SIEMENS安全PLC基础与原理介绍

1. 安全标准概述
2. S7-300安全组件
3. S7-300安全编程组态
4. S7-300安全程序编写
5. 安全程序的测试
6. 模块的钝化与去钝

事故、危险、风险

事故是什么？

一个事故是无法预料的事件，这个事件可能会导致对人身财产或设备的伤害或损毁。

什么是危险？什么是风险？

危险：可能损伤或危害健康的起源

风险：在危险情况下，可能损伤或危害健康的概率和程度的综合。

危险的类别

电的危险：电击，热辐射等

热源导致的危险：灼伤，烫伤

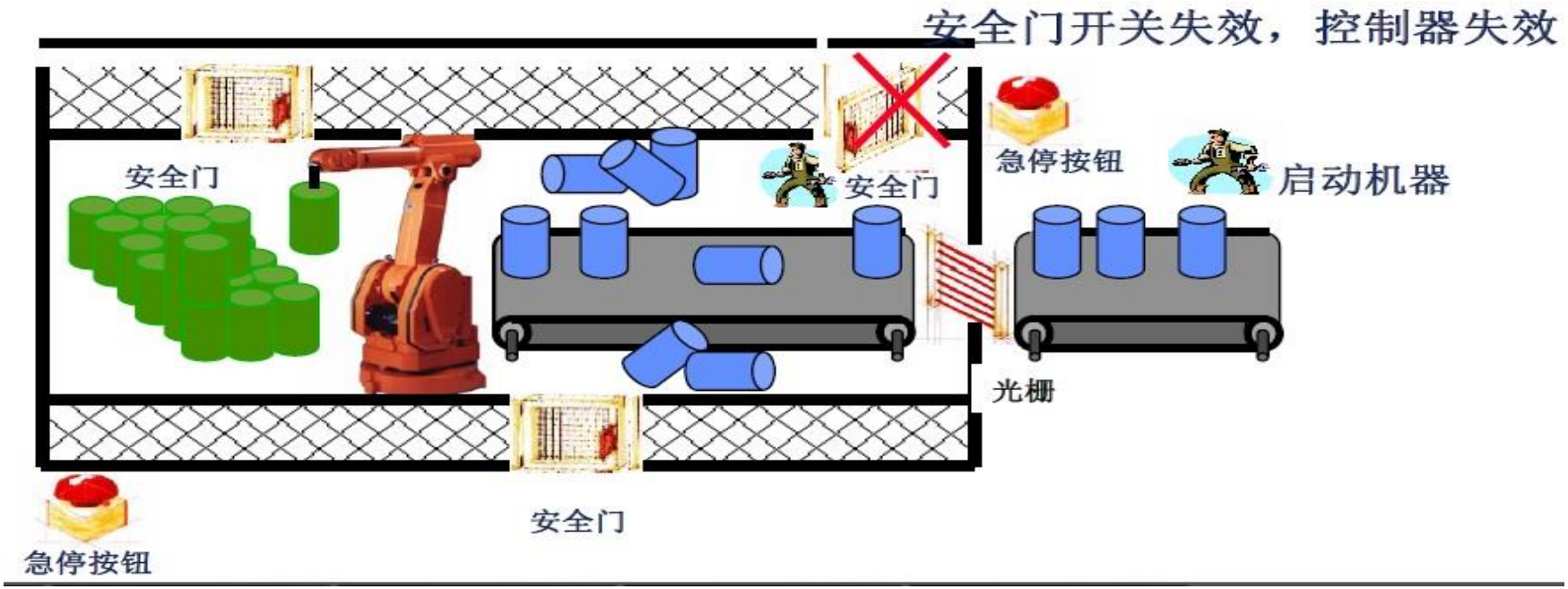
噪声：失聪

气体冲击等等

危险及事故的产生原因

任何一台机器都存在危险。一台安全的设备、或采用安全保护和控制措施的生产过程能够避免事故的发生。

事故是如何发生的？人的不安全行为（如违章、违规操作）和物的不安全状态（如控制器件失效、机器误动作等）。



安全保护装置

如何避免物的不安全状态？

必须提供一种高度可靠的安全保护手段，最大限度地避免机器的不安全状态、保护生产装置和人身安全，防止恶性事故的发生、减少损失。这种手段就是安全系统。安全系统在开车、停车、出现工艺扰动以及正常维护操作期间对生产装置提供安全保护。一旦当工厂装置本身出现危险，或由于人为原因而导致危险时，系统立即做出反应并输出正确信号，使装置安全停车，以阻止危险的发生或事故的扩散。

安全护网

安全PLC

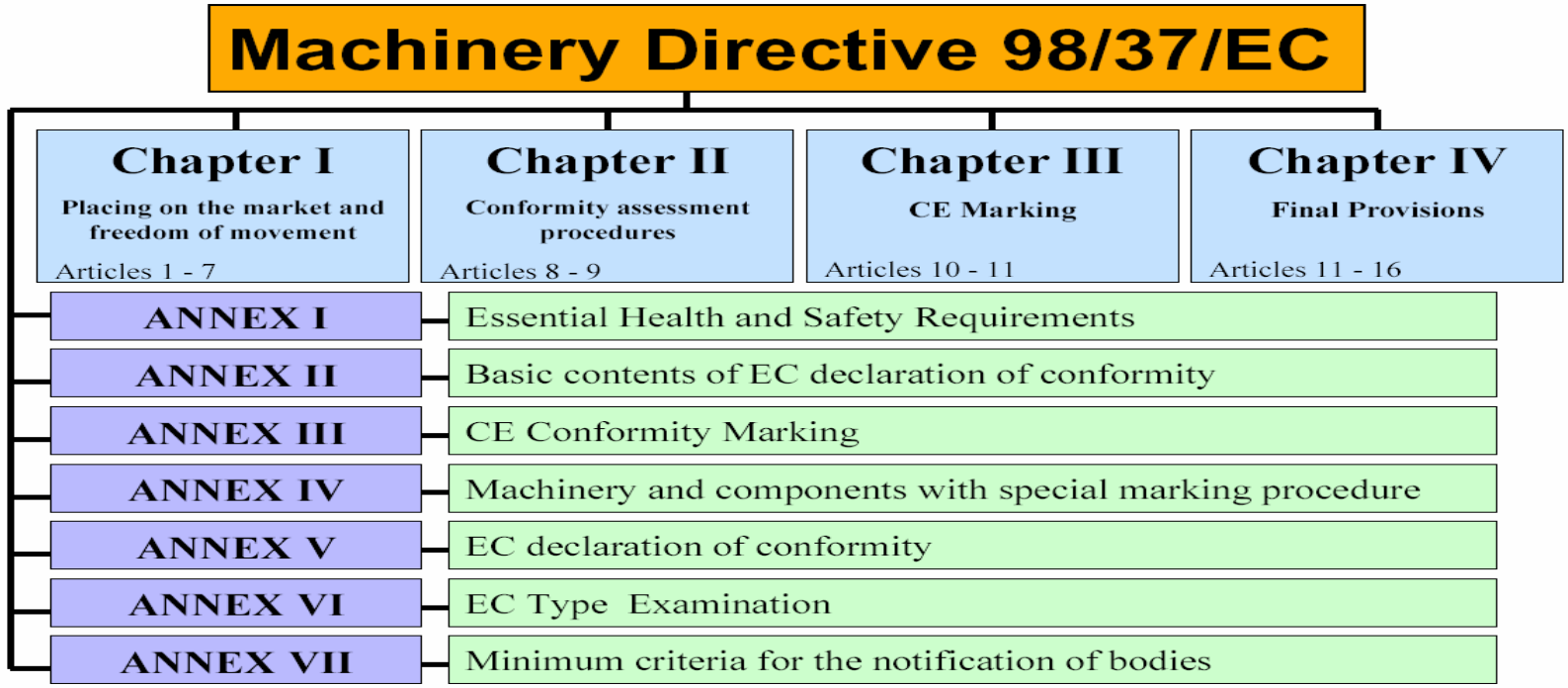
急停按钮、急停拉线

双手开关

CE标准说明

机械产品在加施CE标志和（或）随产品随带EC合格证明时，主要应该遵循机械指令，并且符合其要求。

机械指令是“关于统一各成员国有关机械法律的指令”的简称。



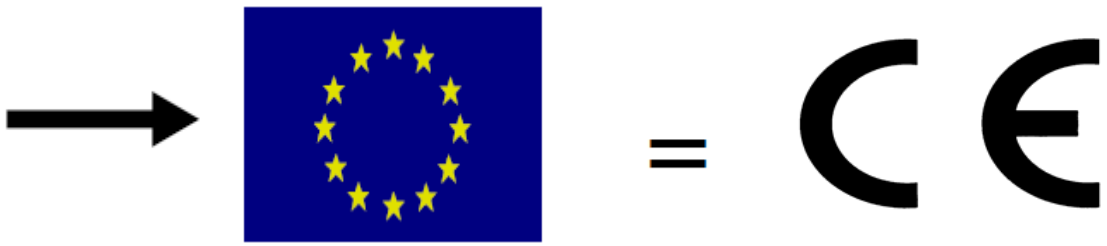
标准设备符合欧盟流通的要求

CE标志是欧盟官方颁布的、统一在工业产品上使用的强制性标志。

CE标志是一种产品安全合格的标志，不具有商业意义。

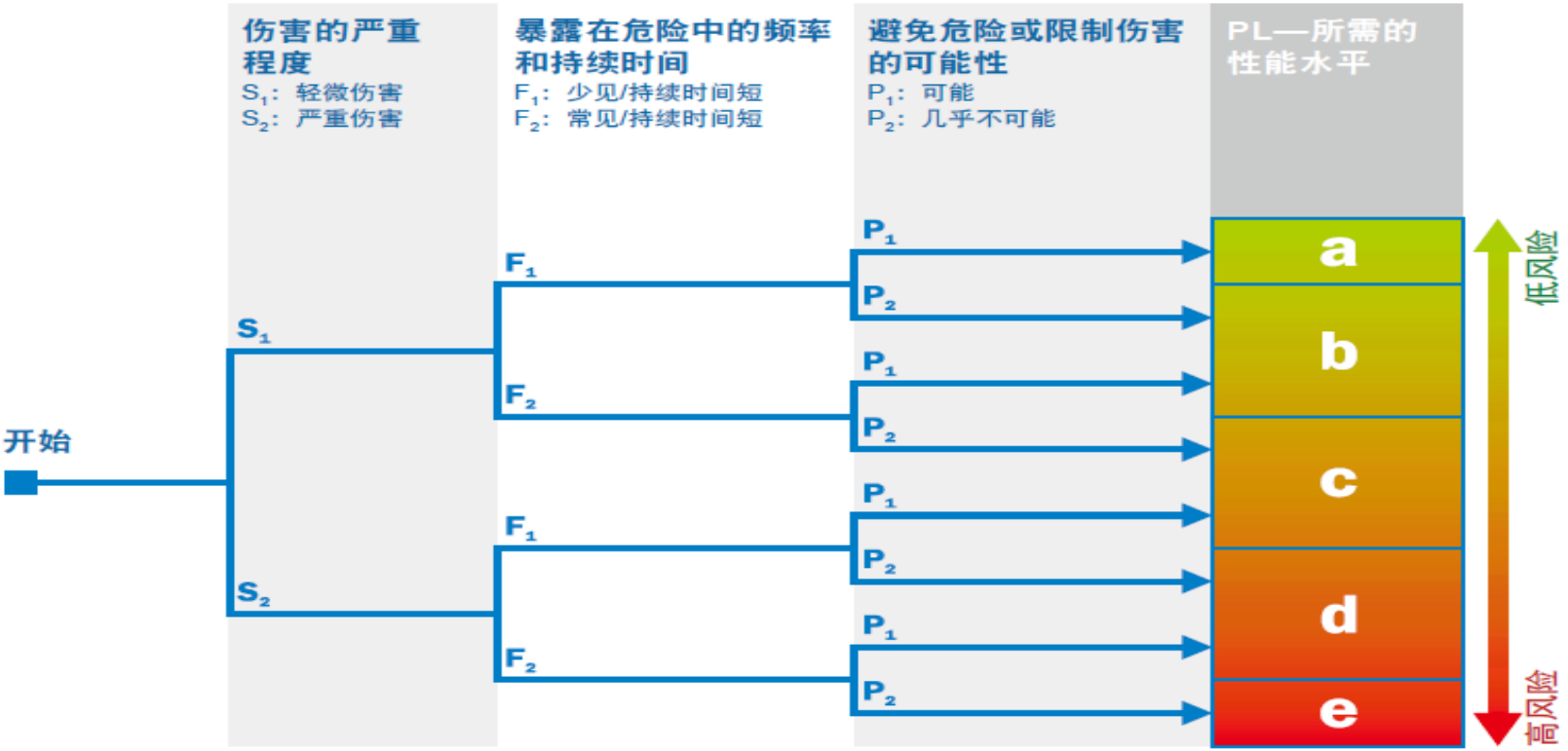
产品上加施了CE标志，就表明产品符合欧盟所颁布的相关新方法指令的要求，产品具有指令所规定的安全水平，产品可以投放市场和使用。

