BECKHOFF New Automation Technology

文档 | ZH

TwinSAFE 应用手册

安全功能的安全参数计算示例

2026-01-06 | 版本： 3.5.0

目录

1 文档说明

1.1 免责声明

倍福产品会持续进行更新。我们保留随时修改本文档的权利，恕不另行通知。不得根据本文档中的数据、图表和说明对已经提供的产品提出修改要求。

在本文档中，我们明确定义了所有可保障其属性与运行条件的合规用例。我们定义的用例均经过全面测试和认证。本文档中未描述的任何其他用例均需经过 Beckhoff Automation GmbH & Co KG 批准。

1.1.1 商标

Beckhoff®、TwinCAT®、TwinCAT/BSD®、TC/BSD®、EtherCAT®、EtherCAT G®、EtherCAT G10®、EtherCAT P®、Safety over EtherCAT®、TwinSAFE®、XFC®、XTS® 和 XPlanar® 是 Beckhoff Automation GmbH 的注册商标和许可商标。

如果第三方使用其他品牌名称或标识，可能会侵犯相关标识所有者的权利。

EtherCAT® 是注册商标和专利技术，由 Beckhoff Automation GmbH 授权使用。

Safety over EtherCAT® 是注册商标和专利技术，由 Beckhoff Automation GmbH 授权使用。

1.1.2 责任范围

操作说明书中描述的本产品的所有组件均根据应用规范以特定的软硬件配置交付。禁止未按文档所述更改和修改硬件和/或软件配置，Beckhoff Automation GmbH & Co. KG 不对此承担责任。

下列情况，我们不承担任何责任：

- 未遵守这些操作说明书
- 使用不当
- 使用未经培训的人员
- 使用未经授权的备件

1.1.3 版权所有

1.1.4 第三方商标

本文档可能使用了第三方商标。有关商标信息，可以访问：https://www.beckhoff.com/trademarks。

1.2 文档发行状态

版本	注释
3.5.0	• 在“速度监测（类别 3，PL d）”和“速度监测（通过 IO-Link）（类别 3，PL d）“章节中，增加了额外的 TwinSAFE SC 端子模块

版本	注释
3.4.0	• 增加了替代型 TwinSAFE SC 产品表格
3.3.0	• 增加了“带集成 EnDat 3 编码器的 AdvPosMon”应用示例 • 校正了拼写错误
3.2.0	• 在 T_1 的*术语解释*一章中，扩展了相关解释内容 • 增加了 *C9900-M800 应用示例*一章 • 更新了合规性确认
3.1.0	• 校正了文件结构：现已重新纳入*使用 TwinSAFE 组件规划安全项目*一章
3.0.0	• 增加了 PROFIsafe 示例 • 修订了文件结构 • 更新了合规性确认
2.2.0	• 更新了 EPP9022-9060 示例
2.1.0	• 迁移 • 增加了 AX8xxx、EL2911、EP1957 和 EPP9022-9060 示例 • 增加了培训课程信息 • 更新了合规性确认
2.0.0	• 增加了 EK1960 示例 • 校正了第 2.26 章中的计算
1.9.1	• 在第 2.17 章和第 2.18 章中增加了注释
1.9.0	• 修订了第 2.18 章 • 增加了*规划安全项目*一章
1.8.0	• 增加了 TwinSAFE SC 示例 • Bosch Rexroth IndraDrive 驱动器系列示例 • *SIL 2 通信*名称已更新为 *TwinSAFE SC* • 更新了 2.25 和 2.26 示例 • 全面修订了所有章节
1.7.0	• 修订了 *TwinSAFE 输出与 TwinSAFE 输入的直接接线（单通道）*一章 • 更新了前言 • 扩展了*目的和适用范围*一章 • 更新了第 2.25 章和第 2.26 章结构图 • 增加了第 2.27 章 • 为第 2.2.3.2 章、第 2.3.3.2 章、第 2.4.3.2 章、第 2.5.3.2 章、第 2.7.3.2 章和第 2.19.3.2 章添加了具体内容（删除了关于直接/间接回读的注释） • 在第 2.19 章中增加了注释文本
1.6.2	• 更新了合规性确认 • 更新了第 2.25 章和第 2.26 章中的图表 • 增加了*目的和适用范围*一章
1.6.1	• 增加了第 2.25 章和第 2.26 章
1.6.0	• 修订了第 2.17 章和第 2.18 章
1.5.0	• 增加了第 2.24 章 • 添加了文档版本 • 添加了文件来源 • 更改了格式设置
1.4.0	• 扩展了各章节标题，增加了类别与性能等级信息 • 在第 2.6 章中移动了注释

版本	注释
1.3.0	• 删除了交货条款
1.2.0	• 校正了第 2.6 章
1.1.0	• 首次发布版

1.3 员工资质

这些操作说明书专供经过培训且具备相关知识的控制技术和自动化领域中的专业人员使用。

经过培训的专业人员必须确保所述产品的应用和使用符合所有安全要求。这包括所有适用且有效的法律、法规、规定和标准。

受过培训的专业人员

经过培训的专业人员通过学习、学徒训练或技术培训掌握了丰富的技术知识。他们了解控制技术和自动化技术。受过培训的专业人员可以：

- 独立识别、避免和消除危险源。
- 应用相关的标准和指令。
- 实施事故预防规程的技术规范。
- 评估、准备和布置工作场地。
- 独立评估、优化和执行工作。

1.4 安全和说明

请阅读与使用产品执行的活动相关的内容。务必阅读操作说明书中的 章节。

遵守章节中的警告事项，从而能够按照预期和安全的方式处理和使用产品。

警示符号说明

为便于说明，书中使用了各种符号：

1. 编号表示应该执行的操作步骤。
- 项目符号点指示枚举项。

[…] 方括号指示对文档中其他文本段落的交叉引用。

[1] 方括号中的数字表示引用文档的编号。

文档中使用的警示信号词分类如下。

警示性词语

人身伤害警告

⚠ 危险

存在死亡或重伤的高度风险。

⚠ 警告

存在死亡或重伤的中度风险。

⚠ 谨慎

存在可能导致中度或轻度伤害的低度风险。

财产或环境损害警告

注意

注意

可能会损坏环境、设备或数据。

操作产品的信息

这些信息包括：
有关产品的操作、帮助或进一步信息的建议。

1.5 技术支持和服务

倍福公司及其合作伙伴在世界各地提供全面的技术支持和服务，对与倍福产品和系统解决方案相关的所有问题提供快速有效的帮助。

下载搜索器

我们的下载搜索器包含我们供您下载的所有文件。您可以通过它搜索我们的应用案例、技术文档、技术图纸、配置文件等等。

可供下载的文件格式多种多样。

倍福分公司和代表处

若需要倍福产品的本地支持和服务，请联系倍福分公司或代表处！

倍福遍布世界各地的分公司和代表处地址可在倍福官网上找到：http://www.beckhoff.com.cn

该网页还提供更多倍福产品组件的文档。

倍福技术支持

技术支持部门为您提供全面的技术援助，不仅帮助您应用各种倍福产品，还提供其他广泛的服务：

- 技术支持
- 复杂自动化系统的设计、编程和调试
- 以及倍福系统组件的各种培训课程

热线电话：	+49 5246 963-157
电子邮箱：	support@beckhoff.com

倍福售后服务

倍福服务中心提供所有售后服务：

- 现场服务
- 维修服务
- 备件服务
- 热线服务

热线电话：	+49 5246 963-460
电子邮箱：	service@beckhoff.com

倍福公司总部

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

电话：	+49 5246 963-0
电子邮箱：	info@beckhoff.com
网址：	www.beckhoff.com

1.6 信息安全说明

Beckhoff Automation GmbH & Co.KG (简称 Beckhoff) 的产品，只要可以在线访问，都配备了安全功能，支持工厂、系统、机器和网络的安全运行。尽管配备了安全功能，但为了保护相应的工厂、系统、机器和网络免受网络威胁，必须建立、实施和不断更新整个操作安全概念。Beckhoff 所销售的产品只是整个安全概念的一部分。客户有责任防止第三方未经授权访问其设备、系统、机器和网络。它们只有在采取了适当的保护措施的情况下，方可与公司网络或互联网连接。

此外，还应遵守 Beckhoff 关于采取适当保护措施的建议。关于信息安全和工业安全的更多信息，请访问本公司网站 https://www.beckhoff.com/secguide。

Beckhoff 的产品和解决方案持续进行改进。这也适用于安全功能。鉴于持续进行改进，Beckhoff 明确建议始终保持产品的最新状态，并在产品更新可用后马上进行安装。使用过时的或不支持的产品版本可能会增加网络威胁的风险。

如需了解 Beckhoff 产品信息安全的信息，请订阅 https://www.beckhoff.com/secinfo 上的 RSS 源。

2 安全说明

2.1 交付状态

所有产品在供货时都配有适用于应用类型的特定硬件和软件配置。严禁未按文档所述修改硬件或软件配置，否则，Beckhoff Automation GmbH & Co. KG 对由此产生的后果不承担责任。

2.2 操作员尽职尽责的义务

操作员必须确保

- TwinSAFE 产品只按设计用途使用（请参见“产品描述”一章）；
- TwinSAFE 产品只能在完好和正常的状态下运行。
- TwinSAFE 产品只能由具备相应资质并获得授权的人员操作。
- 相关人员定期接受有关职业安全和环境保护方面的培训，并熟悉操作手册，特别是其中的安全说明。
- 操作手册应完好、完整，并在 TwinSAFE 产品所在地随时可供查阅。
- TwinSAFE 产品附带的所有安全与警告说明均保留完整，所有注释内容均保持清晰可读。

2.3 目的和适用范围

本应用手册为用户提供了安全功能的安全参数的计算示例，相关计算依据 DIN EN ISO 13849-1 和 EN 62061 或 EN 61508:2010 标准（如适用）执行，涵盖机械设备领域的典型应用场景。

在这些示例中，EL1904 用作安全输入的典型代表，EL2904 用作安全输出的典型代表。此处仅作示例参考；当然也可以采用其他安全输入或输出，例如 EP1908 或 EL2912。在计算时必须使用相应的参数，这些参数可以从相应的产品文档中获取。

注意

应用程序示例

这些示例为用户提供了具体的计算实例。相关示例并不能免除用户执行风险与危害分析的责任，用户仍需依据具体应用场景遵循所有适用的指令、标准及法律法规。

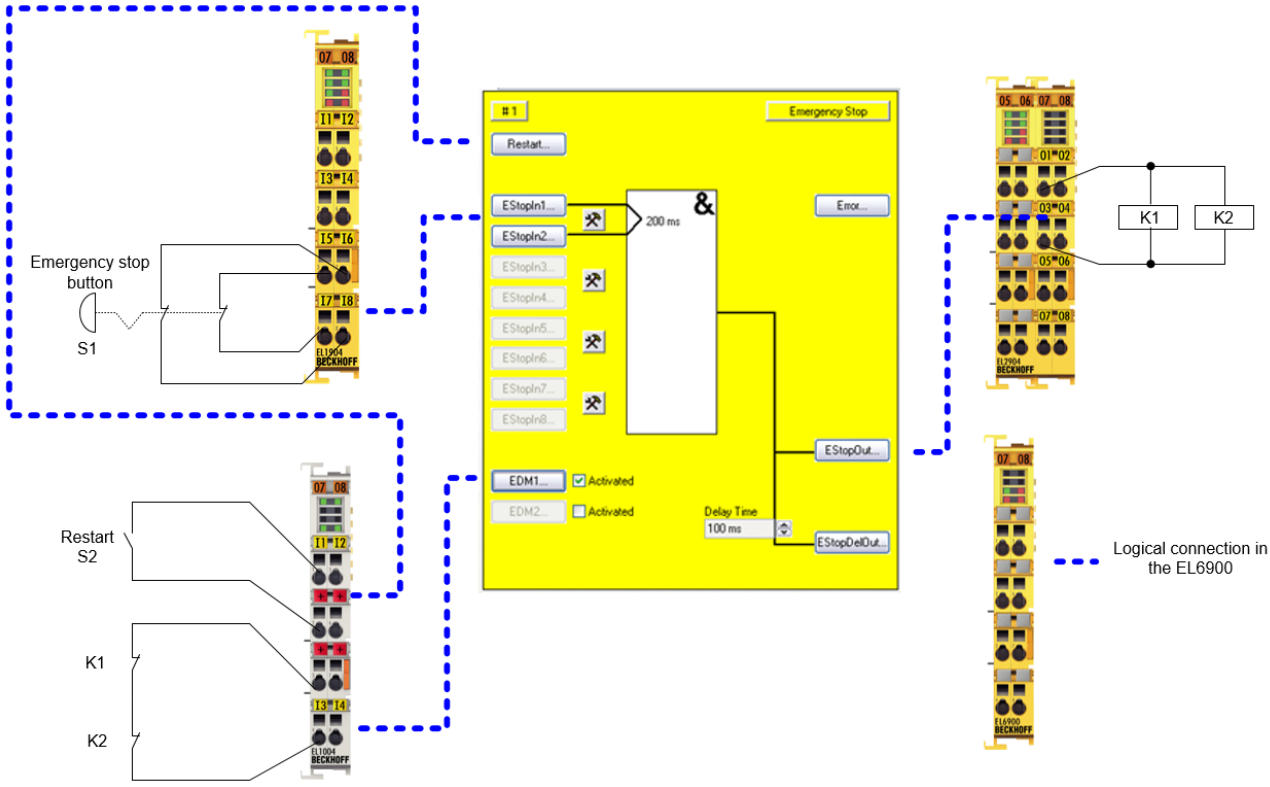
2.4 术语解释

名称	说明
$B10_D$	在 10% 的组件出现危险故障后，平均循环次数
CCF	具有共同原因的故障
d_{op}	每年平均运行时间（天）
DC_{avg}	平均诊断覆盖率
h_{op}	每天平均运行时间（小时）
$MTTF_D$	发生危险故障的平均时间
n_{op}	年平均执行次数
PFH_D	每小时发生危险故障的概率
PL	性能等级
PL_r	所需的性能等级
T_{cycle}	系统的两个连续循环之间的平均时间（在以下示例中以分钟为单位，但也可以秒为单位）
T_1	在验证测试间隔与使用寿命（TwinSAFE 设备通常为 20 年）之间取较小值
λ_D	以 FIT 为单位的危险故障率（10^9 个组件小时中的故障率）
T_{10D}	运行时间 - 例如，机电组件的最长运行时间
TwinSAFE SC	TwinSAFE SC 技术（SC - 单通道）可将来自标准端子模块的信号打包成 FSoE 报文，并通过标准现场总线传输到 TwinSAFE 逻辑。因此，可以排除传输路径上的伪造行为。在 TwinSAFE 逻辑中，该信号会通过另一个独立的信号进行检查。该比较结果通常会产生符合类别 3 和 PL d 的模拟值。 **该技术不支持数字量输入信号，不能用于单通道结构（只有一个 TwinSAFE SC 通道）。**

3 ESTOP 功能

3.1 ESTOP 功能变体 1（类别 3，PL d）

急停按钮通过两个常闭触点连接到 EL1904 安全输入端子模块。启动了对两个信号差异的测试与监控。重启和反馈信号均连接至标准端子模块，并通过标准 PLC 传输至 TwinSAFE。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



3.1.1 安全输入和输出端子模块的参数

EL1904

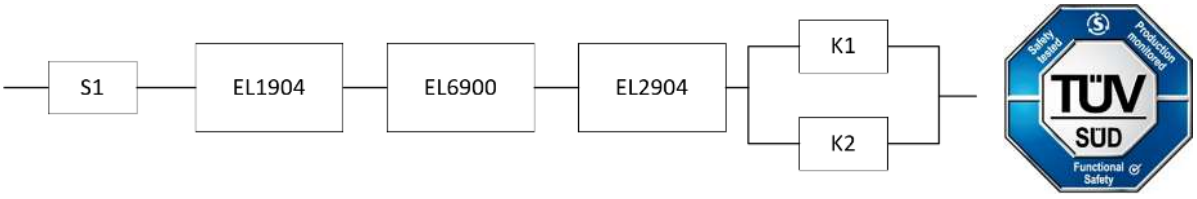
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

3.1.2 功能块结构和安全回路

3.1.2.1 安全功能 1



3.1.3 计算

3.1.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）（7 天，24 小时）
使用寿命（T1）	20 年 = 175200 小时

3.1.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
带测试和 EDM 的 K1/K2 （每周执行 1 次）	DC_{avg}=60%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=90%

3.1.3.3 安全功能 1 的计算

根据 $B10_d$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1*21,90} = 45662,1y = 399999120h$$

K1/K2

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1*21,90} = 593607,3y = 5199997320h$$

并假设 S1、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1*n_{op}*(1-DC)}{B10_D} = \frac{1-DC}{MTTF_D}$$

S1

$$PFH = \frac{1-0,99}{45662,1*8760} = 2,50E-11$$

K1/K2 每周执行 1 次

$$PFH = \frac{1-0,60}{593607,3*8760} = 7,69E-11$$

K1/K2 每班次执行 1 次

$$PFH = \frac{1-0,90}{593607,3*8760} = 1,92E-11$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 B10d 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2,5E-11+1,11E-09+1,03E-09+1,25E-09+10\%*\frac{7,96E-11+7,96E-11}{2} = 3,42E-09$$

在每周执行 1 次的情况下

或

$$PFH_{ges} = 2,5E-11+1,11E-09+1,03E-09+1,25E-09+10\%*\frac{1,92E-11+1,92E-11}{2} = 3,42E-09$$

在每班次执行 1 次的情况下

功能块 1 的 $MTTF_D$ 值（基于相同假设）通过以下公式计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n}\frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}}+\frac{1}{MTTF_{D(EL1904)}}+\frac{1}{MTTF_{D(EL6900)}}+\frac{1}{MTTF_{D(EL2904)}}+\frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1*n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1*n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{60\%}{593607,3y} + \frac{60\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,96\%$$

或：

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,99\%$$

⚠ 谨慎

达到类别 3 所需采取的措施！

由于继电器反馈路径中的错误可能不会被检测到，因此这种结构最多仅能达到类别 3。为了达到类别 3，所有上升沿和下降沿必须与控制器中的时间依赖性一起进行评估，以获得反馈预期！

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

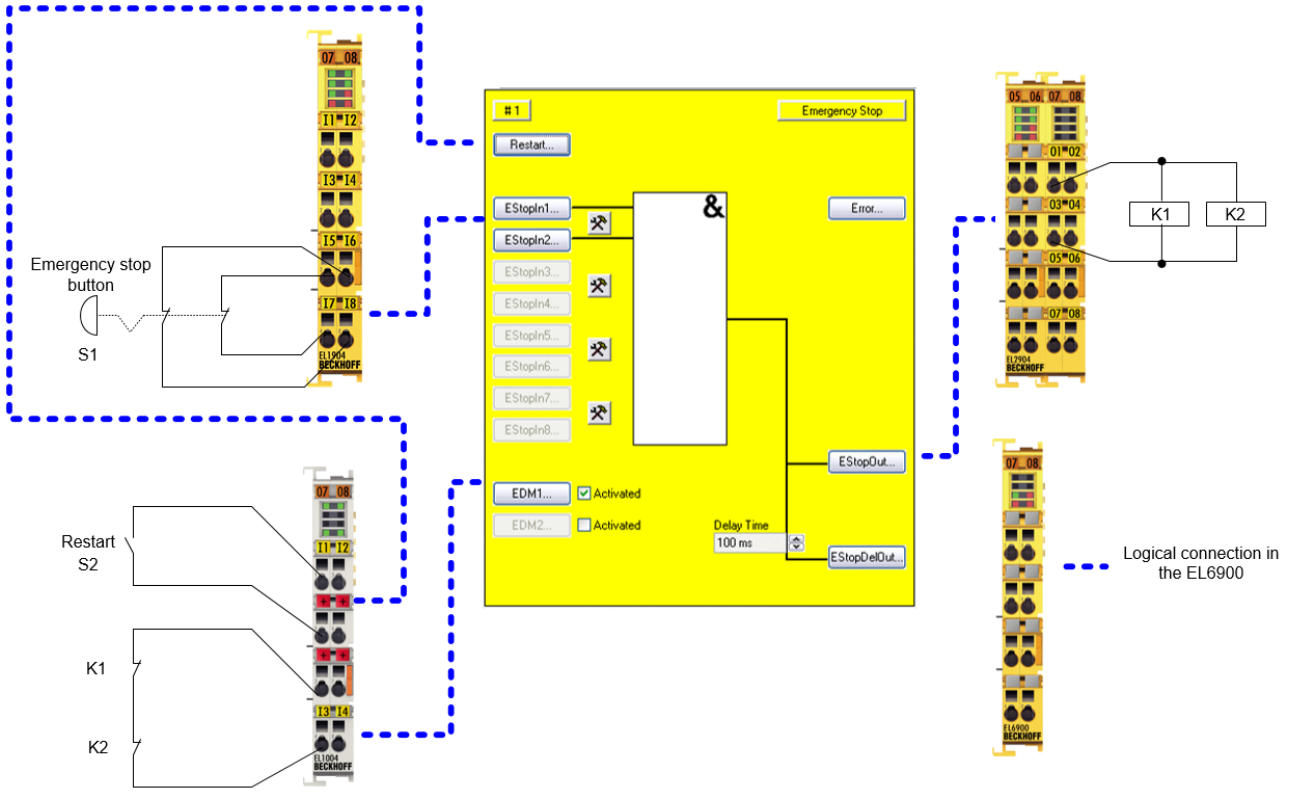
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.2 ESTOP 功能变体 2（类别 3，PL d）

急停按钮通过两个常闭触点连接到 EL1904 安全输入端子模块。启动了对两个信号的测试。这些信号**未**进行差异测试。重启和反馈信号均连接至标准端子模块，并通过标准 PLC 传输至 TwinSAFE。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



3.2.1 安全输入和输出端子模块的参数

EL1904

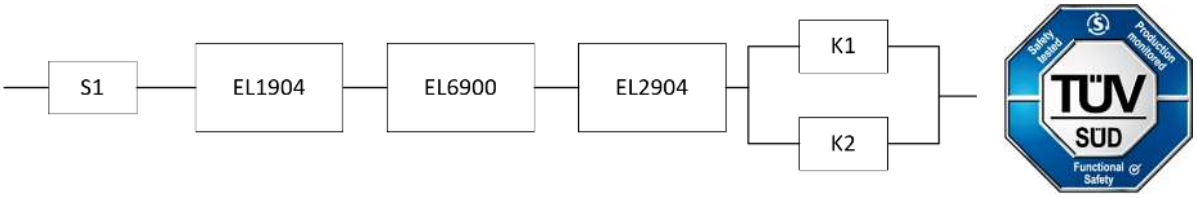
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

3.2.2 功能块结构和安全回路

3.2.2.1 安全功能 1



3.2.3 计算

3.2.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.2.3.2 诊断覆盖率 DC

组件	值
带测试/不带合理性检查的 S1	DC_{avg}=90%
带测试和 EDM 的 K1/K2 （每周执行 1 次）	DC_{avg}=60%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=90%

3.2.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

并假设 S1、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0,90}{45662,1 * 8760} = 2,50E - 10$$

K1/K2：每周执行 1 次

$$PFH = \frac{1 - 0,60}{593607,3 * 8760} = 7,69E - 11$$

K1/K2：每班次执行 1 次

$$PFH = \frac{1 - 0,90}{593607,3 * 8760} = 1,92E - 11$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2,5E-10 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{7,96E-11 + 7,96E-11}{2} = 3,65E-09$$

在每周执行 1 次的情况下

或

$$PFH_{ges} = 2,5E-10 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-11 + 1,92E-11}{2} = 3,65E-09$$

在每班次执行 1 次的情况下

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{60\%}{593607,3y} + \frac{60\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,89\%$$

或：

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,92\%$$

⚠ 谨慎

达到类别 3 所需采取的措施！

由于可能出现休眠错误，因此这种结构最多仅能达到类别 3。为了达到类别 3，所有上升沿和下降沿必须与控制器中的时间依赖性一起进行评估，以获得反馈预期。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

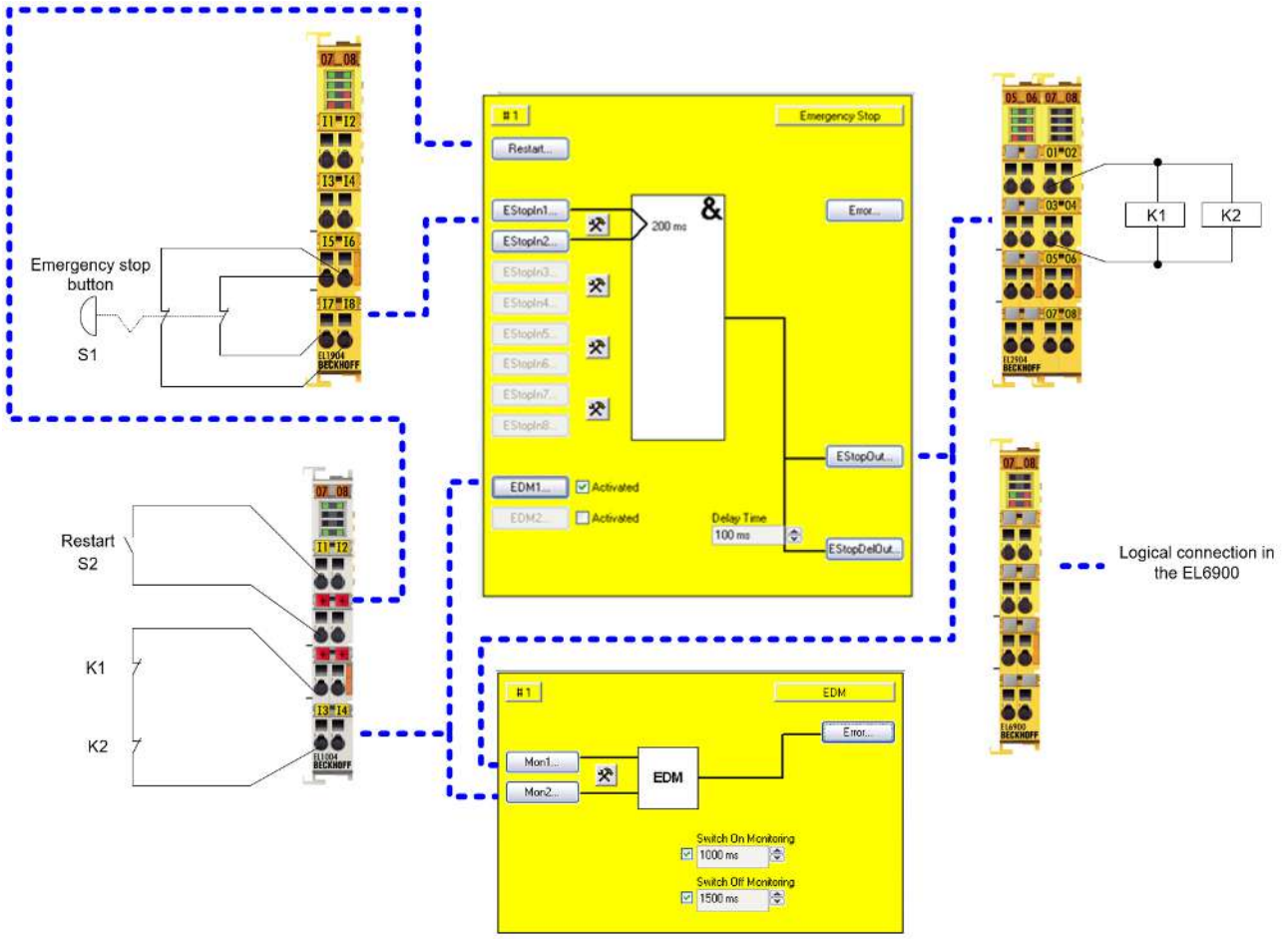
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.3 ESTOP 功能变体 3（类别 4，PL e）

急停按钮通过两个常闭触点连接到 EL1904 安全输入端子模块。启动了对两个信号的测试。这些信号已进行差异检查。重启和反馈信号均连接至标准端子模块，并通过标准 PLC 传输至 TwinSAFE。此外，ESTOP 功能块的输出与反馈信号均连接至 EDM 功能块。这样可以检查反馈信号是否在规定时间内转变为与 ESTOP 输出相反的状态。
接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



3.3.1 安全输入和输出端子模块的参数

EL1904

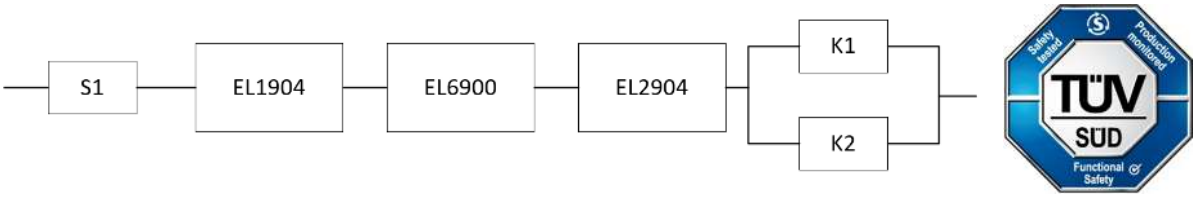
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

3.3.2 功能块结构和安全回路

3.3.2.1 安全功能 1



3.3.3 计算

3.3.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.3.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
带测试和 EDM 的 K1/K2 （每周执行 1 次）	DC_{avg}=90%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=99%

3.3.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662{,}1y = 399999120h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 21{,}90} = 593607{,}3y = 5199997320h$$

并假设 S1、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{45662{,}1 * 8760} = 2{,}50E - 11$$

K1/K2：每周执行 1 次

$$PFH = \frac{1 - 0{,}90}{593607{,}3 * 8760} = 1{,}92E - 11$$

K1/K2：每班次执行 1 次

$$PFH = \frac{1 - 0{,}99}{593607{,}3 * 8760} = 1{,}92E - 12$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 B10d 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2,5E-11 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-11 + 1,92E-11}{2} = 3,42E-09$$

在每周执行 1 次的情况下

或

$$PFH_{ges} = 2,5E-11 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2} = 3,42E-09$$

在每班次执行 1 次的情况下

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,99\%$$

或：

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 99,00\%$$

⚠ 谨慎

达到类别 4 所需采取的措施！

这种结构最多能达到类别 4。为了达到类别 4，所有上升沿和下降沿必须与控制器中的时间依赖性一起进行评估，以获得反馈预期！

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

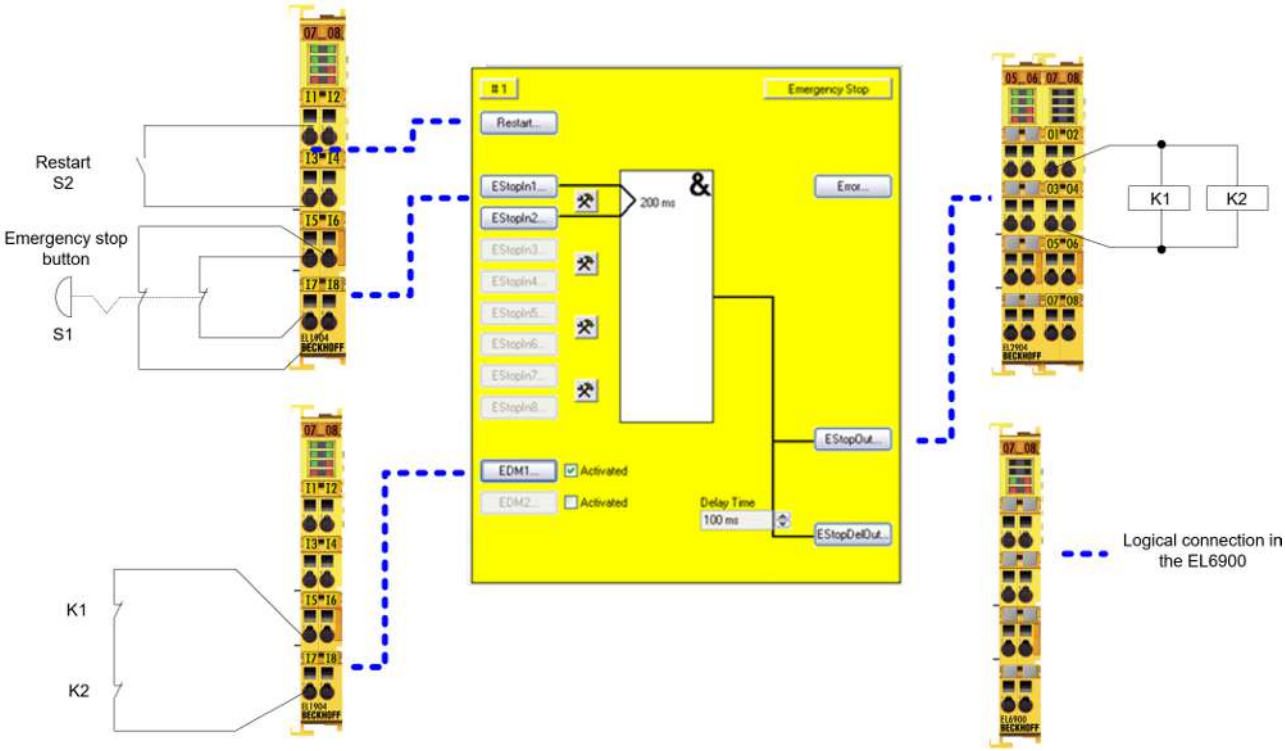
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.4 ESTOP 功能变体 4（类别 4，PL e）

带两个常闭触点的急停按钮、重启和反馈回路均连接至 EL1904 输入端子模块的安全通道。启动了对信号的测试。两个急停信号已进行差异测试。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



3.4.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

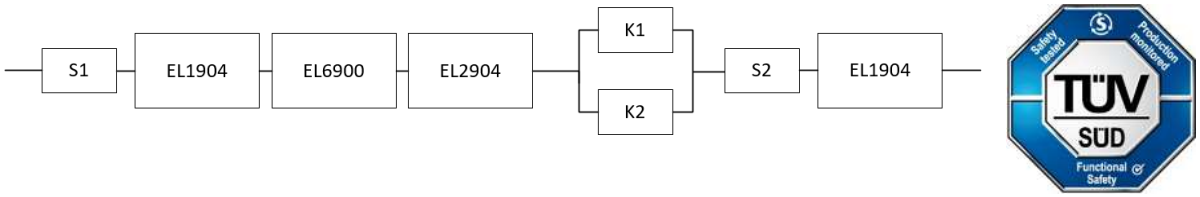
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

