	Q	BOOL	输出	0
	ERROR	BOOL	反馈错误	0
	ACK_REQ	BOOL	确认请求	0
	DIAG	BYTE	检修信息	B#16#0

工作原理

此 F 应用程序块实现反馈监视。

要执行该操作，将检查输出 Q 的信号状态，以便与反馈输入 FEEDBACK 的相反信号状态相同。

输入 ON = 1 后，输出 Q 将立即设置为 1。这要求反馈输入 FEEDBACK = 1 且无法保存反馈错误。

只要输入 ON = 0 后或者如果检测到反馈错误，输出 Q 将立即设置为 0。

如果反馈输入 FEEDBACK（对于输出 Q）的相反的信号状态在最大容差反馈时间内未跟随输出 Q 的信号状态，则将检测到反馈错误 ERROR = 1。保存反馈错误。

如果在反馈输入 **FEEDBACK** 和输出 **Q** 之间的反馈错误后检测到存在差异，则将根据 **ACK_NEC** 的参数分配来确认反馈错误：

- 如果 **ACK_NEC = 0**，则将自动进行确认。
- 如果 **ACK_NEC = 1**，则必须使用输入 **ACK** 处的上升沿来确认反馈错误。

ACK_REQ = 1 输出发出信号，然后指示在输入 **ACK** 处需要一个用户确认以确认反馈错误。确认后，F 应用程序块将 **ACK_REQ** 复位为 **0**。

输出 **Q** 控制的 F-I/O 钝化时，为避免检测到反馈错误以及避免需要确认，必须为输入 **QBAD_FIO** 提供关联的 F-I/O 的 **QBAD** 或 **QBAD_O_xx** 变量。



警告

必须为变量 **ACK_NEC** 分配值 **0**，除非排除反馈错误后，受影响的过程的自动重启。

说明

如果 **F_TOF** F 应用程序块尚不存在，则必须先将 **F_TOF** F 应用程序块从 **Distributed Safety F 库 (V1)** 的 F 应用程序块\块的块文件夹中复制到 **S7** 程序的块文件夹，然后才能插入 **F_FDBACK** F 应用程序块。



警告

使用 **F_FDBACK** F 应用程序块时，F 应用程序块 **F_TOF** 必须具有编号 **FB 186**，且不得重新编号！



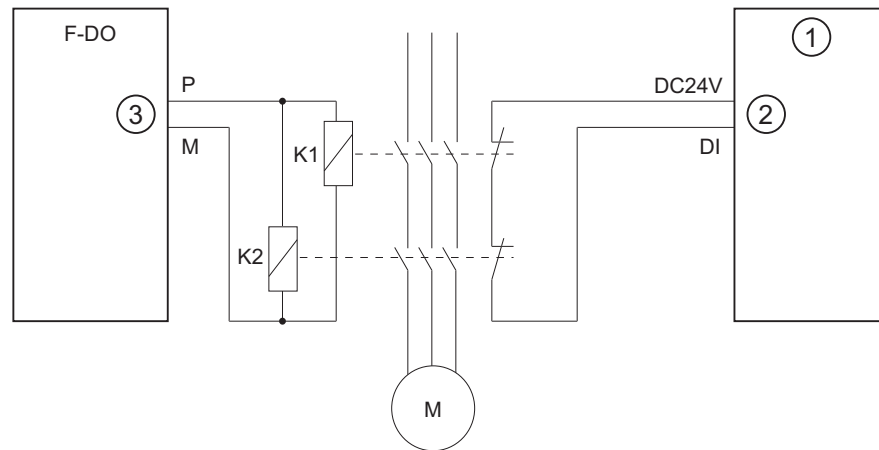
警告

使用 F 应用程序块进行时间处理时，确定响应时间应考虑下列引起计时不准确的源：

- 由周期性处理引起的已知计时不准确（基于标准系统）
- 由 F 应用程序块中使用的时基的更新计时引起的计时不准确（请参阅『F 应用程序块』一章中的图）
- F-CPU 中内部时间监视的容差
 - 对于最高可达 **100 ms** 的时间值，容差最大为（已组态）时间值的 **20%**
 - 对于从 **100 ms** 开始的时间值，容差最大为（已组态）时间值的 **2%**

考虑到可能发生计时不准确，必须对带有时间处理的 F 应用程序块的两次调用时间之间的间隔进行合适选择，使得可以获得要求的响应时间。

互连实例



- (1) 标准 DI
- (2) 输入 FEEDBACK
- (3) 输出 Q

将反馈触点连接至标准 I/O 模块。

启动特性

F 系统启动之后，如果没有错误，则不必确认 F 应用程序块。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，也可以在标准用户程序中评估该信息（如果适用）。直到在输入 ACK 处确认后，DIAG 位 0、2 和 5 才被保存。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	反馈错误或者反馈时间设置不正确 (= ERROR 的状态)	反馈时间设置 < 0	设置反馈时间 > 0
		反馈时间设置过低	设置较高的反馈时间 (如有必要)
		接线故障	检查执行器和反馈触点的接线
		执行器或反馈触点有故障	检查执行器和反馈触点
		反馈输入的 I/O 故障或通道故障	检查 I/O
位 1	F-I/O/输出 Q 控制的通道的钝化 (= QBAD_FIO 的状态)	F-I/O 故障、通道故障、通讯错误或通过 F-I/O 的 PASS_On 的钝化	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
位 2	发生反馈错误后: 反馈输入的信号状态将永久为 0	反馈输入的 I/O 故障或通道故障	检查 I/O
		反馈触点损坏	检查反馈触点
		F-I/O 故障、通道故障、通讯错误或通过反馈输入的 F-I/O 的 PASS_On 进行的钝化	有关解决方案, 请参阅『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
位 3	保留	-	-
位 4	保留	-	-
位 5	对于反馈错误: 输入 ACK 的信号状态将永久为 1	确认按钮故障	检查确认按钮
		接线故障	检查确认按钮的接线
位 6	需要确认 (= ACK_REQ 的状态)	-	-
位 7	输出 Q 的状态	-	-

说明

不允许在安全程序中访问 DIAG 输出!

参见

F-I/O DB (页 104)

F 应用程序块概述 (页 177)

9.1.2.17 FB 217“F_SFDOOR”：安全门监视

连接

	参数	数据类型	说明	缺省值
输入：	IN1	BOOL	输入 1	0
	IN2	BOOL	输入 2	0
	QBAD_IN1	BOOL	F-I/O 的 QBAD 或 QBAD_I_xx 信号/输入 IN1 的通道 (F-I/O)	0
	QBAD_IN2	BOOL	F-I/O 的 QBAD 或 QBAD_I_xx 信号/输入 IN2 的通道 (F-I/O)	0
	OPEN_NEC	BOOL	1 = 启动时需要打开	1
	ACK_NEC	BOOL	1 = 需要确认	1
	ACK	BOOL	确认	0
输出：	Q	BOOL	1= 启用 (安全门关闭)	0
	ACK_REQ	BOOL	确认请求	0
	DIAG	BYTE	检修信息	B#16#0

工作原理

此 F 应用程序块实现安全门监视。

输入 IN1 或 IN2 其中一个具有信号状态 0 后，使能信号 Q 立即复位为 0（安全门打开）。仅当发生以下情况时，使能信号才可复位为 1：


- 打开门之前输入 IN1 和 IN2 均具有信号状态 0（安全门已完全打开）
- 然后输入 IN1 和 IN2 都具有信号状态 1（安全门关闭）
- 发生确认

按照在输入 ACK_NEC 处的参数分配对使能进行确认：

- 如果 ACK_NEC = 0，则将自动进行确认。
- 如果 ACK_NEC = 1，则必须使用输入 ACK 处的上升沿来对使能进行确认。

输出 ACK_REQ = 1 用于发送信号，指示需要为确认在输入 ACK 上输入一个用户确认。门关闭后，F 应用程序块将立即设置 ACK_REQ = 1。确认后，F 应用程序块将 ACK_REQ 复位为 0。

为了使 F 应用程序块可以识别是否仅由于关联的 F-I/O 的钝化而使得输入 IN1 和 IN2 为 0，必须为输入 QBAD_IN1 或 QBAD_IN2 提供关联的 F-I/O 或通道的 QBAD 或 QBAD_I_xx 变量。在 F-I/O 已被钝化的情况下，这将防止在确认之前完全打开安全门。

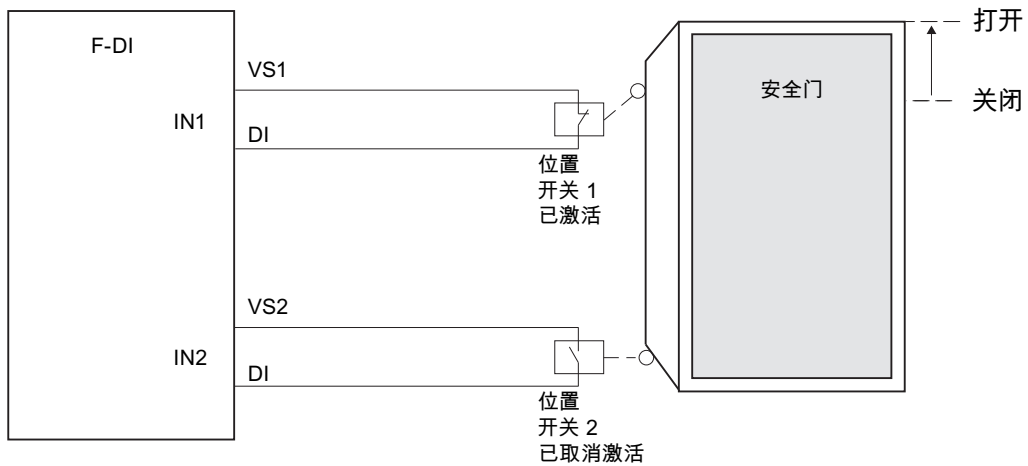
 警告
不得为变量 <code>ACK_NEC</code> 分配值 0，除非排除受影响的过程的自动重启。

F 应用程序块支持 EN 954-1 和 EN 1088 的要求。

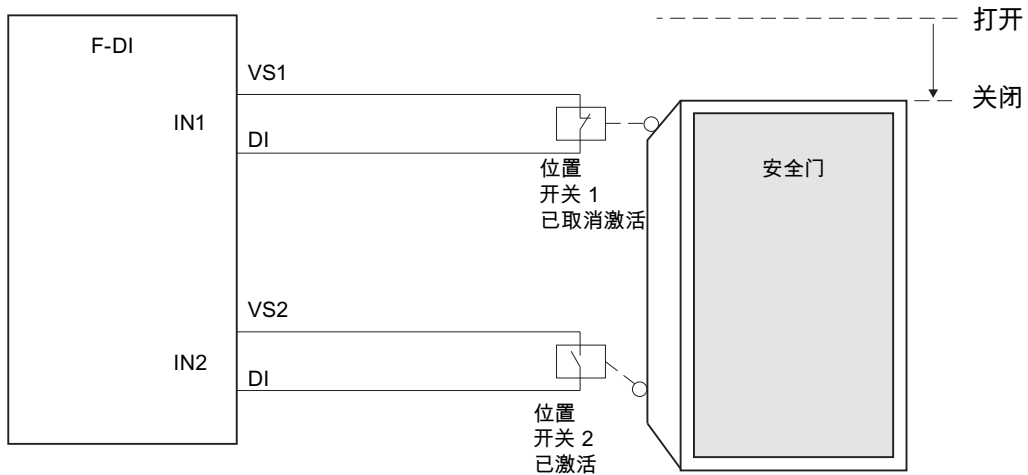
互连实例

必须将输入 IN1 处安全门的位置开关 1 的 NC 触点和输入 IN2 处位置开关 2 的 NO 触点互连。位置开关 1 的安装必须保证在安全门打开时它肯定能动作。位置开关 2 的安装必须保证在安全门关闭时它能动作。

安全门打开：



安全门关闭：



启动特性

F 系统启动后，使能信号 Q 复位为 0。按照在输入 OPEN_NEC 和 ACK_NEC 处的参数分配对使能进行确认：

- OPEN_NEC = 0 时，在重新集成关联的 F-I/O 后两个输入（IN1 和 IN2）首次具有信号状态 1（安全门关闭）时，将**独立于** ACK_NEC，立即进行自动确认。
- OPEN_NEC = 1 时，**或者**如果重新集成关联的 F-I/O 之后，IN1 和 IN2 输入中至少一个信号状态仍为 0，将**按照** ACK_NEC 进行自动确认或者必须为使能在输入 ACK 处使用一个上升沿。确认之前，输入 IN1 和 IN2 均必须先具有信号状态 0（安全门已完全打开），然后具有信号状态 1（安全门关闭）。



警告

不得为变量 OPEN_NEC 分配值 0，除非排除受影响的过程的自动重启。

输出 DIAG

DIAG 输出将提供与错误相关的非故障安全信息，用于检修目的。可以通过操作员监视和控制系统读取该信息，或者，可以的话在标准用户程序中评估该信息。

DIAG 的结构

位号	分配	问题的可能原因	补救措施
位 0	保留	-	-
位 1	IN1 和 IN2 输入处均缺少信号状态 0	F 系统启动后，在 OPEN_NEC = 1 时安全门未完全打开	完全打开安全门
		打开的安全门未完全打开	完全打开安全门
		接线故障	检查位置开关的接线
		位置开关有故障	检查位置开关
		位置开关调整不正确	正确调整位置开关
位 2	IN1 和 IN2 输入处均缺少信号状态 1	安全门未关闭	关闭安全门
		接线故障	检查位置开关的接线
		位置开关有故障	检查位置开关
		位置开关调整不正确	正确调整位置开关

位号	分配	问题的可能原因	补救措施
位 3	QBAD_IN1 和/或 QBAD_IN2 = 1	F-I/O 故障、通道故障、 通讯错误或者通过 IN1 和 /或 IN2 的 F-I/O 或通道 的 PASS_ON 进行的钝化	有关解决方案, 请参阅 『F-I/O DB』一章中的 DIAG 变量的位 0 到 6
位 4	保留	-	-
位 5	如果缺少使能: 输入 ACK 的信号状态永远为 1	确认按钮故障	检查确认按钮
		接线故障	检查确认按钮的接线
位 6	需要确认 (= ACK_REQ 的状态)	-	-
位 7	输出 Q 的状态	-	-

说明

不允许在安全程序中访问 DIAG 输出!

参见

F-I/O DB (页 104)

启动 F 系统后钝化和重新集成 F-I/O (页 111)

9.1.2.18

FB 219“F_ACK_GL”: F 运行组的所有 F-I/O 的全局确认

连接

	参数	数据类型	说明	缺省值
输入:	ACK_REI_GLO B	BOOL	1 = 确认重新集成	0

工作原理

在通讯错误或 F I/O/通道错误发生后，该 F 应用程序块将为所有 F I/O/通道（属于 F 运行组的 F I/O）的同步重新集成创建确认。

对于重新集成，需要在输入 ACK_REI_GLOB 处通过上升沿进行确认。该确认与通过 F-I/O DB 的 ACK_REI 变量执行的用户确认类似，但是对 F 运行组（在其中调用了 F 应用程序块）的所有 F-I/O 同时发生影响。

如果使用 F 应用程序块 F_ACK_GL，则不必通过 F-I/O DB 的 ACK_REI 变量为 F 运行组的每个 F-I/O 提供用户确认。

说明

仅在用 *S7 Distributed Safety V5.4* 或更高版本创建了安全程序，至少已为一个 F-I/O 组态了通道级钝化，或至少将一个 F-I/O 连接到 PROFINET IO 的情况下，才可使用 F_ACK_GL F 应用程序块。然后，F 系统块 F_IO_CGP 将位于“S7 程序”的块文件夹中。仅在 F-I/O DB 的变量 ACK_REI = 0 时，可通过 F_ACK_GL 执行确认。因此，仅在 F 应用程序块的输入 ACK_REI_GLOB = 0 时，可通过 F-I/O DB 的变量 ACK_REI 来执行确认。

每个 F 运行组仅可调用一次 F 应用程序块。

参见

F-I/O DB (页 104)

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

9.1.2.19 FB 223“F_SENDDP”和 FB 224“F_RCVDP”：通过 PROFIBUS DP 发送和接收数据

引言

使用 F 应用程序块 F_SENDDP 和 F_RCVDP，通过以下方式进行故障安全的数据发送和接收：

- 安全相关的主站与主站通讯
- 安全相关的主站与智能从站通讯
- 安全相关的智能从站与智能从站通讯

F 应用程序块 F_SENDDP 的连接

	参数	数据类型	说明	缺省值
输入:	SD_BO_0	BOOL	发送数据 BOOL 00	0
	...			
	SD_BO_15	BOOL	发送数据 BOOL 15	0
	SD_I_00	INT	发送数据 INT 00	0
	SD_I_01	INT	发送数据 INT 01	0
	DP_DP_ID	INT	网络范围内唯一的 F_SENDDP 和 F_RCVDP 之间的地址关联值	0
	TIMEOUT	TIME	安全相关的通讯的监视时间（以 ms 为单位）（请参阅《SIMATIC S7 中的安全工程》系统手册）	0 ms
	LADDR	INT	地址区的起始地址： <ul style="list-style-type: none"> 属于安全相关的主站与主站通讯的 DP/DP 耦合器 用于安全相关的主站与智能从站通讯 用于安全相关的智能从站与智能从站通讯 	0
输出:	ERROR	BOOL	1 = 通讯错误	0
	SUBS_ON	BOOL	1 = 接收方输出故障安全值	1
	RETVAL14	WORD	SFC 14 的错误代码 （可在 SFC 14 的在线帮助中找到错误代码说明）。	0
	RETVAL15	WORD	SFC 15 的错误代码 （可在 SFC 15 的在线帮助中找到错误代码说明）。	0
	DIAG	BYTE	检修信息	0

F 应用程序块 F_RCNDP 的连接

	参数	数据类型	说明	缺省值
输入:	ACK_REI	BOOL	1 = 发生通讯错误后, 对发送数据的重新集成进行确认	0
	SUBBO_00	BOOL	用于接收数据 BOOL 00 的故障安全值	0
	...			
	SUBBO_15	BOOL	用于接收数据 BOOL 15 的故障安全值	0
	SUBI_00	INT	用于接收数据 INT 00 的故障安全值	0
	SUBI_01	INT	用于接收数据 INT 01 的故障安全值	0
	DP_DP_ID	INT	网络范围内唯一的 F_SENDDP 和 F_RCNDP 之间的地址关联值	0
	TIMEOUT	TIME	安全相关的通讯的监视时间 (以 ms 为单位) (请参阅《SIMATIC S7 中的安全工程》系统手册)	0 ms
	LADDR	INT	地址区的起始地址: <ul style="list-style-type: none"> 属于安全相关的主站与主站通讯的 DP/DP 耦合器 用于安全相关的主站与智能从站通讯 用于安全相关的智能从站与智能从站通讯 	0
输出:	ERROR	BOOL	1 = 通讯错误	0
	SUBS_ON	BOOL	1 = 输出故障安全值	1
	ACK_REQ	BOOL	1 = 需要对发送数据的重新集成进行确认	0
	SENDMODE	BOOL	1 = 具有 F_SENDDP 的 F-CPU 处于取消激活的安全模式中	0
	RD_BO_00	BOOL	接收数据 BOOL 00	0
	...			

	参数	数据类型	说明	缺省值
	RD_BO_15	BOOL	接收数据 BOOL 15	0
	RD_I_00	INT	接收数据 INT 00	0
	RD_I_01	INT	接收数据 INT 01	0
	RETV14	WORD	SFC 14 的错误代码（可在 SFC 14 的在线帮助中找到错误代码的说明）。	0
	RETV15	WORD	SFC 15 的错误代码（可在 SFC 15 的在线帮助中找到错误代码的说明）。	0
	DIAG	BYTE	检修信息	0

工作原理

F 应用程序块 F_SENDDP 通过 PROFIBUS DP 以故障安全的方式将数据类型 BOOL 的 16 个数据元素和数据类型 INT 的 2 个数据元素发送到另一个 F-CPU。在该 F-CPU 上，将由关联的 F_RCVDP F 应用程序块接收这些数据元素。

在 F_SENDDP 中，在输入 SD_BO_xx 和 SD_I_xx 处应用要发送的数据（例如，其它 F 块的输出）。

在 F_RCVDP 中，在输出 RD_BO_xx 和 RD_I_xx 处可以获取接收的数据，以供其它 F 块进行其它处理。

在输出 SENDMODE 处提供具有 F_SENDDP 的 F-CPU 的工作模式。如果具有 F_SENDDP 的 F-CPU 处于取消激活的安全模式，则输出 SENDMODE = 1。

F-CPU 之间的通讯是通过特殊安全协议在后台隐藏进行的。必须通过在 F_SENDDP 和 F_RCVDP 的 DP_DP_ID 输入处分配唯一的地址关联，以在一个 F-CPU 中的 F_SENDDP 和另一个 F-CPU 中的 F_RCVDP 之间定义关联。关联的 F_SENDDP 和 F_RCVDP 接收相同的 DP_DP_ID 值。

警告

每个地址关联（输入参数 DP_DP_ID；数据类型：INT）的值都是用户定义的；但是，在网络中的所有安全相关的通讯连接中，它必须是唯一的。

调用 F 应用程序块时，必须为输入 DP_DP_ID 和 LADDR 提供常数值。在安全程序中，不允许在关联的背景数据块中进行直接读取或写入访问！

说明

在安全程序中，必须为每个 F_SENDDP 和 F_RCVDB 调用在 LADDR 输入处分配不同的起始地址。必须为每个 F_SENDDP 和 F_RCVDP 调用使用单独的背景数据块。

不得为 F_RCVDP 的输入和输出参数提供 F 程序块的本地数据。

如果已经为相同 F_RCVDP 调用或者其它 F_RCVDP 或 F_RCVS7 调用的输入参数使用了此实参，则不得为 F_RCVDP 的输出参数使用该实参。如果未遵守上述规定，F-CPU 会切换到 STOP。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

启动特性

发送和接收 F 系统启动之后，必须首先在通讯对 F_SENDDP 和 F_RCVDP 之间建立通讯。在此期间，接收方 F_RCVDP 输出其输入 SUBBO_xx 和 SUBBI_xx 上的故障安全值。

F_SENDDP 和 F_RCVDP 在输出 SUBS_ON 处使用 1 发信号指示此信息。只要输出 SUBS_ON = 1，输出 SENDMODE 就有缺省值 0 且不更新。

发生通讯错误时的行为

如果发生通讯错误，例如，由于测试值错误 (CRC) 或监视时间 TIMEOUT 过期，两个 F 应用程序块的输出 ERROR 和 SUBS_ON 都将设置为 1。然后接收方 F_RCVDP 将输出在其 SUBBO_xx 输入处分配的故障安全值。输出 SUBS_ON = 1 时，输出 SENDMODE 不更新。

只有当不再检测到通讯错误 (ACK_REQ = 1) 并确认输入 ACK_REI 处的正沿时，才再次输出输入 SD_BO_xx 和 SUBI_xx 处的 F_SENDDP 的发送数据。



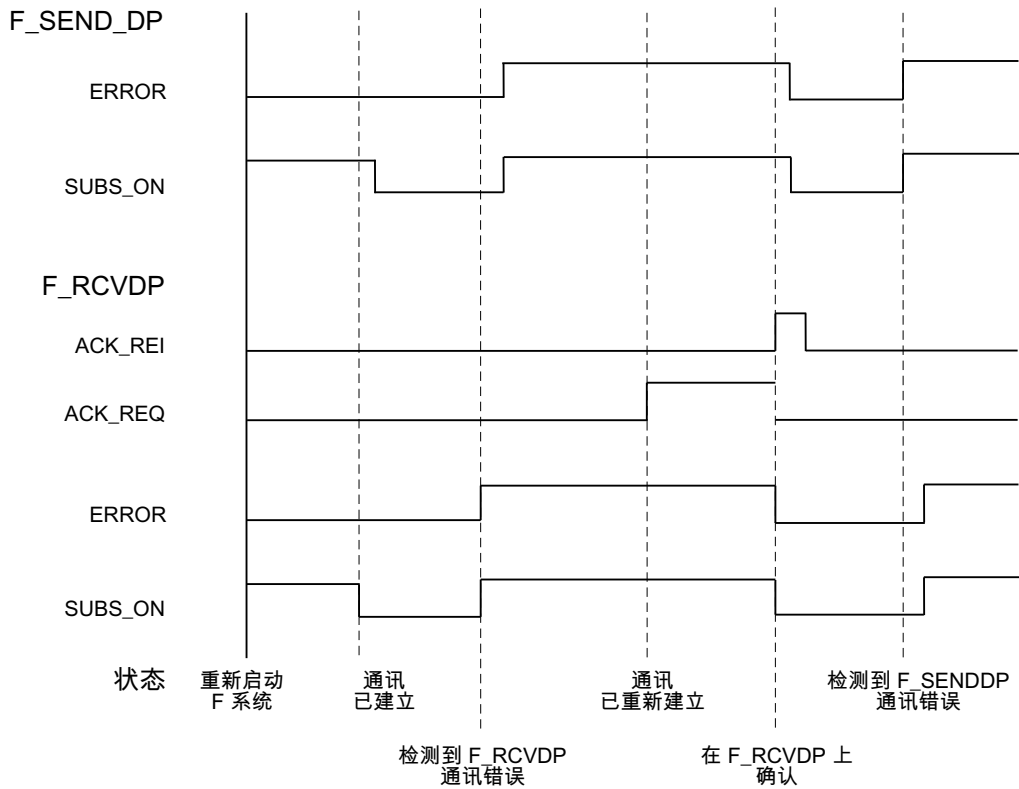
警告

为了进行用户确认，必须将 ACK_REI 输入与通过操作员输入生成的信号互连。
不允许与自动生成的信号进行互连。

请注意，如果已在通讯对 F_SENDDP 和 F_RCVDP 之间建立通讯，则在发生通讯错误时对 ERROR 输出 (1 = 通讯错误) 进行首次置位。如果启动发送和接收 F 系统后无法建立通讯，请检查安全相关的 CPU 与 CPU 通讯的组态、F_SENDDP 和 F_RCVDP 参数分配以及总线连接。通过评估 RETVAL14 和 RETVAL15 输出，也可找到发生错误的可能原因。

