1．故障安全系统概述

1.1 什么是故障安全自动化系统

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

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

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

所谓故障安全自动化系统必须满足下面特征：当我们用一组自动化装置构造一个自动化系统，此系统可以实现一组故障安全保护功能。当其中一个或多个自动化装置发生故障的时候，此系统仍然能够保持安全功能不丢失。

1.2 西门子安全集成的概念

安全集成是西门子用于自动化和驱动的集成安全概念。

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

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

将安全工程集成至标准自动化标准的优点:

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

1.3 SIMATIC S7 中的故障安全系统

1.3.1 SIMATIC S7 自动化系统提供两种故障安全系统:

- S7 分布式故障安全控制系统

用于实现人身和设备的保护（例如机械设备和生产装置的急停保护）和过程控制工业（例如测量和保护设备，加热炉的保护功能）

- 故障安全和容错 S7 F/FH系统

容错的S7 F/FH系统适用于过程控制工业和石油工业的自动化工厂。为了增加自动化系统的可用性，防止由于F系统的错误导致的过程失败，S7 F系统可以选配冗余部分(S7 FH 系统)。 通过部件冗余（例如电源部分、处理器部分、通讯部分和输入输出部分）增加系统可用性。

1.3.2 可实现的安全要求

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

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

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

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

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

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

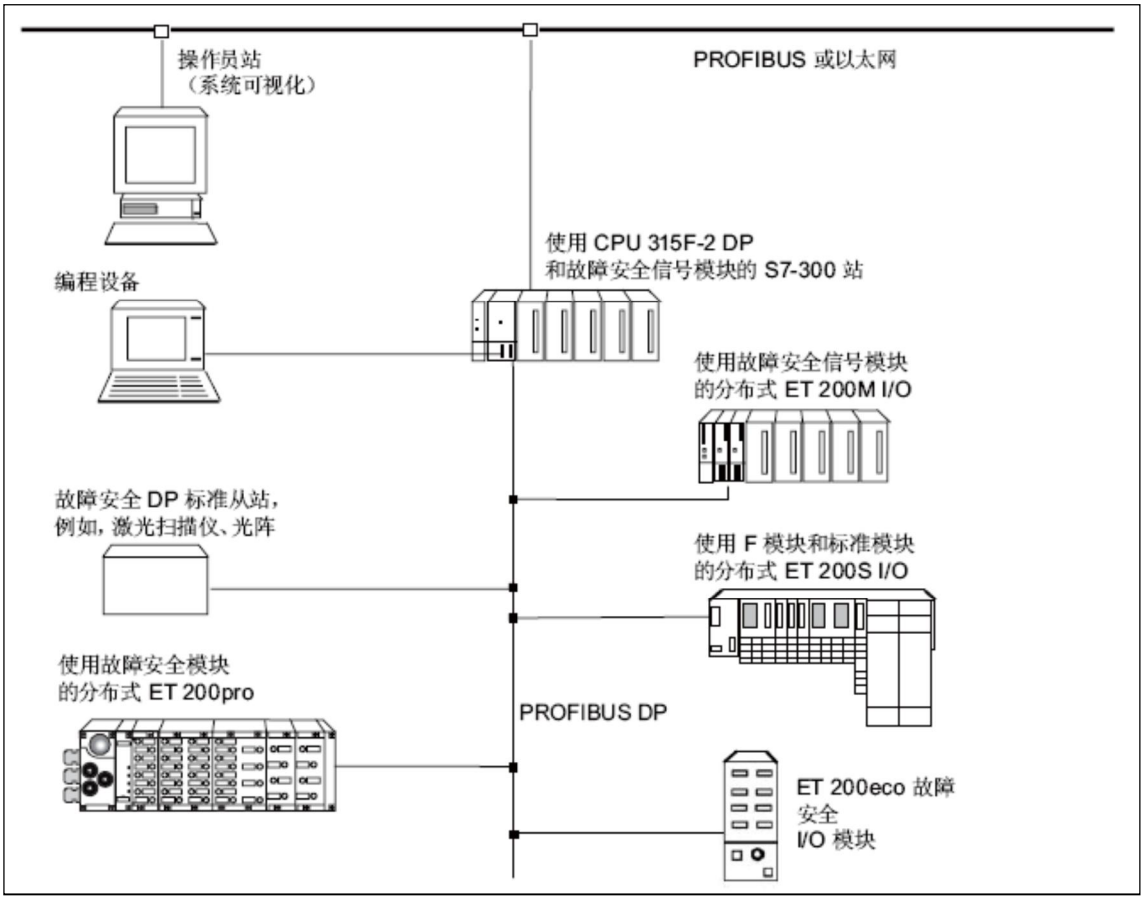
可以通过用户安全功能或故障响应功能提供该过程的安全功能。出现故障时，如果 F 系统无法再执行其实际用户安全功能，则将执行故障响应功能，例如，取消激活关联输出，以及在必要时将 F-CPU 切换至 STOP 模式。

注意：

- **本文档只针对S7 Distributed Safety系统配置和使用进行描述，不涉及S7 F/FH系统的内容。如需了解，请查阅《可编程控制器 S7 F/FH》手册。**
- **本文档不涉及相关故障安全标准的具体内容，如需了解，请查询相关标准。**

2. S7 Distributed Safety 组件

2.1 硬件组件



S7 分布式故障安全系统包含满足特殊安全要求的部分硬件组件：

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

2.2 软件组件

S7 分布式故障安全系统的软件组件包括以下内容：

- STEP7　对SIMATIC可编程控制器进行组态和编程的标准软件包
- S7 Distributed Safety　对分布式故障安全系统进行组态和编程的选件包

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

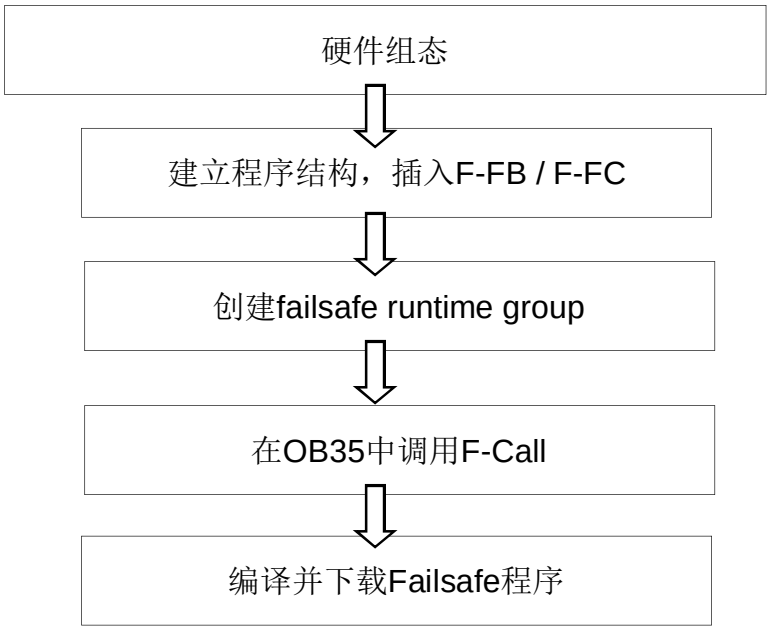
使用这些选件包，用户将获得：

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

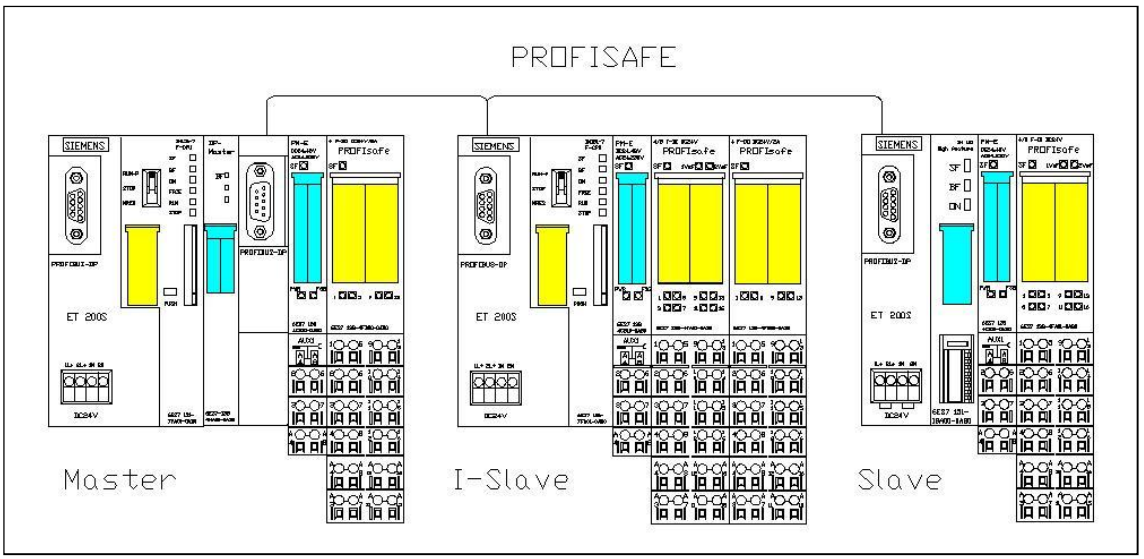
3．分布式故障安全系统的组态和编程

3.1 综述

故障安全系统的组态和编程和普通的 PLC 系统有所不同，不管是硬件组态，还是程序结构，或者是编译下载，都有它的特点。总体来说，如果开始编写一个故障安全系统的新项目，可以按照下面的图示，分五个步骤进行。



3.1.1 本例程使用的设备结构图



3.1.2 软硬件列表

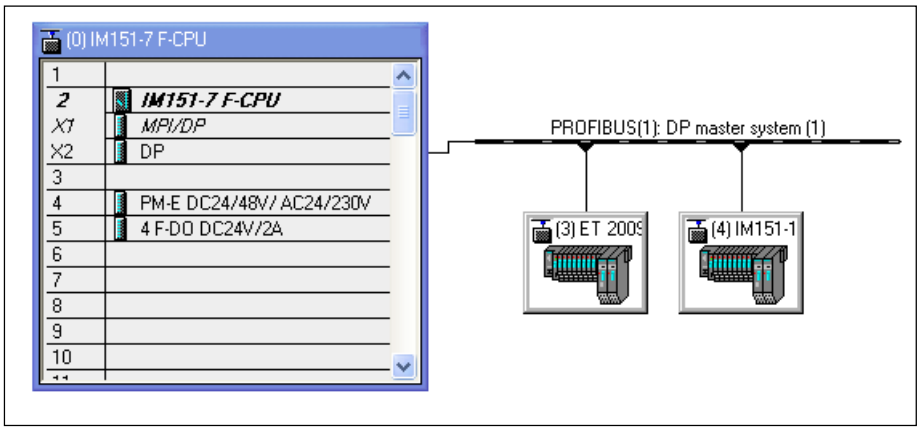
模块名称	模块型号	订货号	数量
Master Station			
CPU	IM151-7F	6ES7151-7FA01-0AB0	1