3.4.2 功能块结构和安全回路

3.4.2.1 安全功能 1



3.4.3 计算

3.4.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.4.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
带合理性检查的 S2	DC_{avg}=90%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=99%

3.4.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662{,}1y = 399999120h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{10.000.000}{0{,}1 * 21{,}90} = 4566210{,}0y = 4E10h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 21{,}90} = 593607{,}3y = 5199997320h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{45662{,}1 * 8760} = 2{,}50E - 11$$

S2：

$$PFH = \frac{1 - 0{,}90}{4566210{,}0 * 8760} = 2{,}50E - 12$$

K1/K2：每班次执行 1 次

$$PFH = \frac{1 - 0{,}99}{593607{,}3 * 8760} = 1{,}92E - 12$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)}$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2{,}5E-11 + 1{,}11E-09 + 1{,}03E-09 + 1{,}25E-09 + 10\% * \frac{1{,}92E-12 + 1{,}92E-12}{2} + 2{,}5E-12 + 1{,}11E-09 = 4{,}53E-09$$

在每班次执行 1 次的情况下

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0{,}1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,99\%$$

或：

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 99,00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

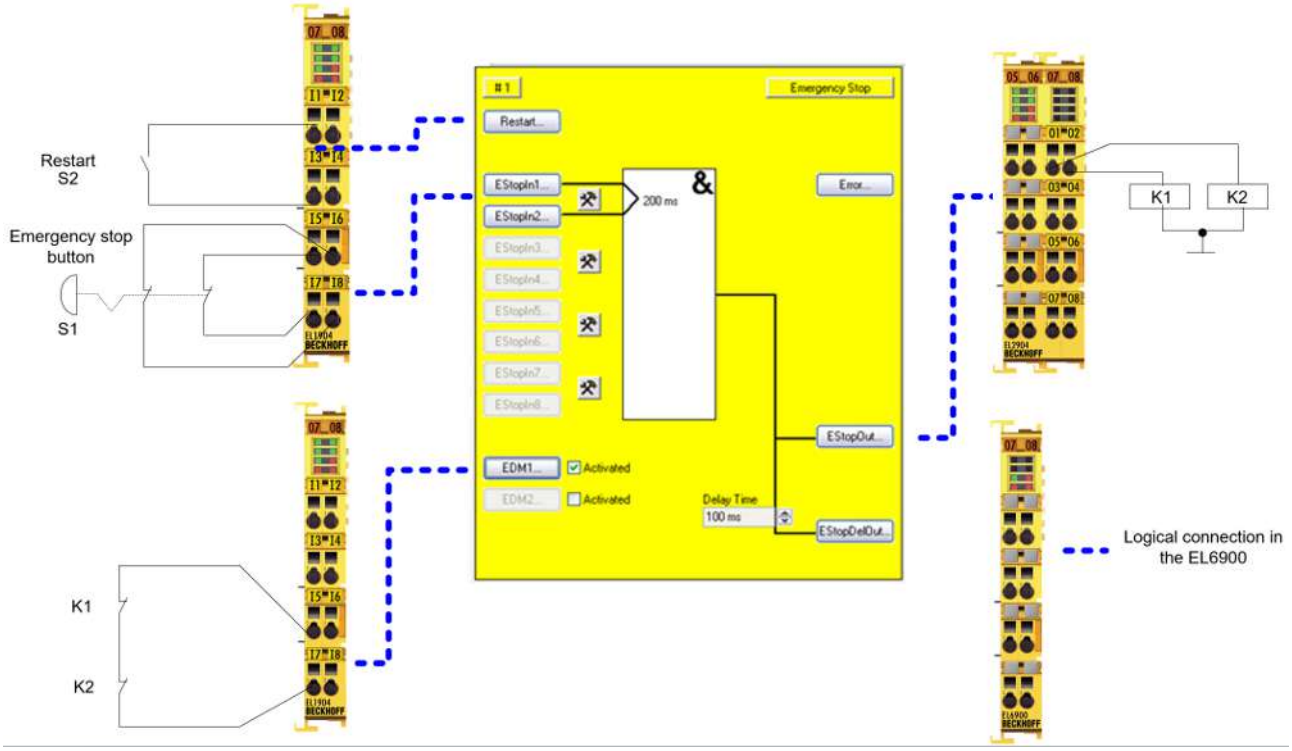
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.5 ESTOP 功能变体 5（类别 4，PL e）

带两个常闭触点的急停按钮、重启和反馈回路均连接至 EL1904 输入端子模块的安全通道。启动了对信号的测试。两个急停信号已进行差异测试。接触器 K1 和 K2 连接至不同的输出通道。两个接触器的 A2 连接点一并接地。该电路已停用输出通道的电流测量功能。输出测试已激活。



3.5.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

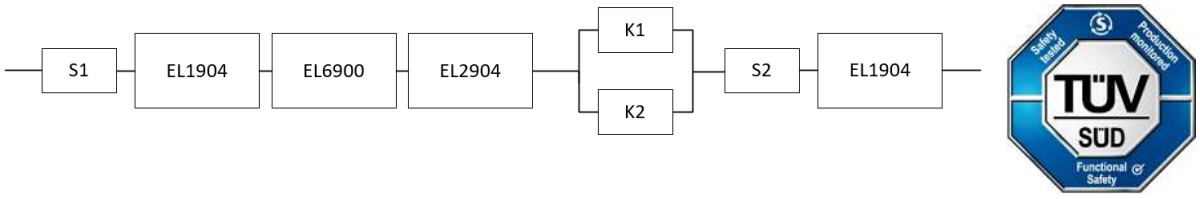
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

3.5.2 功能块结构和安全回路

3.5.2.1 安全功能 1



3.5.3 计算

3.5.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.5.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
带合理性检查的 S2	DC_{avg}=90%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=99%

3.5.3.3 安全功能 1 的计算

根据 $B10_d$ 值计算 PFH_D 和 $MTTF_d$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662{,}1y = 399999120h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{10.000.000}{0{,}1 * 21{,}90} = 4566210{,}0y = 4E10h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 21{,}90} = 593607{,}3y = 5199997320h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{45662{,}1 * 8760} = 2{,}50E - 11$$

S2：

$$PFH = \frac{1 - 0{,}90}{4566210{,}0 * 8760} = 2{,}50E - 12$$

K1/K2：每班次执行 1 次

$$PFH = \frac{1 - 0{,}99}{593607{,}3 * 8760} = 1{,}92E - 12$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 B10d 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)}$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2{,}5E-11 + 1{,}11E-09 + 1{,}03E-09 + 1{,}25E-09 + 10\% * \frac{1{,}92E-12 + 1{,}92E-12}{2} + 2{,}5E-12 + 1{,}11E-09 = 4{,}53E-09$$

在每班次执行 1 次的情况下

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0{,}1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{593607,3y}+\frac{1}{4566210,0y}+\frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}+\frac{99\%}{913,2y}+\frac{90\%}{593607,3y}+\frac{90\%}{593607,3y}+\frac{90\%}{4566210,0y}+\frac{99\%}{1028,8y}}{\frac{1}{45662,1y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{593607,3y}+\frac{1}{593607,3y}+\frac{1}{4566210,0y}+\frac{1}{1028,8y}} = 98,99\%$$

或：

$$DC_{avg} = \frac{\frac{99\%}{45662,1y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}+\frac{99\%}{913,2y}+\frac{99\%}{593607,3y}+\frac{99\%}{593607,3y}+\frac{90\%}{4566210,0y}+\frac{99\%}{1028,8y}}{\frac{1}{45662,1y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{593607,3y}+\frac{1}{593607,3y}+\frac{1}{4566210,0y}+\frac{1}{1028,8y}} = 99,00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

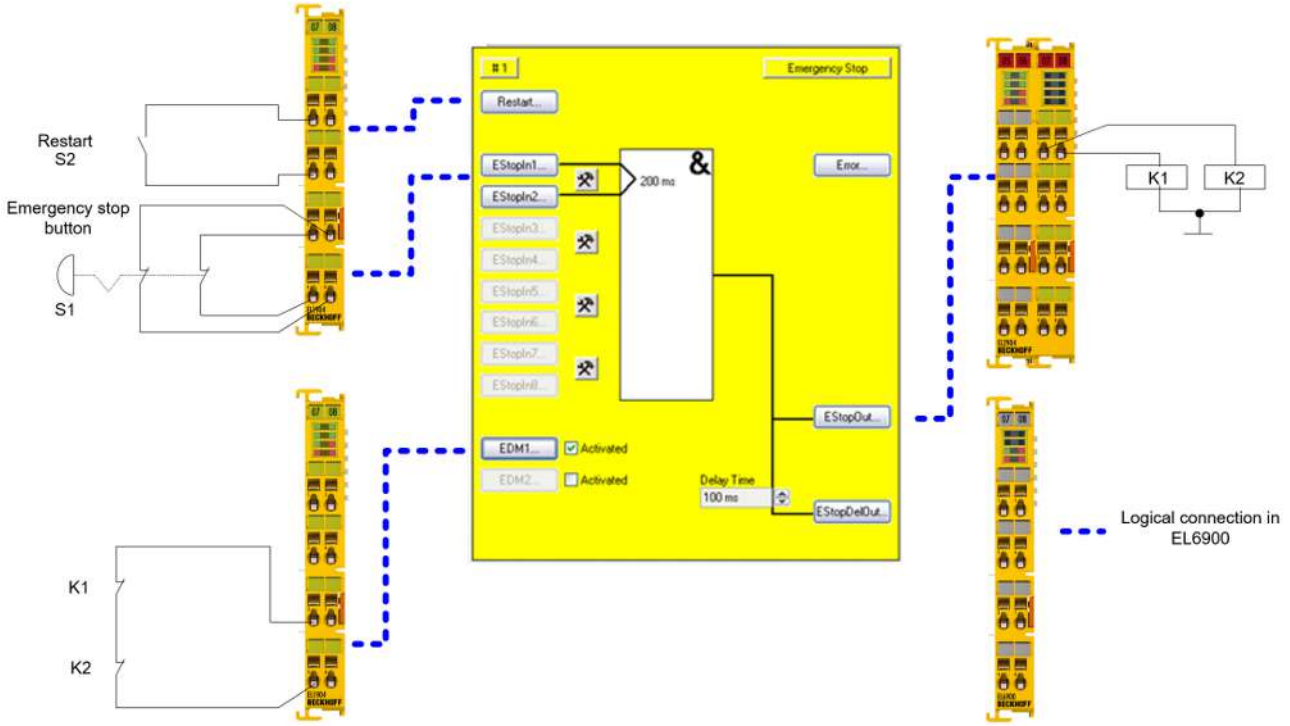
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.6 ESTOP 功能变体 6（类别 3，PL d）

带两个常闭触点的急停按钮、重启和反馈回路均连接至 EL1904 输入端子模块的安全通道。启动了对信号的测试。两个急停信号已进行差异测试。接触器 K1 和 K2 连接至不同的输出通道。两个接触器的 A2 连接点一并接地。该电路已停用输出通道的电流测量功能。输出测试未激活。



⚠ 谨慎

类别

由于可能出现休眠错误，因此这种结构最多仅能达到类别 3。

由于 EL2904 端子模块在此应用中仅支持 SIL2 等级，因此整个链的等级仅限于 SIL2！

3.6.1 安全输入和输出端子模块的参数（SIL 2）

EL1904（适用于所有使用的 EL1904）

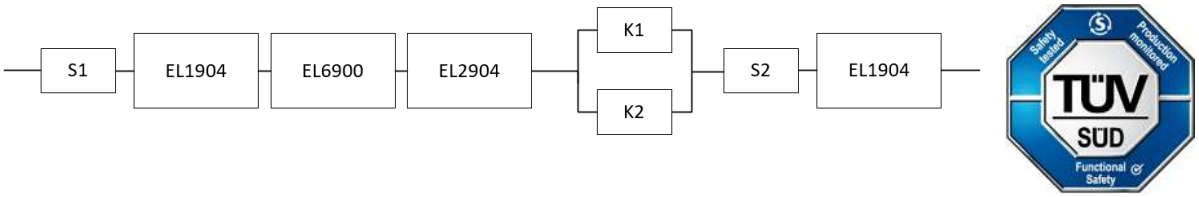
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	否

3.6.2 功能块结构和安全回路

3.6.2.1 安全功能 1



3.6.3 计算

3.6.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.6.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
带合理性检查的 S2	DC_{avg}=90%
K1/K2 不带测试，通过安全输入进行 EDM	DC_{avg}=90%

3.6.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1 * 21,90} = 45662,1y = 399999120h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{10.000.000}{0,1 * 21,90} = 4566210,0y = 4E10h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0,99}{45662,1 * 8760} = 2,50E - 11$$

S2：

$$PFH = \frac{1-0,90}{4566210,0*8760} = 2,50E-12$$

K1/K2：每班次执行 1 次

$$PFH = \frac{1-0,99}{593607,3*8760} = 1,92E-12$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)}$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2,5E-11 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2} + 2,5E-12 + 1,11E-09 = 4,53E-09$$

在每班次执行 1 次的情况下

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{99\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,99\%$$

⚠ 谨慎

类别

由于可能出现休眠错误，因此这种结构最多仅能达到类别 3。

由于 EL2904 端子模块在此应用中仅支持 SIL2 等级，因此整个链的等级仅限于 SIL2！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

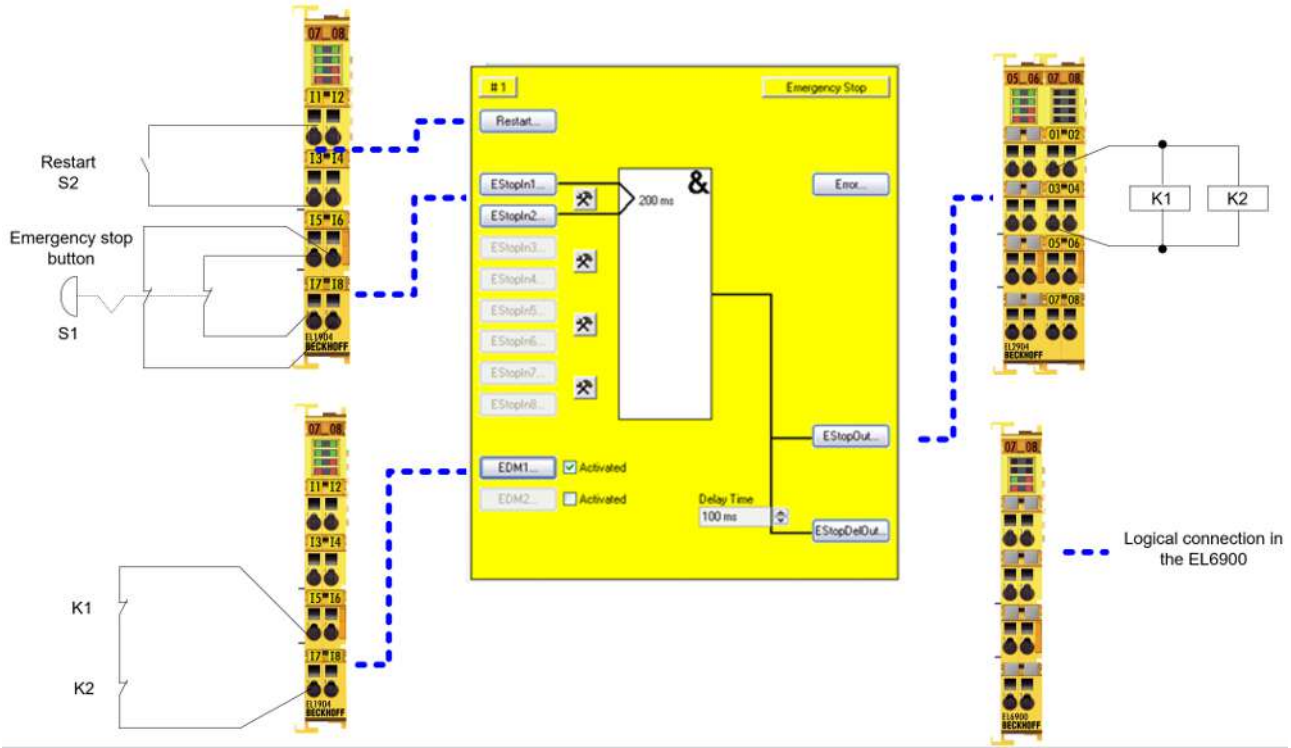
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

3.7 ESTOP 功能变体 7（类别 4，PL e）

带两个常闭触点的急停按钮、重启和反馈回路均连接至 EL1904 输入端子模块的安全通道。两个通道上的急停按钮测试功能均已停用。重启按钮和反馈回路的传感器测试功能已激活。两个急停信号已进行差异测试。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



3.7.1 安全输入和输出端子模块的参数

1. EL1904

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	未使用
传感器测试通道 3 激活	否
传感器测试通道 4 激活	否
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

2. EL1904

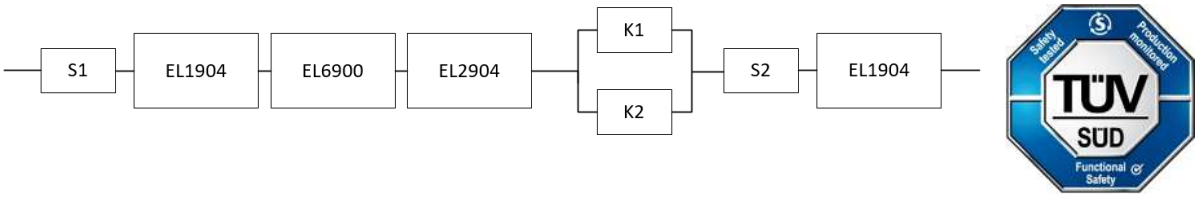
参数	值
传感器测试通道 1 激活	未使用
传感器测试通道 2 激活	未使用
传感器测试通道 3 激活	是
传感器测试通道 4 激活	未使用
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

3.7.2 功能块结构和安全回路

3.7.2.1 安全功能 1



3.7.3 计算

3.7.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.7.3.2 诊断覆盖率 DC

组件	值
带合理性检查的 S1	DC_{avg}=90%
带测试的 S2	DC_{avg}=90%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=99%

3.7.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662{,}1y = 399999120h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{10.000.000}{0{,}1 * 21{,}90} = 4566210{,}0y = 4E10h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 21{,}90} = 593607{,}3y = 5199997320h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}90}{45662{,}1 * 8760} = 2{,}50E - 10$$

S2：

$$PFH = \frac{1 - 0{,}90}{4566210{,}0 * 8760} = 2{,}50E - 12$$

K1/K2：每班次执行 1 次

$$PFH = \frac{1 - 0{,}99}{593607{,}3 * 8760} = 1{,}92E - 12$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)}$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2,5E-10 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2} + 2,5E-12 + 1,11E-09 = 4,75E-09$$

在每班次执行 1 次的情况下

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 252,1y$$

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,94\%$$

或：

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{593607,3y} + \frac{99\%}{593607,3y} + \frac{90\%}{4566210,0y} + \frac{99\%}{1028,8y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y} + \frac{1}{4566210,0y} + \frac{1}{1028,8y}} = 98,95\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

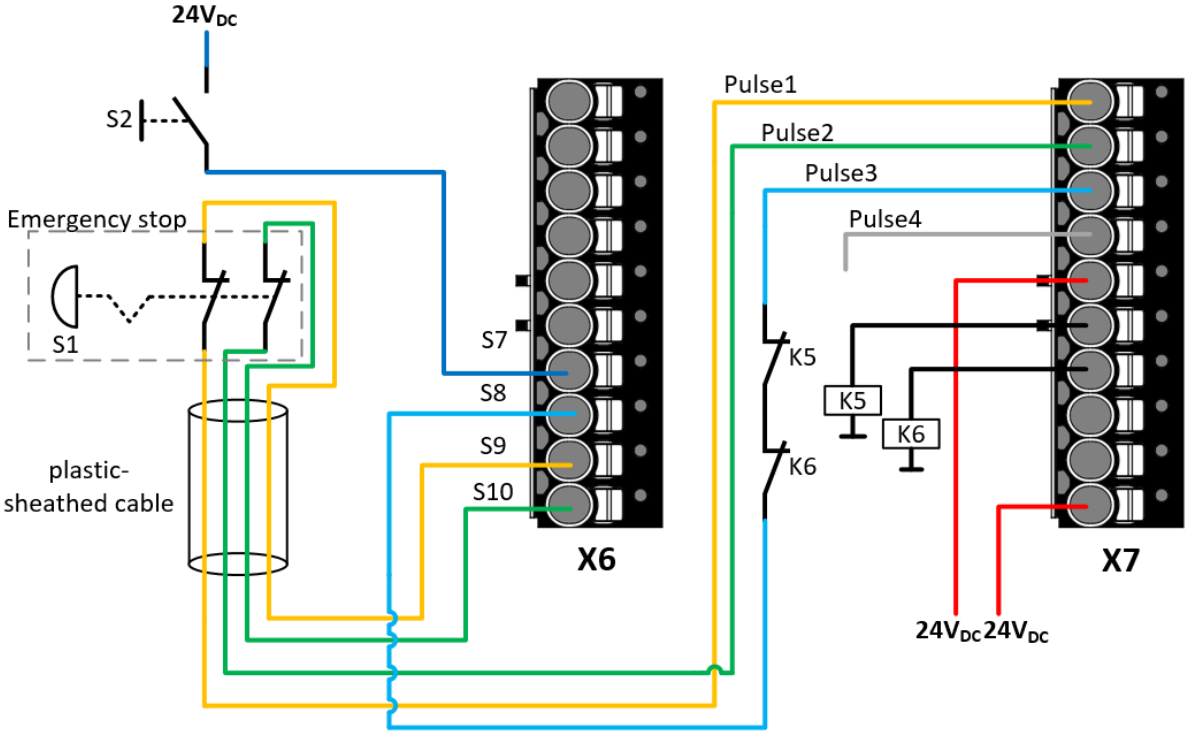
Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

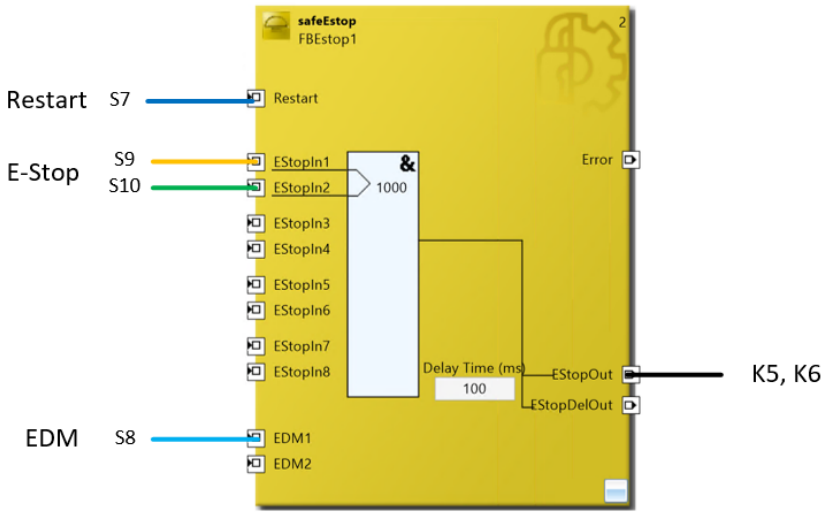
3.8 EK1960 数字量输入和输出（类别 4，PL e）

急停按钮 S1 通过两个常闭触点连接至 10 极 X6 连接器上的安全输入 S9 和 S10。10 极 X7 连接器上的第一个输出组被配置为时钟源（对于 FSOUT 模块 3，参数*输入诊断测试脉冲激活*被设置为 TRUE）。对于输入 S9 和 S10，根据相应的时钟源对参数*通道 x. 测试脉冲诊断模式*进行配置。

接触器 K5 和 K6 连接至 X7 上第二个输出模块上的输出 7.5 和 7.6。接触器的端子模块 A2 连接至端子模块 X7 的 24 V_{DC} 电源的公共地线。两个接触器的反馈回路串联连接，从脉冲 3 连接至输入 S8。

重启 S2 连接至安全输入 S7，不带测试。此应用必须配置重启选项，但该选项不纳入计算范畴。





3.8.1 安全输入和输出模块的参数

EK1960

参数	值
FSOUT 模块 3（X7.1 – X7.4）	-

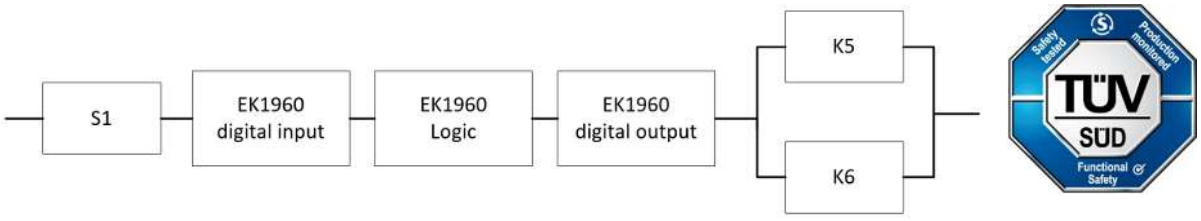
参数	值
8020:01 诊断测试脉冲模数	0x00
8020:02 诊断测试脉冲倍数	0x02
8020:03 标准输出激活	FALSE
8020:04 诊断测试脉冲激活	TRUE
8020:05 输入诊断测试脉冲激活	TRUE
FSOUT 模块 4（X7.5 – X7.8）	-
8030:01 诊断测试脉冲模数	0x00
8030:02 诊断测试脉冲倍数	0x02
8030:03 标准输出激活	FALSE
8030:04 诊断测试脉冲激活	TRUE
8030:05 输入诊断测试脉冲激活	FALSE
FSIN 模块 4	-
80A1:04 通道 2. 输入滤波时间	0x000C
80A1:05 通道 2. 诊断测试脉冲滤波时间	0x0002
80A1:06 通道 2. 测试脉冲诊断模式	（X7.3）测试脉冲检测输出模块 3. 通道 3
FSIN 模块 5	-
80B1:01 通道 1. 输入滤波时间	0x000C
80B1:02 通道 1. 诊断测试脉冲滤波时间	0x0002
80B1:03 通道 1. 测试脉冲诊断模式	（X7.1）测试脉冲检测输出模块 3. 通道 1
80B1:04 通道 2. 输入滤波时间	0x000C
80B1:05 通道 2. 诊断测试脉冲滤波时间	0x0002
80B1:06 通道 2. 测试脉冲诊断模式	（X7.2）测试脉冲检测输出模块 3. 通道 2

ESTOP FB 参数

参数	值
复位时间（ms）（端口 EDM1）	1000
偏差时间（ms）（端口 EStopIn1/EStopIn2）	1000
偏差错误后的安全输入	TRUE

3.8.2 功能块结构和安全回路

3.8.2.1 安全功能 1



3.8.3 计算

3.8.3.1 PFHD / MTTFD / B10D – 值

组件	值
EK1960 数字量输入 – PFH_D	6.40E-11

组件	值
EK1960 安全垫输入 - PFH_D	8.84E-10
EK1960 逻辑 – PFH_D	5.18E-09
EK1960 数字量输 – PFH_D	1.50E-10
EK1960 继电器输出（cat. 4，双通道） - PFH_D	1.46E-09（每小时执行 1 次）
EK1960 继电器 – $B10_D$	1,500,000（DC13 24 V_{DC} 和 I_{max} ≤ 2 A）
S1 – $B10_D$	100,000
K5 – $B10_D$	1,300,000
K6 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

Safety over EtherCAT 通信

Safety over EtherCAT（FSoE）通信的 PFH_D 值包含在 EK1960 逻辑组件的 PFH_D 值中。

3.8.3.2 诊断覆盖率 DC

组件	值
带测试和合理性检查的 S1	DC_{avg}=99%
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行时序监测评估）和测试的 K5/K6	DC_{avg}=99%

3.8.3.3 安全功能 1 的计算

根据 EN ISO 13849-1:2015 标准计算性能等级

根据 $B10_D$ 值计算 $MTTF_D$ 值

从：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662y$$

K5/K6

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 21{,}90} = 593607y$$

根据以下公式计算总 $MTTF_D$ 值：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EK1960-Input)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Output)}} + \frac{1}{MTTF_{D(K5)}}$$

如果仅有 EK1960 组件的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(EK1960-xxx)} = \frac{(1 - DC_{(EK1960-xxx)})}{PFH_{(EK1960-xxx)}}$$

因此：

$$MTTF_{D(EK1960-Input)} = \frac{(1 - DC_{(EK1960-Input)})}{PFH_{D(EK1960-Input)}} = \frac{(1 - 0{,}99)}{6{,}40E-11\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{5{,}60E-07\frac{1}{y}} = 17836y$$

$$MTTF_{D(EK1960-Logic)} = \frac{(1 - DC_{(EK1960-Logic)})}{PFH_{D(EK1960-Logic)}} = \frac{(1 - 0{,}99)}{5{,}18E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{4{,}54E-05\frac{1}{y}} = 220y$$

$$MTTF_{D(EK1960-Output)} = \frac{(1 - DC_{(EK1960-Output)})}{PFH_{D(EK1960-Output)}} = \frac{(1 - 0{,}99)}{1{,}50E-10\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}31E-06\frac{1}{y}} = 7610y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{593607y}} = 210y$$

$$DC_{avg} = \frac{\frac{99\%}{45662y} + \frac{99\%}{17836y} + \frac{99\%}{220y} + \frac{99\%}{7610y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

注意

类别

这种结构最多能达到类别 4。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能**不**属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%

DC	
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN 62061 标准计算 PFH_D 值

假设 S1、K5 和 K6 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH_D = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH_D = \frac{1 - 0{,}99}{45662 * 8760} = 2{,}50E - 11$$

K5/K6：

$$PFH_D = \frac{1 - 0{,}99}{593607 * 8760} = 1{,}92E - 12$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K5 和 K6 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K5 和 K6 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{Dges} = PFH_{D(S1)} + PFH_{D(EK1960-Input)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Output)} + \beta * \frac{PFH_{D(K5)} + PFH_{D(K6)}}{2} + (1 - \beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{Dges} = 2,5E-11 + 6,40E-11 + 5,18E-09 + 1,50E-10 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 5,42E-09$$

安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	**≥ 10^{-8} 至 < 10^{-7}**
2	≥ 10^{-7} 至 < 10^{-6}
1	≥ 10^{-6} 至 < 10^{-5}

注意

安全完整性等级

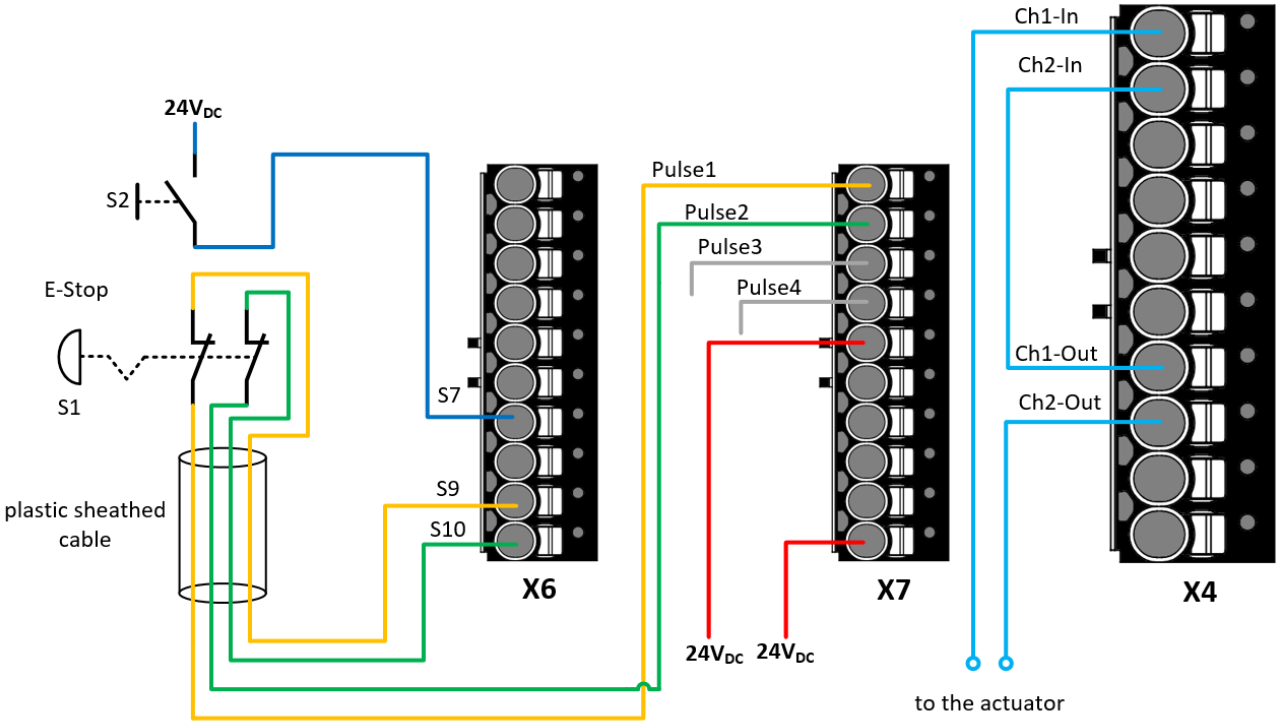
该应用符合 EN 62061 标准的安全完整性等级 SIL3 要求。

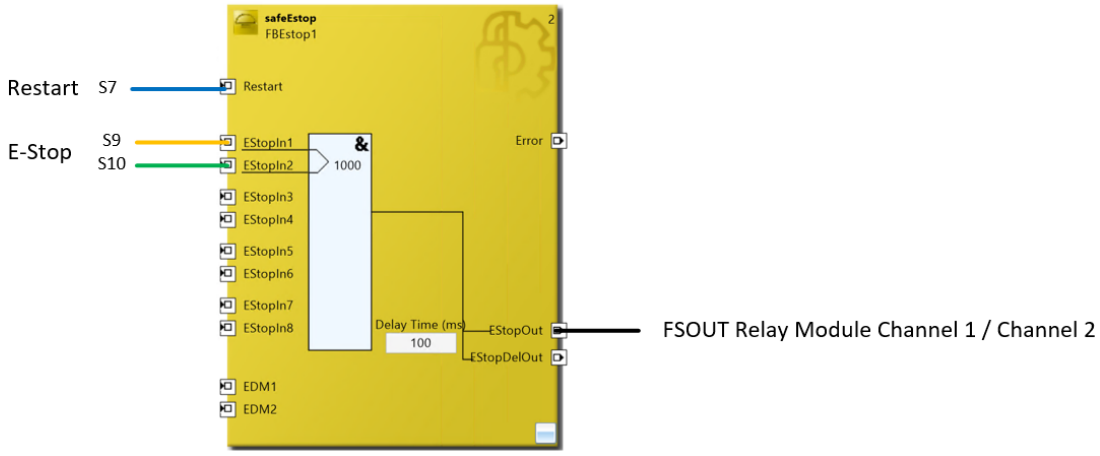
3.9 EK1960 数字量输入/继电器输出（类别 4，PL e）

急停按钮 S1 通过两个常闭触点连接至 10 极 X6 连接器上的安全输入 S9 和 S10。10 极 X7 连接器上的第一个输出组被配置为时钟源（对于 FSOUT 模块 3，参数*输入诊断测试脉冲激活*被设置为 TRUE）。对于输入 S9 和 S10，根据相应的时钟源对参数*通道 x. 测试脉冲诊断模式*进行配置。