通常始终评估 RETVAL14 和 RETVAL15，因为两个输出中只有一个可以接收错误信息。

F_SENDDP/F_RCVDP 的时序图



输出 DIAG

此外，在两个 F 应用程序块 F_SENDDP 和 F_RCVDP 的输出 DIAG 处，为检修目的将提供有关发生的错误类型的非故障安全信息。

可以通过操作员监视和控制系统读取该信息，也可以在标准用户程序中评估该信息（如果适用）。直到在输入 ACK_REI 处进行确认后，才保存 DIAG 位。

F 应用程序块 F_SENDDP/F_RCVDP 中 DIAG 的结构

位号	F_SENDDP 和 F_RCVDP 的分配	问题的可能原因	补救措施
位 0	保留	-	-
位 1	保留	-	-
位 2	保留	-	-
位 3	保留	-	-

位号	F_SENDDP 和 F_RCVD 的分配	问题的可能原因	补救措施
位 4	超时（由 F_SENDDP/F_RCVD P 检测到）	至伙伴 F-CPU 的总线连接中有干扰。	检查总线连接并确保没有外部干扰源。
		F-CPU 和伙伴 F-CPU 的监视时间设置过低。	检查在两个 F-CPU 的 F_SENDDP 和 F_RCVD 处分配的监视时间参数 TIMEOUT。如有必要，请设置较高的值。重新编译安全程序。
		DP/DP 耦合器组态无效。	检查 DP/DP 耦合器组态。
		DP/DP 耦合器发生内部错误	更换 DP/DP 耦合器
		CP 处于 STOP 模式中，或者 CP 发生内部故障	将 CP 切换到 RUN 模式，检查 CP 的诊断缓冲区，并更换 CP（如有必要）
		F-CPU/伙伴 F-CPU 处于 STOP 模式，或者 F-CPU/伙伴 F-CPU 发生内部故障	将 F-CPU 切换到 RUN 模式，检查 F-CPU 的诊断缓冲区，并更换 F-CPU（如有必要）
位 5	顺序编号错误（由 F_SENDDP/F_RCVD P 检测到）	请参阅位 4 的说明	请参阅位 4 的说明
位 6	CRC 错误（由 F_SENDDP/F_RCVD P 识别）	请参阅位 4 的说明	请参阅位 4 的说明
位 7	保留	-	-

说明

在安全程序中无法访问输出 DIAG、RETVAL14 和 RETVAL15。

附加信息

可在“另请参阅”下提供的参考信息中找到有关对不同 F-CPU 上的安全程序之间的安全相关的通讯进行组态和编程的更多信息。

参见

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

安全相关通讯概述 (页 131)

组态地址区 (安全相关的主站与主站通讯) (页 134)

组态地址区 (安全相关的主站与智能从站通讯) (页 143)

组态地址区 (安全相关的智能从站与智能从站通讯) (页 154)

9.1.2.20 FB 225 "F_SENDS7" 和 FB 226 "F_RCVS7": 通过 S7 连接通讯

引言

使用 F_SENDS7 和 F_RCVS7 F 应用程序块, 通过 S7 连接进行故障安全数据的发送和接收。

说明

在 S7 Distributed Safety 中, 通常仅允许在工业以太网上使用 S7 连接!

可与以下 CPU 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-3 PN/DP (仅通过 CPU 的 PN 接口)
 - CPU 416F-2 固件版本 V4.0 及更高版本
-

F 应用程序块 F_SENDS7 的连接

	参数	数据类型	说明	缺省值
输入:	SEND_DB	BLOCK_DB	F 通讯 DB 的编号	0
	TIMEOUT	TIME	安全相关的通讯的监视时间 (以 ms 为单位) (请参阅《SIMATIC S7 中的安全工程》系统手册)	0 ms
	EN_SEND	BOOL	1 = 发送使能	1

	参数	数据类型	说明	缺省值
	ID	WORD	S7 连接的本地 ID (从 <i>NetPro</i> 中获得)	0
	R_ID	DWORD	F_SENDS7 和 F_RCVS7 之间明确的网络地址相关性	0
输出:	ERROR	BOOL	1 = 通讯错误	0
	SUBS_ON	BOOL	1 = 接收方输出故障安全值	1
	STAT_RC V	WORD	SFB/FB URCV (SFB 9/FB 9) 的错误代码 (有关错误代码的说明, 请参考 SFB 9 的在线帮助)	0
	STAT_SN D	WORD	SFB/FB USEND (SFB 8/FB 8) 的错误代码 (有关错误代码的说明, 请参考 SFB 8 的在线帮助)	0
	DIAG	BYTE	检修信息	0

F 应用程序块 F_RCVS7 的连接

	参数	数据类型	说明	缺省值
输入:	ACK_REI	BOOL	发生通讯错误后, 对发送数据的重新集成进行确认	0
	RCV_DB	BLOCK_D B	F 通讯 DB 的编号	0
	TIMEOUT	TIME	安全相关的通讯的监视时间 (以 ms 为单位) (请参阅《SIMATIC S7 中的安全工程》系统手册)	0 ms
	ID	WORD	S7 连接的本地 ID (从 <i>NetPro</i> 中获得)	0
	R_ID	DWORD	F_SENDS7 和 F_RCVS7 之间明确的网络地址相关性	0
输出:	ERROR	BOOL	1 = 通讯错误	0

	参数	数据类型	说明	缺省值
	SUBS_ON	BOOL	1 = 输出故障安全值	1
	ACK_REQ	BOOL	1 = 需要对发送数据的重新集成进行确认	0
	SENDMODE	BOOL	1 = 具有 F_SENDS7 的 F-CPU 处于取消激活的安全模式中	0
	STAT_RCV	WORD	SFB/FB URCV (SFB 9/FB 9) 的错误代码 (有关错误代码的说明, 请参考 SFB 9 的在线帮助)	0
	STAT_SND	WORD	SFB/FB USEND (SFB 8/FB 8) 的错误代码 (有关错误代码的说明, 请参考 SFB 8 的在线帮助)	0
	DIAG	BYTE	检修信息	0

工作原理

F_SENDS7 将包含在 F 通讯 DB 中的发送数据通过 S7 连接以故障安全的方式发送到关联 F_RCVS7 的 F 通讯 DB。

F 通讯 DB 是具有特殊属性的安全相关的 CPU 与 CPU 通讯的 F-DB。在『对通过 S7 连接的安全相关的 CPU 与 CPU 通讯进行编程』一章中说明了 F 通讯 DB 的属性、创建和编辑。

必须在 F 应用程序块 F_SENDS7 和 F_RCVS7 的输入 SEND_DB 和 RCV_DB 处指定 F 通讯 DB 的编号。

在 F_F_RCVS7 的输出 SENDMODE 处提供具有 F_SENDS7 的 F-CPU 的工作模式。如果具有 F_SENDS7 的 F-CPU 处于取消激活的安全模式, 则输出 SENDMODE = 1。

为了减少总线负载, 可临时关闭 F-CPU 之间的通讯。要执行该操作, 请将 F_SENDS7 的输入 EN_SEND 设置为“0” (缺省值 = “1”)。然后, 发送数据将不再发送到关联 F_RCVS7 的 F 通讯 DB, 并且在此期间接收方 F_RCVS7 将提供故障安全值 (缺省的 F 通讯 DB)。如果伙伴之间已建立通讯, 则将检测到通讯错误。

对于 F-CPU, 必须在 F_SENDS7 或 F_RCVS7 的输入 ID 处指定 S7 连接的本地 ID (从 *NetPro* 中的连接表中获得)。

F-CPU 之间的通讯是通过特殊安全协议在后台隐藏进行的。必须通过在 F_SENDS7 和 F_RCVS7 的 R_ID 输入处分配奇数, 以在一个 F-CPU 中的 F_SENDS7 和另一个 F-CPU 中的 F_RCVS7 之间定义通讯关联。关联的 F_SENDS7 和 F_RCVS7 接收相同的 R_ID 值。

**警告**

每个地址关联（输入参数 R_ID；数据类型：DWORD）的值都是用户定义的；但是，在网络中的所有安全相关的通讯连接中，它必须是唯一的。值 R_ID + 1 是内部分配的，一定不能使用。

调用 F 应用程序块时，必须为输入 ID 和 R_ID 提供常数值。在安全程序中，不允许在关联的背景数据块中进行直接读取或写入访问！

说明

每个 F_SENDS7 和 F_RCVS7 调用必须使用单独的背景数据块。不能将这些 F 应用程序块作为多重背景调用。

F_RCVS7 的输入和输出参数不能是 F 程序块的本地数据。

如果一个 F_RCVS7 或 F_RCVDP 调用的输入参数为实参，则该 F_RCVS7 或其它 F_RCVS7 的输出参数不能为实参。如果未遵守上述规定，F-CPU 会切换到 STOP。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”

启动特性

发送和接收 F 系统启动之后，必须首先在通讯对 F_SENDS7 和 F_RCVS7 之间建立通讯。在此期间，接收方 F_RCVS7 将提供故障安全值（其 F 通讯 DB 中的缺省值）。F_SENDS7 和 F_RCVS7 在输出 SUBS_ON 处发送信号 1 指示此情况。只要输出 SUBS_ON = 1，F_RCVS7 的输出 SENDMODE 便有缺省值 0 且不更新。

发生通讯错误时的行为

如果发生通讯错误，例如，由于测试值错误 (CRC) 或监视时间 TIMEOUT 结束，F_SENDS7 和 F_RCVS7 处的输出 ERROR 和 SUBS_ON 都将设置为 1。然后，接收方 F_RCVS7 将提供故障安全值（其 F 通讯 DB 中的缺省值）。输出 SUBS_ON = 1 时，输出 SENDMODE 不更新。

只有不再检测到通讯错误 (ACK_REQ = 1) 并确认了 F_RCVS7 的输入 ACK_REI 处的正沿时，才再次输出 F_SENDS7 的 F 通讯 DB 中存在的发送数据。

**警告**

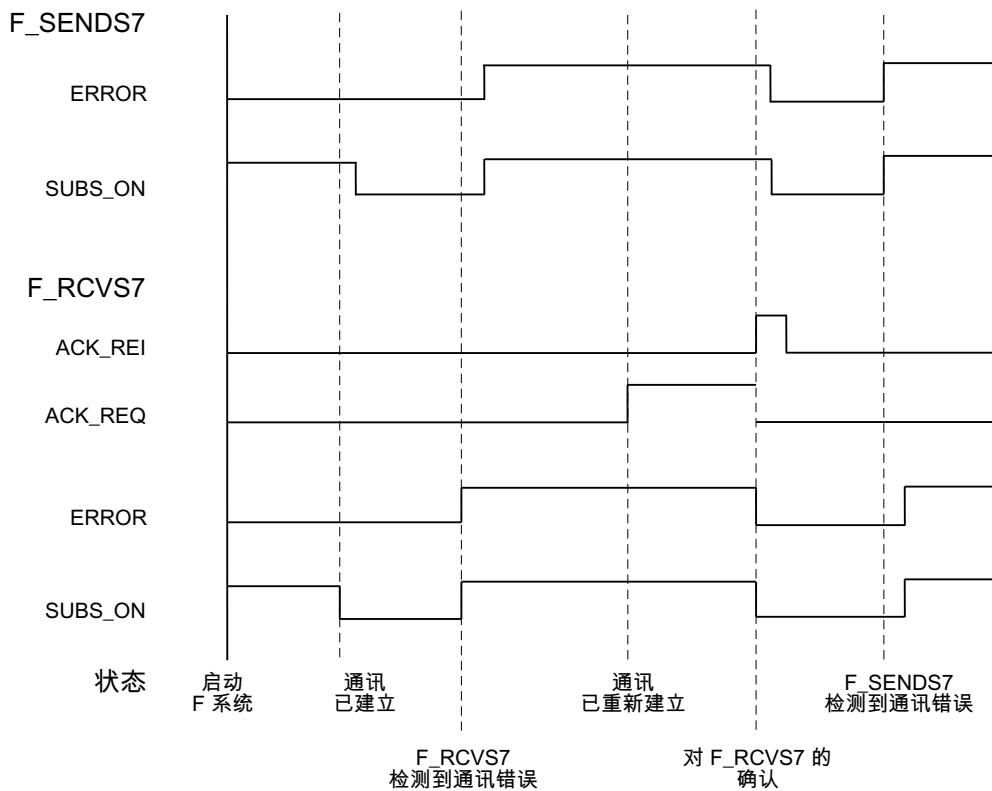
为了进行用户确认，必须将 ACK_REI 输入与通过操作员输入生成的信号互连。不允许与自动生成的信号进行互连。

请注意，发生通讯错误时，如果已在通讯对 F_SENDS7 和 F_RCVS7 之间建立通讯，则对 ERROR 输出（1 = 通讯错误）进行首次置位。如果启动发送和接收 F 系统后无法建立通讯，请检查安全相关的 CPU 与 CPU 通讯的组态、F_SENDS7 和 F_RCVS7 参数分配以及总线连接。通过评估 STAT_RCV 和 STAT_SND 输出，也可以找到发生错误的可能原因。

通常始终评估 STAT_RCV 和 STAT_SND，因为两个输出中只有一个可以接收错误信息。

如果在输出 DIAG 处设置 DIAG 位的某个位，还要检查发送方关联 F 通讯 DB 的长度和结构是否匹配。

F_SENDS7 和 F_RCVS7 的时序图



输出 DIAG

DIAG 输出将为检修目的提供与发生的通讯错误类型有关的非故障安全信息。可以通过操作员监视和控制系统读取该信息，也可以在标准用户程序中评估该信息（如果适用）。直到在关联 F_RCVS7 的输入 ACK_REI 处进行确认后，DIAG 位才被保存。

DIAG 的结构

位号	分配 F_SENDS7 和 F_RCVS7	问题的可能原因	补救措施
位 0	保留	-	-
位 1	保留	-	-
位 2	保留	-	-
位 3	保留	-	-
位 4	超时（由 F_SENDS7 和 F_RCVS7 检测）	至伙伴 F-CPU 的总线连接中有干扰	检查总线连接并确保没有外部干扰源。
		F-CPU 和伙伴 F-CPU 的监视时间设置过低	检查两个 F-CPU 的 F_SENDS7 和 F_RCVS7 处分配的监视时间参数 TIMEOUT。如有必要，请设置较高的值。重新编译安全程序。
		CP 处于 STOP 模式，或者 CP 发生内部故障	将 CP 切换到 RUN 模式 检查 CP 的诊断缓冲区 如有必要，请更换 CP
		F-CPU/伙伴 F-CPU 处于 STOP 模式，或者 F-CPU/伙伴 F-CPU 发生内部故障	将 F-CPU 切换到 RUN 模式 检查 F-CPU 的诊断缓冲区 如有必要，请更换 F-CPU
		通过 EN_SEND = 0 关闭通讯。	通过 EN_SEND = 1 在关联 F_SENDS7 处再次启用通讯
		S7 连接已更改，例如 CP 的 IP 地址已更改	重新编译安全程序并将其下载到 F-CPU
位 5	顺序编号（由 F_SENDS7 和 F_RCVS7 检测到）	请参阅位 4 的说明	请参阅位 4 的说明
位 6	CRC 错误（由 F_SENDS7 和 F_RCVS7 检测到）	请参阅位 4 的说明	请参阅位 4 的说明
位 7	保留	-	-

说明

不允许在安全程序中访问输出 DIAG、STAT_RCV 和 STAT_SND！

附加信息

在『另请参阅』下提供的参考信息中，可以找到有关通过 S7 连接对安全相关的通讯进行组态和编程的更多信息。

参见

在 DP 主站的 F-CPU 或 IO 控制器的安全程序中执行用户确认 (页 121)

在智能从站的 F-CPU 的安全程序中执行用户确认 (页 123)

安全相关通讯概述 (页 131)

用 S7 连接组态安全相关的通讯 (页 168)

9.1.2.21 FC 174 "F_SHL_W": 向左移 16 位

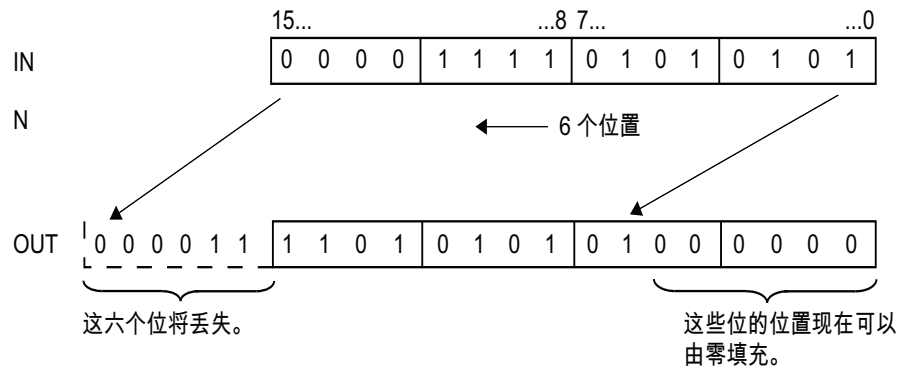
连接

	参数	数据类型	说明	缺省值
输入:	IN	WORD	移位的值	-
	N	INT	移位位数	-
输出:	OUT	WORD	移位操作的结果	-

工作原理

此 F 应用程序块将输入 IN 处的传送值的各位内容逐位向左移动。移位时空出来的各位用零填充。移位数 N 表示要移动的位数。在输出端 OUT 输出移位指令的结果。当 $15 < N \leq 255$ 时，输出 OUT 始终为 0。

注意：当 $N < 0$ 或 $N > 255$ 时，仅将输入 N 上传输值的低字节作为移位数。



9.1.2.22 FC 175 "F_SHR_W": 向右移 16 位

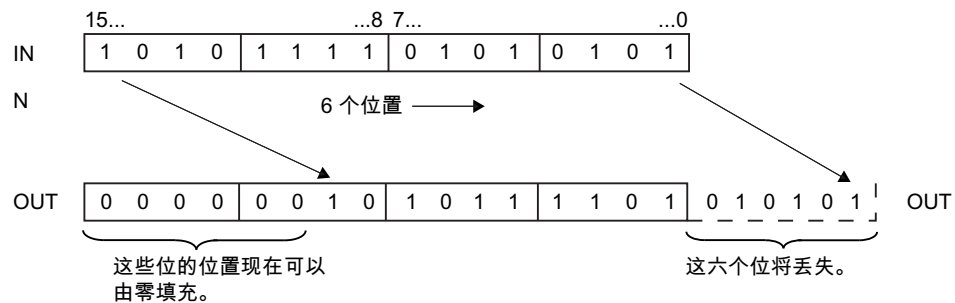
连接

	参数	数据类型	说明	缺省值
输入:	IN	WORD	移位的值	-
	N	INT	移位位数	-
输出:	OUT	WORD	移位操作的结果	-

工作原理

此 F 应用程序块将输入 IN 处的传送值的各位内容逐位向右移动。移位时空出来的各位用零填充。移位数 N 表示要移动的位数。在输出端 OUT 输出移位指令的结果。当 $15 < N \leq 255$ 时，输出 OUT 始终为 0。

注意：当 $N < 0$ 或 $N > 255$ 时，仅将输入 N 上传输值的低字节视为移位数。



9.1.2.23 FC 176 "F_BO_W": 将 16 位的 BOOL 数据类型值转换为一个 WORD 数据类型值

连接

	参数	数据类型	说明	缺省值
输入	IN0	BOOL	WORD 值的位 0	0
	IN1	BOOL	WORD 值的位 1	0
	...			
	IN15	BOOL	WORD 值的位 15	0
输出	OUT	WORD	WORD 值 (包括 IN0 至 IN15)	0

工作原理

此 F 应用程序块将输入 IN0 至 IN15 处的数据类型为 BOOL 的 16 个值转换为数据类型为 WORD 的一个值，并且将其送至输出 OUT 处。转换方式如下：如果输入 IN_i 处的值为 0 (或 1)，则 WORD 值的位 i 也相应设置为 0 (或 1)。

注意：要为输入 IN0 至 IN15 提供包含“0”和“1”的布尔常数，可使用具有完整路径的 DB 访问 (“F_GLOBDB”.RLO0 或“F_GLOBDB”.RLO1) 在 F 共享数据块中访问变量“RLO0”和“RLO1”。

9.1.2.24 FC 177 "F_W_BO": 将一个 WORD 数据类型值转换为 16 位的 BOOL 数据类型值

连接

	参数	数据类型	说明	缺省值
输入	IN	WORD	WORD 值	0
输出	OUT0	BOOL	WORD 值的位 0	0
	OUT1	BOOL	WORD 值的位 1	0
	...			
	OUT15	BOOL	WORD 值的位 15	0

工作原理

此 F 应用程序块将输入 IN 处的数据类型为 WORD 的值转换为数据类型为 BOOL 的 16 个值，并且将其送至输出 OUT0 至 OUT15 处。转换方式如下：如果 WORD 值的位 i 为 0 (或 1)，则输出 OUT_i 相应位也相应为 0 (或 1)。

9.1.2.25 FC 178“F_INT_WR”：将数据类型 INT 的值间接写入 F-DB

连接

	参数	数据类型	说明
输入	IN	INT	要写入 F-DB 的值
	ADDR_INT	POINTE R	F-DB 中 INT 区域的起始地址
	END_INT	POINTE R	F-DB 中 INT 区域的结束地址
	OFFS_INT	INT	INT 区域中的地址偏移量

工作原理

此 F 应用程序块将输入 IN 处给出的数据类型为 INT 的值写入通过 ADDR_INT 和 OFFS_INT 寻址的 F-DB 中的变量。

通过 ADDR_INT 和 OFFS_INT 寻址的变量的地址必须在地址 ADDR_INT 和 END_INT 定义的地址区域内。

如果 F-CPU 因诊断事件 ID 75E2 而切换到 STOP 模式，则需验证是否为以上原因。

使用 ADDR_INT 输入传送 F-DB 中数据类型为 INT 的变量区域的起始地址，向该 F-DB 中，写入输入 IN 处的值。用 OFFS_INT 输入传送该区域的地址偏移量。

ADDR_INT 或 END_INT 输入端传送的地址必须指向 F-DB 中的数据类型为 INT 的变量。ADDR_INT 和 END_INT 地址之间只允许数据类型为 INT 的变量。ADDR_INT 地址必须小于 END_INT 地址。如以下实例所示，ADDR_INT 和 END_INT 地址必须作为具有完整路径的“DBx.DBWy”进行传送，或以相应的符号表示方法进行传送。不允许以其它方式进行传送。