因此，CE标志也可以是产品进入欧盟市场的准入标志。



ISO 13849-1：风险图

风险图用于确定安全功能的必要PL_r



性能水平通过 5 个步骤进行定义，它取决于控制系统的结构、所使用部件的可靠性、故障检测能力以及在多通道控制系统中对多个共因失效的抵抗力。

IEC 62061：风险图

IEC 62061的附录中也给出了采用以下表格形式的一种方法。

Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency and duration, Fr		Probability of hzd. event, Pr		Avoida Av
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Common	5	
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4	
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impos
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Pos
							> 1 yr	2	Negligible	1	Li

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure

Comments

PL与SIL的比较

该表说明了PL与SIL应用于采用低复杂性电动机械技术的典型回路结构时，PL与SIL之间的大致关系。

PL (性能级别)	PFH_D (每小时的危险性失效概率)	SIL (安全完整性级别)
A	$\geq 10^{-5}$ to $<10^{-4}$	无
B	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
C	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ to $<10^{-6}$	2
E	$\geq 10^{-8}$ to $<10^{-7}$	3

PL与SIL之间的大致相同部分

功能安全的实现方法

Risk assessment
- 风险评估

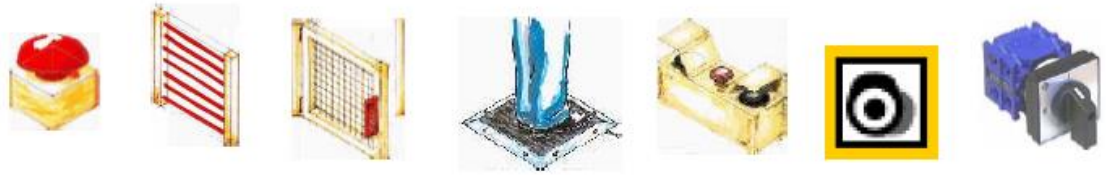
Risk reduction
- 风险降低

Proof
- 通过安全功能验证

风险降低三步法

1. 安全的结构设计
2. 技术措施应用：1，检测 2.执行 3.评估
3. 编写用户手册

安全系统的组成



安全输入信号

安全控制模块

输出控制元件

一致性评估

本身风险评估的过程是一个专家组依据标准（可以是PL，也可以是SIL）的一个“主观的”、“经验的”讨论过程。

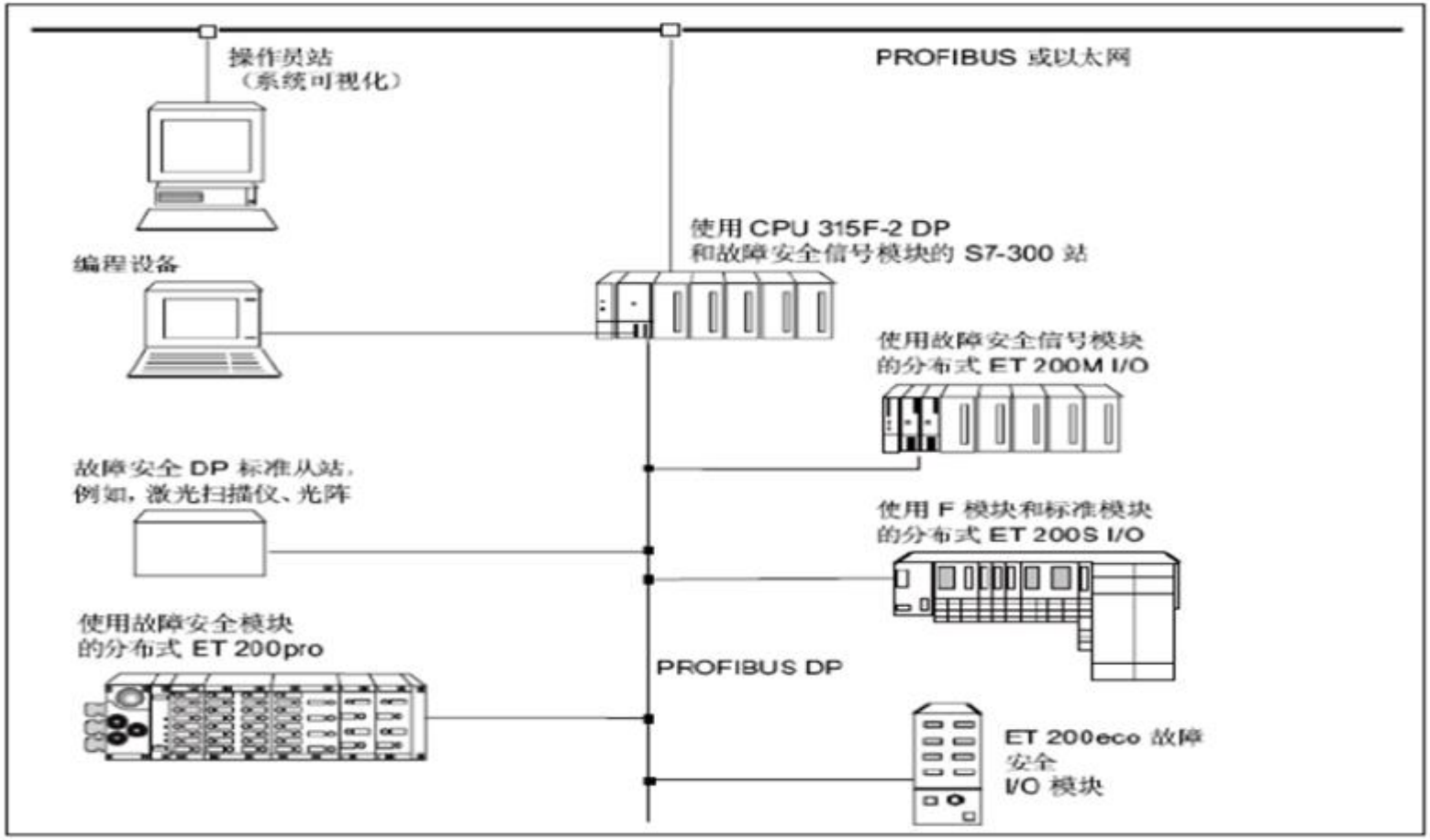
定好“安全等级”后，要参照“协调标准”进行传感器、执行器、控制机构、相关“安全功能”指令（对上述传感器和执行机构进行检测）的选择了，确保能够达到对该安全功能所要求的“安全等级”。

按照这些标准做出来“功能安全”，并通过了验收测试后，该产品就可以获得MD的认证，在欧盟内部自由流通。而该产品的“功能安全”部分也有应该有要有一个欧盟内的通行认证，这就是厂家所出具的“一致性评估报告”（与“协调标准”相一致）。

注：“协调标准”是由欧洲标准委员会和欧洲电工标准委员会制定的，在欧盟官方杂志上列出的，且各欧盟成员国必须采用的技术细节标准。

S7 Distributed Safety 组件

硬件组件



S7 Distributed Safety 组件

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

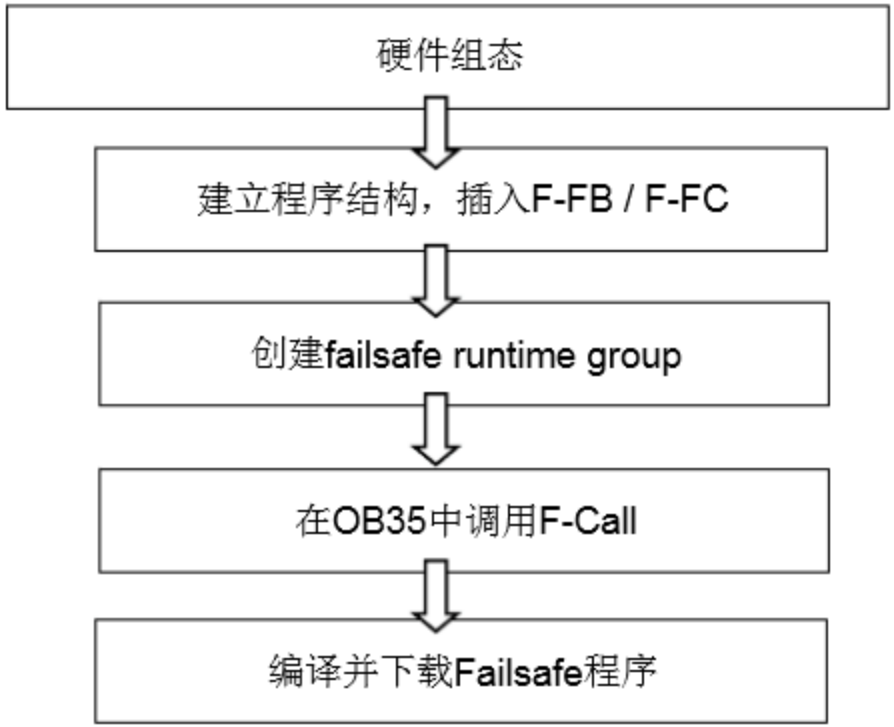
S7 Distributed Safety 对分布式故障安全系统进行组态和编程的选件包