继电器输出通道 1 和通道 2 串联连接，可用于安全相关功能（例如，向上游或下游设备传递急停消息）。EDM 未连接至 ESTOP 输入，因为继电器模块执行 EDM 监控，并在发生错误时报告继电器模块的模块错误。之后，应用程序可以对该模块错误做出响应，或者可以对 TwinSAFE 组进行配置，使模块错误触发通信错误。

重启 S2 连接至安全输入 S7，不带测试。此应用必须配置重启选项，但该选项不纳入计算范畴。





3.9.1 安全输入和输出模块的参数

EK1960

参数	值
FSOUT 模块 3（X7.1 – X7.4）	-
8020:01 诊断测试脉冲模数	0x00

参数	值
8020:02 诊断测试脉冲倍数	0x02
8020:03 标准输出激活	FALSE
8020:04 诊断测试脉冲激活	TRUE
8020:05 输入诊断测试脉冲激活	TRUE
FSOUT 继电器模块	-
8060:03 标准输出激活	FALSE
FSIN 模块 5	-
80B1:01 通道 1. 输入滤波时间	0x000C
80B1:02 通道 1. 诊断测试脉冲滤波时间	0x0002
80B1:03 通道 1. 测试脉冲诊断模式	（X7.1）测试脉冲检测输出模块 3. 通道 1
80B1:04 通道 2. 输入滤波时间	0x000C
80B1:05 通道 2. 诊断测试脉冲滤波时间	0x0002
80B1:06 通道 2. 测试脉冲诊断模式	（X7.2）测试脉冲检测输出模块 3. 通道 2

ESTOP FB 参数

参数	值
复位时间（ms）（端口 EDM1）	1000
偏差时间（ms）（端口 EStopIn1/EStopIn2）	1000
偏差错误后的安全输入	TRUE

注意

继电器模块中的模块错误

如果出现 EDM 错误，则报告继电器模块的模块错误。然后，该模块进入安全关断状态。通过信号 *FSOUT Relais Module.Err Ack* 可以进行错误确认。

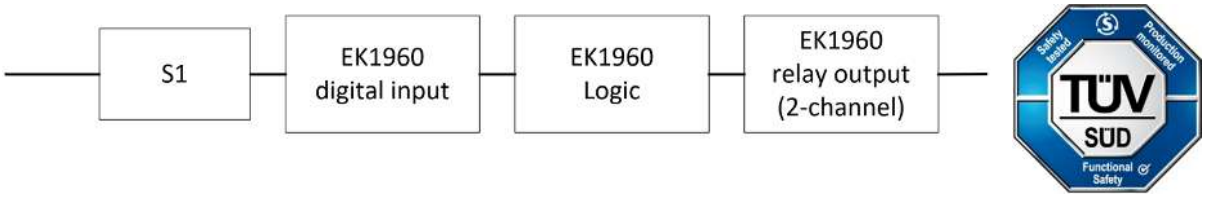
注意

开关频率

为了达到 PL e，必须每月至少激活一次继电器输出。本示例假定开关频率为每周 1 次。

3.9.2 功能块结构和安全回路

3.9.2.1 安全功能 1



3.9.3 计算

3.9.3.1 PFHD / MTTFD / B10D – 值

组件	值
EK1960 数字量输入 – PFH_D	6.40E-11

组件	值
EK1960 安全垫输入 - PFH_D	8.84E-10
EK1960 逻辑 – PFH_D	5.18E-09
EK1960 数字量输 – PFH_D	1.50E-10
EK1960 继电器输出（cat. 4，双通道） - PFH_D	1.46E-09（每小时执行 1 次）
EK1960 继电器 – $B10_D$	1,500,000（DC13 24 V_{DC} 和 I_{max} ≤ 2 A）
S1 – $B10_D$	100,000
K5 – $B10_D$	1,300,000
K6 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

Safety over EtherCAT 通信

Safety over EtherCAT（FSoE）通信的 PFH_D 值包含在 EK1960 逻辑组件的 PFH_D 值中。

3.9.3.2 诊断覆盖率 DC

组件	值
带测试和合理性检查的 S1	DC_{avg}=99%
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估）和测试的双通道继电器输出	DC_{avg}=99%

3.9.3.3 安全功能 1 的计算

根据 EN ISO 13849-1:2015 标准计算性能等级：

根据 $B10_D$ 值计算 $MTTF_D$ 值。

从：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662y$$

继电器

为继电器同时规定了 $B10_D$ 和 PFH_D 值。在这种情况下，使用两个值中的较低值来计算 $MTTF_D$ 值（在本示例中为 PFH_D 值 – 请参见下文）。

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{1.500.000}{0,1*21,90} = 684.931y$$

根据以下公式计算总 $MTTF_D$ 值：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EK1960-Input)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Relay)}}$$

如果仅有 EK1960 组件的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(EK1960-xxx)} = \frac{(1-DC_{(EK1960-xxx)})}{PFH_{(EK1960-xxx)}}$$

因此：

$$MTTF_{D(EK1960-Input)} = \frac{(1-DC_{(EK1960-Input)})}{PFH_{D(EK1960-Input)}} = \frac{(1-0,99)}{6,40E-11\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{5,60E-07\frac{1}{y}} = 17836y$$

$$MTTF_{D(EK1960-Logic)} = \frac{(1-DC_{(EK1960-Logic)})}{PFH_{D(EK1960-Logic)}} = \frac{(1-0,99)}{5,18E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{4,54E-05\frac{1}{y}} = 220y$$

$$MTTF_{D(EK1960-Relay)} = \frac{(1-DC_{(EK1960-Relay)})}{PFH_{D(EK1960-Relay)}} = \frac{(1-0,99)}{1,46E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,28E-05\frac{1}{y}} = 781y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{781y}} = 169y$$

$$DC_{avg} = \frac{\frac{99\%}{45662y} + \frac{99\%}{17836y} + \frac{99\%}{220y} + \frac{99\%}{781y}}{\frac{1}{45662y} + \frac{1}{17836y} + \frac{1}{220y} + \frac{1}{781y}} = 99,00\%$$

注意

类别

这种结构最多能达到类别 4。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能**不**属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**
DC	
名称	**范围**

$MTTF_D$	
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN 62061 标准计算 PFH_D 值：

假设 S1 为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH_D = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH_D = \frac{1 - 0{,}99}{45662 * 8760} = 2{,}50E - 11$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{Dges} = PFH_{D(S1)} + PFH_{D(EK1960-Input)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Relay)}$$

至：

$$PFH_{Dges} = 2{,}5E - 11 + 6{,}40E - 11 + 5{,}18E - 09 + 1{,}46E - 09$$
$$= 6{,}73E - 09$$

安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	**⩾ 10^{-8} 至 < 10^{-7}**
2	⩾ 10^{-7} 至 < 10^{-6}
1	⩾ 10^{-6} 至 < 10^{-5}

注意

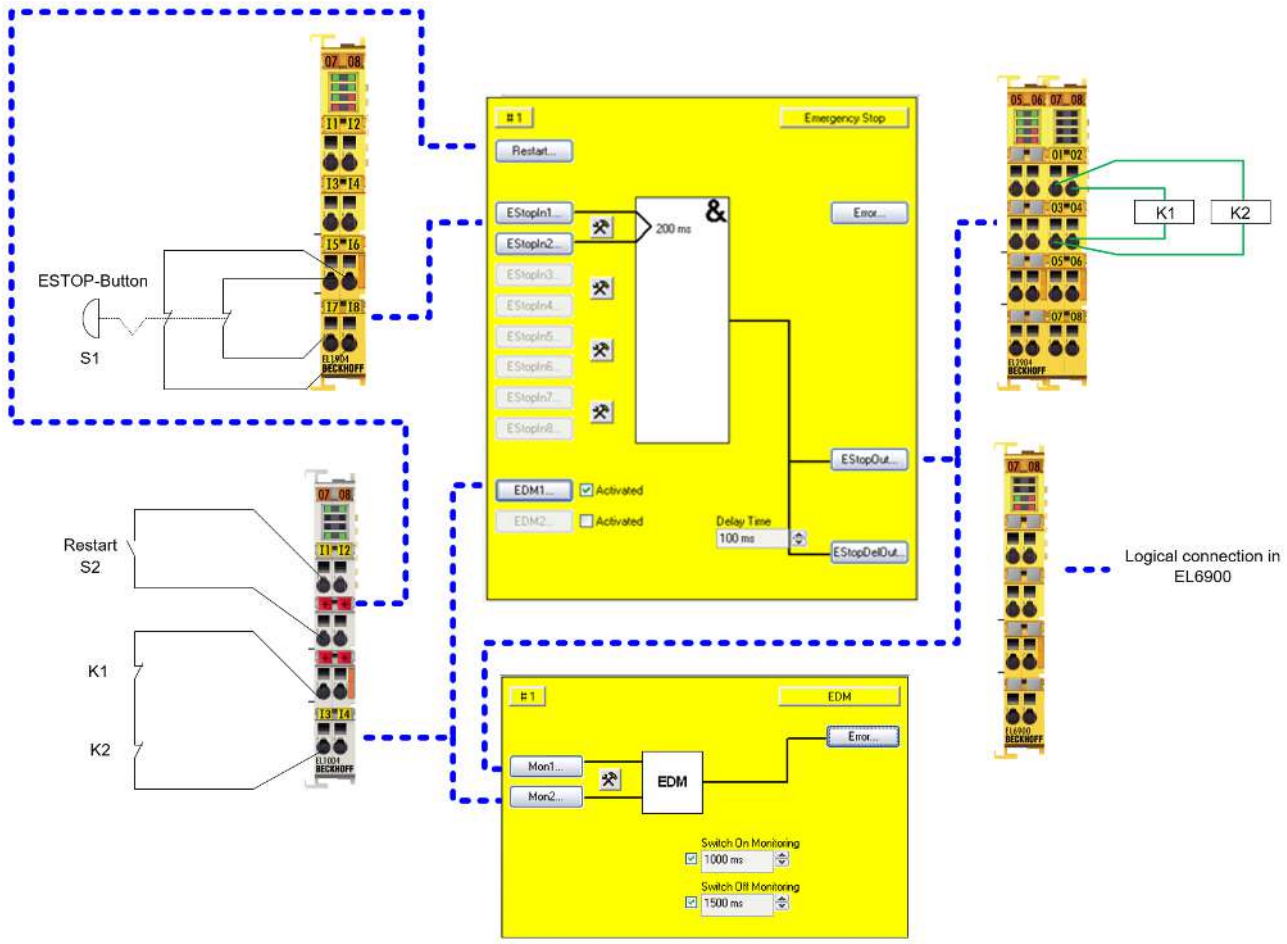
安全完整性等级

该应用符合 EN 62061 标准的安全完整性等级 SIL 3 要求。

3.10 ESTOP 功能（类别 3，PL d）

急停按钮通过两个常闭触点连接到 EL1904 安全输入端子模块。两个信号的测试功能均已关闭。在 ESTOP 功能块内部会对这些信号进行差异测试。接触器 K1 和 K2 中的重启和反馈信号均连接至标准端子模块，并通过标准 PLC 传输至 TwinSAFE。此外，ESTOP 功能块的输出与反馈信号均连接至 EDM 功能块。这样可以检查反馈信号是否在规定时间内转变为与 ESTOP 输出相反的状态。

接触器 K1 和 K2 连接至不同的输出通道。两个接触器的 A2 连接点反馈回到 EL2904。该电路已停用输出通道的电流测量功能。输出测试同样未激活。



3.10.1 安全输入和输出端子模块的参数（SIL 2）

EL1904（适用于所有使用的 EL1904）

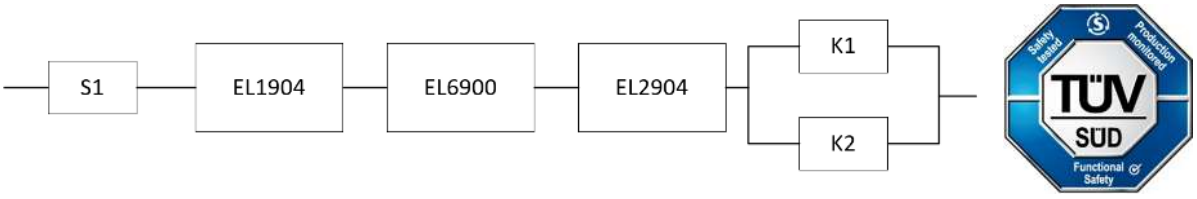
参数	值
传感器测试通道 1 激活	-
传感器测试通道 2 激活	-
传感器测试通道 3 激活	否
传感器测试通道 4 激活	否
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	否

3.10.2 功能块结构和安全回路

3.10.2.1 安全功能 1



3.10.3 计算

3.10.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
S2 – $B10_D$	10,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

3.10.3.2 诊断覆盖率 DC

组件	值
带合理性检查的 S1	DC_{avg}=90%
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=90%

3.10.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{100.000}{0{,}1 * 21{,}90} = 45662{,}1y = 399999120h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21{,}90$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 21{,}90} = 593607{,}3y = 5199997320h$$

并假设 S1、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}90}{45662{,}1 * 8760} = 2{,}50E - 10$$

K1/K2：每周执行 1 次，间接反馈

$$PFH = \frac{1 - 0{,}90}{593607{,}3 * 8760} = 1{,}92E - 11$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2,5E-10 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,92E-11 + 1,92E-11}{2} = 3,65E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y}} = 334,1y$$

$$DC_{avg} = \frac{\frac{90\%}{45662,1y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{593607,3y} + \frac{90\%}{593607,3y}}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{593607,3y} + \frac{1}{593607,3y}} = 98,92\%$$

⚠ 谨慎

类别

由于可能出现休眠错误，因此这种结构最多仅能达到类别 3。

由于 EL2904 端子模块在此应用中仅支持 SIL2 等级，因此整个链的等级仅限于 SIL2！

⚠ 谨慎

达到类别 3 所需采取的进一步措施！

这种结构最多能达到类别 3。为了达到类别 3，所有上升沿和下降沿必须与控制器中的时间依赖性一起进行评估，以获得反馈预期！

这可以通过已实施的 EDM 功能块实现。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

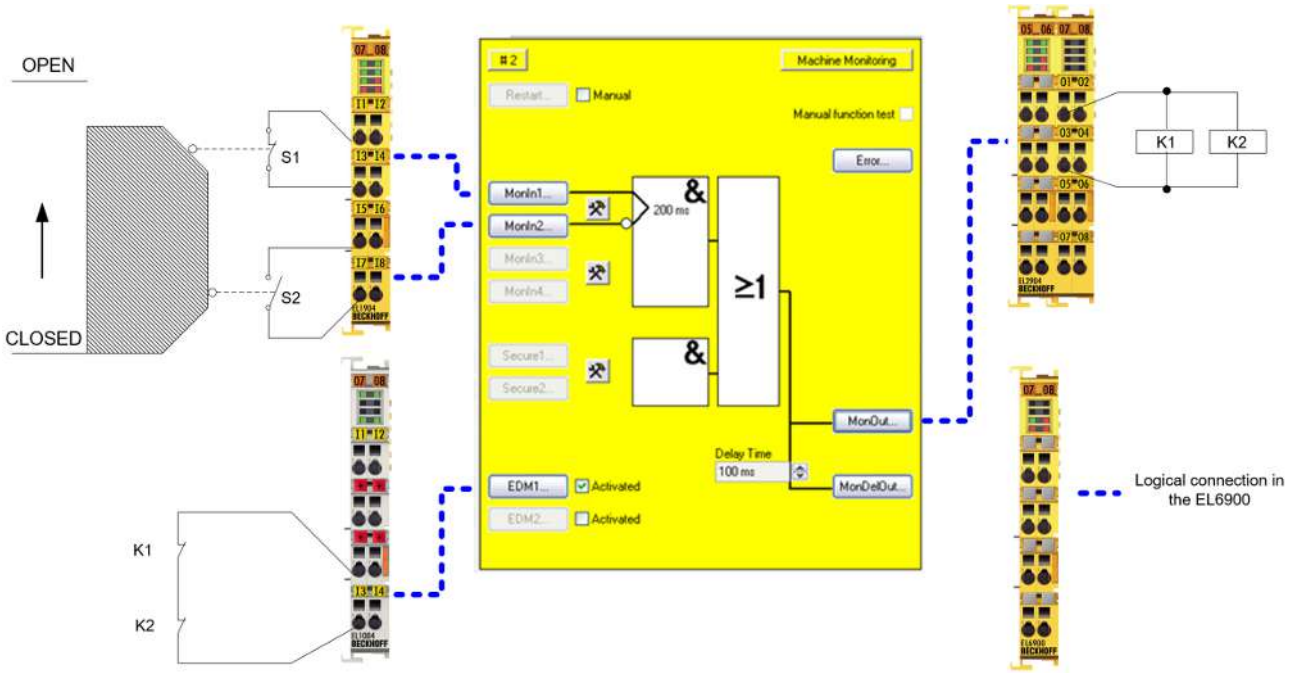
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4 准入功能

4.1 防护门功能变体 1 （类别 3，PL d）

防护门使用 EL1904 安全输入上的常闭和常开触点组合。输入测试已激活，并对信号进行差异测试（200 ms）。通过标准输入读入反馈回路，并通过标准 PLC 传输至 TwinSAFE。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



4.1.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

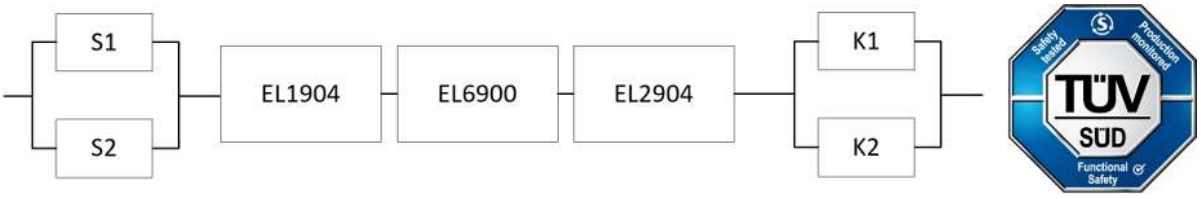
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.1.2 功能块结构和安全回路

4.1.2.1 安全功能 1



4.1.3 计算

4.1.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

4.1.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=90%

4.1.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1*14720} = 679,3y = 5951087h$$

S2：

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1*14720} = 1358,7y = 11902174h$$

K1/K2：

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0,1*14720} = 883,2y = 7736413h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1*n_{op}*(1-DC)}{B10_D} = \frac{1-DC}{MTTF_D}$$

S1：

$$PFH = \frac{1-0,99}{679,3*8760} = 1,68E-09$$

S2：

$$PFH = \frac{1-0,99}{1358,7*8760} = 8,4E-10$$

K1/K2：

$$PFH = \frac{1-0,90}{883,2*8760} = 1,29E-08$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta*\frac{PFH_{(S1)}+PFH_{(S2)}}{2} + (1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+\beta*\frac{PFH_{(K1)}+PFH_{(K2)}}{2} + (1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$$

由于 $(1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1$ 和 $(1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{1,68E-09 + 1,68E-09}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,29E-08 + 1,29E-08}{2} = 4,85E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y}} = 179,4y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{90\%}{883,2y} + \frac{90\%}{883,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y}} = 96,26\%$$

⚠ 谨慎

达到类别 3 所需采取的措施！

由于可能出现休眠错误，因此这种结构最多仅能达到类别 3。为了达到类别 3，所有上升沿和下降沿必须与控制器中的时间依赖性一起进行评估，以获得反馈预期。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年
中等	10 年 ≤ $MTTF_D$ < 30 年

$MTTF_D$	
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

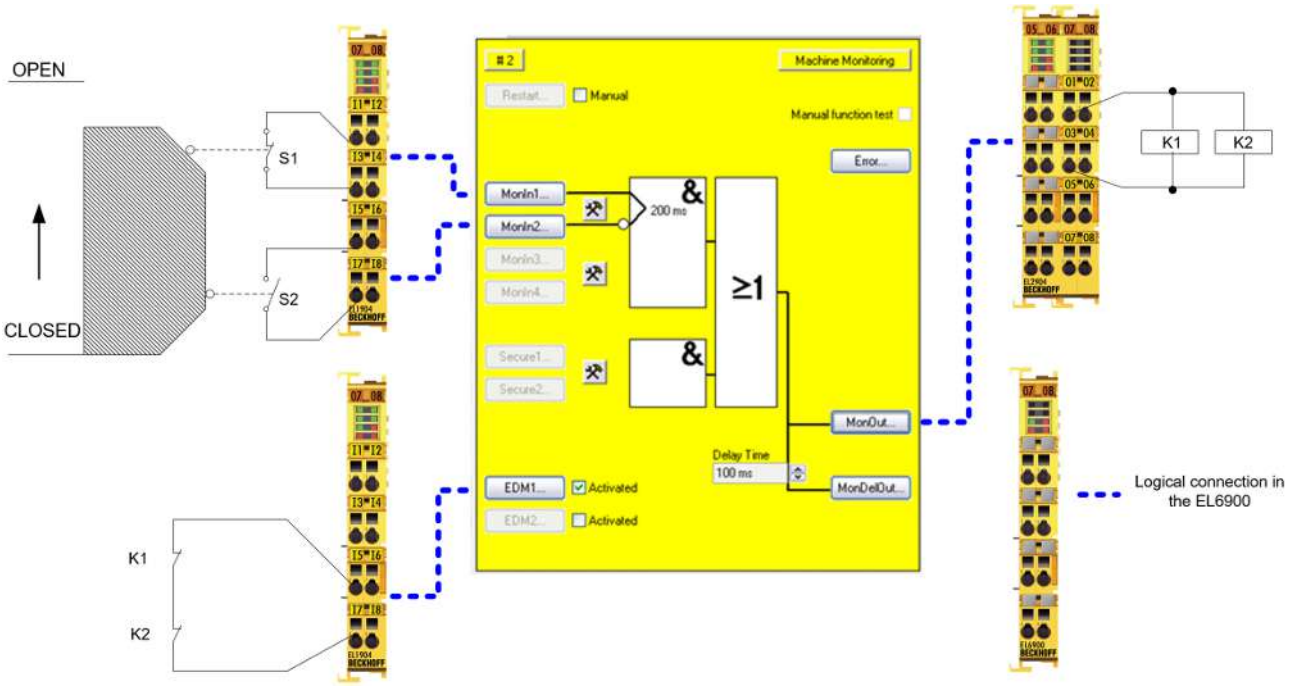
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.2 防护门功能变体 2（类别 4，PL e）

防护门使用 EL1904 安全输入上的常闭和常开触点组合。输入测试已激活，并对信号进行差异测试（200 ms）。通过安全输入读入反馈回路。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



4.2.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

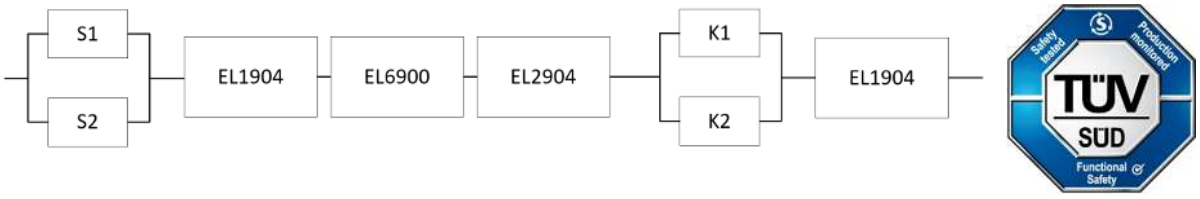
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.2.2 功能块结构和安全回路

4.2.2.1 安全功能 1



4.2.3 计算

4.2.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

4.2.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.2.3.3 安全功能 1 的计算

根据 $B10_d$ 值计算 PFH_D 和 $MTTF_d$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1:

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1*14720} = 679,3y = 5951087h$$

S2:

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1*14720} = 1358,7y = 11902174h$$

K1/K2:

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0,1*14720} = 883,2y = 7736413h$$

并假设 S1、S2、K1 和 K2 均为单通道:

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1*n_{op}*(1-DC)}{B10_D} = \frac{1-DC}{MTTF_D}$$

S1:

$$PFH = \frac{1-0,99}{679,3*8760} = 1,68E-09$$

S2:

$$PFH = \frac{1-0,99}{1358,7*8760} = 8,4E-10$$

K1/K2:

$$PFH = \frac{1-0,99}{883,2*8760} = 1,29E-09$$

现在必须做出以下假设:

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合!

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下:

$$PFH_{ges} = \beta*\frac{PFH_{(S1)}+PFH_{(S2)}}{2} + (1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+\beta*\frac{PFH_{(K1)}+PFH_{(K2)}}{2} + (1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1 + PFH_{(EL1904)}$$

由于 $(1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1$ 和 $(1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges}=10\%*\frac{1,68E-09+1,68E-09}{2}+1,11E-09+1,03E-09+1,25E-09+10\%*\frac{1,29E-09+1,29E-09}{2}+1,11E-09=4,80E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}}=\sum_{i=1}^{n}\frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}}=\frac{1}{MTTF_{D(S1)}}+\frac{1}{MTTF_{D(EL1904)}}+\frac{1}{MTTF_{D(EL6900)}}+\frac{1}{MTTF_{D(EL2904)}}+\frac{1}{MTTF_{D(K1)}}+\frac{1}{MTTF_{D(EL1904)}}$$

及：

$$MTTF_{D(S1)}=\frac{B10_{D(S1)}}{0,1*n_{op}}$$

$$MTTF_{D(S2)}=\frac{B10_{D(S2)}}{0,1*n_{op}}$$

$$MTTF_{D(K1)}=\frac{B10_{D(K1)}}{0,1*n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)}=\frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)}=\frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}}=\frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}}=\frac{0,01}{9,72E-06\frac{1}{y}}=1028,8y$$

$$MTTF_{D(EL6900)}=\frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}}=\frac{(1-0,99)}{1,03E-09\frac{1}{h}*8760\frac{h}{y}}=\frac{0,01}{9,02E-06\frac{1}{y}}=1108,6y$$

$$MTTF_{D(EL2904)}=\frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}}=\frac{(1-0,99)}{1,25E-09\frac{1}{h}*8760\frac{h}{y}}=\frac{0,01}{1,1E-05\frac{1}{y}}=913,2y$$

$$MTTF_{Dges}=\frac{1}{\frac{1}{679,3y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{883,2y}+\frac{1}{1028,8y}}=152,7y$$

$$DC_{avg}=\frac{\frac{99\%}{679,3y}+\frac{99\%}{1358,7y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}+\frac{99\%}{913,2y}+\frac{99\%}{883,2y}+\frac{99\%}{883,2y}+\frac{99\%}{1028,8y}}{\frac{1}{679,3y}+\frac{1}{1358,7y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{883,2y}+\frac{1}{883,2y}+\frac{1}{1028,8y}}=99,0\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**

$MTTF_D$	
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

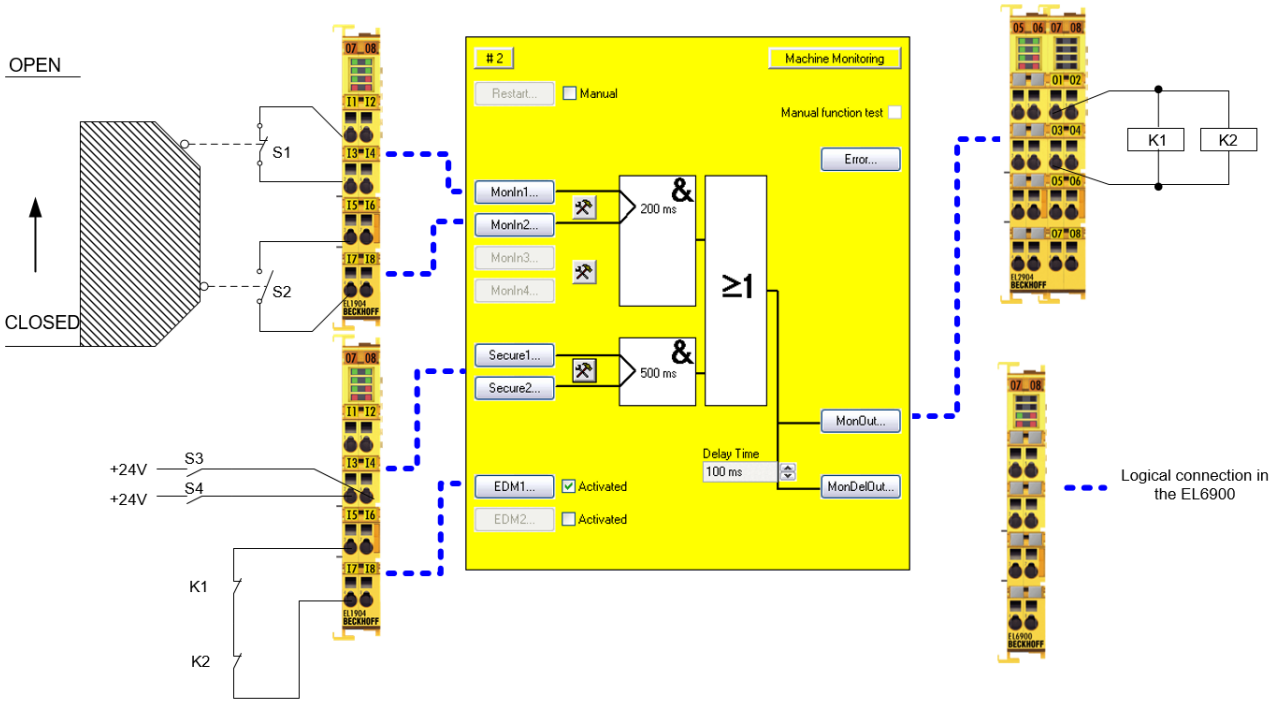
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

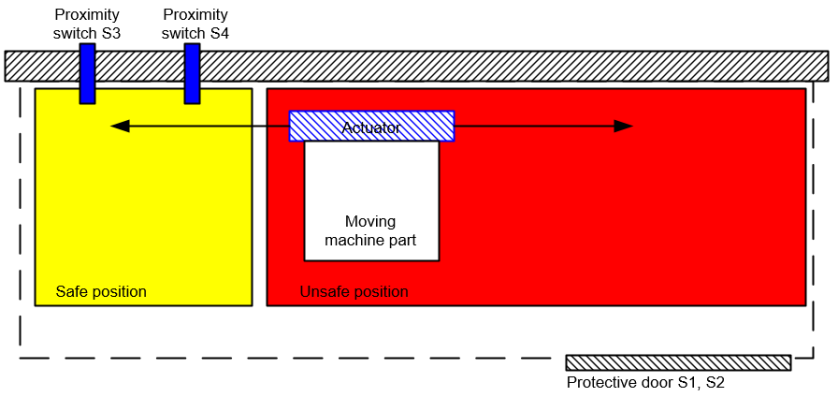
Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.3 带范围监控的防护门功能（类别 4，PL e）

防护门使用 EL1904 安全输入上的常闭和常开触点组合。输入测试已激活，并对信号进行差异测试（200 ms）。通过安全输入读入反馈回路。接近传感器 S3 和 S4 连接至安全输入，可检测危险设备部件是否处于安全位置等情况，以便在设备运行期间允许开启防护门。这些输入的测试功能均已停用，以便使用传感器的静态 24 V 电压。

接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。





4.3.1 安全输入和输出端子模块的参数

EL1904（图纸中上部的 EL1904）

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL1904（图纸中下部的 EL1904）

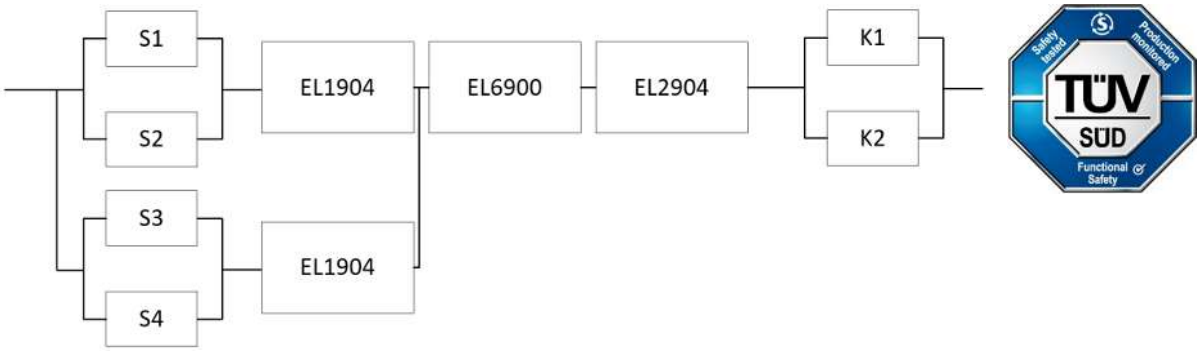
参数	值
传感器测试通道 1 激活	否
传感器测试通道 2 激活	否
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904（适用于所有使用的 EL2904）

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.3.2 功能块结构和安全回路

4.3.2.1 安全功能 1



4.3.3 计算

4.3.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
S3 – $B10_D$	20,000,000
S4 – $B10_D$	20,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

4.3.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带/不带测试/带合理性检查的 S3/S4	DC_{avg}=90%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.3.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 14720} = 679{,}3y = 5951087h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 14720} = 1358{,}7y = 11902174h$$

S3：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{20.000.000}{0{,}1 * 14720} = 13586{,}9y = 119021739h$$

S4：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{20.000.000}{0{,}1 * 14720} = 13586{,}9y = 119021739h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 14720} = 883{,}2y = 7736413h$$

并假设 S1、S2、S3、S4、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{679{,}3 * 8760} = 1{,}68E - 09$$