ADDR_INT、END_INT 和 OFFS_INT 的参数分配的实例

Address	Declaration	Name	Type	Initial Value	Comments
0.0	stat		STRUCT		
+0.0	stat	VAR_BOOL10	BOOL	FALSE	
+0.1	stat	VAR_BOOL11	BOOL	FALSE	
+0.2	stat	VAR_BOOL12	BOOL	FALSE	
+0.3	stat	VAR_BOOL13	BOOL	FALSE	
+2.0	stat	VAR_TIME10	TIME	T#0MS	
+6.0	stat	VAR_TIME11	TIME	T#0MS	
+10.0	stat	VAR_INT10	INT	0	<- ADDR_INT = "F-DB", VAR_INT10 Example 1
+12.0	stat	VAR_INT11	INT	0	
+14.0	stat	VAR_INT12	INT	0	
+16.0	stat	VAR_INT13	INT	0	<-OFFS_INT = 3
+18.0	stat	VAR_INT14	INT	0	
+20.0	stat	VAR_INT15	INT	0	<- END_INT = "F-DB", VAR_INT15
+22.0	stat	VAR_BOOL20	BOOL	FALSE	
+22.1	stat	VAR_BOOL21	BOOL	FALSE	
+22.2	stat	VAR_BOOL22	BOOL	FALSE	
+22.3	stat	VAR_BOOL23	BOOL	FALSE	
+24.0	stat	VAR_INT20	INT	0	<- ADDR_INT = "F-DB", VAR_INT20 <-OFFS_INT = 0 Example 2
+26.0	stat	VAR_INT21	INT	0	
+28.0	stat	VAR_INT22	INT	0	
+30.0	stat	VAR_INT23	INT	0	<- END_INT = "F-DB", VAR_INT23
+32.0	stat	VAR_INT30	INT	0	<- ADDR_INT = "F-DB", VAR_INT30 Example 3
+34.0	stat	VAR_INT31	INT	0	<-OFFS_INT = 1
+36.0	stat	VAR_INT32	INT	0	
+38.0	stat	VAR_INT33	INT	0	
+40.0	stat	VAR_INT34	INT	0	<- END_INT = "F-DB", VAR_INT34
+42.0	stat	VAR_TIME20	TIME	T#0MS	
-46.0	stat		END_STRUCT		

9.1.2.26 FC 179“F_INT_RD”： 从 F-DB 间接读取数据类型 INT 的值

连接

	参数	数据类型	说明
输入	ADDR_INT	POINTER	F-DB 中 INT 区域的起始地址
	END_INT	POINTER	F-DB 中 INT 区域的结束地址
	OFFS_INT	INT	INT 区域中的地址偏移量
输出	OUT	INT	要从 F-DB 读取的值

工作原理

此 F 应用程序块在 F-DB 中读取使用 ADDR_INT 和 OFFS_INT 寻址的数据类型 INT 的变量，并将其送至输出 OUT 处。

通过 ADDR_INT 和 OFFS_INT 寻址的变量的地址必须在地址 ADDR_INT 和 END_INT 定义的地址区域内。

如果 F-CPU 因诊断事件 ID 75E2 而切换到 STOP 模式，则需验证是否为以上原因。

使用 ADDR_INT 输入传送 F-DB 中具有数据类型 INT 的变量的区域的起始地址，从该地址处读取变量。用 OFFS_INT 输入传送该区域的地址偏移量。

ADDR_INT 或 END_INT 输入端传送的地址必须指向 F-DB 中的数据类型为 INT 的变量。ADDR_INT 和 END_INT 地址之间只允许数据类型为 INT 的变量。ADDR_INT 地址必须小于 END_INT 地址。

ADDR_INT 和 END_INT 地址必须作为具有完整路径的“DBx.DBWy”进行传送，或以相应的符号表示方法进行传送。不允许以其它方式进行传送。可以在“参阅”下提供的参考信息中找到 ADDR_INT、END_INT 和 OFFS_INT 的参数分配的实例。

参见

FC 178“F_INT_WR”： 将数据类型 INT 的值间接写入 F-DB (页 249)

9.1.3 F 系统块

功能

编译安全程序时，将自动添加 F 系统块，以从您创建的安全程序中创建可执行安全程序。

使用 F 系统块，将故障控制措施自动添加到安全程序，并执行其它安全相关的测试。

F 系统块的概述

可以使用以下 F 系统块：

- F_CTRL_1
- F_CTRL_2
- F_IO_BOI
- FSIO_BOI

9.1 Distributed Safety F 库 (V1)

- F_RTGCO2
- F_IO_CGP
- FSIO_CGP
- F_DIAG_N
- FISCA_I
- FICTU
- FICTD
- FICTUD
- FITP
- FITON
- FITOF
- FIACK_OP
- FI2HAND
- FIMUTING
- FI1oo2DI
- FI2H_EN
- FIMUT_P
- FIACK_GL
- FISHL_W
- FISHR_W
- FIBO_W
- FIW_BO
- FIINT_WR
- FIINT_RD

当编译安全程序时，系统将自动添加 F 系统块，并将其存储在为“F 功能块”预留的编号范围中，以从已编程的安全程序中创建可执行的安全程序。

说明

不得从 F-PB/F-FB/F-FC 中的 *F* 系统块的块文件夹插入 F 系统块。同样，不得修改（重命名）或删除 *Distributed Safety* F 库 (V1) 或用户项目块文件夹中的 F 系统块。

参见

组态概述 (页 25)

9.1.4 F 共享 DB

功能

F 共享数据块是一个故障安全块，其中包含 F 系统所需的安全程序的所有共享数据，以及附加信息。在 *HW Config* 中保存并编译硬件配置时，将自动插入并扩展 F 共享 DB。

使用 F 共享 DB 的符号名（即，F_GLOBDB），可以在标准用户程序中评估安全程序的某些数据。



警告

不得将 F 共享 DB 从一个安全程序复制到另一个安全程序（例外：复制整个 S7 程序）。

参见

数据从安全程序传送到标准用户程序 (页 127)

数据从标准用户程序传送到安全程序 (页 129)

9.1.5 自定义 F 库

引言

对于 *S7 Distributed Safety*，您可以选择创建自己的 F 库。

如何创建 F 库

请按照以下步骤创建自己的 F 库：

1. 在 *SIMATIC 管理器* 中，选择 **文件 (File) > 新建 (New)**。
2. 在“库” (Libraries) 选项卡页中，从“类型” (Type) 列表中选择“F 库” (F-Library)。
3. 为 F 库分配名称。
4. 指定“文件路径”。
5. 单击“确定” (OK) 关闭对话框。已创建 F 库。

使用用户创建的 F 库

要使用用户创建的 F 库中的 F-FB/F-FC/应用程序模板，必须在用于创建 F-FB、F-FC 或应用程序模板的 PC 或编程设备上安装相同版本的 *S7 Distributed Safety*。

必须检查现有的用户创建的 F 库是否仍然最新。如有必要，必须用较新的、可用的版本替换用户创建的 F 库。*S7 Distributed Safety* 不检查用户创建的 F 库中的 F-FB/F-FC 版本。编译安全程序时，也无法用该 F 库的较新的版本中相应的 F-FB/F-FC 自动替换用户创建的 F 库中的 F-FB/F-FC。如有必要，将较新的版本中的 F-FB/F-FC 从用户创建的 F 库复制到安全程序的块文件夹中。

不能将 *Distributed Safety* F 库 (V1) 的 F 应用程序块的符号名用于用户创建的 F-FB、F-FC 和块。

用户创建的 F 库中的 F-FB/F-FC 的处理方式与 *Distributed Safety* F 库 (V1) 中的相同。

删除 S7 Distributed Safety

删除 *S7 Distributed Safety* 时，保留用户创建的 F 库。

编译和调试安全程序

10.1 “Safety Program”（安全程序）对话框

引言

“安全程序”(Safety Program) 对话框提供了有关安全程序的信息，并包含了可用于编辑安全程序的重要功能。

说明

在 *SIMATIC 管理器* 和“安全程序”(Safety Program) 对话框中，用黄色高亮显示 F 块。

- 在 *SIMATIC 管理器* 中，知识保护块也用锁定符号表示。

安全程序成功编译后，安全程序的所有块都是知识保护块。但是您创建的任何 F 块（F-PB、F-FB、F-FC、F-DB）除外，并且无法为其指定知识保护。

- 在“安全程序”(Safety Program) 对话框中，具有 F 属性的 F 块也在块符号中用“F”表示。

安全程序成功编译后，仅安全程序块具有 F 属性。

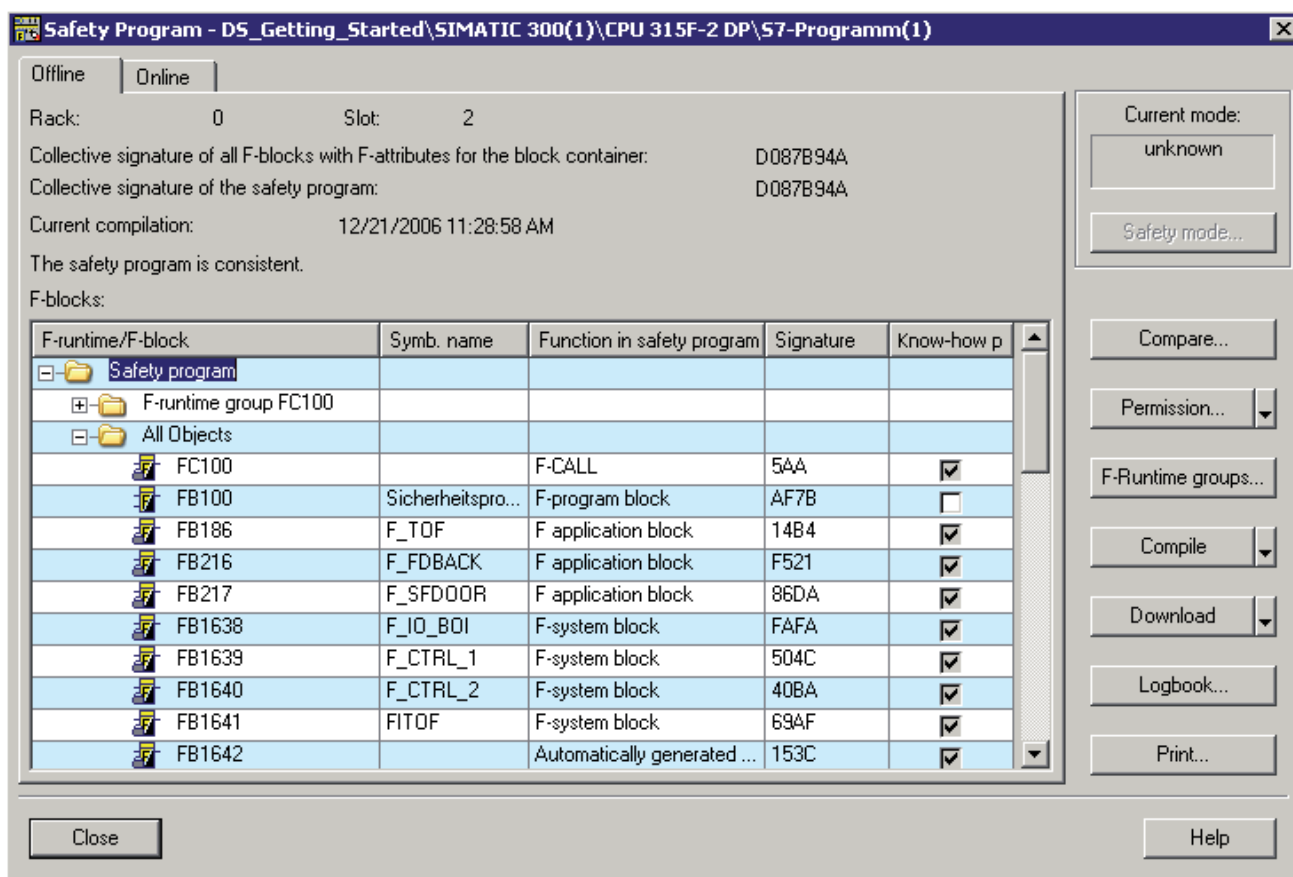
调用“安全程序”(Safety Program) 对话框的步骤

1. 选择正确的 F-CPU 或为其指定的 S7 程序。

10.1 “Safety Program” (安全程序) 对话框

2. 在 *SIMATIC* 管理器中，选择选项 (Options) > 编辑安全程序 (Edit safety program) 菜单命令，或在 *STEP 7*V5.4 及更高版本中，选择工具栏中的相应图标。

将显示“安全程序”(Safety Program) 对话框。



有关安全程序的 F 块的信息

块文件夹的所有 F 块都显示在此对话框中。使用“离线”(Offline)、“在线”(Online) 选项卡选择要列出离线还是在线块文件夹的 F 块。

- “F 运行组...” (F-Runtime Group...) 文件夹包含安全程序的 F 运行组结构。仅为包含一个现有的 F 共享 DB 和至少一个定义的 F 运行组的离线安全程序显示 F 运行组 (F-Runtime Groups) 视图。F 运行组文件夹名称的构成格式如下：“F 运行组”+ F 运行组的 F-CALL 名称

以下各项均显示在“F 运行组...”文件夹中：所有 F-FB、F-FC、F 应用程序块、背景数据块、F-DB、F-CALL，以及各个 F 运行组用于 F 运行系统通讯的 DB（如果适用）。

“F 运行组”文件夹还包含一个“F-I/O DBs”文件夹。此文件夹包含从 F 运行组寻址的所有 F-I/O DB。

说明

如果不存在一致的安全程序，则“F 运行组...” (F-Runtime Group...) 和“F-I/O DBs”文件夹的内容就不完整。

- “完整的”文件夹包含离线块文件夹的所有 F 块。

将显示每个 F 块的以下属性：

- 块标识（类型/编号），具有/不具有 F 属性（该 F 属性在块符号中具有/不具有知识保护）
 - 符号块名称
 - 安全程序中的功能
 - F 块的签名
 - 已选定知识保护（对于离线安全程序）
-

说明

不得更改 Distributed Safety F 库(V1) 中的和自动生成的 F 块的符号名。 这些 F 块的符号名必须始终与标题名匹配；否则，安全程序编译操作将中止。

有关安全程序的信息

将显示以下有关安全程序的信息：

- 上次编译操作的日期和编译时计算的集体签名：
 - “块文件夹中所有具有 F 属性的 F 块的集体签名”
 - “安全程序的集体签名”： 在安全程序的 F 运行组中调用的贯穿所有 F 块的值
- 有关安全程序状态的信息。 有以下三种可能的状态：
 - 一致
 - 不一致
 - 已修改

10.1 “Safety Program” (安全程序) 对话框

- “当前模式：” 包含有关以下内容的信息：
 - 安全模式是否已“激活”或
 - 安全模式是否已“取消激活”
 - “CPU 是否处于 STOP 模式”
 - 安全模式的状态是否为“未知”，即是否无法确定，或
 - 是否未调用 F 运行组： 没有为至少一个 F 运行组调用关联 F-CALL（例如，因为在 OB [OB35]、FB 或 FC 中没有编写 F-CALL 程序）。

说明

如果“当前模式”下的文本括在方括号中，如 [abc]，这说明在线和离线的安全程序的集体签名和/或密码不匹配。这表示发生了以下某种情况：

- 下载离线安全程序后，对其进行了修改。
- 对错误的 F-CPU 进行了寻址。您可以根据块文件夹中所有具有 F 属性的 F 块的在线集体签名来验证后者。

单击块列表的标题行，对列表进行排序。

请注意，如果编程设备或 PC 未直接连接至 F-CPU/智能 DP 从站，并且已打开此 F-CPU 上的安全程序的安全程序 (Safety Program) 对话框，则当前的安全模式显示可能不是最新的。在这种情况下，会为该模式输出“未知”。

解决方案： 将编程设备或 PC 直接连接至应打开其安全程序 (Safety Program) 对话框的 F-CPU。

要记录安全程序，请参阅『打印安全程序的项目数据』一章。

参见

安全程序状态 (页 259)

打印输出项目数据 (页 281)

10.2 安全程序状态

可能的状态

安全程序可能具有以下状态：

- 一致

块文件夹中所有具有 F 属性的 F 块的集体签名与安全程序的集体签名相同。

未在安全程序的 F 运行组中调用的 F 块显示在“安全程序”(Safety Program) 对话框中，但在块符号中没有 F 属性，并且不包括在集体签名的计算中。编译安全程序时，系统将通知您块文件夹中未使用的 F 块。

为了使得程序更加清晰，建议您删除未使用的 F 块。另一方面，可能需要在安全程序中组态尚未寻址的 F-I/O，并且仍需要编译一致的安全程序。安全程序必须一致才能被验收。

- 不一致

块文件夹中所有具有 F 属性的 F 块的集体签名与安全程序的集体签名不同。例如，由于复制了一个具有 F 属性的 F 块，但是未在安全程序的 F 运行组中调用复制的此具有 F 属性的 F 块。

如果在 F-CPU 中安全程序的状态为“不一致”，则当 F-CPU 支持此 ID 时，F-CPU 将无法启动（请参阅各个 F-CPU 的产品信息）。要获得一致的安全程序，必须重新生成安全程序。

- 已修改

由于 F-CPU 和 F I/O 的安全程序或安全相关参数已被更改，安全程序的集体签名被设置为“0”。

块文件夹中所有具有 F 属性的 F 块的集体签名与安全程序的集体签名不同。

如果在 F-CPU 中安全程序的状态为“已修改”，则当 F-CPU 支持此 ID 时，F-CPU 将无法启动（请参阅各个 F-CPU 的产品信息）。如果 F-CPU 不支持此 ID，则在启用安全程序的情况下执行状态为“已修改”的安全程序可能会导致 F-CPU 切换到 STOP。

要获得一致的安全程序，必须重新生成安全程序。

参见

系统验收测试概述 (页 297)

10.3 编译安全程序

说明

编译安全程序之前，关闭 *LAD/FBD 编辑器*、*显示 S7 参考数据和检查块一致性应用程序*，以及符号表。

编译安全程序的步骤

1. 选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 *SIMATIC 管理器* 中，选择 **选项 (Options) > 编辑安全程序 (Edit Safety Program)** 菜单命令。

将显示“安全程序”(Safety Program) 对话框。

3. 激活“编译”(Compile) 按钮。

现在将编译安全程序。

此外，还可以使用 *SIMATIC 管理器* 中的“检查块的一致性”功能来编译安全程序（请参阅『创建和编辑 F-FB/F-FC』一章中的“检查块的一致性”功能）。

编译安全程序

编译仅适用于有效的运行组。即，F 运行组中不会丢失您在“F 运行组”(F-Runtime Groups) 对话框中定义的所有 F 块。

编译安全程序时，将执行一致性检查。即，将针对错误和您在块文件夹中创建但没有在 F 运行组中使用的 F 块，检查安全程序。所有出错消息将在出错窗口中输出。

只有是安全程序的一部分的 F 块才能接收 F 属性。编译操作成功完成后，块文件夹始终包含一致的安全程序，该安全程序完全由具有 F 属性的 F 块组成。

离线块文件夹可包含不具有 F 属性的 F 块。

成功检查一致性后，将添加所需的其它 F 系统块和自动生成的 F 块。

系统会将编译操作期间标识的错误消息和警告收集起来，并在完成编译时在对话框中输出。警告将被特别标记出来。

使用“编译”(Compile) 按钮上的下拉箭头，您可以：

- 查看和保存最新编译过程的记录
- 启用“检查标准中的访问”(Check for accesses from standard)
- 启用或禁用“更新参考数据”(Update reference data)

**警告**

不得在 F-PB/F-FB/F-FC 中插入 *Distributed Safety* F 库 (V1) 的 F 系统块文件夹中 F 系统块。同样：

- 在 *Distributed Safety* F 库(V1) 中，不得：
- 在 *Distributed Safety* F 库(V1) 或用户项目（离线）的块文件夹中插入、删除或重命名 F 系统块。这样可能导致在下次编译操作期间出现错误。
- 在 *Distributed Safety* F 库(V1) 或用户项目（在线）的块文件夹中插入、删除或重命名 F 系统块。这样可能导致 F-CPU 切换到 STOP 模式。

根据干涉的程度，可能无法执行已编译的安全程序。

在这种情况下，必须删除所有自动添加的 F 块（即，*SIMATIC* 管理器中使用 F-STL 编程语言创建或由编写者 FALGxxxx 创建的、以黄色符号指示的所有 F 块，以及 F 共享 DB）；然后必须执行以下操作：

- 将所有块从 *Distributed Safety* F 库 (V1) 的 F 应用程序块文件夹中复制到用户项目。
- 在 *HW Config* 中保存并编译
- 定义 F 运行组
- 编译完整的安全程序。

“检查标准程序中的访问”

将检查以下情况：

- 标准用户程序中的 OB、FB 和 FC 是否正通过具有完整资格的 DB 访问写入安全程序的 F-DB。
- 标准用户程序中的 OB、FB 和 FC 是否正通过过程映像访问或直接 I/O 访问写入 F-I/O 的地址区。
- 是否在标准用户程序的 OB、FB 和 FC 中调用 F 块。
- F 块中的时钟存储器是否是读取访问。
(您已在 *HW Config* 的 F-CPU 的组态过程中，在 F-CPU 对象属性对话框中定义了时钟存储器。)

结果显示在消息窗口中。

说明

请注意，上述检查并不彻底，例如确定是否从标准用户程序中对 F-DB 进行写访问的检查，当在标准用户程序中进行间接寻址或对 F-DB 进行具有部分资格的访问时，该检查便不会成功。

“更新参考数据”

可以在编译操作末尾禁用参考数据更新。这样可以缩短编译完整的安全程序所需的时间。

注意：如果禁用了参考数据更新，参考数据中显示的程序结构可能不正确。

默认情况下，将启用参考数据更新。

此设置应用于当前 Windows 用户。

参见

创建和编辑 F-FB/F-FC (页 83)

10.4 下载安全程序

引言

编译安全程序后，可将其下载到 F-CPU。有以下几种选择：

- 在 STOP 模式下，在“安全程序”(Safety Program) 对话框中下载整个安全程序。这是推荐的下载一致安全程序的方法。
- 在 STOP 模式下，在“安全程序”(Safety Program) 对话框中下载安全程序的更改
- 在 *SIMATIC 管理器* 或 *FBD/LAD 编辑器* 中下载各个 F 块

在“安全程序”(Safety Program) 对话框中将整个安全程序下载到 F-CPU 的步骤

1. 选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 *SIMATIC 管理器* 中，选择 **选项 (Options) > 编辑安全程序 (Edit Safety Program)** 菜单命令。

将显示“安全程序”(Safety Program) 对话框。

3. 激活“下载”(Download) 按钮。

标识所有属于安全程序的具有 F 属性的 F 块，并将其下载到 F-CPU。

系统将显示一个提示，为您提供除下载除安全程序外，用于下载标准用户程序的选项（如果已经启用此提示）。

如果安全程序已被修改或不一致，则系统将通知您选择生成（编译）一致的安全程序。

4. 确认指示 F-CPU 将停止的提示。

说明

要下载整个安全程序，F-CPU 必须处于 STOP 模式。

如果仅下载 F 块，则不会下载在其中调用 F-CALL 块的块（例如，循环中断 OB35）。然后必须以下载标准程序的相同方式单独下载这些 OB。

说明

在“安全程序”(Safety Program) 对话框中下载安全程序时，将对安全程序中所有具有 F 属性的 F 块自动执行在线/离线比较。在 F-CPU 中删除所有不具有 F 属性的 F 块。现在，F-CPU 包含与离线块文件夹完全相同的具有 F 属性的 F 块。

5. 在“安全程序”(Safety Program) 对话框中，依次选择“离线”(Offline) 和“在线”(Online) 选项卡，检查在线和离线块文件夹中所有具有 F 属性的 F 块的集体签名是否匹配。如果匹配，则说明已成功下载。如果不匹配，则需要重新下载。
6. 要激活安全模式，请将 F-CPU 从 STOP 模式切换到 RUN 模式。

说明

如果下载操作被中止，则必须重复下载步骤（第 3 步），并重新检查在线和离线块文件夹中所有具有 F 属性的 F 块的集体签名（第 5 步）。

在“安全程序”(Safety Program) 对话框中下载安全程序更改的操作步骤

1. 选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 SIMATIC 管理器中，选择选项 (Options) > 编辑安全程序 (Edit Safety Program) 菜单命令。
将显示“安全程序”(Safety Program) 对话框。
3. 在“下载”(Download) 按钮上单击下拉箭头“下载更改”(Download Changes)。

标识安全程序中所有具有 F 属性的新的和更改过的 F 块，将其下载到 F-CPU。

剩余的操作步骤与在“安全程序”(Safety Program) 对话框中下载整个安全程序相同（请参阅上文）。

说明

请注意，下载安全程序的更改仅用于调试阶段。对安全程序进行验收测试之前，必须将完整的安全程序下载到 F-CPU。如果上述操作失败，则可能导致块文件夹中 F 块的在线和离线时间戳不同。

将安全程序下载到编程设备或 PC

说明

原则上，可以将安全程序从 F-CPU 下载到编程设备或 PC。但是，请注意由于 F-CPU 中不保存任何符号信息，因此安全程序中使用的所有符号都将被删除，且无法重新创建。仅当使用离线项目时才可使用符号。