存储卡	MMC 128K	6ES7953-8LG11-0AB0	1
DP 主站模块	DP-Master	6ES7138-4HA00-0AB0	1
ET200S 电源模板	PM-E	6ES7138-4CB11-0AB0	1
F 输出模板	4 F-DO	6ES7138-4FB02-0AB0	1
ET200S 终端模块	TM-P15S23-A0	6ES7193-4CD20-0AB0	1
ET200S 终端模块	TM-E30S46-A1	6ES7193-4CF40-0AA0	1
I-Slave Station			
CPU	IM151-7F	6ES7151-7FA01-0AB0	1
存储卡	MMC 128K	6ES7953-8LG11-0AB0	1
ET200S 电源模板	PM-E	6ES7138-4CB11-0AB0	1
F 输入模板	4/8 F-DI	6ES7138-4FA02-0AB0	1
F 输出模板	4 F-DO	6ES7138-4FB02-0AB0	1
ET200S 终端模块	TM-P15S23-A0	6ES7193-4CD20-0AB0	1
ET200S 终端模块	TM-E30S46-A1	6ES7193-4CF40-0AA0	2
Slave Station			
ET200S 接口模板	IM151 HF	6ES7151-1BA02-0AB0	1
ET200S 电源模板	PM-E	6ES7138-4CB11-0AB0	1
F 输入模板	4/8 F-DI	6ES7138-4FA00-0AB0	1
ET200S 终端模块	TM-P15S23-A0	6ES7193-4CD20-0AB0	1
ET200S 终端模块	TM-E30S46-A1	6ES7193-4CF40-0AA0	1
软件名称	版本号	订货号	数量
STEP7	2006 Prof. Version	6ES7810-5CC10-0YA5	1
S7-Distributed Safety	V5.4+SP3	6ES7833-1FC02-0YA5	1

3.2 硬件组态步骤

3.2.1 组态硬件

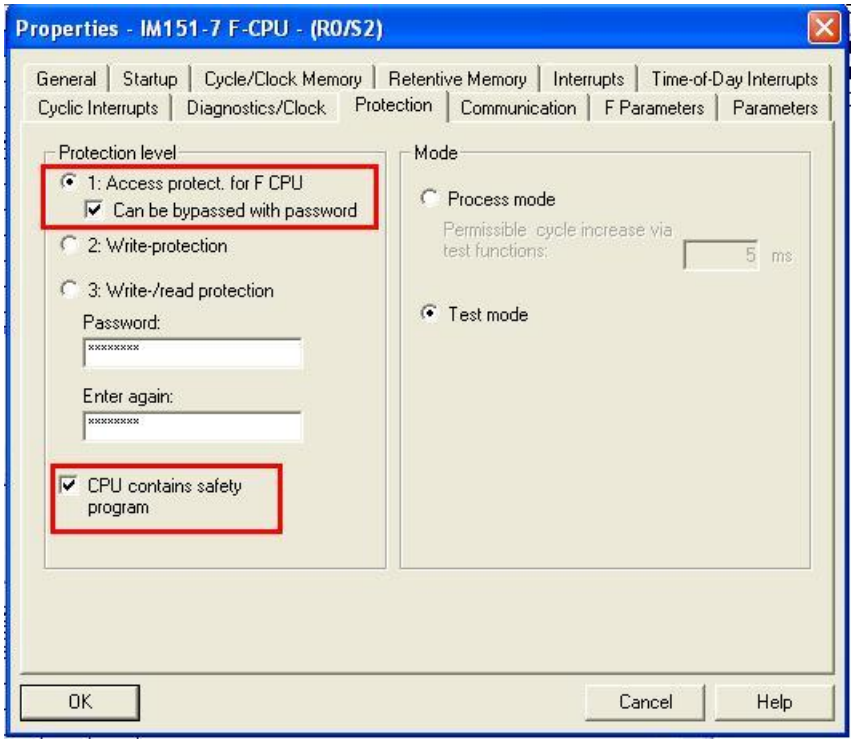
这个环节与普通 PLC 系统组态方法基本一致，根据实际的硬件配置，对 F-CPU，ET200S 的电源模板、F-DI/DO，逐一进行组态。



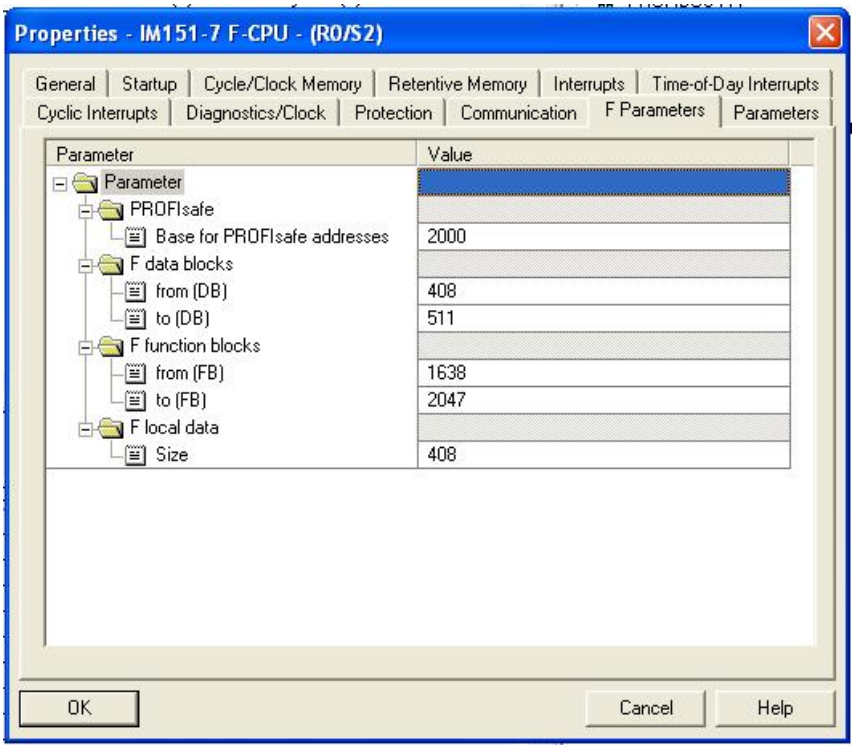
3.2.2 组态 F-CPU

相对于普通 CPU，F-CPU 还需要如下两步配置：

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

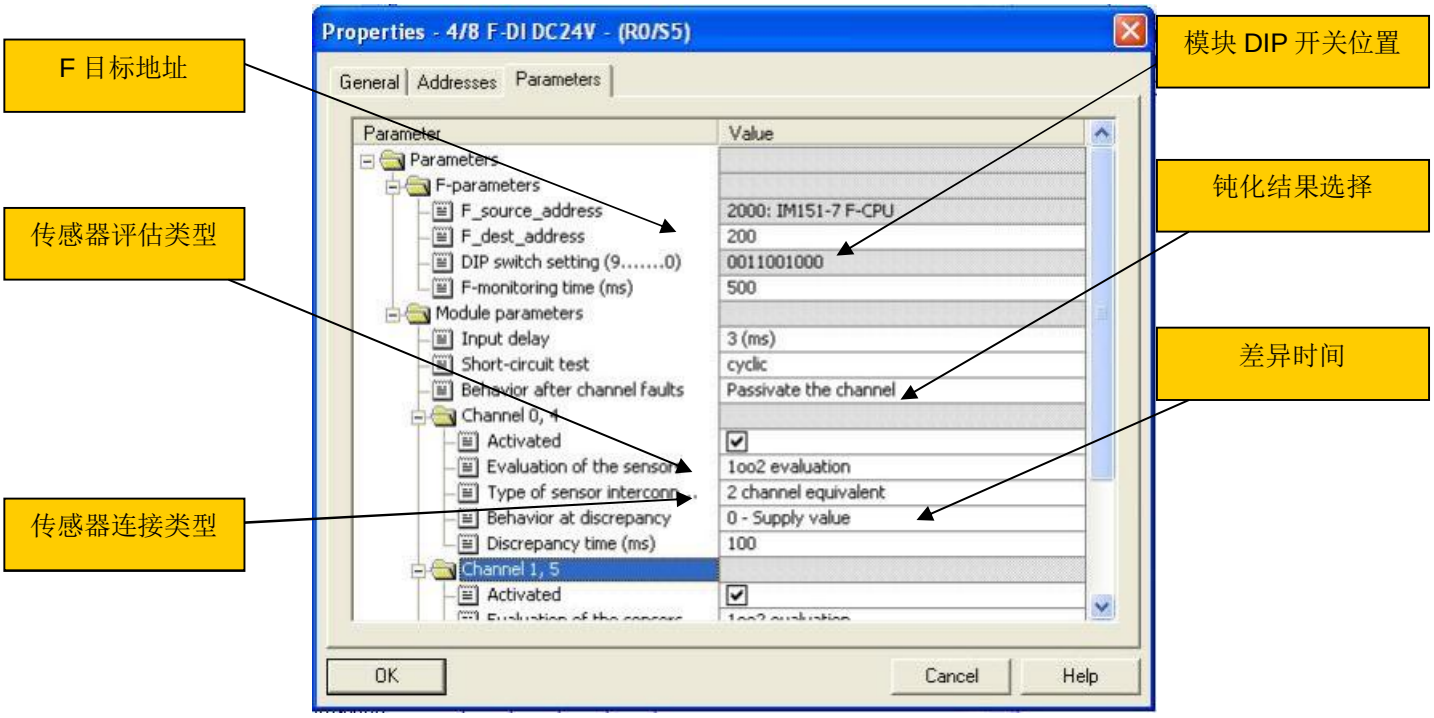


2）配置 F 参数，这些参数都是安全程序编辑所要用到的保留区域，通常不用修改。值得注意的是，当点击F Parameters标签页后，会出现一个密码输入对话框，此时需要设定一个安全程序密码（不是上边提及的F-CPU密码），安全程序密码防止对F-CPU和F-I/O设置的组态和参数进行未授权的更改。



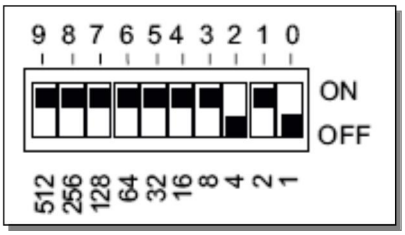
3.2.3 组态 F-IO

对 ET200S 4/8 F-DI （6ES7138-4FA02-0AB0）组态实例；ET200S 4-FO 参数配置与之相似，不再说明。



1）F 目标地址：每个安全模板都会有唯一的F 目标地址，该地址由系统自动分配并保证其唯一性，通常不用修改。

2）模块 DIP 开关位置：通常位于安全模板的侧面和背面，位置设定对应该模板 F 目标地址（该模板 F 目标地址的二进制编码）。



3）钝化结果选择：当通道出现错误后，选择是出错的通道钝化或者整个模板钝化。从S7 Distributed Safety V5.4开始支持该功能，并且需要相应信号的模板支持。

钝化的含义：如果 F-I/O 检测到故障，则将受影响的通道或所有通道切换至安全状态，即该 F-I/O的通道被钝化。F-I/O 通过从站诊断将检测到的故障报告给CPU。对于具有输入的 F-I/O，如果发生钝化，则 F 系统为安全程序提供的是故障安全值，而不是故障安全输入处未决的过程数据。对于具有输出的 I/O，如果发生钝化，则 F 系统将故障安全值（0）传送给故障安全输出，而不是安全程序提供的输出值。

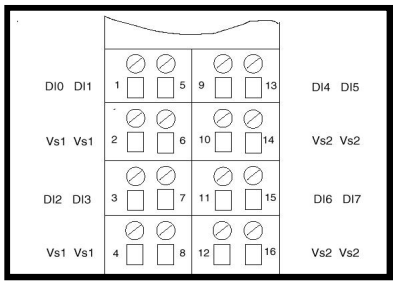
4）传感器评估类型：

1oo1评估：通过一个通道将一个非冗余传感器连接至F模板。

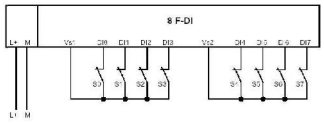
1oo2评估：两个输入通道由一个双通道传感器或两个单通道传感器占用。在内部比较输入信号是对等还是非对等。