S2：

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}4E - 10$$

S3/S4：

$$PFH = \frac{1 - 0{,}90}{13586{,}9 * 8760} = 8{,}4E - 10$$

K1/K2：

$$PFH = \frac{1 - 0{,}99}{883{,}2 * 8760} = 1{,}29E - 09$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

对接近传感器 S3/S4 进行合理性（时序/逻辑）监控，根据 EN 61508 标准，它们属于 A 类系统（在错误条件下其行为完全已知的简单组件）。每班次执行一次安全位置移动。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1/S2/EL1904)} + PFH_{(S3/S4/EL1904)}}{2} + (1-\beta)^2 * (PFH_{(S1/S2/EL1904)} * PFH_{(S3/S4/EL1904)}) * T1 + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+ \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(S1/S2/EL1904)} * PFH_{(S3/S4/EL1904)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{(S1/S2/EL1904)} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + PFH_{(EL1904)} = 10\% * \frac{1{,}68E - 09 + 8{,}4E - 10}{2} + 1{,}11E - 09 = 1{,}24E - 09$$

$$PFH_{(S3/S4/EL1904)} = \beta * \frac{PFH_{(S3)} + PFH_{(S4)}}{2} + PFH_{(EL1904)} = 10\% * \frac{8{,}4E - 10 + 8{,}4E - 10}{2} + 1{,}11E - 09 = 1{,}19E - 09$$

$$PFH_{ges} = 10\% * \frac{1{,}24E - 09 + 1{,}19E - 09}{2} + 1{,}03E - 09 + 1{,}25E - 09 + 10\% * \frac{1{,}29E - 09 + 1{,}29E - 09}{2} = 2{,}53E - 09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(S3)} = \frac{B10_{D(S3)}}{0,1 * n_{op}}$$

$$MTTF_{D(S4)} = \frac{B10_{D(S4)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y}} = 179,4y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{90\%}{13586,9y} + \frac{90\%}{13586,9y} + \frac{99\%}{1028,8y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{883,2y} + \frac{99\%}{883,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{13586,9y} + \frac{1}{13586,9y} + \frac{1}{1028,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y}} = 98,85\%$$

注意

类别

这种结构最多能达到类别 4。传感器 S3 和 S4 的监控必须通过时序和逻辑编程实现。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年
中等	10 年 ≤ $MTTF_D$ < 30 年
高	**30 年 ≤ $MTTF_D$ ≤ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

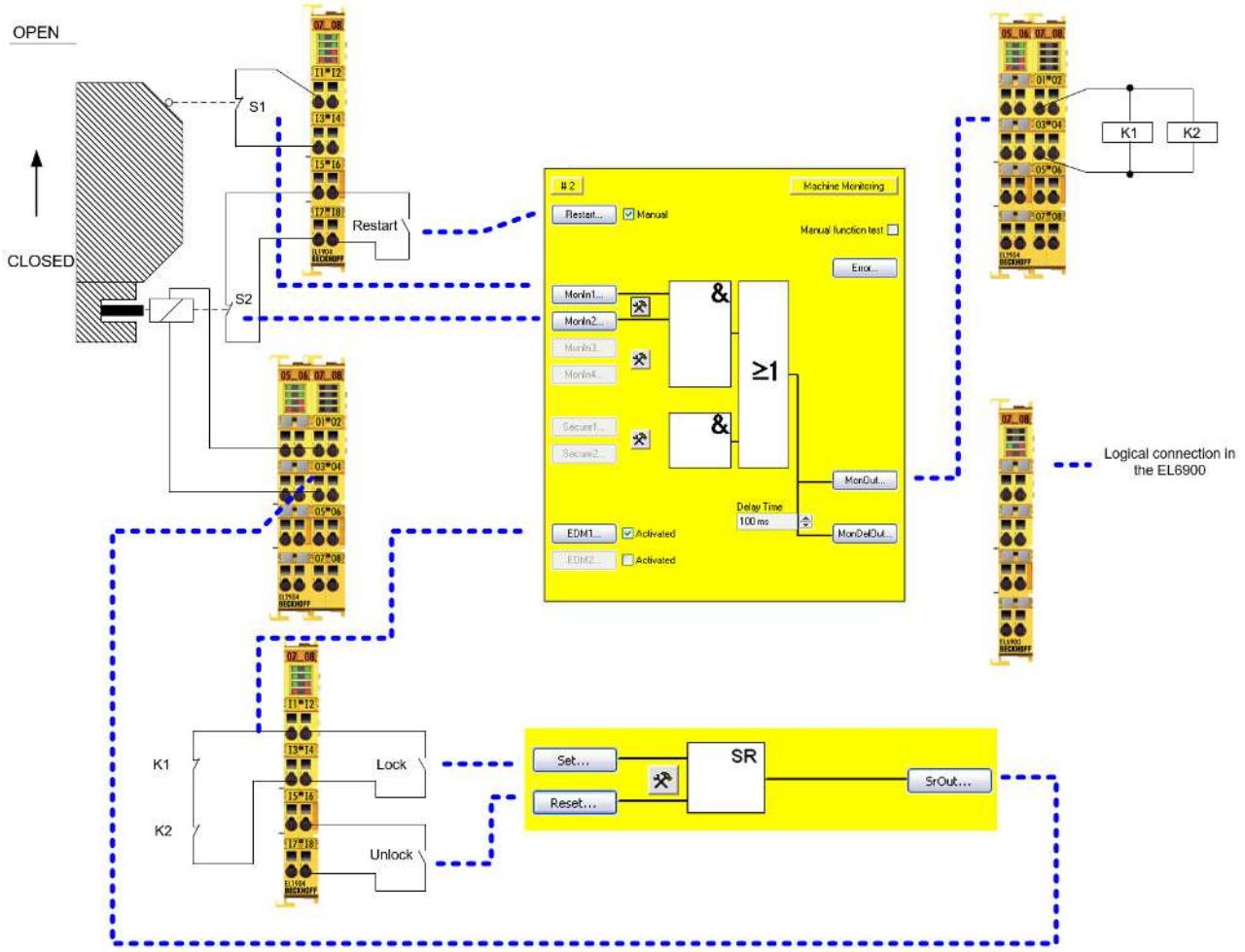
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.4 带锁芯的防护门功能（类别 4，PL e）

防护门有两个触点：S1“门已关闭”和S2“门已关闭并锁定”，它们均连接至 EL1904 的安全输入。输入测试已激活。由于信号之间没有时序关系，因此无法对信号进行差异检查。通过安全输入读入反馈回路和重启信号。此处的输入测试也已激活。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。

锁芯通过 2 个安全输入进行切换，且其测试功能已激活。在锁芯安全输出上，测试与电流测量功能均已激活。



4.4.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

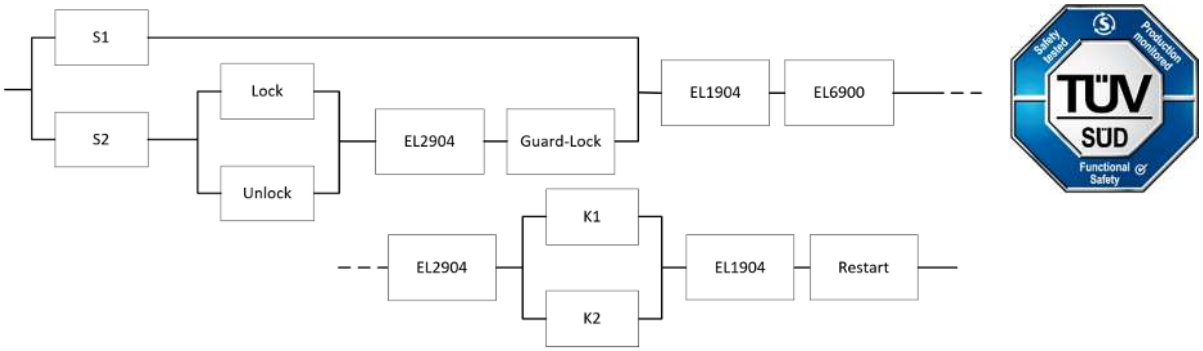
EL2904（适用于所有使用的 EL2904）

参数	值
电流测量激活	是

参数	值
输出测试脉冲激活	是

4.4.2 功能块结构和安全回路

4.4.2.1 安全功能 1



4.4.3 计算

4.4.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	2,000,000
S2 – $B10_D$	2,000,000
重启 - $B10_D$	10,000,000
锁定 – $B10_D$	100,000
解锁 – $B10_D$	100,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
锁芯（防护锁） - $B10_D$	2,000,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

4.4.3.2 诊断覆盖率 DC

组件	值
带测试的 S1	DC_{avg}=90%
带测试和预期检测的 S2	DC_{avg}=99%
带测试/合理性检查的锁定/解锁	DC_{avg}=99%
重启	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

组件	值
锁芯	DC_{avg}=99%

4.4.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 14720} = 1358{,}7y = 11902174h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 14720} = 1358{,}7y = 11902174h$$

锁定/解锁：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{100.000}{0{,}1 * 14720} = 67{,}9y = 595108h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 14720} = 883{,}2y = 7736413h$$

重启：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{10.000.000}{0{,}1 * 14720} = 6793{,}5y = 59511060h$$

锁芯：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 14720} = 1358{,}7y = 11902174h$$

并假设 S1、S2、S3、S4、K1、K2 和旋转锁均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}90}{1358{,}7 * 8760} = 8{,}40E - 09$$

S2：

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}4E - 10$$

锁定/解锁：

$$PFH = \frac{1 - 0{,}99}{67{,}9 * 8760} = 1{,}68E - 08$$

重启：

$$PFH = \frac{1 - 0{,}90}{6793{,}5 * 8760} = 1{,}68E - 09$$

K1/K2：

$$PFH = \frac{1 - 0{,}99}{883{,}2 * 8760} = 1{,}29E - 09$$

锁芯：

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}4E - 10$$

现在必须做出以下假设：

门开关 S1/S2 必须同时触发。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

锁芯以机械方式连接至开关 S2，确保其耦合不可分离。

重启功能受到监控，因此信号变化只有在门关闭后才有效。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S2/Lock/Unlock/EL2904/GuardLock)} + PFH_{(S1)}}{2} + (1-\beta)^2 * (PFH_{(S2/Lock/Unlock/EL2904/GuardLock)} * PFH_{(S1)}) * T1 + PFH_{(EL1904)}$$
$$+ PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(EL1904)} + PFH_{(Restart)}$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{(S2//Lock/Unlock/EL2904/GuardLock)} = PFH_{(S2)} + \beta * \frac{PFH_{(Lock)} + PFH_{(Unlock)}}{2} + PFH_{(EL2904)} + PFH_{(GuardLock)}$$
$$= 8,4E-10 + 10\% * \frac{1,68E-08 + 1,68E-08}{2} + 1,25E-09 + 8,4E-10 = 4,61E-09$$

$$PFH_{ges} = 10\% * \frac{4,61E-09 + 8,4E-09}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09$$
$$+10\% * \frac{1,29E-09 + 1,29E-09}{2} + 1,11E-09 + 1,68E-09$$
$$= 6,96E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S2/Lock/Unlock/EL2904/GuardLock)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(Restart)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(Lock)} = \frac{B10_{D(Lock)}}{0,1 * n_{op}}$$

$$MTTF_{D(Unlock)} = \frac{B10_{D(Unlock)}}{0,1 * n_{op}}$$

$$MTTF_{D(GuardLock)} = \frac{B10_{D(GuardLock)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,72E-06 \frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{9,02E-06 \frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0,01}{1,1E-05 \frac{1}{y}} = 913,2y$$

$$MTTF_{D(S2/Lock/Unlock/EL2904/GuardLock)} = \frac{1}{\frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(Lock)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(GuardLock)}}}$$

$$= \frac{1}{\frac{1}{1358,7y} + \frac{1}{67,9y} + \frac{1}{913,2y} + \frac{1}{1358,7y}} = 57,82y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{57,82y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{1028,8y} + \frac{1}{6793,5y}} = 44,41y$$

$$DC_{avg} = \frac{\frac{99\%}{57,82y} + \frac{99\%}{1358,7y} + \frac{99\%}{67,9y} + \frac{99\%}{67,9y} + \frac{99\%}{913,2y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{883,2y} + \frac{99\%}{883,2y} + \frac{99\%}{1028,8y} + \frac{90\%}{6793,5y}}{\frac{1}{57,82y} + \frac{1}{1358,7y} + \frac{1}{67,9y} + \frac{1}{67,9y} + \frac{1}{913,2y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{883,2y} + \frac{1}{883,2y} + \frac{1}{1028,8y} + \frac{1}{6793,5y}}$$

$$= 98,98\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

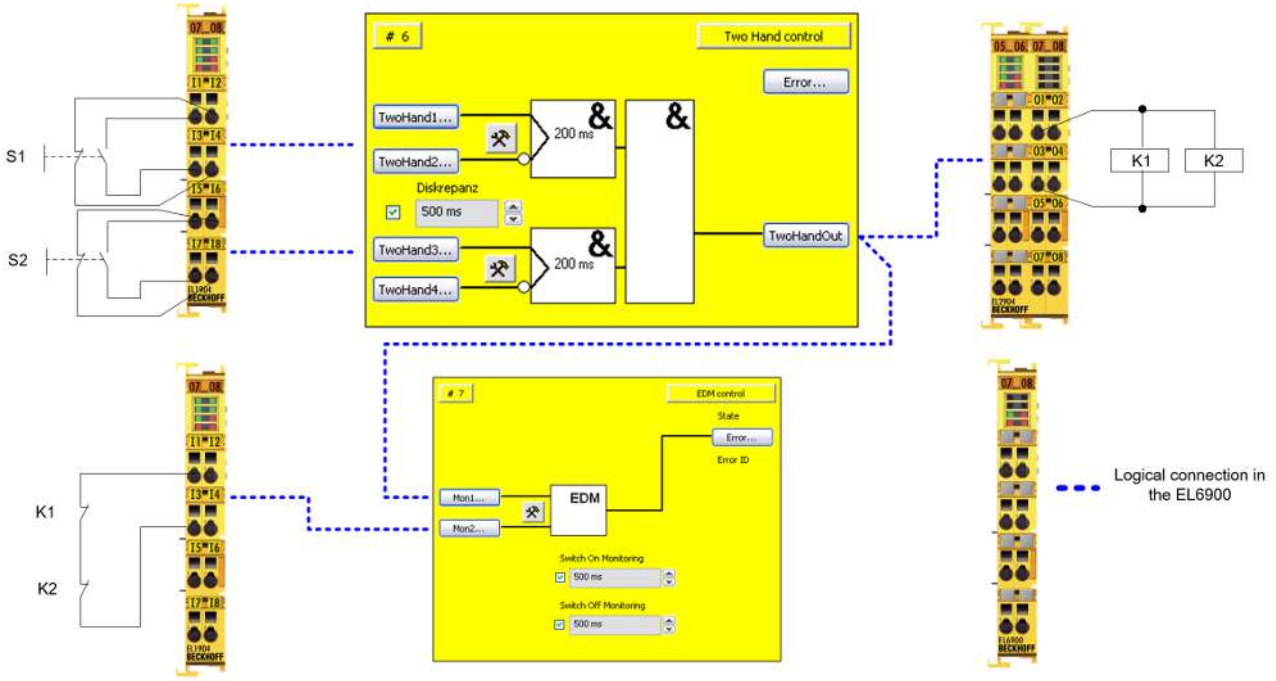
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.5 双手控制器（类别 4，PL e）

每个双手按钮均包含 EL1904 安全输入上的常闭和常开触点组合。输入测试已激活，并对信号进行差异测试（200 ms）。此外，两个按钮已启动同步触发监测，监测时间为 500 ms。

通过安全输入读入反馈回路。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



4.5.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

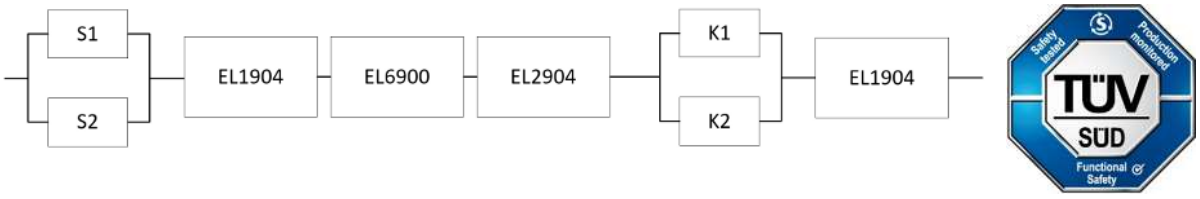
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.5.2 功能块结构和安全回路

4.5.2.1 安全功能 1



4.5.3 计算

4.5.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	20,000,000
S2 – $B10_D$	20,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	1（每分钟 1 次）
使用寿命（T1）	20 年 = 175200 小时

4.5.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.5.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1/S2：

$$n_{op} = \frac{230 * 16 * 60}{1} = 220.800$$

$$MTTF_D = \frac{20.000.000}{0{,}1 * 220.800} = 905{,}8y = 7.934.783h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{1} = 220.800$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 220.800} = 58{,}9y = 515.760h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1/S2：

$$PFH = \frac{1 - 0{,}99}{905{,}8y * 8760} = 1{,}26E - 09$$

K1/K2：

$$PFH = \frac{1 - 0{,}99}{58{,}9y * 8760} = 1{,}94E - 08$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)}$$
$$+ PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(EL1904)}$$

由于 $(1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{1{,}26E-09 + 1{,}26E-09}{2} + 1{,}11E-09 + 1{,}03E-09 + 1{,}25E-09 + 10\% * \frac{1{,}94E-08 + 1{,}94E-08}{2} + 1{,}11E-09$$
$$= 6{,}56E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(EL1904)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{905,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y} + \frac{1}{1028,8y}} = 45,4y$$

$$DC_{avg} = \frac{\frac{99\%}{905,8y} + \frac{99\%}{905,8y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{58,9y} + \frac{99\%}{58,9y} + \frac{99\%}{1028,8y}}{\frac{1}{905,8y} + \frac{1}{905,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{58,9y} + \frac{1}{58,9y} + \frac{1}{1028,8y}} = 99,0\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年
中等	10 年 ≤ $MTTF_D$ < 30 年
高	**30 年 ≤ $MTTF_D$ ≤ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ≤ DC < 90%

DC	
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

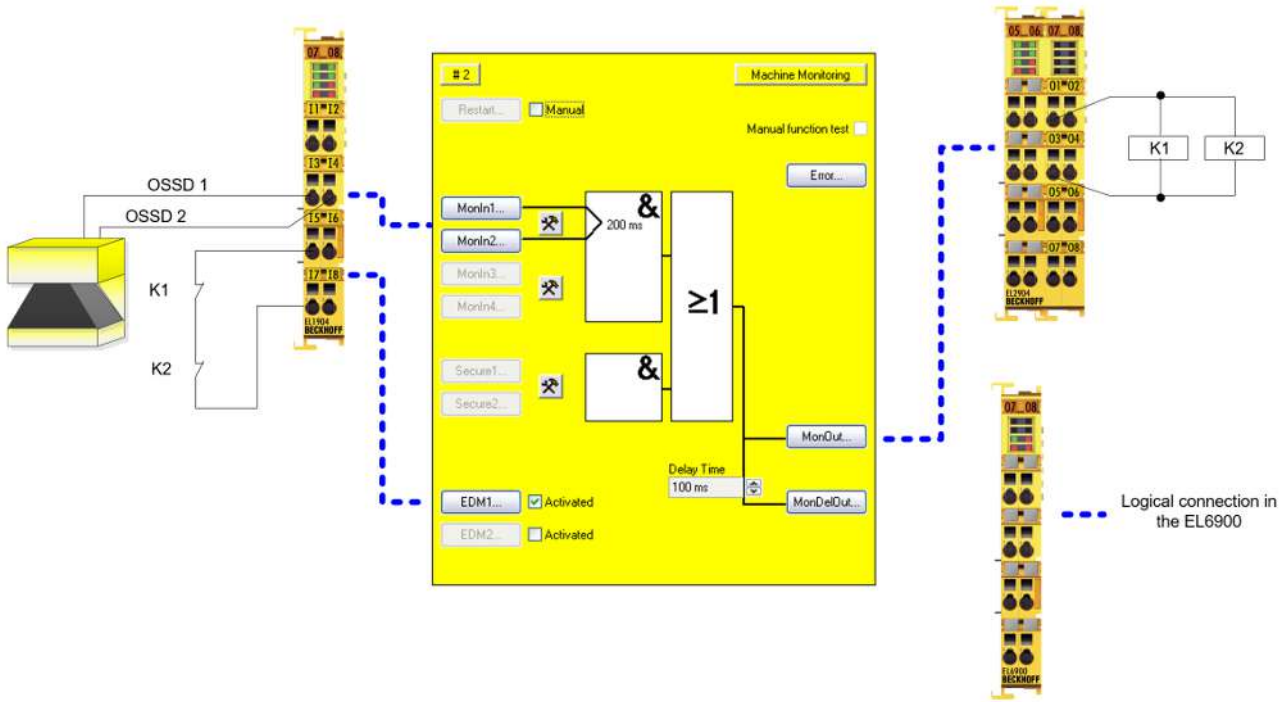
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.6 激光扫描器（类别 3，PL d）

激光扫描器有两个 OSSD 输出（输出信号切换设备），它们已连接至 EL1904 的安全输入。输入测试未激活，因为 OSSD 输出可自行进行测试。此外，信号已进行差异检查（200 ms）。通过安全输入读入反馈回路。该输入测试已激活。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



4.6.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

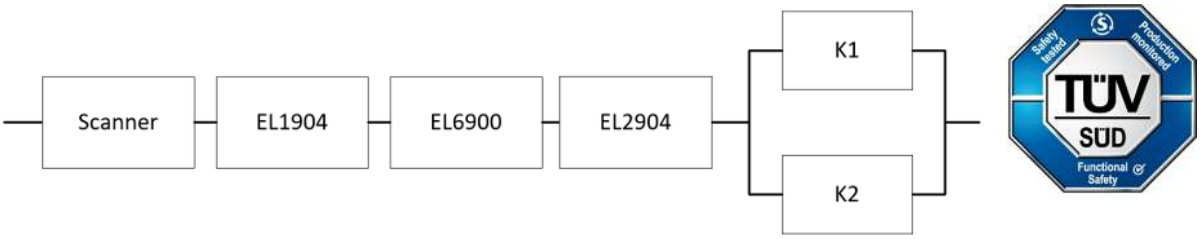
参数	值
传感器测试通道 1 激活	否
传感器测试通道 2 激活	否
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	OSSD 任意脉冲类型
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.6.2 功能块结构和安全回路

4.6.2.1 安全功能 1



4.6.3 计算

4.6.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
激光扫描器 – PFH_D	7.67E-08
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10（每小时 6 次）
使用寿命（T1）	20 年 = 175200 小时

4.6.3.2 诊断覆盖率 DC

组件	值
带测试（通过扫描器）/合理性检查的 OSSD1/2	DC_{avg}=90%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.6.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10} = 22.080$$

$$MTTF_D = \frac{1.300.000}{0,1 * 22.080} = 588,7y = 5.157.012h$$

并假设 K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

K1/K2：

$$PFH = \frac{1 - 0,99}{588,7y * 8760} = 1,94E - 09$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(Scanner)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 7,67E - 08 + 1,11E - 09 + 1,03E - 09 + 1,25E - 09 + 10\% * \frac{1,94E - 09 + 1,94E - 09}{2}$$
$$= 8,03E - 08$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{D(Scanner)} = \frac{(1-DC_{(Scanner)})}{PFH_{(Scanner)}} = \frac{(1-0,90)}{7,67E-08\frac{1}{h}*8760\frac{h}{y}} = \frac{0,1}{6,72E-04\frac{1}{y}} = 148,8y$$

根据 EN ISO 13849-1 标准中引入的类别 3 结构组件的 $MTTF_D$ 限值为 100 年（类别 4 的限值为 2500 年），在进一步处理扫描器的 $MTTF_D$ 时，限值为 100 年。

$$MTTF_{D(Scanner)} = 100y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{100y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{588,7y}} = 68,2y$$

$$DC_{avg} = \frac{\frac{90\%}{100}+\frac{99\%}{1028,8}+\frac{99\%}{1108,6}+\frac{99\%}{913,2}+\frac{99\%}{588,7}+\frac{99\%}{588,7}}{\frac{1}{100}+\frac{1}{1028,8}+\frac{1}{1108,6}+\frac{1}{913,2}+\frac{1}{588,7}+\frac{1}{588,7}} = 93,5\%$$

注意

类别

通过使用 3 类（类别 3）激光扫描器，这种结构最多能达到类别 3。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**区域**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

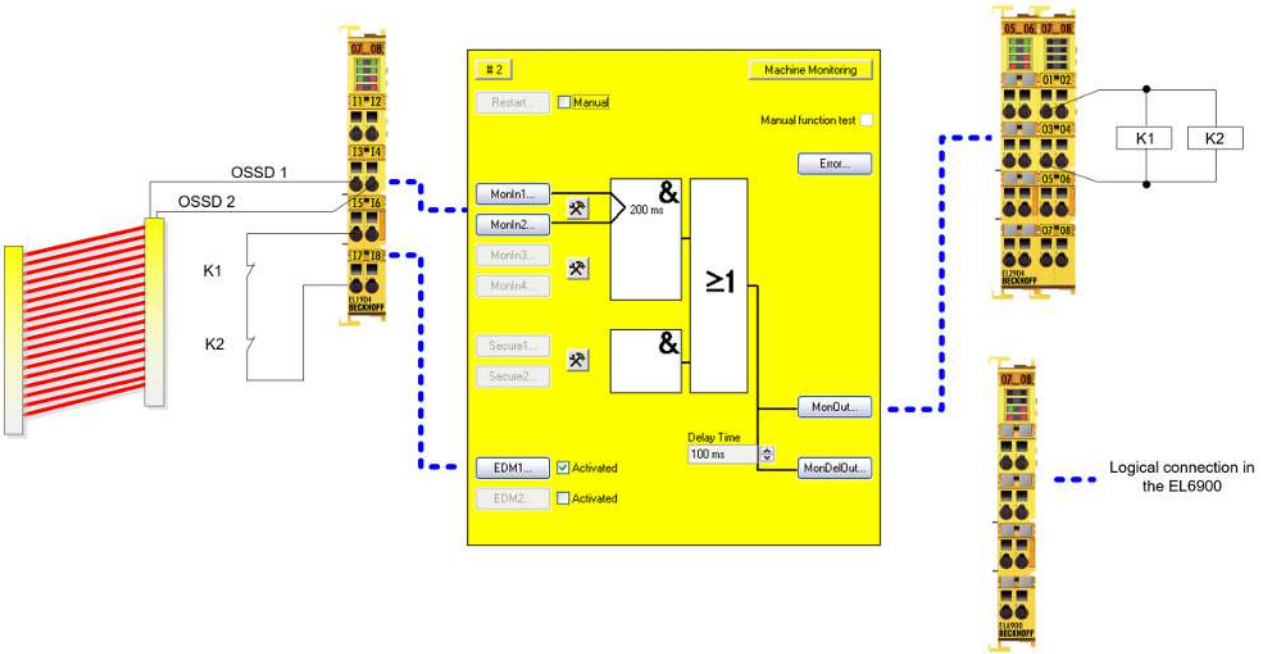
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.7 光幕（类别 4，PL e）

光幕有两个 OSSD 输出（输出信号切换设备），它们已连接至 EL1904 的安全输入。输入测试未激活，因为 OSSD 输出可自行进行测试。此外，信号已进行差异检查（200 ms）。通过安全输入读入反馈回路。该输入测试已激活。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



4.7.1 安全输入和输出端子模块的参数

EL1904

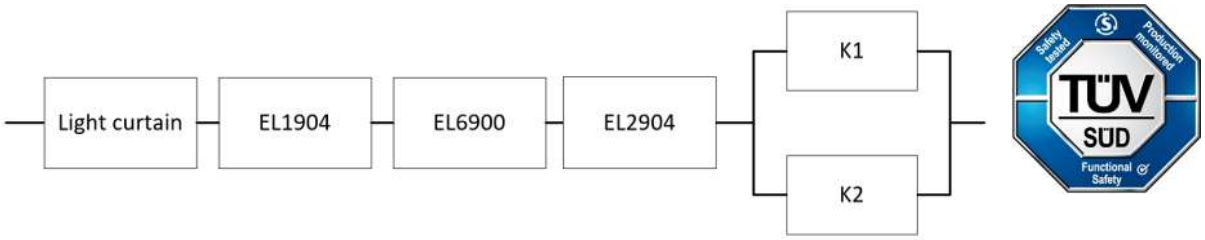
参数	值
传感器测试通道 1 激活	否
传感器测试通道 2 激活	否
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	OSSD 异步评估
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.7.2 功能块结构和安全回路

4.7.2.1 安全功能 1



4.7.3 计算

4.7.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
光幕 – PFH_D	1.50E-08
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	5（每小时 12 次）
使用寿命（T1）	20 年 = 175200 小时

4.7.3.2 诊断覆盖率 DC

组件	值
带测试（通过光幕）/ 合理性检查的 OSSD1/2	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.7.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

K1/K2：

$$n_{op} = \frac{230*16*60}{5} = 44.160$$

$$MTTF_D = \frac{1.300.000}{0{,}1*44.160} = 294{,}4y = 2.578.944h$$

并假设 K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1*n_{op}*(1-DC)}{B10_D} = \frac{1-DC}{MTTF_D}$$

K1/K2：

$$PFH = \frac{1-0{,}99}{294{,}4y*8760} = 3{,}88E-09$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(Lightcurtain)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta*\frac{PFH_{(K1)}+PFH_{(K2)}}{2} + (1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$$

由于 $(1-\beta)^2*(PFH_{(K1)}*PFH_{(K2)})*T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 1{,}50E-08 + 1{,}11E-09 + 1{,}03E-09 + 1{,}25E-09 + 10\%*\frac{3{,}88E-09+3{,}88E-09}{2}$$
$$= 1{,}88E-08$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n}\frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Lightcurtain)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0{,}1*n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}99)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}72E-06\frac{1}{y}} = 1028{,}8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0{,}99)}{1{,}03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}02E-06\frac{1}{y}} = 1108{,}6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

$$MTTF_{D(Lightcurtain)} = \frac{(1 - DC_{(Lightcurtain)})}{PFH_{(Lightcurtain)}} = \frac{(1 - 0{,}99)}{1{,}50E-08\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}31E-04\frac{1}{y}} = 76{,}1y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{76{,}1y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{294{,}4y}} = 51{,}3y$$

$$DC_{avg} = \frac{\frac{99\%}{76{,}1y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{1108{,}6y} + \frac{99\%}{913{,}2y} + \frac{99\%}{294{,}4y} + \frac{99\%}{294{,}4y}}{\frac{1}{76{,}1y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{294{,}4y} + \frac{1}{294{,}4y}} = 99{,}00\%$$

注意

类别

通过使用 4 类（类别 4）光幕，这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年
中等	10 年 ≤ $MTTF_D$ < 30 年
高	**30 年 ≤ $MTTF_D$ ≤ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ≤ DC < 90%
中等	90% ≤ DC < 99%
高	**99% ≤ DC**

注意

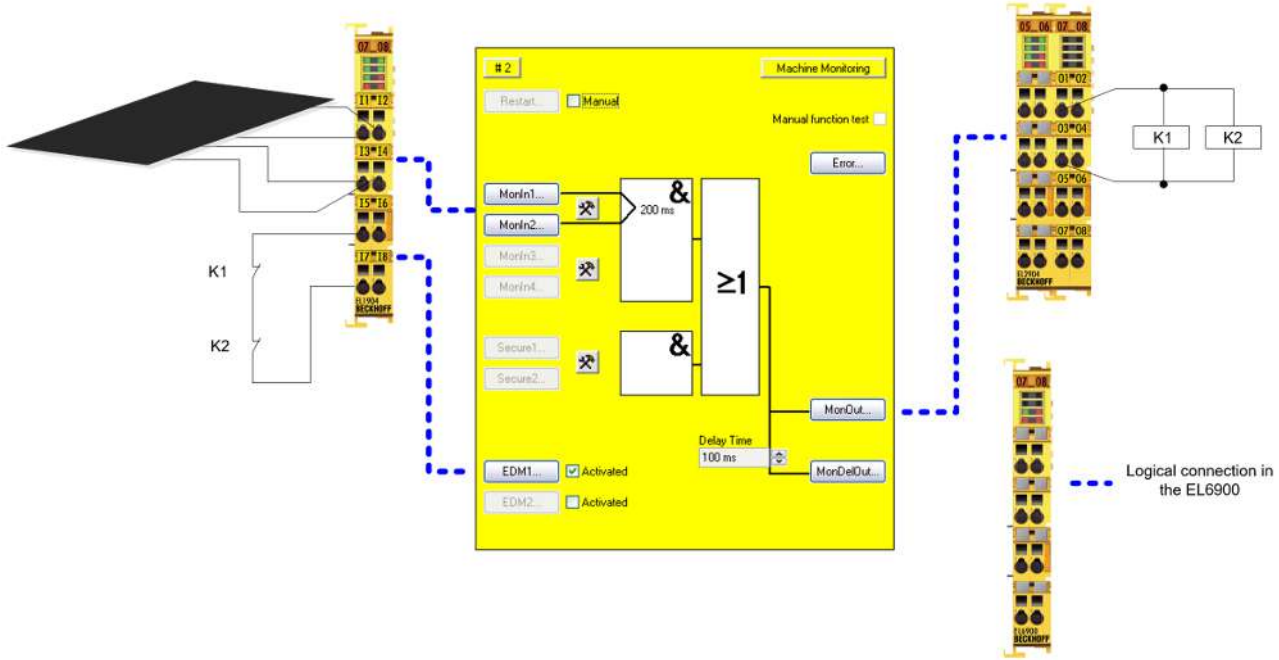
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.8 安全开关垫/安全缓冲器（类别 4，PL e）

安全开关垫或安全缓冲器根据交叉电路原理工作。设备的接触面连接至 EL1904 的安全输入。输入测试已激活，并对信号进行差异测试（200 ms）。一旦检测到信号之间存在交叉短路（安全垫被踩踏），EL1904 输入端子模块将输出逻辑 0 信号。如果交叉短路不再存在，则输出逻辑 1 信号。通过安全输入读入反馈回路。此处的输入测试也已激活。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。