将安全程序上传到编程设备或 PC 后，只要没有修改安全程序，便可再次将其下载到 F-CPU 且无需重复验收测试。再次下载到 F-CPU 的安全程序只能在以下情况下执行：

- F-CPU 在将安全程序上传到编程设备或 PC 之前未执行安全程序。
- 安全相关的通讯的硬件配置已被更改（请参阅『对通讯进行组态和编程』一章）。

说明

如果安全程序已被更改或已在 F-CPU 中执行，则必须在将**完整**的安全程序再次下载到 F-CPU 之前执行以下操作：

1. 从块文件夹中删除所有 F 块的背景数据块
2. 从“Distributed Safety”库 (V1) 或从离线块文件夹的自定义 F 库中重新插入安全程序内使用所有 F 块，这样将覆盖现有的 F 块
3. 为“指针”数据类型的 F 块的参数重新分配常数（仅 F 块 F_INT_WR、F_INT_RD 需要）
4. 重新编译安全程序。这样将重新创建删除的背景数据块。

如果不执行这些操作，F-CPU 可能会切换到 STOP 模式。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序：内部 CPU 故障；内部错误信息：404”



对安全程序的修改导致集体签名被更改，因此，可能需要进行新的验收测试。

下载到 S7-PLCSIM

可以使用 STEP 7 的 S7-PLCSIM 功能（硬件模拟）来测试安全程序。

下载到 S7-PLCSIM 的要求

- 在编程设备或 PC 上安装了 S7-PLCSIM V5.3（或更高版本）选件包。
- 对安装了 Distributed Safety F 库(V1) 的目录具有写授权。
- S7-PLCSIM 处于激活状态。要激活 S7-PLCSIM，请在 *SIMATIC 管理器* 中选择 **选项 (Options) > 模拟模块 (Simulate Modules)**。

将启动 S7-PLCSIM 应用程序，并显示“CPU”子窗口。

- 下载具有 F-CPU 的硬件配置。要下载此硬件配置，请打开 *HW Config* 并下载所需的组态，下载方式与将其下载到真实的 CPU 相同。
- 安全程序是一致的。

下载到 S7-PLCSIM 的操作步骤

1. 选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 *SIMATIC 管理器* 中，选择 **选项 (Options) > 编辑安全程序 (Edit Safety Program)** 菜单命令。

将显示“安全程序”(Safety Program) 对话框。

3. 在“安全程序”(Safety Program) 对话框中，按“下载”(Download) 按钮。
将标识所有属于安全程序的具有 F 属性的 F 块，并将其下载到 S7-PLCSIM。
4. 确认指示 F-CPU 将停止的提示。

说明

S7 Distributed Safety 自动确定目标设备是“真实的”F-CPU 还是 S7-PLCSIM。如果目标设备是 S7-PLCSIM，则可将特殊模拟块（F 系统块）从 *S7 Distributed Safety F 库 (V1)* 自动下载到 S7-PLCSIM。

下载到 S7-PLCSIM 后，离线安全程序未更改且一致。所有具有 F 属性的 F 块的集体签名将不再与 S7-PLCSIM 中的集体签名匹配。

为支持 S7-PLCSIM，离线安全程序未更改，因此在下载到 S7-PLCSIM 后，也可将其下载到 F-CPU。要将安全程序下载到 F-CPU，只需取消激活 S7-PLCSIM 即可。

5. 每次 S7-PLCSIM 处于 STOP 模式后，您都必须将安全程序重新下载到 S7-PLCSIM。
也可以将安全程序的更改下载到 S7-PLCSIM（请参阅上文）。

在 SIMATIC 管理器或 FBD/LAD 编辑器中下载

使用标准的 *STEP 7* 工具可将 F 块和标准块同时下载到 F-CPU。但是，开始下载 F 块之前，系统会立即执行检查以确定 F-CPU 是否处于 STOP 模式或取消激活的安全模式。如果不是，您可选择切换到取消激活的安全模式，或将 F-CPU 置于 STOP 模式。

请注意，下载各个 F 块时，不能保证 F-CPU 中安全程序的一致性。因此，请在 F-CPU 处于 STOP 模式的情况下使用“安全程序”(Safety Program) 对话框进行下载，以确保安全程序的一致性。

说明

如果在 F-CPU 启动过程中 *S7 Distributed Safety* 检测到不一致的安全程序，则当 F-CPU 支持此检测功能时 F-CPU 将无法启动（请参阅特定 F-CPU 的产品信息）。然后，以下诊断事件将被输入到 F-CPU 的诊断缓冲区中：

- “安全程序不一致”

如果 F-CPU 不支持此检测功能，则在启用了安全模式的情况下执行不一致的安全程序时，F-CPU 可能会切换到 STOP 模式。然后以下诊断事件之一将被输入到 F-CPU 的诊断缓冲区中：

- “数据在输出到 F-I/O 之前在安全程序中遭到破坏”
- “数据在输出到伙伴 F-CPU 之前在安全程序中遭到破坏”
- “安全程序： 内部 CPU 故障； 内部错误信息： 404”

尽管在 *SIMATIC 管理器*或 *FBD/LAD 编辑器*中可以将安全程序下载到 S7-PLCSIM，但是不会自动下载任何模拟块，因此安全程序不能运行。在取消激活的安全模式下，在 *SIMATIC 管理器*或 *FBD/LAD 编辑器*中将各个 F 块下载到 S7 PLCSIM 仅用于测试性操作。



如果在 *SIMATIC 管理器*或 *FBD/LAD 编辑器*中下载 F 块，必须确保在块文件夹中没有未使用的 F-CALL。如果始终在“安全程序”(Safety Program) 对话框中下载安全程序，则所有未调用的 F 块（包含未使用的 F-CALL 块）会自动删除。

在 SIMATIC 管理器或 FBD/LAD 编辑器中下载 F 块的规则

下载 F 块时应该遵守以下规则：

- 只有在取消激活的安全模式下或 F-CPU 处于 STOP 模式时，才可以下载。
- F 块只能下载到已使用“安全程序”(Safety Program) 对话框下载安全程序的 F-CPU。
- 安全程序的离线密码和在线密码必须匹配。
- 只有通过使用“安全程序”(Safety Program) 对话框下载安全程序，才可在 F-CPU 中激活对安全程序密码的更改（“安全程序”[Safety Program] 对话框中的“许可”[Permission] 按钮）。
- 仅允许将离线安全程序作为源程序使用。

因此，第一次下载安全程序时以及更改安全程序的密码之后，必须使用“安全程序”(Safety Program) 对话框下载安全程序。

如果不能下载 F 块（因为 F-CPU 处于安全模式，或因为没有输入安全程序的密码或输入的密码错误），则系统会提示您选择继续下载剩余的标准块。

参见

测试安全程序 (页 291)

10.5 安全程序的工作存储器要求

估计

您可按以下方法估计安全程序的工作存储器要求：

安全程序的工作存储器要求

- F 系统块 F_CTRL_1、F_CTRL_2、F_IO_CGP/F_IO_BOI 和 F_DIAG_N 需要 31 KB
- + F 系统块 F_RTGCO2 需要 4.3 KB（仅适用于 F 运行组通讯）
 - + $4.5 \times$ 所有 F-FB/F-FC/F-PB 工作存储器要求
 - + $4.5 \times$ 使用的所有 F 块
（除 F_SENDDP、F_RCVDP、F_SENDS7 和 F_RCVS7 之外）的工作存储器要求
 - + 使用的 F_SENDDP 和 F_RCVDP F 应用程序块的工作存储器要求（每个 4.4 KB）
 - + 使用的 F_SENDS7 和 F_RCVS7 F 应用程序块的工作存储器要求（每个 9.5 KB）

数据的工作存储器要求

5 × 所有 F-DB（包含 F 通讯 DB，但不包含 F 运行组通讯 DB）和 F-PB/F-FB 的 I-DB 的工作存储器要求

- + 24 × 所有 F 运行组通讯 DB 的工作存储器要求
- + 2.3 × 所有 F 应用程序块（除 F_SENDDP、F_RCVDP、F_SENDS7 和 F_RCVS7 之外）的 I-DB 的工作存储器要求
- + 所有 F 应用程序块 F_SENDDP (0.2 KB)、F_RCVDP (0.3 KB)、F_SENDS7 (0.6 KB) 和 F_RCVS7 (1.0 KB) 的 I-DB 的工作存储器要求。
- + 每个 F-FC（包括类型为 FC 的 F 应用程序块）占 0.7 KB
- + 每个 F-I/O（用于 F-I/O DB 等）占 0.7 KB
- + 4.5 KB

自动生成的 F 块的块大小

要确保自动生成的 F 块未超出特定 F-CPU 中最大可能的容量，请遵守以下规则：

- F-FB/F-FC/F-PB 不应超出 FB 或 FC 最大容量的 25%（请参阅*所用 F-CPU 的手册中的技术规范*）。
- F-FB/F-FC/F-PB 必须符合以下要求：

2 × 数据类型为 BOOL 的所有参数或静态数据的数目

- + 4 × 数据类型为 INT/WORD 的所有参数或静态数据的数目
- + 6 × 数据类型为 TIME 的所有参数或静态数据的数目
- + 36

< 数据块的最大容量（以字节为单位）（请参阅*所用 F-CPU 的手册中的技术规范*）

- F-DB 必须符合以下要求：

2 × 数据类型为 BOOL 的 F-DB 的所有变量的数目

+ 4 × 数据类型为 INT/WORD 的 F-DB 的所有变量的数目

+ 6 × 数据类型为 TIME 的 F-DB 的所有变量的数目

+ 36

< 数据块的最大容量（以字节为单位）

（请参阅所用 *F-CPU* 的手册中的技术规范）

如果在将安全程序下载到 F-CPU 时收到消息“不能复制块 x”(Block x could not be copied)，请检查是否满足这些条件。如有必要，请减少以下各项：

- F-FB/F-FC/F-PB 的大小
- F-FB/F-FC/F-PB 的参数和静态数据的数目
- F-DB 的变量的数目
- 块的数目。不得超出 F-CPU 的最大块限制（请参阅所用 *F-CPU* 的手册中的技术规范）。

10.6 通过程序标识对安全程序和保护进行功能测试

进行完整的功能测试或对更改进行测试

创建安全程序后，必须按照自动化任务执行完整的功能测试。

对于已经过完整功能测试的安全程序所做的更改，仅需测试更改部分。

使用编程设备或 PC 将安全程序传送到 F-CPU

已插入存储卡（闪存卡或 MMC）的 F-CPU

将安全程序从编程设备或 PC 传送至以下设备时会应用下列警告：

- 已插入闪存卡的 F-CPU（例如，CPU 416F-2）
- 具有 MMC 的 F-CPU
（例如，CPU 317F-2 DP、CPU 315F-2 PN/DP 或 IM 151-7 F-CPU）

 **警告**

如果未在目标 F-CPU 中对安全程序执行功能测试，则使用**编程设备或 PC** 将安全程序传送到 F-CPU 时，必须遵循以下操作步骤，以确保 F-CPU 不包含“旧的”安全程序：

- 对于具有 MMC 的 F-CPU：在“安全程序”(Safety Program) 对话框中将安全程序下载到 F-CPU。
- 对于已插入闪存卡的 F-CPU：在“将用户程序下载到存储卡”(Download User Program to Memory Card) 对话框中将安全程序下载到 F-CPU。
- 执行程序标识（即，检查以确定在线和离线块文件夹中所有具有 F 属性的 F 块的集体签名是否匹配）。
- 使用模式选择器或通过编程设备/PC 对 F-CPU 执行存储器复位。一旦删除工作存储器，便会再次从装载存储器（F-CPU 3xxF 和 IM 151-7 F-CPU 的存储卡 MMC 或 F-CPU 4xxF 的闪存卡）中传送安全程序。

 **警告**

如果一台**编程设备或 PC** 通过网络（例如 MPI）可以访问**多个 F-CPU**，则必须采取以下措施以确保将安全程序下载到正确的 F-CPU：

对于每个 F-CPU 都使用特定的密码，例如 F-CPU 的统一密码再加上各自的 MPI 地址作为扩展：“Password_8”。


请注意以下几点：


- 第一次为 F-CPU 分配密码时，必须使用点对点连接（与第一次为 F-CPU 分配 MPI 地址相似）。
- 将安全程序下载到没有获得通过 F-CPU 密码获得访问授权的 F-CPU 前，必须首先取消对所有其它 F-CPU 的现有访问授权。

未插入闪存卡的 F-CPU

将安全程序从编程设备或 PC 传送到以下设备时会应用下列警告：

- 未插入闪存卡的 F-CPU（例如，CPU 416F-2）

 警告
<p>如果未在目标 F-CPU 中对安全程序执行功能测试，则使用编程设备或 PC 将安全程序传送到 F-CPU 时，必须遵循以下操作步骤，以确保 F-CPU 不包含“旧的”安全程序：</p> <ul style="list-style-type: none">• 使用模式选择器或通过编程设备/PC 对 F-CPU 执行存储器复位。• 在 HW Config 中将组态下载到 F-CPU。• 在“安全程序”(Safety Program) 对话框中将安全程序下载到 F-CPU。• 执行程序标识（即，检查以确定在线和离线块文件夹中所有具有 F 属性的 F 块的集体签名是否匹配）。

 警告
<p>如果一台编程设备或 PC 通过网络（例如 MPI）可以访问多个 F-CPU，则必须采取以下措施以确保将安全程序下载到正确的 F-CPU：</p> <p>对于每个 F-CPU 都使用特定的密码，例如 F-CPU 的统一密码再加上各自的 MPI 地址作为扩展：“Password_8”。</p> <p>请注意以下几点：</p> <ul style="list-style-type: none">• 第一次为 F-CPU 分配密码时，必须使用点对点连接（与第一次为 F-CPU 分配 MPI 地址相似）。 <p>将安全程序下载到没有获得通过 F-CPU 密码获得访问授权的 F-CPU 前，必须首先取消对所有其它 F-CPU 的现有访问授权。</p>

使用存储卡将安全程序传送到 F-CPU

使用 MMC 或闪存卡

使用以下设备传送安全程序时会应用下列警告：

- 闪存卡（例如，CPU 416F-2）
- MMC（例如，CPU 317F-2 DP、CPU 315F-2 PN/DP 或 IM 151-7 F-CPU）

警告

如果未在目标 F-CPU 中对安全程序执行功能测试，则使用存储卡（MMC 或闪存卡）将安全程序传送到 F-CPU 时，必须遵循以下操作步骤，以确保 F-CPU 不包含“旧的”安全程序：

- 关闭 F-CPU 的电源。对于使用备用电池的 F-CPU（例如，CPU 416F-2），请将电池拆除（如果存在）。（要确保 F-CPU 断电，请等待所用电源的放电时间结束，如果不知道此时间有多长，可以拆除 F-CPU）。
- 从 F-CPU 中拆除存有旧安全程序的存储卡（MMC 或闪存卡）。
- 在 F-CPU 中插入存有新安全程序的存储卡（MMC 或闪存卡）。
- 再次接通 F-CPU 的电源。对于使用备用电池的 F-CPU（例如，CPU 416F-2），请将电池重新插入（如果已拆除电池）。

必须确保插入的存储卡（MMC 或闪存卡）包含正确的安全程序。可通过程序标识或其它措施来执行此操作，例如存储卡（MMC 或闪存卡）上的唯一标识符。

将安全程序下载到存储卡（MMC 或闪存卡）时，必须遵循以下操作步骤：

- 将安全程序下载到存储卡（MMC 或闪存卡）。
- 执行程序标识 — 换句话说，检查离线块文件夹中和存储卡（MMC 或闪存卡）上的所有具有 F 属性的 F 块的集体签名是否匹配。
- 在存储卡（MMC 或闪存卡）上粘贴适当的标签。

必须通过组织措施确保执行上述操作步骤。

参见

比较安全程序 (页 275)

10.7 修改安全程序

10.7.1 在 RUN 模式下修改安全程序

引言

只有在取消激活的安全模式下才可在操作期间（RUN 模式下）对安全程序进行更改。按照与标准程序相同的方式，在 *FBD/LAD 编辑器* 中对离线 F 块进行更改。不能在线修改 F 块。

说明

如果操作期间不想修改安全程序，请参阅『在 F-FBD/F-LAD 中创建 F 块』一章。

在 RUN 模式下修改安全程序的操作步骤

1. 在 *FBD/LAD 编辑器* 中修改并保存 F-PB 或 F-FB 及其关联的背景数据块、F-FC 或 F-DB。
2. 将修改的 F 块从 *FBD/LAD 编辑器* 下载到 F-CPU。如果要下载多个修改的 F 块，请在 *SIMATIC 管理器* 中进行选择并下载。在取消激活的安全模式下下载 F 块的操作步骤与下载标准程序的操作步骤相同。请遵循 *STEP 7* 在线帮助中有关下载顺序的适用规则。
3. 如果安全模式处于激活状态，则将出现一个用于取消激活安全模式的对话框。确认此对话框。

说明

在 *SIMATIC 管理器* 中进行下载时，只能在取消激活的安全模式下下载您创建的故障安全块（F-PB、F-FB、F-FC 或 F-DB）、F 应用程序块或标准块及其关联的背景数据块。如果自动下载添加的 F 块（F-SB 或自动生成的 F 块及其关联的背景数据块或 F 共享 DB），则 F-CPU 可能会切换到 STOP 模式或激活安全模式。

因此，在 *SIMATIC 管理器* 中进行下载时，始终选择各个 F 块，而不是“站”、“S7 程序”或“块文件夹”对象。

安全相关的 CPU 与 CPU 通讯的限制

操作期间（在 RUN 模式下），不能通过新的 F_SENDDP/F_RCVDP 和 F_SENDS7/F_RCVS7 块对来建立新的安全相关的 CPU 与 CPU 通讯。

在为 F_SENDDP、F_SENDS7、F_RCVDP 或 F_RCVS7 插入新的块调用后，要建立新的安全相关的 CPU 与 CPU 通讯，始终必须在 STOP 模式下重新编译相关的安全程序并将其整体下载到 F-CPU。

F 运行组通讯的限制

在 RUN 模式下，不能对 F 运行组之间的安全相关的通讯进行任何更改。这表示在“定义新的 F 运行组”(Define New F-Runtime Groups) 对话框、“编辑 F 运行组”(Edit F-Runtime Groups) 对话框或在 *SIMATIC 管理器* 中，不能添加、删除或修改 F 运行通讯的 DB。

在 F 运行组通讯中进行更改之后，始终必须在 STOP 模式下重新编译安全程序并将其整体下载到 F-CPU。

F-I/O 访问的限制

如果操作期间（在 RUN 模式下），插入了对 F-I/O（在安全程序中尚未使用其关联的 F-I/O DB 的单通道或变量）的 F-I/O 访问，则 F-I/O 访问只有在 STOP 模式下重新编译安全程序并将其整体下载到 F-CPU 后才生效。

对标准用户程序的修改

当 F-CPU 处于 RUN 模式时，无论安全模式是处于激活状态还是取消激活状态，您都可以将修改下载到标准用户程序。



警告

在安全模式中，对标准用户程序进行更改时，由于也会对安全程序进行更改，因此不允许通过 F-CPU 密码方式进行访问。要排除这种可能性，必须组态**保护级别 1**。如果仅授权一人可以对标准用户程序和安全程序进行更改，则应组态保护级别“2”或“3”，从而使其它人员仅能有限地访问或根本无法访问整个用户程序（标准程序和安全程序）。

修改 F 运行组调用

如果操作期间（在 RUN 模式下）将 OB（例如，OB35）或具有 F-CALL 调用的 FB 下载到 F-CPU，则仅当在关闭然后重新打开“安全程序”(Safety Program) 对话框后才会更新模式。

将更改应用于安全程序的操作步骤

如果操作期间（在 RUN 模式下）将各个 F 块下载到 F-CPU，则既不会更新也不会下载 F 系统块 (F-SB) 和自动生成的 F 块，这样将导致 F-CPU 中出现不一致的安全程序。使用以下操作步骤接受对安全程序的更改：

1. 在“安全程序”(Safety Program) 对话框中编译安全程序。
2. 在 STOP 模式下使用“安全程序”(Safety Program) 对话框将完整的安全程序下载到 F-CPU，并通过将 F-CPU 从 STOP 模式切换到 RUN 模式来激活安全模式。
3. 按照『安全程序验收测试』一章中的说明步骤进行操作。

参见

组态 F-CPU (页 28)

使用 F-FBD/F-LAD 创建 F 块 (页 82)

编译安全程序 (页 260)

下载安全程序 (页 262)

安全程序验收测试 (页 301)

10.7.2 比较安全程序

比较安全程序的标准

可按照以下标准来比较两个安全程序：

- 块文件夹中所有具有 F 属性的 F 块的集体签名
- 各个 F 块的参数
- 各个 F 块的签名

可以比较 F 块签名，来识别已修改或已删除的 F 块。

可比较的安全程序

可以将安全程序与下列程序进行比较：

- 在线安全程序（此安全程序的在线版本）
- 离线安全程序（任何离线安全程序）
- 在线安全程序（任何在线安全程序）
- 存储卡上的安全程序
- 访问的站点的安全程序

比较安全程序的操作步骤

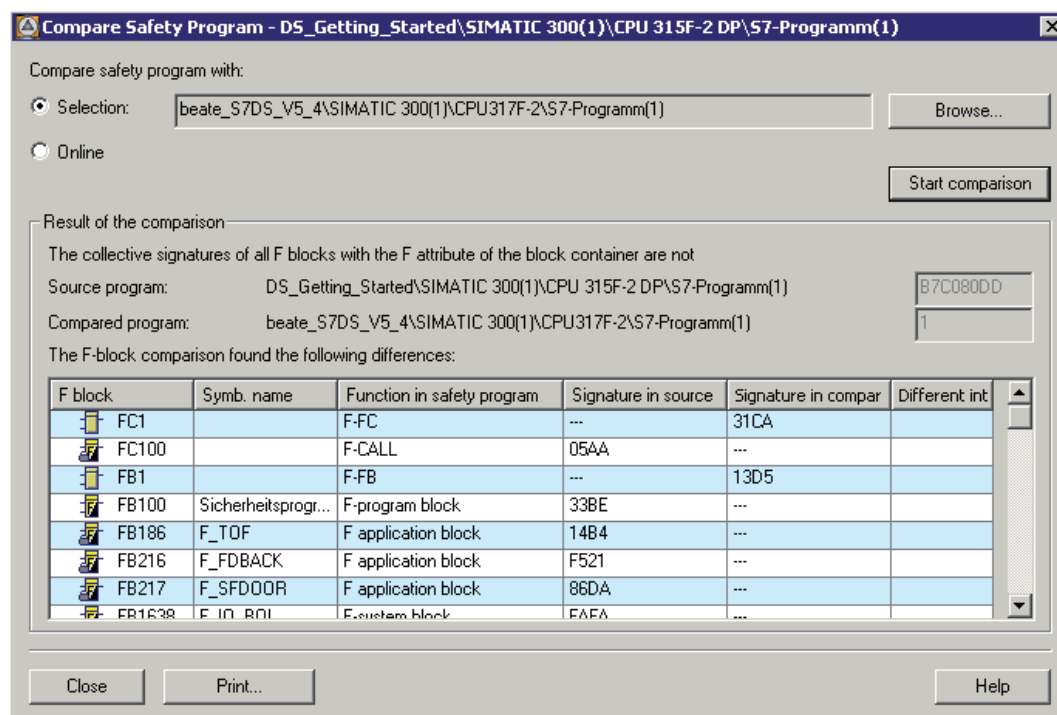
要比较两个安全程序，请：

1. 选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 *SIMATIC 管理器* 中，选择选项 (Options) > 编辑安全程序 (Edit Safety Program) 菜单命令。

将显示“安全程序”(Safety Program) 对话框。

3. 单击“比较”(Compare) 按钮。

将显示“比较安全程序”(Compare safety program) 对话框。



4. 选择要与其进行比较的安全程序。激活“浏览...”(Browse...) 按钮来指明其路径。

5. 激活“开始比较”(Start comparison) 按钮。

将执行所需的块比较，并将不同的 F 块以表格形式显示在对话框中。

比较结果

比较结果将显示已修改的 F 块（“源程序中的签名”[Signature in Source Program] 列和“被比较程序中的签名”[Signature in Compared Program] 列中的不同条目）、仅在源程序中的 F 块（仅在“源程序中的签名”[Signature in Source Program] 列中的条目）以及仅在被比较程序中的 F 块（仅在“被比较程序中的签名”[Signature in Compared Program] 列中的条目）。“接口不同”(Interface Different) 列指示 F 块的声明表是否更改过。