5）传感器连接类型：

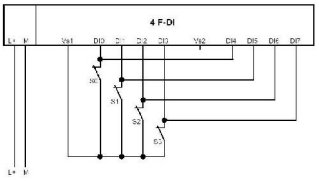
- Failsafe 的输入方式



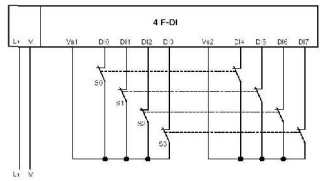
单通道传感器
1 oo 1 evaluation
Short circuit test
AK4/SIL2/Kat.3



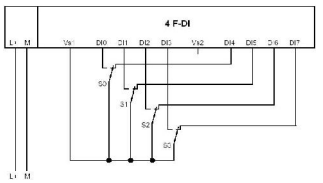
单通道传感器
1 oo 2 evaluation
Short circuit test
AK6/SIL3/Kat.4



双通道传感器或
两个单通道传感器
1 oo 2 evaluation Short circuit test
AK6/SIL3/Kat.4

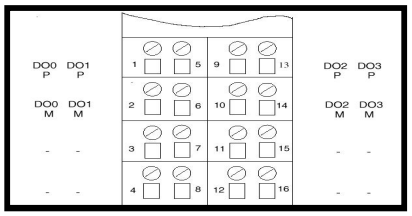


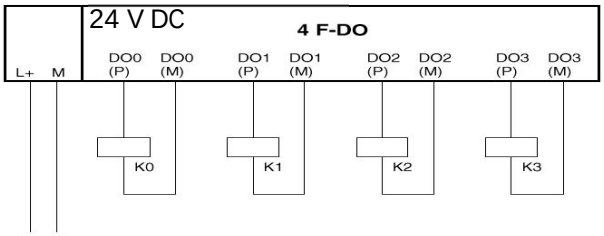
Antivalent传感器
1 oo 2 evaluation
Short circuit test
AK6/SIL3/Kat.4



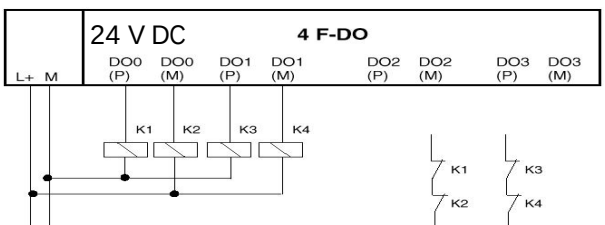
- Failsafe 的输出方式

Failsafe执行器





继电器



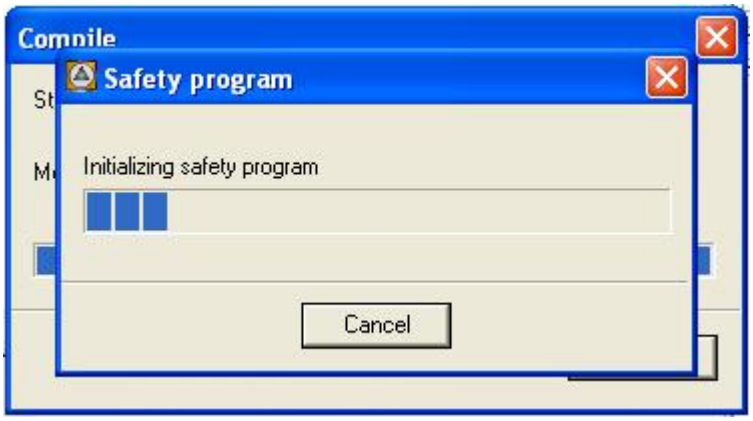
5）差异时间：对于 1oo2 传感器信号评估，在设置的差异时间内，如果 2 个信号不一样，按照设定的替代值输入；如果差异时间已到，2 个信号还不一样，输入值变为 0。

依次完成其他模板的组态。

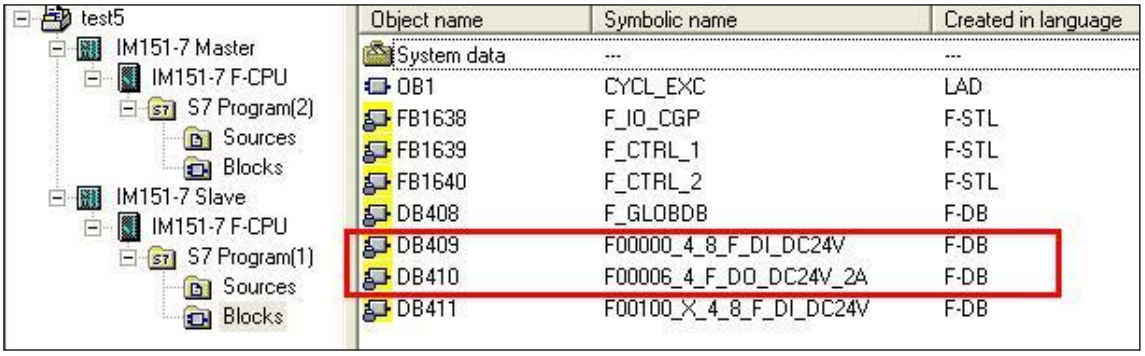
3.2.4 保存编译

完成正确的硬件配置，保存编译通过后，系统会自动生成与硬件相关的安全程序。

硬件配置编译界面：



编译完成后，SIMATIC Manager 显示界面：



从上图可以看到，系统自动生成与安全有关的块都是黄色图标并且处于加密状态。其中需要注意的是，每个安全模板都会对应生成一个安全数据块 F-I/O DB（红色框内）。F-I/O DB 作用很大，判断模板是否钝化以及模板故障排除后需要完成去钝，都需要通过访问 F-I/O DB 来完成。

3.3 程序结构

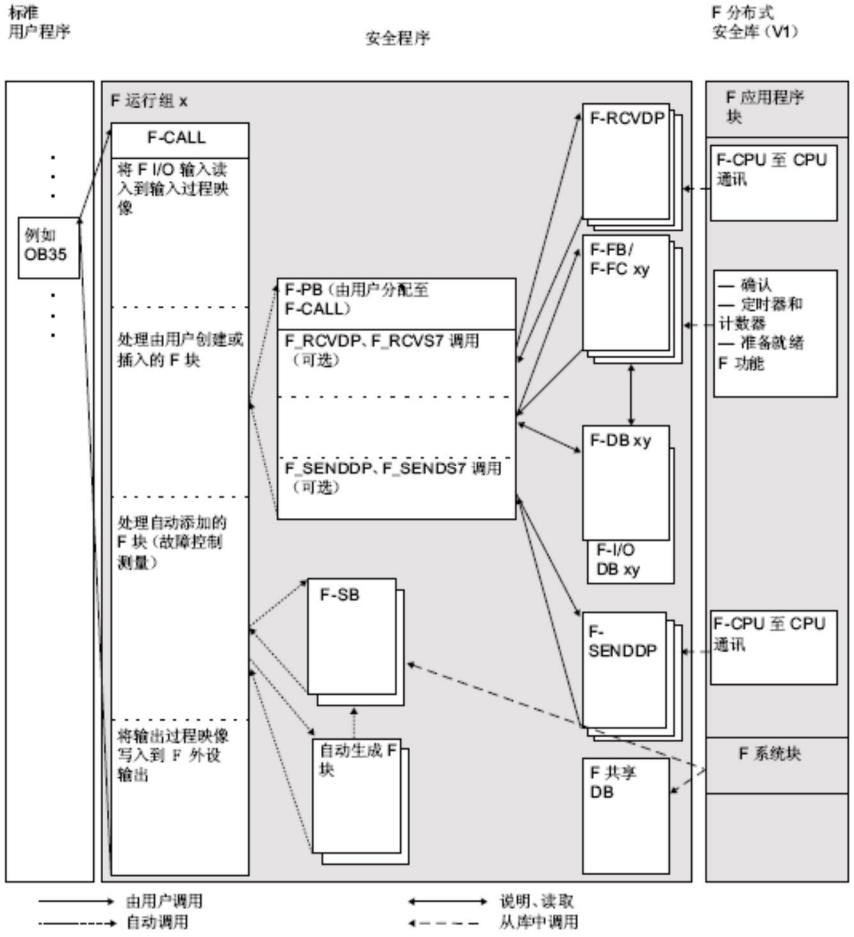
在开始编写安全程序前，先了解S7 Distributed Safety安全程序的结构。

为了结构化，一个安全程序由一个或两个 F 运行组组成。安全程序包括以下组件：

- 由用户创建或从 F 库（例如 Distributed Safety F 库 [V1]）中选择的 F 块。

- 自动添加的 F 块（F-SB、自动生成的 F 块和 F 共享 DB）

下图显示了 S7 Distributed Safety 安全程序的示意图结构。



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

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

3.4 程序实例

现在通过一个程序实例来了解安全程序的配置过程。硬件配置见 3.1。

硬件接线：

主站 4 F-DO 模块：DO0 接指示灯 L4；DO1 接指示灯 L5。

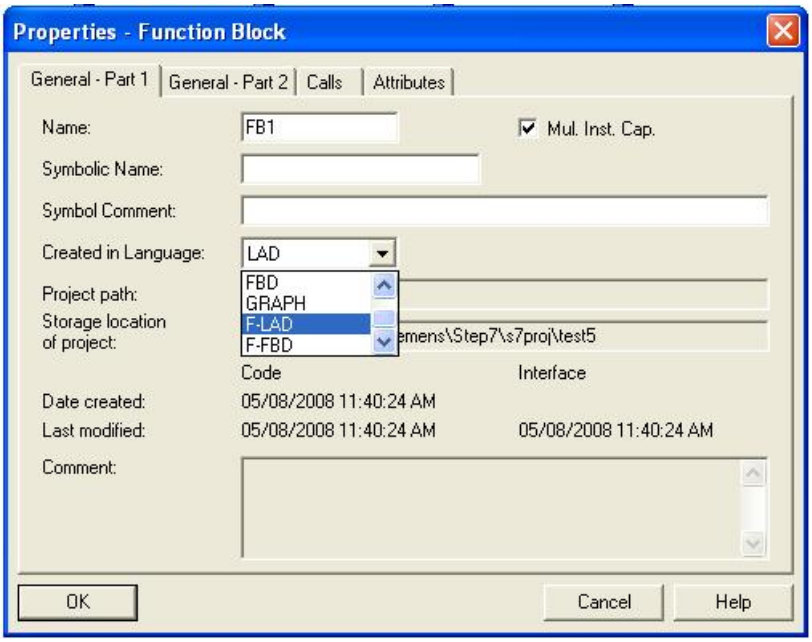
从站 4/8 F-DI 模块：DI2/6 接 1oo2 non-equivalent 开关 S8；DI3/7 接 1oo2 non-equivalent 开关 S9。

实现功能：停止类别 1 安全停车功能

S9 作为急停开关，S8 作为确认开关。当没有急停信号时，指示灯 L4、L5 点亮。当急停信号到来或急停信号故障，指示灯 L4 立即熄灭；L5 延时设定时间熄灭。当急停信号离去或故障恢复，应答请求 ACK_REQ 变为 1，再经过 S8 确认后，指示灯 L4、L5 才会重新点亮。

3.4.1 配置 F-FB

1）先插入 F-FB，选择 Failsafe 程序特定的语言：F-FBD 或 F-LAD。这里选择 F-LAD.