4.8.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

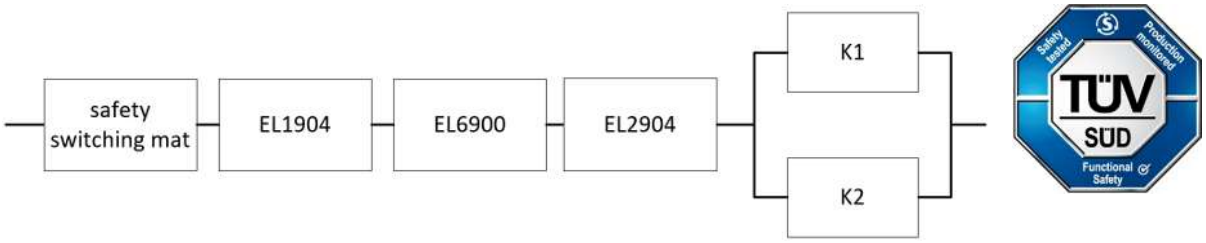
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	交叉短路并非模块错误
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.8.2 功能块结构和安全回路

4.8.2.1 安全功能 1



4.8.3 计算

4.8.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
安全开关垫 – $B10_D$	6.00E06
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	1（每分钟 1 次）
使用寿命（T1）	20 年 = 175200 小时

4.8.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的切换输出（垫）	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.8.3.3 安全功能 1 的计算

根据 $B10_d$ 值计算 PFH_D 和 $MTTF_d$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

K1/K2：

$$n_{op} = \frac{230*16*60}{1} = 220.800$$

$$MTTF_D = \frac{1.300.000}{0{,}1*220.800} = 58{,}9y = 515.760h$$

安全垫：

$$n_{op} = \frac{230*16*60}{1} = 220.800$$

$$MTTF_D = \frac{6{,}00E06}{0{,}1*220.800} = 271{,}7y = 2.380.434h$$

并假设 K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1*n_{op}*(1-DC)}{B10_D} = \frac{1-DC}{MTTF_D}$$

K1/K2：

$$PFH = \frac{1-0{,}99}{58{,}9y*8760} = 1{,}94E-08$$

安全垫：

$$PFH = \frac{1-0{,}99}{271{,}7y*8760} = 4{,}20E-09$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(SafetyMat)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 4{,}20E-09 + 1{,}11E-09 + 1{,}03E-09 + 1{,}25E-09 + 10\% * \frac{1{,}94E-08 + 1{,}94E-08}{2}$$
$$= 9{,}53E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SafetyMat)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0{,}1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}99)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}72E-06\frac{1}{y}} = 1028{,}8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0{,}99)}{1{,}03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}02E-06\frac{1}{y}} = 1108{,}6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{271{,}7y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{58{,}9y}} = 42{,}3y$$

$$DC_{avg} = \frac{\frac{99\%}{271{,}7y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{1108{,}6y} + \frac{99\%}{913{,}2y} + \frac{99\%}{58{,}9y} + \frac{99\%}{58{,}9y}}{\frac{1}{271{,}7y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{58{,}9y} + \frac{1}{58{,}9y}} = 99{,}00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

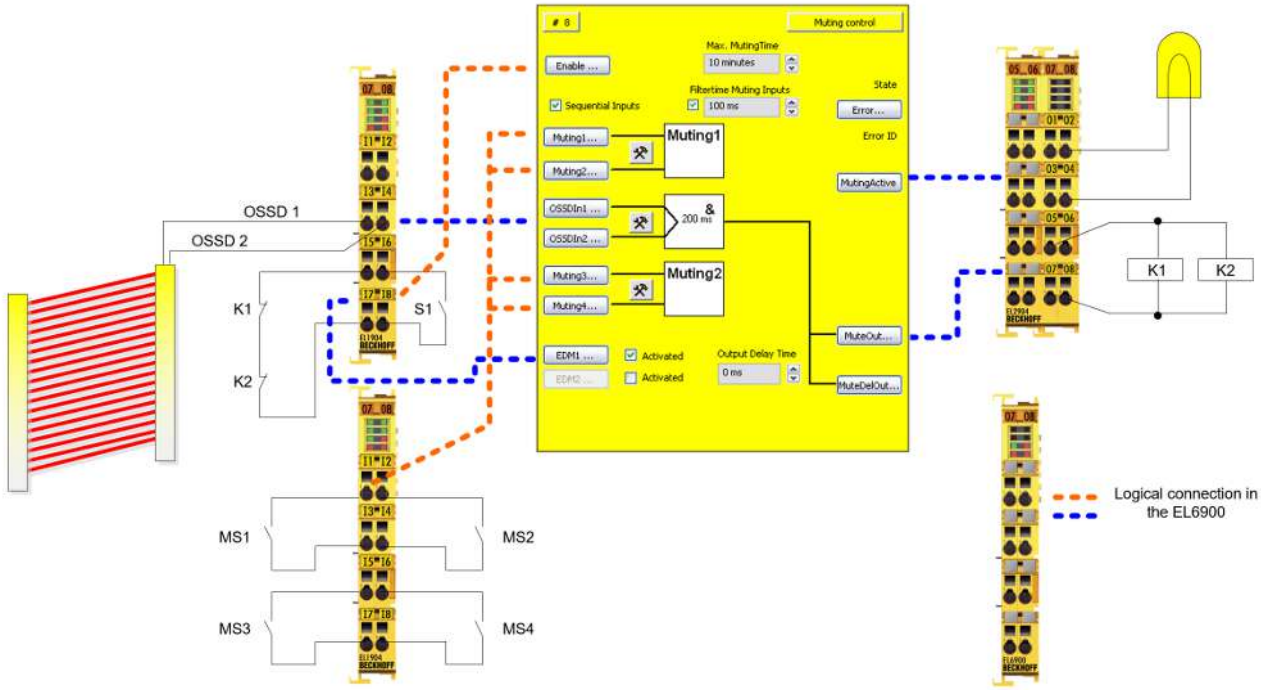
诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.9 屏蔽（类别 4，PL e）

光幕有两个 OSSD 输出（输出信号切换设备），它们已连接至 EL1904 的安全输入。输入测试未激活，因为 OSSD 输出可自行进行测试。此外，信号已进行差异检查（200 ms）。通过安全输入读入反馈回路。屏蔽开关和启动开关也连接至安全输入。这些输入测试已激活。
接触器 K1 和 K2 并联连接至安全输出。屏蔽灯也连接至安全输出。该电路已激活电流测量与输出测试功能。



4.9.1 安全输入和输出端子模块的参数

EL1904（图纸中上部的端子模块）

参数	值
传感器测试通道 1 激活	否
传感器测试通道 2 激活	否
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	OSSD 异步评估
逻辑通道 3 和 4	单逻辑

EL1904（图纸中下部的端子模块）

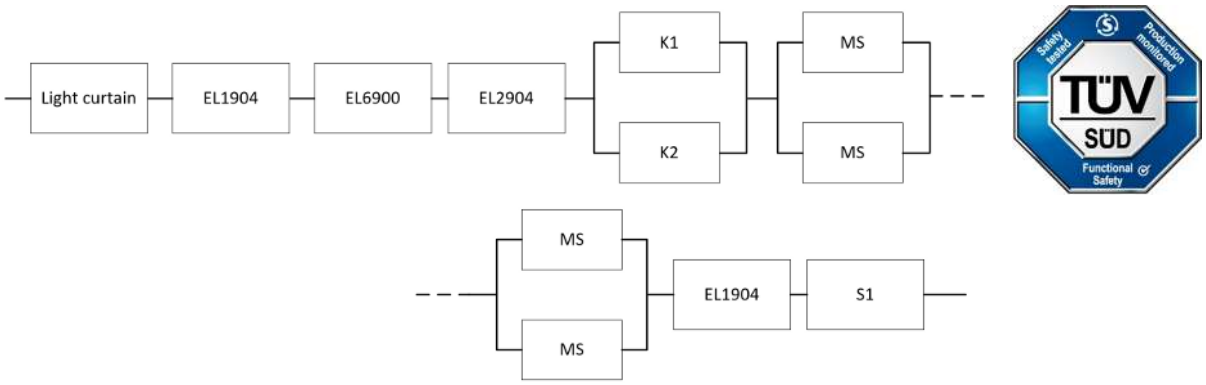
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

4.9.2 功能块结构和安全回路

4.9.2.1 安全功能 1



4.9.3 计算

4.9.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	100,000
光幕 – PFH_D	1.50E-08
MS1 – $B10_D$	100,000
MS2 – $B10_D$	100,000
MS3 – $B10_D$	100,000
MS4 – $B10_D$	100,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	60（每小时 1 次）
使用寿命（T1）	20 年 = 175200 小时

4.9.3.2 诊断覆盖率 DC

组件	值
带测试（通过光幕）/ 合理性检查的 OSSD1/2	DC_{avg}=99%
带测试/合理性检查的 MS1/2/3/4	DC_{avg}=90%
带测试和 EDM 的 K1/K2	DC_{avg}=99%
带测试的 S1	DC_{avg}=90%

4.9.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0{,}1 * 1840} = 543{,}5y = 4761060h$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 1840} = 7065{,}2y = 61891152h$$

MS1/MS2/MS3/S4：

$$n_{op} = \frac{230 * 16 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0{,}1 * 1840} = 543{,}5y = 4761060h$$

并假设 S1、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}90}{543{,}5 * 8760} = 2{,}10E - 08$$

K1/K2：

$$PFH = \frac{1-0,99}{7065,2*8760} = 1,62E-10$$

MS1/MS2/MS3/S4：

$$PFH = \frac{1-0,90}{543,5*8760} = 2,10E-08$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$\begin{aligned}PFH_{ges} &= PFH_{(Lightcurtain)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 \\ &+ \beta * \frac{PFH_{(MS1)} + PFH_{(MS2)}}{2} + (1-\beta)^2 * (PFH_{(MS1)} * PFH_{(MS2)}) * T1 + \beta * \frac{PFH_{(MS3)} + PFH_{(MS4)}}{2} + (1-\beta)^2 * (PFH_{(MS3)} * PFH_{(MS4)}) * T1 \\ &+ PFH_{(EL1904)} + PFH_{(S1)}\end{aligned}$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$\begin{aligned}PFH_{ges} &= 1,50E-08 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 10\% * \frac{1,62E-10 + 1,62E-10}{2} + 10\% * \frac{2,10E-08 + 2,10E-08}{2} \\ &+ 10\% * \frac{2,10E-08 + 2,10E-08}{2} + 1,11E-09 + 2,10E-08 \\ &= 4,47E-08\end{aligned}$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\begin{aligned}\frac{1}{MTTF_{Dges}} &= \frac{1}{MTTF_{D(Lightcurtain)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} \\ &+ \frac{1}{MTTF_{D(MS1)}} + \frac{1}{MTTF_{D(MS3)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(S1)}}\end{aligned}$$

及：

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{D(Lightcurtain)} = \frac{(1-DC_{(Lightcurtain)})}{PFH_{(Lightcurtain)}} = \frac{(1-0,99)}{1,50E-08\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,31E-04\frac{1}{y}} = 76,1y$$

$$MTTF_{D(MS1/MS3)} = \frac{(1-DC_{(MS1/MS3)})}{PFH_{(MS1/MS3)}} = \frac{(1-0,90)}{2,10E-08\frac{1}{h}*8760\frac{h}{y}} = \frac{0,1}{1,84E-04\frac{1}{y}} = 543,6y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{76,1y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{7065,2y}+\frac{1}{543,6y}+\frac{1}{543,6y}+\frac{1}{1028,8y}+\frac{1}{543,5y}} = 44,0y$$

$$DC_{avg} = \frac{\frac{99\%}{76,1y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}+\frac{99\%}{913,2y}+\frac{99\%}{7065,2y}+\frac{99\%}{7065,2y}+\frac{90\%}{543,6y}+\frac{90\%}{543,6y}+\frac{90\%}{543,6y}+\frac{90\%}{543,6y}+\frac{99\%}{1028,8y}+\frac{99\%}{543,5y}}{\frac{1}{76,1y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{7065,2y}+\frac{1}{7065,2y}+\frac{1}{543,6y}+\frac{1}{543,6y}+\frac{1}{543,6y}+\frac{1}{543,6y}+\frac{1}{1028,8y}+\frac{1}{543,5y}} = 96,51\%$$

注意

类别

通过使用 4 类（类别 4）光幕，这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年
中等	10 年 ≤ $MTTF_D$ < 30 年
高	**30 年 ≤ $MTTF_D$ ≤ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ≤ DC < 90%
中等	90% ≤ DC < 99%
高	**99% ≤ DC**

注意

诊断覆盖率

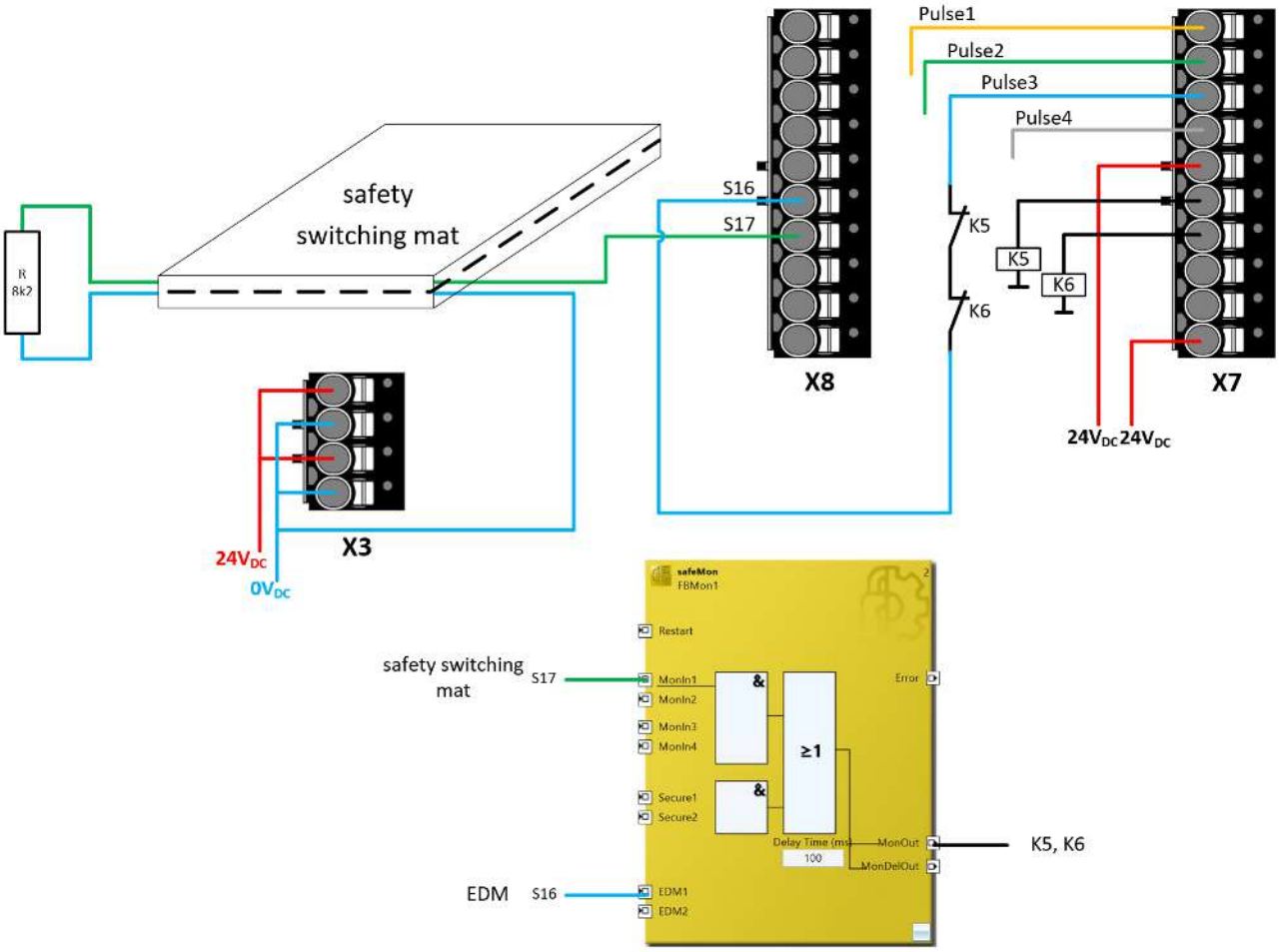
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

4.10 EK1960 安全垫输入/数字量输出（类别 2，PL d）

安全垫连接至 X8 10 极连接器上的安全输入 S17（或 8.7）。10 极 X7 连接器上的第一个输出组被配置为时钟源（对于 FSOUT 模块 3，参数*输入诊断测试脉冲激活*被设置为 TRUE）。对于输入 S16，根据相应的时钟源对参数*通道 x. 测试脉冲诊断模式*进行配置。

接触器 K5 和 K6 连接至 X7 上第二个输出模块上的输出 7.5 和 7.6。接触器的端子模块 A2 连接至端子模块 X7 的 24 V_{DC} 电源的公共地线。两个接触器的反馈回路串联连接，从脉冲 3 连接至输入 S16（或 8.6）。



⚠ 谨慎

安全垫接线

仅支持根据电阻变化原理（电阻值：8k2）工作的安全垫。根据上述图纸所示，安全垫的接地线必须连接至 EK1960 电源电压的接地线。

4.10.1 安全输入和输出模块的参数

EK1960

参数	值
FSOUT 模块 3（X7.1 – X7.4）	-
8020:01 诊断测试脉冲模数	0x00
8020:02 诊断测试脉冲倍数	0x02
8020:03 标准输出激活	FALSE
8020:04 诊断测试脉冲激活	TRUE

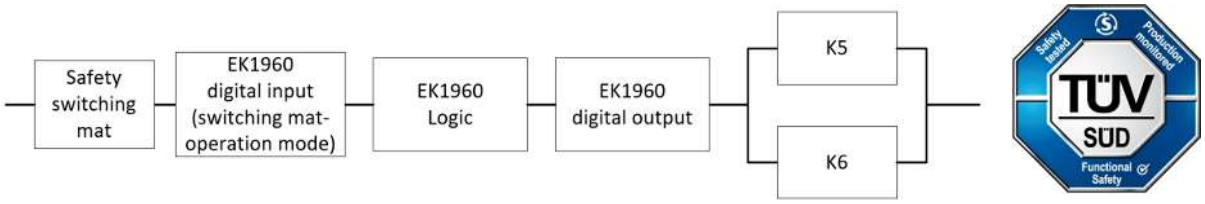
参数	值
8020:05 输入诊断测试脉冲激活	TRUE
FSOUT 模块 4（X7.5 – X7.8）	-
8030:01 诊断测试脉冲模数	0x00
8030:02 诊断测试脉冲倍数	0x02
8030:03 标准输出激活	FALSE
8030:04 诊断测试脉冲激活	TRUE
8030:05 输入诊断测试脉冲激活	FALSE
FSIN 模块 8（X8.5 – X8.6）	-
80E1:04 通道 2. 输入滤波时间	0x0014
80E1:05 通道 2. 诊断测试脉冲滤波时间	0x0002
80E1:06 通道 2. 测试脉冲诊断模式	（X7.3）测试脉冲检测输出模块 3. 通道 3
FSIN 模块 9（X8.7 – X8.8）	-
80F0:03 输入模式	缓冲器模式通道 1（1）
80F1:01 通道 1. 输入滤波时间	0x0014
80F1:02 通道 1. 诊断测试脉冲滤波时间	0x0002
80F1:03 通道 1. 测试脉冲诊断模式	外部测试脉冲（0）

MON FB 参数

参数	值
复位时间（ms）（端口 EDM1）	1000

4.10.2 功能块结构和安全回路

4.10.2.1 安全功能 1



4.10.3 计算

4.10.3.1 PFHD / MTTFD / B10D – 值

组件	值
EK1960 数字量输入 – PFH_D	6.40E-11
EK1960 安全垫输入 - PFH_D	8.84E-10
EK1960 逻辑 – PFH_D	5.18E-09
EK1960 数字量输 – PFH_D	1.50E-10
安全垫 – $B10_D$	6,000,000
K5 – $B10_D$	1,300,000
K6 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16

组件	值
循环时间（分钟）（T_{cycle}）	60（每小时 1 次）
使用寿命（T1）	20 年 = 175200 小时

Safety over EtherCAT 通信

Safety over EtherCAT（FSoE）通信的 PFH_D 值包含在 EK1960 逻辑组件的 PFH_D 值中。

4.10.3.2 诊断覆盖率 DC

组件	值
带测试的安全垫	DC_{avg}=90%
带 EDM 监控（每小时执行 1 次，并对所有上升沿和下降沿进行时序监测评估）和测试的 K5/K6	DC_{avg}=99%

4.10.3.3 安全功能 1 的计算

根据 EN ISO 13849-1:2015 标准计算性能等级：

根据 $B10_D$ 值计算 $MTTF_D$ 值。

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

安全开关垫：

$$n_{op} = \frac{230 * 16 * 60}{60} = 3680$$

$$MTTF_{D(SwitchingMat)} = \frac{6.000.000}{0{,}1 * 3680} = 16304y$$

K5/K6：

$$n_{op} = \frac{230 * 16 * 60}{60} = 3680$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 3680} = 3532y$$

根据以下公式计算总 $MTTF_D$ 值：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SwitchingMat)}} + \frac{1}{MTTF_{D(EK1960-InputSwitchingMat)}} + \frac{1}{MTTF_{D(EK1960-Logic)}} + \frac{1}{MTTF_{D(EK1960-Output)}} + \frac{1}{MTTF_{D(K5)}}$$

如果仅有 EK1960 组件的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(EK1960-xxx)} = \frac{(1 - DC_{(EK1960-xxx)})}{PFH_{(EK1960-xxx)}}$$

因此：

$$MTTF_{D(EK1960-InputSwitchingMat)} = \frac{(1 - DC_{(EK1960-InputSwitchingMat)})}{PFH_{D(EK1960-InputSwitchingMat)}} = \frac{(1 - 0{,}90)}{8{,}84E-10\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{7{,}74E-06\frac{1}{y}} = 12913y$$

$$MTTF_{D(EK1960-Logic)} = \frac{(1 - DC_{(EK1960-Logic)})}{PFH_{D(EK1960-Logic)}} = \frac{(1 - 0{,}99)}{5{,}18E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{4{,}54E-05\frac{1}{y}} = 220y$$

$$MTTF_{D(EK1960-Output)} = \frac{(1 - DC_{(EK1960-Output)})}{PFH_{D(EK1960-Output)}} = \frac{(1 - 0{,}99)}{1{,}50E-10\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}31E-06\frac{1}{y}} = 7610y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{16304y} + \frac{1}{12913y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{3532y}} = 196y$$

$$DC_{avg} = \frac{\frac{90\%}{16304y} + \frac{90\%}{12913y} + \frac{99\%}{220y} + \frac{99\%}{7610y} + \frac{99\%}{3532y} + \frac{99\%}{3532y}}{\frac{1}{16304y} + \frac{1}{12913y} + \frac{1}{220y} + \frac{1}{7610y} + \frac{1}{3532y} + \frac{1}{3532y}} = 98{,}76\%$$

注意

类别

这种结构最多能达到类别 2。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能**不**属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN 62061 标准计算 PFH_D 值：

假设安全垫、K5 和 K6 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH_D = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

安全开关垫：

$$PFH_D = \frac{1 - 0{,}90}{16304 * 8760} = 7{,}00E - 10$$

K5/K6：

$$PFH_D = \frac{1 - 0{,}99}{3532 * 8760} = 3{,}23E - 10$$

现在必须做出以下假设：

继电器 K5 和 K6 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K5 和 K6 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{Dges} = PFH_{D(SwitchingMat)} + PFH_{D(EK1960-InputSwitchingMat)} + PFH_{D(EK1960-Logic)} + PFH_{D(EK1960-Output)} + \beta * \frac{PFH_{D(K5)} + PFH_{D(K6)}}{2} + (1-\beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{D(K5)} * PFH_{D(K6)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{Dges} = 7{,}00E - 10 + 8{,}84E - 10 + 5{,}18E - 09 + 1{,}50E - 10 + 10\% * \frac{3{,}23E - 10 + 3{,}23E - 10}{2} = 6{,}94E - 09$$

安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	≥ 10-8 至 < 10-7
2	**≥ 10^{-7} 至 < 10^{-6}**
1	≥ 10^{-6} 至 < 10^{-5}

注意

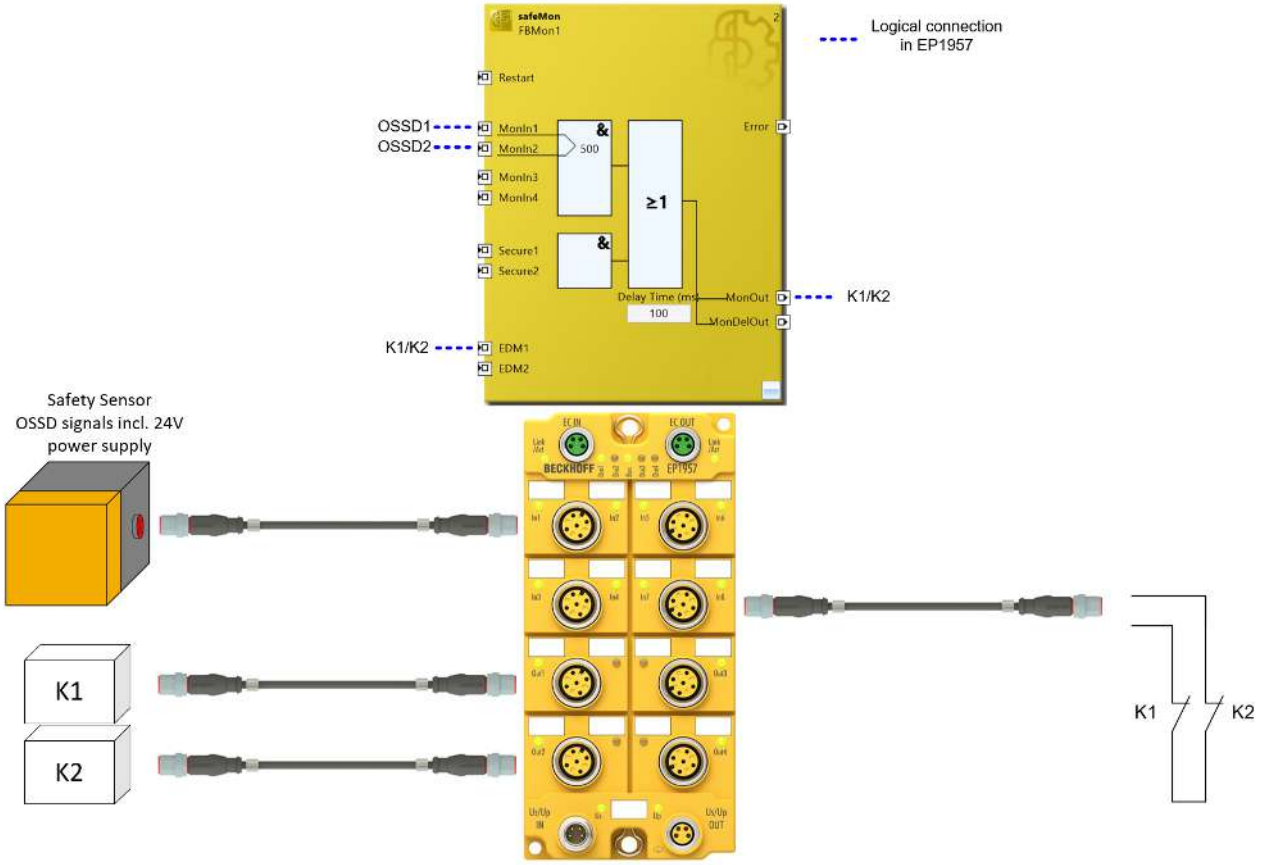
安全完整性等级

该应用符合 EN 62061 标准的安全完整性等级 SIL2 要求，因为安全垫输入可达到的最高 SIL 被限制为 SIL 2。

4.11 EP1957 接 OSSD 传感器用于防护门（类别 4，PL e）

OSSD 安全传感器（在这种情况下，例如采用符合 EN 60947-5-3 标准、具备错误状态下明确定义行为（PDDB）的接近限位开关）通过 M12 接口连接至 EP1957，可用于防护门等应用场景。通过 M12 接口（电源模式 A）的引脚 1 和 3 提供电源。传感器通过两个 OSSD 通道上的测试脉冲检查传感器和 EP1957 之间的接线，并在出现错误时将两个 OSSD 信号切换到安全状态。两个 OSSD 输入受到监控，以防逻辑出现偏差。

两个执行器 K1 和 K2 根据防护门状态进行切换。两个执行器的反馈回路连接至安全输入。为该输入激活测试脉冲。



4.11.1 安全输入和输出模块的参数

EP1957

参数	值
FSOUT 模块 1 公共设置	-
8000:04 诊断测试脉冲激活	TRUE
8000:07 模块故障链路激活	TRUE
FSOUT 模块 2 公共设置	-
8010:04 诊断测试脉冲激活	TRUE
8010:07 模块故障链路激活	TRUE
FSIN 模块 1 公共设置	-
8040:04 诊断测试脉冲激活	FALSE
8040:05 模块故障链路激活	TRUE
8040:0C 输入功率模式	电源模式 A：引脚 1（+）/引脚 3（-）
FSIN 模块 1 设置通道	-
8041:01 通道 1. 输入滤波时间	0x000A（1ms）

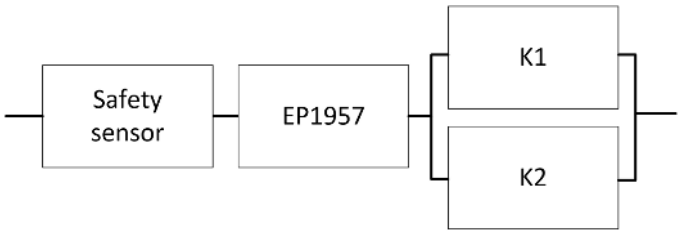
参数	值
8041:02 通道 1. 诊断测试脉冲滤波时间	0x0002（0.2 ms）
8041:04 通道 2. 输入滤波时间	0x000A（1ms）
8041:05 通道 2. 诊断测试脉冲滤波时间	0x0002（0.2 ms）
FSIN 模块 4 公共设置	-
8070:04 诊断测试脉冲激活	TRUE
8070:05 模块故障链路激活	TRUE
8070:0C 输入功率模式	诊断测试脉冲
FSIN 模块 4 设置通道	-
8071:01 通道 1. 输入滤波时间	0x000A（1ms）
8071:02 通道 1. 诊断测试脉冲滤波时间	0x0002（0.2 ms）

MON FB 参数

参数	值
复位时间（ms）（端口 EDM1）	1000
偏差时间（ms）（端口 MonIn1/MonIn2）	500
偏差错误后的安全输入	TRUE

4.11.2 功能块结构和安全回路

4.11.2.1 安全功能 1



4.11.3 计算

4.11.3.1 PFHD / MTTFD / B10D – 值

组件	值
EP1957 – PFH_D	6.50E-09
安全传感器 – PFH_D（已经过认证，符合 EN 60947-5-3 和 EN ISO 13849 标准）	1.00E-08（Cat. 4 / PL e）
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

4.11.3.2 诊断覆盖率 DC

组件	值
带 OSSD 输出的安全传感器	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%

4.11.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

K1/K2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

并假设 K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

K1/K2

$$PFH = \frac{1 - 0{,}99}{1766{,}3 * 8760} = 6{,}46E - 10$$

现在必须做出以下假设：

接触器 K1 和 K2 均连接至安全功能。接触器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：接触器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(SafetySensor)} + PFH_{(EP1957)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1 - \beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 1,00E-08 + 6,50E-09 + 10\% * \frac{6,46E-10 + 6,46E-10}{2}$$
$$= 1,66E-08$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(SafetySensor)}} + \frac{1}{MTTF_{D(EP1957)}} + \frac{1}{MTTF_{D(K1)}}$$

如果仅有 EP1957 和安全传感器的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EP1957)} = \frac{(1 - DC_{(EP1957)})}{PFH_{(EP1957)}} = \frac{(1 - 0,99)}{6,50E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{5,69E-05\frac{1}{y}} = 175y$$

$$MTTF_{D(SafetySensor)} = \frac{(1 - DC_{(SafetySensor)})}{PFH_{(SafetySensor)}} = \frac{(1 - 0,99)}{1,00E-08\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{8,76E-05\frac{1}{y}} = 114y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{114y} + \frac{1}{175y} + \frac{1}{1766,3y}} = 66y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(SafetySensor)}} + \frac{DC}{MTTF_{D(EP1957)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(SafetySensor)}} + \frac{1}{MTTF_{D(EP1957)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{114y} + \frac{99\%}{175y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y}}{\frac{1}{114y} + \frac{1}{175y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 99,00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	**⩾ 10^{-8} 至 < 10^{-7}**
2	⩾ 10^{-7} 至 < 10^{-6}
1	⩾ 10^{-6} 至 < 10^{-5}

注意

安全完整性等级

该应用符合 EN 62061 标准的安全完整性等级 SIL3 要求。

5 电位组

5.1 具有下游无干扰标准端子模块的电位组全极断开（类别 4，PL e）

防护门使用 EL1904 安全输入上的常闭和常开触点组合。输入测试已激活，并对信号进行差异测试（200 ms）。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。

来自 KL/EL9110 的诊断信息（电源触点存在 24 V 电压）经取反后，与接触器 K1、K2、K3 和 K4 的反馈信号进行“与”运算，再传送至 EDM 输入。

通过接触器 K1 和 K2 的常开触点关闭电位组电源触点（24 V 和 0 V）的供电。所用负载（在本示例中为 K3 和 K4）的 0 V 电位必须始终反馈至电位组。

注意

安全考量

使用的 EL/KL9110 和 EL/KL2xxx 端子模块并非安全控制器的有源部分。因此，达到的安全等级只能通过上级安全控制器定义。标准端子模块**不**包括在计算中。
标准端子模块的外部布线会导致最大可达到的安全级别有限。

注意

电源单元要求

标准端子模块必须由 SELV/PELV 电源单元提供 24 V 电压，在发生故障时，最大输出电压 U_{max} 限制为 60 V。

⚠ 谨慎

预防反馈

通过各种措施可以预防反馈（请参见下文更多信息）：

- 不能切换有独立电源的负载
- 接地反馈和全极断线**（在本例中使用）**
  或
  电缆短路故障排除（独立的护套电缆，仅在控制柜内布线，每个导线的专用接地线）

