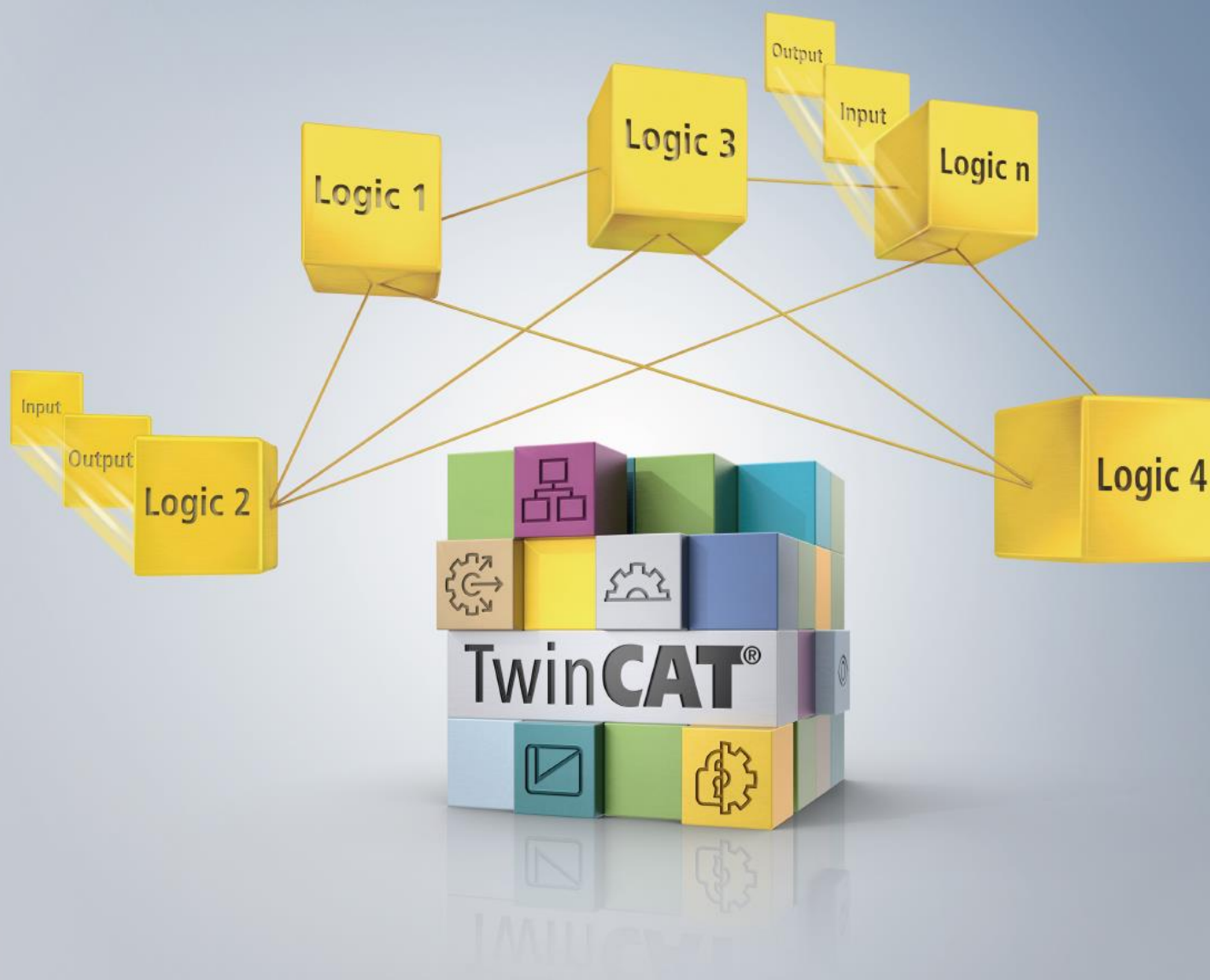


TwinSAFE 使用指南 V1.0



前言

与普通的 IO 产品相比，功能安全产品在使用、编程等上面都存在很大的差异，并且涉及到很多的标准，比如 IEC 61508、ISO 13849 等，在使用/销售安全相关产品时，除了产品本身外对于相关的安全标准也需要有一定的了解。

我们在 2005 年的时候推出基于 K-bus 的安全产品，2009 年推出了基于 EtherCAT 的安全产品，再到 2017 年推出 EJ 安全产品，截止到 2021 年 1 月安全产品全球总共销售超过 2,000,000 片；在功能方面我们也在不断的更新，陆续推出可以支持 PROFI-safe、模拟量、独立安全 PLC 等不同产品，以及带有输入或/和输出同时具备安全逻辑功能的产品，在不断拓展功能的同时也提供了性价比更高的解决方案。

该文档目前主要面向内部的销售以及技术同事，因此技术方面对于基础的使用内容没有作详细介绍，另外新推出的安全产品以及软件功能的更新都是针对于 TwinCAT 3 平台的，因此本文的产品使用基于 TwinCAT 3 平台。

另外 Motion 相关的安全产品本文档中没有描述，特别是 AX8000-0200 系列产品的 Safe Motion 功能使用相对复杂，官网上已经提供了不同功能使用的文档和视频教程，由于网络原因视频无法访问，目前放到把视频放到内网中，后续根据实际需求再更新 Motion 部分功能的使用，[\\beckhoff.com\china\ProductsManager\Automation\TwinSAFE\AX8000 Safe Wizard](http://beckhoff.com/china/ProductsManager/Automation/TwinSAFE/AX8000%20Safe%20Wizard)。

最后希望该文档能对安全产品的销售以及使用带来帮助，关于文档中没有提到的功能，欢迎大家进行反馈，在后续版本上会进行更新修正。

I/O 产品经理 陈利雄

2022 年 2 月 9 日

增加部分内容

V1.1	增加问题部分内容

目录

1.1 功能安全.....	4
1.1.1 相关名词定义.....	4
1.1.2 安全标准.....	4
1.1.3 认证信息.....	6
1.2 TwinSAFE	7
1.2.1 安全逻辑.....	7
1.2.2 安全通讯 FSoE.....	7
1.2.3 软件.....	7
1.3 安全回路搭建.....	9
1.3.1 安全等级.....	9
1.3.2 硬件回路注意事项.....	10
1.4 硬件产品以及选型.....	12
1.4.2 选型注意事项.....	14
1.4.3 安全模块容量.....	14
1.5 软件新功能.....	16
1.5.1 Multi-Download.....	16
1.5.2 Multi Setting	16
1.5.3 自定义 FB 以及库.....	17
1.5.4 Hash 表	19
1.6 使用.....	20
1.6.1 EL1918 作为安全逻辑模块使用	20
1.6.2 SC 模块使用.....	20
1.6.3 安全逻辑模块之间的通讯.....	21
1.6.4 PROFIsafe 通讯.....	22
1.6.5 TwinSAFE Loader 使用	25
1.6.6 Customizing 功能	27
1.6.7 EL1918 等在 TwinCAT 2 环境以及第三方 EtherCAT 主站下的使用	31
1.6.8 备份还原.....	32
1.7 安全工程诊断.....	35
1.7.1 在线诊断.....	35
1.7.2 通过 PLC 代码诊断	35
1.8 常见问题.....	38
1.8.1 EL1904 接入光栅等 PNP 信号以及脉冲检测介绍.....	38
1.8.2 EL2904 模块电压低报错.....	38
1.8.3 AX5000 安全选项卡 FDD9 错误	39
1.8.4 EK9300 能否带安全模块?	39
1.8.5 安全模块是否支持类似热连接的功能?	39
1.8.6 Group 处于 startup 状态或者安全通讯异常.....	40
1.8.7 安全工程版本问题.....	42
1.8.8 无法创建安全工程或者打开已有的安全工程.....	42
1.8.9 安全工程编译时报模块 CRC 错误.....	43
1.8.10 The Feedback of the inactive Channel Switch is wrong. Module 0x2 /Channel:0x1	44

1.1 功能安全

1.1.1 相关名词定义

安全：免于难以承受的风险

风险：危害发生的概率和严重程度的组合

功能安全：与 EUC 和 EUC 控制系统有关的整体安全的组成部分，它取决于 E/E/PE 安全相关系统，其它技术安全相关系统和外部风险降低设施功能的正确行使。（IEC 61508）

EUC：受控设备

E/E/PE：电气/电子/可编程电子

DC：诊断覆盖率

MTTF_D：平均无危险故障时间

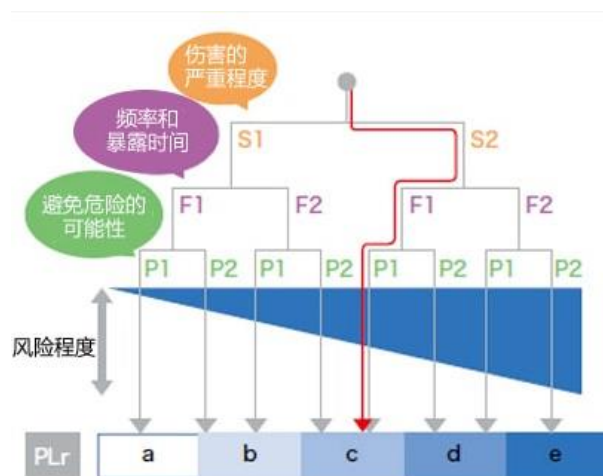
PFH_D：每小时危险失效概率

1.1.2 安全标准

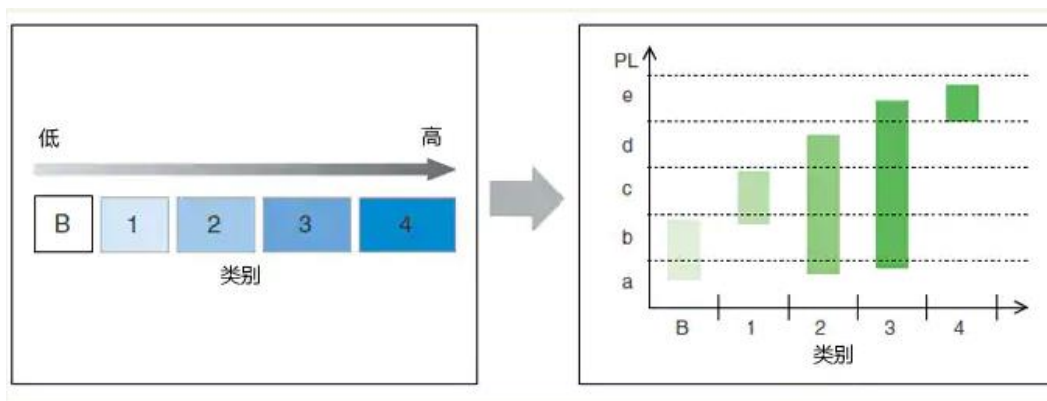
ISO 13849(PL)/EN954-1(CAT)

EN954-1 于 2011 年底退出使用，继任标准为 ISO13849；EN954-1 定义了安全系统的 CAT（类别），ISO 13849 定义了安全系统的 PL（性能等级）

对于一个系统需要达到的 PL 等级可以通过以下方式评估。

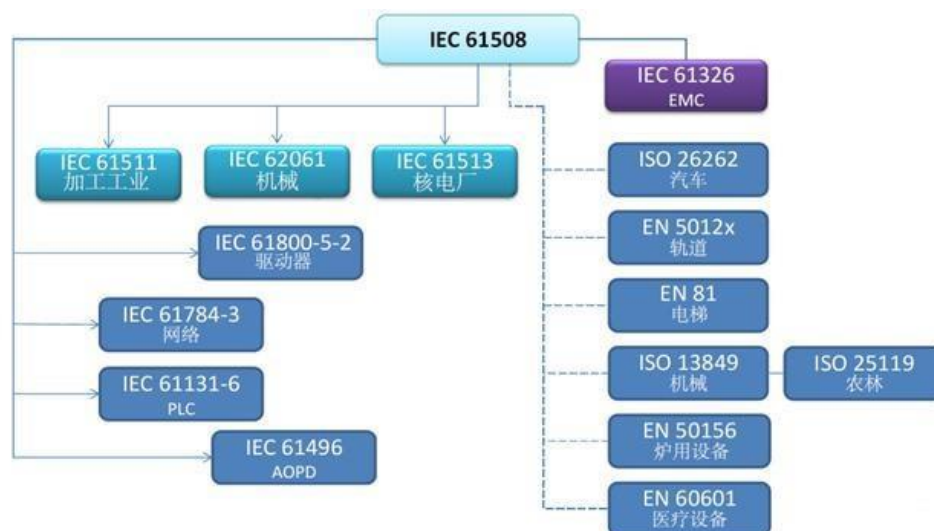


CAT 和 PL 两者的关系如下



IEC 61508 (SIL)

IEC61508 主要针对采用电气电子可编程电子等技术实现的功能安全系统，定义了 SIL（安全完整性等级）。IEC62061 主要针对机器安全应用中，采用电气电子可编程电子等技术实现的功能安全系统，机器的 SIL 的级别是在 IEC62061 中提出的，它只有三级，SIL1、2、3，其计算方法和思路来自于 IEC61508。



PL 与 SIL 对应关系如下：

每小时危险失效概	PL	SIL (IEC 61508-1, 高要求或连续操作模式)	每小时危险失效概率 (高要求或连续操作模式)
$\geq 10^{-5}$ 且 $< 10^{-4}$	a	无对应关系	$\geq 10^{-5}$ 且 $< 10^{-5}$
$\geq 3 \times 10^{-6}$ 且 $< 10^{-5}$	b	1	$\geq 10^{-6}$ 且 $< 10^{-5}$
$\geq 10^{-6}$ 且 $< 3 \times 10^{-6}$	c	1	$\geq 10^{-6}$ 且 $< 10^{-5}$
$\geq 10^{-7}$ 且 $< 10^{-6}$	d	2	$\geq 10^{-7}$ 且 $< 10^{-6}$
$\geq 10^{-8}$ 且 $< 10^{-7}$	e	3	$\geq 10^{-8}$ 且 $< 10^{-7}$

IEC61800-5-2:

IEC61800-5-2 定义了调速电气传动系统安全部分的功能要求，对应国标为 GBT 12668.502，通过定义可以帮助我们更好地理解文档中安全功能的实时。

以下截取了 GBT 12668.502-2013 中部分功能的定义：

PDR (SR) 电气传动系统 (安全相关)

4.2.2.2 安全转矩取消 (STO)

能够引起转动(或运动,如果是直线电机)的电源不被应用到电动机。**PDR(SR)**将不对产生扭矩(或力,如果是直线电机)的电动机提供能量。

4.2.2.3 安全停止 1 (SS1)

PDR (SR) 应满足以下条件之一:

- a) 在设定的限值内,启动并控制电动机减速使电动机停止,当电动机速度低于规定的限值时启动 **STO** 功能;或
- b) 在设定限值内,启动并监视电动机减速使电动机停止,当电动机速度低于规定的限值时启动 **STO** 功能;或
- c) 在应用规定的时间延时后,启动电动机减速并停止 **STO** 功能。

4.2.3.4 安全极限速度 (SLS)

SLS 功能防止电动机超过规定的速度限值。

1.1.3 认证信息

Marks	Description
TÜV SÜD Z10	A Z10 certificate is issued for the use of the product in the European Union and contains the relevant DIN, EN or IEC standards for the product (e.g. EN ISO 13849-1:2015). The corresponding standards are listed in the table.
Declaration of conformity	A TÜV SÜD conformity declaration typically has no expiration date and confirms a specific property of a product at the time of testing.
TÜV SÜD U8	A U8 certificate is issued for NRTL, NFPA, CSA certification and includes standards relevant to the North American market. The table lists the relevant standards.
M6A	An M6A certificate is the EC-Type Examination Certificate for the corresponding TwinSAFE product.
EC	Beckhoff Automation GmbH & Co. KG issues the EC Declaration of Conformity on the basis of the corresponding M6A certificate.
cULus	The entry cULus refers to a certification according to UL 508 / UL 61010-1 / UL 61010-2-201 / UL 508C / UL 61800-5-1.
RoHS	The EC declaration of conformity listed the EN 50581:2012. Thus the RoHS marking <i>RoHS 2011/65/EU</i> may be attached to the product. This mark is not listed separately in the table.
CE	On the basis of the EC declaration of conformity, a CE mark may be affixed to the product. This mark is not listed separately in the table.
EAC	For the Russian market or the countries Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan, the EAC logo must be affixed to the product. For manufacturers outside Russia or the EAWU (Eurasian Economic Union), an authorized representative in the EAWU is required, who is responsible for the marking.
CCC	<i>China Compulsory Certification</i> is a certification for the Chinese market.
KC	KC (Korea Certification) is a certification for the South Korean market.
RCM	<i>Regulatory Compliance Mark</i> is used for the Australian market and is focused on electrical safety and electromagnetic compatibility. (Australian Standard AS/NZS 4417 - <i>Regulatory compliance mark for electrical and electronic equipment</i> supplemented by Amendment 2 of January 2016)

https://www.beckhoff.com/media/downloads/downloads/twinsafe_certificates-2.pdf

安全相关产品的认证信息汇总可以如上地址中获取,包括功能安全的认证以及其它认证。倍福安全产品最高可以到的安全等级为 PL e 以及 SIL 3。

另外对于 SC 产品,不提供功能安全的认证,SC 模块与普通模块的要区别是与安全逻辑模块之间可以进行基于 FSoE 的通讯,FSoE 通讯具有功能安全认证的。

1.2 TwinSAFE

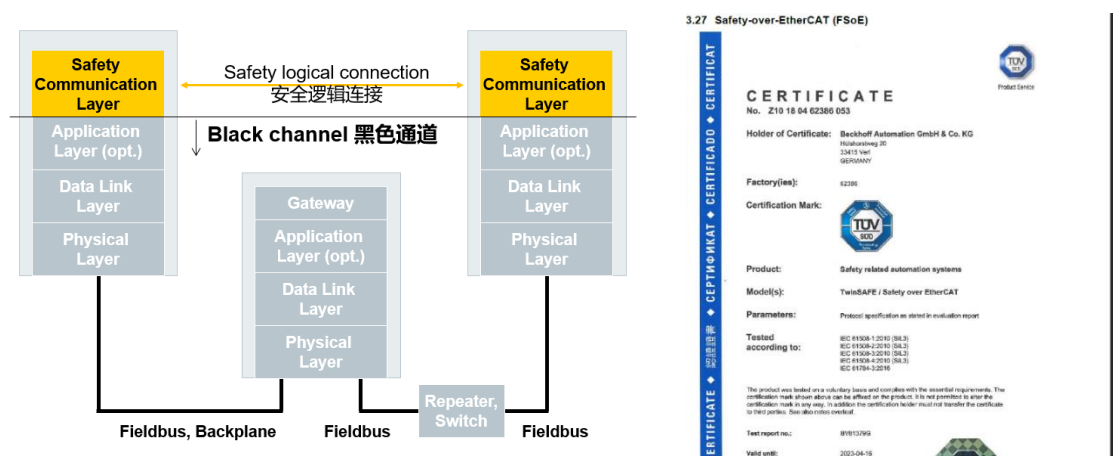
1.2.1安全逻辑

区别于其它 TwinCAT 软件功能，安全程序运行于安全逻辑模块内，可以通过 TwinCAT 或 TwinSAFE Loader 等软件下载到逻辑模块中，安全逻辑模块通过映射实现与其它安全模块以及 PLC 等的交互。