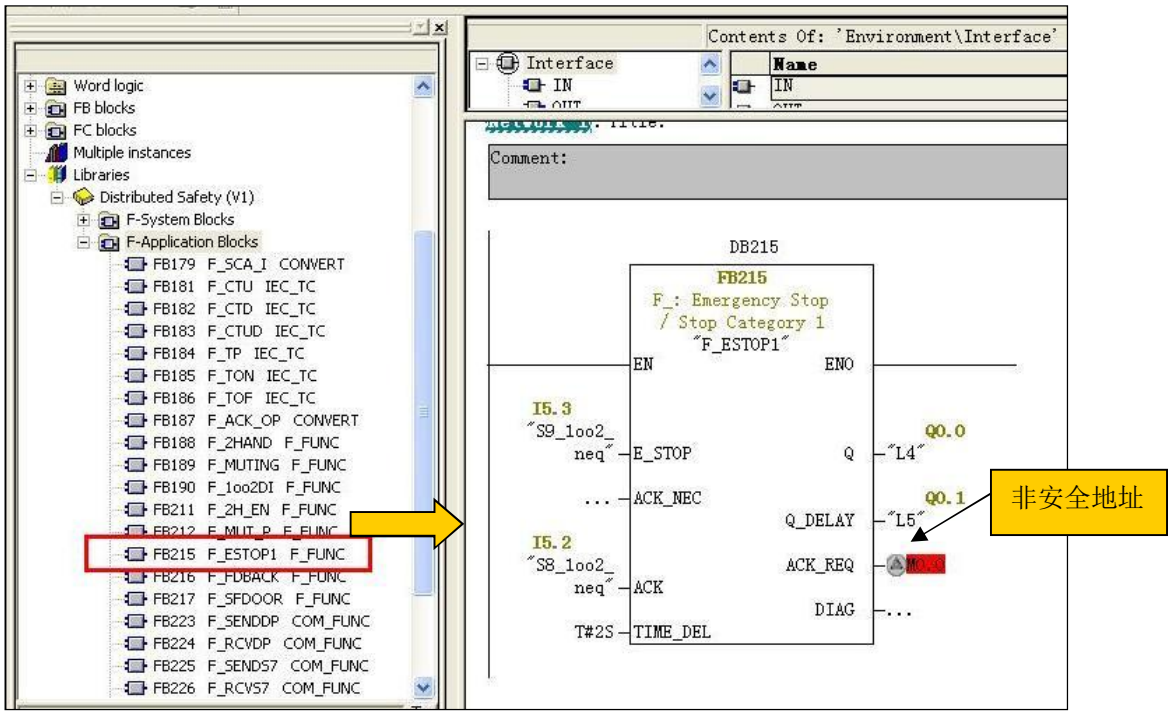


2）创建完后，在 FB1 中编程。从 F-Application 库中调用 FB215，实现停车类别 1 安全停车功能控制。需要注意的是，从图中可以看到，来自安全模板通道 I5.2、I5.3、Q0.0、Q0.1 都是安全地址，而非安全地址 M0.0 以红色标示。

注：在安全程序中可以处理来自标准用户程序的数据，但是由于这些数据不安全，用户必须在安全程序中执行其它针对过程的似然性检查，以确保不会发生危险状况。

在该程序中，ACK_REQ 只是作为急停信号离去后，可以触发应答的一个标志位，并不是作为参与急停的控制位，所以可以使用非安全地址。

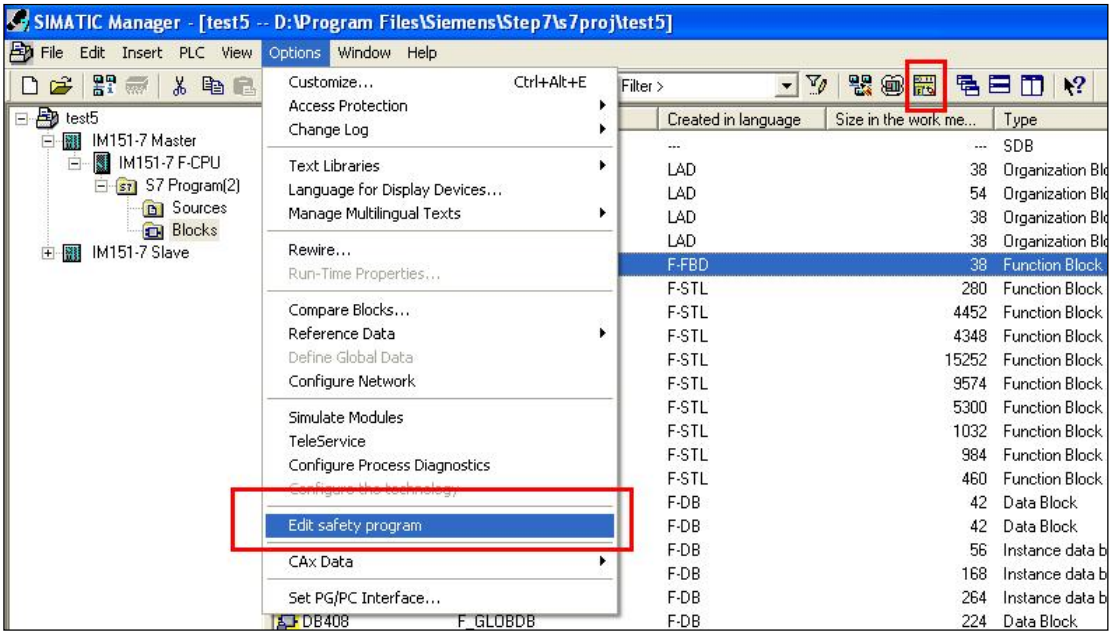
F-FB 编辑完成后，保存关闭。



3.4.2 创建 Failsafe Runtime Group

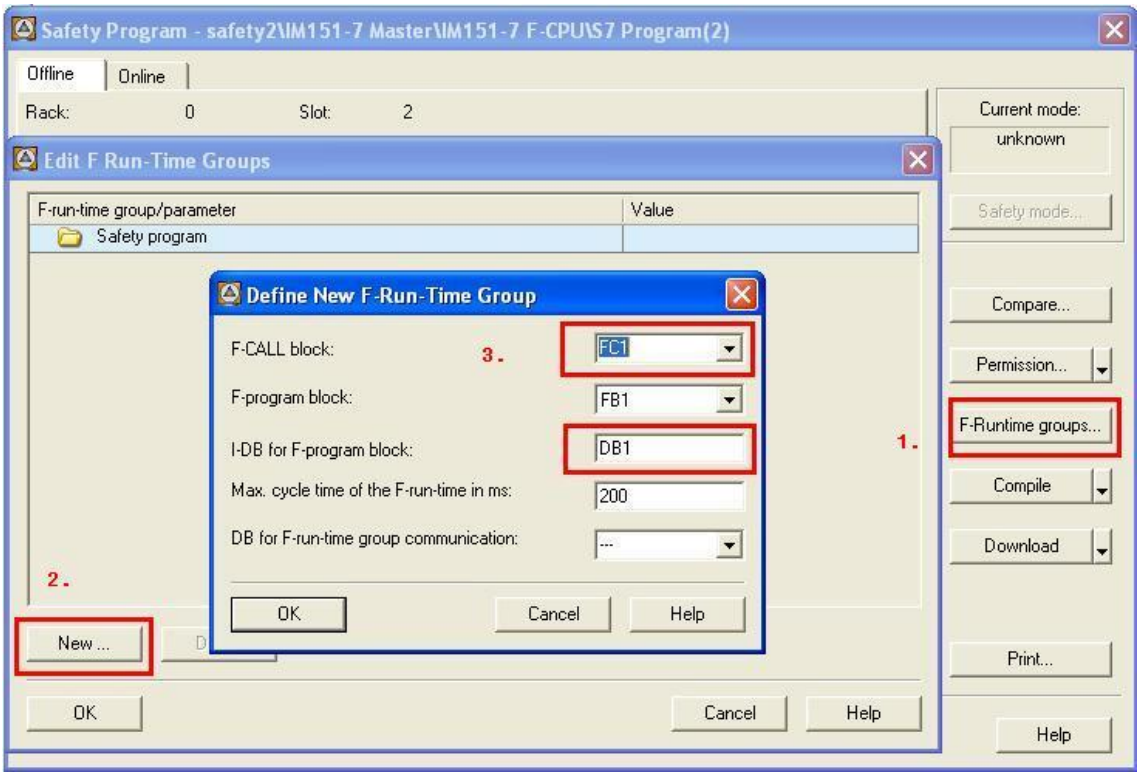
1）进入安全程序编译界面

在 SIMATIC Manager 主界面下，点击菜单 Options>Edit Safety Program，或者直接点击工具栏中图标，启动安全程序编译界面。



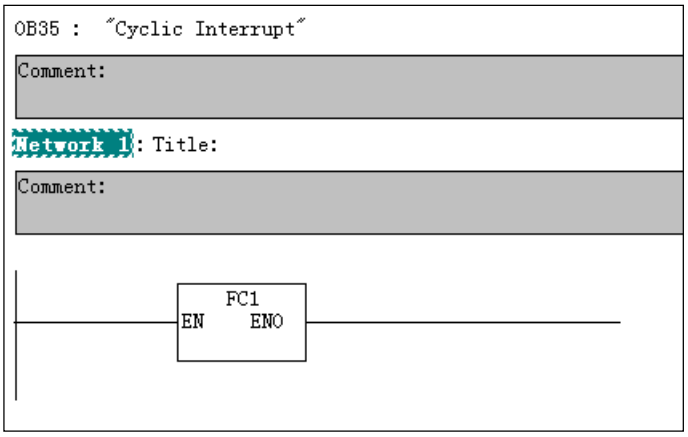
2）创建 Failsafe Runtime Group

上一步创建完的 FB1 不能直接在标准用户程序中被调用，需要创建一个对应的 F-CALL 调用块和 I-DB。如下图：FC1、DB1。点击“ OK ”后，它们会有系统自动生成并且处于加密状态，不能由用户进行编辑。