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。

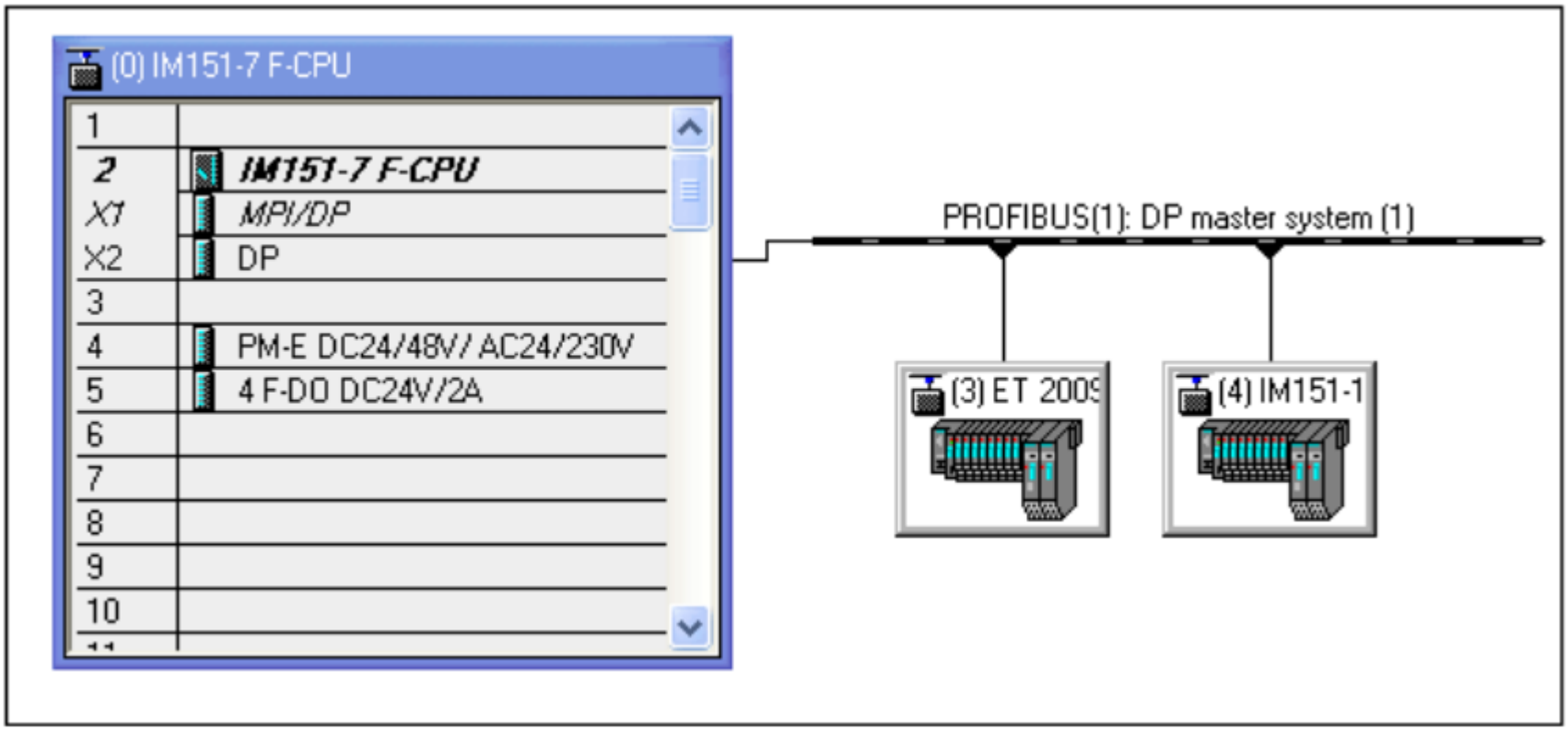
分布式故障安全系统的组态和编程

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：



硬件组态步骤

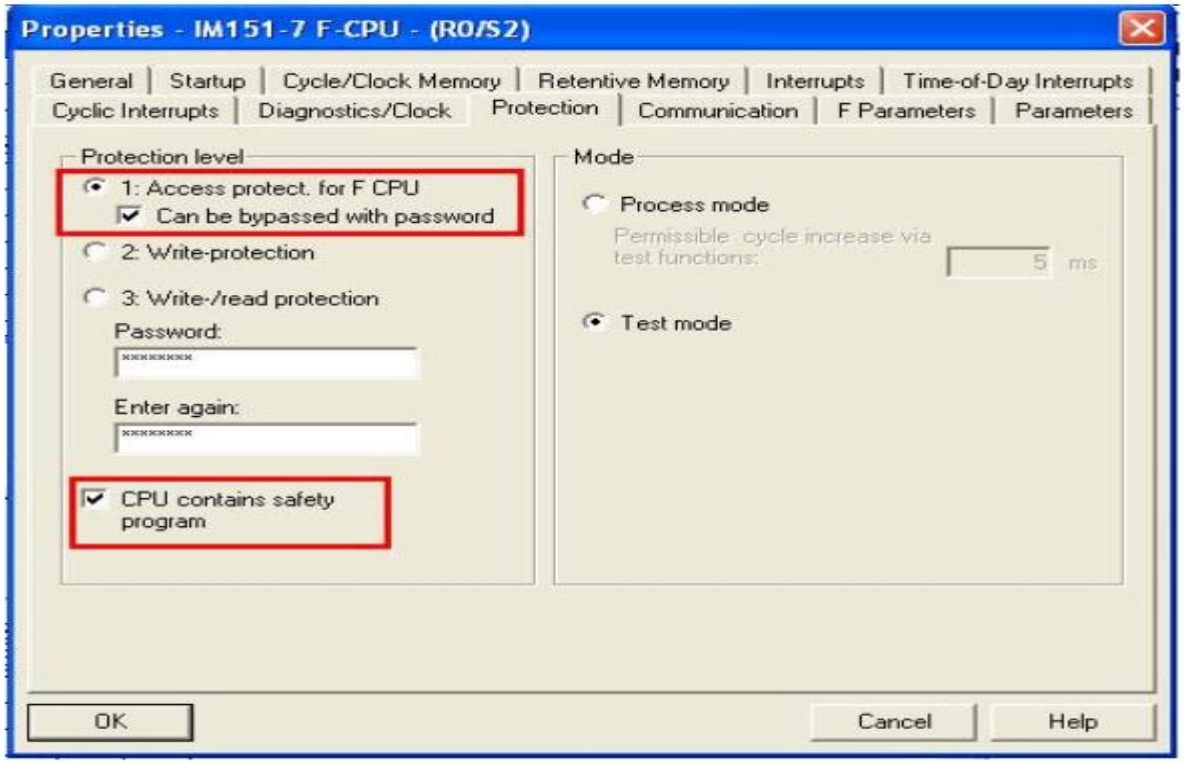
这个环节与普通PLC系统组态方法基本一致，根据实际的硬件配置，对F-CPU，ET200S的电源模板、F-DI/DO，逐一进行组态，ET200M上用于电位隔离模块不需组态。



组态F-CPU

相对于普通CPU，F-CPU还需要如下两步配置：

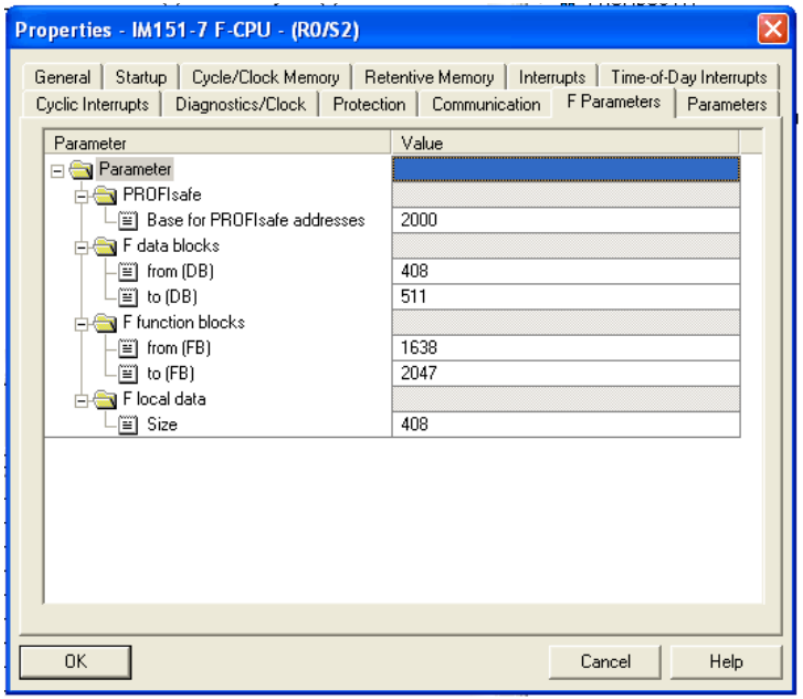
配置 F-CPU 密码保护，F-CPU 的密码防止将F系统从工程系统（ES）或编程设备（PG）未经授权下载至F-CPU。



编写安全程序时，注意勾选左图中CPU包含安全程序选项.

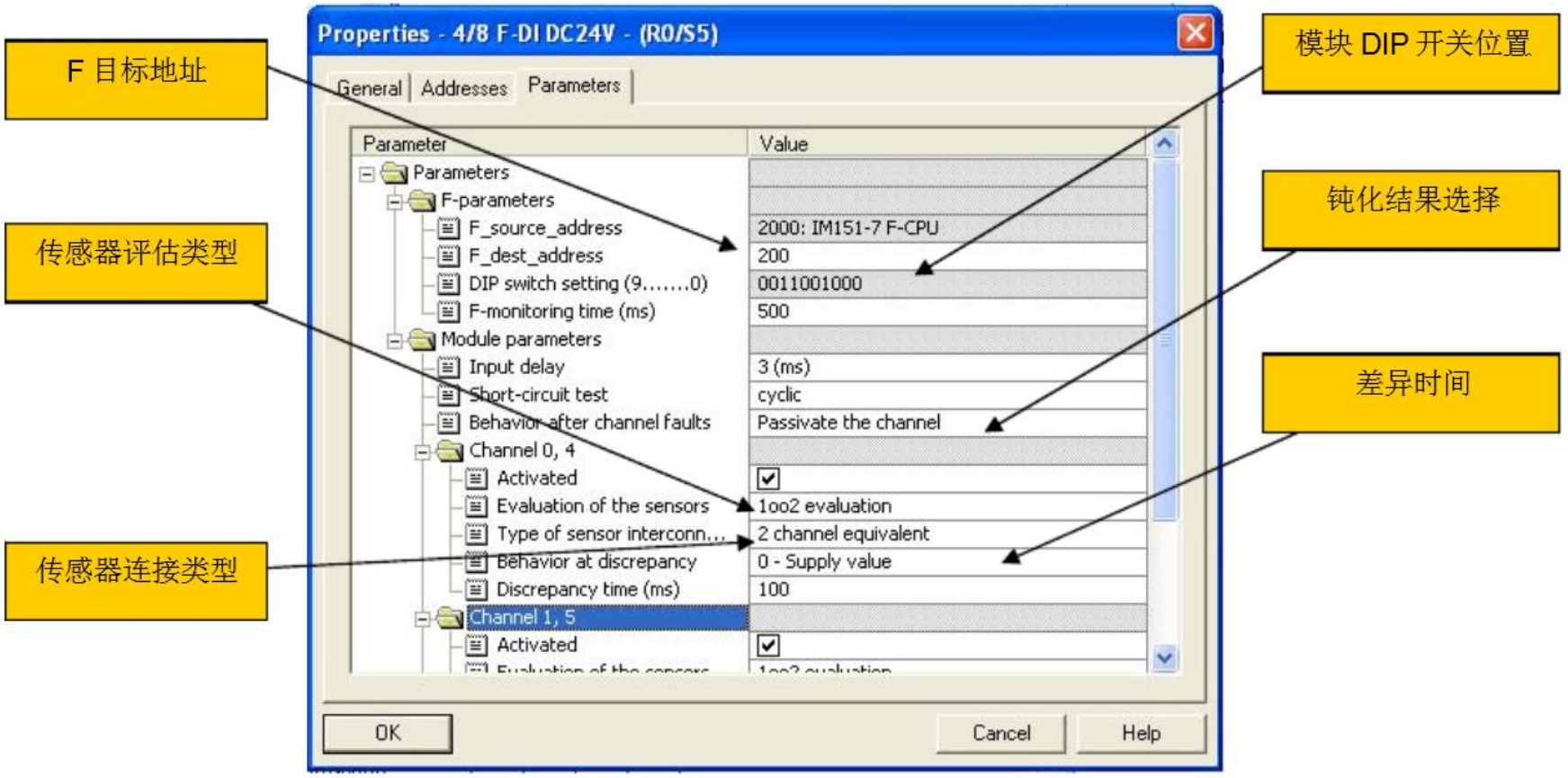
组态F-CPU

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。



组态 F-IO

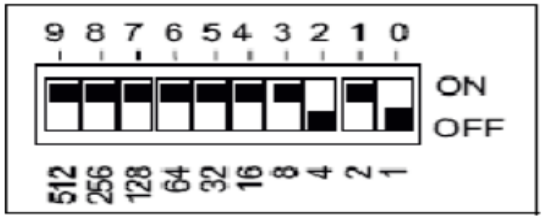
需要注意，安全模块侧面有DIP开关，F目标地址的设定值必须与DIP开关的位置设定值一致。