在 TwinCAT 中，集成安全软件环境已经自动帮我们实现了安全模块之间的数据映射；通过手动映射的方式，也可以实现第三方 EtherCAT 主站带我们的安全模块或者 TwinCAT2 平台运行 EL6910、EL1918 等安全产品，修改安全程序以及在线监视安全程序都需要在 TwinCAT 3 平台实现。

1.2.2安全通讯 FSoE

在 EtherCAT 总线中，安全模块之间通过 FSoE (FailSafe over EtherCAT) 实现数据交互，基于 IEC61784-3 功能安全通讯模型，使用黑色通道原理方式实现，在应用层上面有一个安全层实现安全数据连接。FSoE 规范对于通讯层、接口、传输速度、安全数据长度等没有限制，可以通过非安全的网关，现场总线或者背板总线，甚至无线都可以进行路由。并且 FSoE 提供了最高 SIL3 的安全认证。



1.2.3软件

TwinCAT 2 以及 TwinCAT 3 均可以支持安全产品的使用，其中 TwinCAT 2 支持进行安全逻辑编程下载的逻辑模块包括 KL6904、EL6900、EL6930，其它的安全逻辑产品的程序编写需要在 TwinCAT 3 环境下进行。

TwinCAT 3 中的 Safety Editor 软件 TE9000 可以单独进行下载更新，可以在如下链接中

找到 [TE9000 | TwinCAT 3 Safety Editor | 倍福 中国 \(beckhoff.com.cn\)](#)，需要 TwinCAT 3 版本 4024.11 以上支持。另外，为了避免不同版本 TwinCAT 软件导致的安全工程兼容性问题，建议使用同一版本的 TwinCAT 进行安全项目开发管理。

除了集成于 TwinCAT 的安全软件之外，我们还提供了 TwinSAFE Loader 和 TwinSAFE User 软件。这两个软件支持在 Windows 或者 Linux 平台的电脑上运行，无需安装 TwinCAT 环境，通过 ADS Over EtherCAT (AoE) 或者 EtherCAT Mailbox Gateway 以命令行的方式与安全逻辑模块进行交互；使用 AoE 方式时，软件本身提供了一个 ADS 客户端，但是没有添加路由部分，因此需要手动进行添加路由的操作；使用 Mailbox Gateway，需要在组态中设置 mailbox 部分。

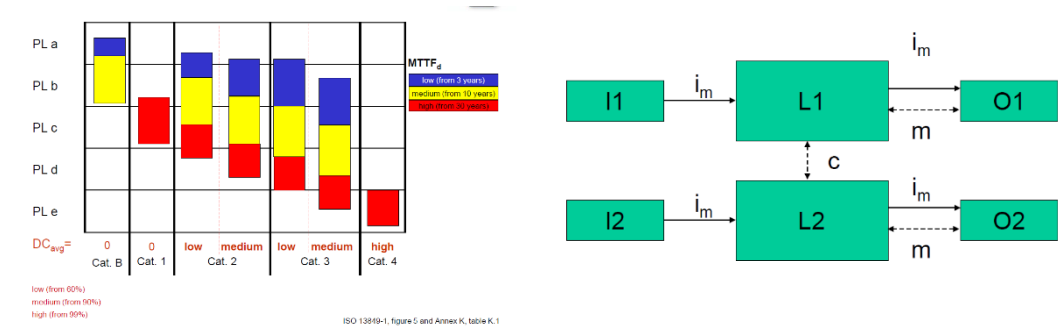
TwinSAFE Loader 可以用于安全程序的下载、删除，安全工程多个 Group 的管理；对于批量项目可以通过该软件进行安全逻辑下载，从而减少重复性的工作。

TwinSAFE User 用于安全工程的用户管理，包括创建/删除用户，用户权限管理等。

1.3 安全回路搭建

1.3.1安全等级

我们在官网中提供了 Application guide 文档，里面提供了回路的搭建以及安全系统的安全等级计算。



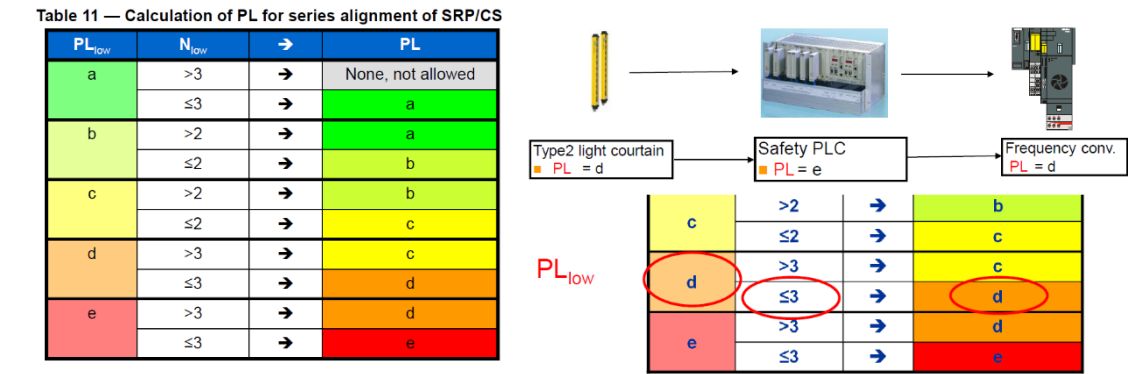
根据 13849-1 标准中的描述，系统达到 PL e 等级需要 Cat3 或者 Cat4；Cat3 和 Cat4 的架构如下，输入输入以及逻辑需要双路冗余，两者主要的区别在于诊断覆盖率。

即实现 PL e 等级至少双路的安全输入和输出。

对于安全输入/输出模块，当关闭脉冲检测、电流检测等功能会导致诊断覆盖率下降，进而可能导致整个系统的安全等级降低。

另外对于整个安全系统的安全等级的计算是一件比较复杂的工作，这里面介绍一种较为简单的计算方式，统计系统中安全等级最低的组件的数量来判断。如下右图中各组件最低安全级别为 PL d，并且数量为 2，故整个系统可以达到 PL d。

这个方式可以计算当前系统至少可以达到的安全等级，实际系统可能可以达到更高的安全等级；比如一个系统中最低的安全等级为 e，并且大于三个，依据表格可以达到 PL d，是否能给达到 PL e 则需要通过计算整个系统的 DC、MTTF_D 来判断。



1.3.2 硬件回路注意事项

1) 供电

对于安全模块而言,只有在模块运行范围内的电压才能确保模块的正常工作;以 EL2904 为例,输出电压需要在 24V(-10%/+20%)范围内,否则模块会报错,并且此时需要对模块的 E-bus 重新断上电恢复。

对于 E-bus 以及 IO 供电,建议使用分别使用单独的开关电源。上电顺序 IO 供电需要先于 E-bus。如果现场存在电源电压波动等可能时,可以使用开关电源缓冲模块。

2) 散热

以下介绍对于关于模块散热的一些布局

EtherCAT 耦合器和供电模块 EL9410 等:

这些模块的发热主要由后面所带的模块的电流消耗所决定

EL69X0:

由于内部时钟和安全逻辑功耗,安全逻辑模块会有较大的发热量

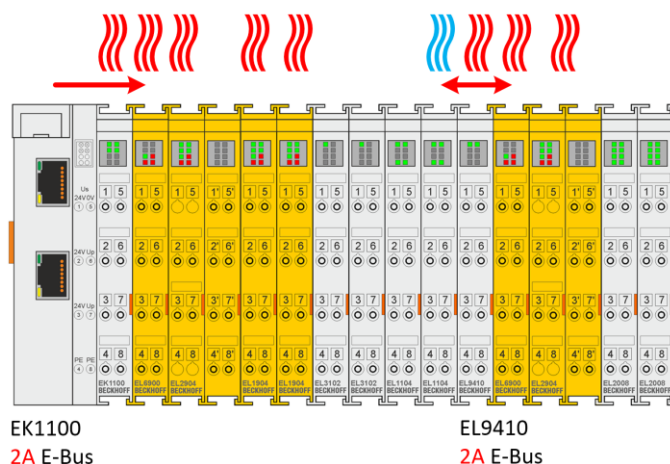
EL2904:

由于对外部执行器件可能需要提供较大的输出电流,模块可能会有较大的发热量

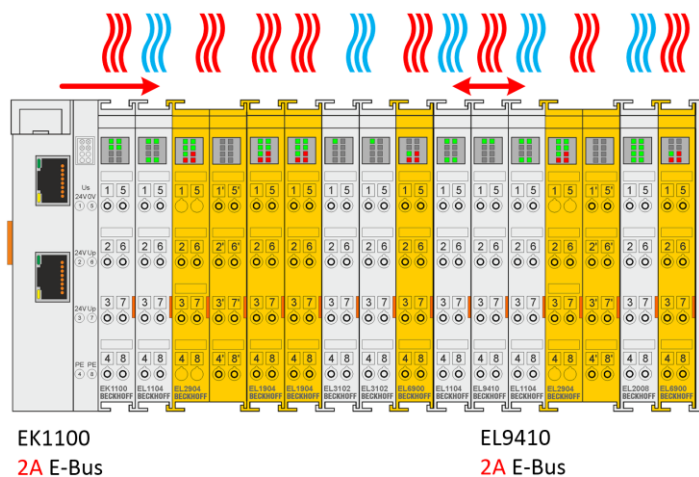
EL1904:

虽然外部时钟信号和安全输入功耗较低,但是 EL1904 模块依旧有很大的发热

下图是一个不合理的散热排布,安全模块和供电模块相邻,进一步导致安全模块内部温度升高,进而可能导致温度超过最大允许范围。

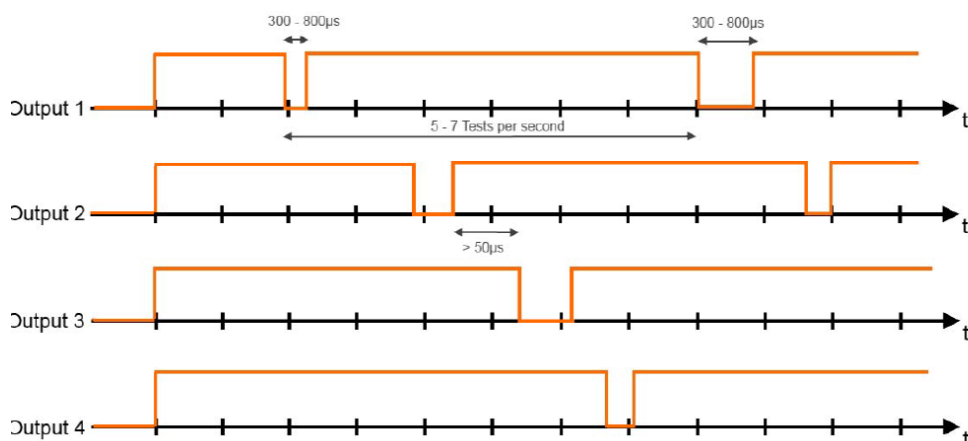


下图为比较合理的模块排布,在安全模块和供电模块之间增加了电流消耗较少的模块来避免安全模块温度过高。



3) 外部器件选型

无论是输入或者输出信号，模块都会生产测试脉冲信号（24V—0V—24V），用于检测模块通道之间是否发生短路，比如对于 EL2904 模块，脉冲典型持续时间在 300 μ s 到 800 μ s 并且 1 秒钟触发 5~7 次。



对于输出模块，选择外部执行器件时，比如继电器等，需要确保检测脉冲不会导致外部器件动作；另外输出通道默认还提供了电流检测功能，需要确保外部电流在通道检测范围内。

4) 通讯

安全模块之间的数据交互依赖于 EtherCAT 数据帧的传输，通讯的故障可能会导致安全程序报错。因此恰当的软件设置以及稳定的电气环境是安全工程正常运行的基础。

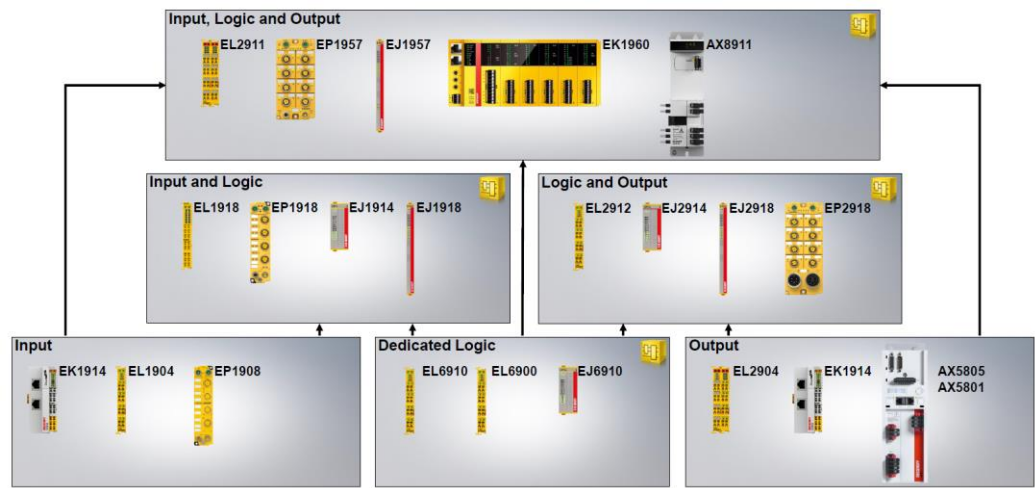
1. 确保使用符合 EtherCAT 规范的网线、以及可靠的连接避免通讯中断、丢帧、CRC 错误等；
2. 恰当的软件设置，合理设置同步单元，确保没有 Task 超时以及个别模块状态异常切换等不会影响到安全模块的正常运行；
3. 良好的电柜 EMC 环境。

5) 其它

安全模块与设备之间的电缆与动力电缆应使用不同的线缆槽并且中间应该保持一定的距离。当无法避免使用同一线槽时，需考虑关闭脉冲检测以及电流检测等功能。关闭检测功能会导致计算系统安全等级时诊断覆盖率的降低。

1.4 硬件产品以及选型

区别于普通的产品，安全模块外观颜色为黄色，另外具备其它的一些特点：
产品需要取得功能安全标准的认证；
安全 PLC 采用冗余 CPU 工作方式，内部数据并行处理和相互校验；
数据传输报文采用 CRC 码校验，每两个字节的的安全数据会被两个字节的 CRC 校验；
硬件内部具有自我诊断功能，芯片的电压诊断、内部温度诊断等；
具有对外设备的诊断，脉冲诊断、电流检测等。



自新一代的 EL6910 开始，新推出的安全模块在带有安全输入和/或输出的同时也集成了安全逻辑，可以提供性价比更高、更加适合的安全解决方案；以 EL1918 为例，模块本身提供了 8 个安全输入+安全逻辑，同时也可以作为单纯的安全输入模块使用，并且作为安全逻辑模块时，可以支持模拟量的功能块。

注：使用 EL1918 等新产品作为安全 I/O 模块时，不能使用 EL6900、EL6930 作为安全逻辑模块；EL6900 可以带的安全 IO 包 EK1914、EL1904、EP1908、EL2904、AX5801/5/6

1) 独立安全 PLC

EP1957 以及 EK1960 可以作为独立的安全 PLC 使用，满足客户功能安全系统独立于通用控制系统的需要；作为独立安全 PLC 使用时需要通过 TwinCAT 进行安全程序的编写下载，此时无法扩展其它 IO。

另外，这两款产品也可以运行于 EtherCAT 总线中，此时使用方式和其它安全逻辑模块一致。

2) SC（Single Channel）模块

我们提供了模拟量、编码器、通讯等相关的产品，可以与安全逻辑模块进行的数据交互。SC 模块与安全逻辑模块的 FS_oE 通讯具有安全认证，SC 模块本身不提供功能安全相关认证。

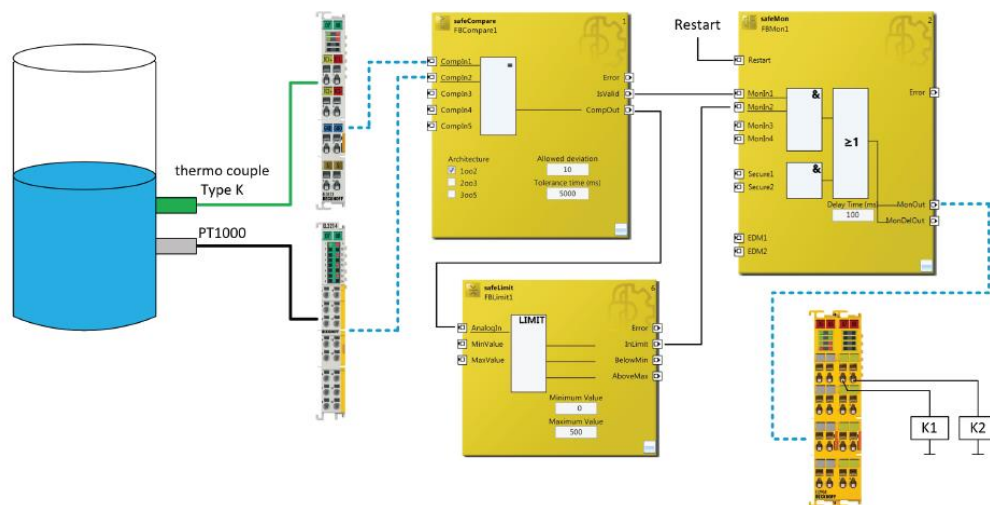
下表列举了部分的 SC 模块，我们的 IP20、EJ 以及 IP67 部分产品均提供了 SC 集成。

模拟量输入	
EL3124-0090	4...20 mA 模拟电流 16 bit, TwinSAFE SC

EL3174-0090	-10/0...+10 V, -20/0/+4...+20 mA, 16 bit, TwinSAFE SC
EL3214-0090	PT100 热电阻, 3 wire, TwinSAFE SC
EL3314-0090	TC 热电偶, TwinSAFE SC
EL3356-0090	电阻桥称重, 24bit, TwinSAFE SC
位置检测	
EL5021-0090	SinCos 编码器, 1 Vpp, TwinSAFE SC
EL5101-0090	增量型编码器, TwinSAFE SC
EL5001-0090	SSI 编码器, TwinSAFE SC
EL5151-0090	差分编码器, 32bit, TwinSAFE SC
通讯	
EL6224-0090	IO-Link terminal, TwinSAFE SC
IP67 高防护等级	
EP3174-0092	± 10 V, 0/4...20 mA, diff., 16 bit, TwinSAFE SC