3.4.3 在 OB35 中调用 F-CALL

直接调用刚才生成的 F-CALL：FC1。

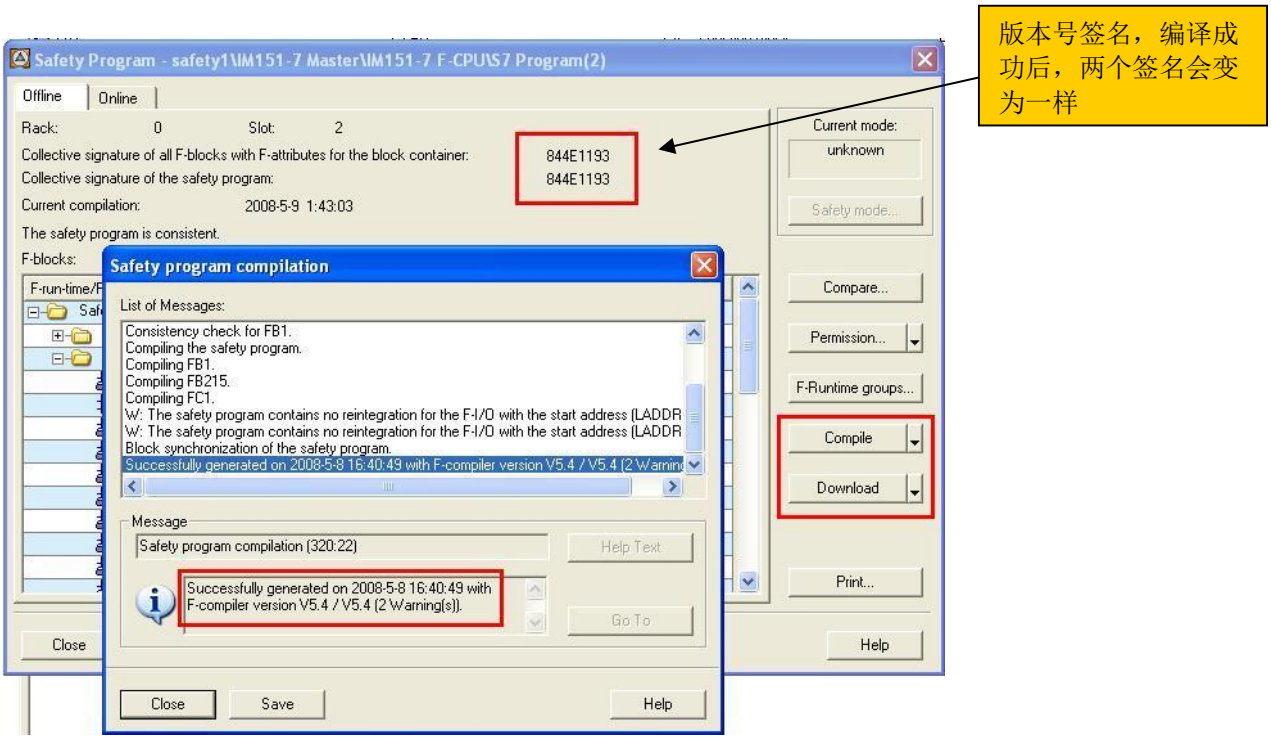


3.4.4 编译下载 Failsafe 程序

点击 Safety 编译窗体中的 Compile，编译 Failsafe 程序；然后点击 Download 下载，这里需要注意：

- 硬件组态应该首先下载；

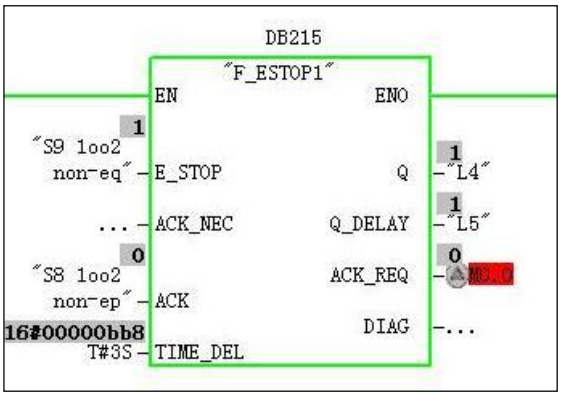
- 如果修改了硬件组态中 CPU、F-I/O 模块的有关参数，或者修改了 Failsafe 程序中的 F 块，就应重新编译并下载 Safety 程序；
- 普通用户程序可以及时修改、编写，对 Failsafe 程序的版本号 signature 没有影响。



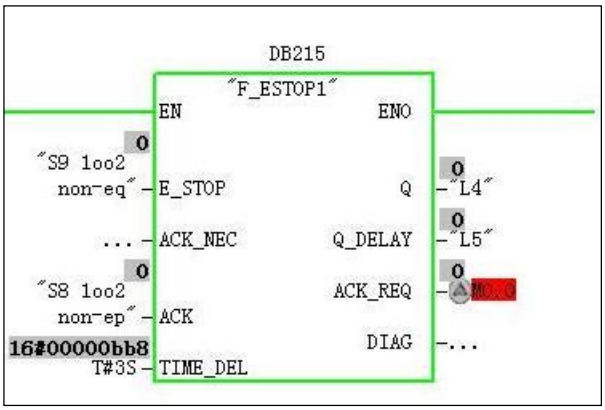
3.5 程序测试

3.5.1 F_ESTOP1 运行结果

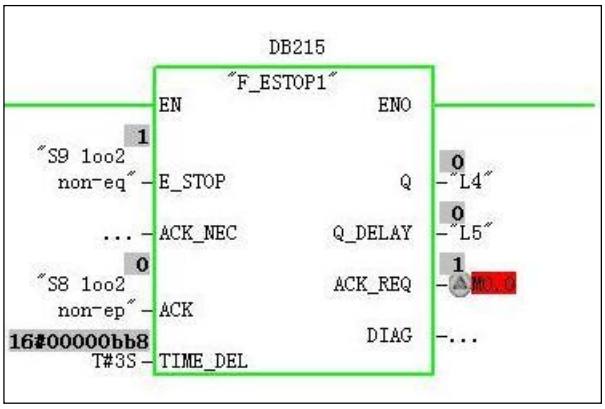
1）没有外部急停信号，Q、Q_DELAY 输出 1 状态；



2）急停信号到来，输入信号 E_STOP 变为 0，Q 输出为 0、Q_DELAY 延时 3 秒输出变为 0；



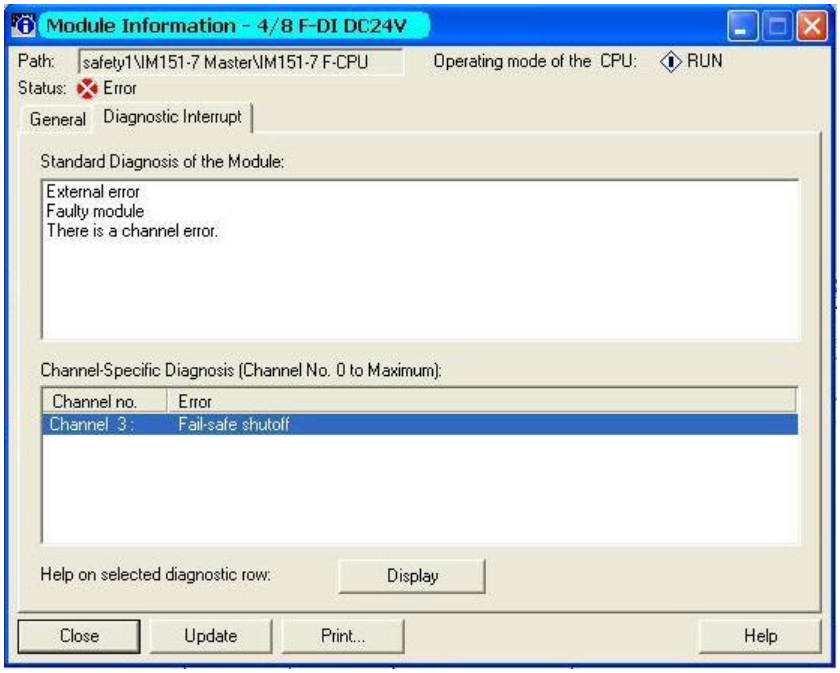
3）急停信号离去，E_STOP 恢复为 1，ACK_REQ 变为 1，请求应答信号变为 1，等待 ACK 应答信号。当 ACK 置为 1 应答后，Q、Q_DELAY 才会恢复为 1。



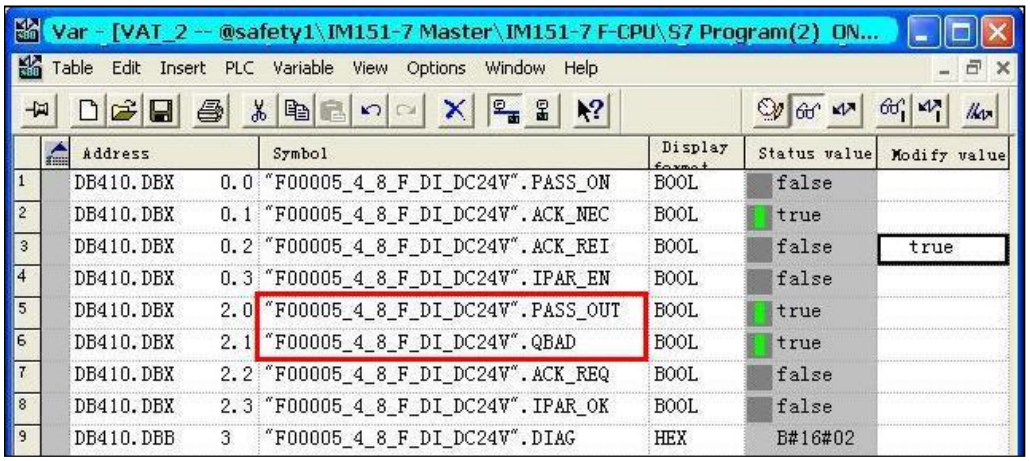
3.5.2 急停信号的钝化与去钝

前边硬件配置提到，S9 是 1oo2 non-equivalent 型号评估 连接到从站 4/8 F-DI 模板 DI 3/7 通道。现在人为将 DI3 的接线端掉，安全模板会自动检测到外部信号错误，并使模板钝化，此时安全模板 SF 指示灯会变亮，S9 的状态会变为 0（保持安全值输入）。安全值 0 通过安全程序会控制执行机构停止工作，如 3.5.1 的描述。

1）通过直接读取安全模板的诊断信息，可以知道错误信息。

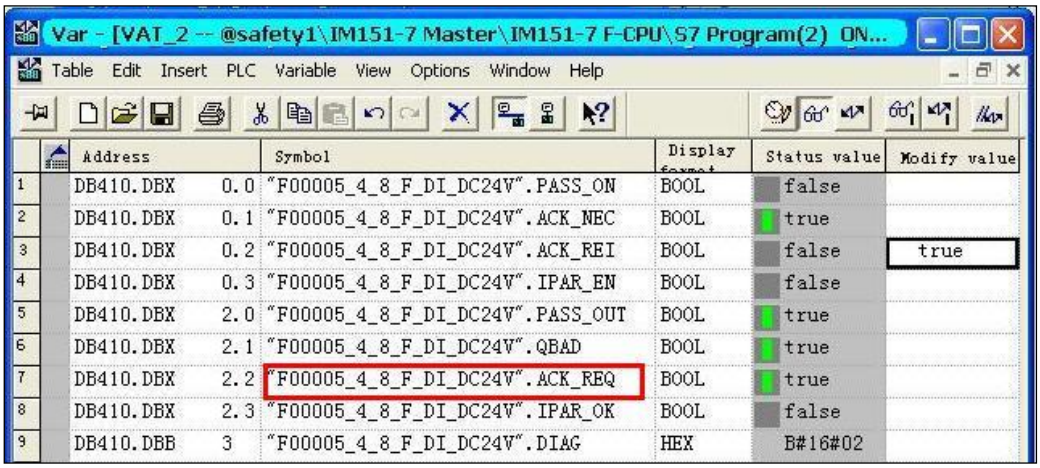


2）在程序中，可以通过访问该安全信号模块的 F-I/O DB 来读取模板的工作状态。本例中该 F-I/O DB 为 DB410。通过 PASS_OUT、QBAD 位的状态，可以知道模板已经钝化（6ES7138-4FA00-0AB0 不支持通道钝化）。



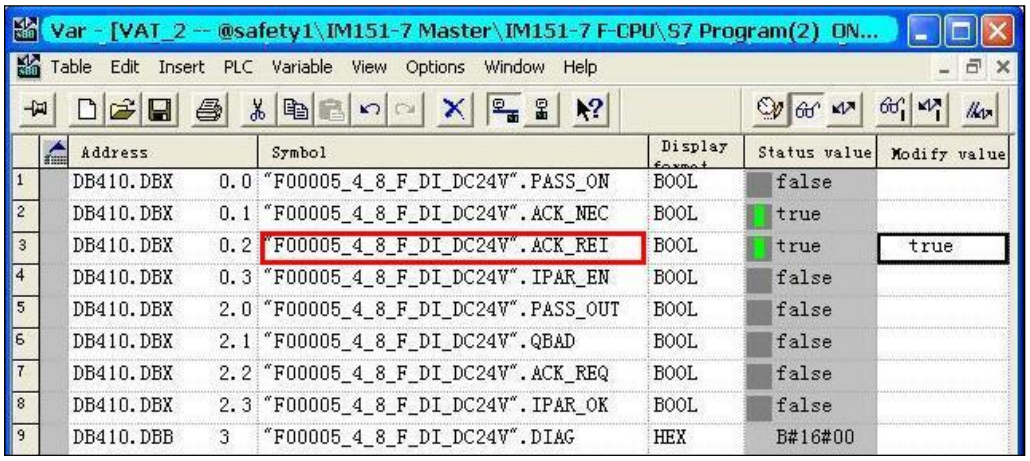
	Address	Symbol	Display format	Status value	Modify value
1	DB410.DBX 0.0	"F00005_4_8_F_DI_DC24V".PASS_ON	BOOL	false	
2	DB410.DBX 0.1	"F00005_4_8_F_DI_DC24V".ACK_NEC	BOOL	true	
3	DB410.DBX 0.2	"F00005_4_8_F_DI_DC24V".ACK_REI	BOOL	false	true
4	DB410.DBX 0.3	"F00005_4_8_F_DI_DC24V".IPAR_EN	BOOL	false	
5	DB410.DBX 2.0	"F00005_4_8_F_DI_DC24V".PASS_OUT	BOOL	true	
6	DB410.DBX 2.1	"F00005_4_8_F_DI_DC24V".QBAD	BOOL	true	
7	DB410.DBX 2.2	"F00005_4_8_F_DI_DC24V".ACK_REQ	BOOL	false	
8	DB410.DBX 2.3	"F00005_4_8_F_DI_DC24V".IPAR_OK	BOOL	false	
9	DB410.DBB 3	"F00005_4_8_F_DI_DC24V".DIAG	HEX	B#16#02	