组态 F-IO

F 目标地址：每个安全模板都会有唯一的F 目标地址，该地址需保证其唯一性。

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）。

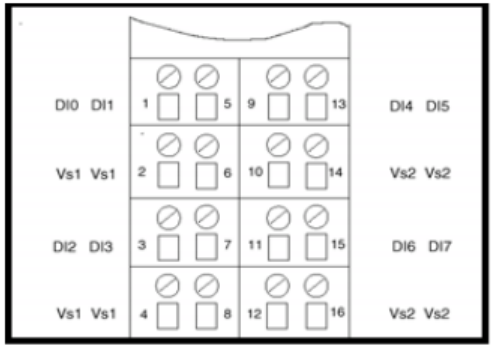


传感器评估类型：

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。

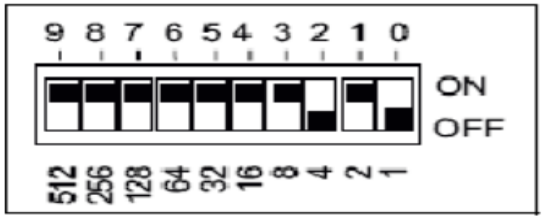
- Failsafe 的输入方式



组态 F-IO

F 目标地址：每个安全模板都会有唯一的F目标地址，该地址需保证其唯一性。

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）。



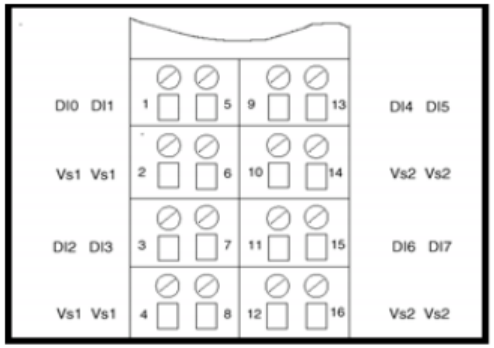
传感器评估类型：

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。

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。

- Failsafe 的输入方式

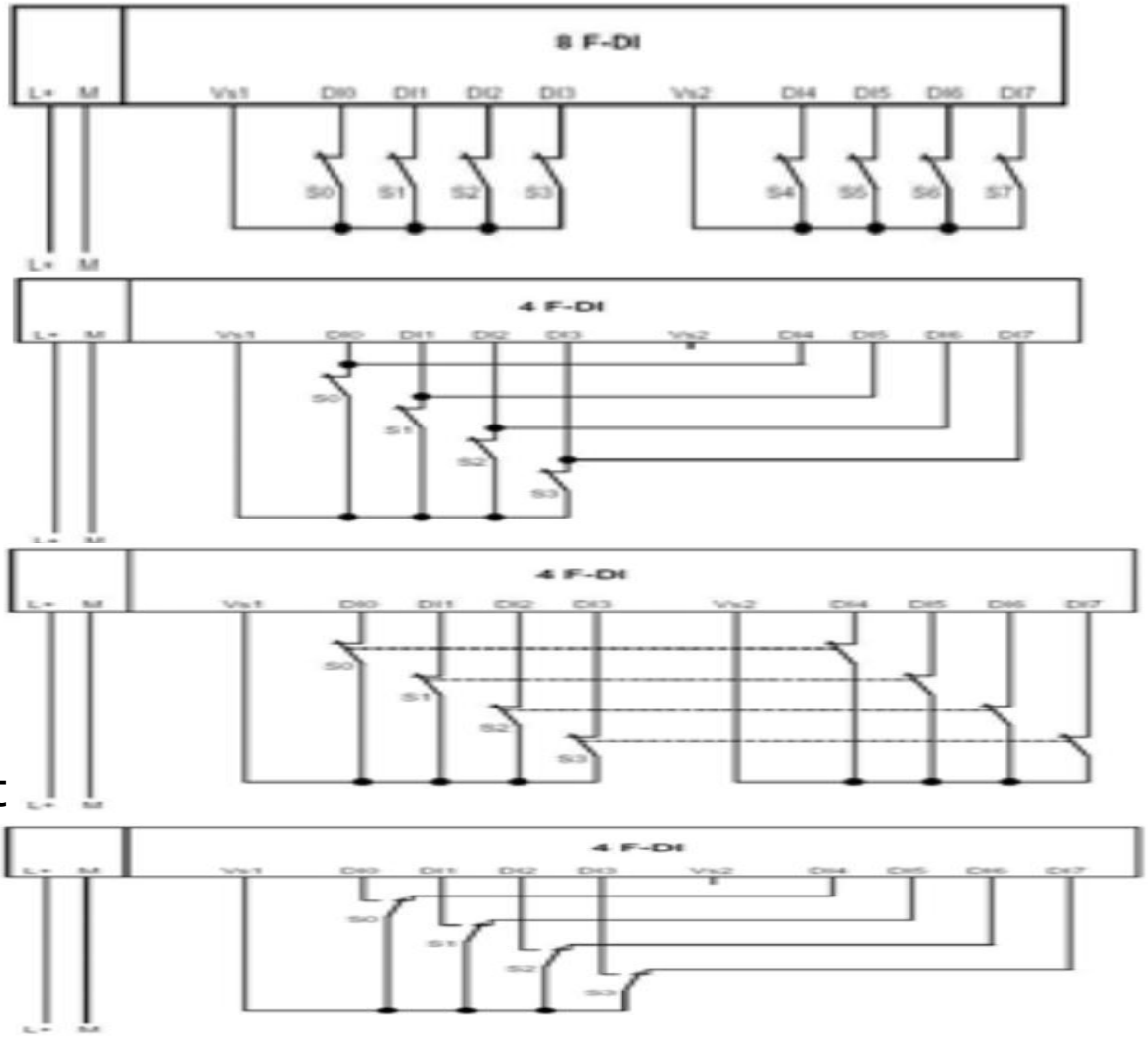


传感器的连接类型

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

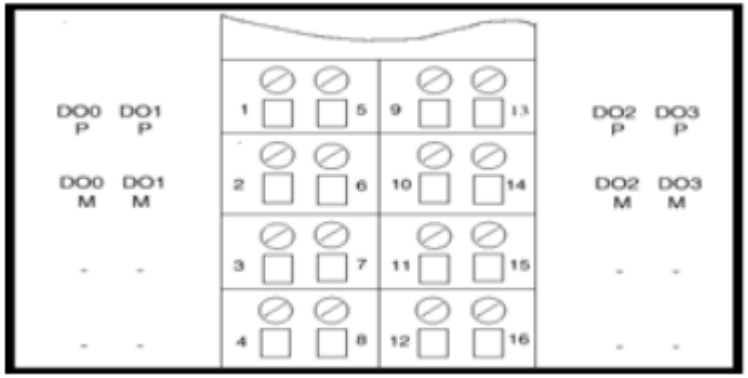
单通道传感器
1 oo 2 evaluation
Short circuit test
AK6/SIL3/Kat.4

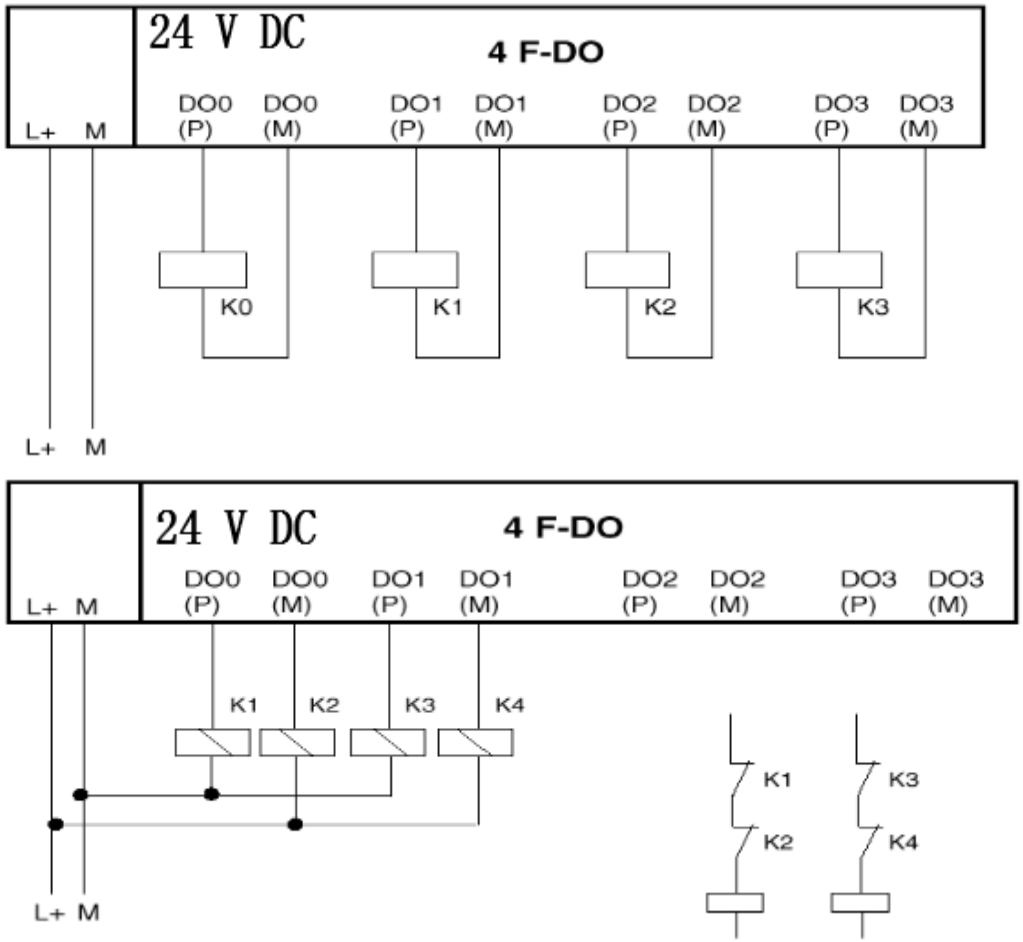
双通道传感器或
两个单通道传感器
1 oo 2 evaluation Short circuit test
AK6/SIL3/Kat.4



Failsafe 的输出方式

安全输出模块

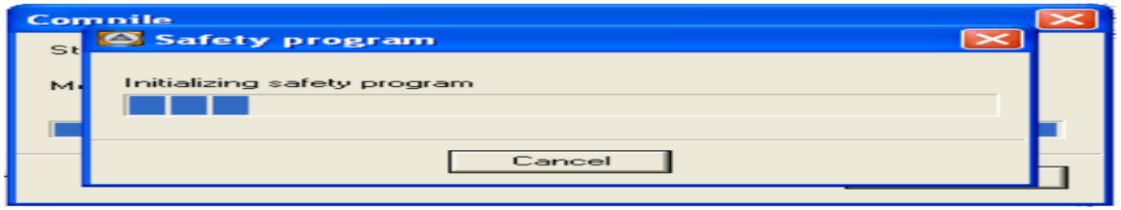




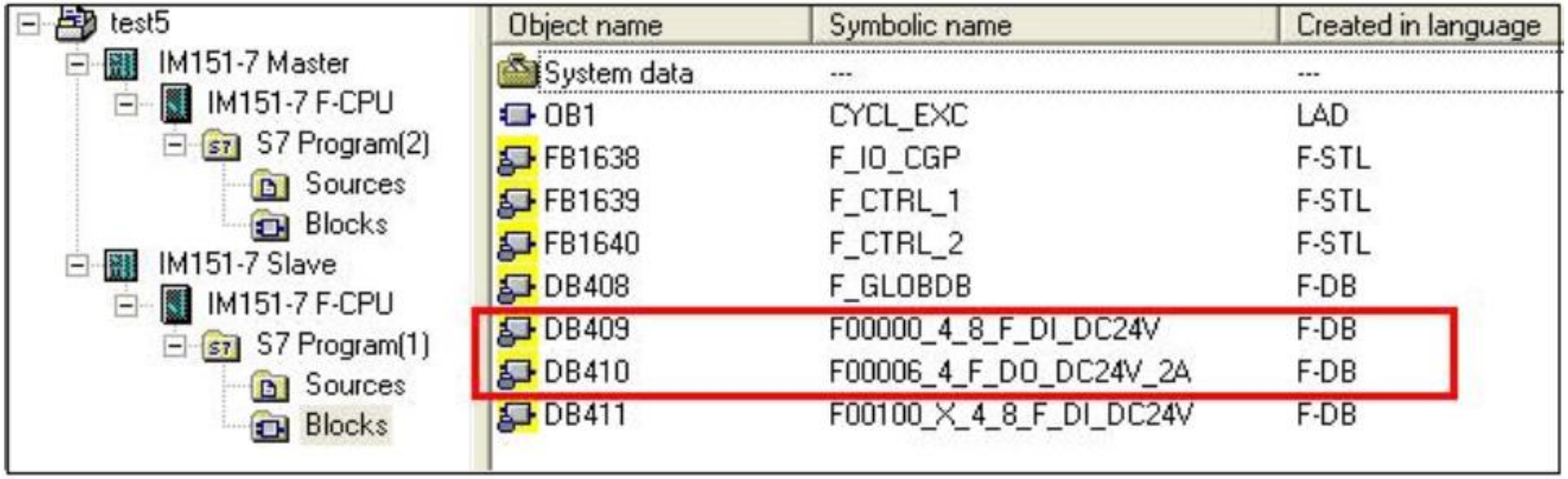
保存编译

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。需要注意的是，系统为每个组态的安全模块自动分配了一个数据块，用于信号的操作和查询。



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。

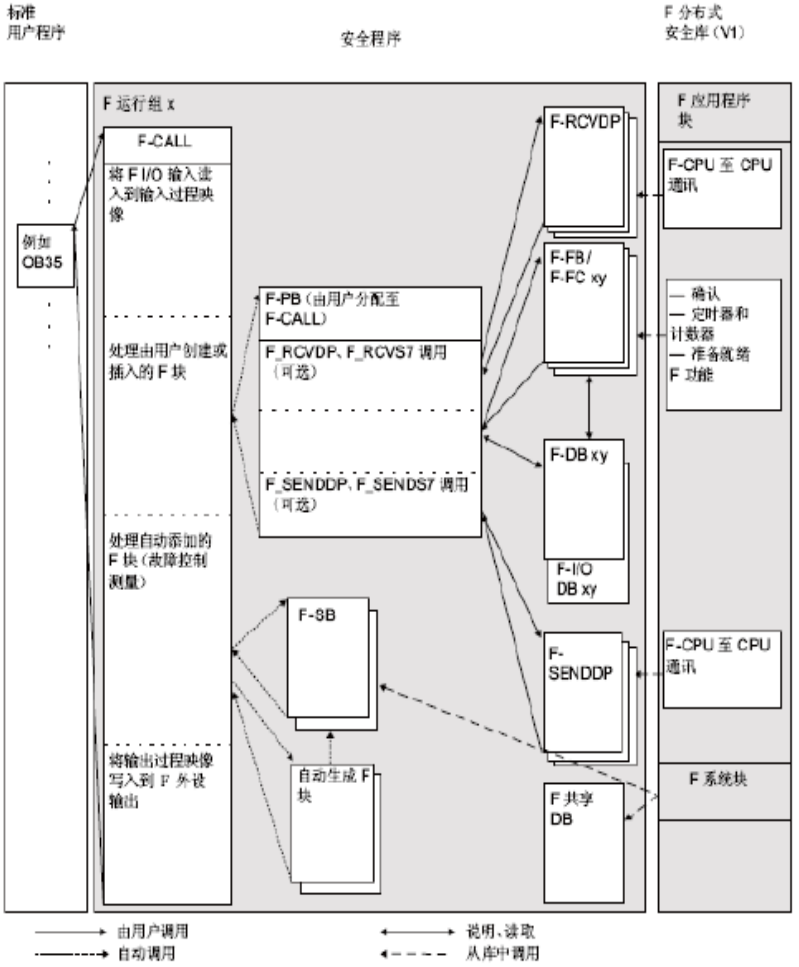
为了结构化，一个安全程序由一个或两个 F 运行组组成。

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）

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



安全运行组的组成

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 （如急停，安全门等）
- 来自自定义 F 库的 F 块
- F 系统块
- 自动生成的 F 块