基于此我们可以实现更多的安全功能，比如温度监控等，如下图所示：

该例子中使用了两路输入，一路为普通的热电偶模块，一路为 SC 的热电阻模块；使用了不同的方式采集温度信号，避免 CCF（共因失效）。



3) Motion 相关产品

标准驱动以及紧凑型驱动模块均可提供了安全集成。

按照功能可以分为如下两类：

1. STO/SS1 功能

- AX5000 的 AX5801 选型卡，STO 通过硬件信号触发
- AX8xxx-0100 系列，集成安全逻辑功能，出厂时内置了 STO 的安全程序，可以通过 FSoE 或者自带的硬件输入信号触发；
- EL72xx-9014/EP7211-9034 等，STO 通过硬件信号触发。

2. Safe Motion

除了 STO/SS1 之外可以提供更多的安全限制功能，包括 SS2、SSR、SLI、SLS、SCA、SLP、SBC、SMA、SAR、SSM、SLT、SMS、SDIn、SDIp。

主要产品为 AX5000 的 AX5805/6 安全选项卡以及 AX8000-0200 系列。

AMP、AMI、ELM 系列驱动产品也可以提供安全功能的集成。

1.4.2 选型注意事项

1. 支持 TWINCAT 2 环境下进行编程的安全逻辑模块：EL6900、EL6930、KL6904；
2. EL6900、EL6930 作为安全逻辑模块时，无法选择 EL1918 等有安全逻辑功能的模块作为 IO；
3. TwinCAT 3 环境下推荐使用 EL6910/EL1918 作为安全逻辑模块，除了数字量安全模块外还可以支持 SC 模块，大部分情况下可以使用 EL1918 实现所需的安全功能；
4. 使用 PROFIsafe 时，推荐使用 EL6910，同时支持 Master 和 Slave，EL6930 只支持 slave 并且只能有一个连接，PROFIsafe 需要配合 Profibus/Net 接口使用，如 EL6631；
5. 使用 AX5805/5806 实现 SafeMotion 功能时，注意电机限制；使用异步电机以及直线电机只能使用 STO 功能，此时如果需要通过 SLS 等功能可以通过 SC 编码器模块获取转速信号通过安全逻辑进行判断比较等的方式实现，具体可参考 ApplicationGuide 里面的例子；
6. AX8000 驱动的安全是一体的，在驱动选型的时候确定，选择 AX8000-0200 实现 SafeMotion 功能时，需要使用带安全功能编码器的电机；

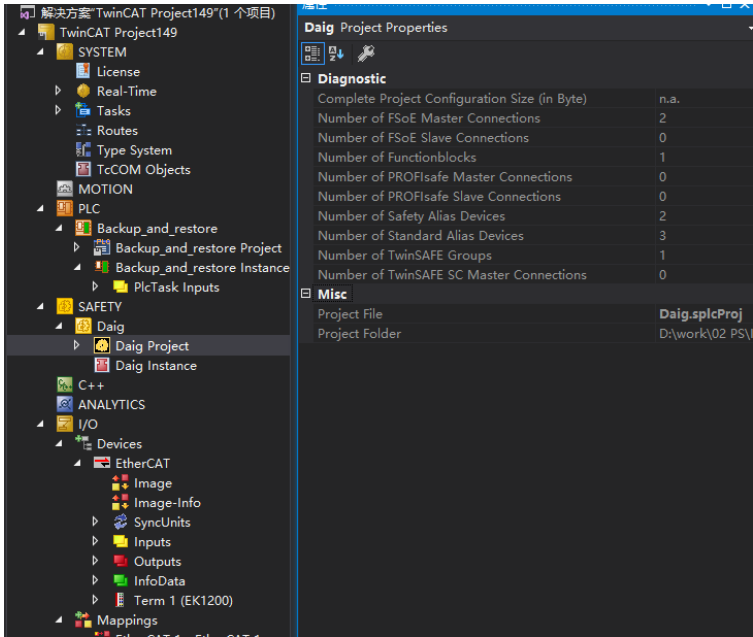
注：我们新的安全产品在集成了 IO 的同时均带有安全逻辑功能，在实际配置中可以考虑使用 EL1918 作为安全逻辑模块。

1.4.3 安全模块容量

对于不同的安全逻辑模块，允许的连接、功能块、Group、用户等数量存在差异，不同模块的限制可以在对应的说明文档中找到，以 EL1918 为例

Process image size	max. 1486 byte per data direction (maximum memory size 0x1E00 for 3 buffers, ie with the same size of input and output process data, a maximum size of 1280 bytes per data direction is possible. Only straight start addresses are possible, so fill bytes must be taken into account)
TwinSAFE connections	128 max. (up to 255 CRCs in total; 1 CRC is required for a TwinSAFE connection with 1 or 2 byte safe data.)
Safe data per TwinSAFE connection	maximum 126 byte (telegram length 255 byte)
TwinSAFE blocks	maximum 512 (when using ESTOP function blocks with complete input and output mapping, other function blocks can lead to a smaller maximum number)
TwinSAFE groups	128 max.
TwinSAFE user	40 max.
Standard PLC inputs	dynamic (memory-dependent), max. 1484 byte
Standard PLC outputs	dynamic (memory-dependent), max. 1484 byte

实际的连接数量可以在安全工程的属性中找到当前工程使用的情况，其中 connections 为 FSoE master/slave 和 PROFIsafe master/slave connections 的总和。

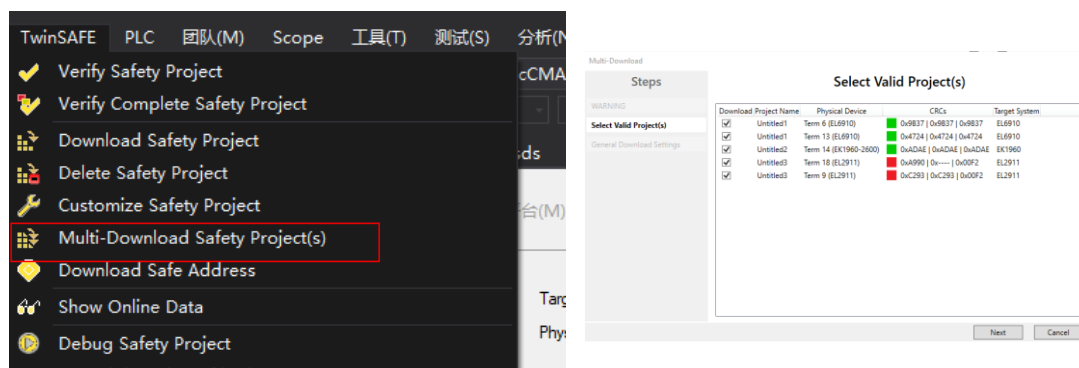


如果程序容量不够用，可以选择容量更大的安全逻辑模块，比如 EL6910，或者将安全工程分成多个安全项目来实现。

1.5 软件新功能

1.5.1 Multi-Download

实现一个 TwinCAT 项目内多个安全工程的同时下载

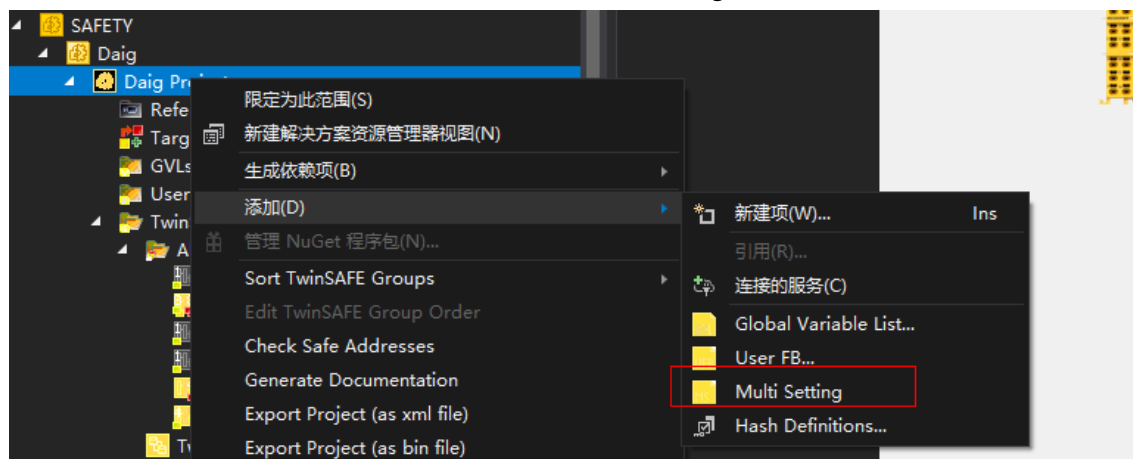


下载窗口可以看到当前哪些工程和安全逻辑模块中运行的工程不一致（红色显示），不需要输入安全逻辑模块序列号，过程和单个安全项目的下载基本一致。

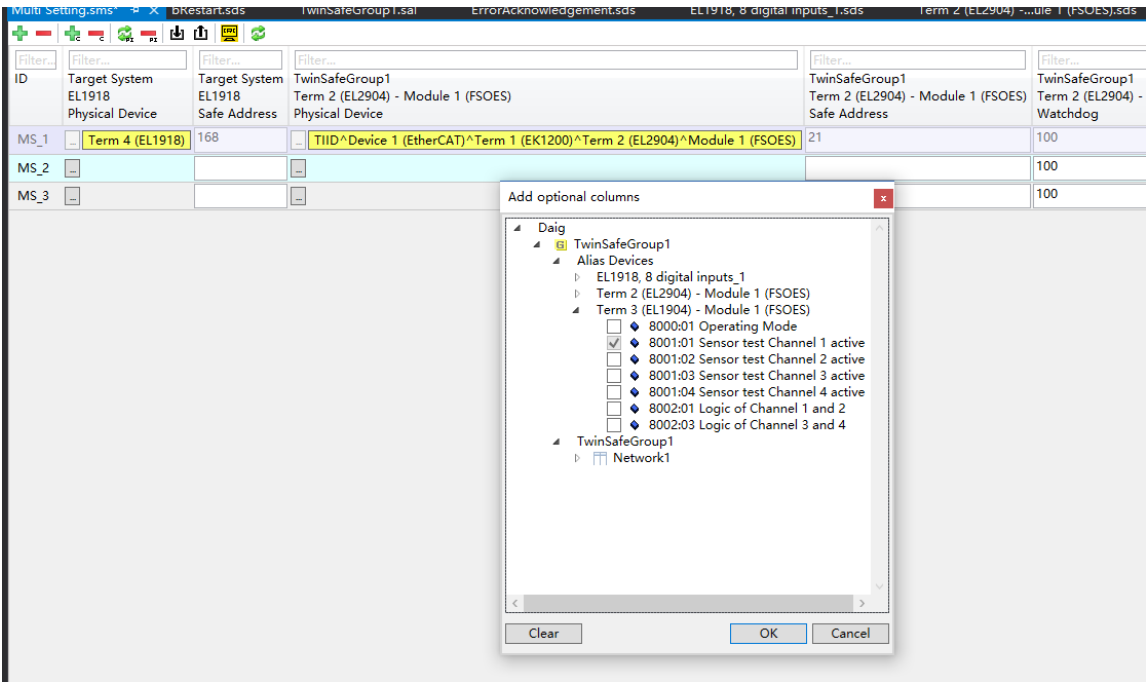
1.5.2 Multi Setting

应用场景：AX8000-0200 驱动自带安全逻辑功能，Safe Motion 功能需要在驱动内并且相对比较复杂，以往的话系统内如果有多个驱动，那么需要分别实现每个驱动的安全逻辑，因此推出了 Multi Setting 功能，实现安全工程的简单复制。

创建一个安全工程后，可以在项目处右键添加 Multi Setting。



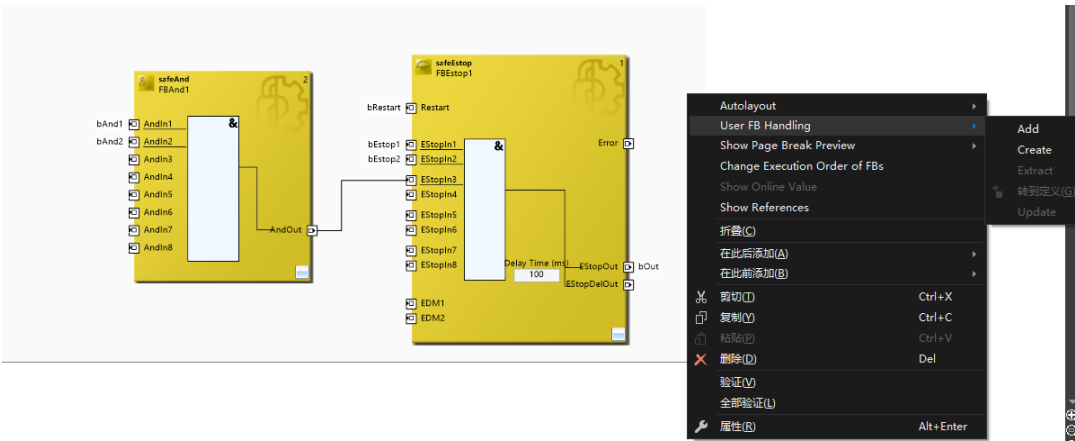
在 MultiSetting 中可以创建副本，实现与 Connection（安全模块，FSOE、PROFIsafe）的关联，以及模块和程序中各FB的个性化参数设置，通过这种方式只需要编写一次安全程序，其它项目通过配置的方式实现。



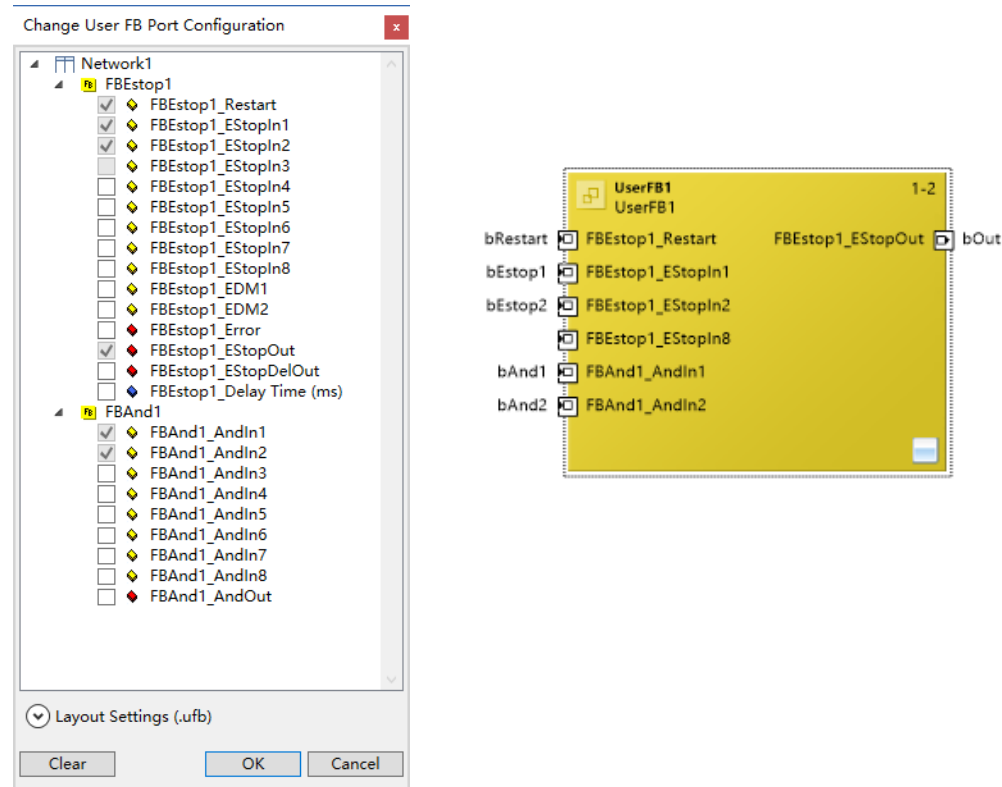
1.5.3自定义 FB 以及库

对于常用的功能可以进行封装以方便同一工程以及不同的工程之间使用，降低重复的代码工作。

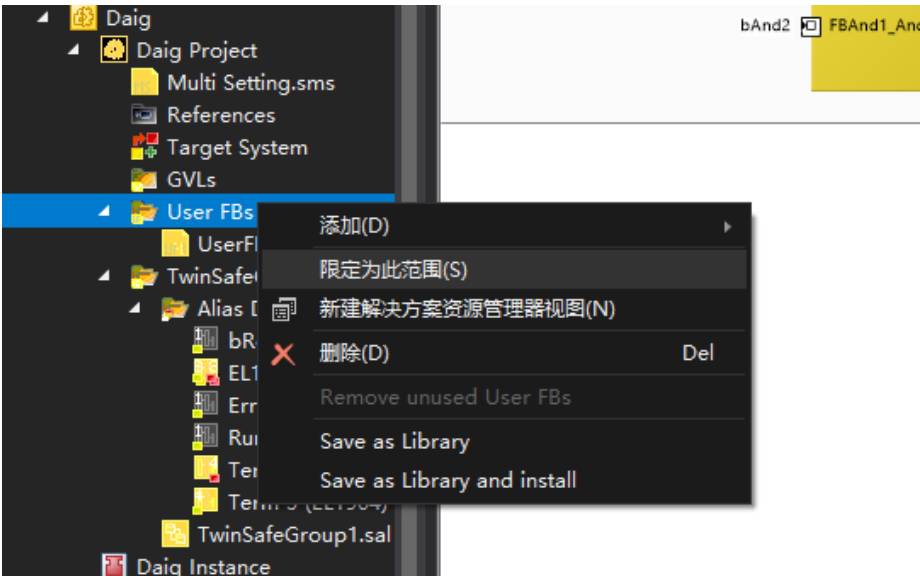
在需要封装的工程 Network 空白处右键创建自定义功能块



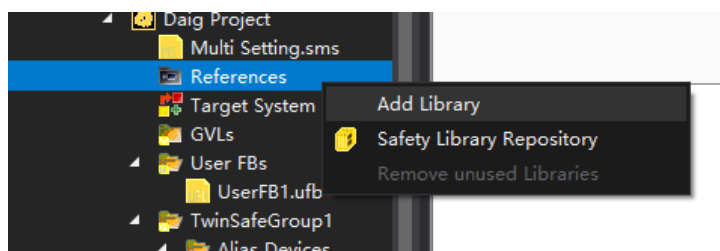
其中已经有关联的变量会自动选择，其它需要的变量另外进行勾选，如下右图为创建好的自定义 FB，此时可以通过工具箱找到自定义的 FB，自定义 FB 不包含 Diag 以及 State 信息。