3）现在恢复 S9 DI3 输入的接线，请求应答信号 ACK_REQ 会变为 1。



	Address	Symbol	Display format	Status value	Modify value
1	DB410.DBX 0.0	"F00005_4_8_F_DI_DC24V".PASS_ON	BOOL	false	
2	DB410.DBX 0.1	"F00005_4_8_F_DI_DC24V".ACK_NEC	BOOL	true	
3	DB410.DBX 0.2	"F00005_4_8_F_DI_DC24V".ACK_REI	BOOL	false	true
4	DB410.DBX 0.3	"F00005_4_8_F_DI_DC24V".IPAR_EN	BOOL	false	
5	DB410.DBX 2.0	"F00005_4_8_F_DI_DC24V".PASS_OUT	BOOL	true	
6	DB410.DBX 2.1	"F00005_4_8_F_DI_DC24V".QBAD	BOOL	true	
7	DB410.DBX 2.2	"F00005_4_8_F_DI_DC24V".ACK_REQ	BOOL	true	
8	DB410.DBX 2.3	"F00005_4_8_F_DI_DC24V".IPAR_OK	BOOL	false	
9	DB410.DBB 3	"F00005_4_8_F_DI_DC24V".DIAG	HEX	B#16#02	

4）置位 ACK_REI，给出应答信号，完成去钝。只有到去钝完成后，在安全程序中才能读到 S9 的外部输入值。



	Address	Symbol	Display format	Status value	Modify value
1	DB410.DBX 0.0	"F00005_4_8_F_DI_DC24V".PASS_ON	BOOL	false	
2	DB410.DBX 0.1	"F00005_4_8_F_DI_DC24V".ACK_NEC	BOOL	true	
3	DB410.DBX 0.2	"F00005_4_8_F_DI_DC24V".ACK_REI	BOOL	true	true
4	DB410.DBX 0.3	"F00005_4_8_F_DI_DC24V".IPAR_EN	BOOL	false	
5	DB410.DBX 2.0	"F00005_4_8_F_DI_DC24V".PASS_OUT	BOOL	false	
6	DB410.DBX 2.1	"F00005_4_8_F_DI_DC24V".QBAD	BOOL	false	
7	DB410.DBX 2.2	"F00005_4_8_F_DI_DC24V".ACK_REQ	BOOL	false	
8	DB410.DBX 2.3	"F00005_4_8_F_DI_DC24V".IPAR_OK	BOOL	false	
9	DB410.DBB 3	"F00005_4_8_F_DI_DC24V".DIAG	HEX	B#16#00	

4. 分布式故障安全系统通信

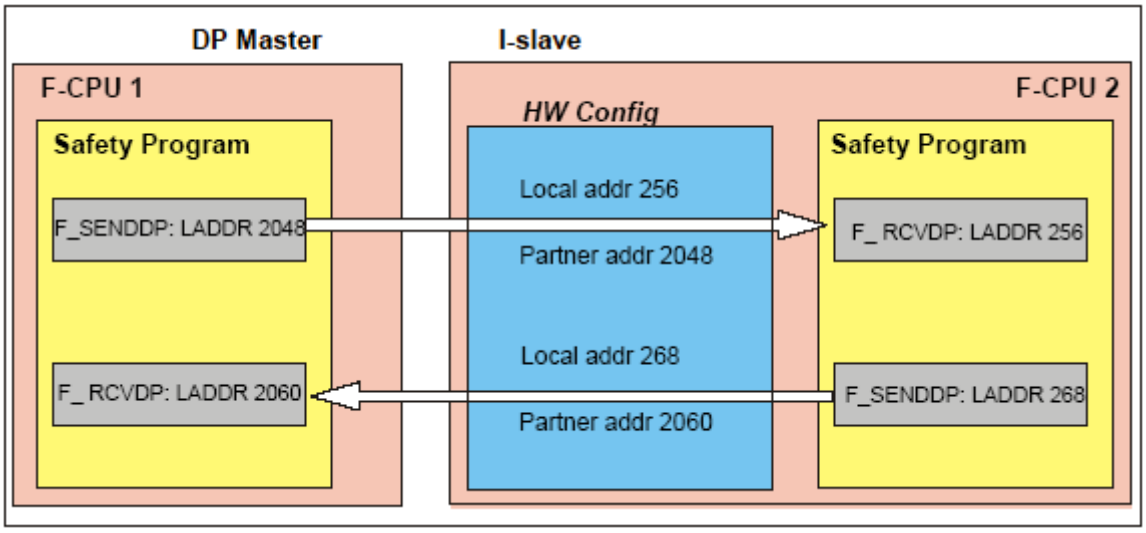
4.1 综述

- 分布式故障安全系统之间可以进行安全相关的通信。有如下几种通讯方式：

- 安全相关主站-主站通信(通过 DP/DP coupler);
- 安全相关主站-智能从站通信(通过 PROFIBUS DP);
- 安全相关智能从站-智能从站通信(通过 PROFIBUS DP);
- 安全相关智能从站-从站通信(通过 PROFIBUS DP);
- 安全相关智能 IO 控制器-IO 控制器通信(通过 PN/PN coupler);
- 通过 S7 连接进行安全相关的通讯（通过 S7 Ethernet Connection）;
- 安全相关的 S7 Distributed Safety 和 S7 F Systems 通信。

安全相关的主站-智能从站通信:

主站-智能从站 F-CPU 间的通讯连接，必须在硬件组态中设置彼此的通讯地址区。如下图所示的设置中，两个 CPU 都可以发送和接收数据。



下面通过一个例程来描述如何实现主站-智能从站安全通信。其他通讯方式这里不作描述，具体操作可参考手册。

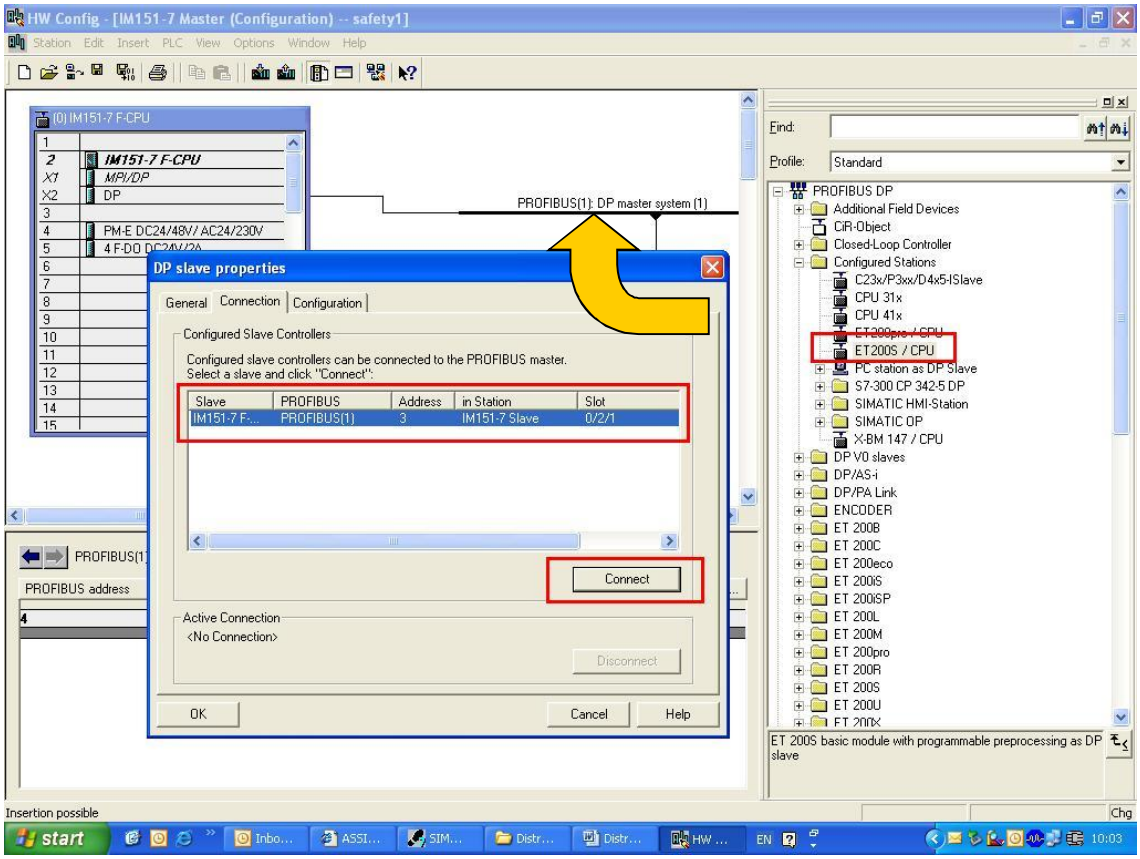
4.2 硬件组态

4.2.1 从站组态

组态步骤与前边主站的组态方法一致，这里不在描述，参见本文档 3.2 节。

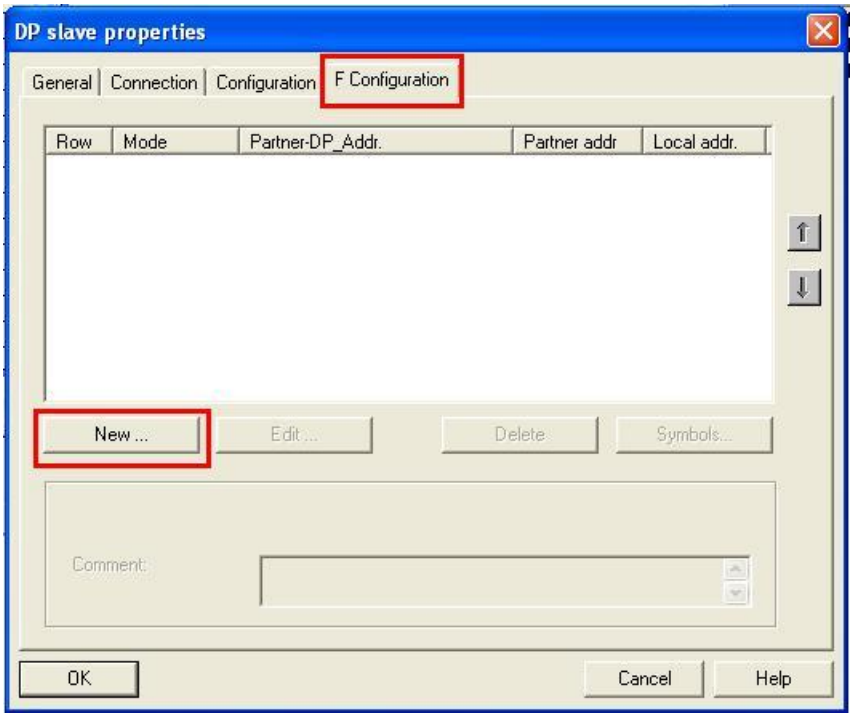
4.2.2 添加从站

在主站硬件配置窗口中，插入 ET200S 智能从站。这一步骤与在普通 CPU 中配置过程一样。



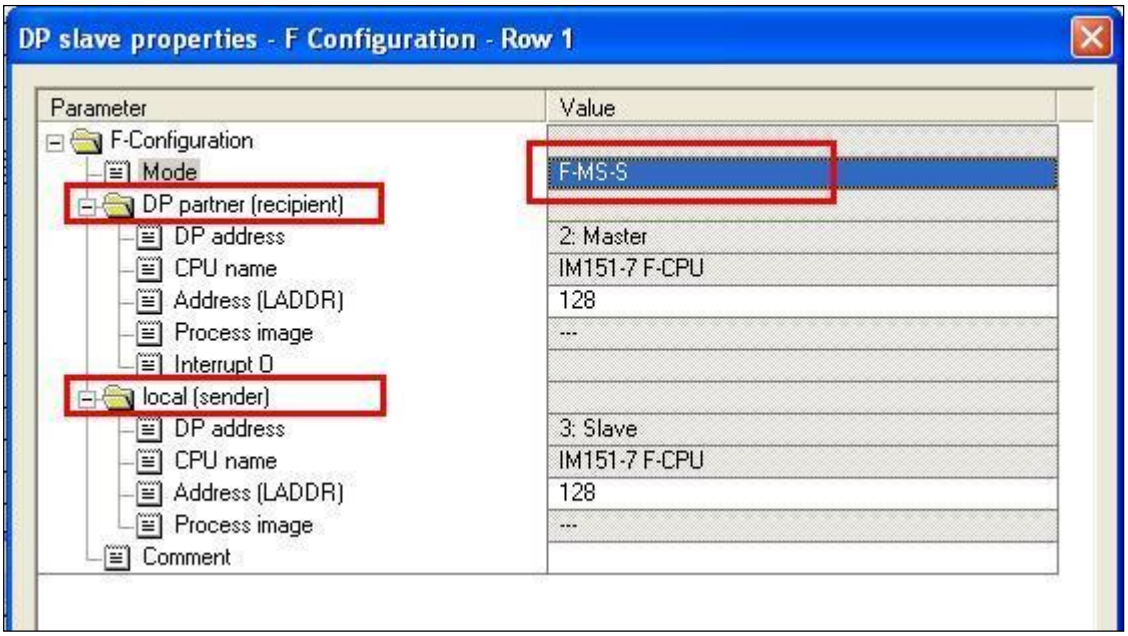
4.2.3 组态安全相关的通信地址区

1）双击 ET200S 从站图标，打开“ DP slave properties”设置窗口，选择“ F Configuration”标签页（普通 CPU 站没有这个标签页），点击“ NEW”创建 F 通信连接。



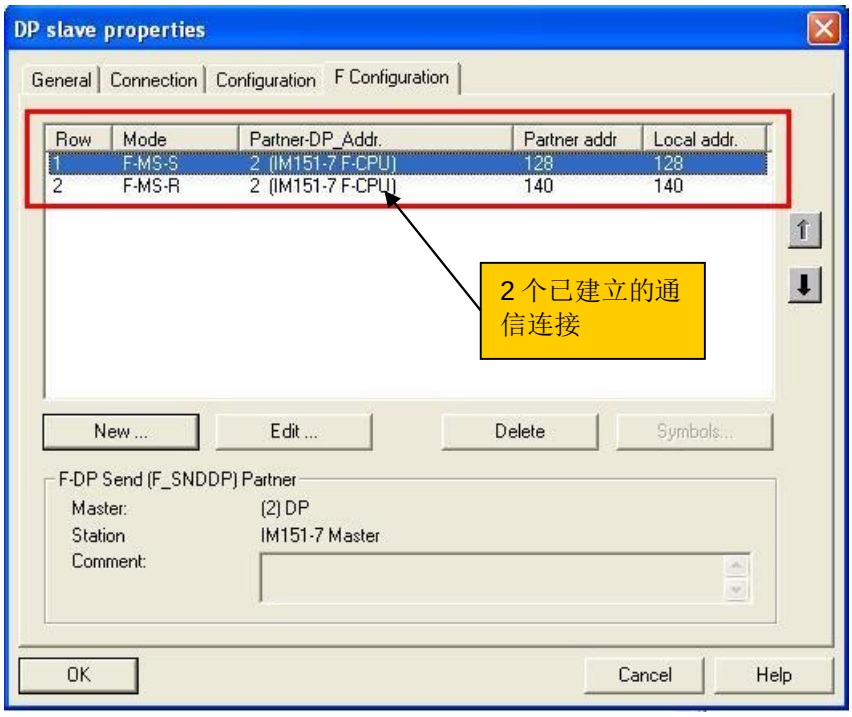
2）配置智能从站到主站的发送通讯 F-MS-S模式，会自动列出通讯的发送方（sender）和接收方（recipient）的详细参数。对于F-MS-R都是相对从站来讲的，F-MS-S从站发送、主站接受；F-MS-R从站接受、主站发送。

图中“Address（LADDR）”表示为通信所设定的地址区的起始地址。

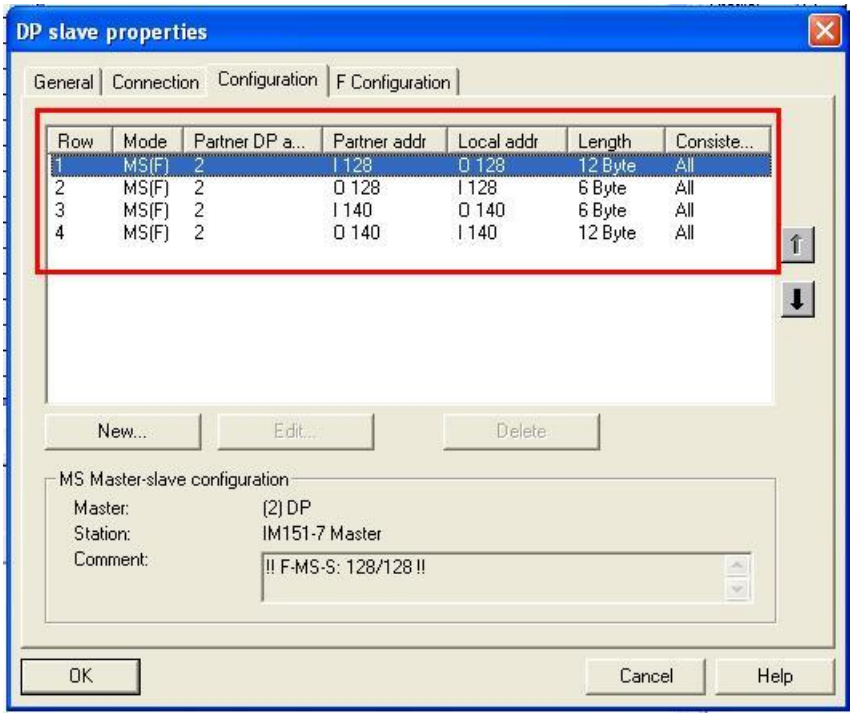


同样方法，配置智能从站到主站的接收通讯 F-MS-R 模式。

3）完成配置后，回到“DP slave properties”窗口，可以看到已经建立的通信连接。



同时，在“Configuration”标签页中，可以看到系统自动生成了相关通信设置，从这里可以了解通信地址区的使用情况，这些设置不能修改。



从上两图可以看出，用于发送和接收通讯连接所分配的地址区如下表所示：

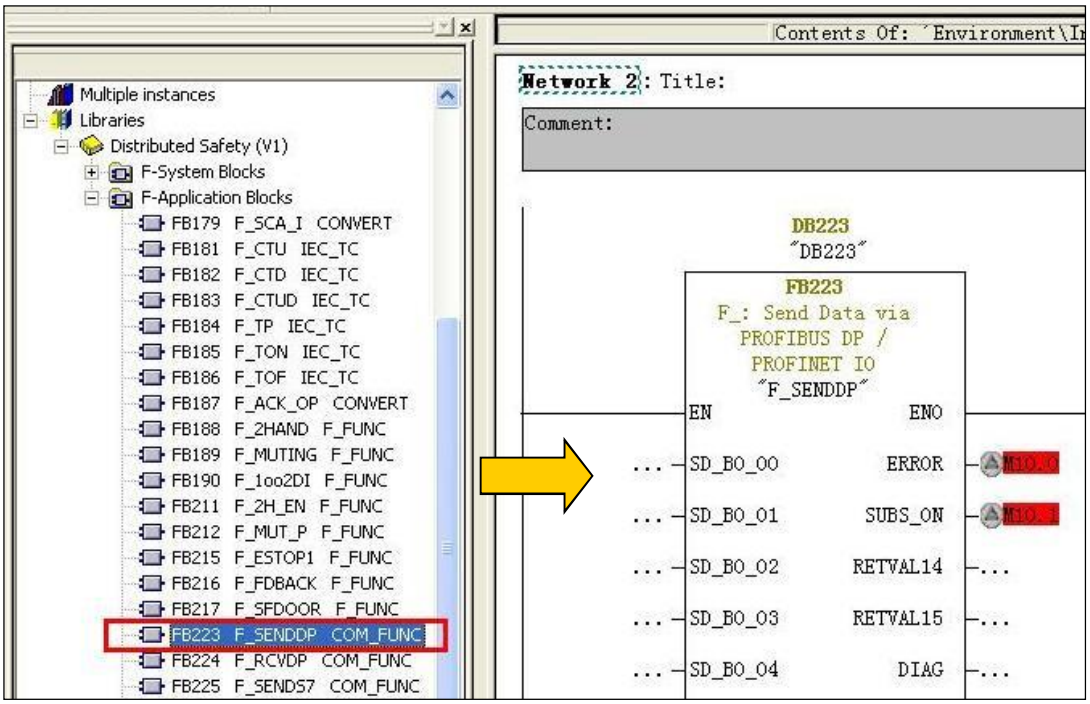
连接类型	所分配的地址区
发送：智能从站到主站	智能从站：12 字节输出、6 字节输入
	主站：12 字节输入、6 字节输出
接收：智能从站从主站	智能从站：12 字节输入、6 字节输出
	主站：12 字节输出、6 字节输入

4.2.4 编程通信

实现主站与智能从站之间的安全相关的通信，必须在安全程序中调用 F 功能块：F_SENDDP（发送）和 F_RCVDP（接受）。这两个块可传送 16 个布尔型数据和 2 个整形数据。需要注意的是 F_RCVDP 必须在 F 程序块的开头调用，F_SENDDP 必须在 F 程序块的结尾调用。