注意

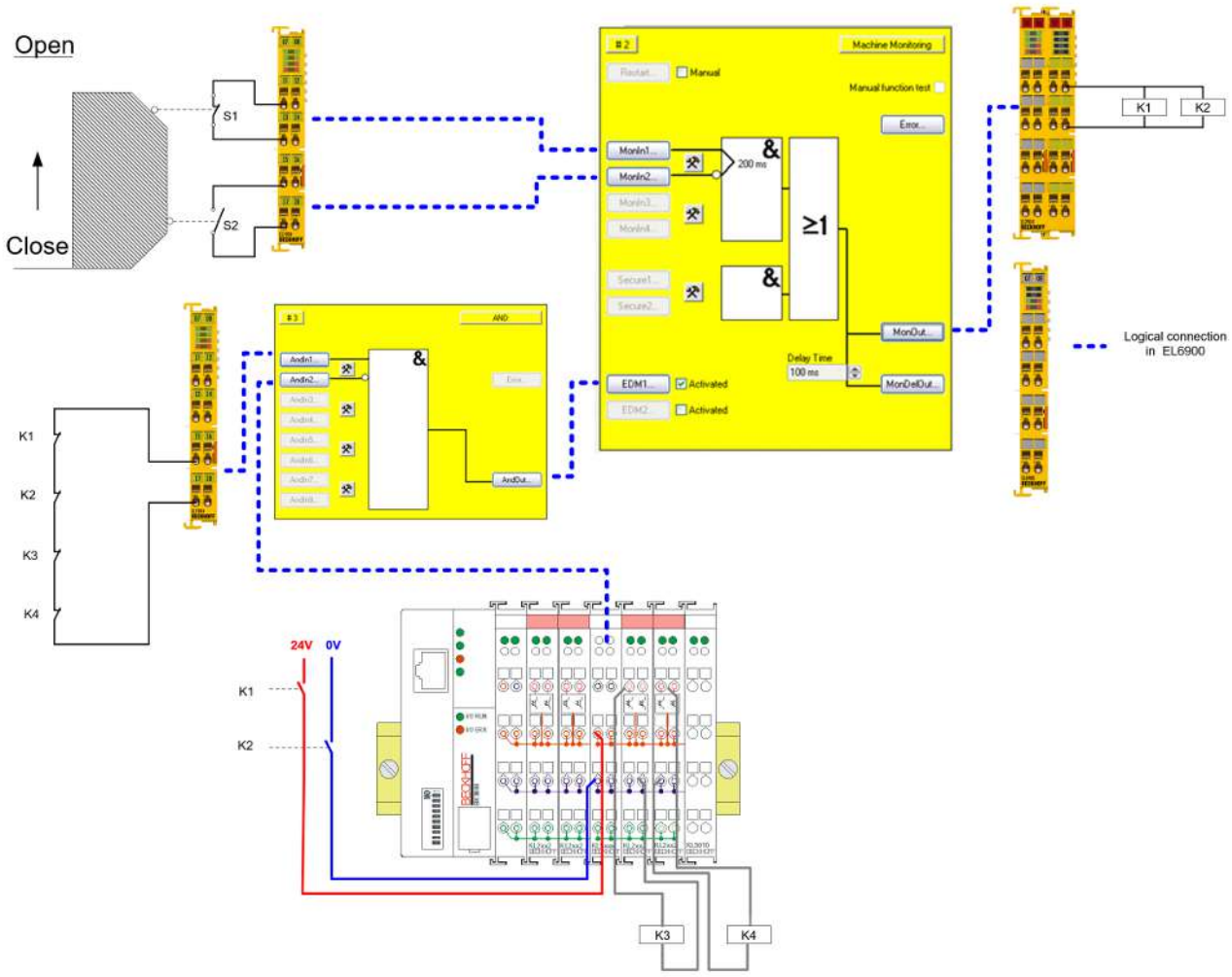
无干扰总线端子模块

无干扰总线端子模块的列表可在倍福信息系统中找到 http://infosys.beckhoff.de。

注意

最大可达到的安全级别

通过接地反馈和全极断线避免反馈：
DIN EN ISO 13849-1：最大 cat. 4 PL e
IEC 61508：最大 SIL3
EN 62061：最大 SIL3



⚠ 谨慎

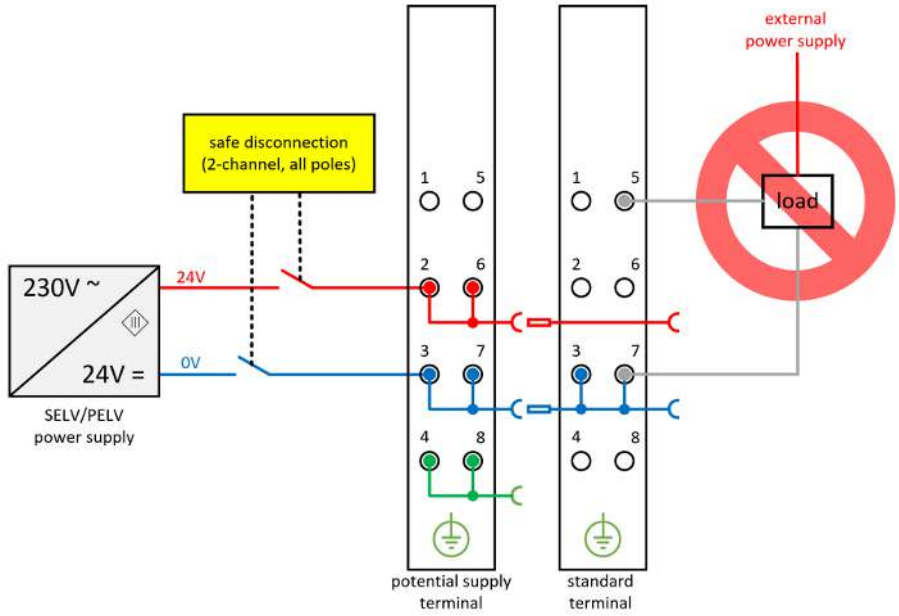
延迟时间

切断电位组的电源供应可能会延迟下游接触器与执行器的关断。此延迟时间取决于下游执行器、负载和线路，用户必须在安全评估中予以考量。

5.1.1 关于预防反馈的说明

5.1.1.1 不能切换有独立电源的负载

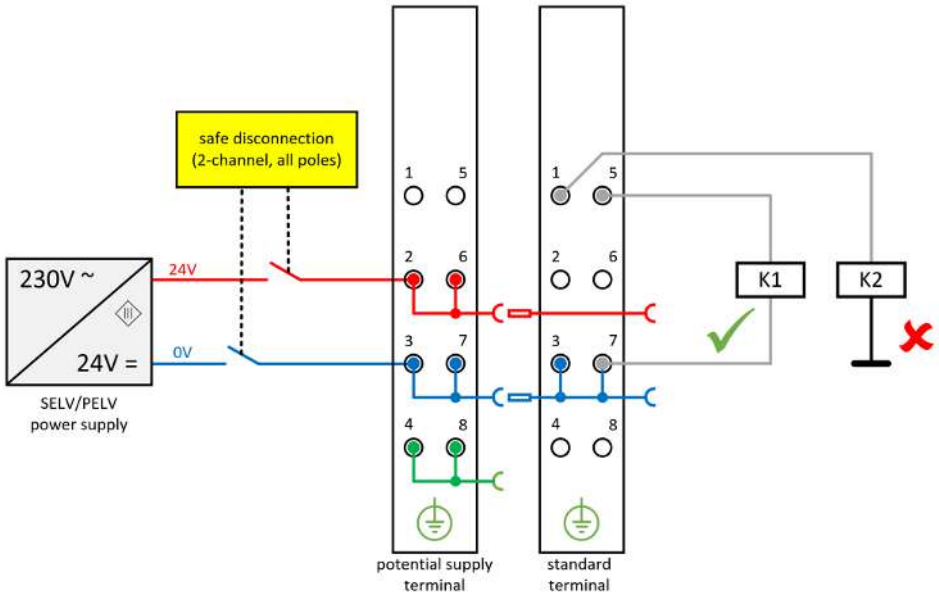
有独立电源的负载不能通过标准端子模块进行切换，因为在这种情况下不能排除通过负载的反馈。



只有当连接负载的制造商保证不会发生对控制输出的反馈时，才允许有一般要求的例外情况。

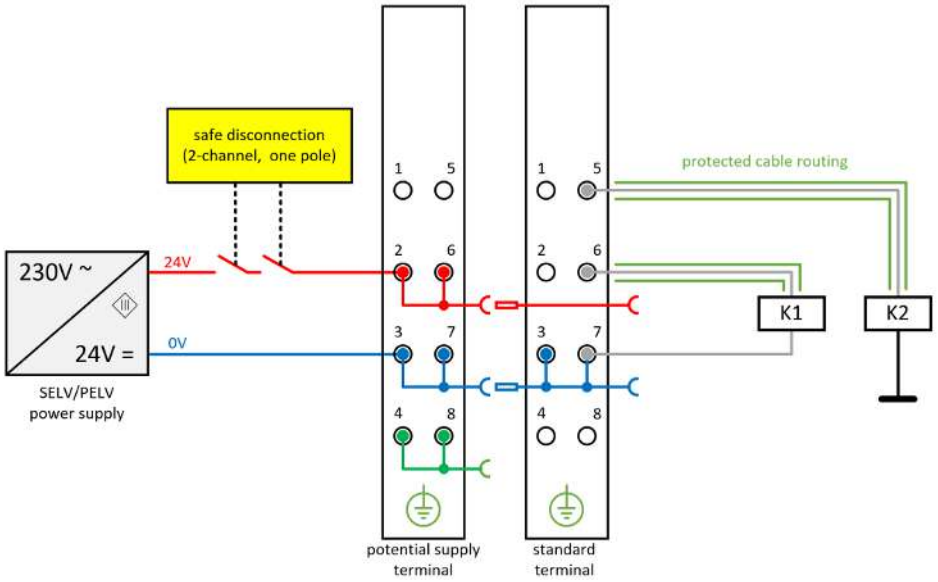
5.1.1.2 选项 1：接地反馈和全极关断（在本例中使用）

所连接负载的接地线必须反馈至相应输出端子模块或电位组的安全切换的接地线。（此处：K1 – 正确接线，K2 – 错误接线）



5.1.1.3 选项 2：电缆短路故障排除

如果选项 1 不可行，如果可以通过其他措施排除电缆短路引起的反馈危险，则可以不采用接地反馈和全极断线。以下措施可作为替代方案实施。



替代方案 1: 通过独立的护套电缆进行负载连接

标准端子模块的非安全切换电位不能与同一护套电缆内的其他带电位导线一起传导

替代方案 2: 仅在控制柜内部布线

所有连接到非安全标准端子模块的负载必须与端子模块位于同一个控制柜内。完全在控制柜内布线。

替代方案 3: 每个导线的专用接地线

所有连接到非安全标准端子模块的导线都由独立的接地线保护。

替代方案 4: 永久（固定）接线，防止外部损坏

所有连接到非安全标准端子模块的导线都固定安装，并通过电缆通道或铠装管等方式防止外部损坏。

⚠ 谨慎

故障排除

设备制造商或用户须全权负责所采用替代方案的正确实施与安全评估。

5.1.2 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

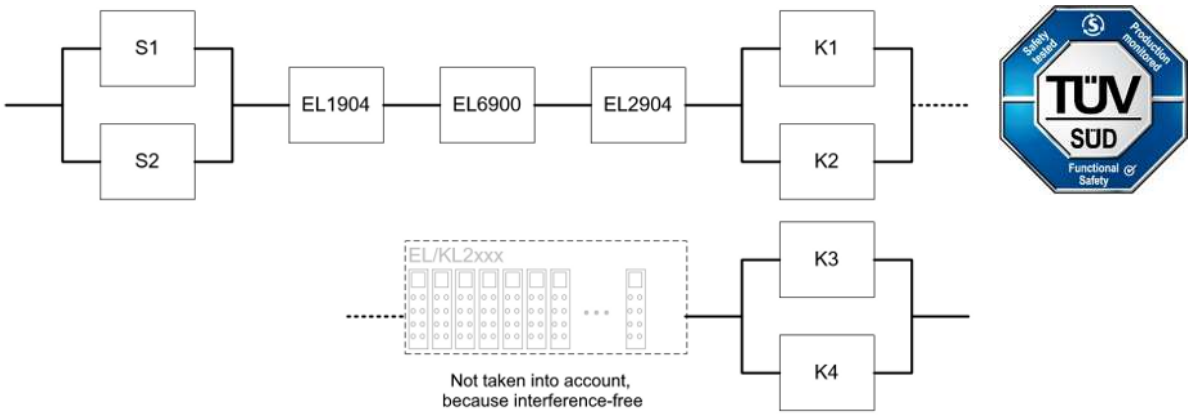
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

5.1.3 功能块结构和安全回路

5.1.3.1 安全功能 1



5.1.4 计算

5.1.4.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
K3 – $B10_D$	1,300,000
K4 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

5.1.4.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%
带 EDM 的 K3/K4	DC_{avg}=90%

5.1.4.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K1/K2/K3/K4：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

并假设 S1、S2、K1、K2、K3 和 K4 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}40E - 10$$

S2

$$PFH = \frac{1 - 0{,}99}{2717{,}4 * 8760} = 4{,}20E - 10$$

K1/K2

$$PFH = \frac{1 - 0{,}99}{1766{,}3 * 8760} = 6{,}46E - 10$$

K3/K4

$$PFH = \frac{1 - 0{,}90}{1766{,}3 * 8760} = 6{,}46E - 09$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

接触器 K1、K2、K3 和 K4 均连接至安全功能。接触器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1、K2、K3 和 K4 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：接触器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09$$
$$+10\% * \frac{6,46E-10 + 6,46E-10}{2} + 10\% * \frac{6,46E-09 + 6,46E-09}{2}$$
$$= 4,16E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K3)}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 206,7y$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y} + \frac{99\%}{1766,3y} + \frac{99\%}{1766,3y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}}$$
$$= 97,39\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	**⩾ 10^{-8} 至 < 10^{-7}**
2	⩾ 10^{-7} 至 < 10^{-6}
1	⩾ 10^{-6} 至 < 10^{-5}

5.2 采用故障排除且具有下游无干扰标准端子模块的电位组全极断开（类别 4，PL e）

防护门使用 EL1904 安全输入上的常闭和常开触点组合。输入测试已激活，信号已进行差异检查（在本示例中为 200 ms）。接触器 K1 和 K2 并联连接至安全输出。该电路已激活电流测量与输出测试功能。
接触器 K1、K2、K3 和 K4 的反馈信号被传送至 EDM 输入。

通过接触器 K1 和 K2 的常开触点仅关闭电位组电源触点的 24 V 供电。电源触点的 0 V 连接直接反馈至电源的 0 V 端。

所有使用的负载与设备的 0 V 电位必须处于或连接至同一电位。

注意

安全考量

使用的 EL/KL9110 和 EL/KL2xxx 端子模块并非安全控制器的有源部分。因此，达到的安全等级只能通过上级安全控制器定义。标准端子模块**不**包括在计算中。
标准端子模块的外部布线会导致最大可达到的安全级别有限。

注意

电源单元要求

标准端子模块必须由 SELV/PELV 电源单元提供 24 V 电压，在发生故障时，最大输出电压 U_{max} 限制为 60 V。

⚠ 谨慎

预防反馈

通过各种措施可以预防反馈（请参见下文更多信息）：

- 不能切换有独立电源的负载
- 接地反馈和全极断线
  或
  电缆短路故障排除（独立的护套电缆，仅在控制柜内布线，每个导线的专用接地线）
  （在本例中使用）

注意

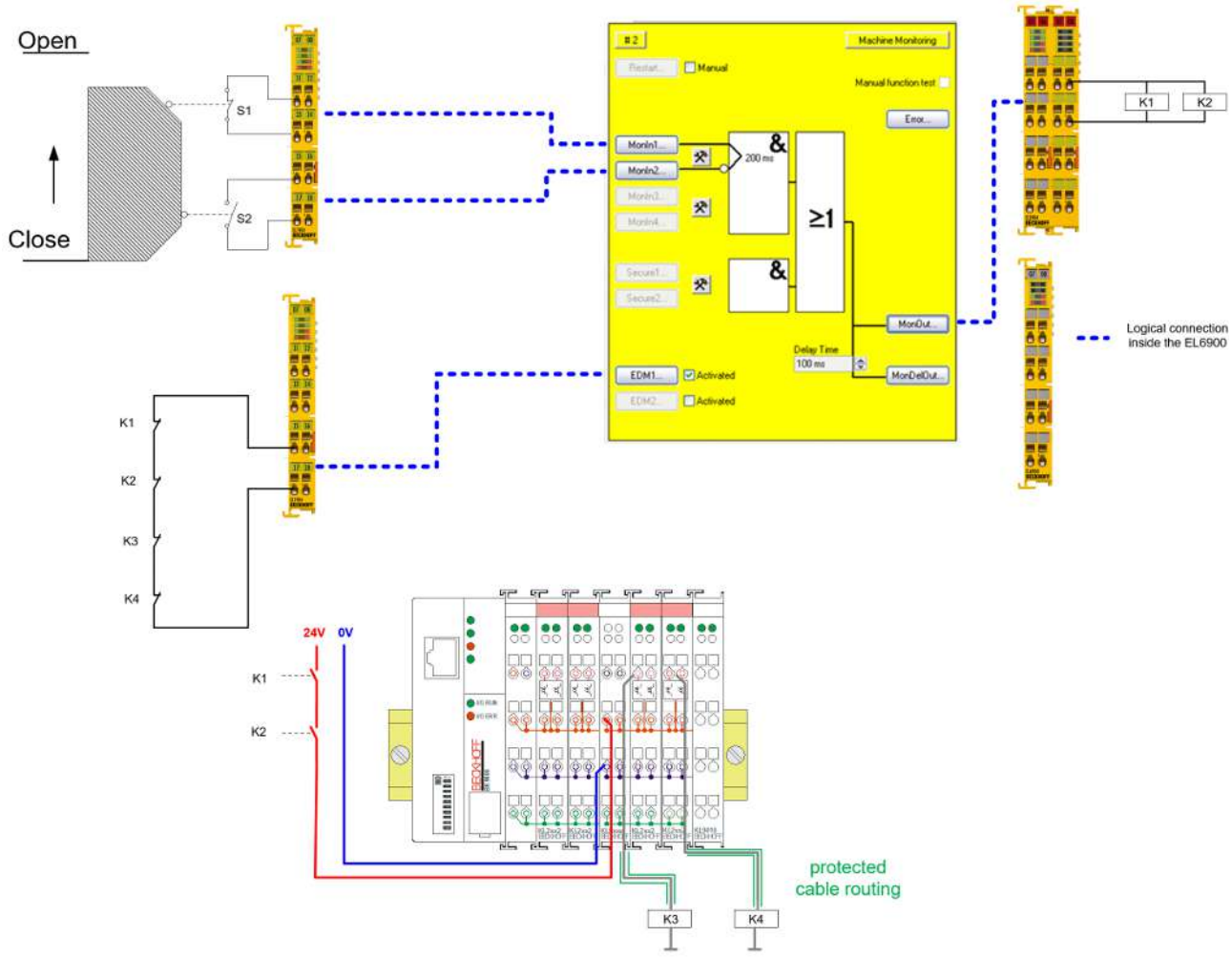
无干扰总线端子模块

无干扰总线端子模块的列表可在倍福信息系统中找到
http://infosys.beckhoff.de。

注意

最大可达到的安全级别

通过短路故障排除避免反馈：
DIN EN ISO 13849-1：最大 cat. 4 PL e
IEC 61508：最大 SIL3
EN 62061：最大 SIL2



注意

故障排除

由于在从无干扰标准输出端子模块 EL/KL2xxx 至负载（在本示例中为 K3、K4）的接线中采用了“线路短路”故障排除，因此在这种情况下无需使用带诊断功能的馈电端子模块。因此，可以使用 EL/KL9xxx 型馈电端子模块。
负载（在本示例中为 K3、K4）的 0 V 电位必须与电位组电源的 0 V 电位相同。

⚠ 谨慎

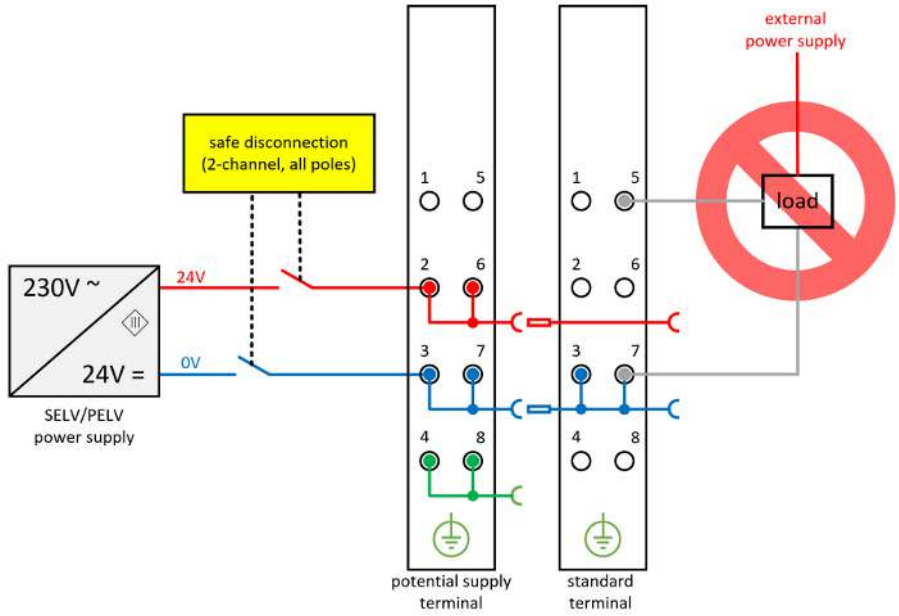
延迟时间

切断电位组的电源供应可能会延迟下游接触器与执行器的关断。此延迟时间取决于下游执行器、负载和线路，用户必须在安全评估中予以考量。

5.2.1 关于预防反馈的说明

5.2.1.1 不能切换有独立电源的负载

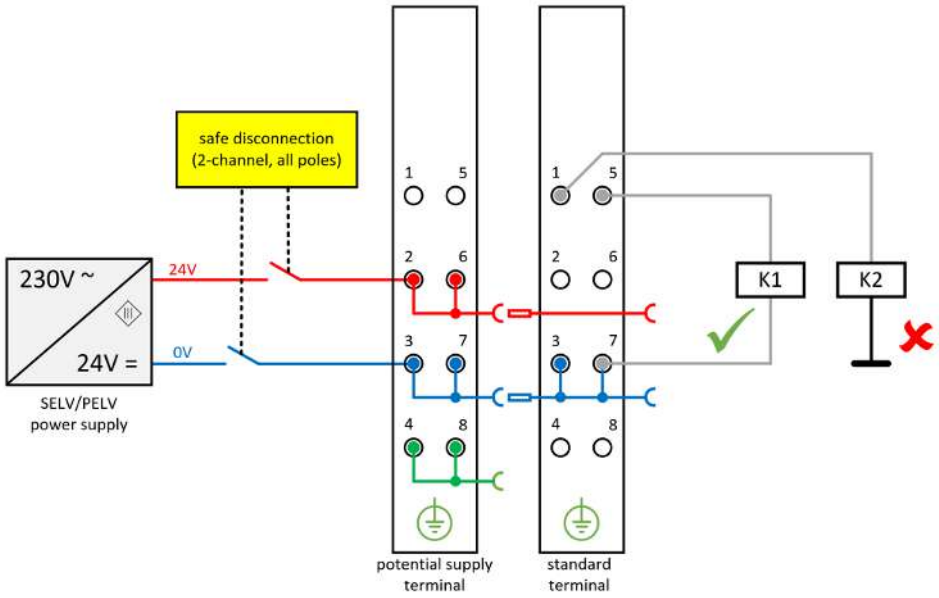
有独立电源的负载不能通过标准端子模块进行切换，因为在这种情况下不能排除通过负载的反馈。



只有当连接负载的制造商保证不会发生对控制输入的反馈时，才允许有一般要求的例外情况。

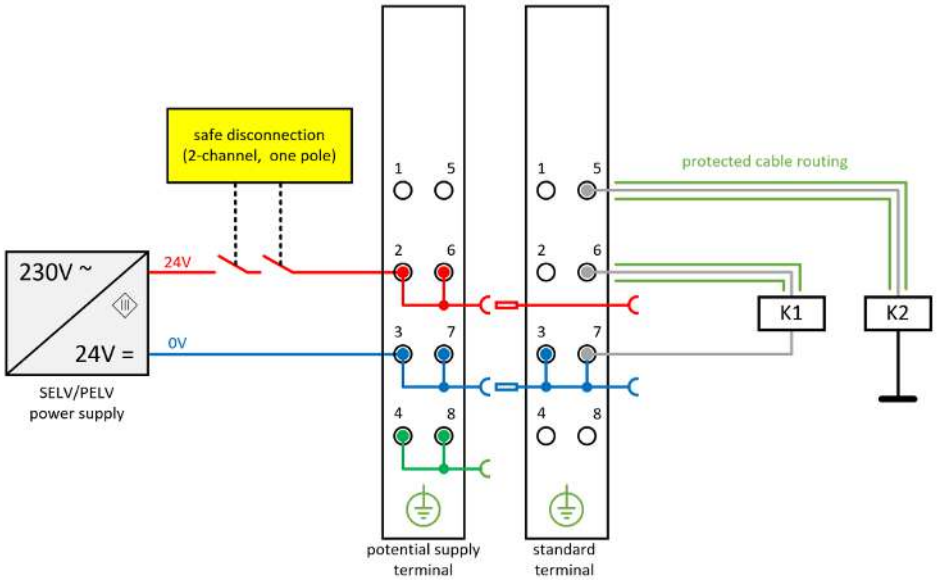
5.2.1.2 选项 1：接地反馈和全极断线

所连接负载的接地线必须反馈至相应输出端子模块或电位组的安全切换的接地线。（此处：K1 – 正确接线，K2 – 错误接线）



5.2.1.3 选项 2：电缆短路错误排除（在本例中使用）

如果选项 1 不可行，如果可以通过其他措施排除电缆短路引起的反馈危险，则可以不采用接地反馈和全极断线。以下措施可作为替代方案实施。



替代方案 1: 通过独立的护套电缆进行负载连接

标准端子模块的非安全切换电位不能与同一护套电缆内的其他带电位导线一起传导

替代方案 2: 仅在控制柜内部布线

所有连接到非安全标准端子模块的负载必须与端子模块位于同一个控制柜内。完全在控制柜内布线。

替代方案 3: 每个导线的专用接地线

所有连接到非安全标准端子模块的导线都由独立的接地线保护。

替代方案 4: 永久（固定）接线，防止外部损坏

所有连接到非安全标准端子模块的导线都固定安装，并通过电缆通道或铠装管等方式防止外部损坏。

⚠ 谨慎

故障排除

设备制造商或用户须全权负责所采用替代方案的正确实施与安全评估。

5.2.2 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

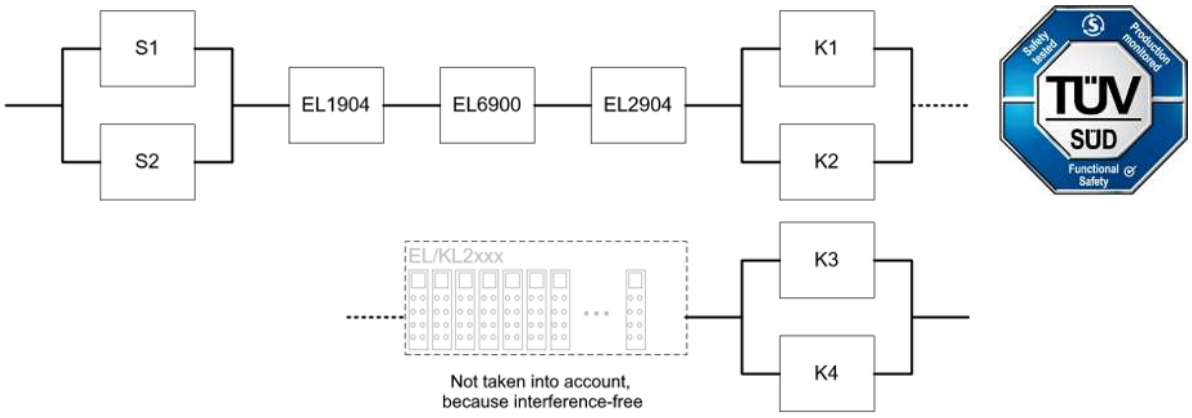
EL2904

参数	值
电流测量激活	是

参数	值
输出测试脉冲激活	是

5.2.3 功能块结构和安全回路

5.2.3.1 安全功能 1



5.2.4 计算

5.2.4.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
K3 – $B10_D$	1,300,000
K4 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

5.2.4.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试和 EDM 的 K1/K2	DC_{avg}=99%
带 EDM 的 K3/K4	DC_{avg}=90%

5.2.4.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K1/K2/K3/K4：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

并假设 S1、S2、K1、K2、K3 和 K4 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}40E - 10$$

S2

$$PFH = \frac{1 - 0{,}99}{2717{,}4 * 8760} = 4{,}20E - 10$$

K1/K2

$$PFH = \frac{1 - 0{,}99}{1766{,}3 * 8760} = 6{,}46E - 10$$

K3/K4

$$PFH = \frac{1-0,90}{1766,3*8760} = 6,46E-09$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

接触器 K1、K2、K3 和 K4 均连接至安全功能。接触器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1、K2、K3 和 K4 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：接触器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09$$
$$+10\% * \frac{6,46E-10 + 6,46E-10}{2} + 10\% * \frac{6,46E-09 + 6,46E-09}{2}$$
$$= 4,16E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K3)}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{1766,3y}+\frac{1}{1766,3y}} = 206,7y$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y}+\frac{99\%}{2717,4y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}+\frac{99\%}{913,2y}+\frac{99\%}{1766,3y}+\frac{99\%}{1766,3y}+\frac{90\%}{1766,3y}+\frac{90\%}{1766,3y}}{\frac{1}{1358,7y}+\frac{1}{2717,4y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{1766,3y}+\frac{1}{1766,3y}+\frac{1}{1766,3y}+\frac{1}{1766,3y}} = 97,39\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2(*)	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

(*) 根据 EN 62061 标准第 6.7.7.2 章，对于 HFT 为 0 且已对可能导致危险失效的故障采取故障排除措施的子系统，其结构约束下的 SILCL 上限为 SIL2。

5.3 具有无干扰标准端子模块的 EL2911 电位组（类别 4，PL e）

防护门使用常闭和常开触点组合，并连接至 EL2911 的安全输入。输入测试已激活，信号已进行差异检查（在本示例中为 500 ms）。在安全输出处关闭电位组电源触点的 24 V 供电。电源触点的 0 V 连接直接反馈至 EL2911 电源的 0 V 端。

EL2911 监测电源触点至 24 V_{DC} 端的反馈信号，一旦在关断状态下读取到高于 5 V 的电压，即进入模块错误状态。

接触器 K3 和 K4 的反馈回路连接至 EL2911 的安全输入。

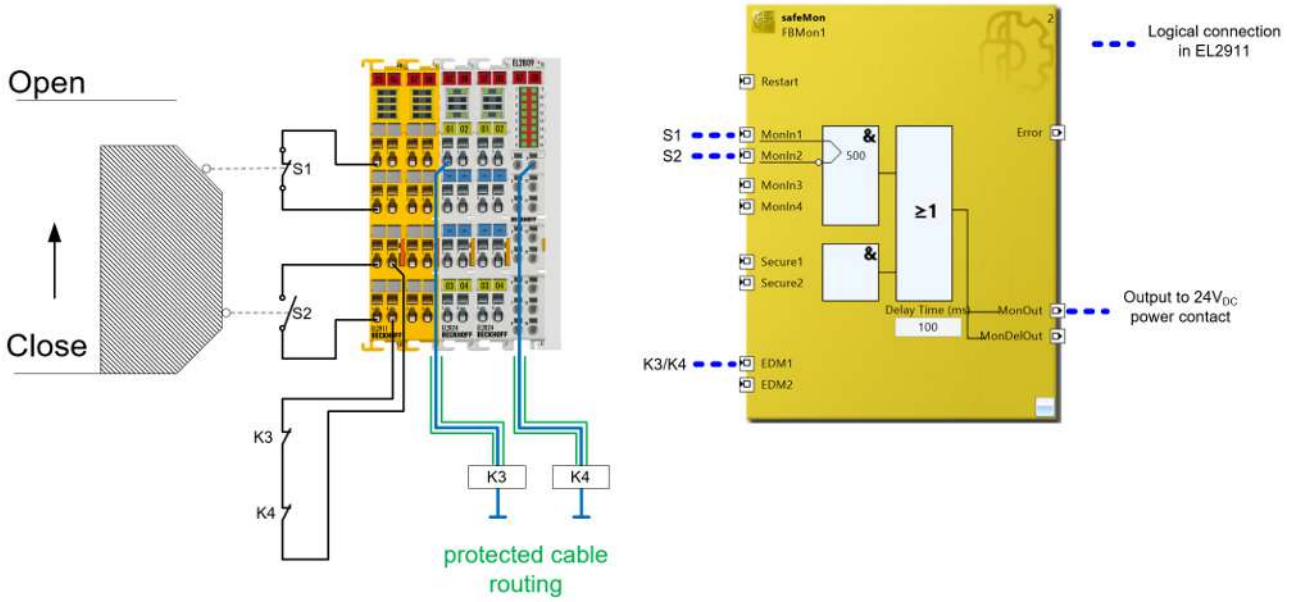
所有使用的负载与设备的 0 V 电位必须处于或连接至同一电位。

注意

安全考量

使用的 EL2xxx 端子模块并非安全控制器的有源部分。因此，达到的安全等级只能通过上级安全控制器定义。标准端子模块**不**包括在计算中，但它们必须无干扰。

标准端子模块的外部布线会导致最大可达到的安全级别有限。



⚠ 谨慎

电源单元要求

标准端子模块必须由 SELV/PELV 电源单元提供 24 V_{DC} 电压，在发生故障时，最大输出电压 U_{max} 限制为 36 V。

⚠ 谨慎

预防反馈

通过各种措施可以预防反馈（请参见下文更多信息）：

- 不能切换有独立电源的负载
- 电缆短路故障排除（独立的非金属护套电缆，仅在控制柜内布线，每个导线的专用接地线，固定安装）

⚠ 谨慎

无干扰 EtherCAT 端子模块

在通过 EL2911 连接的电位组中，只能使用无干扰标准端子模块。无干扰 EtherCAT 端子模块的列表可在倍福信息系统中找到
http://infosys.beckhoff.de。