创建自定义 FB 后安全工程内会自动创建 User FBs 文件夹，可以右键创建自定义库，以方便其它 TwinCAT 工程使用。



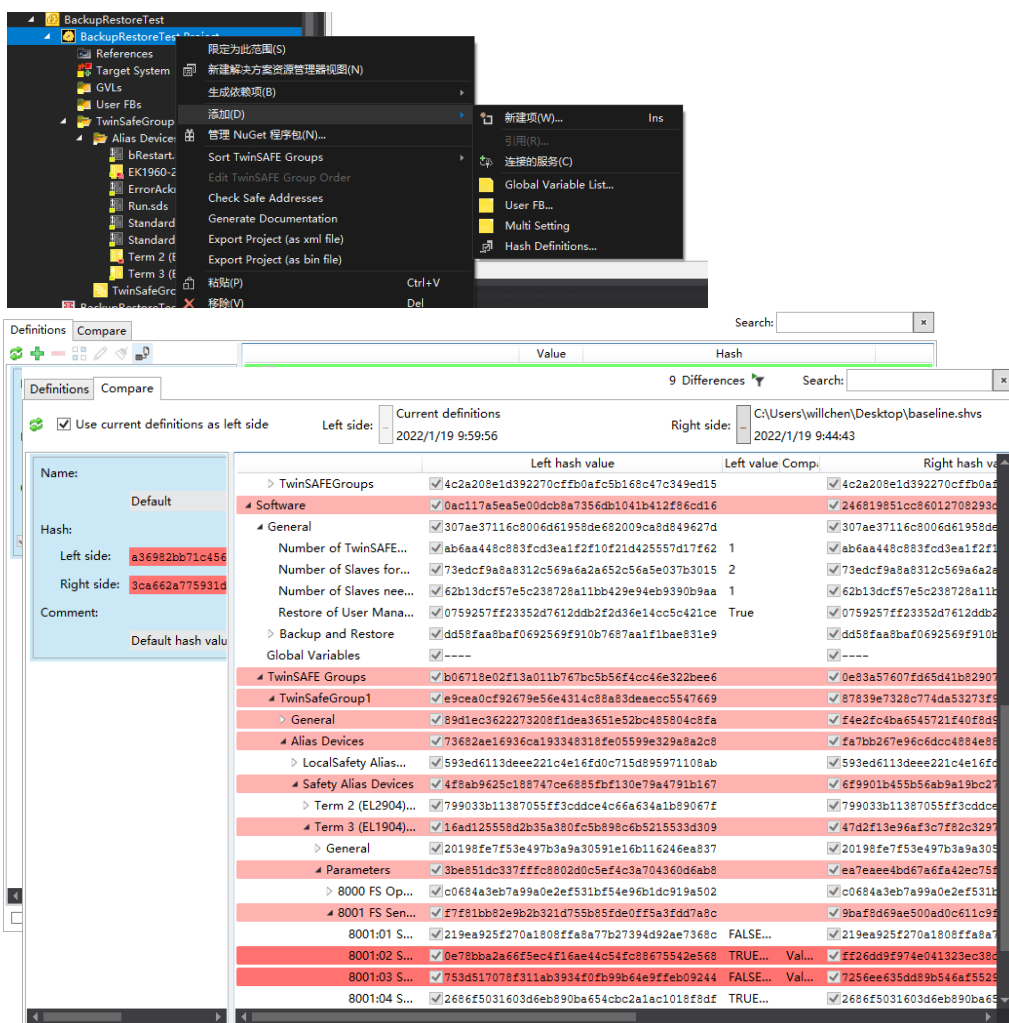
自定义库添加，References 右键添加自定义库。



1.5.4 Hash 表

哈希表可以用于追溯安全项目的修改记录以及快速比较不同版本的安全项目之间的差异。

完成安全工程后可以在项目处右键创建哈希表，里面包含了所有安全工程相关的设置（模块参数设置、安全地址、映射、程序等），并且可以根据当前配置创建一个基准版本用于比较或者每次修改后创建一个当前版本的哈希表用于记录设置信息。



当安全项目有变动时，可以通过比较哈希表来快速定位修改项以及修改前后的值。

1.6 使用

以下主要介绍 TwinCAT 3 环境下部分功能的使用

1.6.1 EL1918 作为安全逻辑模块使用

NOTE

Project development

TwinCAT 3.1 Build 4022.25 or newer is required to use the internal logic functions. If the EL1918 is used as TwinSAFE slave with the default project, at least an EL6910, EK1960 or newer logic component is required as TwinSAFE master.

首先作为安全逻辑模块使用时，对于 TwinCAT 的版本有要求。

使用时和专用的安全逻辑模块 EL6900、EL6910 等有一些区别

The screenshot shows the TwinCAT 3.1 interface. On the left, the 'Project Tree' displays a project named 'TwinCAT Project147' with a 'SAFETY' folder containing 'Untitled1'. Under 'Untitled1', there is a 'TwinSafeGroup1' folder, which contains 'Alias Devices'. The 'Alias Devices' folder is expanded, showing 'EL1918, 8 digital inputs, 1.sds' and 'ErrorAcknowledgement.sds'. On the right, the 'Configuration' window for the 'EL1918' module is open. It has tabs for 'Linking', 'Connection', 'Safety Parameters', 'Process Image', 'Internal Safety Parameters', and 'Interfacing'. The 'Linking' tab is active, showing fields for 'FSOE Address' (0), 'External Safe Address', 'Linking Mode' (Automatic), 'Physical Device' (Automatic), 'Dip Switch' (Local), 'Input Full Name' (not available), 'Linked to' (not available), 'Output Full Name' (not available), 'Linked to' (not available), and 'Name' (not available).

在 Target System 选择 EL1918 作为安全逻辑后，需要在 Alias Devices 下手动添加 EL1918，并且选择为 Local 模式，其它的功能使用的操作没有区别。其它的带有 I/O 以及安全逻辑的模块使用类似。

注：作为安全逻辑模块后想作为一个单纯的安全输入模块使用，需要先删除安全逻辑。

1.6.2 SC 模块使用

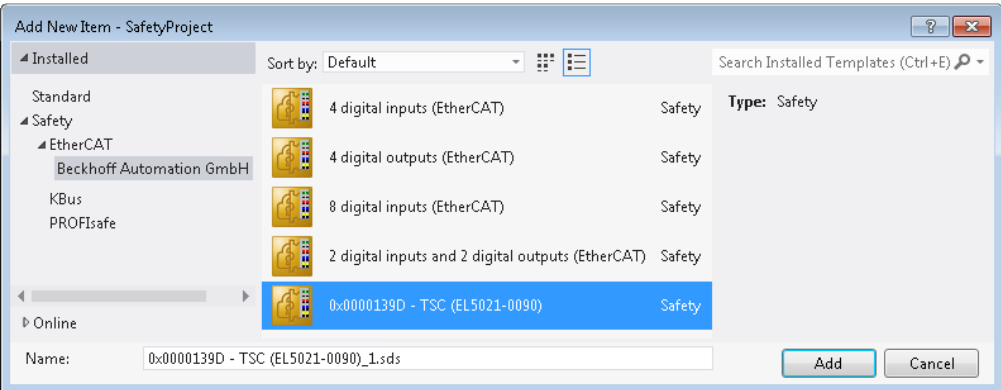
使用 SC 模块时，不能选择 EL6900、EL6930 作为安全逻辑模块（不支持模拟量功能）；

使用说明：

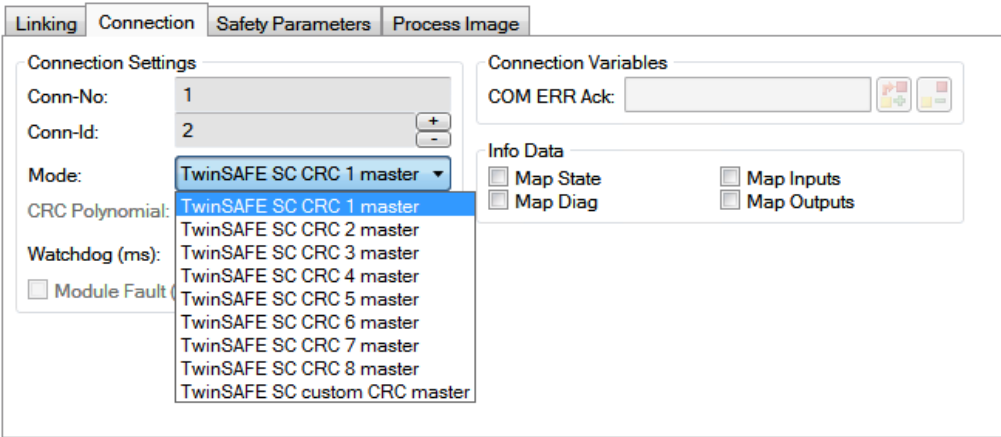
模块添加安全 Module

The screenshot shows the 'Slots' tab in the configuration window. It has tabs for 'General', 'EtherCAT', 'DC', 'Process Data', 'Slots', 'Startup', 'CoE - Online', and 'Online'. The 'Slots' tab is active, showing a table with 'Slot' and 'Module' columns. The table has one row: 'TSC Connection' and 'EL5021-0090'. Below the table, there are checkboxes for 'Download SlotCfg' and '(!->P)'. On the right, there is a 'Module' table with columns 'Module', 'ModuleIdent', and 'Description'. It has one row: 'EL5021-0090', '0x0000139D', and 'Module 1 (EL5021-0090)'. Below the table, there is a button 'Create project specific XML File...'.

安全工程中创建对于 SC 模块的连接



在连接中设置 SC 模块的安全地址以及 CRC，里面预设了 8 组 CRC，同一个系统中的 SC 模块必须设置不同的 CRC。如果超过，可以使用自定义 CRC，高位需要设置为 0x00ff。



另外模块本身也需要设置地址和 CRC，在 CoE 中设置

8010:0	TSC Settings	RW	> 2 <
8010:01	Address	RW	0x0000 (0)
8010:02	Connection Mode	RW	TwinSAFE SC CRC1 master (97039)

EL3214-0090 、EL3314-0090 索引为 8040

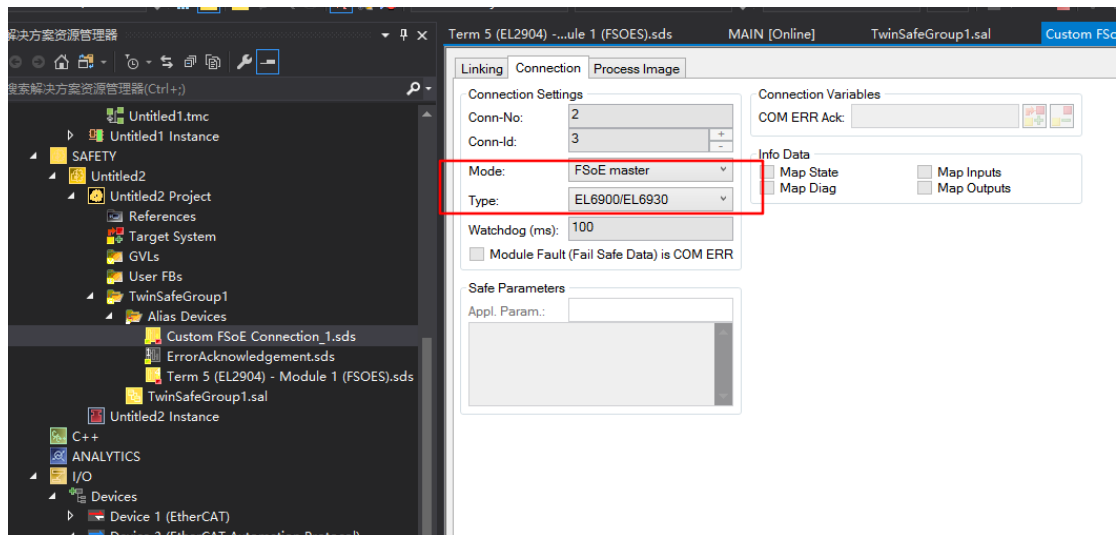
EL5021-0090 索引为 8010

EL6224-0090 索引为 800F

1.6.3安全逻辑模块之间的通讯

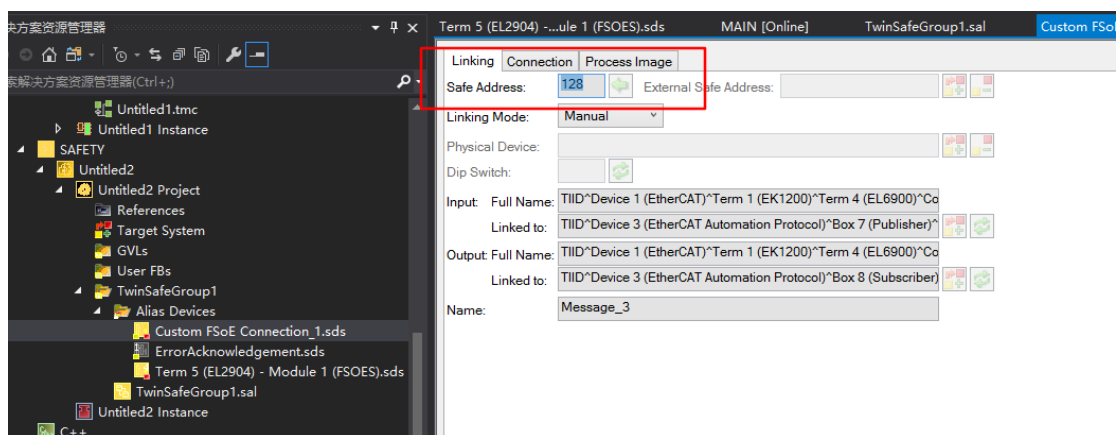
安全逻辑模块之间可以通过 FSoE 的方式进行安全数据交互，支持同一 EtherCAT 总线以及不同 EtherCAT 总线之间的通讯，可以使用 RT-Ethernet、EtherCAT 乃至无线等方式。

需要在两侧安全逻辑模块分别创建 FSoE 连接，根据模块实际配置设置 Mode 和 Type；Process Image 为需要交换的安全数据大小，两侧需要设置为一致。



FSOE master 需要设置 slave 的安全地址：

注：当 slave 为 EL6900 时，安全地址为 slave 的拨码地址；当使用 EL6910、EL1918 等作为 slave 时，安全地址需设置为 slave 的 FSoE Safe Address



Master 和 Slave 需要在 Linking 页面中进行变量的关联以实现安全数据的传输。

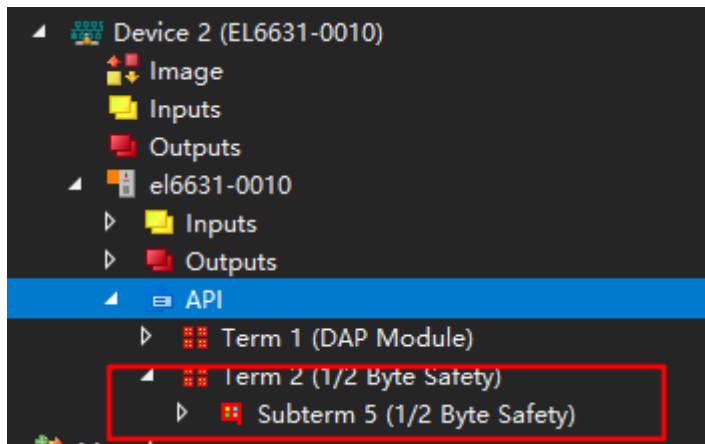
1.6.4 PROFI-safe 通讯

在 TwinCAT 3 环境使用 PROFI-safe 通讯时，推荐使用 EL6910，另外需要搭配 Profibus/net 接口实现通讯转换；EL6930 只支持作为 PROFI-safe slave 使用，并且只能有一个连接。下面以使用 EL6910+EL6631-0010 为 PROFI-safe slave 使用时与西门子 F 系列控制器进行安全通讯的例子，主要介绍配置过程。

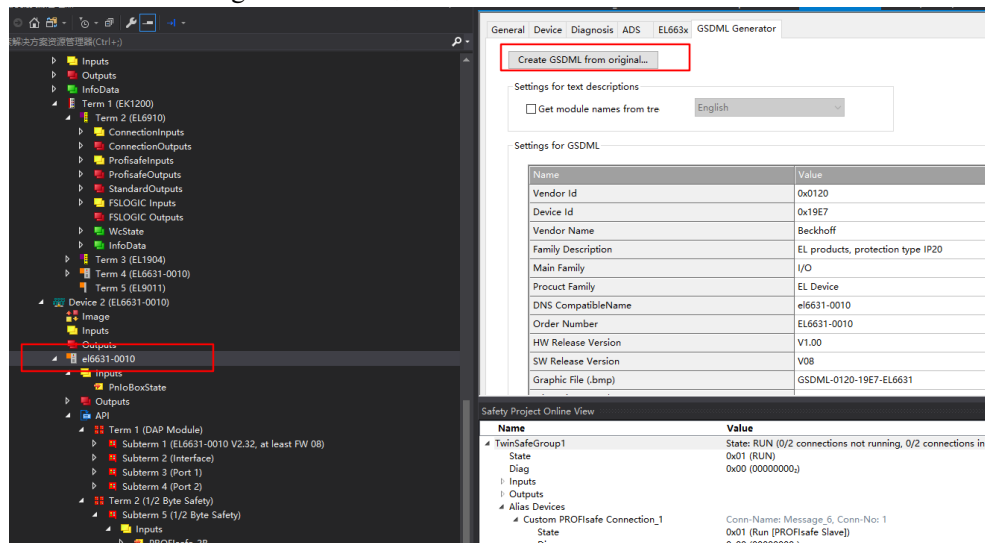
倍福 PROFI-safe slave 侧配置

配置 PROFINET 从站

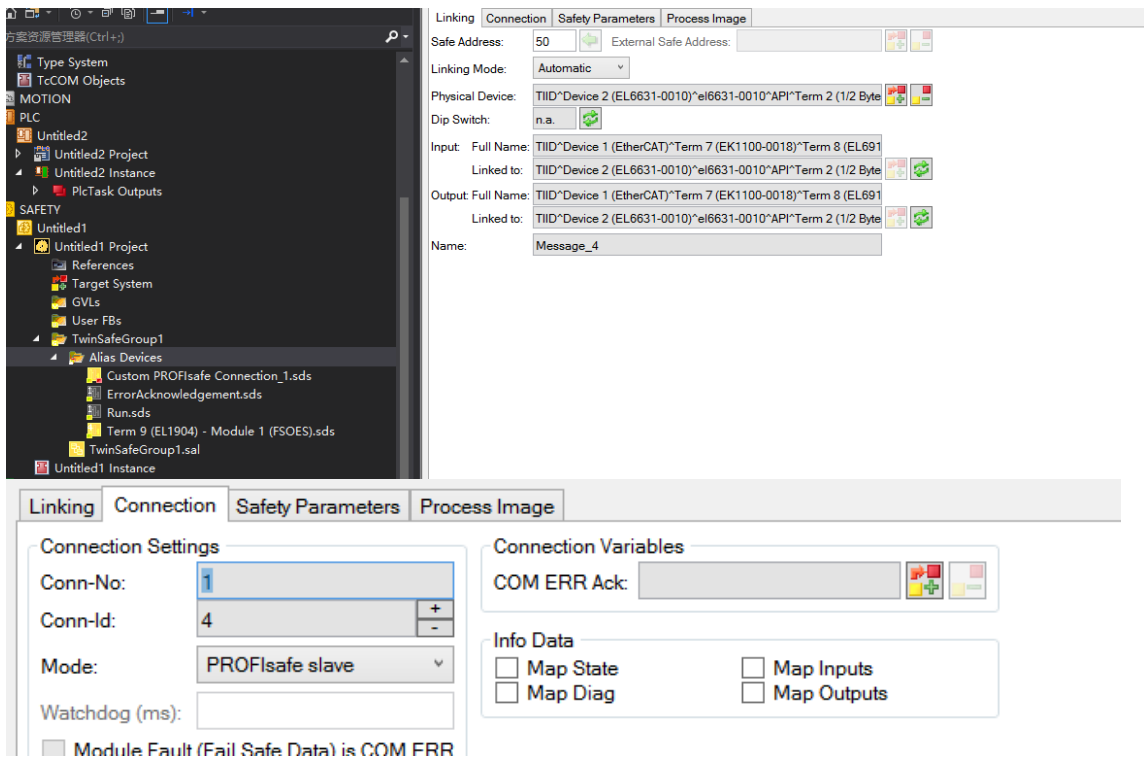
添加需要的安全数据大小（需要选择带有 Safe Module 的 EL6631 描述文件）