现在通过编程实现前边配置的第 2 个连接通信：F-MS-R（主站发送、从站接受）。

1）在主站安全程序中调用 F_SENDDP 功能块；



参数说明：

输入变量：

DP_DP_ID：连接号，相同连接号的功能块互相对应发送/接受数据，例中赋值为 1。

TIMOUT：安全相关通信的监控时间。例中赋值 T#500ms。

LADDR：通信区域的开始地址。上边组态时分配的起始地址为 140，所以这里赋值 140。

SD_B0_00-SD_B0-15：通信地址区，对应发送的 16 个位变量地址。

SD_I_00、SD_I_01：通信地址区，对应发送的 2 个整形变量地址。

输出变量：

ERROR：1=通信错误。

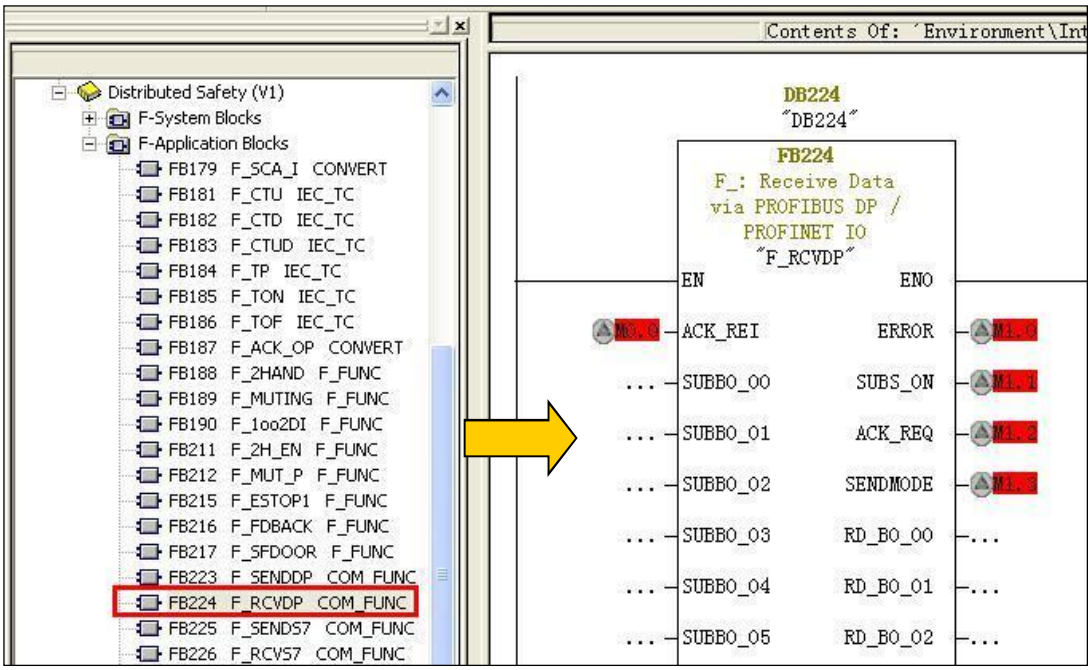
SUBS_ON：1=接收方输出故障安全值。

RETVAL14：SFC14 的错误代码。

RETVAL15：SFC15 的错误代码。

DIAG：服务信息。

2）在从站安全程序中调用 F_RCVDP 功能块。



参数说明：

输入变量：

DP_DP_ID：连接号，相同连接号的功能块互相对应发送/接受数据，例中赋值为 1。

TIMOUT：安全相关通信的监控时间。例中赋值 T#500ms。

LADDR：通信区域的开始地址。上边组态时分配的起始地址为 140，所以这里赋值 140。

ACK_REI：通讯错误后的去钝。

SUBBO_00-SUBBO_15：布尔型接受数据的故障安全值。

SUBI_00、SUBI_01：整形接受数据的故障安全值。

输出变量：

ERROR：1=通信错误。

SUBS_ON：1=输出故障安全值。

ACK_REQ：发送数据的去钝请求。

SENDMODE：1=F_SENDDP 的 F_CPU 处于安全模式失效。

RD_BO_00-RD_BO_15：接受数据布尔变量 00-15。

RD_I_00、RD_I_01：接受数据整形变量 00-01。

RETVAL14：SFC14 的错误代码。

RETVAL15：SFC15 的错误代码。

DIAG：服务信息。

在 F_SENDDP 中，要发送的数据位于输入端 SD_BO_xx 和 SD_I_xx；在 F_RCVDP 中，接收到的数据位于输出端 RD_BO_xx 和 RD_I_xx。

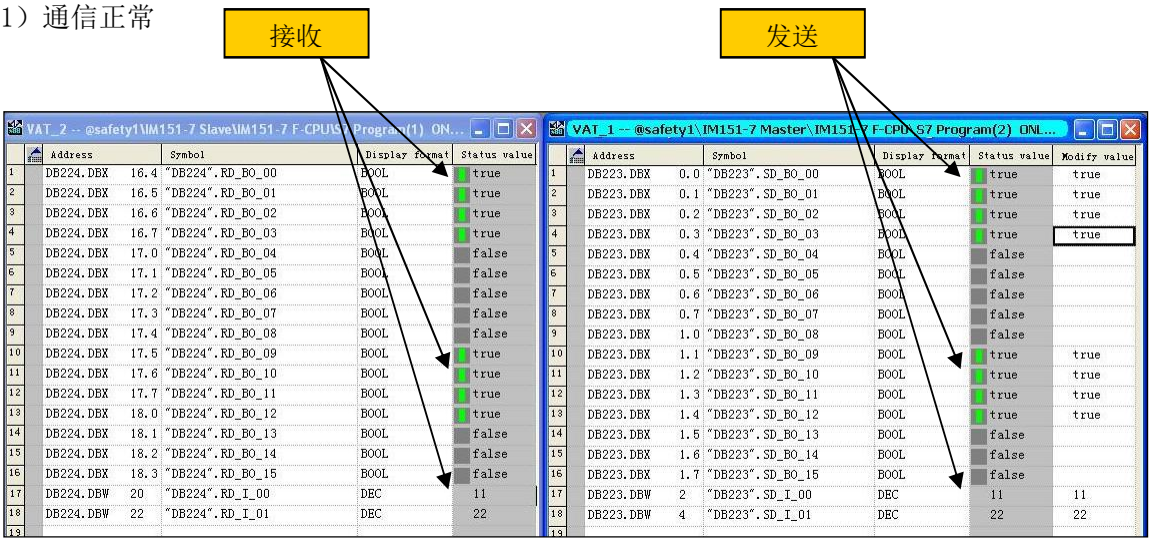
F_RCVDP 的输出端 SENDMODE，提供了调用 F_SENDDP 的 F-CPU 的操作模式。如果该 F-CPU 处于失效的安全模式，则 SENDMODE＝1。

F-CPU 间的通讯在后台以专门的安全协议进行。必须在 F_SENDDP 和 F_RCVDP 的输入端 DP_DP_ID 分配一个网络范围的用户自定义的唯一值，用来建立一个 F-CPU 的 F_SENDDP 与另一个 F-CPU 的 F_RCVDP 之间的联系。相联系的 F_SENDDP 和 F_RCVDP 使用相同的 DP_DP_ID 值。

3）重新编译主站和从站的安全程序，然后分别下载到主从 F-CPU 中，运行测试。

4.2.5 通信结果

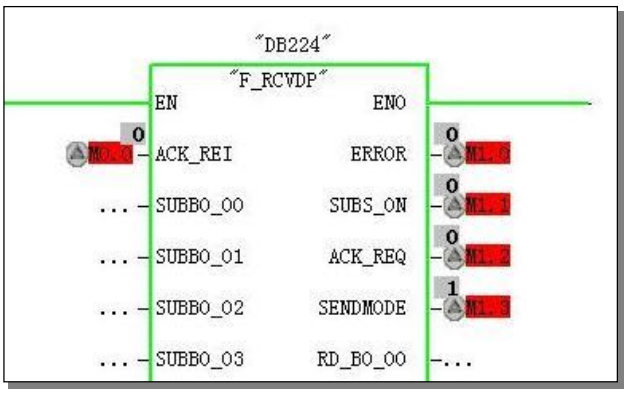
1）通信正常



从上图可以看到，发送端发送的 8 个布尔变量和 2 个整形变量都被接受端成功接受到。

需要注意的是，在安全模式下，安全变量不能在变量表中被直接写操作。如果一定要写入，必须不激活安全模式。这里为了测试，没有激活主站安全模式。

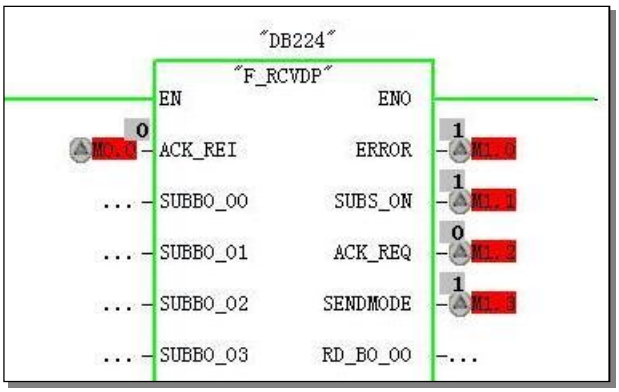
通过下图可以看到当前的通信状态。通信正常，没有错误。SENDMODE=1 表明主站的 F_CPU 安全模式没有激活。



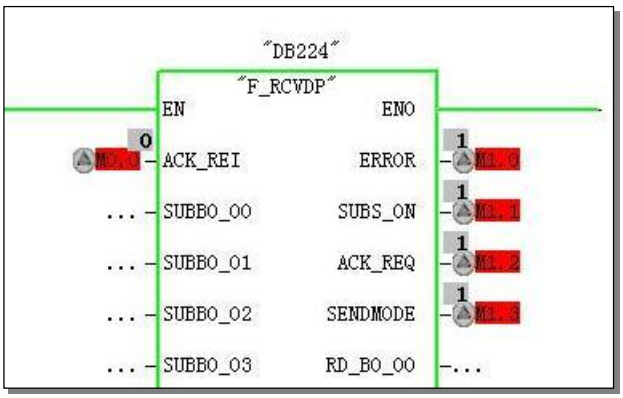
2）测试通信失败：拔掉 PROFIBUS-DP 电缆，中断通信。从下图可以看到：

ERROR=1 通信错误；

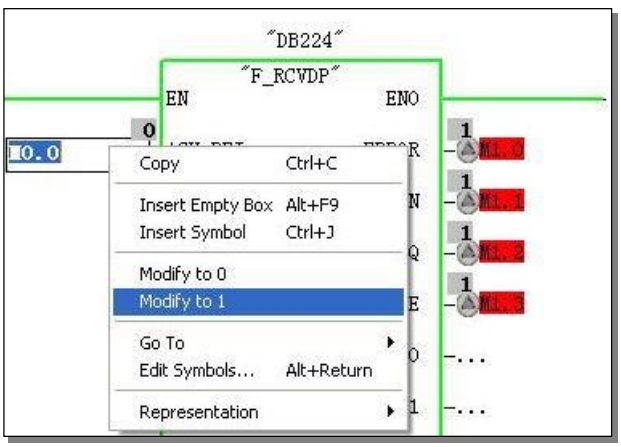
SUBS_ON=1 使用安全替代值（SUBBO_00-SUB0-15、SUBI_00-SUBI_01）作为接受数据。



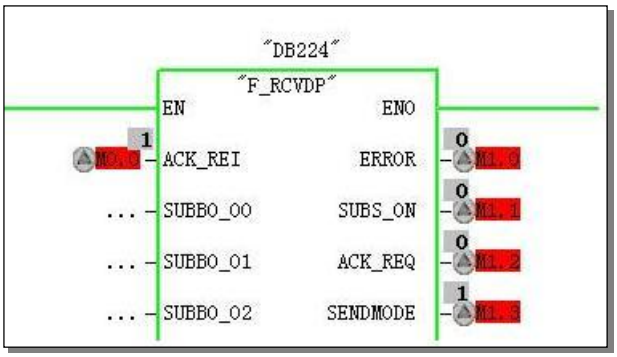
重新恢复 PROFIBUS-DP 电缆连接。ACK_REQ=1 表明故障去除，发送故障确认请求。在故障确认前，继续使用安全替代值（SUBBO_00-SUB0-15、SUBI_00-SUBI_01）作为接受数据。



置位 ACK_REI 确认应答。



应答确认后，通信恢复正常。


"DB224"
"F_RCVDP"
EN
ENO
1
M0.0
ACK_REI
ERROR
0
M1.0
...
SUBBO_00
SUBS_ON
0
M1.1
...
SUBBO_01
ACK_REQ
0
M1.2
...
SUBBO_02
SENDMODE
1
M1.3