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。

主站 4 F-D0模块：

DOO接指示灯L4; DO1接指示灯L5。

从站 4/8 F-DI 模块：

DI 2/6 接 1oo2 non-equivalent 开关 S8;

DI 3/7 接 1oo2 non-equivalent 开关S9。

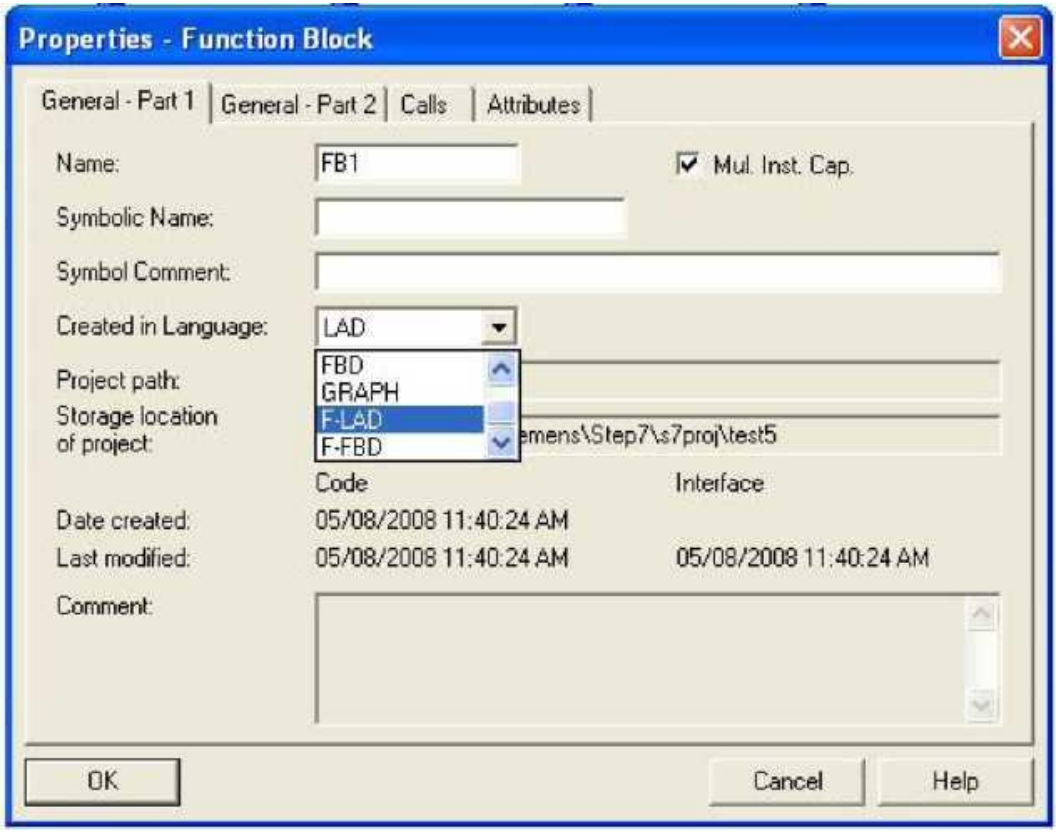
实现功能：

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。

程序实例

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.



程序实例

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。

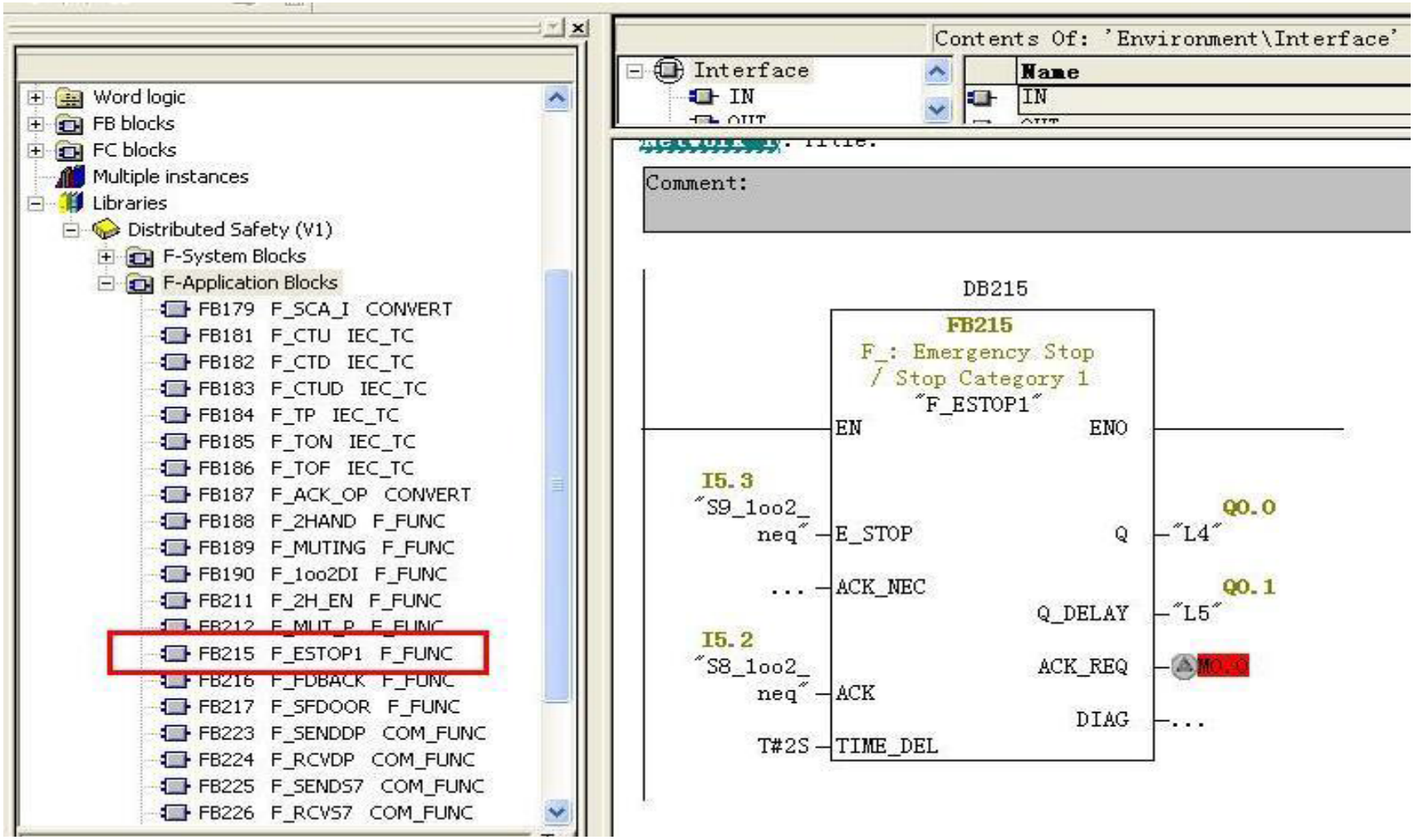
需要注意的是，从图中可以看到，来自安全模板通道I5.2、I5.3、Q0.0、Q0.1都是安全地址，而非安全地址M0.0以红色标示。

注：在安全程序中可以处理来自标准用户程序的数据。

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。

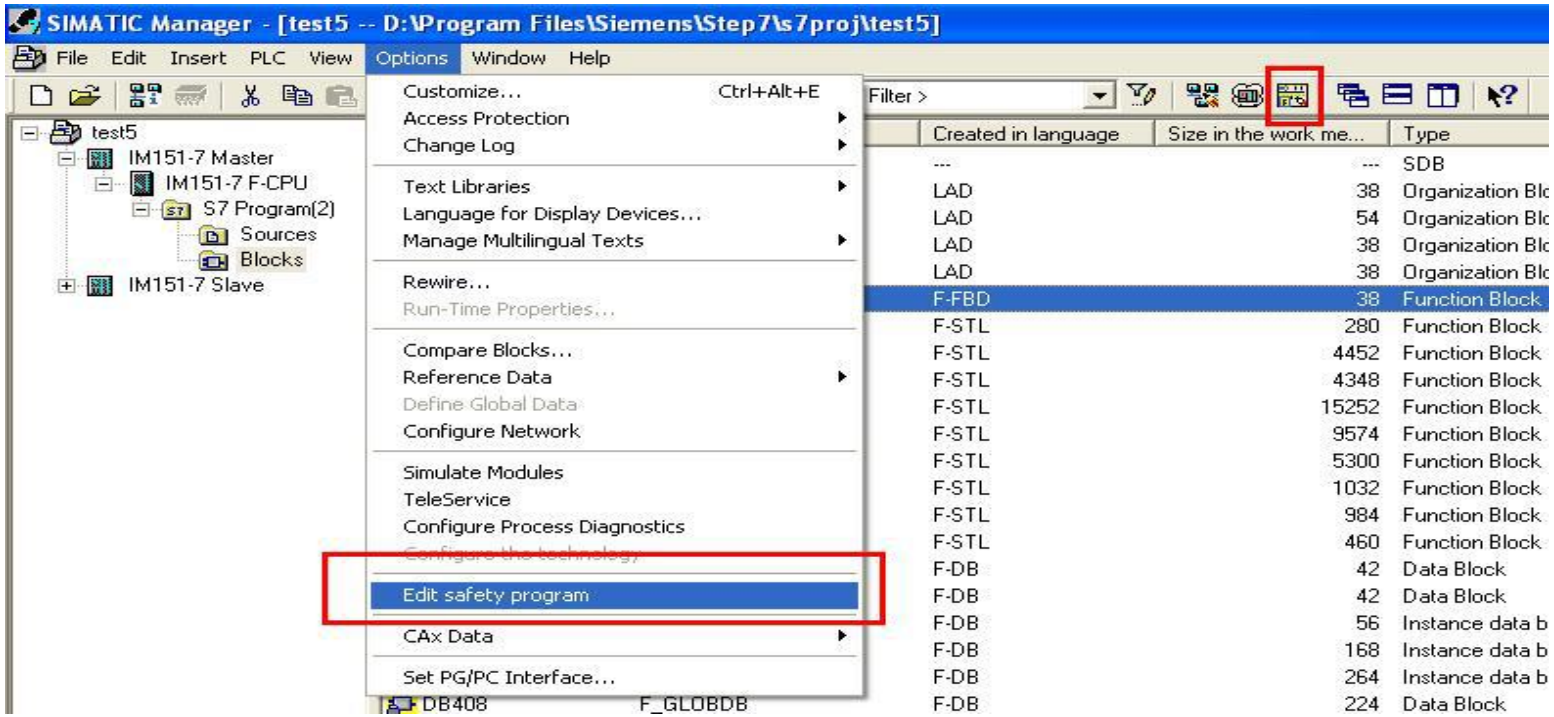
程序实例


Word logic
FB blocks
FC blocks
Multiple instances
Libraries
Distributed Safety (V1)
F-System Blocks
F-Application Blocks
FB179 F_SCA_I CONVERT
FB181 F_CTU IEC_TC
FB182 F_CTD IEC_TC
FB183 F_CTUD IEC_TC
FB184 F_TP IEC_TC
FB185 F_TON IEC_TC
FB186 F_TOF IEC_TC
FB187 F_ACK_OP CONVERT
FB188 F_2HAND F_FUNC
FB189 F_MUTING F_FUNC
FB190 F_1oo2DI F_FUNC
FB211 F_2H_EN F_FUNC
FB215 F_ESTOP1 F_FUNC
FB216 F_FDBACK F_FUNC
FB217 F_SFDOOR F_FUNC
FB223 F_SENDDP COM_FUNC
FB224 F_RCVDP COM_FUNC
FB225 F_SENDS7 COM_FUNC
FB226 F_RCVS7 COM_FUNC
Contents Of: 'Environment\Interface'
Interface
IN
Name
IN
Comment:
DB215
FB215
F_: Emergency Stop
/ Stop Category 1
"F_ESTOP1"
EN
ENO
I5.3
"S9_1oo2_
neq"
E_STOP
Q
Q0.0
"L4"
...
ACK_NEC
Q_DELAY
Q0.1
"L5"
I5.2
"S8_1oo2_
neq"
ACK
ACK_REQ
M0.0
DIAG
...
T#2S
TIME_DEL