配置好后可以导出 gsd 文件以方便西门子侧直接导入配置

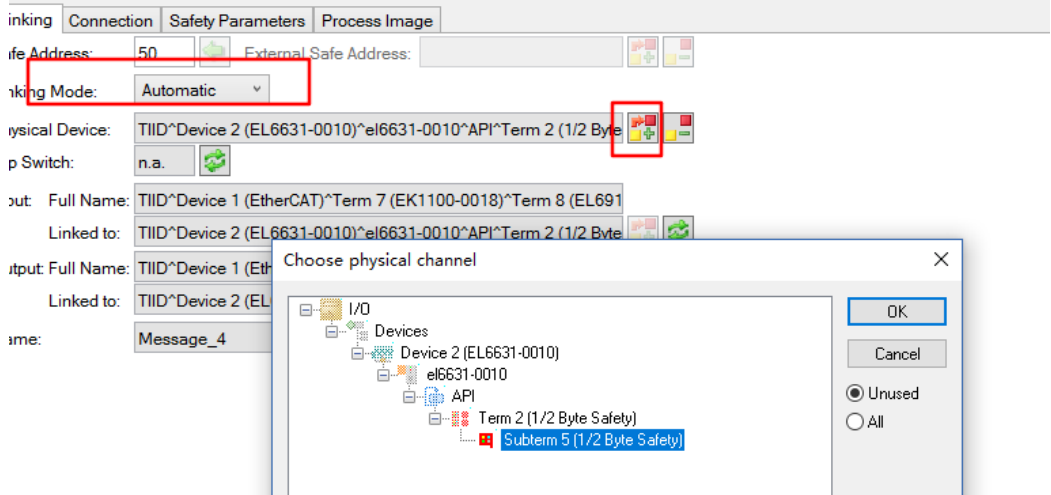


安全工程设置，手动创建 PROFIsafe 连接



其中 safe address 为 PROFIsafe master 侧使用的 F_Dest_Add 地址，例如此处设置为 50，设置模式为 PROFIsafe slave。

关联 PROFINET 中的报文，此处选择 Automatic 方式直接关联到 EL6631 的 safe module。



Connection 中配置为 PROFIsafe slave 模式

在安全工程中与来自 PROFIsafe 的数据进行交互。



Note

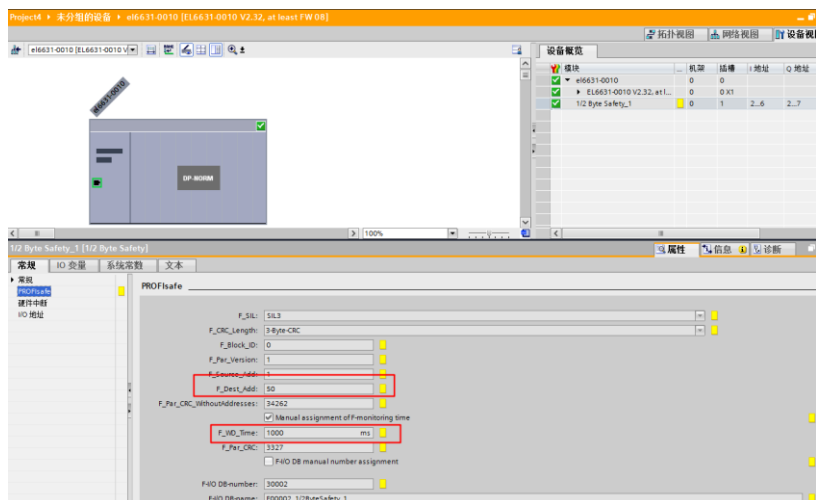
Saving PROFIsafe parameters persistently

The safety parameters for the slave connection transferred by the PROFIsafe master to the EL6910 are only transferred once when the PROFIsafe master starts up. On restart of the EL6910 these parameters would not be transferred again, so that the stored data have to be transferred again. If this is not done, the master must be restarted when the slave restarts.

另外作为 slave 使用时需要增加 PLC 代码以实现 PROFIsafe 参数保存，代码参考 EL6910 说明文档 PROFIsafe 配置部分。

西门子 PROFIsafe master 侧设置

- 导入倍福 EL6631 的 gsd 文件；
- 配置 PROFIsafe 信息，设置 F_Dest_Add 为从站的地址和看门狗时间；
- 在西门子组态环境中编写相关安全代码。



1.6.5 TwinSAFE Loader 使用

TwinSAFE_Loader 可以用于下载、删除、以及激活安全逻辑以及安全工程中的 Group 管理。详细使用说明参照官网 PDF 描述文档：

https://download.beckhoff.com/download/Document/automation/twinsafe/TwinSAFE_Loader_en.pdf

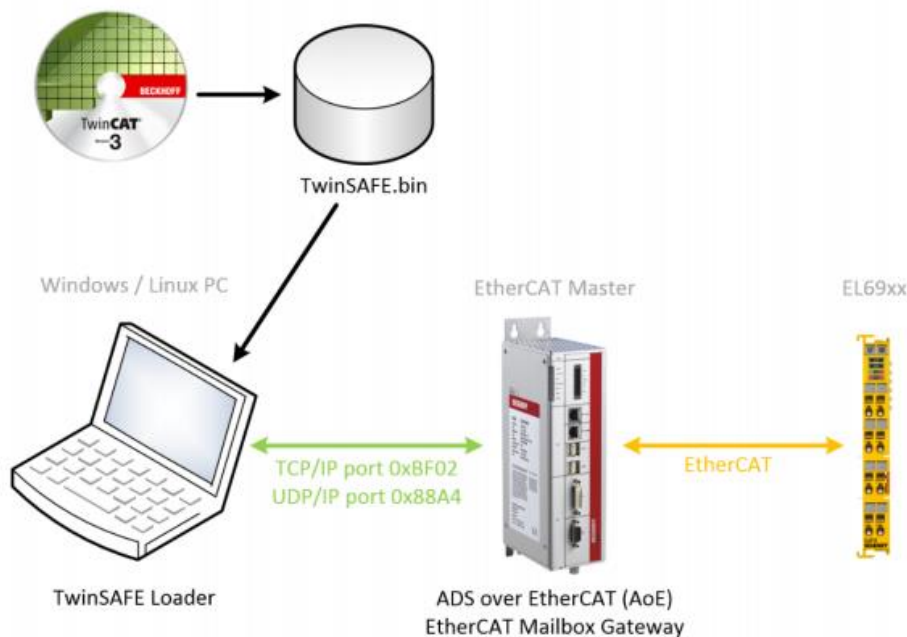


Fig. 1: TwinSAFE Loader - Overview

该软件可以在 Windows 以及 Linux 平台中运行，无需安装 TwinCAT 软件。可以通过 ADS Over EtherCat (AoE) 或者 EtherCat Gateway 的方式进行设置。

AoE 方式的下载、删除、激活安全程序。

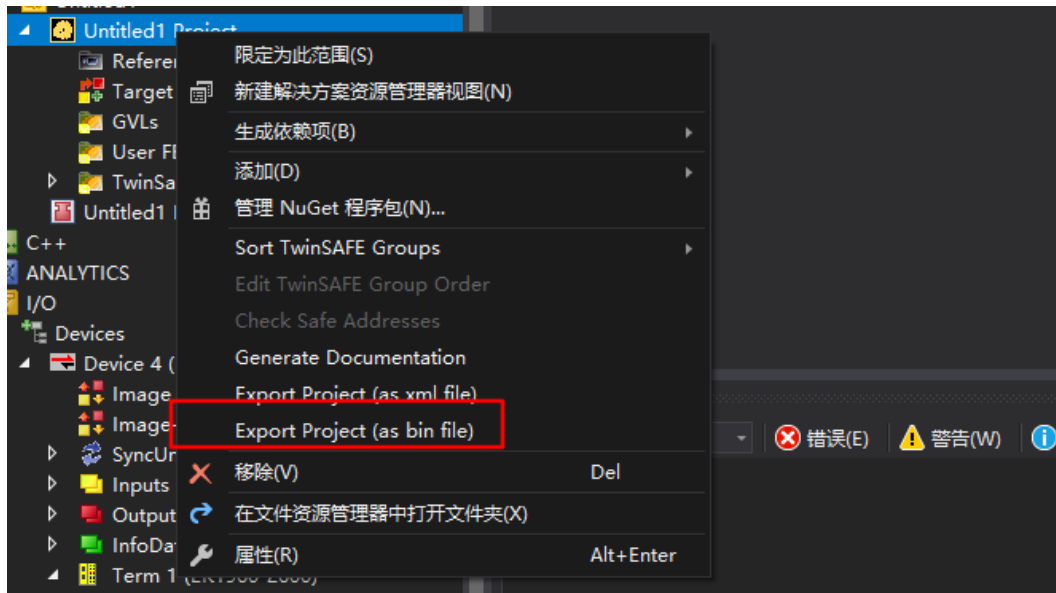
Command line parameters	Description
--gw <IPv4 address>	Specification of the IPv4 address of the EtherCAT mailbox gateway or, in AoE mode, the IPv4 address of the EtherCAT master. As of version v5, the EtherCAT master can also be addressed via the host name in AoE mode.
--ams <NetId>	Specification of the AmsNetID, if ADS over EtherCAT (AoE) is to be used.
--localams <NetId>	if --ams is used the local AMSNetID can be specified. If the parameter is not used, the AmsNetID is formed from its own IP address + ".1.1".

软件提供了一个 ADS 客户端，通过 AoE 进行设置时，EtherCAT Master 侧需要有软件所在的电脑的路由信息：

- 对于安装了 TwinCAT 的电脑，可以使用 TwinCAT 和控制器进行添加路由操作；
- 对于没有 TwinCAT 或者 Linux 的电脑，可以在控制器侧手动创建路由信息，建议设置 AMS NetID 为 IP 地址+ “.1.1” 的方式

导出安全工程

建议将导出的 bin 文件放入到 TwinSAFE Loader 所在的根目录下，方便后续操作：



下载 bin 程序

```
C:\TwinSAFE_Loader>TwinSAFE_Loader --gw 169.254.86.76 --localams 169.254.120.1.1.1 --ams 169.254.86.76.5.1
--user Administrator --pass TwinSAFE --slave 1001 --proj ./Untitled1.bin
2020-12-31T09:47:52 Info: TwinSAFE Loader - v7
2020-12-31T09:47:52 Info: Connected to 169.254.86.76
2020-12-31T09:47:52 Info: 'Administrator' is downloading 'Untitled1' to EK1960-2600 @2
2020-12-31T09:47:58 Info: Download of 'Untitled1' (0xecd9) to EK1960-2600 @2 completed
2020-12-31T09:47:58 Info: connection closed by remote
```

通过命令提示窗口，进入到 TwinSAFE Loader 目录后执行如上命令

--gw 工控机的 IP 地址；

--localams 调试电脑的 AMSNetID（若为 IP+ “.1.1”，可以不用该指令）；

--ams 安全逻辑模块所在的 EtherCAT 主站的 NetID；

--user --pass 用户名以及密码；

--slave 需要下载程序的安全逻辑模块地址

--proj TwinCat 工程导出的 bin 文件

激活 bin 程序文件

```
C:\TwinSAFE_Loader>TwinSAFE_Loader --gw 169.254.86.76 --localams 169.254.120.1.1.1 --ams 169.254.86.76.5.1
--user Administrator --pass TwinSAFE --slave 1001 --proj ./Untitled1.bin --crc 0xecd9
2020-12-31T09:26:58 Info: TwinSAFE Loader - v7
2020-12-31T09:26:58 Info: Connected to 169.254.86.76
2020-12-31T09:26:59 Info: Project activation successful
2020-12-31T09:26:59 Info: connection closed by remote
```

--crc 安全程序的 CRC，可以在 TwinCat 安全程序中找到该 CRC。

删除安全工程

```
C:\TwinSAFE_Loader>TwinSAFE_Loader --gw 169.254.86.76 --localams 169.254.120.1.1.1 --ams 169.254.86.76.5.1
--user Administrator --pass TwinSAFE --slave 1001 --delete
2020-12-31T10:05:22 Info: TwinSAFE Loader - v7
2020-12-31T10:05:22 Info: Connected to 169.254.86.76
2020-12-31T10:05:22 Info: 'Administrator' deletes project from EK1960-2600 @2
2020-12-31T10:05:23 Info: Project was successfully deleted from EK1960-2600 @2
2020-12-31T10:05:23 Info: connection closed by remote
C:\TwinSAFE_Loader>
```

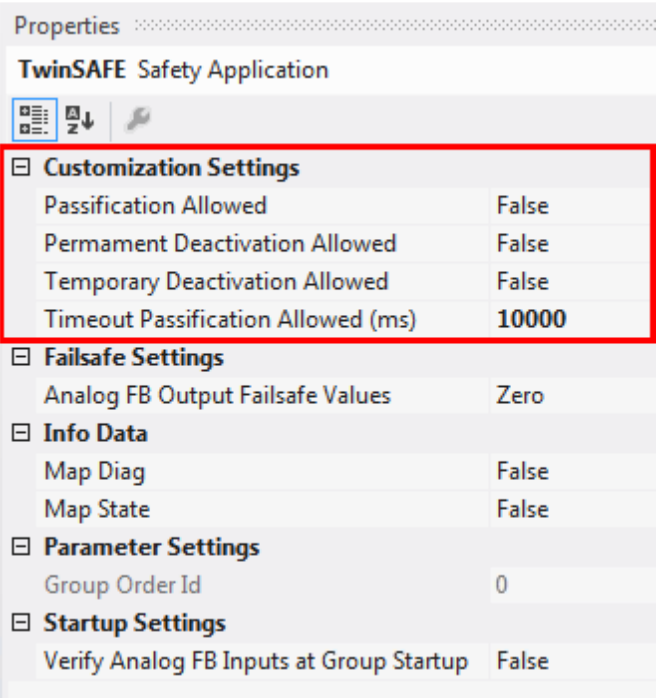
1.6.6 Customizing 功能

Customizing 功能  可以通过 safety 工具栏或者 TwinSAFE 菜单栏进行选择。可以用于启用/禁用 TwinSAFE Group。包括几种不同的方式，见如下表格。

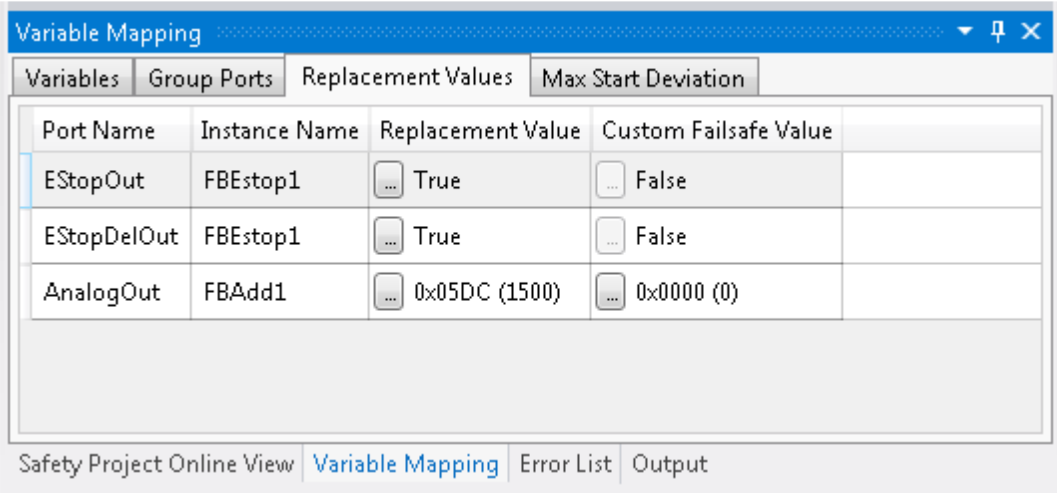
钝化	描述
持久钝化	TwinSAFE Group 被用户永久禁用。Group 的输出被设置为参数化的替代值。 如果 Group 被重新启用，为了使 Group 启动，需要将 Run 信号重新从 0 切换到 1。 设置参数： Permanent Deactivation Allowed: TRUE/FALSE
安全逻辑模块重新切换状态前保存钝化	TwinSAFE group 在逻辑模块状态切换前保持禁用状态。Group 的输出被设置为参数化的替代值。该钝化设置无法作为安全程序下载时的默认设置。 如果 Group 被重新启用(除了逻辑模块重新切换状态外)，为了使 Group 启动，需要将 Run 信号重新从 0 切换到 1。 设置参数： Temporary Deactivation Allowed: TRUE/FALSE
手动控制单元钝化	当开始启用钝化时，Group 中定义的连接在到达设定时间（默认为 10s）后必须报出 COM error。否则，Group error 将被置位以及生成对应的诊断信息。Group 中只能定义一个连接，并且必须是作为 Master 连接。 设置参数： Passification Allowed : TRUE/FALSE Timeout Passification Allowed: Time in ms