可使用“打印”(Print) 按钮将结果打印输出。

如果正在比较离线安全程序和在线安全程序，但在比较过程中与 F-CPU 的连接中断，则比较结果将不正确。

对更改的分配

您可以根据比较结果中指示的已修改的 F 块来分配安全程序中的更改。

已修改的 F 块	安全程序中的更改
F 程序块、F-FB、F-FC	<ul style="list-style-type: none"> 此块中的更改 更改所调用的 FB/FC 中或所用 F-DB 的 F-PB/F-FB/F-FC 中的声明表 作为多重背景包含的 F-FB 内声明表中的更改 缺少作为多重背景调用的 F-FB
F 程序块的 I-DB、 F-FB 的 I-DB	<ul style="list-style-type: none"> 每个 I-DB 的 F-PB/F-FB 内声明表中的更改
F 应用程序块 F 系统块	<ul style="list-style-type: none"> F 块的修改版本（例如，由于使用了新版本的 <i>S7 Distributed Safety</i> 中的 F 块） 缺少作为多重背景调用的 F-FB
F 应用程序块的 I-DB	<ul style="list-style-type: none"> 关联 F 应用程序块的修改版本
F-DB	<ul style="list-style-type: none"> F-DB 声明表中的更改

已修改的 F 块	安全程序中的更改
F-I/O DB	<ul style="list-style-type: none"> • 各个 F-I/O 的硬件配置中的更改 • F-CPU 的 F 参数中的更改 • F 系统块的修改版本
自动生成的 F 块	<ul style="list-style-type: none"> • F 运行组最大周期时间中的更改 • F-CPU 的 F 参数中的更改 • F 系统块的修改版本 • F 运行组通讯中的更改，例如 F 运行组通讯的 DB 编号中的更改。
F-CALL	<ul style="list-style-type: none"> • F-PB 及其背景数据块的分配中的更改 • 在安全程序中寻址的 F-I/O 中的更改 • 对标准用户程序的数据的读访问中的更改 • F-CPU 的 F 参数中的更改 • F 系统块的修改版本 • F 运行组通讯中的更改

更改还可能以组合方式发生，这表示对 F 块的更改可由多种原因引起。

如果没有指示任何已修改的 F 块，但是集体签名却不同，则差异存在于自动生成的块中（这些块不包含在比较中）。例如，如果在 *HW Config* 中 F-CPU 的对象属性对话框内，对 F 块重新编号或者对为安全程序保留的资源进行修改，则会发生上述情况。

10.7.3 删除安全程序

删除单独的 F 块

要删除 F 块，请执行与标准程序相同的操作步骤。

删除 F 运行组

1. 在“编辑 F 运行组”(Edit F-Runtime Groups) 对话框中，选择要删除的 F 运行组文件夹。
2. 按下“删除”(Delete) 按钮。
3. 单击“确定”(OK) 关闭对话框。

分配给 F 运行组的 F 块即会删除。但 F 块仍然存在。

删除整个安全程序

1. 离线删除 *SIMATIC Manager* 中所有以黄色高亮显示的 F 块。
2. 在 *HW Config* 中，选择 F-CPU，然后选择**编辑 (Edit) > 对象属性 (Object Properties)** 菜单命令。打开“保护”(Protection) 选项卡并取消激活“CPU 包含安全程序”(CPU Contains Safety Program) 选项。保存并编译硬件配置。

离线项目不再包含安全程序。

3. 以下操作适用于已插入存储卡（MMC 或闪存卡）的 F-CPU：

要删除存储卡（MMC 或闪存卡）上的安全程序，请将存储卡（MMC 或闪存卡）插入编程设备或 PC 中。在 *SIMATIC 管理器* 中，选择**文件 (File) > S7 存储卡 (S7 Memory Card) > 删除 (Delete)** 菜单命令。

现在即可将离线标准用户程序复制到存储卡（MMC 或闪存卡）。

以下操作适用于未插入闪存卡的 F-CPU：

可以通过在 *SIMATIC 管理器* 中复位模块（菜单命令 **PLC > 复位 [Reset]**）来删除安全程序。

然后，便可以将离线标准用户程序下载到 F-CPU。

10.7.4 安全程序的记录册

记录册

记录册中记录安全程序的更改和操作。各用户操作都会在记录册中产生相应的条目。

每个安全程序都有自己的记录册。条目将按时间顺序列出。记录册最多可包含 300 个条目。当条目数超过 300 时，条目会按顺序依次覆盖。

安全程序的记录册功能不像 IEC 61508 中定义的一样，它不是安全相关的。

记录册的内容

将针对以下操作在安全程序记录册中记录条目：

- 更改安全程序的硬件配置
- 创建 F 块
- 保存 F 块
- 重命名 F 块
- 重新接线 F 块
- 更改 F 块的对象属性
- 删除 F 块
- 更改 F 运行组
- 编译安全程序
- 取消激活安全模式
- 下载 F 块
- 下载安全程序或安全程序更改

记录册条目的实例：

操作： 创建 F 块 FB1

记录册中的条目： 日期、时间（记录册中的条目时间）、用户 ID、程序路径、操作“创建 F 块 FB1”

显示、保存、打印和复制记录册

1. 选择 F-CPU 或为其指定的 S7 程序。
2. 在 SIMATIC 管理器中，选择**选项 (Options) > 编辑安全程序 (Edit safety program)** 菜单命令或选择工具栏上的相应图标。

将显示“安全程序”(Safety Program) 对话框。

3. 单击“记录册...”(Logbook...)。

这将打开记录册（消息窗口）。

可以将记录册以文本文件形式保存在 Windows 目录结构中，以便以后进行打印。

复制安全程序时，与安全程序关联的记录册（如果存在）也会一起被复制。

安全程序 < V5.4 SP1

如果安全程序是使用 *S7 Distributed Safety V5.4 SP1* 之前的版本进行创建的，则仅当使用 V5.4 SP1 或更高版本执行与记录册相关的操作后，记录册才可用。

10.8 打印输出项目数据

引言

使用“安全程序”(Safety Program) 对话框的“打印”(Print) 按钮，可以打印输出所需的硬件配置和安全程序的所有重要项目数据，例如，进行系统验收测试所需的数据。打印输出页脚中的签名确保了打印输出与安全程序的明确关联性。

说明

打印输出项目数据之前，请关闭 *HW Config* 和 *LAD/FBD 编辑器* 应用程序及符号表。

打印硬件配置和安全程序的所有重要项目数据的操作步骤

1. 在 *SIMATIC 管理器* 中，选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 *SIMATIC 管理器* 中，选择选项 (Options) > 编辑安全程序 (Edit Safety Program) 菜单命令。

将显示“安全程序”(Safety Program) 对话框。

3. 单击“打印”(Print) 按钮。

然后，您可以选择打印内容：

- “功能块图/梯形图”(Function Block Diagram/Ladder Diagram):
在安全程序中以适当编程语言创建的所有 F 块 (F-PB、F-FB、F-FC、F-DB)。对于 F-DB，将打印数据视图。
- “安全程序”(Safety program):
安全程序的所有 F 块的列表和与验收测试相关的其它数据 (请参阅『打印的安全程序项目数据』一章)
- “硬件配置...”(Hardware Configuration...) (请参阅『打印的硬件配置项目数据』一章)
- “符号表”(Symbol table)

必须为系统验收测试打印输出所有打印内容。

打印输出的页脚

打印输出的页脚中将显示以下信息：

- 块文件夹中所有具有 F 属性的 F 块的集体签名
- 符号的签名（仅用于离线安全程序的打印输出）
- 用于创建打印输出的 *S7 Distributed Safety* 的版本标识符
- 取决于安全程序的状态：“安全程序已更改”、“安全程序未更改”或“符号已更改”

说明

如果输出“符号已更改”，这表示对全局符号或本地符号的分配已更改（例如，符号表中发生更改或更改了 F-DB 或 F-FB 的参数名称），但并未在所有受影响的 F-FB/F-FC 中进行了更改。

要校正这种情况，请使用“检查块的一致性”功能（请参阅 *STEP 7* 在线帮助）。如有必要，您必须重新编译安全程序。

10.8.1 打印的硬件配置的项目数据

操作步骤

如果选择了“硬件配置...”(Hardware Configuration...) 打印内容，则会弹出一个对话框。

1. 选择“全部”(All) 作为打印范围。打印输出则将包含“模块说明”(Module description) 和“地址列表”(Address list)。
2. 要在打印输出中包含参数说明，请选择“包含参数说明”(Including parameter description) 选项。

打印的信息

硬件配置打印输出（“硬件配置...”[Hardware Configuration...] 打印内容）中的以下信息对组态验收测试来说非常重要：

- 以下 F-CPU 参数：
 - 保护级别
 - F 参数
- F-I/O 的所有参数

安全相关的智能从站与从站通讯的操作步骤

对于通过安全相关的智能从站与从站通讯的系统验收测试，还需要打印输出通过安全相关的智能从站与从站通讯寻址的 F-I/O 的参数。具有 DP 主站的站的硬件配置打印输出中包含此信息。

如果 DP 主站的 CPU 是被分配了安全程序的 F-CPU，则可以在 *SIMATIC 管理器* 中选择 DP 主站的 F-CPU 或为其分配的 S7 程序，然后使用 **选项 (Options) > 安全程序 (Safety Program)** 菜单命令按照上述说明启动打印输出，来打印输出这些 F-I/O 的参数。

如果 DP 主站的 CPU 是标准 CPU，则可以打印输出这些 F-I/O 的参数，方法如下：

1. 选择具有 DP 主站的站。
2. 在 *SIMATIC 管理器* 中，选择 **选项 (Options) > 对象内容 (Object Content)** 菜单命令。
将弹出一个对话框。
3. 选择“全部”(All) 作为打印范围。打印输出则将包含“模块说明”(Module description) 和“地址列表”(Address list)。
4. 要在打印输出中包含参数说明，请选择“包含参数说明”(Including parameter description) 选项。

10.8.2 打印的安全程序项目数据

打印的信息

安全程序的打印输出（“安全程序”[Safety program] 打印内容）包含对安全程序验收测试来说非常重要的以下信息：

- 集体签名：
 - “块文件夹中具有 F 属性的 F 块”（=“安全程序”[Safety Program] 对话框中的“块文件夹中所有具有 F 属性的 F 块的集体签名”[collective signature of all F-blocks with F-attribute in the block container]；也显示在打印输出的页脚中）
 - “安全程序”（=“安全程序”[Safety Program] 对话框中的“安全程序的集体签名”[collective signature of the safety program] = F 共享 DB 中“F_PROG_SIG”变量的值）

这两个签名必须与验收测试一致。

两个签名之间的差异通常表示安全程序已被更改或不一致。这在页脚处也给予了注明。

- 上次用于编译安全程序的 *S7 Distributed Safety* 的版本标识符
- 编译安全程序的时间
- 指示是否已超过为安全程序保留的本地数据量的消息
- 块文件夹中包含的所有 F 块的列表（由方括号括起的块名称和签名指示不具有 F 属性的 F 块）

为每个 F 块提供的信息：

- 块编号
- 符号名
- 安全程序中的功能（F-CALL、F 程序块等）
- 签名
- 未自动生成的所有 F-FB 的初始值签名

- 安全相关的 CPU 与 CPU 通讯的参数列表，例如：
 - F_SENDDP、F_RCVDP 的 DP_DP_ID 和 LADDR
 - F_SENDS7、F_RCVS7 的 ID、R_ID 和 F 通讯 DB 的编号
 - F_SENDDP、F_RCVDP、F_SENDS7、F_RCVS7 的 TIMEOUT为参数提供了以下信息：
 - 参数名称
 - 关联 F 应用程序块的名称
 - 用于调用 F 应用程序块的背景数据块的编号
 - 在其中调用了 F 应用程序块的 F 块的名称
 - 调用的程序段编号
 - F 运行组的名称（F-CALL 的名称）
 - 参数值
- 从标准用户程序传送的数据列表：
 - 地址
 - 符号
 - 在其中使用了数据元素的 F 运行组
- 用于在 F 运行组之间进行数据交换的数据列表
 - “发送方” F 运行组的 F-CALL 的编号
 - “接收方” F 运行组的 F-CALL 的编号
 - F 运行组通讯 DB 的编号
- 每个运行组的运行组信息：
 - F-CALL 的编号
 - F-CALL 的符号名
 - 被调用的 F 程序块的编号
 - F 程序块的符号名
 - 关联背景数据块的编号（如果适用）
 - 关联背景数据块的符号名
 - F 运行组的最大周期时间

10.8 打印输出项目数据

- F 运行组中使用的所有 F 块（F 系统块、F 共享 DB 和自动生成的 F 块除外）的列表。（由方括号括起的块名称和签名指示不具有 F 属性的 F 块。）

为每个 F 块提供的信息：

- 块编号
 - 符号名
 - 安全程序中的功能（F-CALL、F 程序块等）
 - 签名
 - 未自动生成的所有 F-FB 的初始值签名
- 在 F 运行组中寻址的 F-I/O 的列表（即，不是列出在 *HW Config* 中组态的所有 F-I/O，而是仅列出那些实际使用的 F-I/O）：
 - F-I/O DB 的符号名
 - F-I/O DB 的编号
 - 起始地址
 - F-I/O 的名称/标识符
 - 模块类型
 - F_Monitoring_Time
 - 通过参数分配进行的循环冗余检查（以便快速检测到 I/O 上发生的更改）
 - PROFIsafe 源地址和目标地址
 - PROFIsafe 模式
 - 钝化类型

- 会为安全程序的 F 共享 DB 注明以下信息：
 - F 共享 DB 的编号
 - 符号名 F_GLOBDB
 - 安全程序集体签名的绝对地址和符号地址
 - 用于读出工作模式的绝对地址和符号地址
 - 用于读出错误信息的绝对地址和符号地址
 - 用于读出编译时间的绝对地址和符号地址
 - RLO 0 的绝对地址和符号地址
 - RLO 1 的绝对地址和符号地址
- 附加信息
 - 安全程序的“可以取消激活安全模式”参数的设置
 - 打印输出的创建时间
 - 此打印输出中的总页数

参见

“Safety Program”（安全程序）对话框 (页 255)

10.9 测试安全程序

10.9.1 测试安全程序概述

测试选项

通常，安全程序及安全模式也可以使用所有只读测试功能（如变量监视）。虽然所有 F 块均可用作受监视对象，但这只对您创建的 F-Block（F-PB、F-FB、F-FC 和 F-DB）有用。可无限制地进行监视。

可以使用“Monitor/modify variable”（监视/修改变量）功能来修改安全程序的数据，也可以使用 *HW Config* 或 *FBD/LAD 编辑器* 来获取写入权限。但必须取消激活限制应用和安全模式。不允许对安全程序进行其他的写访问，这些写访问可导致 F-CPU 切换到 STOP 模式。

使用 STEP 7 的 S7-PLCSIM 功能进行测试

可以使用 STEP 7 的 S7-PLCSIM V5.3 及更高（硬件模拟）功能测试安全程序。S7-PLCSIM 的使用方式与标准用户程序相同。

说明

可将 F 应用程序块 F_SENDDP、F_RCVDP、F_SENDS7 及 F_RCVS7 与 STEP 7 的 S7-PLCSIM 功能（硬件模拟）结合使用。但是，请注意，当 F 应用程序块在模拟 CPU 中运行时，会不断发出“通讯错误”信号。

10.9.2 取消激活安全模式

引言

安全程序通常在 F-CPU 中以安全模式运行。这表示会激活所有故障控制措施。在安全模式下进行操作（在 RUN 模式下）的过程中，无法修改安全程序。必须取消激活安全程序的安全模式，才能在 RUN 模式下下载对安全程序的更改。在下次将 F-CPU 从 STOP 模式切换至 RUN 模式之前，安全模式会保持取消激活状态。

可以在 F-CPU 对象属性的“F 参数”选项卡中，启用或禁用用于取消激活安全模式的选项。

**警告**

由于取消激活安全模式后，可以在 RUN 模式下更改安全程序，因此必须考虑以下事项：

- 安全模式的取消激活适用于测试用途、开机调试等。取消激活安全模式后，必须通过其他组织措施（例如操作监视和手动安全关闭）来确保系统的安全。
- 必须指出对安全模式的取消激活。
安全程序的打印输出包含 F 共享 DB 中的变量地址 ("F_GLOBDB".MODE)，您可以评估该地址以读出工作模式（1 = 已取消激活的安全模式）。因此，取消激活的安全模式不但可以显示在编程设备或 PC 上的取消激活安全模式对话框中，而且还可以通过由标准用户程序控制的指示灯指示，或通过评估 F 共享 DB 中的“取消激活的安全模式”变量生成并提供给操作员监视和控制系统的消息来指示。
- 取消激活安全模式后，在 RUN 模式下更改安全程序可能导致出现转换效应。在取消激活的安全模式下下载 F 块的操作步骤与下载标准程序的操作步骤相同。请遵循 *STEP 7* 在线帮助中有关下载顺序的适用规则。
- 在尽可能的情况下，应该分别修改标准用户程序和安全程序，并且应该下载更改；否则，可能会同时将错误下载到标准用户程序，从而破坏安全程序和标准程序中的必要防护功能，或导致在其中发生切换。
- 必须能够验证已取消激活安全模式。需要进行记录，如有可能可以记录向操作员监视和控制系统提供的信息；但如有必要则请通过组织措施进行记录。此外，建议在操作员监视和控制系统上指示取消激活安全模式。
- 仅通过 F-CPU 取消激活安全模式。对于安全相关的 CPU 与 CPU 通讯，必须考虑以下事项：如果具有 F_SENDDP 或 F_SENDS7 的 F-CPU 处于取消激活的安全模式下，则不能再认为由此 F-CPU 发送的数据是以安全方式生成的。这样，就必须实施组织措施（例如操作监视和手动安全关闭），以确保系统中受发送数据影响的那些部分的安全性。或者，必须通过评估 SENDMODE，输出带 F-RCVDP 或 F-RCVS7 的 F-CPU 的故障安全值而不是接收的数据。

取消激活安全模式的要求

在 *HW Config* 中 F-CPU 的“F 参数”选项卡中，已启用“可以取消激活安全模式”(Safety mode can be deactivated) 参数（请参阅『组态 F-CPU』一章）。

F-CPU 处于 RUN 模式，并且安全模式已激活。

取消激活安全模式的操作步骤

1. 选择正确的 F-CPU 或为其指定的 S7 程序。
2. 在 *SIMATIC 管理器* 中，选择 **选项 (Options) > 编辑安全程序 (Edit Safety Program)** 菜单命令。
将显示“安全程序”(Safety Program) 对话框。
3. 如果系统提示您输入 F-CPU 密码，请立即输入。
4. 检查“已激活安全模式”(Safety mode activated) 是否指示为“当前模式”(Current mode)。如果是，请继续执行下一步；如果不是，请停止该过程，因为安全模式已取消激活或无法取消激活。

说明

如果“当前模式：”(Current mode:) 下的文本 以方括号括起（如 [abc]），这表示在线和离线安全程序的集体签名和/或密码不匹配。这表示发生了以下某种情况：

- 下载离线安全程序后，对其进行了修改。
- 对错误的 F-CPU 进行了寻址。您可以根据块文件夹中所有具有 F 属性的 F 块的在线集体签名来验证后者。

-
5. 激活“安全模式”(Safety mode) 按钮，然后输入在线安全程序的密码。
如果密码无效，则安全模式不会取消激活，并保持激活状态。
 6. 如果输入的密码正确，则会出现另一个提示，其中也包含 F-CPU 中安全程序的集体签名。检查这是否是期望的集体签名。
 7. 如果这不是期望的集体签名，请验证是否对正确的 F-CPU 进行了寻址，并检查 F-CPU 中是否包含正确的 F 块。要执行以上操作，请关闭所有 *STEP 7* 应用程序，然后打开“安全程序”(Safety Program) 对话框；必须执行此操作，以防多个应用程序同时访问 F-CPU。
 8. 单击“确定”(OK) 确认对取消激活安全模式的提示。
安全模式将会取消激活。

现在即可在操作过程中（在 RUN 模式下），将安全程序中的更改下载到 F-CPU。

说明

要激活安全模式，必须将 F-CPU 从 STOP 模式切换到 RUN 模式。

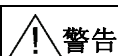
将 F-CPU 从 STOP 模式切换到 RUN 模式时，即使安全程序已被修改或不一致，也始终会激活安全模式。F 共享 DB 中的 MODE 变量设置为“0”。评估 MODE 变量以读出工作模式时，请记住这一点。

如果已修改安全程序，但是尚未对其进行重新编译和下载，则 F-CPU 可以返回 STOP 模式。

评估安全模式/取消激活的安全模式

如果要评估安全程序中的安全模式/取消激活的安全模式，可以评估 F 共享 DB 中的“MODE”变量（1 = 取消激活的安全模式）。需要使用具有完整资格的访问来访问该变量（“F_GLOBDB”.MODE）。F 共享 DB 的编号和符号名及变量的绝对地址将在安全程序的打印输出中指明。

例如，当安全程序处于取消激活的安全模式时，可以使用此评估来钝化 F-I/O。要进行此操作，请将 F 共享 DB 中的“MODE”变量分配给要钝化的 F-I/O 的 F-I/O DB 中所有“PASS_ON”变量。



当安全程序处于取消激活的安全模式时，F 共享 DB 中的“MODE”变量也可以在取消激活的安全模式下进行评估。

即使因“MODE”变量的评估而导致 F-I/O 在取消激活的安全模式下被钝化，也必须通过其他组织措施（例如操作监视和手动安全关闭）来确保在取消激活的安全模式下的系统安全。

参见

在 RUN 模式下修改安全程序 (页 273)

10.9.3 测试安全程序

引言

在已取消激活的安全模式下，会取消激活安全程序的某些故障管理措施，以便能够在 RUN 模式下在线更改安全程序。这样，就可以使用标准 *STEP 7* 工具来更改安全程序数据。

使用“监视/修改变量”功能来修改安全程序数据

除了始终可以修改的标准用户程序数据之外，您还可以在取消激活的安全模式下，使用“监视/修改变量”功能修改以下安全程序数据：

- F-I/O 的过程映像
- F-DB（用于 F 运行组通讯的 DB 除外）、F-FB 的背景数据块
- F 应用程序块的背景数据块
- F-I/O DB（有关允许的信号，请参阅『F-I/O DB』一章）

说明

F-I/O 只能在 F-CPU 的 RUN 模式下进行修改。必须在变量表中为每个要修改的通道分配单独的行；举例来说，这表示无法逐字节或逐字对数据类型为 **BOOL** 的数字通道进行修改。

最多可以修改一个变量表中的 5 个输入/输出。可以使用多个变量表。

无法修改已组态的 F-I/O（其中未使用来自关联 F-I/O DB 的任何单通道或变量）。因此，始终至少使用一个来自关联 F-I/O DB 的变量或一个要在安全程序中控制的 F-I/O 通道。

作为触发点，必须设置“扫描周期的开始”(Begin scan cycle) 或“扫描周期的结束”(End scan cycle)。但是请注意，不管触发点设置为何，修改 F-I/O 输入 (PII) 的请求始终会在执行 F-PB 前生效，并且修改输出 (PIQ) 的请求始终会在执行 F-PB 后生效。

对于输入 (PII)，修改请求优先于故障安全值输出；而对于输出 (PIQ)，故障安全值输出则优先于修改请求。对于未在 *HW Config* 内 F-I/O 对象属性中激活的输出（通道）（请参阅 *F-I/O 手册*），修改请求仅影响 PIQ，而不影响 F-I/O。

作为触发频率，可以设置“一次”或“永久”。

警告

在下列情况下，F-I/O 的永久修改始终保持激活：

- 编程设备与 F-CPU 之间的连接中断（通过拔下总线电缆）
- 变量表不再响应

只能通过 F-CPU 的存储器复位或将 F-CPU 从 STOP 模式切换到 RUN 模式，并且同时断开 F-CPU 与编程设备或 PC 的连接来删除这些修改请求。

接线测试

使用信号的符号名可简化接线测试。

通过修改输入信号并验证新值是否到达 PII，可对输入执行接线测试。

可以通过修改功能修改输出并验证所需执行器是否响应，来为输出执行接线测试。

对于接线测试（为输入和输出）请注意，安全程序必须在 F-CPU 上运行，其中至少已使用一个要修改的 F-I/O 通道或一个关联 F-I/O DB 的变量。

对于也可以作为标准 I/O 来操作的 F-I/O（例如，S7-300 故障安全信号模块），还可以在 STOP 模式下（而不是在安全模式下）通过将 F-I/O 作为标准 I/O 进行操作，使用修改功能为输出执行接线测试。这样做时，必须遵守其他测试规则。