创建 Failsafe Runtime Group

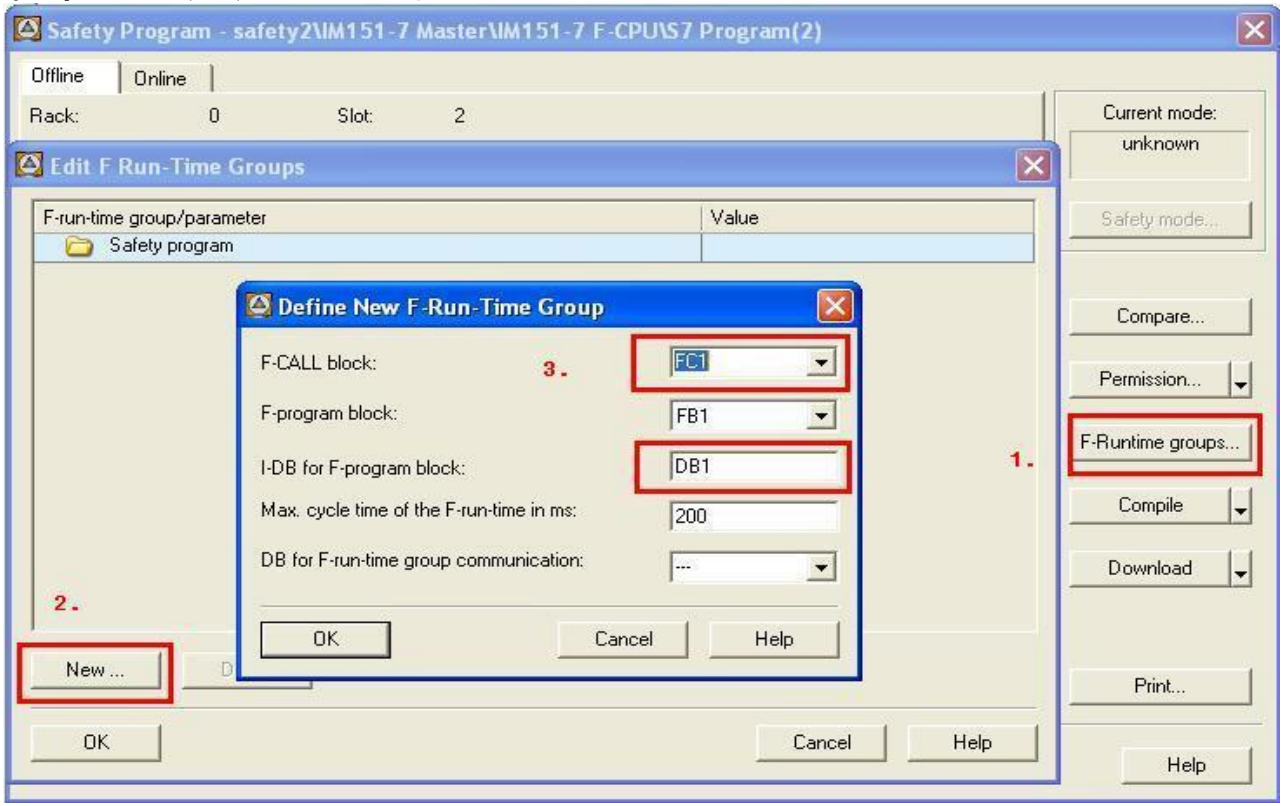
进入安全程序编译界面

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。



创建 Failsafe Runtime Group

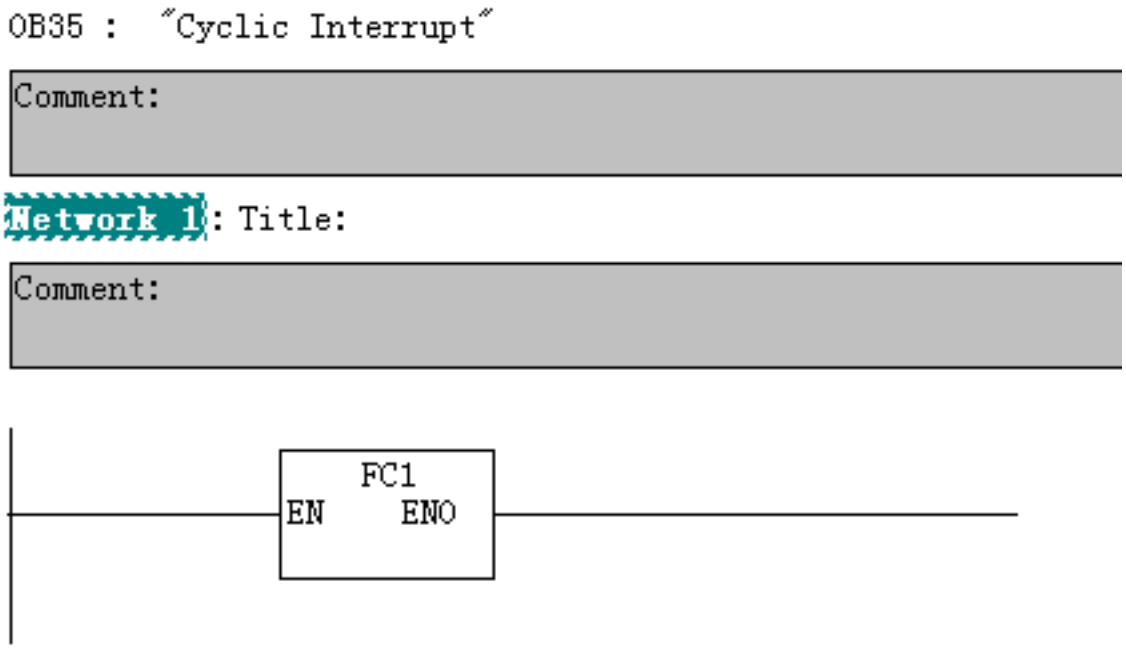
上一步创建完的FB1不能直接在标准用户程序中被调用，需要创建一个对应的F-CALL调用块和I-DB。如下图：FC1、DB1。点击“OK”后，它们会有系统自动生成并且处于加密状态，不能由用户进行编辑。



创建 Failsafe Runtime Group

在 OB35 中调用 F-CALL

直接调用刚才生成的F-CALL：FC1。



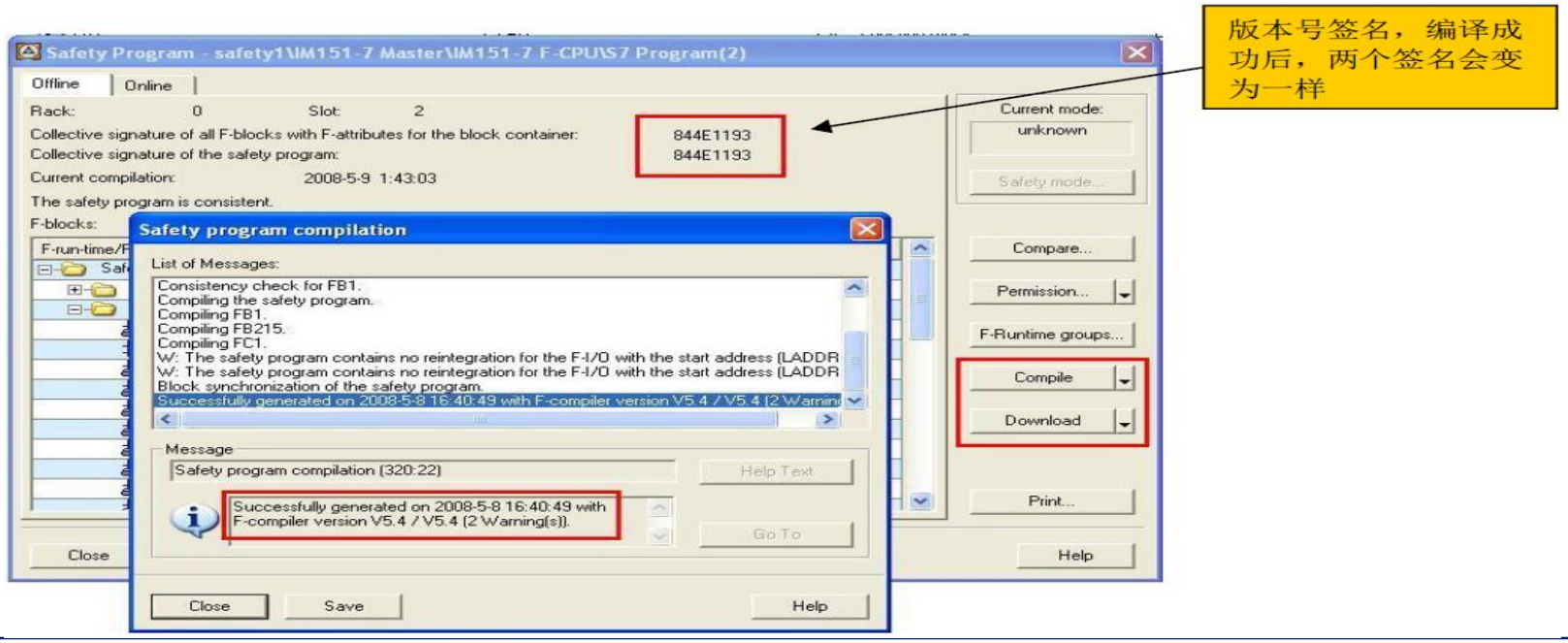
编译下载Failsafe程序

点击Safety编译窗体中的Compile，编译Failsafe程序；

这里需要注意：

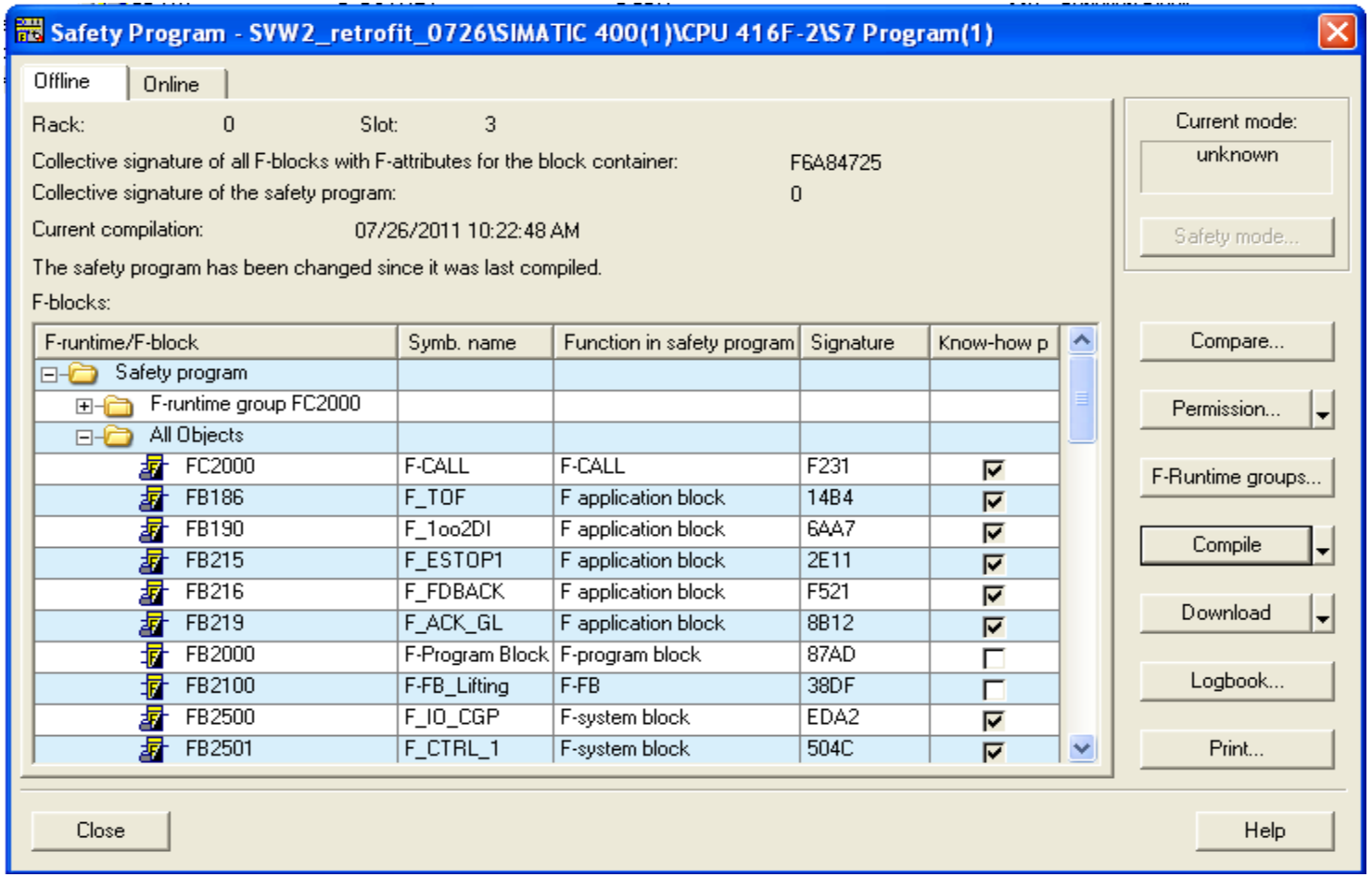
硬件组态应该首先下载；如果修改了硬件组态中CPU、F-I/O模块的有关参数，或者修改了 Failsafe程序中的F块，就应重新编译并下载Safety程序；