⚠ 谨慎

最大可达到的安全级别

通过短路故障排除避免反馈：
DIN EN ISO 13849-1：最大 cat. 4 PL e
IEC 61508：最大 SIL3
EN 62061：最大 SIL2

⚠ 谨慎

电位 0V

负载（在本示例中为 K3、K4）的 0 V 电位必须与 EL2911 电源的 0 V 电位相同。

⚠ 谨慎

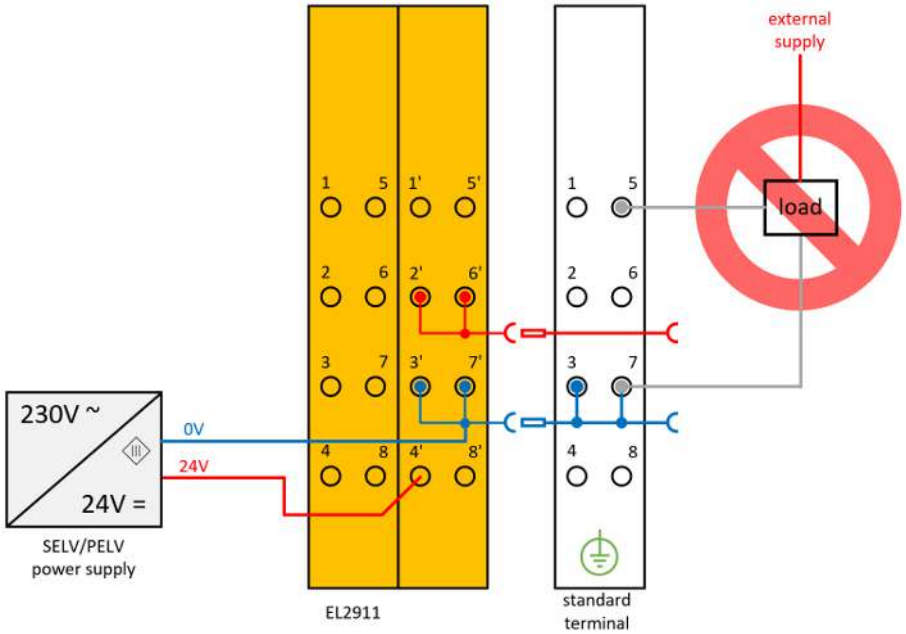
延迟时间

切断电位组的电源供应可能会延迟下游接触器与执行器的关断。此延迟时间取决于下游执行器、负载和线路，用户必须在安全评估中予以考量。

5.3.1 关于预防反馈的说明

5.3.1.1 不能切换有独立电源的负载

有独立电源的负载不能通过标准端子模块进行切换，因为在这种情况下不能排除通过负载的反馈。



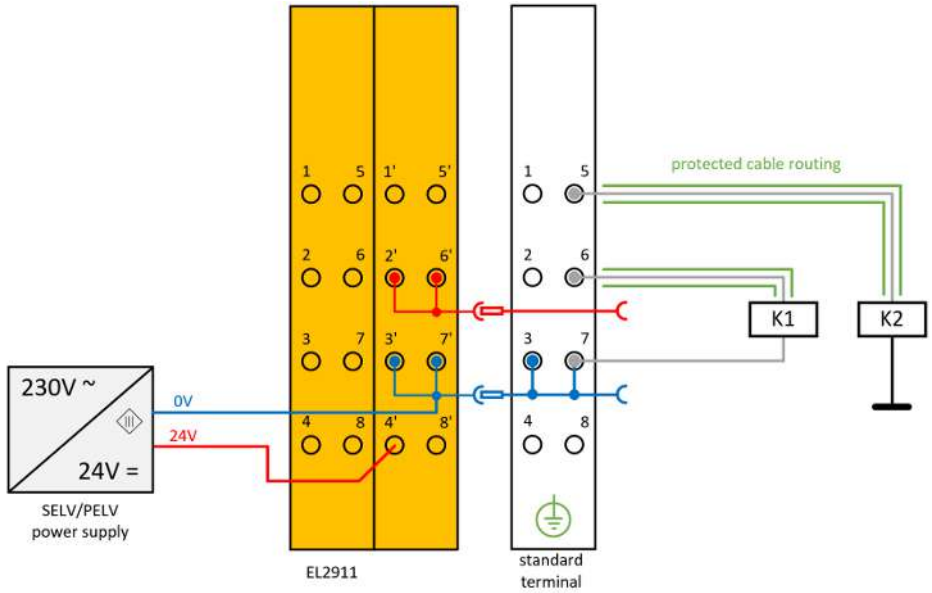
⚠ 谨慎

制造商的数据

只有当连接负载的制造商保证不会发生对控制输入的反馈时，才允许有一般要求的例外情况。

5.3.1.2 电缆短路故障排除

务必通过进一步措施排除因电缆短路导致反馈的危险。以下措施可作为替代方案实施。



替代方案 1: 通过独立的护套电缆进行负载连接

标准端子模块的非安全切换电位不能与同一护套电缆内的其他带电位导线一起传导

替代方案 2: 仅在控制柜内部布线

所有连接到非安全标准端子模块的负载必须与端子模块位于同一个控制柜内。完全在控制柜内布线。

替代方案 3: 每个导线的专用接地线

所有连接到非安全标准端子模块的导线都由独立的接地线保护。

替代方案 4: 永久（固定）接线，防止外部损坏

所有连接到非安全标准端子模块的导线都固定安装，并通过电缆管道或铠装管等方式防止外部损坏。

⚠ 谨慎

故障排除

设备制造商或用户须全权负责所采用替代方案的正确实施与安全评估。

5.3.2 EL2911 参数

EL2911

参数	值
FSOUT 公共设置	-
0x8000:04 – 诊断测试脉冲激活	TRUE
0x8000:12 – 输出交叉短路检测延迟	1000 ms
FSIN 公共设置	-
0x8010:02 - 诊断测试脉冲倍数	0x01
0x8010:04 – 诊断测试脉冲激活	TRUE
FSIN 设置通道	-
0x8011:01 – 通道 1. 输入滤波时间	0x0014（2 ms）
0x8011:02 – 通道 1. 诊断测试脉冲滤波时间	0x0002（0.2 ms）

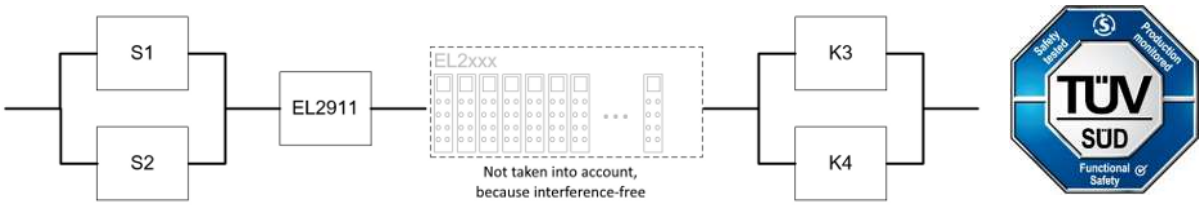
参数	值
0x8011:04 – 通道 2. 输入滤波时间	-
0x8011:05 – 通道 2. 诊断测试脉冲滤波时间	-
0x8011:07 – 通道 3. 输入滤波时间	0x0014（2 ms）
0x8011:08 – 通道 3. 诊断测试脉冲滤波时间	0x0002（0.2 ms）
0x8011:0A – 通道 4. 输入滤波时间	0x0014（2 ms）
0x8011:0B – 通道 4. 诊断测试脉冲滤波时间	0x0002（0.2 ms）

FB MON

参数	值
复位时间（ms）（端口 EDM1）	1000
偏差时间（ms）（端口 MonIn1/MonIn2）	500
偏差错误后的安全输入	TRUE

5.3.3 功能块结构和安全回路

5.3.3.1 安全功能 1



5.3.4 计算

5.3.4.1 PFHD / MTTFD / B10D – 值

组件	值
EL2911 – PFH_D	4.50E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K3 – $B10_D$	1,300,000
K4 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

5.3.4.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带 EDM 的 K3/K4	DC_{avg}=90%

5.3.4.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K3/K4：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

并假设 S1、S2、K3 和 K4 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}40E - 10$$

S2

$$PFH = \frac{1 - 0{,}99}{2717{,}4 * 8760} = 4{,}20E - 10$$

K3/K4

$$PFH = \frac{1 - 0{,}90}{1766{,}3 * 8760} = 6{,}46E - 09$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

接触器 K3 和 K4 均连接至安全功能。接触器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K3 和 K4 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：接触器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL2911)}$$
$$+\beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 4,50E-09 + 10\% * \frac{6,46E-09 + 6,46E-09}{2}$$
$$= 5,21E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}}$$

如果仅有 EL2911 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL2911)} = \frac{(1-DC_{(EL2911)})}{PFH_{(EL2911)}} = \frac{(1-0,99)}{4,50E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{3,94E-05\frac{1}{y}} = 253y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{253y} + \frac{1}{1766,3y}} = 190y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(K3)}} + \frac{DC}{MTTF_{D(K4)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}} + \frac{1}{MTTF_{D(K4)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{253y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{253y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 97,35\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2(*)	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

(*) 根据 EN 62061 标准第 6.7.7.2 章，对于 HFT 为 0 且已对可能导致危险失效的故障采取故障排除措施的子系统，其结构约束下的 SILCL 上限为 SIL2。

5.4 带 EPP9022-9060 的 EPP 电位组（类别 4，PL e）

防护门使用常闭和常开触点组合，并连接至第一个 EL2911（1）的安全输入。输入测试已激活，信号已进行差异检查（在本示例中为 500 ms）。在第二个 EL2911（2）的安全输出处关闭电位组的 24 V 供电 Up。0 V 连接直接反馈至 EL2911 电源的 0 V 端。两个 EL2911 的 0 V 电位处于同一电位或进行桥接。

接触器 K3 和 K4 的反馈回路连接至 EL2911 的安全输入。

所有使用的负载与设备的 0 V 电位必须处于或连接至同一电位。

诊断

EtherCAT p 电缆无法采用故障排除，因为 Us 和 Up 位于共同的护套电缆中，且每个电缆没有专用的接地线。

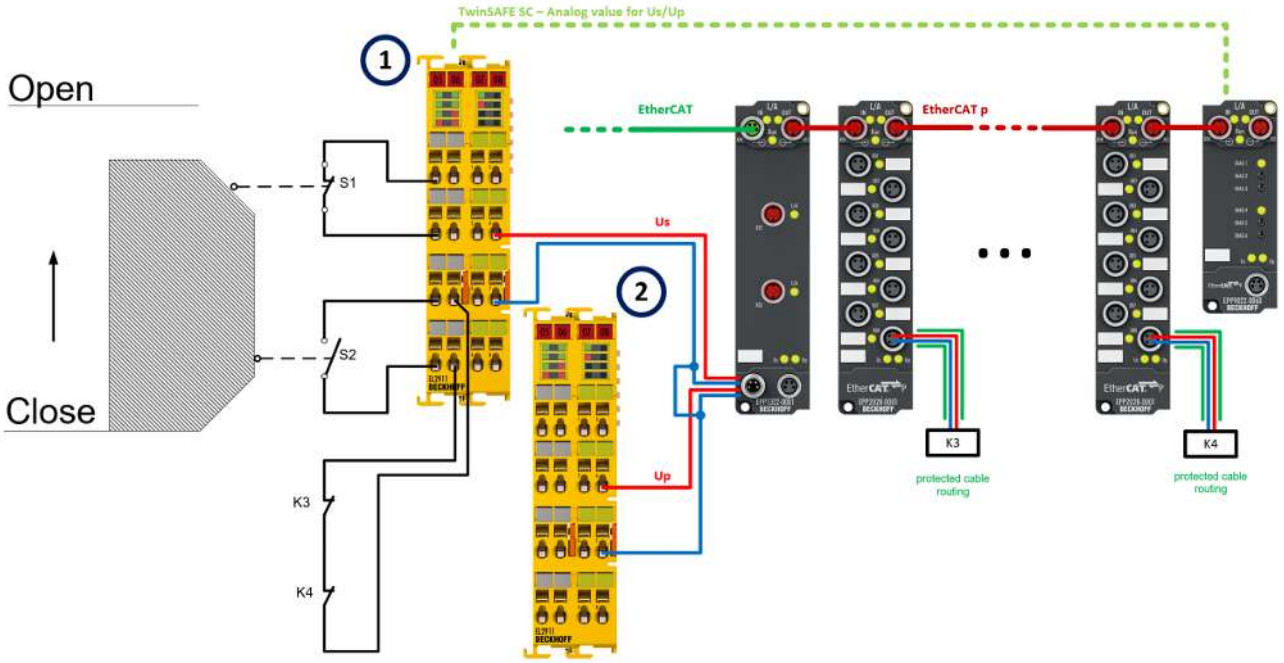
首先，为了诊断 EtherCAT p 电缆上是否存在反馈或交叉短路，EPP9022-9060 EtherCAT p 端子盒会测量电压 Us 和 Up，并由 TwinSAFE SC 将其作为模拟值传输至 EL2911。由此，通信路径上的模拟信号干扰得以排除。其次，EL2911 监测安全输出至 24 V_{DC} 端的反馈信号，一旦在关断状态下读取到高于 5 V 的电压，即进入模块错误状态。

注意

安全考量

使用的 EPP2xxx 端子盒并非安全控制器的有源部分。因此，达到的安全等级只能通过上级安全控制器定义。标准端子盒**不**包括在计算中。

标准端子盒的外部布线会导致最大可达到的安全级别有限（另请参见 关于预防反馈的说明 [▶ 159]）。



⚠ 谨慎

电源单元要求

标准端子模块必须由 SELV/PELV 电源单元提供 24 V_{DC} 电压，在发生故障时，最大输出电压 U_{max} 限制为 36 V。

⚠ 谨慎

预防反馈

通过各种措施可以预防反馈（请参见下文更多信息）：

- 不能切换有独立电源的负载
- 电缆短路故障排除（独立的非金属护套电缆，仅在控制柜内布线，每个导线的专用接地线，固定安装）

⚠ 谨慎

最长安全响应时间

检测故障的最长时间（故障检测时间）出现在通过读取接触器 K3 和 K4 的反馈回路进行故障检测时，因为该时间通常比通过回读 EL2911 和 EPP9022-9060 上的电压进行故障检测的时间要长得多。该时间在安全逻辑中进行设置，并应设置得足够长，以实现快速错误检测，但同时还须确保设备的可用性。

故障响应时间由以下部分构成：EL2911 的输入滤波时间（反馈回路所连接的安全输入）、在 EL2911 上运行的逻辑程序的循环时间的两倍（也可从 CoE 对象中读取）以及在 EL2911 输出处切断电压后接触器 K3 和 K4 的释放时间。该时间在很大程度上取决于所使用的执行器。

这两个时间之和就是安全响应时间。

$$SafetyResponseTime = FaultDetectionTime + FaultReactionTime$$
$$= EDMtime + InputfilterTimeEL2911 + 2 * LogicCycleTime + SwitchOffTimeAktuators$$

用户或设备制造商在对其应用进行安全评估时，必须参考并检查该安全响应时间。

安全应用

如果用于 Up 的 EL2911（2）安全输出被切断，则通过 TwinSAFE SC 传输的 Up 模拟值信号必须小于 5 V。如果不是这样，则必须同时切断两个 EL2911 输出（1） + （2）。这可以通过 EDM 功能块实现，例如将其与输出 Us 和 Up 编程在同一 TwinSAFE 组中，从而在发生错误时切断整个组及组内配置的所有输出。

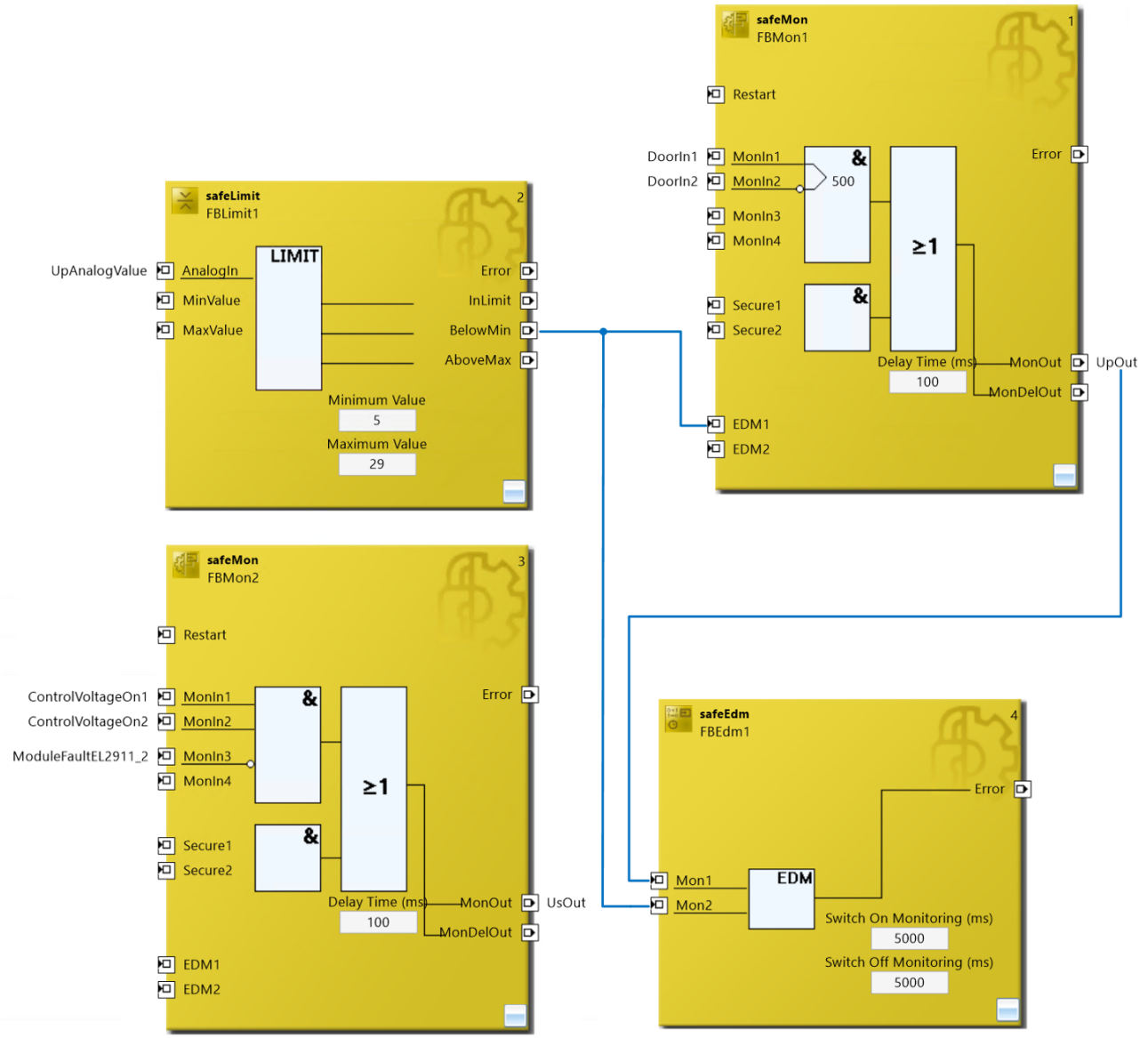
此外，在发生模块错误的情况下，必须切断用于 Up 的 EL2911（2）和用于 Us 的 EL2911（1）。

⚠ 谨慎

安全应用的实施

用户或设备制造商须全权负责安全应用的正确实施与测试。

安全应用示例



注意

反馈回路

为了清晰起见，未显示执行器 K3 和 K4 的反馈回路，但用户必须予以考量。

注意

最大可达到的安全级别

通过短路故障排除避免反馈：
DIN EN ISO 13849-1：最大 cat. 4 PL e
IEC 61508：最大 SIL3
EN 62061：最大 SIL2

注意

电位 0 V

负载（在本示例中为 K3、K4）的 0 V 电位必须与两个 EL2911 电源的 0 V 电位相同。

⚠ 谨慎

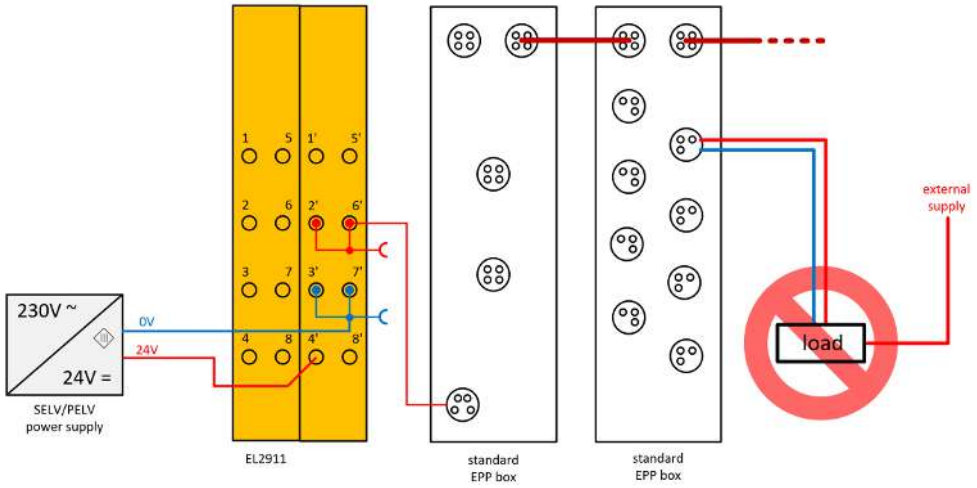
延迟时间

切断电位组的电源供应可能会延迟下游接触器与执行器的关断。此延迟时间取决于下游执行器、负载和线路，用户必须在安全评估中予以考量。

5.4.1 关于预防反馈的说明

5.4.1.1 不能切换有独立电源的负载

有独立电源的负载不能通过标准端子盒进行切换，因为在这种情况下不能排除通过负载的反馈。



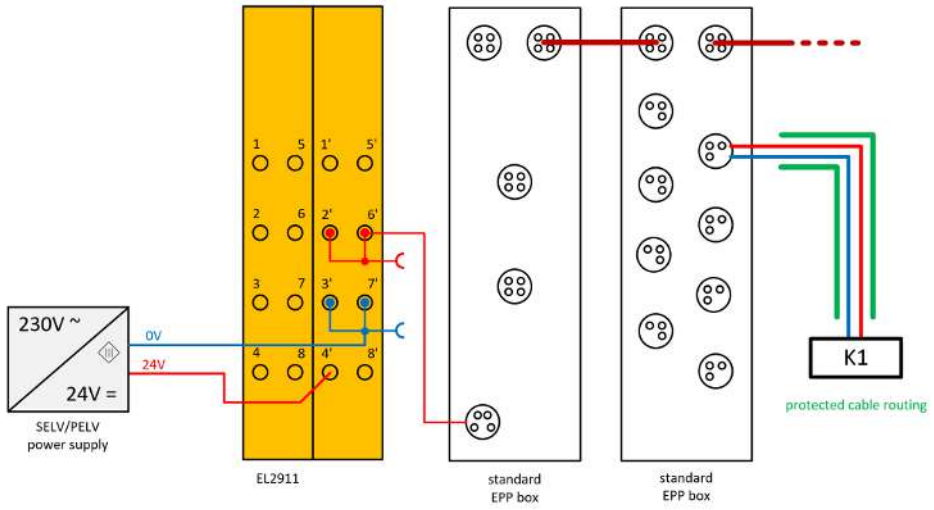
⚠ 谨慎

制造商的数据

只有当连接负载的制造商保证不会发生对控制输入的反馈时，才允许有一般要求的例外情况。

5.4.1.2 电缆短路故障排除

务必通过进一步措施排除因电缆短路导致反馈的危险。以下措施可作为替代方案实施。



替代方案 1: 通过独立的护套电缆进行负载连接

标准端子模块的非安全切换电位不能与同一护套电缆内的其他带电位导线一起传导

替代方案 2: 仅在控制柜内部布线

所有连接到非安全标准端子模块的负载必须与端子模块位于同一个控制柜内。完全在控制柜内布线。

替代方案 3: 每个导线的专用接地线

所有连接到非安全标准端子模块的导线都由独立的接地线保护。

替代方案 4: 永久（固定）接线，防止外部损坏

所有连接到非安全标准端子模块的导线都固定安装，并通过电缆管道或铠装管等方式防止外部损坏。

⚠ 谨慎

故障排除

设备制造商或用户须全权负责所采用替代方案的正确实施与安全评估。

5.4.2 EL2911 参数

EL2911（适用于所有 EL2911）

参数	值
FSOUT 公共设置	-
0x8000:04 – 诊断测试脉冲激活	TRUE
0x8000:12 – 输出交叉短路检测延迟	1000 ms
FSIN 公共设置	-
0x8010:02 - 诊断测试脉冲倍数	0x01
0x8010:04 – 诊断测试脉冲激活	TRUE
FSIN 设置通道	-
0x8011:01 – 通道 1. 输入滤波时间	0x0014（2 ms）
0x8011:02 – 通道 1. 诊断测试脉冲滤波时间	0x0002（0.2 ms）
0x8011:04 – 通道 2. 输入滤波时间	-
0x8011:05 – 通道 2. 诊断测试脉冲滤波时间	-

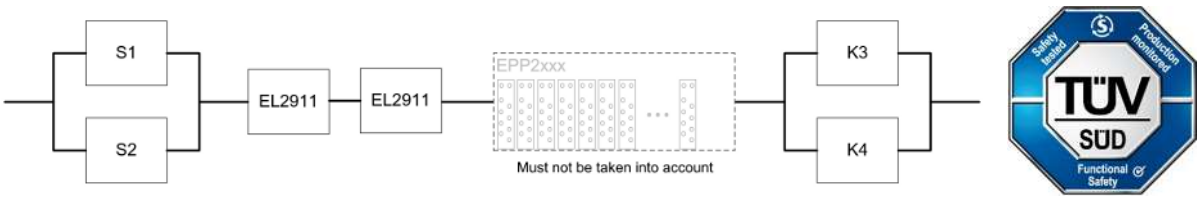
参数	值
0x8011:07 – 通道 3. 输入滤波时间	0x0014（2 ms）
0x8011:08 – 通道 3. 诊断测试脉冲滤波时间	0x0002（0.2 ms）
0x8011:0A – 通道 4. 输入滤波时间	0x0014（2 ms）
0x8011:0B – 通道 4. 诊断测试脉冲滤波时间	0x0002（0.2 ms）

FB MON

参数	值
复位时间（ms）（端口 EDM1）	1000
偏差时间（ms）（端口 MonIn1/MonIn2）	500
偏差错误后的安全输入	TRUE

5.4.3 功能块结构和安全回路

5.4.3.1 安全功能 1



5.4.4 计算

5.4.4.1 PFHD / MTTFD / B10D – 值

组件	值
EL2911 – PFH_D	4.50E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K3 – $B10_D$	1,300,000
K4 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

5.4.4.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带 EDM 的 K3/K4	DC_{avg}=90%

5.4.4.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K3/K4：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

并假设 S1、S2、K3 和 K4 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}40E - 10$$

S2

$$PFH = \frac{1 - 0{,}99}{2717{,}4 * 8760} = 4{,}20E - 10$$

K3/K4

$$PFH = \frac{1 - 0{,}90}{1766{,}3 * 8760} = 6{,}46E - 09$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

接触器 K3 和 K4 均连接至安全功能。接触器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K3 和 K4 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：接触器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL2911)} + PFH_{(EL2911)} + \beta * \frac{PFH_{(K3)} + PFH_{(K4)}}{2} + (1-\beta)^2 * (PFH_{(K3)} * PFH_{(K4)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{8,40E-10 + 4,20E-10}{2} + 4,50E-09 + 4,50E-09 + 10\% * \frac{6,46E-09 + 6,46E-09}{2} = 9,71E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}}$$

如果仅有 EL2911 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL2911)} = \frac{(1-DC_{(EL2911)})}{PFH_{(EL2911)}} = \frac{(1-0,99)}{4,50E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{3,94E-05\frac{1}{y}} = 253y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y} + \frac{1}{253y} + \frac{1}{253y} + \frac{1}{1766,3y}} = 108y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(EL2911)}} + \frac{DC}{MTTF_{D(K3)}} + \frac{DC}{MTTF_{D(K4)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(EL2911)}} + \frac{1}{MTTF_{D(K3)}} + \frac{1}{MTTF_{D(K4)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y} + \frac{99\%}{2717,4y} + \frac{99\%}{253y} + \frac{99\%}{253y} + \frac{90\%}{1766,3y} + \frac{90\%}{1766,3y}}{\frac{1}{1358,7y} + \frac{1}{2717,4y} + \frac{1}{253y} + \frac{1}{253y} + \frac{1}{1766,3y} + \frac{1}{1766,3y}} = 98,00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2(*)	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

(*) 根据 EN 62061 标准第 6.7.7.2 章，对于 HFT 为 0 且已对可能导致危险失效的故障采取故障排除措施的子系统，其结构约束下的 SILCL 上限为 SIL2。

6 STO/SS1 功能

6.1 AX8xxx-x1xx STO 功能（类别 4，PL e）

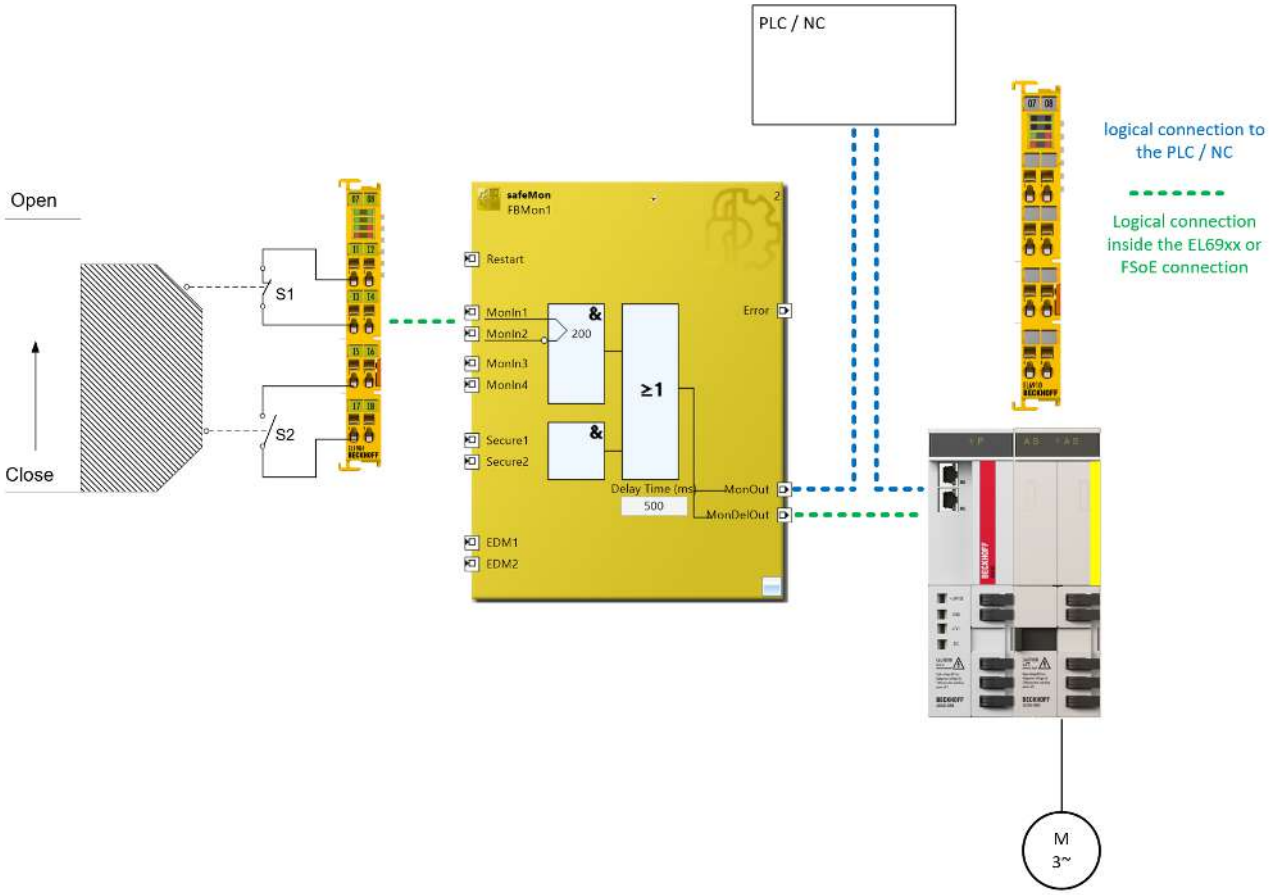
防护门通过常闭/常开触点组合连接至 EL1904 的安全输入。输入测试脉冲已激活。在 TwinSAFE 逻辑中，防护门连接至 FB Mon，直接切换输出用于通知 NC 控制器，例如，在 500 ms 后将执行 STO，因此需要启动停止斜坡。

例如，在 500 ms 后，将通过延迟切换输出通知 AX8xxx-x1xx 将要激活 STO。

在本例中，假设在门开启和 AX8xxx-x1xx 延迟切换的作用下，在用户抵达危险点之前，设备将在 STO 之后进入安全状态。

设备制造商必须对设备和应用进行评估。

如果要在驱动器上执行其他应用，则可通过 AX8xxx-x1xx 上的客户特定逻辑应用来实现。



6.1.1 安全输入和输出模块的参数

EL1904

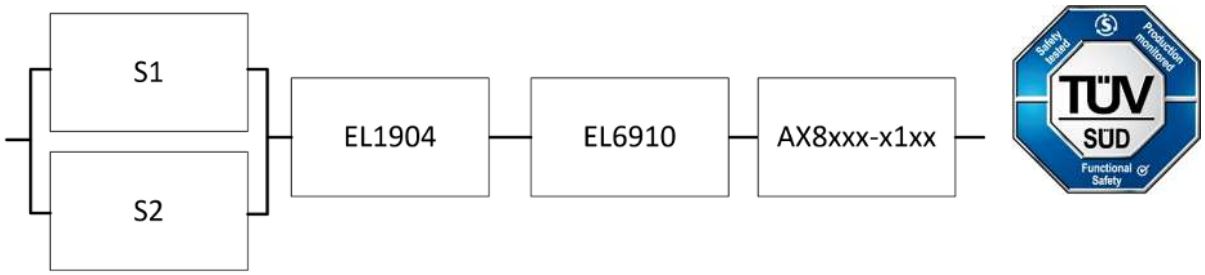
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	-
传感器测试通道 4 激活	-
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