说明

由 F 系统控制的修改功能需要使用带 *S7 Distributed Safety* 选件包的 *STEP 7*。如果使用操作员监视和控制系统或不带 *S7 Distributed Safety* 选件包的 *STEP 7* 来修改变量，则 F-CPU 会切换到 STOP 模式。

测试和调试功能可使用标准 *STEP 7* 工具（*FBD/LAD 编辑器*、*变量编辑器*、*HW Config*）进行选择。在安全模式下修改安全程序会被拒绝，并会显示相应的错误信息或用于取消安全模式的对话框。在某些情况下，修改请求可导致 F-CPU 切换到 STOP 模式。

打开 F 块

FBD/LAD 编辑器 仅可用于将 F-CPU 中的 F 块作为写保护块在线打开，即，即使取消激活安全模式您也无法直接修改 F-CPU 中的 F 块。相反，您必须离线编辑它，然后下载。

修改 F-DB 中的值

F-DB 中的值仅可在 F-CPU 中在线修改。如果还要离线更改该值，则还必须离线编辑实际值并编译安全程序。

请仅修改本文档中说明的参数。

其他测试规则

- 不能强制 F-I/O。
- 在标准用户程序中设置断点将导致在安全程序中发生以下错误：
 - F 周期时间监视超时
 - 与 F-I/O 通讯过程中出错
 - 安全相关的 CPU 与 CPU 通讯过程中出错
 - 内部 CPU 故障

如果仍要将断点用于测试，必须先取消激活安全模式。这将导致以下错误：

- 与 F-I/O 通讯过程中出错
- 安全相关的 CPU 与 CPU 通讯过程中出错
- 只有在已保存并下载硬件组态之后，以及在“安全程序”(Safety Program) 对话框中编译并下载安全程序之后，才可以测试 F-I/O 组态或安全相关的 CPU 与 CPU 通讯组态中的更改。

说明

如果使用“监视/修改变量”功能测试安全程序，则此功能不会检测 F-CPU 中使用其他应用程序所做出的其他所有更改。

例如，如果取消激活安全模式后，通过修订/修改更改了安全程序的集体签名，则可能无法检测到这些更改，并且可能会继续显示旧的集体签名。

在这种情况下，必须结束“监视/修改变量”功能然后重新启动此功能，这样才能使用更新过的数据。

“在接触点上控制” (Control at contact) 功能

对于 F 块，不支持 *STEP 7*V5.2 及更高版本中支持的“在接触点上控制” (Control at contact) 功能。

测试安全程序的操作步骤

使用以下操作步骤进行测试：

1. 取消激活安全模式。
2. 监视和修改所需的来自变量表、*HW Config* 或 *FBD/LAD* 编辑器的 F 数据和 / 或 F-I/O。
3. 在激活安全模式前，完成测试后，结束现有的修改请求。
4. 要激活安全模式，请将 F-CPU 从 STOP 模式切换到 RUN 模式。

如果测试过程中，安全程序的表现与您的期望不符，您可以选择在 RUN 模式下修改安全程序，并立即继续进行测试，直至安全程序的表现与要求相符。

『在 RUN 模式下修改安全程序』一章中，可以找到有关在 RUN 模式下修改安全程序的附加信息。

使用 S7-PLCSIM 测试安全程序

可在 S7-PLCSIM 中监视和修改安全程序的变量，并执行安全程序中的其他写访问功能。

要使用 S7-PLCSIM，只需将一致的安全程序下载到 S7-PLCSIM。

说明

如果要在 S7-PLCSIM 中修改变量，首先必须取消激活安全模式。

否则，S7-PLCSIM 会切换到 STOP 模式。只能在“安全程序”(Safety Program) 对话框中取消激活安全模式。

有关 *STEP 7* 的 S7-PLCSIM 功能的详细说明，请参考《*S7-PLCSIM V5.x* 用户手册》。

S7 Distributed Safety 中安全程序的程序结构，过程或故障安全值（在 RUN 模式下对安全程序的更改）

参见

S7 Distributed Safety 中安全程序的结构 (页 61)

过程数据或故障安全值 (页 102)

F-I/O DB (页 104)

下载安全程序 (页 262)

在 RUN 模式下修改安全程序 (页 273)

取消激活安全模式 (页 288)

系统验收测试

11.1 系统验收测试概述

引言

在系统验收测试过程中，必须遵守所有相关的应用程序特定标准和下述操作步骤。这也适用于不是“正在进行验收测试”的系统。对于验收测试，必须考虑《认证报告》中的系统。

通常由独立的专家执行 F 系统的验收测试。

要求

硬件组态和参数分配是完整的。

已创建和编译安全程序，且该安全程序是一致的。

操作步骤

使用以下操作步骤进行系统验收测试：

1. 备份整个 STEP 7 项目。
2. 在“安全程序”(Safety Program) 对话框中选择“离线”(Offline) 选项卡。
3. 打印包含所有打印内容的项目数据（请参阅『打印项目数据』一章）。
4. 检查所有打印输出（请参阅『检查打印输出』一章）。
5. 将完整的安全程序下载到 F-CPU（请参阅『在将安全程序下载到 F-CPU 之后进行检查』一章）。
6. 执行完整的功能测试。

参见

下载安全程序 (页 262)

打印输出项目数据 (页 281)

测试安全程序 (页 291)

11.2 检查打印输出

操作步骤

如下检查打印输出：

1. 检查打印输出页脚中的两个签名与所有四个打印输出中的签名是否匹配：
 - 块文件夹中所有具有 F 属性的 F 块的集体签名
 - 符号签名
2. 检查打印输出页脚中是否输出了“符号已更改”。
3. 检查硬件组态的打印输出（请参阅『F-CPU 和 F-I/O 的组态验收测试』一章）。
4. 检查您创建的 F 块（F-PB、F-FB、F-FC 和 F-DB）的打印输出。
5. 检查符号表的打印输出。
6. 检查“安全程序”打印输出（请参阅『安全程序验收测试』一章）

说明

如果输出“符号已更改”，这表示对全局符号或本地符号的分配已更改（例如，符号表中发生更改或更改了 F-DB 或 F-FB 的参数名称），但并未在所有受影响的 F-FB/F-FC 中进行了更改。

要校正这种情况，请使用“检查块的一致性”功能（请参阅 *STEP 7* 在线帮助）。必要的话，需要重新编译安全程序。

11.2.1 对 F-CPU 和 F-I/O 组态进行的验收测试

检查硬件组态 (“硬件组态...”[Hardware Configuration...] 打印内容)

1. 检查打印输出中 F-CPU 的参数。

尤其要检查 F-CPU 的保护级别设置以及是否选择了“CPU 包含安全程序”(CPU contains a safety program) 选项。



警告

在安全模式下，对标准用户程序进行更改时，由于也会更改安全程序，因此不得授权通过 F-CPU 密码的访问。要排除这种可能性，必须组态保护级别 1。如果仅授权一个人可以对标准用户程序和安全程序进行更改，则应组态保护级别“2”或“3”，以使其他人员仅能有限地访问或根本无法访问整个用户程序（标准程序和安全程序）。

2. 检查打印输出中所有已组态 F-I/O 的安全相关的参数。

在“参数 – F 参数”(Parameters – F-Parameters) 和“参数 – 模块参数”(Parameters – Module parameters) 下可找到安全相关的参数。


对于要通过安全相关的智能从站与从站通讯进行寻址的 F-I/O，可以在 DP 主站的站硬件配置打印输出中找到这些参数（请参阅『打印的硬件组态项目数据』一章）。

对于故障安全 DP 标准从站/标准 I/O 设备，可以在“PROFIsafe”下找到安全相关的参数。此外，请注意与任何其他安全相关的（技术）参数相关的故障安全 DP 标准从站/标准 I/O 设备的文档。

说明

在组态过程中，可以复制要为其分配相同的安全相关参数的 F-I/O（除 PROFIsafe 地址外）。除 PROFIsafe 地址外，不再需要单独检查安全相关的参数。在故障安全 DP 标准从站/标准 I/O 设备下，只需将已复制 F-I/O 的“参数 CRC（无 F 地址）”或“F_Par_CRC（无 F 地址）”与已检查 F-I/O 的相应循环冗余检查进行比较即可。“参数 CRC（无 F 地址）”可以在 F-I/O 各模块说明中的硬件组态打印输出中找到。

3. 检查 PROFIsafe 目标地址相互之间是否唯一。

 警告
<p>PROFIBUS 子网规则:</p> <p>F-I/O 的 PROFIsafe 目标地址以及地址开关的开关设置在网络范围*和站范围**（系统范围）内必须是唯一的。对于 S7-300 F-SM 和 ET 200S、ET 200eco、ET 200pro F 模块，最多可以分配 1022 个不同的 PROFIsafe 目标地址。</p> <p>例外情况：可为不同智能从站中的 F-I/O 分配相同的 PROFIsafe 目标地址，因为仅在站内对它们进行寻址，即通过智能从站中的 F-CPU 寻址。</p> <p>以太网子网和 PROFIBUS 与以太网子网混合组态的规则:</p> <p>F-I/O 的 PROFIsafe 目标地址以及地址开关设置只需在以太网子网范围***（包括所有低级别 PROFIBUS 子网）和站范围**（系统范围）内是唯一的。对于 S7-300 F-SM 和 ET 200S、ET 200eco、ET 200pro F 模块，最多可以分配 1022 个不同的 PROFIsafe 目标地址。</p> <p>例外情况：可为不同智能从站中的 F-I/O 分配相同的 PROFIsafe 目标地址，因为仅在站内对它们进行寻址，即通过智能从站中的 F-CPU 寻址。</p> <p>以太网子网联网节点的特点是 IP 地址具有相同的子网地址，即，在子网掩码中 IP 地址均使用数字“1”。</p> <p>实例：</p> <p>IP 地址： 140.80.0.2.</p> <p>子网掩码： 255.255.0.0 = 11111111.11111111.00000000.00000000</p> <p>含义： IP 地址的字节 1 和 2 用于定义子网；子网地址 = 140.80。</p>

*网络由一个或多个子网组成。“网络范围”表示超出子网边界。

**该地址对于 *HW Config* 中组态的站是唯一的（例如 S7-300 站或智能从站）

***在以太网子网中，周期性 PROFINET IO 通讯（RT 通讯）除外

11.2.2 安全程序验收测试

检查安全程序（“安全程序”[Safety Program] 打印内容）

1. 在打印输出中，检查两个集体签名是否匹配：
 - 块文件夹中所有具有 F 属性的 F 块的集体签名
 - 安全程序的集体签名
2. 检查用于创建打印输出（打印输出的页脚）的 *S7 Distributed Safety* 的版本是否是用于编译安全程序的版本（“安全程序”[Safety program] 打印输出的信息部分）或高于该版本。
3. 检查用于编译安全程序的 *S7 Distributed Safety* 的版本（“安全程序”[Safety program] 打印输出的信息部分）是否与《认证报告》的『附录 1』中的版本相对应。
4. 检查所有 F 应用程序块和 F 系统块的签名和初始值签名是否与《认证报告》的『附录 1』中指定的签名相匹配。
5. 确保您已为所有安全相关的通讯连接（用于进行安全相关的主站与主站、主站与智能从站、智能从站与智能从站和 IO 控制器-IO 控制器通讯）分配了在网络范围内唯一的 DP_DP_ID 参数。
6. 确保您已为所有安全相关的通讯连接（用于通过 S7 连接进行安全相关的通讯）分配了在网络范围内唯一的 R_ID 参数。
7. 检查以确定是否对传送自标准用户程序中的安全程序内的所有数据编写了有效性检查。
8. 检查安全程序中 F 运行组的数目（最多 2 个）以及 F 运行组中是否存在所有的必需 F 块。
9. 对于每个 F 运行组，请检查 F 运行组信息中的以下值是否与您组态的值相对应：
 - F-CALL 的编号
 - 被调用的 F 程序块的编号
 - 关联背景数据块的编号（如果适用）
 - F 运行组的最大周期时间
 - F 运行组通讯 DB 的编号（如果适用）

11.2 检查打印输出

10. 对于 F 运行组中寻址的每个 F-I/O，请进行以下检查：

- 根据 F-I/O 的起始地址，检查安全程序中使用的符号名称和 F-I/O DB 的编号是否属于合适的 F-I/O。
- 检查 F_Monitoring_Time 的值与“硬件组态”(Hardware configuration) 打印输出中具有相同起始地址的 F-I/O 的相应值（或故障安全 DP 标准从站/标准 I/O 设备的“F_WD_Time”）是否匹配。
- 在 PROFINET IO 上或在基于 IE/PB 链接的 PROFIBUS DP 和 PROFINET IO 上的混合组态中使用 F-I/O 时，请检查 PROFIsafe 是否处于 V2 模式。
- 检查钝化类型是否与您组态的值相对应。

11. 检查附加信息：

- 检查“可以取消激活安全模式”(Safety mode can be deactivated) 设置是否与您组态的值相对应。
- 根据总页数计算，检查项目数据的打印输出是否完整。

参见

打印输出项目数据 (页 281)

11.3 在将安全程序下载到 F-CPU 之后进行的检查

引言

请按照『下载安全程序』一章中的说明将 S7 程序下载到 F-CPU。然后，执行下述检查。

说明

必须使用“安全程序”(Safety Program) 对话框进行验收测试前的最后一次 F 块下载。仅下载更改内容并不够。

下载后还需要执行检查

1. 将安全程序下载到 F-CPU 之后，请检查以下事项：

- 检查块文件夹中所有具有 F 属性的 F 块的在线集体签名与已验收的离线打印输出中的集体签名是否匹配。
- 验证在线安全程序是否不包含未使用的 F-CALL。
- 验证 F-CPU 中存在的 F-CALL 块是否不多于两个。

如果情况并非如此，请检查以确定是否已将安全程序下载到正确的 F-CPU；如果需要，请重新下载安全程序。

说明

如果重新进行测试，您可以通过将块文件夹中所有具有 F 属性的 F 块的在线集体签名与已验收的离线打印输出中的集体签名进行比较，来确定 F-CPU 是否包含正确的安全程序。

如果没有可用于进行重新测试的安装有 *S7 Distributed Safety V5.4* 的编程设备或 PC，您可以使用操作员监视和控制系统从 F 共享 DB 读出安全程序的集体签名。可以从“安全程序”(Safety program) 打印输出中获取安全程序集体签名 (“F_PROG_SIG”变量) 所在 F 共享 DB 中的地址。如果您不必执行操纵，则只能使用该选项。

参见

下载安全程序 (页 262)

11.4 更改的验收测试

引言

对于更改的验收测试，必须使用与初始验收测试相同的操作步骤（请参阅『系统验收测试概述』一章）。

对于更改的验收测试，只需检查硬件配置和 F 块的以下方面，并执行以下功能测试即可：

- 检查硬件配置打印输出中已更改的或新添加的 F-I/O 的安全相关参数。
- 检查 F 块打印输出中已更改的或新添加的 F 块。
- 检查安全程序打印输出中已修改的 F 应用程序块和 F 系统块的签名和初始值签名是否与《认证报告》的『附件 1』中指定的签名相匹配。
- 执行更改的功能测试。

确定更改的基本步骤

要确定安全相关的更改，请将已修改且要进行验收测试的安全程序中的“安全程序”(Safety program) 打印输出中信息部分内的两个集体签名与已验收安全程序的打印输出中的签名进行比较。

如果签名不同，则说明 F-CPU 和/或 F-I/O 的组态中和/或安全程序中存在安全相关的更改。

检测 F-I/O 参数分配中安全相关的更改

要确定安全程序中寻址的 F-I/O 的参数分配中安全相关的更改，请将“安全程序”(Safety program) 打印输出的“寻址的 F-I/O”部分中所有 F-I/O 的参数 CRC 与已验收安全程序的打印输出中的参数 CRC 进行比较。

如果 F-I/O 的“参数 CRC”不同，则说明此 F-I/O 的参数分配中存在安全相关的更改（例如对于 PROFIsafe 地址）。

在这种情况下，也需要将已修改硬件配置的打印输出中的“参数 CRC（无 F 地址）”或故障安全 DP 标准从站/标准 I/O 设备的“F_Par_CRC（无 F 地址）”与已验收硬件配置的打印输出中的相应循环冗余检查进行比较。

硬件配置的打印输出包含 F-I/O 相关模块说明中的此信息。如果此信息相同，则仅更改了 PROFIsafe 地址。在这种情况下，您不必单独检查 F-I/O 的其他安全相关参数。请确保所有已组态 F-I/O 的 PROFIsafe 目标地址仍与所有其他地址不同。

如果您要确定所有已组态 F-I/O 参数分配中的安全相关更改，必须在硬件配置打印输出中直接比较“参数 CRC”或故障安全 DP 标准从站/标准 I/O 设备的“F-Par_CRC”。

请不要忘记比较通过安全相关的智能从站与从站通讯进行寻址的 F-I/O 的参数 CRC。

检测 F-I/O 起始地址的更改

要确定安全程序寻址的 F-I/O 的起始地址中的更改，请将“安全程序”(Safety program) 打印输出的“寻址的 F-I/O”部分中所有 F-I/O 的起始地址与已验收安全程序的打印输出中的起始地址进行比较。

如果要确定所有已组态 F-I/O 的起始地址中的更改，必须在硬件配置打印输出中直接比较更改。

检测安全程序中的更改

要确定安全程序中的更改，请将更改的安全程序与保存的已验收程序进行离线比较（使用“安全程序”[Safety Program] 对话框中的“比较...”[Compare...] 按钮）。

这可让您识别出已更改的 F-Block。通过比较打印输出（“功能块/梯形图”[Function Block Diagram/Ladder Diagram] 打印内容）来确认您创建的 F 块（F-PB、F-FB、F-FC 和 F-DB）中的更改。

使用标准用户程序中的软件包

对于可与标准程序及安全程序并行使用的软件包（例如 SW 冗余），必须遵守的常规条件可能适用：

说明

如果安全程序占用了软件包所需的块编号（用于 FB、DB 和 FC），那么为了软件包的后续使用，可能需要更改安全程序，以释放块编号。这需要对安全程序中的更改执行其他验收测试。

参见

下载安全程序 (页 262)

比较安全程序 (页 275)

测试安全程序 (页 291)

操作和维护

12.1 有关安全程序的安全模式的注意事项

引言

请注意以下有关安全程序的安全模式的重要注意事项。

使用模拟设备/模拟程序



警告

如果操作可生成安全消息帧（例如基于 PROFIsafe）的模拟设备或模拟程序，并通过总线系统（例如 PROFIBUS DP 或 PROFINET IO）将其提供给 S7 Distributed Safety F 系统，则必须使用组织措施（例如操作监视和手动安全关闭）来确保 F 系统的安全。

如果使用 STEP 7 的 S7-PLCSIM 功能来模拟安全程序，则不必采取这些措施，因为 S7-PLCSIM 无法与实际的 S7 组件建立在线连接。

请注意，举例来说，协议分析器可能不会执行可再生带有正确时间特性的记录消息帧顺序的功能。

通过编程设备或 PC、模式选择器或通讯功能触发 STOP



警告

使用编程设备或 PC 接口、模式选择器或通讯功能从 STOP 模式到 RUN 模式的切换未互锁。例如，只需在编程设备或 PC 上操作一个按键就能从 STOP 模式切换到 RUN 模式。出于此原因，通过编程设备或 PC、模式选择器或通讯功能设置的 STOP 不必视为安全条件。

因此，执行维护工作时，请始终直接在设备上关闭 F-CPU。

由 SFC 46“STP”启动的 F-CPU 停机



警告

可以非常容易地（且不必特意地）从编程设备或 PC 中取消由 SFC46“STP”触发的 STOP 状态。出于此原因，SFC46 启动的 F-CPU STOP 不是故障安全 STOP。

参见

编写启动保护程序 (页 99)

测试安全程序概述 (页 288)

12.2 更换软件和硬件组件

更换软件组件

在编程设备或 PC 上更换软件组件时（例如使用新版 *STEP 7*），必须注意这些产品的文档和自述文件中有关向上和向下兼容性的注意事项。

更换硬件组件

S7 Distributed Safety 的硬件组件（F-CPU、F-I/O、电池等）的更换方式与标准自动化系统中的更换方式相同。

在操作过程中拆除和插入 F-I/O

可以在操作过程中拆除和插入 F-I/O（与标准 F-I/O 相同）。但是请记住，在使用中更换 F-I/O 模块可导致 F-CPU 中发生通讯错误。

必须在安全程序中 F-I/O DB 的 ACK_REI 变量中确认通讯错误。否则，F-I/O 将保持钝化状态。

CPU 操作系统更新

检查 CPU 操作的 F 有效性：使用新 CPU 操作系统（操作系统更新）时，必须检查正在使用的 CPU 操作系统是否已获准用于 F 系统。

在《认证报告》的附录中指定了具有保证的 F 能力的最低 CPU 操作系统版本。必须考虑此信息和有关新 CPU 操作系统的所有注意事项。

接口模块的操作系统更新

使用接口模块（例如 ET 200S 的 IM 151-1 HIGH FEATURE）的新操作系统（有关操作系统更新，请参阅 *STEP 7* 在线帮助）时，必须遵守以下要求：

如果为操作系统更新选择了“下载后激活固件”(Activate firmware after download) 复选框，则 IM 会在加载操作成功后自动复位，并且随后将在新操作系统上运行。IM 启动后，整个 F-I/O 都会被钝化。

F-I/O 以与发生通讯错误时相同的方式重新集成，即需要确认 F-I/O DB 中的 ACK_REI 变量。

预防性维护（检测测试）

经过验证的 F 系统组件概率值所保证的普通组态检测测试间隔为 10 年。有关详细信息，请参考 F-I/O 手册。复杂电子器件的检测测试通常指更换为未使用的器件。如果由于特定原因，您需要检测测试的间隔在 10 年以上，请与您的 Siemens 销售代表联系。

通常，传感器和执行器需要的检测测试间隔较短。

删除 *S7 Distributed Safety*

要删除该软件，请参阅『安装/删除 *S7 Distributed Safety* V5.4 SP4 选件包』一章。

F 系统硬件的拆除和处理方式与标准自动化系统相同；请参考相应的 *硬件手册*。

参见

安装/删除 *S7 Distributed Safety* V5.4 SP4 选件包 (页 19)

F-I/O 访问 (页 101)

12.3 诊断指南

引言

本章介绍了出错时可以对系统评估诊断功能进行的编译。大多数的诊断功能与标准自动化系统中的诊断功能相同。步骤顺序表示了一个建议。

评估诊断功能的步骤

步骤	操作步骤	参考
1	<p>评估硬件（F-CPU、F-I/O）上的 LED：</p> <ul style="list-style-type: none"> • F-CPU 上的 BUSF LED：当 PROFIBUS DP/PROFINET IO 上发生通讯错误时闪烁； 对 OB85 和 OB121 编程之后，当出现编程错误时（例如未装载背景数据块）亮起 • F-CPU 上的 STP LED：当 F-CPU 处于 STOP 模式时亮起 • F-I/O 上的故障 LED：单个 F-I/O 中发生任何故障时，SF-LED（组错误 LED）均会亮起 	F-CPU 和 F-I/O 手册
2	<p>在 STEP 7 中评估诊断缓冲区：</p> <p>在 <i>HW Config</i> 中，请使用 PLC > 模块状态 (Module Information) 菜单命令读出模块（F-CPU、F-I/O、CP）的诊断缓冲区</p>	<i>STEP 7 在线帮助</i> 以及 F-CPU 和 F-I/O 手册
3	<p>评估 STEP 7 中的栈：</p> <p>如果 F-CPU 处于 STOP 模式，请在 <i>HW Config</i> 中使用 PLC > 模块状态 (Module Information) 菜单命令以连续顺序读出以下信息：</p> <ul style="list-style-type: none"> • B 栈：检查安全程序的 F 块是否触发了 F-CPU 的 STOP 模式 • U 栈 • L 栈 	<i>STEP 7 在线帮助</i>

步骤	操作步骤	参考
4	<p>使用测试和调试功能或在标准用户程序中评估 F-I/O DB 的诊断变量</p> <p>评估 F-I/O DB 中的 DIAG 变量</p>	『F-I/O 访问』一章
5	<p>使用测试和调试功能或在标准用户程序中评估 F 应用程序块的背景数据块诊断参数：</p> <ul style="list-style-type: none"> • 在分配的背景数据块中针对 F_MUTING、F_1oo2DI、F_2H_EN、F_MUT_P、F_ESTOP1、F_FDBBACK 和 F_SFDOOR 评估以下参数： <ul style="list-style-type: none"> - DIAG 参数 • 在分配的背景数据块中针对 F_SENDDP 或 F_RCVDP 评估以下参数： <ul style="list-style-type: none"> - RETVAL14 参数 - RETVAL15 参数 - DIAG 参数 • 在分配的背景数据块中针对 F_SENDS7 或 F_RCVS7 评估以下参数： <ul style="list-style-type: none"> - STAT_RCV 参数 - STAT_SND 参数 - DIAG 参数 	与相关 F 应用程序块有关的章节