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。



编译下载Failsafe程序

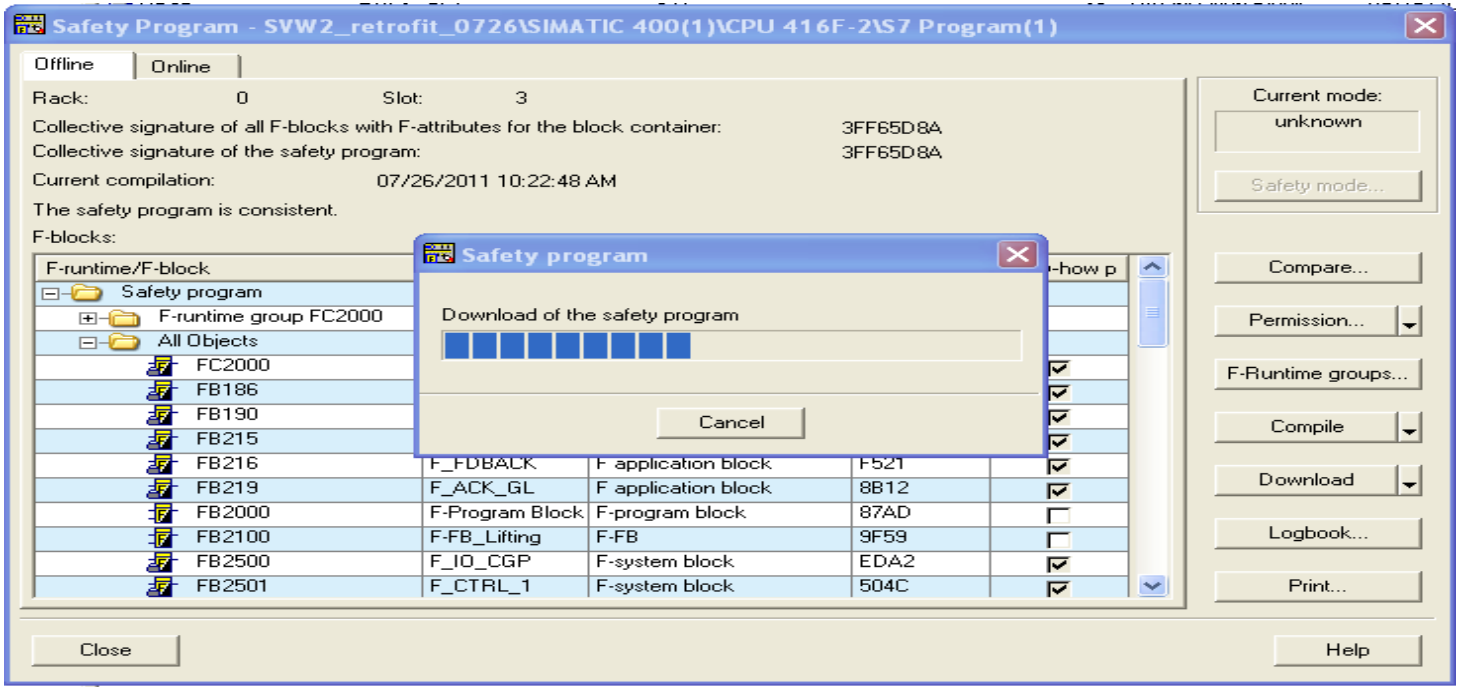
一旦修改过硬件配置或安全程序，则数字签名会不一致



编译下载Failsafe程序

只有在CPU停机的情况下才能下载安全程序。

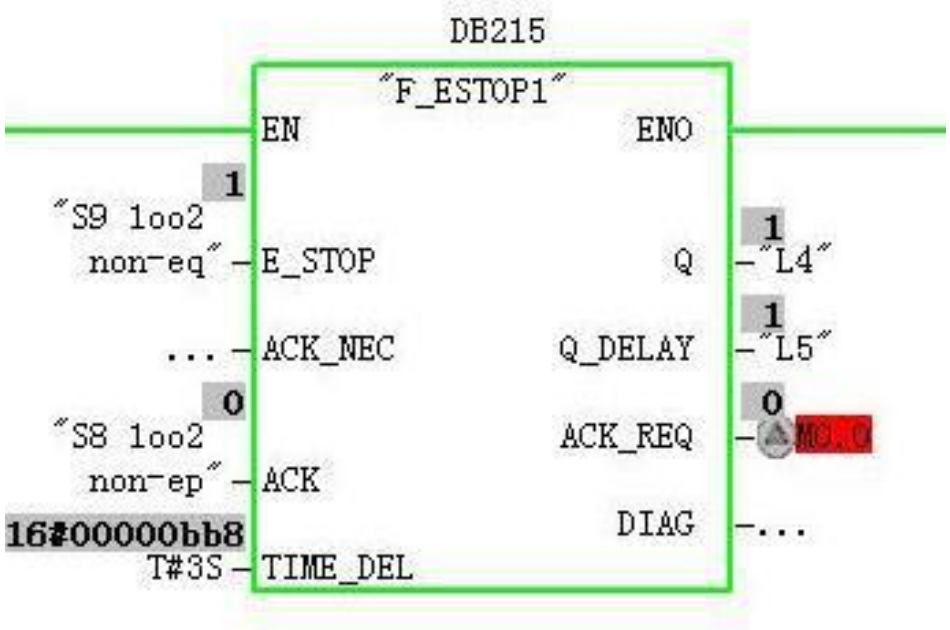
如果在程序监控状态下直接下载某个安全块，程序会弹出多个对话框要求确认，并且将取消安全模式。需特别注意的是，一旦PLC停机，CPU将无法再次起动。只有重新编译并下载后， CPU才可起动。



程序测试

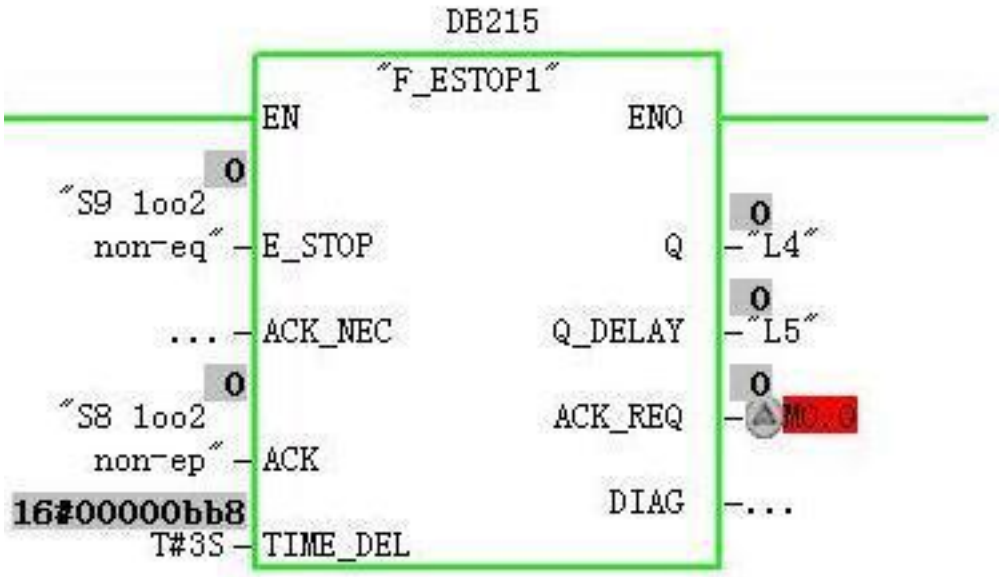
F—ESTOP1 运行结果

没有外部急停信号，Q、Q—DELAY输出1状态;



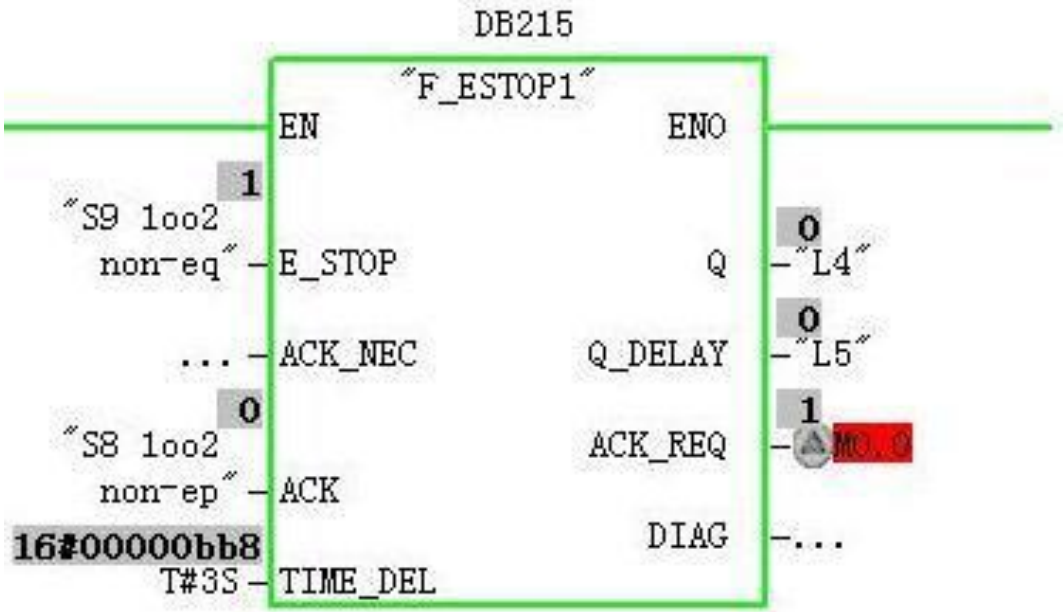
程序测试

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;



程序测试

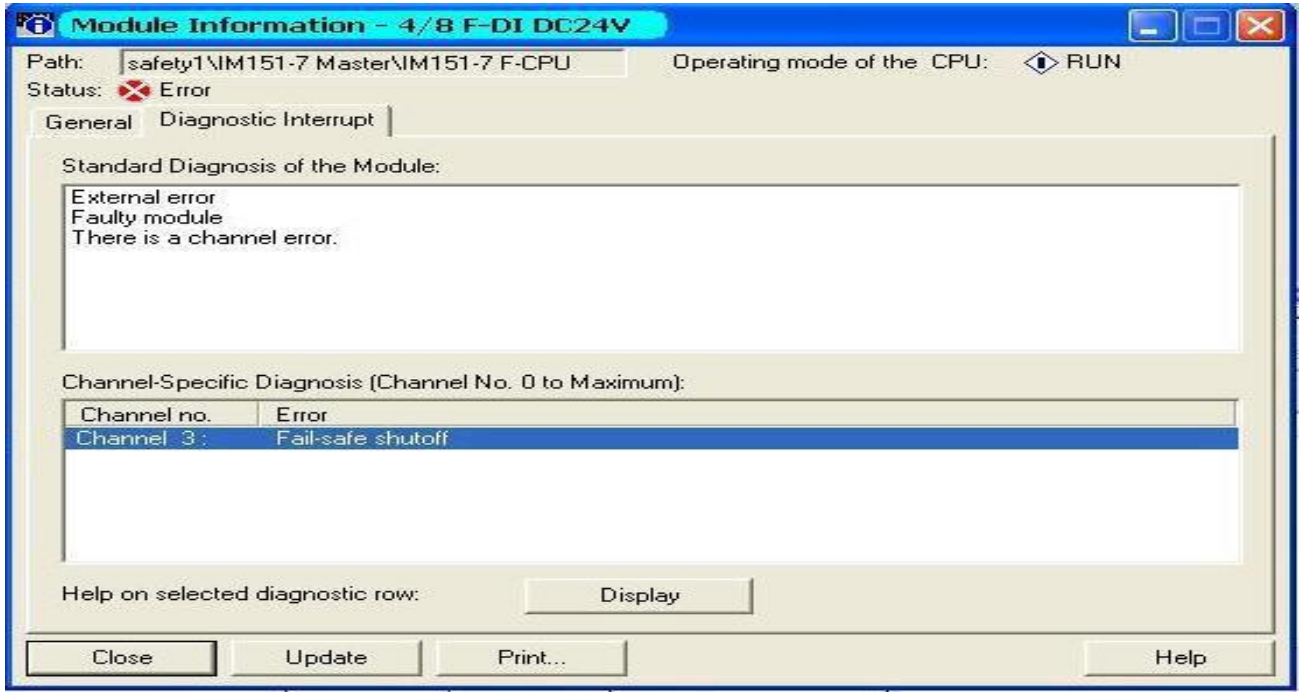
急停信号离去，E—STOP恢复为1，ACK—REQ变为1，请求应答信号变为1，等待ACK应答信号。 当ACK置为1应答后，Q、Q—DELAY才会恢复为1。