注：使用手动控制单元钝化该功能时，需要让 Group 在设定时间内报出 COM error 才能确保该功能的正常生效，比如为模块的话在硬件上移除。

为了使用 Customizing 功能，需要对 Group 属性进行设置。



设置完 Group 中的参数后，Group 中的安全功能块的输出会在 Replacement Values 中列出。可以设置 Group 被钝化后替代的输出值。

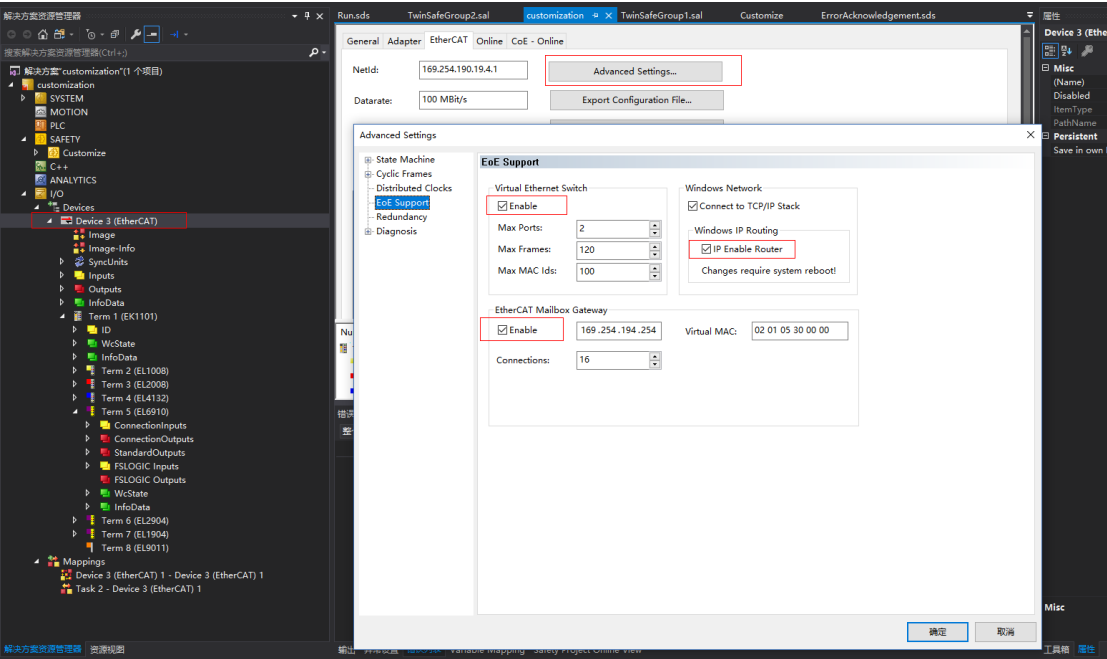


设置完安全工程后，可以通过  按钮来进行 Group 的启用/禁用。



启用/禁用的功能同样也可以使用 TwinSAFE Loader 实现。

首先需要开启 EtherCAT Mailbox Gateway 功能。在 EtherCat EoE 选项中勾选 Virtual Ethernet Switch, IP Enable Router 和 EtherCAT Mailbox Gateway; 确保可以 ping 通 EtherCAT Mailbox Gateway 对应的 IP 地址, 如下为 169.254.194.254。



测试例程使用了两个 Group, 设置了 Permanent Deactivation Allowed 和 Temporary Deactivation Allowed 为 True。

通过如下命令获取当前安全工程的 Group 设置信息:

```
TwinSAFE_Loader --gw 169.254.194.254 --user Administrator --pass TwinSAFE --slave 1007 --list ./groupconfig.csv
```

获取的 groupconfig.csv 信息如下

1				
id	activate	passivate	temporarily	permanent
1 A		D	E	E
2 A		D	E	E

第一列: TwinSAFE Group ID

第二列: 指示对应 Group 是否激活

第三列: 指示对应 Group 是否可以钝化以及当前的状态

第四列: 指示对应 Group 是否可以临时钝化以及当前的状态

第五列: 指示对应 Group 是否可以持久钝化以及当前的状态

A: Active

D: 无法激活该方式

E: 可以激活, 但是当前为激活

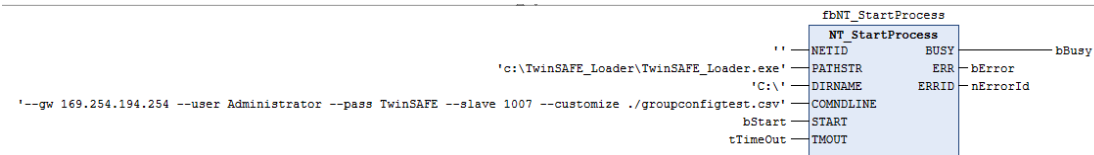
此时我们通过 Gateway 修改 Group 2 的状态，新建一个 CSV 文件，设置 active 状态为未激活，并且启用临时钝化功能

1				
id	activate	passivate	temporarily	permanent
1	A	D	E	E
2	E	D	A	E

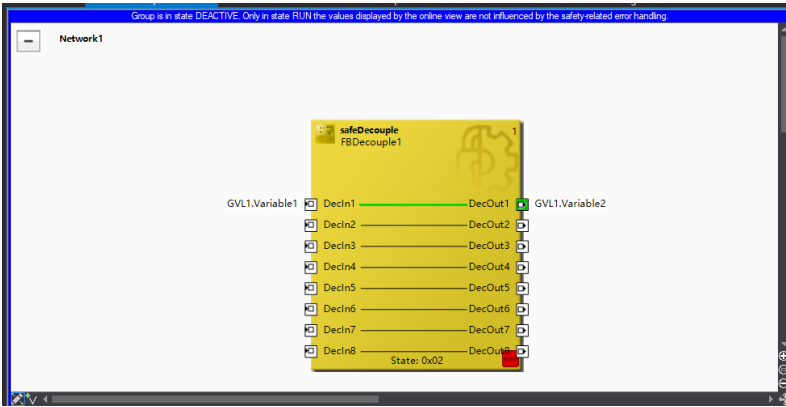
通过批处理命令生效设置，也可以通过 PLC 代码调用批处理命令来实现

```
Pinging 169.254.194.254 with 32 bytes of data:
Reply from 169.254.194.254: bytes=32 time=7ms TTL=128
Reply from 169.254.194.254: bytes=32 time=7ms TTL=128
Reply from 169.254.194.254: bytes=32 time=7ms TTL=128

Ping statistics for 169.254.194.254:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 7ms, Average = 7ms
Control-C
^C
C:\TwinSAFE_Loader>TwinSAFE_Loader --gw 169.254.194.254 --user Administrator --p
ass TwinSAFE --slave 1005 --customize ./groupconfigtest.csv
2022-02-14T11:23:33 Info: TwinSAFE Loader - v?
2022-02-14T11:23:34 Info: 'Administrator' is customizing FSoE device 1
2022-02-14T11:23:35 Info: Customization of FSoE device 1 complete
C:\TwinSAFE_Loader>ping 169.254.194.254_
```



此时可以看到 Group 2 为钝化状态，并且功能块的输出为在 Replacement value 中预设的值。



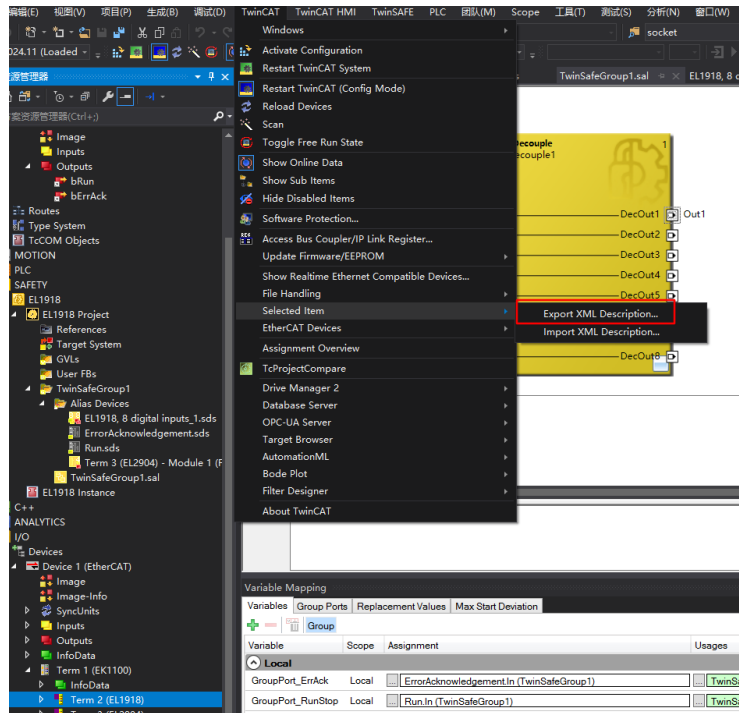
另外 TwinSAFE User 功能的使用类似，这里不作介绍。

1.6.7 EL1918 等在 TwinCAT 2 环境以及第三方 EtherCAT 主站下的使用

首先需要通过 TwinCAT 3 环境进行安全程序的编写下载。这一步骤这里不作介绍。以下以 EL1918 为例。

主要缺点，每次修改都需要通过 TwinCAT 3 环境进行，调试诊断时无法在线监视等。

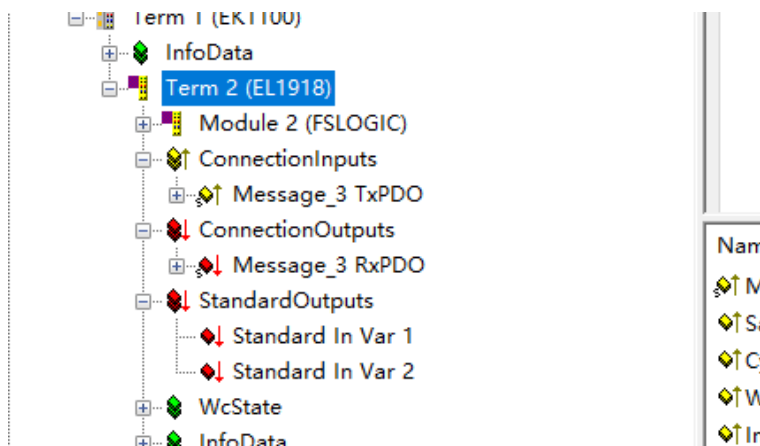
安全工程完成后，导出 EL1918 的 XML 文件，同时在 EtherCAT 总线的 EL1918 下可以查看变量的对应关系，包括 Acknowledgement、Run 以及定义的有关信号。



对于 TWINCAT 2，里面已经定义的 FSoE 数据类型虽然存在结构一样的类型，但是名称不一致，因此无法导致，可以通过在 TWINCAT 2 里面手动添加 TwinCAT 3 的 FSoE 类型或者直接修改 XML 文件中的类型名称为 TWINCAT 2 对应类型的名称。

另外如果 TWINCAT 2 和 TwinCAT 3 中模块的 EtherCAT 路径以及配置不一致，也可能导致 XML 文件无法导入；这里提供一种简单的方式，在 TWINCAT 2 中手动添加 EL1918，在 TWINCAT 2 中再次导出该 EL1918 的 XML 文件，将该文件中关于 EtherCAT 配置部分的数据覆盖 TwinCAT 3 中导出的 XML 文件，然后再导入到 TwinCAT 2 中。

在 TwinCAT 2 导入中 XML 后，信息如下：



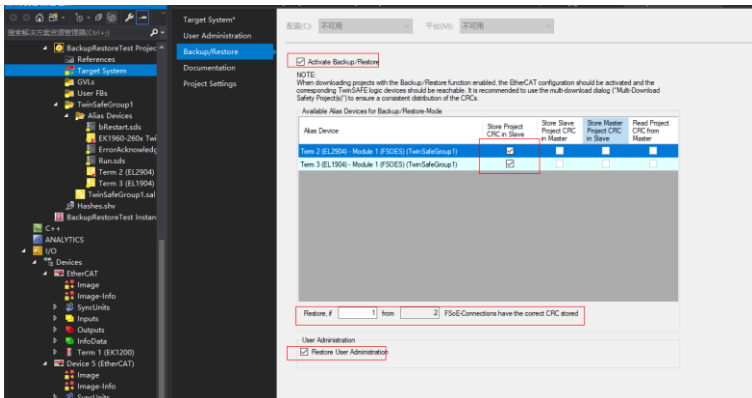
其中 Message 为与其它安全 IO 的关联信息，Standard 为 Acknowledgement、Run 信号等，在 TwinCAT 2 中实现与安全 IO 以及 PLC 的变量映射，就可以运行安全程序了。

在第三方 EtherCAT 主站下的使用与在 TwinCAT 2 下的使用类似，这里就不展开介绍了。

1.6.8 备份还原

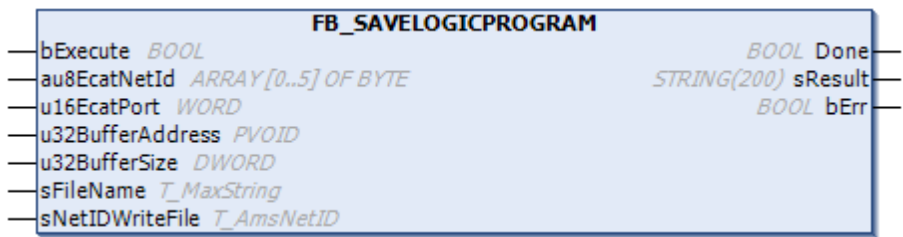
对于 EL6910、EJ6910、EK1960，系统中更换了新的模块后可以通过备份还原机制将安全工程加载到新模块中，无需通过 TwinCAT，减少现场工作，下面介绍具体的实现方式，以 EK1960 为例，。

使用这个功能，首先需要在安全工程中启用备份还原机制，选择模块以用于存储模块 CRC 以及其中几个连接正确存储了 CRC 后可以进行还原，设置完成后下载安全程序即可。

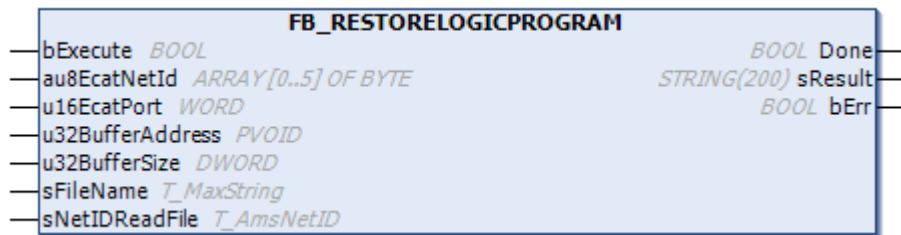


备份与还原需要通过 PLC 代码来实现，需要加载库 `TC3_EL6910_Backup_Restore`，https://download.beckhoff.com/download/document/automation/twinsafe/TC3_EL6910_Backup_Restore.zip 可以在通过该连接下载。

这个库共提供了三个功能块：`FB_DeleteLogic`、`FB_RestoreLogicProgram`、`FB_SaveLogicProgram` 用于安全程序的删除、还原、备份。



FUNCTION_BLOCK FB_SAVELOGICPROGRAM						
名称	类型	继承自	地址	初始化	注释	
bExecute	BOOL				Positive edge starts the backup process	
au8EcatNetId	ARRAY [0..5] OF BYTE				EtherCAT Net-ID of the TwinSAFE Logic - link to e.g. EL6910/InfoData/AdsAddr/netId	
u16EcatPort	WORD				Port of TwinSAFE Logic - link to e.g. EL6910/InfoData/AdsAddr/port	
u32BufferAddress	PVOID				Address of buffer, in which the TwinSAFE Logic program should be stored temporarily - buffer e.g. ARRAY[0..16#FFFF] OF BYTE	
u32BufferSize	DWORD				size of buffer	
sFileName	T_MaxString				File, in which the TwinSAFE Logic program should be stored	
sNetIDWriteFile	T_AmsNetID				AmsNetID of device where the file should be written to	
Done	BOOL				User information that the FB finished the operation	
sResult	STRING(200)				FB Result	
bErr	BOOL				An error occurred during operation, details in sResult	



FUNCTION_BLOCK FB_RESTORELOGICPROGRAM						
名称	类型	继承自	地址	初始化	注释	
bExecute	BOOL				Positive edge starts the restore process	
au8EcatNetId	ARRAY [0..5] OF BYTE				EtherCAT-Net-ID of the TwinSAFE Logic - link to e.g. EL6910/InfoData/AdsAddr/netid	
u16EcatPort	WORD				Port of TwinSAFE-Logic - link to e.g. EL6910/InfoData/AdsAddr/port	
u32BufferAddress	PVOID				Address to buffer, in which the TwinSAFE Logic program should be stored - buffer e.g. ARRAY[0..16#FFFF] OF BYTE	
u32BufferSize	DWORD				size of buffer	
sFileName	T_MaxString				File which contains the TwinSAFE logic program and should be restored	
sNetIDReadFile	T_AmsNetID				AmsNetID of device where the file is stored	
Done	BOOL				User information that the FB finished the operation	
sResult	STRING(200)				FB result	
bErr	BOOL				An error occurred during operation, details in Result	

下面实际举例备份还原操作的过程

备份,通过上升沿触发,可以看到在设置目录下生成了安全程序文件 safetyprojectTest.bin

```

// backup of the TwinSAFE logic program
fb_save (
  bExecute := FALSE := StartBackup := FALSE,
  au8EcatNetId := SafetyLogicAmsNetID,
  u16EcatPort := SafetyLogicPort := 1001,
  u32BufferAddress := ADR(internalBuffer),
  u32BufferSize := SIZEOF(internalBuffer),
  sFileName := FileString := FileString := FileString,
  sNetIDWriteFile := LocalAmsNetID := LocalAmsNetID,
  Done := FALSE := SaveDone := FALSE,
  sResult := TwinSAFE := SaveResult := TwinSAFE,
  bErr := FALSE := SaveErr := FALSE;
// Restore of the TwinSAFE logic program

```

Name	Size	Type	Date Modified
BKipCdiag		File Folder	4/23/2020 2:58 PM
Documents and Settings		File Folder	1/10/2022 3:46 AM
RegFiles		File Folder	4/23/2020 2:58 PM
System		File Folder	7/7/2020 6:08 PM
TwinCAT		File Folder	4/23/2020 2:58 PM
UPnP		File Folder	4/23/2020 2:58 PM
WWW		File Folder	4/23/2020 2:58 PM
BOOT	1.07KB	INI File	8/10/2005 7:30 PM
CBx053_CE600_HPS_v408...	0 bytes	10 File	10/31/2002 8:42 PM
NK	32.7MB	BIN File	7/9/2020 8:12 PM
Splash	4.47KB	BMX File	1/31/2007 1:35 AM
safetyprojectTest	14KB	BIN File	1/18/2022 7:56 AM