评估 F-I/O DB 或背景数据块的诊断变量或参数

说明

以下诊断变量/参数为您提供了详细的诊断信息：DIAG、RETVAL14、RETVAL15、STAT_RCV 和 STAT_SND。可使用编程设备上的测试和调试功能或使用操作员监视和控制系统来读出这些参数，也可在标准用户程序中对其进行评估。

不得在安全程序中访问这些参数。

评估标准用户程序中的诊断变量或参数

请勿在安全程序中评估诊断变量或参数，而应该使用以下操作步骤：

1. 以具有完整资格的 DB 访问方式，将上述变量/参数的诊断信息从 F-I/O DB 或相应背景数据块中装载到标准用户程序中（F-I/O DB 实例：L "F00005_4_8_F_DI_DC24V".DIAG）。如有必要，请在符号表中为背景数据块分配符号名。
2. 将诊断信息放入标准用户程序中，例如使用“T MB x”指令将其放入位存储器地址区中。
3. 之后，可以评估标准用户程序中诊断信息的各个位，即此实例中的 M x.y。

RETVAL14 和 15 的相关提示

RETVAL14 和 RETVAL15 参数中包含的诊断信息对应于 SFC 14 和 SFC 15 的诊断信息。有关说明，请参考有关 SFC 14 和 SFC 15 的 *STEP 7 在线帮助*。

STAT_RCV 和 STAT_SND 的相关提示

STAT_RCV 参数中包含的诊断信息对应于 SFB 9/FB 9 的 STATUS 参数中包含的诊断信息。STAT_SND 参数中包含的诊断信息对应于 SFB 8/FB 8 的 STATUS 参数中包含的诊断信息。有关说明，请参考有关 SFB 8 和 SFB 9 的 *STEP 7 在线帮助*。

参见

F-I/O 访问 (页 101)

核对清单

A.1 核对清单

故障安全自动化系统的生命周期

下表包含的核对清单总结了故障安全 S7 Distributed Safety 系统生命周期中的所有活动（包括在各阶段中必须遵守的要求和规则）。

核对清单

注：

- 引用本文档的独立章节参考。
- “SM”表示《SIMATIC S7 中的安全工程》系统手册。
- “F-SM 手册”表示《自动化系统 S7-300，故障安全信号模块》手册。
- “F 模块手册”表示《ET 200S 分布式 I/O 系统，故障安全模块》手册。
- “ET 200eco 手册”表示《ET 200eco 分布式 I/O 站，故障安全 I/O 模块》手册。
- “ET 200pro 手册”表示《ET 200pro 分布式 I/O 站，故障安全模块》手册。

阶段	要求/规则	参考	检查
计划			
要求：“安全要求规格” 可用于适用的应用程序	与过程相关	-	
系统结构的规范	与过程相关	-	
系统组件的功能和子功能分配	与过程相关	『产品概述』一章； SM, 第 1.5、2.4 章	
传感器和执行器的选择	执行器的要求	F-SM 手册, 第 6.5 章； F 模块手册, 第 4.5 章； ET 200eco 手册, 第 5.5 章 ET 200pro 手册, 第 4.4 章	

A.1 核对清单

阶段	要求/规则	参考	检查
各个组件所需安全属性的规范	<ul style="list-style-type: none"> • DIN V 19 250 • IEC 61508 	SM, 第 4.7、4.8 章	
组态			
安装选件包	安装要求	『安装/删除...』一章	
S7 组件的选择	组态规则	『硬件和软件组件』一章； SM, 第 2.4 章； F-SM 手册, 第 3 章； F 模块手册, 第 3 章； ET 200eco 手册, 第 3 章 ET 200pro 手册, 第 2 章	
硬件的组态	<ul style="list-style-type: none"> • F 系统规则 • 根据《认证报告》的『附录 1』验证所使用的硬件组件 	『组态概述』一章、『组态...的特性』一章； 《认证报告》的『附录 1』	
F-CPU 的组态	<ul style="list-style-type: none"> • 保护级别, “CPU 包含安全程序” • 密码 • 定义/设置 F-特定参数 • F 运行组的调用时间, 将在此期间执行安全程序, 按照要求和安全规则进行定义 (与标准系统相同) 	『组态 F-CPU』一章； S7-300 标准； S7-400 标准； IM 151-7 CPU	
F-I/O 的组态	<ul style="list-style-type: none"> • 安全模式设置 • 组态监视时间 • 定义传感器互连/评估的类型 • 定义诊断特性 • 分配符号名称 	『组态 F-I/O』一章及后续章节； SM, 『附录 A』； F-SM 手册, 第 3、9、10 章； F 模块手册, 第 2.4、7 章； ET 200eco 手册, 第 3、8 章； ET 200pro 手册, 第 2.4、8 章	
保存、编译和装载硬件配置	<ul style="list-style-type: none"> • 系统数据已生成 • F 共享 DB、F 系统块和 F-I/O DB 已生成 	—	

阶段	要求/规则	参考	检查
编程			
定义程序设计和结构	<ul style="list-style-type: none"> 注意编程警告和注意事项 根据《认证报告》的『附录 1』验证所使用的软件组件 	『编程概述』一章、『编程结构...』一章、『定义编程结构』一章、『对启动保护进行编程』一章； 《认证报告》的『附录 1』	
创建/插入 F 块	<ul style="list-style-type: none"> 按照程序结构的要求生成、编辑和保存 F-FB、F-FC 及 F-DB 适用于下列操作的规则： <ul style="list-style-type: none"> F-I/O 访问 F-I/O 的钝化和重新集成 插入 Distributed Safety F 库 (V1) 和用户创建的 F 库中的 F 块 安全相关的 CPU 与 CPU 通讯 与标准用户程序的通讯 	『在 Distributed Safety F 库(V1)的 F-FBD/F-LAD 中创建 F 块』一章 『F-I/O 访问』一章 『执行用户确认』一章 『F 库』一章 『对通讯进行组态和编程』一章 『标准用户程序和安全程序之间的数据交换』一章	
创建 F 运行组	<ul style="list-style-type: none"> 创建 F-CALL 将 F-FB/F-FC 分配给 F-CALL 按照要求（根据过程和安全规则）设置 F 运行组的最长循环时间 为 F 运行组通讯创建 DB 	『定义 F 运行组』一章； SM, 『附录 A』	
编译安全程序		『编译安全程序』一章	
执行安全程序调用	直接在 OB（例如 OB35）、FB 或 FC 中调用 F-CALL 块	『定义 F 运行组』一章	

A.1 核对清单

阶段	要求/规则	参考	检查
安装			
硬件配置	<ul style="list-style-type: none"> • 安装规则 • 接线规则 	『组态概述』一章、『组态...的特性』一章； <i>F-SM 手册</i> , 第 5、6 章； <i>F 模块手册</i> , 第 3、4 章； <i>ET 200eco 手册</i> , 第 3、4 章； <i>ET 200pro 手册</i> , 第 2、3 章	
调试、测试			
上电	调试规则（与标准系统相同）	S7-300 标准； S7-400 标准	
下载安全程序和标准用户程序	<ul style="list-style-type: none"> • 下载规则 • 程序标识规则 • 比较安全程序 	『下载安全程序』一章 『比较安全程序』一章	
测试安全程序	<ul style="list-style-type: none"> • 取消激活安全模式的规则 • 更改安全程序数据的操作步骤 	『安全程序的功能测试或通过程序标识进行保护』一章、『测试安全程序』一章、『取消激活安全模式』一章	
更改安全程序	<ul style="list-style-type: none"> • 取消激活安全模式的规则 • 修改安全程序的规则 	『在 RUN 模式下修改安全程序』一章、『取消激活安全模式』一章、『删除安全程序』一章	
测试安全相关的参数	组态规则	『打印输出安全程序的项目数据』一章； <i>F-SM 手册</i> , 第 4、9、10 章； <i>F 模块手册</i> , 第 2.4、7 章； <i>ET 200eco 手册</i> , 第 3、8 章； <i>ET 200pro 手册</i> , 第 2.4、8 章	
验收测试	<ul style="list-style-type: none"> • 验收测试规则和注意事项 • 打印输出 	『系统验收测试』一章	

阶段	要求/规则	参考	检查
操作、维护			
常规操作	操作注意事项	『...安全模式的注意事项』一章	
访问保护		『访问保护』一章	
诊断	对故障和事件的响应	『诊断指南』一章	
更换软件和硬件组件	<ul style="list-style-type: none"> • 模块更换规则 • F-CPU 操作系统的更新规则（与标准系统相同） • 软件组件更新规则 • IM 操作系统更新注意事项 • 预防性维护注意事项 	『更换软件和硬件组件』一章、 『F-I/O 访问』一章； <i>STEP 7</i> 在线帮助	
删除、拆卸	<ul style="list-style-type: none"> • 删除软件组件的注意事项 • 拆卸模块的注意事项 	『安装/删除...』一章、『更换软件和硬件组件』一章	

参见

概述 (页 15)

安装/删除 S7 Distributed Safety V5.4 SP4 选件包 (页 19)

组态概述 (页 25)

对 F 系统进行组态的特性 (页 26)

组态 F-CPU (页 28)

对 F-I/O 进行组态 (页 37)

访问保护概述 (页 49)

编程概述 (页 59)

S7 Distributed Safety 中安全程序的结构 (页 61)

定义程序结构 (页 81)

使用 F-FBD/F-LAD 创建 F 块 (页 82)

安全程序的 F 运行组的规则 (页 91)

F-I/O 访问 (页 101)

Distributed Safety F-Library (V1) 概述 (页 177)

自定义 F 库 (页 253)

编译安全程序 (页 260)

下载安全程序 (页 262)

在 RUN 模式下修改安全程序 (页 273)

比较安全程序 (页 275)

删除安全程序 (页 278)

打印输出项目数据 (页 281)

取消激活安全模式 (页 288)

测试安全程序 (页 291)

系统验收测试概述 (页 297)

有关安全程序的安全模式的注意事项 (页 307)

更换软件和硬件组件 (页 308)

诊断指南 (页 310)

词汇表

CRC

循环冗余检查 -> CRC 签名

CRC 签名 CRC Signature

通过安全消息帧中包含的 CRC 签名确保 -> 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。

DP/DP 耦合器 DP/DP Coupler

S7 Distributed Safety 中连接两个 PROFIBUS DP 子网的设备，可以在不同 -> F-CPU 中的 -> 安全程序之间实现主站与主站的通讯。

一个 DP/DP 耦合器在安全相关的主站与主站通讯中至少涉及两个 F-CPU。每个 F-CPU 均通过其 PROFIBUS DP 接口链接至 DP/DP 耦合器。

F 共享 DB F-shared DB

F 共享 DB 是一个故障安全数据块，它包含 -> 安全程序的所有共享数据和 F 系统所需的其他信息。在 HW Config 中保存并编译硬件配置时，将自动插入并扩展 F 共享 DB。使用其符号名 F_GLOBDB，用户可以评估 -> 安全程序的某些数据。

F 块 F-blocks

以下故障安全块称为 F 块：

- 用户使用编程语言 -> F-FBD/F-LAD、F-CALL 和 F-DB 创建的块
- 用户从 F 库中选择的块
- 自动添加到 -> 安全程序中的块（-> F-SB、-> 自动生成的 F 块和 -> F 共享 DB）

在“安全程序”(Safety Program) 对话框和 *SIMATIC 管理器* 中所有 F 块均以黄色背景显示。

F 通讯 DB F-Communication DBs

F 通讯 DB 是故障安全数据块，用于通过 S7 连接进行安全相关 CPU-CPU 通讯。

F 系统 F-systems

-> 故障安全系统

F 系统块 F-system blocks

包含 -> F-SB 和 -> F 共享 DB 的 *Distributed Safety* F 块的块文件夹。

F 应用程序块 F-application blocks

块文件夹，用于包含 -> F 应用程序块的 *Distributed Safety* F 库。

F 应用程序块 F-Application Blocks

F 应用程序块是指 *Distributed Safety* F 库中带有预制功能的 F 块（F-FB、F-FC）。在 -> F-PB 中以及在其他 -> F-FB 和 -> F-FC 中，用户可以调用 F 应用程序块。

F 运行组 F-runtime group

-> 安全程序由一个或两个 F 运行组组成。F 运行组是由多个关联 F 块组成的逻辑结构。它由 F 系统在内部生成。F 运行组由以下 F 块组成：

-> F-CALL、-> F-PB、-> F-FB/ -> F-FC（如果适用）、-> F-DB（如果适用）、-> F-I/O DB、*Distributed Safety* F 库和用户创建的 F 库的 F 块、背景数据块、-> F-SB 和 -> 自动生成的 F 块。

F 运行组通讯的 DB DB for F-Runtime Group Communication

安全程序的 F 运行组之间进行安全相关通讯的 -> F-DB。

F 属性 F-attribute

-> 安全程序中的所有 -> F 块都具有 F 属性（在“安全程序”[Safety Program] 对话框中通过 F 块符号中的“F”识别）。-> 成功编译安全程序后，仅 -> 安全程序的块具有 F 属性。

F-CALL

F-CALL 是用于 S7 Distributed Safety 中的 -> 安全程序的“F-Call 块”。

F-CALL 是用户使用“F-CALL”编程语言创建的功能，无法进行编辑。F-CALL 从 -> 标准用户程序中调用 -> F 运行组。F-CALL 包含一个对 -> F-PB 的调用和多个对自动添加的 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 的故障安全功能，可以在 F-CPU 中运行 -> 标准用户程序，此外还可以在其中运行安全程序。

F-DB

可以从安全程序中的任何地方进行读/写访问的可选故障安全数据块（例外：F 运行组通讯的 DB）

F-FB

F-FB 是故障安全功能块（使用背景数据块），用户可以使用 -> F-FBD 或 -> F-LAD 在其中编写 -> 安全程序。

F-FBD

F-FBD 是一种用于在 S7 Distributed Safety 中编写 -> 安全程序的编程语言。可以使用 STEP 7 中的标准 *FBD/LAD 编辑器* 进行编程。

F-FC

F-FC 是故障安全 FC，用户可以使用 -> F-FBD 或 -> F-LAD 在其中编写 -> 安全程序。

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，专用于在 *S7 Distributed Safety* 中进行集成。以下 F-I/O 模块可用于 *S7 Distributed Safety*:

- ET 200eco 故障安全 I/O 模块
- S7-300 故障安全信号模块 (-> F-SM)
- ET 200S 的 -> 故障安全模块
- ET 200pro 的 -> 故障安全模块
- -> 故障安全 DP 标准从站
- -> 故障安全标准 I/O 设备

F-I/O DB

F-I/O DB 是故障安全数据块，用于 *S7 Distributed Safety* 中的 ->F-I/O。在 *HW Config* 中进行编译时，将为每个 F-I/O 自动创建一个 F-I/O DB。F-I/O 数据块包含用户可在安全程序中评估的变量，或者可以或必须写入到如下所示内容的变量：

- 要在发生通讯错误、F-I/O 故障或通道故障后重新集成 F-I/O
- 应将 F-I/O 作为特殊安全程序条件的结果进行钝化（例如，组钝化）时
- 为故障安全 DP 标准从站重新分配参数
- 为了评估是输出故障安全值还是输出过程数据

F-I/O 故障 F-I/O faults

F-I/O 故障是 F-I/O 的模块相关的故障（例如通讯错误或参数分配错误）

F-LAD

-> F-FBD

F-Module

-> 故障安全模块

F-PB

F-PB 是用于在 S7 Distributed Safety 中编写故障安全 -> 安全程序的“引导性故障安全块”。F-PB 是一个 -> F-FB 或 -> F-FC，用户将其分配给 -> F 运行组的 -> F-CALL。

F-PB 包含 F-FBD 或 F-LAD 安全程序、用于程序结构化的其他 -> F-FB/F-FC 的所有调用以及所有 *Distributed Safety* F 库的 -> F 应用程序块文件夹中的所有 -> F 应用程序块和 -> 用户创建的 F 库中的 F 块。

F-SB

F-SB 是故障安全系统块，为了从用户安全程序中生成可执行安全程序，在编译 -> 安全程序时将自动插入并调用该块。

F-SM

F-SM 是 S7-300 故障安全信号模块，可用于在 S7 300 中作为中央模块或在 ET 200M 分布式 I/O 系统中作为分布式模块进行安全相关的操作（在 -> 安全模式下）。F-SM 具有集成的 -> 安全功能。

i 参数 i-Parameter

-> 故障安全 DP 标准从站的各个参数

MSR

仪表和控制技术

PROFIsafe

PROFIBUS DP/PA 和 PROFINET IO 的安全相关的总线规约用于 > F 系统中的 -> 安全程序和 -> F-I/O 之间的通讯。

PROFIsafe 地址 PROFIsafe Address

每个 -> F-I/O 模块都具有一个 PROFIsafe 地址。必须在 STEP 7 的 *HW Config* 中组态 PROFIsafe 地址并且通过 F-I/O 上的开关设置地址。

S7-PLCSIM

S7-PLCSIM 应用程序使您能够在编程设备或 PC 的模拟自动化系统上执行和测试程序。由于模拟完全发生在 STEP 7 中，因此无需任何硬件（CPU、I/O）。

安全程序 Safety Program

安全程序是安全相关的用户程序。

安全功能 Safety Function

安全功能是内置于 -> F-CPU 和 -> F-I/O 中的机制，使 -> F-CPU 和 -> F-I/O 可以在 -> 故障安全系统中使用这些功能。

依据 IEC 61508：安全系统将执行安全功能，以便将系统 -> 维持在安全模式下，或发生特殊故障时将系统置于安全状态中。（-> 用户安全功能）

安全模式 Safety Mode

1. 安全模式是 -> F-I/O 的工作模式，允许使用 -> 安全帧 -> 进行安全相关的通讯。
2. 安全程序的工作模式。在安全程序的安全模式下，将激活所有用于故障检测和响应的安全机制。在安全模式下，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）。

安全完整性等级 Safety Integrity Level

安全完整性等级 (SIL) 是在 IEC 61508 和 prEN 50129 中定义的安全等级。安全完整性等级越高，用于避免和控制系统故障以及随机硬件故障的操作就越严格。

S7 Distributed Safety 可在最高为 SIL3 的安全模式下使用。

安全相关的通讯 Safety-related communication

安全相关的通讯用于交换故障安全数据。

安全消息帧 Safety Message Frame

在 -> 安全模式下，数据通过安全帧在 -> F-CPU 和 -> F-I/O 之间传送，或通过安全相关的 CPU-CPU 通讯在 F-CPU 之间传送。

安全协议 Safety Protocol

-> 安全消息帧

安全状态 Safe State

-> 故障安全系统中安全概念的基本原理是：对于所有过程变量，均存在一个安全状态。对于数字 -> F-I/O，该值始终为“0”。

标准模式 Standard Mode

标准模式是 -> F-I/O 的工作模式，在该模式下无法通过 ->安全帧进行 ->安全相关的通讯，仅可进行 -> 标准通讯。

标准通讯 Standard Communication

标准通讯用于交换非安全相关的数据。

标准用户程序 Standard User Program

标准用户程序是非安全相关的用户程序。

程序签名 Program Signature

-> 集体签名

传感器评估 Sensor Evaluation

有两种类型的传感器评估：

- 1oo1 评估 — 读入传感器信号一次
- 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

电压组 Voltage Group

在 ET 200S 和 ET 200pro 分布式 I/O 系统中：电压组是由一个电源模块供电的一组电子模块。

钝化 Passivation

具有输入的 -> F-I/O 模块中发生钝化时，-> F 系统为安全程序提供的是故障安全值 (0)，而不是故障安全输入处 PII 中未决的过程数据。

具有输出的 F-I/O 模块中发生钝化时，F 系统将故障安全值 (0)（而不是 PIQ 中由安全程序提供的输出值）传送给故障安全输出。

访问保护 Access protection

必须对 -> 故障安全系统进行保护以防发生危险的、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。

非对等传感器 Non-equivalent Sensor

非对等传感器是一个双向开关，在 -> 故障安全系统（双通道）中，它被连接至 -> F-I/O 模块的两个输入（适用于传感器信号的 1oo2 评估；-> 传感器评估）。

故障安全 DP 标准从站 Fail-safe DP standard slaves

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。它们的表现必须符合 IEC 61784-1:2002 Ed1 CP 3/1 和 PROFIsafe 规约。GSD 文件用于组态故障安全 DP 标准从站。

故障安全 I/O 模块 Fail-Safe I/O Modules

ET 200eco 模块是可用于安全相关的操作（在 -> 安全模式下）的故障安全 I/O 模块。这些模块具有集成的 -> 安全功能的特点。它们的表现符合 IEC 61784-1:2002 Ed1 CP 3/1 和 PROFIsafe 总线规约。

故障安全标准 I/O 设备 Fail-safe standard I/O devices

故障安全标准 I/O 设备是根据 IO 协议在 PROFINET 上运行的标准设备。它们的表现必须符合 IEC 61784-1:2002 Ed1 CP 3/3 和 PROFIsafe 总线规约（在 V2 模式下）。GSD 文件用于组态故障安全 DP 标准从站。

故障安全模块 Fail-Safe Modules

ET 200S 和 ET 200pro 模块，可用于 ET 200S 和 ET 200pro 分布式 I/O 系统中安全相关的操作（在 -> 安全模式中）。这些模块具有集成的 -> 安全功能。它们的表现必须符合 IEC 61784-1:2002 Ed1 CP 3/1 和 3/3 以及 PROFIsafe 总线规约。

故障安全系统 Fail-Safe Systems

故障安全系统 (F 系统) 是保持在安全状态的系统, 或发生特殊故障后立即切换到其他安全状态的系统。

故障响应功能 Fault Reaction Function

-> 用户安全功能

故障响应时间 Fault Reaction Time

F 系统的最大故障响应时间是指从发生错误到所有受到影响的安全故障输出做出安全反应的时间间隔。

集体签名 Collective Signatures

集体签名用于唯一识别 F-CPU 和 F-I/O 的安全程序及安全相关的参数的特定状态。集体签名对于安全程序的预备验收测试 (例如由 -> 专家执行) 来说非常重要。

以下签名由编程软件显示而且还可以打印输出:

- 块文件夹中所有具有 F 属性的 F 块的集体签名
- 安全程序的集体签名

这两个签名必须与验收测试一致。

检测测试间隔 Proof Test Interval

检测测试间隔之后必须将组件置入无故障状态。即, 由未使用的组件进行替换或证明其完全无故障。

类别 Category

根据 EN 954-01 定义的类别

可在 -> 安全模式下 (最多可达类别 4) 使用 S7 Distributed Safety。

启动 F 系统 Startup of F-system

当 -> F-CPU 从 STOP 模式切换到 RUN 模式时, -> 标准用户程序将按照通常的方式启动。-> 安全程序启动时, 将使用装载存储器的值初始化所有具有 -> F 属性的数据块 (冷启动时也会执行该操作)。这意味着将丢失保存的错误信息。

-> F 系统将自动执行 -> F-I/O 的 -> 重新集成。

签名 Signature

-> 集体签名

取消钝化 Depassivation

-> 重新集成

取消激活的安全模式 Deactivated Safety Mode

取消激活的安全模式是指为进行测试、调试等操作而临时取消激活 -> 安全模式。

以下操作仅在取消激活的安全模式下才可执行：

- 在操作过程中（在 RUN 模式下），将 -> 安全程序的更改下载到 -> F-CPU。
- 测试功能（例如“修改”）或对 -> 安全程序数据进行的其他写访问（受限制）

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

通道故障 Channel Fault

通道相关的故障，例如断路或短路。

误差分析 Discrepancy Analysis

将对等或非对等的误差分析用于故障安全输入，以根据具有相同功能的两个信号的时间特性来确定错误。检测到两个相关输入信号的级别不同时（对于非对等测试，则在检测到的级别相同时），启动误差分析。在所谓的 -> 误差时间过去之后，将检查信号以确定差异（当检查非对等时）是否已消失。如果未消失，则存在误差错误。将在故障安全输入中 1oo2 传感器评估（-> 传感器评估）的两个输入信号之间执行误差分析。

误差时间 Discrepancy Time

误差时间是 -> 误差分析设置的一个时间段。如果误差时间设置得太长，则故障检测时间和 -> 故障响应时间将被不必要地延长。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，而不必要地降低了可用性。

用户安全功能 User safety function

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。用户仅需对用户安全功能进行编程。如果发生故障并且 F 系统无法再执行其实际用户安全功能，其将执行故障响应功能：例如，取消激活关联的输出并将 F-CPU 切换到 STOP 模式（如有必要）。