信号的钝化与去钝

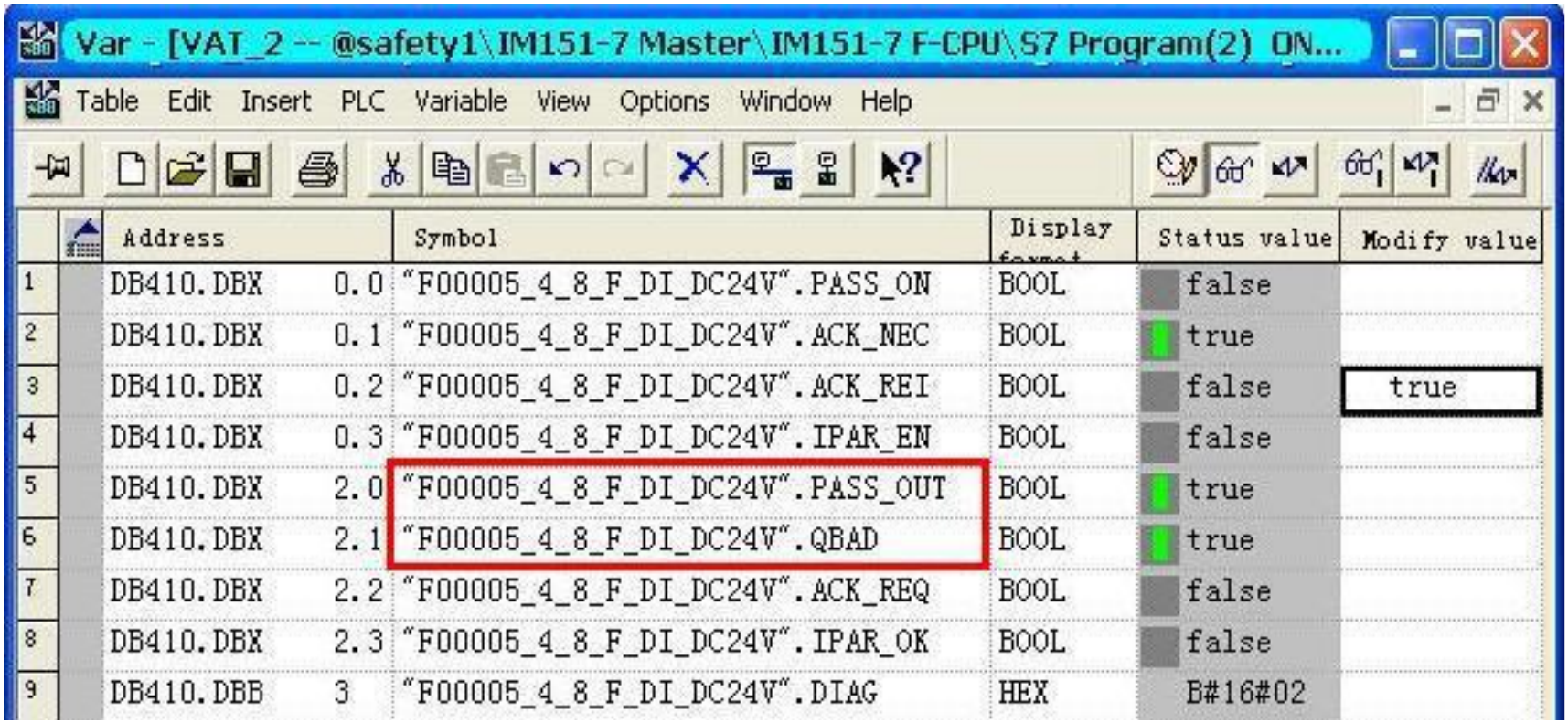
如果将DI3的接线端掉，安全模板会自动检测到外部信号错误，并使模板钝化，此时安全模板SF指示灯会变亮，DI3的状态会变为0(保持安全值输入）。安全值0通过安全程序会控制执行机构停止工作。

通过直接读取安全模板的诊断信息，可以知道错误信息。



信号的钝化与去钝

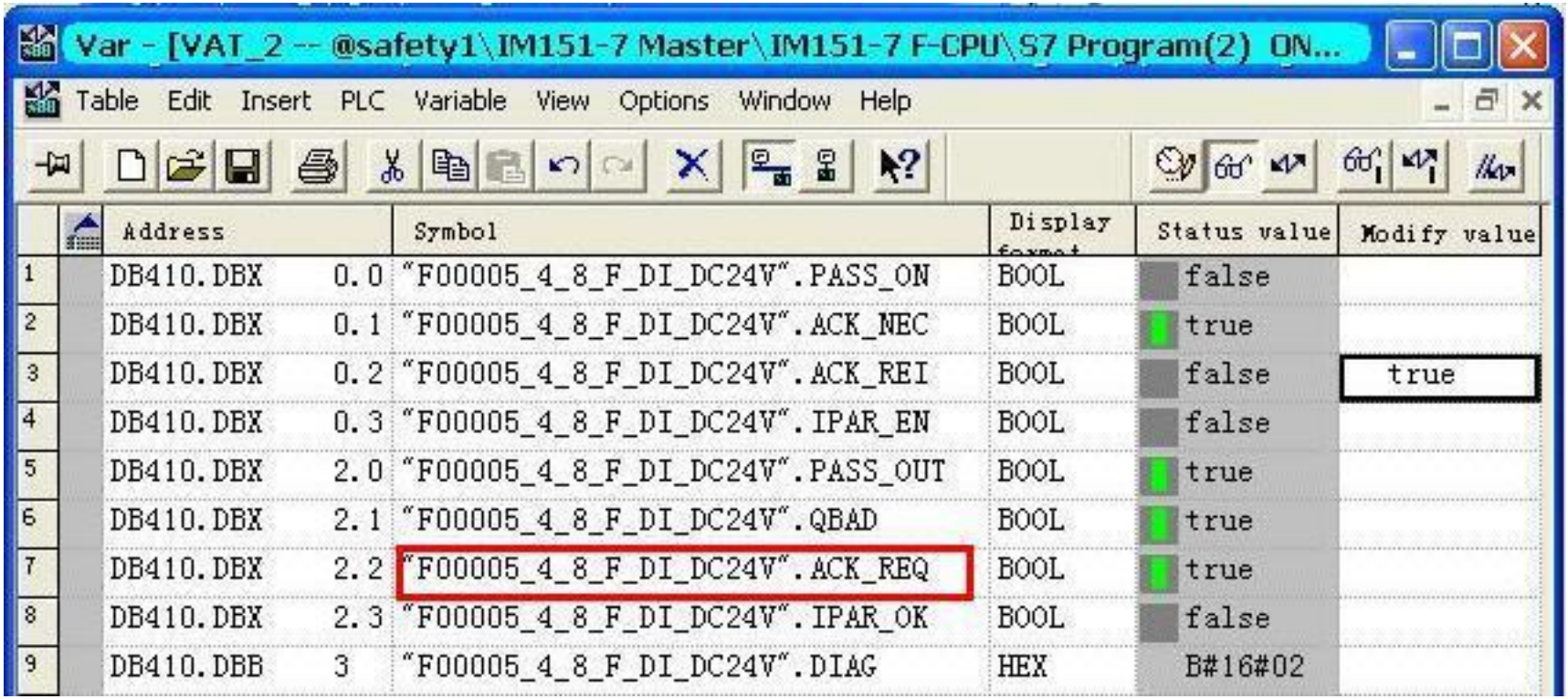
在程序中，可以通过访问该安全信号模块的F-I/O DB来读取模板的工作状态。本例中该F-I/ODB 为 DB410， 通过PASS—OUT、QBAD位的状态，可以知道模板已经钝化。



	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	

信号的钝化与去钝

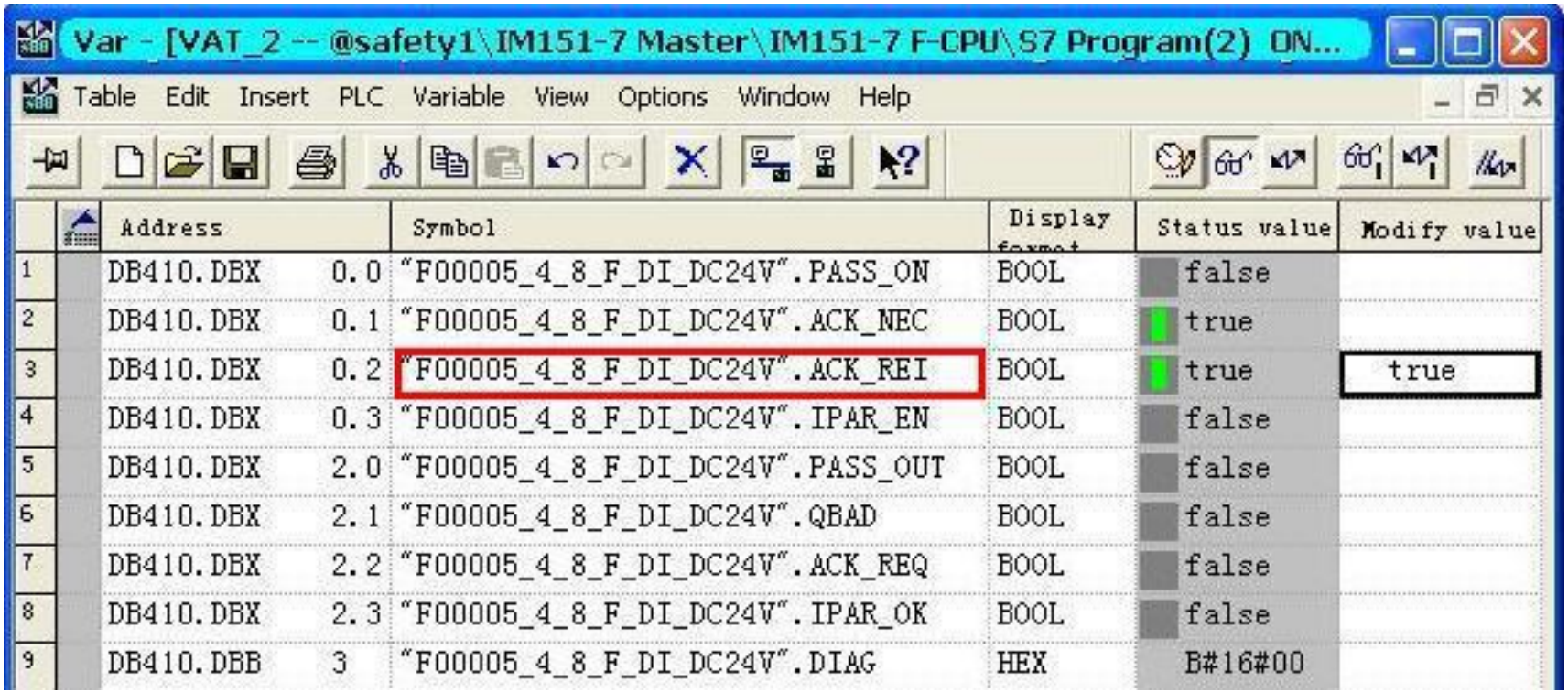
恢复DI3输入的接线后，请求应答信号ACK—REQ会变为1。



	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	

信号的钝化与去钝

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DI3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	

感谢您的聆听