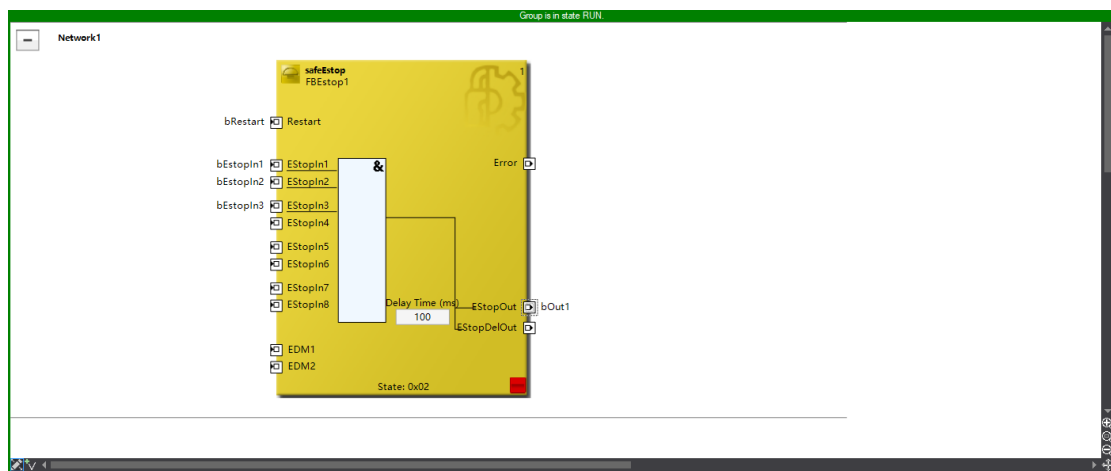
备份成功后, 由于没有额外的 EK1960, 实际通过手动删除模块里面的安全工程再测试还原功能。

注: 在还原的过程中, 在检查存储到其它模块的 CRC 时才会确认安全程序是否匹配。安全逻辑模块中原先的安全逻辑会被删除, 该过程是不可逆的。

还原工程

通过上升沿触发，可以看到当前已经成功还原了工程，并且可以对安全工程在线监视。

```
fb_restore(  
  bExecute TRUE := StartRestore TRUE ,  
  au8EcatNetId:= SafetyLogicAmsNetID,  
  ul6EcatPort 1001:= SafetyLogicport 1001,  
  u32BufferAddress 16#E4618197:= ADR(internalBuffer2),  
  u32BufferSize 65536:= SIZEOF(internalBuffer2),  
  sFileName /Hard Disk := FileString /Hard Disk ,  
  sNetIDReadFile := LocalAmsNetID ,  
  Done TRUE => RestoreDone TRUE ,  
  sResult .Restorin => RestoreResult .Restorin ,  
  bErr FALSE => RestoreErr FALSE ; RETURN , Restoring of TwinSAFE Restore Program from File /Hard Disk/safetyprojectTest.bin successfully done'
```

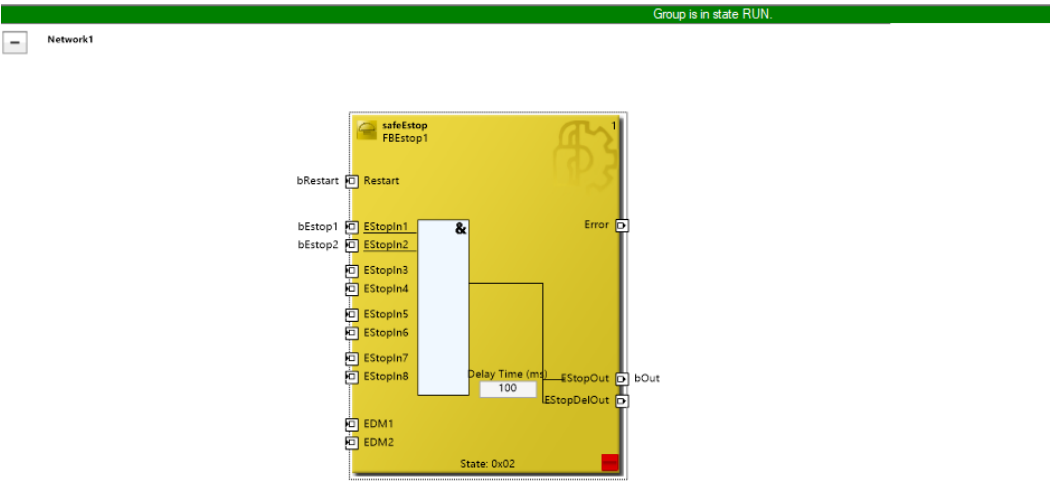


1.7 安全工程诊断

当安全工程被触发时，及时地了解触发原因是非常重要的，以下介绍安全工程的诊断。

1.7.1在线诊断

通过菜单栏 TwinSAFE→Show Online Data 可以对安全工程进行在线监视，可以查看当前安全工程的运行状态以及各个安全功能的执行情况



在 Variable Mapping 界面可以查看各变量的当前状态

Variables Group Ports Replacement Values Max Start Deviation						
Group						
Search:						
Variable	Scope	Assignment	Usages	Online Value	Comment	
Local						
GroupPort_ErrAck	Local	ErrorAcknowledgementIn (TwinSafeGroup1)	TwinSafeGroup1 Err Ack	FALSE (0)		
bRestart	Local	bRestartIn (TwinSafeGroup1)	TwinSafeGroup1.Network1.FBEstop1.Restart	FALSE (0)		
bEstop1	Local	EL1918_8.digital.inputs_1.FSIN.Module.2.Input (TwinSafeGroup1)	TwinSafeGroup1.Network1.FBEstop1.EStopIn1	FALSE (0)		
bEstop2	Local	Term 3 (EL1904) - Module 1 (FSOES).InputChannel.1 (TwinSafeGroup1)	TwinSafeGroup1.Network1.FBEstop1.EStopIn2	FALSE (0)		
bOut	Local	TwinSafeGroup1.Network1.FBEstop1.EStopOut	Term 2 (EL2904) - Module 1 (FSOES).OutputChannel.1 (TwinSafeGroup1)	FALSE (0)		
GroupRun	Local	RunIn (TwinSafeGroup1)	TwinSafeGroup1.Run/Stop	TRUE (1)		

输出 报警设置 错误列表

Variable Mapping

Safety Project Online View

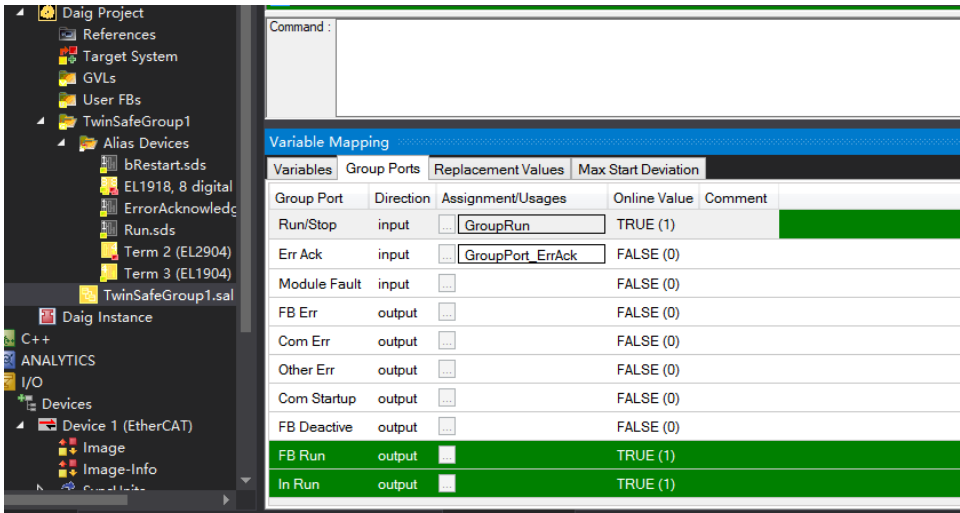
在 Safety Project Online View 可以查看 Group、安全模块、功能块的状态，如果默认没有这个窗口，可以通过菜单栏一视图→其它窗口→Safety Project Online View 调出

Safety Project Online View	
Name	Value
▲ TwinSafeGroup1	State: RUN (0/2 connections not running, 0/2 connections in error, 0/1 functions blocks in error)
State	0x01 (RUN)
Diag	0x00 (00000000)
Inputs	
Outputs	
Alias Devices	
Term.2 (EL2904) - Module.1 (FSOES)	Conn-Name: Message_2, Conn-No: 1
Term.3 (EL1904) - Module.1 (FSOES)	Conn-Name: Message_3, Conn-No: 2
Function Blocks	
▲ FBEstop1 (safeEstop)	
State	0x03 (SAFE)
Diag	0x0000 (0000000000000000)

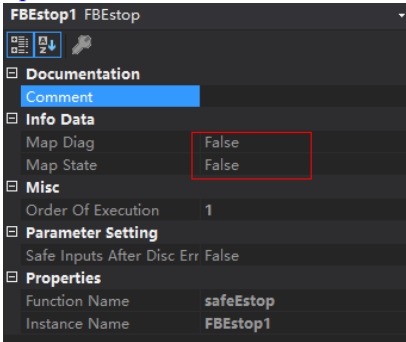
1.7.2通过 PLC 代码诊断

实际现场安全功能被触发时，大部分情况下由于现场并不具备在线查看的条件，此时可以通过 HMI 等直观的方式将原因展示给现场人员。对于在线监视中看到的信息都可以通过变量映射的方式由 PLC 程序获取。

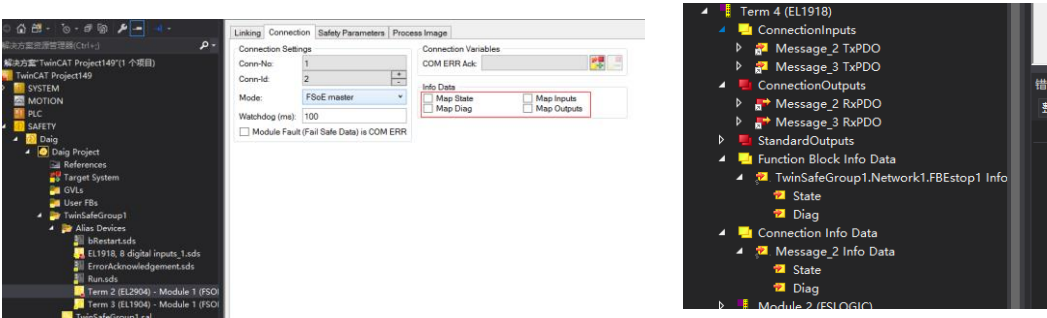
Group 的 FB Err、Com Err 等变量可以通过在 Alias Devices 下添加普通变量的方式实现与 PLC 之间的交互。



Group 中功能块的 Diag、State 信息可以在属性窗口将 Map Diag、Map State 设置为 True 来实现。不同功能块的 Diag 以及 State 对应描述不一致，详见功能块的 PDF 文档 <https://download.beckhoff.com/download/Document/automation/twinsafe/TwinSAFE-Logic-FBen.pdf>



与其它安全模块以及包括 FSoE 和 PROFIsafe 的连接可以在 Info Data 中勾选对应的 Map State。勾选后诊断信息可以在安全逻辑模块下找到对应的变量实现与 PLC 变量之间的映射。



另外通过 CoE 可以读取安全模块提供的诊断信息，使用功能更 FB_EcCoeSdoRead 实现，以下为 EL1904 对应的诊断信息，可以在模块的说明文档中找到。

Index	Name	Meaning	Flags	Default
FA80:01	Temperature 1	Temperature measurement 1	RO	0 _{bin}
FA80:02	Temperature 2	Temperature measurement 2	RO	0 _{bin}

The CoE objects 800E_{hex} display further diagnostic information.

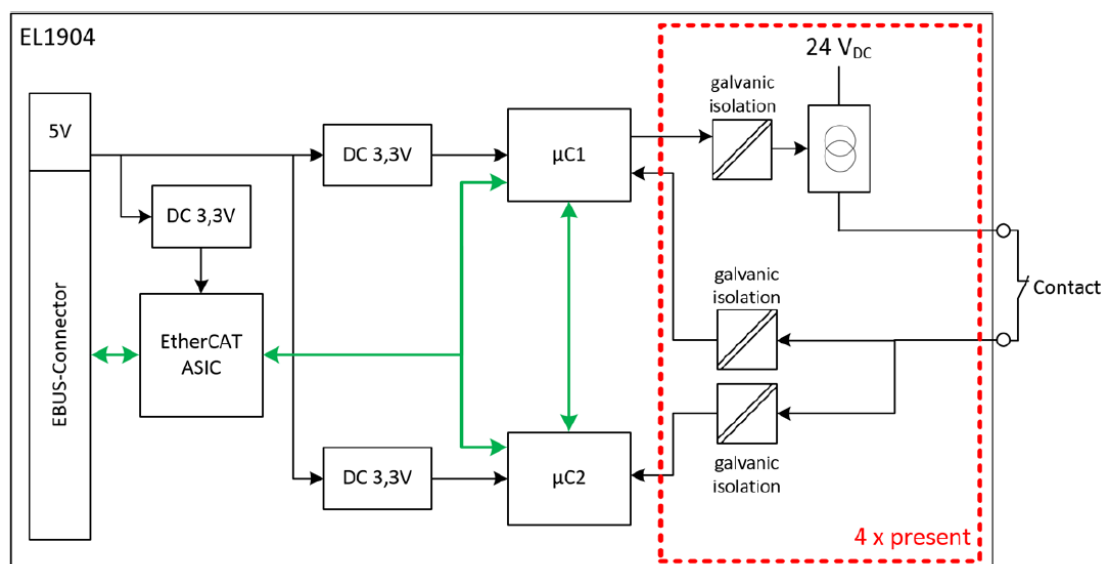
Index 800E_{hex}: Diagnostic objects

Index	Name	Meaning	Flags	Default
800E:0	Diag	The following sub-indices contain detailed diagnostic information.	RO	
800E:0A	Sensor test error	Bit Error during the sensor test	RO	
		0 1 _{bin} Error at input 1		0 _{bin}
		1 1 _{bin} Error at input 2		0 _{bin}
		2 1 _{bin} Error at input 3		0 _{bin}
		3 1 _{bin} Error at input 4		0 _{bin}
800E:0B	Error during two-channel evaluation	Bit Error during the contiguous evaluation of two channels, i.e. the two channels contradict each other.	RO	
		0 1 _{bin} Error in the first input pair		0 _{bin}
		1 1 _{bin} Error in the second input pair		0 _{bin}
800E:0C	Error in the safety mat operating mode: input pair disagree	Bits Error in the input pair	RO	
		1, 0 11 _{bin} Error in the first input pair		00 _{bin}
		3, 2 11 _{bin} Error in the second input pair		00 _{bin}
800E:0D	Error in the safety mat operating mode: external supply	Bit Error in the test pulses in the safety mat operating mode; i.e. the terminal has detected an external supply.	RO	
		0 1 _{bin} Error at input 1		0 _{bin}
		1 1 _{bin} Error at input 2		0 _{bin}
		2 1 _{bin} Error at input 3		0 _{bin}
		3 1 _{bin} Error at input 4		0 _{bin}

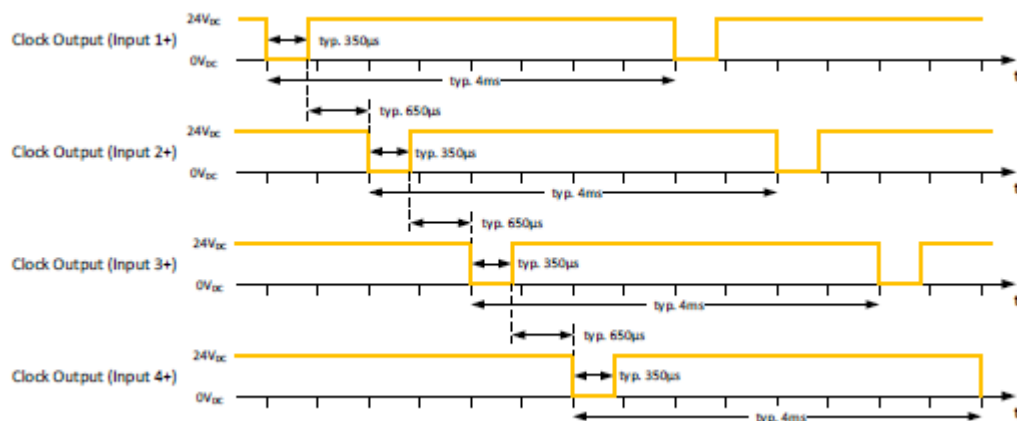
1.8 常见问题

1.8.1 EL1904 接入光栅等 PNP 信号以及脉冲检测介绍

默认情况下，EL1904 模块的脉冲检测功能均处于开启状态，下图为文档中关于输入通道的说明



接入接点信号时，通道的+端输出的 24V 会定时的中断输出，由 - 端进行检测；如果不同通道之间接入的干信号发生短路，模块可以检测到脉冲信号异常从而触发安全功能。



接入 PNP 信号时，由于信号本身提供了 24V，我们只需要接入到通道的-端即可，**需要注意关闭脉冲检测功能**；接入光栅时，光栅一般会提供两个接入信号并且自带了脉冲功能，可以根据信号类型通过安全参数设置输入信号成对使用以及脉冲类型为异步重复脉冲或者任意重复脉冲。

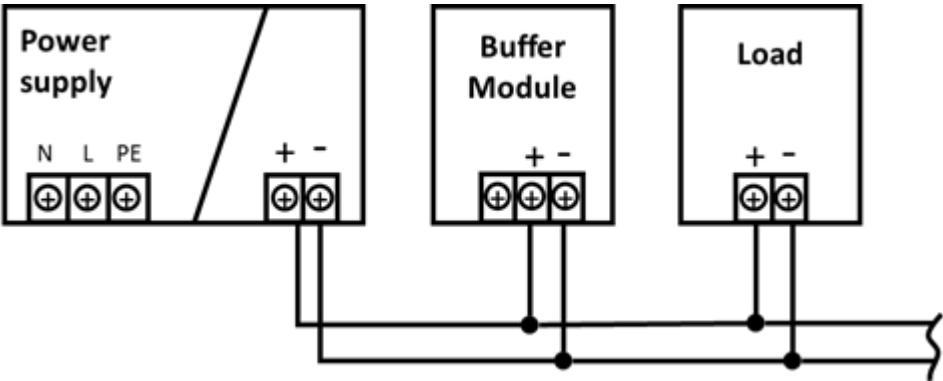
1.8.2 EL2904 模块电压低报错

当 EL2904 检测到 IO 的电压超出允许范围时，模块会报错，并且该故障只能通过对模块 E-bus 进行重新上电的方式进行复位。

应对措施：

规范电柜设计以及现场布线等，避免 EMC 错误；

可以将安全模块的 IO 供电由单独的开关电源提供；
尽量减少 EL2904 模块到执行器件（如继电器等）的线缆距离，减少压降
使用开关电源缓冲模块，可以有效应对电源电压下降、波动以及峰值负载。我们也提供了此类产品，如 PS9011-2420-0001，可以在开关电源断开时可以维持 200ms 20A 的供电能力。可以推荐客户使用我的开关电源+缓冲模块方式进行供电。