重新集成(下装) Reintegration

将自动从替换值 (0) 切换到过程数据 (-> F-I/O 模块的重新集成) 或用户在 F-I/O DB 中确认之后再此操作。重新集成的方法取决于以下因素：

- F-I/O 或 F-I/O 通道钝化的原因
- -> F-I/O DB 中的参数分配

对于具有输入的 -> F-I/O 模块，重新集成后，F 输入处 PII 中的未决过程数据将被再次提供给安全程序。F 系统会将安全程序中提供的 PIO 输出值传送给 F-I/O 的故障安全输出。

专家 Expert

系统通常是经过认证的，即系统的安全验收测试通常由独立的专家（例如，来自 TÜV）来实施。

自定义 F 库 Custom F-Libraries

用户创建的 F 库是指由用户创建的 F 库，它包含 F-FB、F-FC 和应用程序模板（网络模板）。

自动生成的 F 块 Automatically Generated F-Blocks

生成 -> 安全程序以便从用户编写的安全程序中产生可执行安全程序时，自动创建并且必要时启动的 -> F 块。

索引

A

ACK_NEC, 104
ACK_REI, 104
ACK_REI_GLOB, 232
ACK_REQ, 104

B

BOOL, 66

C

CPU 与 CPU 通讯, 25, 26, 131, 139, 150, 173
 安全相关的, 26, 131, 139, 150, 173
 安全相关的选项, 25
CPU 操作系统更新, 308

D

DIAG, 204, 209, 212, 222, 225, 229
 F_1oo2DI, 204
 F_2H_EN, 209
 F_ESTOP1, 222
 F_FDBACK, 225
 F_MUT_P, 212
 F_MUTING, 196
 F_RCVS7, 240
 F_SENDDP/F_RCVDP, 233
 F_SENDS7, 240
 F_SFDOOR, 229
 F-I/O DB, 104
Distributed Safety F 库 (V1), 177
 F 块, 63

目录, 59

Distributed Safety F-Library (V1): 概述, 177
DP/DP 耦合器, 138, 139
 组态安全相关的主站与主站通讯, 135
 编写安全相关的主站与主站通讯程序, 138, 139

E

EN, 209
ENO, 66

F

F 本地数据, 28
 最大可能的数量, 28
F 共享 DB, 63, 127, 253
F 块, 63
 F 运行组, 63
 存储写保护, 83
F 库, 177
 用户创建的, 253
F 应用程序块, 63
F 系统块, 63, 251
 概述, 251
F 运行组, 63
 F 块, 63
 F 运行组的规则, 91
 定义 F 运行组, 91
F 运行组的规则, 91
F 运行组通讯, 91
F 运行组通讯的 DB, 91
 定义, 91

- F 组件, 25
 - 组态, 25
- F 相关的选项卡, 26
- F 调用块, 63
- F 通讯 DB
 - 安全相关的 CPU 与 CPU 通讯, 171
 - 编程, 171
- F 程序块, 63, 91
 - 定义, 91
- F_1oo2DI, 204
- F_2H_EN, 209
- F_2HAND, 194
- F_ACK_GL, 232
- F_ACK_OP, 192
- F_BO_W, 248
- F_Check_SeqNr, 42
- F_CRC_Length, 42
- F_CTD, 183
- F_CTU, 182
- F_CTUD, 184
- F_Dest_Add, 42
- F_ESTOP1, 222
- F_FDBACK, 225
- F_GLOBDB, 127, 253
- F_INT_RD, 250
- F_INT_WR, 249
- F_IO_StructureDescCRC, 42
- F_MUT_P, 212
- F_MUTING, 196
 - DIAG 的结构, 196
- F_MUTING 并行, 212
- F_Par_Version, 42
- F_RCVDP, 233
 - DIAG 的结构, 233
 - 发生通讯错误时的行为, 233
 - 时序图, 233
 - 接收数据, 233
 - 编写安全相关的主站与主站通讯程序, 138, 139
 - 编写安全相关的主站与智能从站通讯程序, 148
 - 编写安全相关的智能从站与智能从站通讯程序, 148
- F_RCVS7, 240
- F_SCA_I, 181
- F_SENDDP, 233
 - DIAG 的结构, 233
 - 发生通讯错误时的行为, 233
 - 发送数据, 233
 - 时序图, 233
 - 编写安全相关的主站与主站通讯程序, 138, 139
 - 编写安全相关的主站与智能从站通讯程序, 148
 - 编写安全相关的智能从站与智能从站通讯程序, 148
- F_SENDS7, 240
- F_SFDOOR, 229
- F_SHL_W, 246
- F_SHR_W, 247
- F_SIL, 42
- F_Source_Add, 42
- F_TOF, 190
- F_TON, 188
- F_TP, 186
- F_W_BO, 248
- F_WD_Time, 42
- FB 179, 181
- FB 181, 182
- FB 182, 183
- FB 183, 184
- FB 184, 186
- FB 185, 188
- FB 186, 190
- FB 187, 192
- FB 188, 194
- FB 189, 196
- FB 190, 204

- FB 211, 209
 - FB 212, 212
 - FB 215, 222
 - FB 216, 225
 - FB 217, 229
 - FB 219, 232
 - FB 223, 233
 - FB 225, 240
 - FB 226, 240
 - FC 174, 246
 - FC 175, 247
 - FC 176, 248
 - FC 177, 248
 - FC 178, 249
 - FC 179, 250
 - F-CALL, 63, 81, 91
 - 定义, 91
 - F-CPU, 25, 57
 - 设置访问许可, 57
 - 更改 F-CPU 的现有密码, 57
 - F-CPU 的 F 参数, 28
 - F 功能块, 28
 - F 本地数据, 28
 - F 数据块, 28
 - PROFIsafe 地址的基数, 28
 - 组态, 28
 - F-CPU 的保护级别, 28
 - 组态, 28
 - F-DB, 87
 - 设置知识保护, 87
 - F-FB, 87
 - 设置知识保护, 87
 - F-FBD, 66
 - F-FBD 和 F-LAD 编程语言, 66
 - F-FBD 和 F-LAD 编程语言与标准 FBD 和 LAD 编程语
言之间的区别, 66
 - F-FC, 87
 - 设置知识保护, 87
 - F-I/O, 104
 - 在操作过程中拆除和插入, 308
 - F-I/O DB, 104
 - DIAG 的结构, 104
 - 评估诊断变量/参数, 310
 - 符号名, 47
 - F-I/O DB 的变量, 104
 - F-I/O DB 的符号名, 110
 - F-I/O 访问, 101
 - 通过过程映像, 101
 - 操作期间, 273
 - F-I/O 的故障安全值输出, 102
 - F-I/O 的故障安全输入/输出, 26
 - 分配符号, 26
 - F-I/O 的钝化和重新集成
 - 发生 F-I/O 故障和通道故障后, 115
 - 发生通讯错误后, 113
 - 启动 F 系统后, 111
 - F-I/O 故障和通道故障, 115
 - F-LAD, 66
- ## G
- GSD 文件, 42
 - 参数, 42
 - 组态, 42
- ## I
- IE/PB 连接器, 168
 - IM 151-1 High Feature (ET 200S) , 308
 - INT, 250

- Internet, 3
 - SIMATIC 文档, 3
 - 服务与支持, 3
- IPAR_EN, 104
- IPAR_OK, 104

- M**
- MMC, 269

- P**
- PASS_ON, 104
- PASS_OUT/QBAD, 104
- PN/PN 耦合器, 168
- PROFIBUS DP
 - 硬件组件, 16
- PROFIBUS IO
 - 硬件组件, 16
- PROFIsafe 地址设置, 37

- Q**
- QBAD, 104

- R**
- RETV14, 310
- RETV15, 310

- S**
- S7 Distributed Safety, 16, 308
 - 对软件进行组态和编程, 16
 - 产品概述, 8
 - 创建程序的步骤, 79
 - 安全功能的原理, 8
 - 删除, 308
- S7 Distributed Safety 中安全功能的原理, 8
- S7 Distributed Safety 中安全程序的结构, 61
- S7 Distributed Safety 故障安全系统, 8
 - S7 Distributed Safety 选件包, 16
 - 安全程序, 16
 - 硬件组件和软件组件, 16
- S7 连接, 131, 173
 - 对安全相关的通讯进行编程, 173
 - 安全相关的通讯, 通过, 131
- S7-PLCSIM, 262, 288
 - 下载到, 262
- SFC 46, 307
- Siemens Intranet, 3
 - SIMATIC 文档, 3
- STEP 7, 83
- STEP 7 指令, 66
- STL, 83
- STOP, 222
 - 由 SFC 46, 307
 - 通过通讯功能, 307
 - 通过编程设备或 PC, 307
 - 通过模式选择器, 307

- T**
- TIME, 66

- W**
- WORD, 66

- 一划**
- 一致, 259

三划

下载, 262

在, 262

在 SIMATIC 管理器或 FBD/LAD 编辑器中, 262

安全程序, 262

下载到 S7-PLCSIM, 262

大小, 262

自动生成的 F 块, 262

工业以太网, 131

安全相关的通讯, 通过, 131

工作存储器要求, 262, 267

安全程序, 262, 267

工作原理, 181, 204, 209, 212, 222, 225, 229, 246, 247, 248, 249, 250

ACK_REI_GLOB, 232

F_1oo2DI, 204

F_2H_EN, 209

F_2HAND, 194

F_ACK_OP, 192

F_BO_W, 248

F_CTD, 183

F_CTU, 182

F_CTUD, 184

F_ESTOP1, 222

F_FDBACK, 225

F_INT_RD, 250

F_INT_WR, 249

F_MUT_P, 212

F_MUTING, 196

F_RCVDP, 233

F_RCVS7, 240

F_SCA_I, 181

F_SENDDP, 233

F_SENDS7, 240

F_SFDOOR, 229

F_SHL_W, 246

F_SHR_W, 247

F_TOF, 190

F_TON, 188

F_TP, 186

F_W_BO, 248

四划

不一致, 259

不允许的地址区, 66

不允许的指令, 66

不允许的数据类型和参数类型, 66

从 F-DB 间接读取 INT 类型的数值, 250

从标准用户程序中读取数据

在 F 运行组的运行期间, 何时可进行更改, 129

双手操作监视, 209

双向连接, 135

反射挡光板, 196

反馈监视, 225

引言, 66

支持, 3

其它, 3

支持的地址区, 66

支持的指令, 66

支持的数据类型和参数类型, 66

文档, 3

其它, 3

范围, 3

比较安全程序, 275

订货号, 3

S7 Distributed Safety, 3

认证, 3

五划

- 主站与主站通讯, 135
 - 组态, 135
- 主站与智能从站通讯, 148
 - 组态, 145
- 主站与智能从站通讯的地址区
 - 分配, 143
 - 定义, 143
- 发生 F-I/O 故障和通道故障后的特性, 115
- 发生通讯错误后的行为, 113
- 可以取消安全模式, 29
- 对安全程序进行功能测试, 269
- 对安全程序进行完整的功能测试, 269
- 对话框, 262
- 对标准用户程序的修改, 273
- 打开 F 块, 291
- 打印
 - 安全程序, 281
- 打印输出项目数据, 281
- 未链接, 66
 - DB, 66
- 本文档用途, 3
- 本地 ID, 169
 - S7 连接的, 169
- 本地数据, 28
- 用户创建的 F 库, 253
- 用户安全功能, 8
 - 实例, 8
- 用户确认, 121, 123
 - 用于重新集成 F-I/O, 121, 123
 - 光幕中断期间, 196
 - 通过确认键, 121, 123
 - 通过操作员监视和控制系统, 121, 123
- 闪存卡, 269

六划

- 产品概述, 8
- 伙伴 ID, 169
 - S7 连接的, 169
- 传送带设备
 - 停止, 196
- 传感器对 1 上的误差错误, 196
 - 时序图, 196
- 光幕, 196
- 光幕中断, 196
- 光幕中断期间重新启动抑制, 212
 - F_MUT_P, 212
- 创建
 - F-FB/F-FC, 83
- 创建 OFF 延迟, 190
- 创建 ON 延迟, 188
- 创建安全程序, 79
- 创建安全程序的基本步骤, 79
- 创建和编辑 F-FB/F-FC, 83
- 创建脉冲, 186
- 创建程序段模板, 82
- 向右移 16 位, 247
- 向左移 16 位, 246
- 在 RUN 模式下修改安全程序, 273
- 在 SIMATIC 管理器或 FBD/LAD 编辑器中下载
 - 规则, 262
- 在 SIMATIC 管理器或 FBD/LAD 编辑器中下载 F 块的
 - 规则, 262
- 地址区, 66
 - 对于安全相关的智能从站与从站通讯, 160
 - 用于安全相关的主站与智能从站通讯, 143
 - 用于安全相关的智能从站与智能从站通讯, 154
- 地址设置, 37
 - PROFIsafe, 37
- 存储卡, 269
- 存储器复位, 269, 291

- 存储器要求, 262
 - 安全程序, 262
- 安全门监视, 229
- 安全相关的 CPU 与 CPU 通讯, 171
 - F 通讯 DB, 171
 - F_RCVDVP, 233
 - F_SENDDP, 233
 - 组态新程序, 273
 - 选项, 25
 - 编程, 131
 - 概述, 131
- 安全相关的 IO 控制器与 IO 控制器通讯, 168
- 安全相关的主站与主站通讯
 - 组态, 135
 - 编程, 139
- 安全相关的主站与主站通讯: 数据传输的限制, 142
- 安全相关的主站与智能从站通讯, 148
 - 组态, 145
 - 组态地址区, 143
 - 编程, 150
- 安全相关的参数, 26
 - 更改, 26
- 安全相关的通讯, 131
 - F 运行组之间, 91
- 安全相关的智能从站与从站通讯, 160
 - 组态, 162
 - 组态地址区, 160
- 安全相关的智能从站与智能从站通讯, 148
 - 组态, 156
 - 组态地址区, 154
 - 编程, 150
- 安全要求, 8
 - 可达到的, 8
- 安全程序, 61
 - 下载, 262
 - 不一致, 259
 - 比较, 275
 - 打印输出, 281
 - 传送到多个 F-CPU, 57
 - 创建的基本步骤, 79
 - 创建程序的步骤, 79
 - 安全模式注意事项, 307
 - 设置访问许可, 52
 - 测试, 288
 - 结构化, 61
 - 密码, 52
 - 程序结构的规则, 81
 - 编译, 260
- 安全程序 (Safety Program) 对话框, 255
- 安全程序状态, 259
- 安全程序的记录册, 279
- 安全程序的项目数据, 281
- 安全程序的读取访问, 55
- 安全模式, 288
 - 安全程序, 307
 - 取消激活, 288
- 执行用户确认, 121, 123
 - 在 DP 主站的 F-CPU 的安全程序中, 121
 - 在智能 DP 从站的 F-CPU 的安全程序中, 123
- 有 4 个暂时失效传感器的暂时失效过程, 196
- 有效性检查, 129
- 约定, 3
- 自动生成的 F 块, 262
 - 块大小, 262
- 设置 F-CPU 的访问许可, 57
- 访问 F-I/O DB 的变量, 110
- 访问许可, 57
 - 设置, F-CPU 的, 57
 - 设置, 安全程序的, 52
 - 取消, F-CPU 的, 57
 - 取消, 安全程序的, 52

- 访问保护, 49
 - 概述, 49
- 过程映像, 101
- 过程数据或故障安全值, 102
- 过程输入映像, 66
- 过程输出映像, 66, 127

- 七划**
- 两个 F-CPU 之间通过 DP/DP 耦合器的通讯连接, 135
 - 组态, 135
 - 编程, 135
- 位存储器, 66, 127
- 删除, 308
 - S7 Distributed Safety, 253, 308
- 启动 F 系统, 111
- 启动后的行为, 111
- 启动保护, 99
- 启动特性, 204, 212, 222, 225, 229
 - ACK_REI_GLOB, 232
 - F_1oo2DI, 204
 - F_CTD, 183
 - F_CTU, 182
 - F_CTUD, 184
 - F_ESTOP1, 222
 - F_FDBACK, 225
 - F_MUT_P, 212
 - F_RCVDP, 233
 - F_RCVS7, 240
 - F_SENDDP, 233
 - F_SENDS7, 240
 - F_SFDOOR, 229
 - F_TOF, 190
 - F_TON, 188
 - F_TP, 186
- 应用对安全程序的更改, 273

- 时序图, 233
 - F_1oo2DI, 204
 - F_MUT_P, 212
 - F_MUTING, 196
 - F_RCVDP, 233
 - F_SENDDP, 233
 - F_TOF, 190
 - F_TON, 188
 - F_TP, 186
- 更改 F 运行组, 91
- 更新参考数据, 262
- 系统操作安全, 8
 - 维护, 8
- 评估, 310
 - 诊断变量/参数, 310
- 诊断, 310
 - 指南, 310
- 诊断参数, 310
 - 评估, 310
- 诊断变量, 310
 - 评估, 310
- 诊断选项, 310
 - 评估步骤, 310
- 连接, 168
 - ACK_REI_GLOB, 232
 - F_1oo2DI, 204
 - F_2H_EN, 209
 - F_2HAND, 194
 - F_ACK_OP, 192
 - F_BO_W, 248
 - F_CTD, 183
 - F_CTU, 182
 - F_CTUD, 184
 - F_ESTOP1, 222
 - F_FDBACK, 225
 - F_INT_RD, 250

F_INT_WR, 249
 F_MUT_P, 212
 F_MUTING, 196
 F_RCVDP, 233
 F_RCVS7, 240
 F_SCA_I, 181
 F_SENDDP, 233
 F_SENDS7, 240
 F_SFDOOR, 229
 F_SHL_W, 246
 F_SHR_W, 247
 F_TOF, 190
 F_TON, 188
 F_TP, 186
 F_W_BO, 248

连接表, 169

八划

使用 F-FBD/F-LAD 创建 F 块, 82
 使用 F-FBD/F-LAD 创建 F 块:不分配给 F-CPU, 82
 使用 S7-PLCSIM 进行测试, 291
 使用反射挡光板的暂时失效操作步骤, 196
 使用对 F-I/O DB 的访问, 104
 使能输入, 66
 使能输出, 66
 具有完整资格的 DB 访问, 66, 110
 具有使能的双手操作监视, 209
 具有输入的 F-I/O, 102
 具有输出的 F-I/O, 102
 刻度 INT, 181
 单向连接, 135
 参考文档, 3
 取消激活安全模式, 288
 周期时间, 91
 F 运行组, 91

定义 F 运行组, 91
 定义程序结构, 81
 定时器和计数器, 63
 服务与支持, 3
 自动化与驱动, 3
 知识保护, 87
 为用户创建的 F-FB 和 F-FC, 87
 组诊断, 37
 对于 S7-300 F-SM, 37
 组态, 135
 F-CPU 的 F 参数, 28
 F-CPU 的保护级别, 28
 F-I/O, 37
 PROFIsafe 地址设置, 37
 与标准相同, 26, 37
 安全相关的主站与主站通讯, 135
 安全相关的主站与智能从站通讯, 145
 安全相关的主站与智能从站通讯的地址区, 143
 安全相关的智能从站与从站通讯, 162
 安全相关的智能从站与从站通讯的地址区, 160
 安全相关的智能从站与智能从站通讯, 156
 安全相关的智能从站与智能从站通讯的地址区, 154
 两个 F-CPU 之间通过 DP/DP 耦合器的通讯连接, 135
 使用 GSD 文件: , 42
 组诊断, 37
 故障安全 DP 标准从站, 42
 特性, 26
 通过 DP/DP 耦合器的通讯连接, 135
 通过 S7 连接的安全相关的通讯, 169
 符号名, 47
 概述, 25
 组态主站与智能从站通讯, 145
 组态通过 S7 连接进行的通讯, 168
 组态智能从站与从站通讯, 162
 组态智能从站与智能从站通讯, 156

- 组钝化, 119
- 软件组件, 16
 - 更换, 308
- 软件要求, 19
- 九划**
- 保护, 83
 - F-FB/F-FC/F-DB 的知识产权, 87
- 信息图景
 - 定位, 3
- 修改 F-DB 中的值, 291
- 修改安全程序的数据, 291
- 前言, 3
- 将 BOOL 转换为 WORD, 248
- 将 INT 间接写入 F-DB, 249
- 将 WORD 转换为 BOOL, 248
- 将安全程序传送到 F-CPU, 269
 - 使用 PG/PC, 269
 - 具有闪存卡, 269
 - 具有存储卡 (MMC), 269
- 将安全程序传送到多个 F-CPU, 57
- 带有误差分析的 1oo2 评估, 204
- 急停 (最高可达停止类别 1), 222
- 指南, 3
- 故障安全 DP 标准从站
 - 组态, 42
- 故障安全自动化系统的生命周期, 313
- 故障安全块, 63
- 故障安全标准 I/O 设备
 - 组态, 42
- 故障安全值或过程数据, 102
- 故障安全确认, 192
- 故障安全输出
 - 较长时期的钝化, 308
- 故障响应功能, 8
 - 实例, 8
- 标准用户程序和安全程序之间的通讯, 127, 129
- 测试安全程序, 291
- 测试规则, 291
- 测试选项, 288
- 背景数据块, 66, 310
 - 访问, 66
 - 评估诊断变量/参数, 310
- 选项卡, 26
- 重新启动保护, 99
- 重复使用已创建的 F 块, 82
- 重新启动抑制, 212
 - 光幕中断期间, 196
- 重新集成, 115
- 重新集成 F-I/O, 121, 123
 - 发生 F-I/O 故障和通道故障后, 115
 - 发生通讯错误后, 113
 - 启动 F 系统后, 111
 - 组钝化, 119
 - 编写用户确认程序, 121, 123
- 钝化和重新集成 F-I/O 的信号图表
 - 发生 F-I/O 故障和通道故障后, 115
 - 发生通讯错误后, 113
 - 启动 F 系统后, 111
 - 组钝化, 119
- 十划**
- 核对清单, 313
- 监视/修改变量功能, 291
- 通用模块, 135
- 通讯
 - 通过 F_SENDS7 和 F_RCVS7, 168
- 通讯错误, 113
 - F_SENDDP/F_RCVDP, 233

通过 DP/DP 耦合器的通讯连接, 135

组态, 135

编程, 135

通过 S7 连接发送和接收数据, 240

通过 S7 连接进行安全相关的通讯: 数据传输的限制, 175

通过 S7 连接进行通讯, 168, 169

组态, 169

通过 S7 连接的安全相关的通讯, 169

组态, 169

编程, 173

通过程序标识进行保护, 269

预防性维护 (检测测试), 308

预制的 F 功能, 63

十一划

减计数, 183

培训中心, 3

基本知识, 3

需要的, 3

密码

F-CPU, 57

为安全程序分配新密码, 52

分配, 49

安全程序, 52

有效性, 49

更改安全程序的现有密码, 52

提示, 49

接线测试, 291

检查块的一致性, 89

检测测试, 308

符号名, 110

F-I/O DB, 47

分配, 47

十二划

智能从站与从站通讯, 160

组态, 162

智能从站与从站通讯的地址区

分配, 160

定义, 160

智能从站与智能从站通讯, 148

组态, 156

智能从站与智能从站通讯的地址区

分配, 154

定义, 154

硬件组件, 16

硬件配置, 26

保存并编译, 26

硬件模拟, 262

确认, 121, 123

程序标识, 269

程序结构的规则, 81

编号区

F 功能块, 28, 41

F 数据块, 28

编译安全程序, 260

编程, 171

F 通讯 DB, 171

安全相关的 CPU 与 CPU 通讯, 131

安全相关的主站与主站通讯, 139

安全相关的主站与智能从站通讯, 150

安全相关的智能从站与智能从站通讯, 150

有效性检查, 129

组钝化, 119

通过 S7 连接的安全相关的 CPU 与 CPU 通讯, 173

概述, 59

编程: 启动保护, 99

编辑

F-FB/F-FC, 83

十三划

数据传输

从安全程序到标准用户程序, 127

从标准用户程序到安全程序, 129

数据传输: 安全相关的主站与主站通讯的限制, 142

数据传输: 通过 S7 连接进行的安全相关的通讯的限制, 175

数据传输的限制: 安全相关的主站与主站通讯, 142

数据传输的限制: 通过 S7 连接进行安全相关的通讯, 175

数据块, 28

访问, 66

数据类型和参数类型, 66

数据结构

保护, 42

输入, 更改, 或取消安全程序的密码, 52

十四划

模拟, 262

硬件, 262

模拟设备, 307

使用, 307

十五划

增计数, 182

增计数和减计数, 184

十六划

操作系统更新, 308