1.8.3 AX5000 安全选项卡 FDD9 错误

AX5805/6 内部比较两个转速(来自编码器的转速和通过 PWM 频率计算的内部转速)，当两个转速偏差过大时就会报 FDD9 错误。

编码器的输出速度非常准确，但内部计算(PWM)的输出速度可能不准确。可以通过修改电机默认参数进行修改。此电机默认数据值将增加磁通电流，这将有助于改进基于 PWM 的内部计算。

0x3028 将产生 20%的磁通电流，取 28 的一半，0x3014 将产生 10%的磁通电流；需要注意的是过高的磁通电流会导致电机发热。

			pairs	Window	Violationlevel	Data
AM8011-xBxx	0	TwinCAT version ≥ 2.11 R3 build 2221: Motor type in text form (see chapter 3.4)	3	0xB4	0x14	AX5805 SW ≤ 04 0x3028

电机默认参数可以在如下链接中找到。

https://download.beckhoff.com/download/document/automation/twinsafe/ax5805_de_faultmotorvalues_en.pdf

1.8.4 EK9300 能否带安全模块？

不能。

作为 PROFINET 从站耦合器，EK9300 能带的 IO 可以在 C:\TwinCAT\3.1\Config\Io\Profinet\GSDML-V2.33-beckhoff-EK9300-20180718.xml 中找到；使用安全模块要通过控制器进行中转，如 CX9020+B930 接口，并且需要安全逻辑模块，如果需要进行进行 PROFIsafe 通讯，需选择安全逻辑模块为 EL6910。

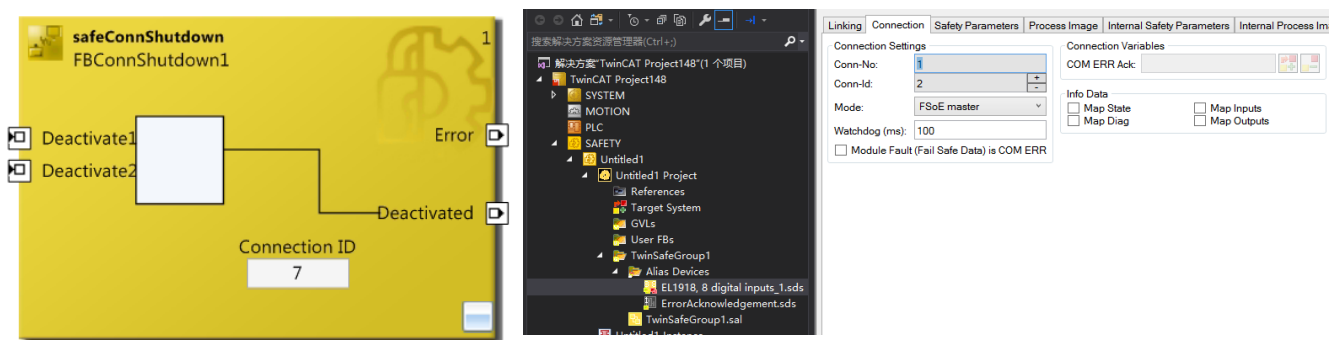
1.8.5 安全模块是否支持类似热连接的功能？

可以。

硬件配置上，将需要断开的 I/O 模块设置同步单元，避免影响到其它模块的 WcState。

安全工程上，安全模块的断开会导致对应的连接处于异常状态，同一 Group 下的安全程序会受到影响。可以通过如下方式解决：

- a. 创建不同 Group，避免安全 IO 的断开影响到其它 Group；
- b. 如果在同一个 Group 下，可以通过功能块断开与安全 IO 的连接，此时对应的 IO 连接的异常（包括断开）不会影响到 Group 里面的其它部分，其中功能块的 Connection ID 对应安全工程中模块的 Conn-Id；



1.8.6 Group 处于 startup 状态或者安全通讯异常

可以通过查看 FSoE 数据来判断，其中 CMD 含义如下

Safety over
EtherCAT

CMD

Safe Data

CRC_0

Safe Data

CRC_1

...

Conn ID

Kommando	Beschreibung
0x36	ProcessData
0x2A	Reset
0x4E	Session
0x64	Connection
0x52	Parameter
0x08	FailSafeData
0x78	Connection shutted down

Name	Online	Type	Size	> Addr...	In/Out	User ID	Linked to
Message_4 TxPDO X	2A 0 86 F8 00 00	Safety.FSO...	6.0	39.0	Input	0	FSOE . RxPDO . Module ...
Message_5 TxPDO X	4E 0A 6A 91 00 00	Safety.FSO...	6.0	45.0	Input	0	FSOE . RxPDO . Module ...
Message_8 TxPDO X	2A 05 59 6E 00 00	Safety.FSO...	6.0	51.0	Input	0	Message_4 RxPDO . Con...
Standard Out Va...	0	BIT	0.1	57.0	Input	0	GVL_10ms.bComErrorEL...
TwinSafeGroup1...	0x000002 (2)	INFODATA...	3.0	58.0	Input	0	
Message_4 Info ...	0x0000C564 (50532)	INFODATA...	4.0	61.0	Input	0	
Message_5 Info ...	0x0000C565 (50533)	INFODATA...	4.0	65.0	Input	0	
Message_8 Info ...	0x0000F564 (62820)	INFODATA...	4.0	69.0	Input	0	
TwinSafeGroup1...	0x0004 (4)	INFODATA...	2.0	73.0	Input	0	
Project CRC	0x8432	WORD	2.0	75.0	Input	0	
Serial Number	978484	UDINT	4.0	77.0	Input	0	
Safety Project St...	0x1 (1)	BIT3	0.3	81.0	Input	0	
Login Active	0	BIT	0.1	81.7	Input	0	
Input Size Mism...	0	BIT	0.1	82.0	Input	0	
Output Size Mis...	0	BIT	0.1	82.1	Input	0	
TxPDO State	0	BIT	0.1	82.6	Input	0	
TxPDO Toggle	1	BIT	0.1	82.7	Input	0	
WcState	0	BIT	0.1	1522.1	Input	0	
InputToggle	1	BIT	0.1	1524.1	Input	0	
State	8	UINT	2.0	3086.0	Input	0	
AdsAddr	5.36.70.177.6.1:1002	AMSADDR	8.0	3088.0	Input	0	
Message_4 RxPDO X	4E 5 72 CD 00 00	Safety.FSO...	6.0	39.0	Output	0	FSOE . TxPDO . Module ...
Message_5 RxPDO X	2A 0 86 F8 00 00	Safety.FSO...	6.0	45.0	Output	0	FSOE . TxPDO . Module ...
Message_8 RxPDO X	00 00 00 00 00 00	Safety.FSO...	6.0	51.0	Output	0	Message_4 TxPDO . Con...
Standard In Var 1	0	BIT	0.1	57.0	Output	0	GVL_10ms.bErrorAckEL6...
Standard In Var 2	1	BIT	0.1	57.1	Output	0	GVL_10ms.bRunStopEL6...
Standard In Var 7	0	BIT	0.1	57.2	Output	0	GVL_10ms.bRestartFbE...
Control	0	UINT	2.0	58.0	Output	0	

如果 TxPDO 和 RxPDO 在 0x2A 和 0x4E 之间跳变，则表示 startup 过程超时，可能原因包括：

通讯超时——检测安全模块所在的 Task 时间

确认安全参数以及地址

确保安全通讯的看门狗时间（默认为 100ms）大于 3 个 Task 时间

4.2.5 TwinSAFE reaction times

The TwinSAFE terminals form a modular safety system that exchanges safety-oriented data via the Safety-over-EtherCAT protocol. This chapter is intended to help you determine the system's reaction time from the change of signal at the sensor to the reaction at the actuator.

Typical reaction time

The typical reaction time is the time that is required to transmit information from the sensor to the actuator, if the overall system is working without error in normal operation.

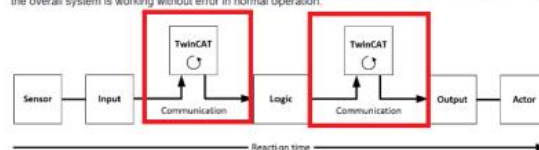


Fig. 11: Typical reaction time

Definition	Description
RTSensor	Reaction time of the sensor until the signal is provided at the interface. Typically supplied by the sensor manufacturer.
RTInput	Reaction time of the safe input, such as EL1904 or EP1908. This time can be found in the technical data. In the case of the EL1904 it is 4 ms.
RTComm	Reaction time of the communication. This is typically 3x the EtherCAT cycle time, because new data can only be sent in a new Safety-over-EtherCAT telegram. These times depend directly on the higher-level standard controller (cycle time of the PLC/NC).
RTLogic	Reaction time of the logic terminal. This is the cycle time of the logic terminal and typically ranges from 500 µs to 10 ms for the EL6900, depending on the size of the safety project. The actual cycle time can be read from the terminal.
RTOutput	Reaction time of the output terminal. This typically lies within the range of 2 to 3 ms.
RTActor	Reaction time of the actuator. This information is typically supplied by the actuator manufacturer.
WDComm	Watchdog time of the communication

This results in the following equation for the typical reaction time:

$$ReactionTime_{typ} = RT_{Sensor} + RT_{Input} + 3 \cdot RT_{Comm} + RT_{Logic} + 3 \cdot RT_{Comm} + RT_{Output} + RT_{Actor}$$

with, for example

$$ReactionTime_{typ} = 5ms + 4ms + 3 \cdot 1ms + 10ms + 3 \cdot 1ms + 3ms + 20ms = 49ms$$

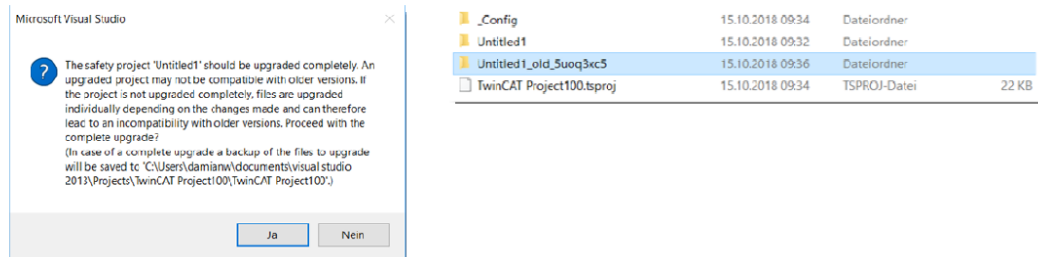
Worst-case reaction time

The worst case reaction time is the maximum time required to switch off the actuator in the case of an error.

如果 TxPDO 为 0X2A，RxPDO 为 0x00，则说明安全通讯没有反应，确认模块是否在

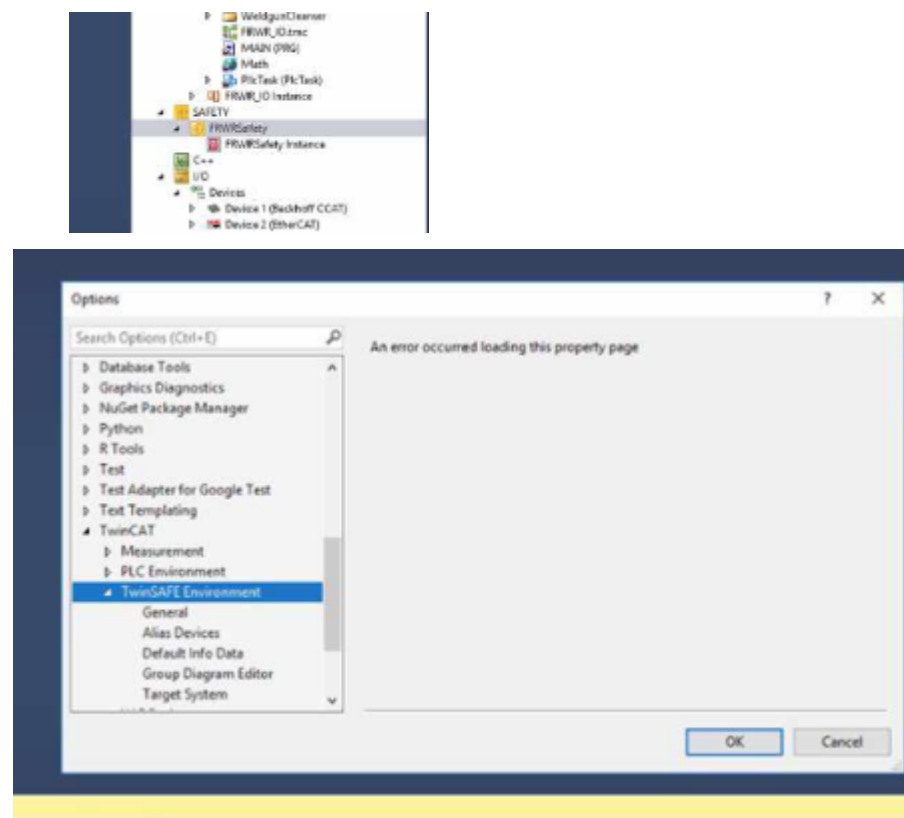
OP 状态, WcState 是否正常等。

1.8.7 安全工程版本问题

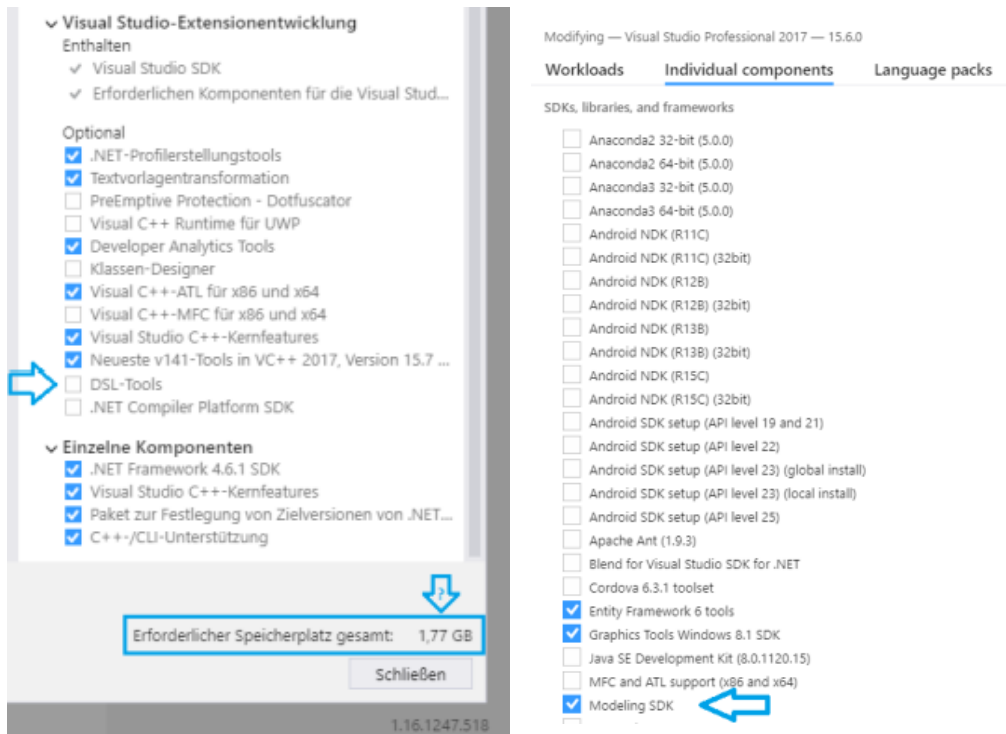


在某些 TwinCAT 版本中，打开低版本的工程会提示要求升级安全工程，其中升级后会在文件夹中保留老版本的工程备份。

1.8.8 无法创建安全工程或者打开已有的安全工程

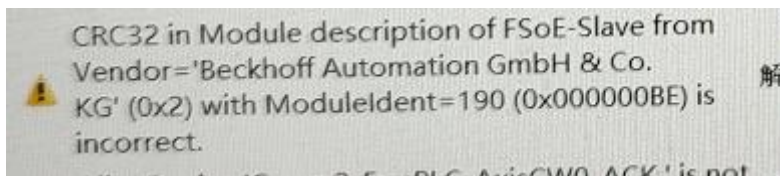


VS2017 或者 VS2019 中均有出现，默认安装策略导致，可以通过手动安装 DSL Tools/Modeling SDK 解决。可能安装选择中没有 DSL tools，选择安装 Modeling SDK，中文版本为“建模 SDK”

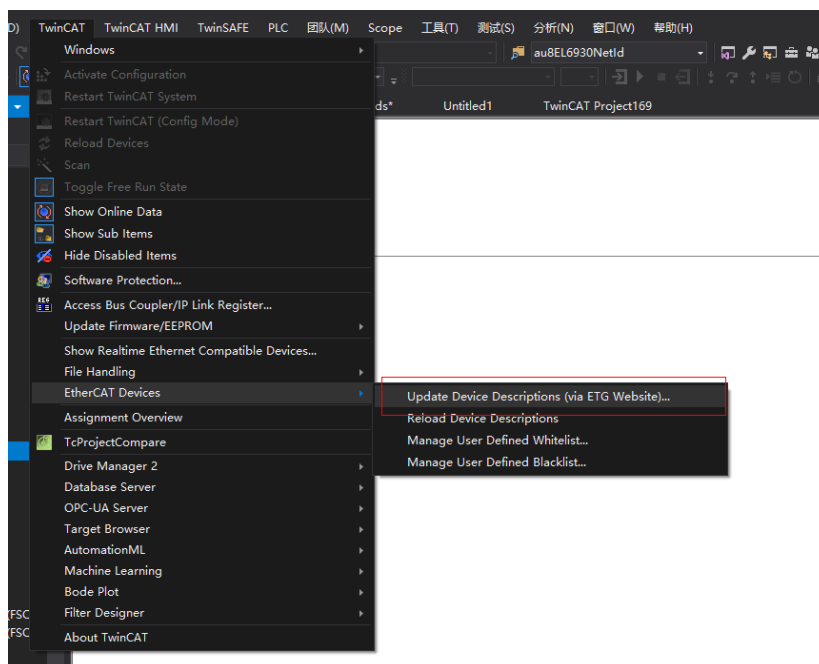


如果重装后依旧没有，卸载 TE9000 重装。

1.8.9 安全工程编译时报模块 CRC 错误



可以通过更新对应报错的安全模块描述文件解决。可以在官网手动下载更新或者在 TwinCAT 软件中直接进行更新。



1.8.10 The Feedback of the inactive Channel Switch is wrong. Module 0x2 /Channel:0x1

“新”的安全输出模块增加了输出电压检测，即使处于低电平状态。上述的文字说明模块的 Module 2 通道 1 在低电平输出状态是检测到电压在异常范围内。