MON FB 参数

参数	值
偏差时间（ms）（端口 MonIn1/MonIn2）	200
偏差错误后的安全输入	TRUE
MON 延迟时间	500

6.1.2 功能块结构和安全回路

6.1.2.1 安全功能 1



6.1.3 计算

6.1.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL6910 – PFH_D	1.79E-09
AX8xxx-x1xx - PFH_D	3.04E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

6.1.3.2 诊断覆盖率 DC

组件	值
带测试和合理性检查的 S1	DC_{avg}=99%
AX8xxx-x1xx STO 功能	DC_{avg}>99%

6.1.3.3 安全功能 1 的计算

根据 EN ISO 13849-1:2015 标准计算性能等级

根据 $B10_D$ 值计算 $MTTF_D$ 值

从：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 14720} = 679y$$

S2

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 14720} = 1358y$$

根据以下公式计算总 $MTTF_D$ 值：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}$$

如果仅有 EL1904、EL6910 和 AX8xxx-x1xx 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}99)}{1{,}11E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0{,}01}{9{,}72E-06 \frac{1}{y}} = 1028{,}8y$$

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0{,}01}{15{,}68E-06 \frac{1}{y}} = 637y$$

$$MTTF_{D(AX8xxx-x1xx)} = \frac{(1 - DC_{(AX8xxx-x1xx)})}{PFH_{D(AX8xxx-x1xx)}} = \frac{(1 - 0{,}99)}{3{,}04E-09 \frac{1}{h} * 8760 \frac{h}{y}} = \frac{0{,}01}{2{,}66E-05 \frac{1}{y}} = 375y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679y} + \frac{1}{1028y} + \frac{1}{637y} + \frac{1}{375y}} = 149y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(S2)}} + \frac{DC}{MTTF_{D(EL1904)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(AX8xxx-x1xx)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{679y} + \frac{99\%}{1358y} + \frac{99\%}{1028y} + \frac{99\%}{637y} + \frac{99\%}{375y}}{\frac{1}{679y} + \frac{1}{1358y} + \frac{1}{1028y} + \frac{1}{637y} + \frac{1}{375y}} = 99{,}00\%$$

注意

类别

这种结构最多能达到类别 4。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能**不**属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN 62061 标准计算 PFH_D 值

假设 S1 和 S2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH_D = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH_D = \frac{1 - 0,99}{679 * 8760} = 1,68E - 09$$

S2:

$$PFH_D = \frac{1 - 0,99}{1358 * 8760} = 8,41E - 10$$

现在必须做出以下假设:

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下:

$$PFH_{Dges} = \beta * \frac{PFH_{D(S1)} + PFH_{D(S2)}}{2} + (1 - \beta)^2 * (PFH_{D(S1)} * PFH_{D(S2)}) * T1 + PFH_{D(EL1904)} + PFH_{D(EL6910)} + PFH_{D(AX8xxx-x1xx)}$$

由于 $(1 - \beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至:

$$PFH_{Dges} = 10\% * \frac{1,68E - 09 + 8,41E - 10}{2} + 1,11E - 09 + 1,79E - 09 + 3,04E - 09$$
$$= 6,07E - 09$$

安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	**⩾ 10^{-8} 至 < 10^{-7}**
2	⩾ 10^{-7} 至 < 10^{-6}
1	⩾ 10^{-6} 至 < 10^{-5}

注意

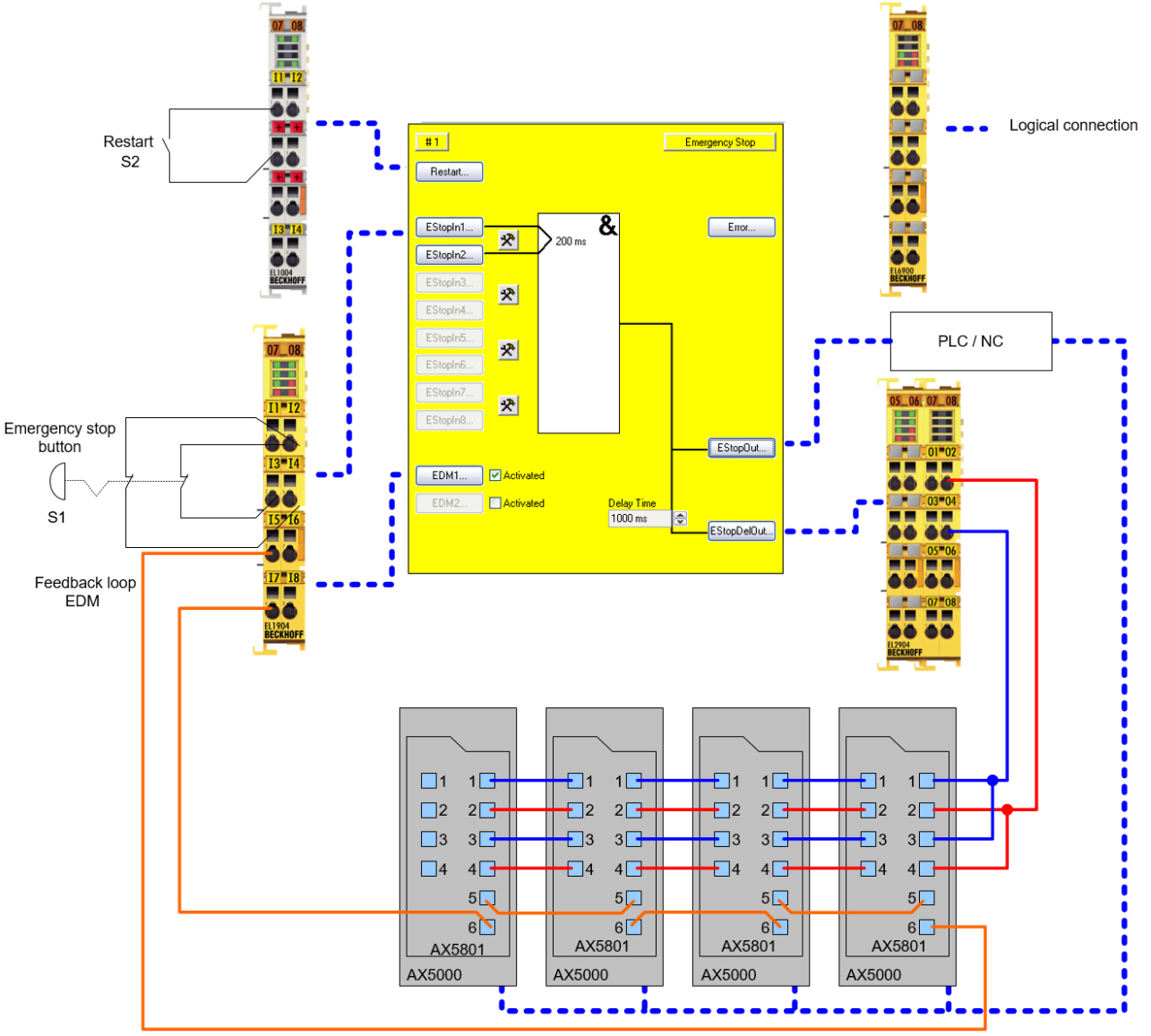
安全完整性等级

该应用符合 EN 62061 标准的安全完整性等级 SIL 3 要求。

6.2 带 SS1 停止功能的 AX5801 驱动器选件（类别 4，PL e）

通过触发急停按钮，FB ESTOP 的输入 EStopIn1 和 EStopIn2 切换为“0”状态，导致 FB ESTOP 的输出 EStopOut 和 EStopDelOut 切换为“0”状态。因此，系统通过 EtherCAT 向 PLC 及 AX5000 发出快速停止指令。ESTOP FB 的输出 EStopDelOut 可确保在指定的延迟时间（在本示例中为 1000 ms）结束后，切断安全选件 AX5801 的 24 V 供电，从而使 AX5801 的内部继电器断电。通过 AX5000 的内部关断路径，两个通道（电机）被切换至无转矩状态。

启动了对输入信号的测试和差异检查。输出测试也已激活。4 个 AX5801 选件卡的继电器并联连接至 EL2904 的安全输出。反馈回路串联连接至安全输入。重启信号连接至非安全输入。



6.2.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是

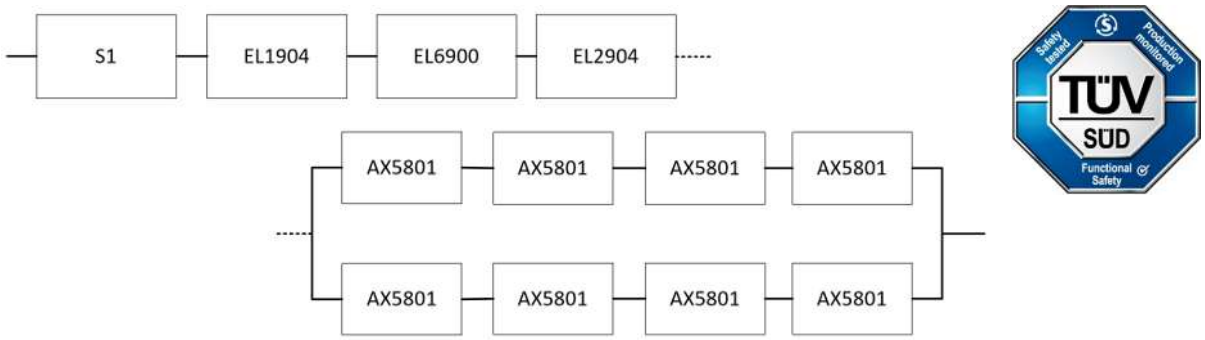
参数	值
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

6.2.2 功能块结构和安全回路

6.2.2.1 安全功能 1



6.2.3 计算

6.2.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
AX5801 – $B10_D$	780,000
S1 – $B10_D$	100,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	60（每小时 1 次）
使用寿命（T1）	20 年 = 175200 小时

6.2.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
AX5801	DC_{avg}=99%

6.2.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{100.000}{0{,}1 * 1840} = 543{,}5y = 4761060h$$

AX5801：

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{780.000}{0{,}1 * 1840} = 4239{,}1y = 37134516h$$

$$T_{10D} = \frac{B10_D}{n_{op}} \frac{780.000}{1840 \frac{1}{y}} = 423y$$

并假设 S1 为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{543{,}5 * 8760} = 2{,}10E - 09$$

AX5801：

$$PFH = \frac{1 - 0{,}99}{4239{,}1 * 8760} = 2{,}70E - 10$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + \beta * \frac{4 * PFH_{(AX5801)} + 4 * PFH_{(AX5801)}}{2} + 4 * (1-\beta)^2 * (PFH_{(AX5801)} * PFH_{(AX5801)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 2{,}10E-09 + 1{,}11E-09 + 1{,}03E-09 + 1{,}25E-09 + 10\% * \frac{4 * 2{,}70E-10 + 4 * 2{,}70E-10}{2} = 5{,}60E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}} + \frac{1}{MTTF_{D(AX5801)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(AX5801)} = \frac{B10_{D(AX5801)}}{0{,}1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0{,}99)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}72E-06\frac{1}{y}} = 1028{,}8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0{,}99)}{1{,}03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}02E-06\frac{1}{y}} = 1108{,}6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{543{,}5y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y}} = 173{,}8y$$

$$DC_{avg} = \frac{\frac{99\%}{543{,}5y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{1108{,}6y} + \frac{99\%}{913{,}2y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y} + \frac{99\%}{4239{,}1y}}{\frac{1}{543{,}5y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y} + \frac{1}{4239{,}1y}} = 99{,}00\%$$

注意

类别

这种结构最多能达到类别 4。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

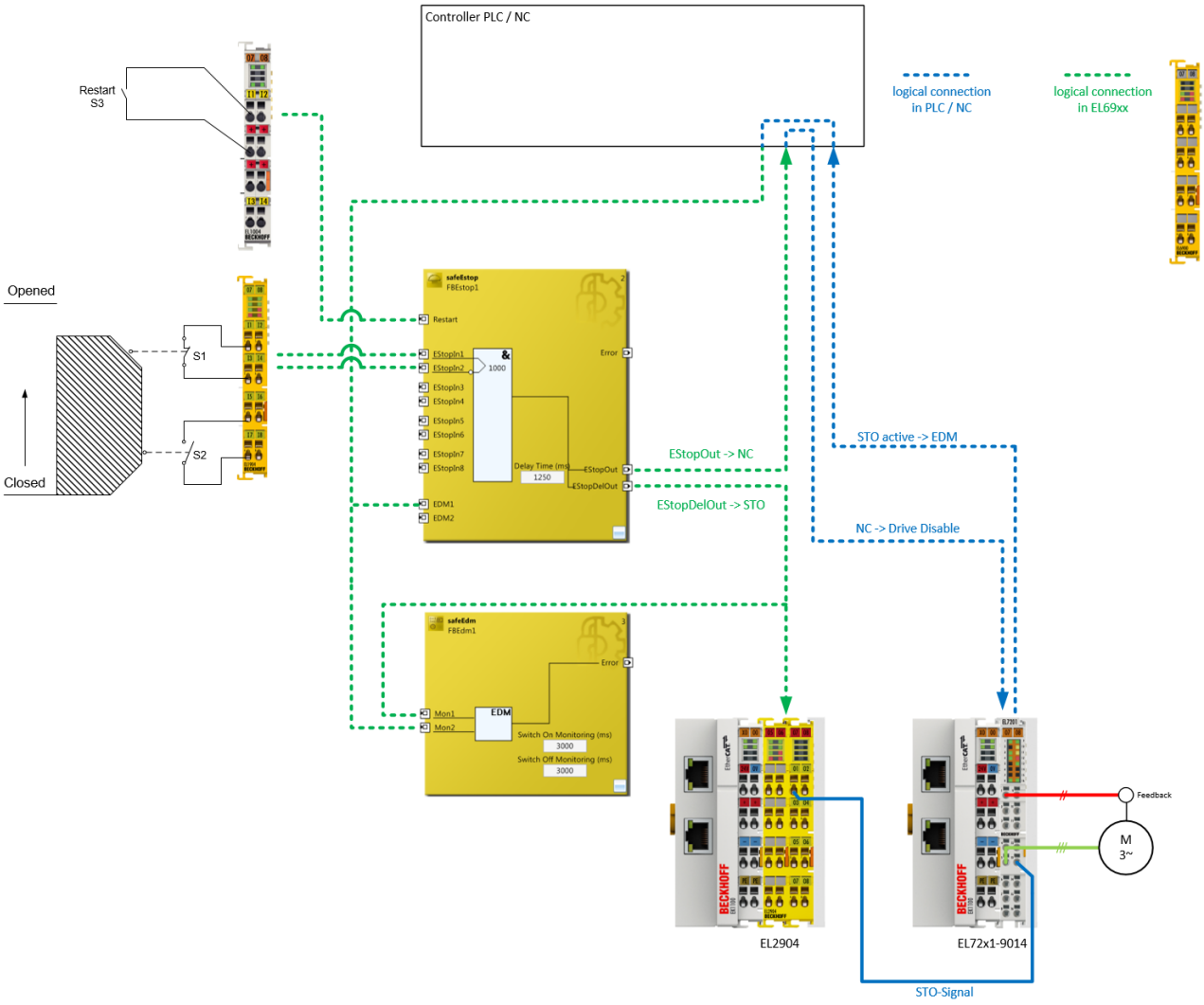
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

6.3 使用 EL72x1-9014 的 STO 功能（类别 3，PL d）

以下应用示例展示了如何将 EL72x1-9014 与 EL2904 配合接线，以实现符合 EN 61800-5-2 标准的 STO 功能。

防护门（S1 和 S2）和重启信号（S3）在 ESTOP 功能块上进行逻辑连接。EStopOut 信号被传输到 NC 控制器，例如，通过它可以切换 EL72x1-9014 的启用信号。EL72x1-9014 的 STO 输入通过延迟输出 EStopDelOut 进行控制。EL72x1-9014 通过标准控制器提供 STO 功能已激活的信息。该信息将被传送到 ESTOP 功能块的 EDM 输入，并被传送至 EDM 功能块，以生成该信号的预期值。



⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

如果风险分析结果表明需在安全控制器中实现重启，则重启也**必须**置于安全输入上。

⚠ 警告

仅在控制柜内部布线

EL2904 和 EL72x1-9014 的 STO 输入之间的布线必须位于同一控制柜中，以便能够承担 EL2904 和 EL72x1-9014 之间布线的交叉短路或外部电源的故障排除。

对该布线的评估以及是否允许故障排除的评估必须由设备制造商或用户完成。

注意

计算 EL72x1-9014

根据 DIN EN ISO 13849-1 标准，在计算性能等级时不考虑 EL72x1-9014，因为它对安全功能无干扰。

根据 EN 62061 标准进行计算时，PFH_D 值以 0 计入。

6.3.1 安全输入和输出端子模块的参数

EL1904

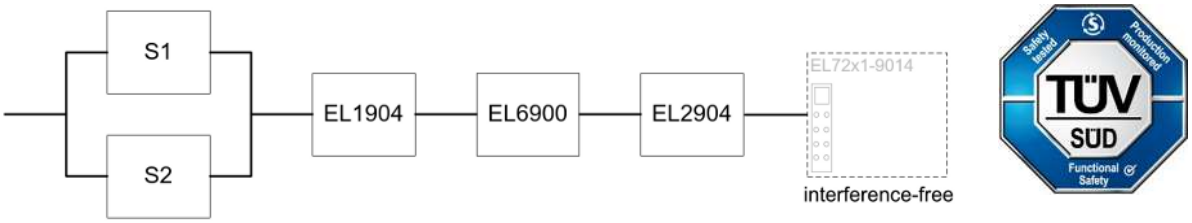
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

6.3.2 功能块结构和安全回路

6.3.2.1 安全功能 1



6.3.3 计算

6.3.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
EL72x1-9014 - PFH_D	0.00
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16

组件	值
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

6.3.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试的 EL2904	DC_{avg}=99%

6.3.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 14720} = 679{,}3y = 5951087h$$

S2：

$$n_{op} = \frac{230 * 16 * 60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 14720} = 1358{,}7y = 11902174h$$

并假设 S1 和 S2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{679{,}3 * 8760} = 1{,}68E - 09$$

S2：

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}4E - 10$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(EL72x1-9014)}$$

由于 $(1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{1,68E-09 + 1,68E-09}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09 + 0,00 = 3,558E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL6900 和 EL2904 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679,3y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 225,2y$$

$$DC_{avg} = \frac{\frac{99\%}{679,3y} + \frac{99\%}{1358,7y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{913,2y}}{\frac{1}{679,3y} + \frac{1}{1358,7y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{913,2y}} = 99,00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

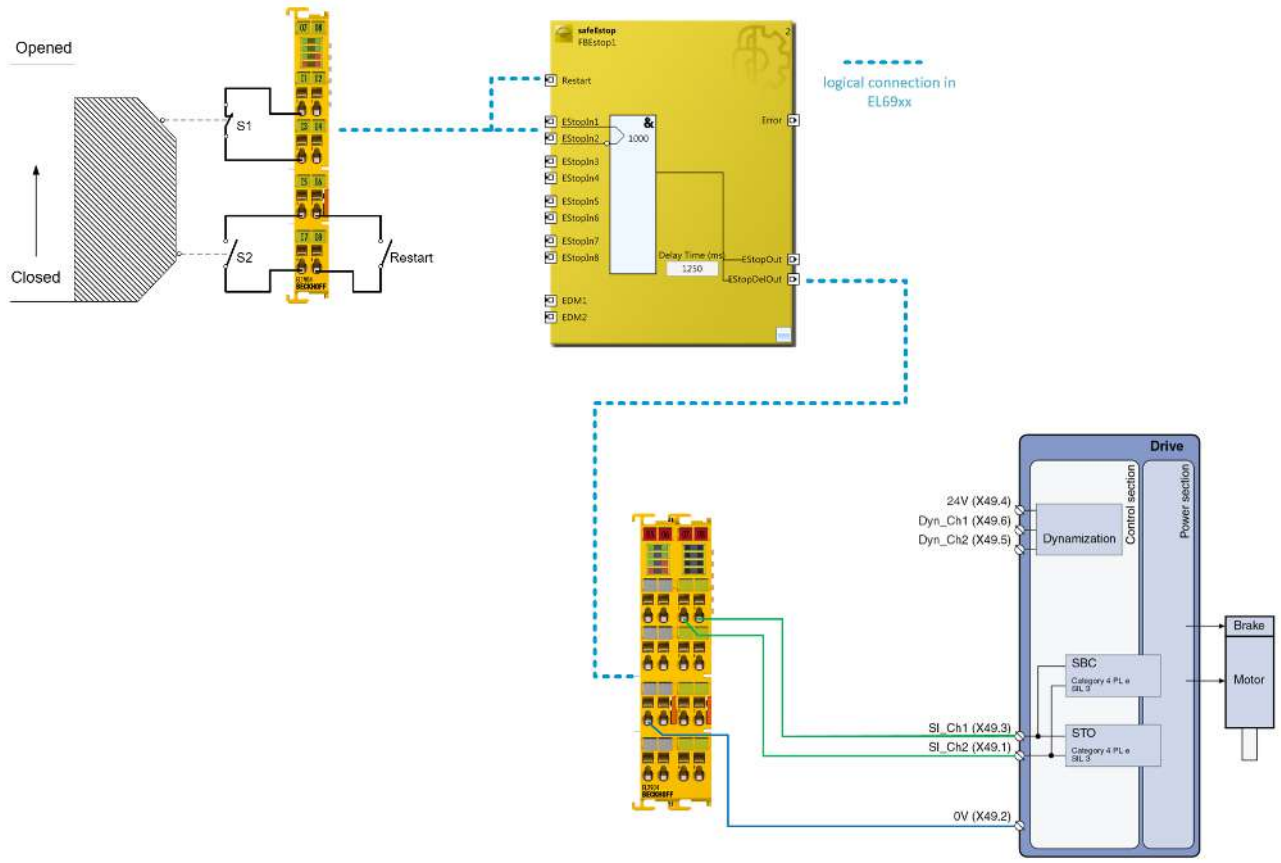
Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

6.4 使用 IndraDrive 的 STO 功能（类别 4，PL e）

以下示例展示了如何将 EL2904 安全输出与 BOSCH Rexroth IndraDrive 配合使用，以在该驱动器上实现 STO 功能。

例如，将防护门与重启信号以双通道模式接入安全输入（在本示例中为 EL1904）。在 TwinSAFE 逻辑中，这些信号可用于 ESTOP 功能块。ESTOP 功能块的切换延迟，可用于两个 EL2904 安全输出。EStopOut 输出可用于通过 NC 控制器对驱动器进行电气停止。

EL2904 的一个输出连接至 Bosch Rexroth IndraDrive 的 STO 输入 X49.1，另一个输出连接至 X49.3。相应的 GND 连接（X49.2）被接回 EL2904，以说明 EL2904 和 IndraDrive 使用相同的 24 V 电源的接地电位。



⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能**不**属于安全链的组成部分，必须在设备中独立实施！

6.4.1 安全输入和输出端子模块的参数

EL1904

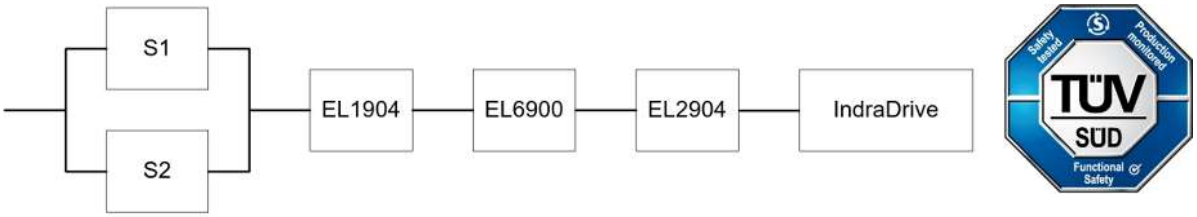
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

6.4.2 功能块结构和安全回路

6.4.2.1 安全功能 1



6.4.3 计算

6.4.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
Bosch Rexroth IndraDrive[1] - PFH_D	0.50E-09
Bosch Rexroth IndraDrive[1] - $MTTF_D$	> 200 年
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

[1] 请注意 Bosch Rexroth 用户文档中提供的信息

6.4.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%
带测试的 EL2904	DC_{avg}=99%
Bosch Rexroth IndraDrive[1]	DC_{avg}=99%

[1] 请注意 Bosch Rexroth 用户文档中提供的信息

6.4.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{1.000.000}{0,1*14720} = 679,3y = 5951087h$$

S2：

$$n_{op} = \frac{230*16*60}{15} = 14720$$

$$MTTF_D = \frac{2.000.000}{0,1*14720} = 1358,7y = 11902174h$$

并假设 S1 和 S2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0,1*n_{op}*(1-DC)}{B10_D} = \frac{1-DC}{MTTF_D}$$

S1：

$$PFH = \frac{1-0,99}{679,3*8760} = 1,68E-09$$

S2：

$$PFH = \frac{1-0,99}{1358,7*8760} = 8,4E-10$$

现在必须做出以下假设：

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合！

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = \beta*\frac{PFH_{(S1)}+PFH_{(S2)}}{2} + (1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(IndraDrive)}$$

由于 $(1-\beta)^2*(PFH_{(S1)}*PFH_{(S2)})*T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\%*\frac{1,68E-09+8,40E-10}{2} + 1,11E-09 + 1,03E-09 + 1,25E-09 + 0,50E-09 = 4,016E-09$$

注意

根据 EN 62061 标准计算

根据 EN 62061 表 3，该值对应于 SIL3。

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(IndraDrive)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(IndraDrive)} = 200y$$

如果仅有 EL1904、EL6900 和 EL2904 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}99)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}72E-06\frac{1}{y}} = 1028{,}8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0{,}99)}{1{,}03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{9{,}02E-06\frac{1}{y}} = 1108{,}6y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{679{,}3y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{200y}} = 105{,}9y$$

$$DC_{avg} = \frac{\frac{99\%}{679{,}3y} + \frac{99\%}{1358{,}7y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{1108{,}6y} + \frac{99\%}{913{,}2y} + \frac{99\%}{200y}}{\frac{1}{679{,}3y} + \frac{1}{1358{,}7y} + \frac{1}{1028{,}8y} + \frac{1}{1108{,}6y} + \frac{1}{913{,}2y} + \frac{1}{200y}} = 99{,}00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**

DC	
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	**⩾ 10^{-8} 至 < 10^{-7}**
2	⩾ 10^{-7} 至 < 10^{-6}
1	⩾ 10^{-6} 至 < 10^{-5}

6.4.4 Bosch Rexroth AG 的技术说明

Rexroth
Bosch Group

Technical Note

Bosch Rexroth AG
Postfach 1357
97803 Lohr am Main
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr am Main
Tel. +49 9352 18-0
Fax +49 9352 18-8400
www.boschrexroth.com

09. März 2017

Sehr geehrte Damen und Herren,

Folgend bestätigen wir Ihnen die Anwendungsbedingungen für die sichere Anwahl von Sicherheitsfunktionen unseres IndraDrive.
Die Anwendungsbedingungen gelten für die IndraDrive Antriebsfamilien Cs, C/M, Mi, ML mit folgenden Sicherheitsoptionen

- L3, L4: Anwahl über Klemme X49 des Steuerteils
- S4, S5: Anwahl über Klemme X41 des Sicherheitszonenmoduls HSZ01

Die Installations- und Projektierungshinweise in der Kundendokumentation sind zu beachten.

Rexroth
Bosch Group

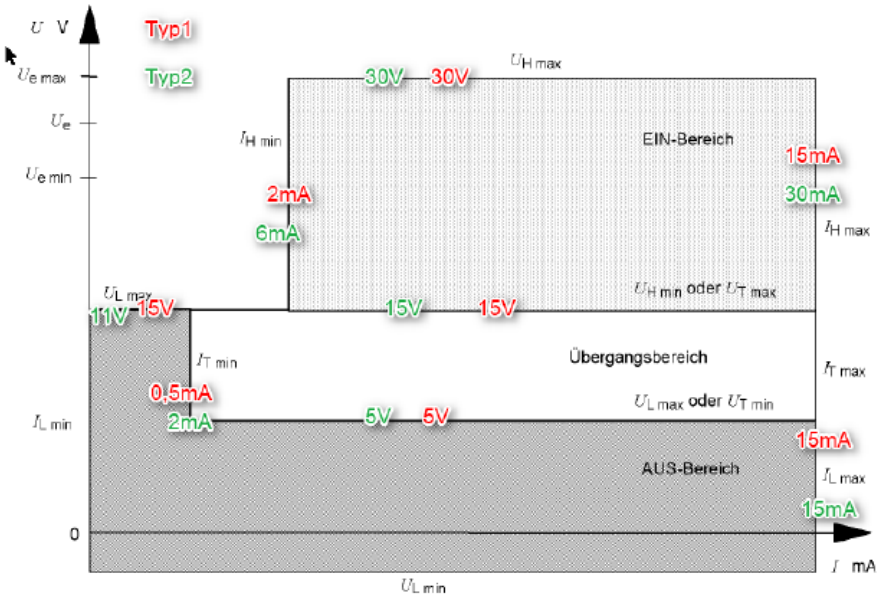
09. März 2017
Seite 2 von 4

1 Safety Anforderungen

Die Anforderungen von Kat.4 Ple nach EN 13849 bzw. SIL 3 gemäß EN 61062 sind für die sichere Anwahl der Sicherheitsfunktionen des Antriebssystems IndraDrive gegeben, wenn die Ansteuereinheit (z.B EL2904 Fa. Beckhoff) folgende Anwendungsbedingungen erfüllt:

1.1 Elektrische Anforderungen

Die sicheren Eingänge verhalten sich konform zur IEC61131-2, Typ 2 (Sicherheitsoption L3, L4) bzw. Typ 1 (Sicherheitsoption S4, S5). Entsprechend muss der Ausgang der aktiven Ansteuereinheit folgende Pegel für das Low-Signal einhalten. Im einfachen Fall liegt das Low-Signal vor, wenn die Ausgangspannung <5V und der Leckstrom Ausgangstufe <0,5mA ist.



1.2 Durch Testungen des Ausgangs der Ansteuereinheit werden folgende Fehler aufgedeckt.

- Kurzschluss der Anwahlsignale mit 24 V
- Kurzschluss zwischen den beiden Anwahlsignalen

Dies entspricht dem Verhalten von OSSD-Ausgängen

Rexroth
Bosch Group

09. März 2017
Seite 3 von 4

2 Funktionale Anforderungen an die Anwahl (für Verfügbarkeit)

Folgende funktionale Anforderungen an die Testimpulse der aktiven Ansteuereinheit müssen erfüllt sein.

2.1 Anforderung IndraDrive mit Sicherheitsoption L3/L4

Zweikanalige Anwahl über Klemme X49 (Eingang nach IEC 61131-2, Typ 2)

Dynamisierungspulse der OSSD-Ausgänge folgende Grenzwerte einhalten:

	Wert	Erklärung
t_{PLmax}	1 ms	maximale Low-Zeit des Testpulses
t_{PLmin}	20 µs	minimale Low-Zeit des Testpulses
t_{Pmax}	1 h	maximale Periodendauer der Testpulse
t_{Pmin}	500 µs	minimale Periodendauer der Testpulse
t_{Vmax}	1 s	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{Dmin} = t_{PH} / t_P$	90 %	minimales Tastverhältnis der Anwahlsignale
t_{Prell}	400 ms	maximale Prelldauer bei einer An- oder Abwahl
φ	-	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

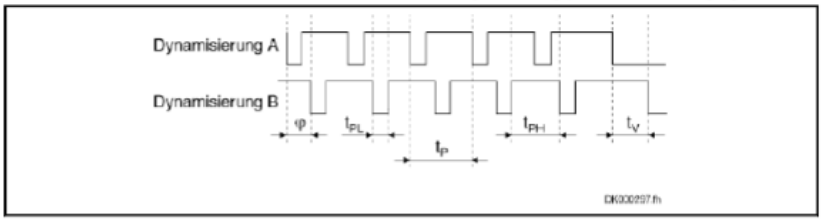
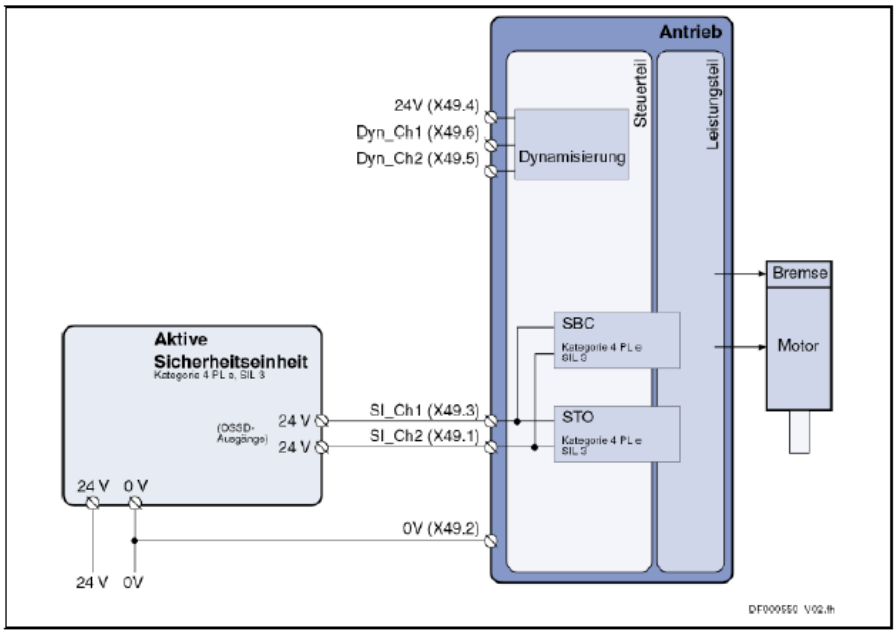


Abb. 5-2: Beispiel für dynamisierte Anwahlsignale



Rexroth
Bosch Group

2.2 Anforderung IndraDrive mit Sicherheitsoption S4, S5

Zweikanalige Anwahl über Klemme X41 des Sicherheitszonenmoduls HSZ01 (Eingang nach IEC 61131-2, Typ 1)

Grenzwert	Erklärung
t_{PLmax} = 1 ms	maximale Low-Zeit des Testpulses
t_{PLmin} = 0 ms	minimale Low-Zeit des Testpulses
t_{Vmax} [1)] = 1 s	maximale Verzugszeit der Anwahlsignale bei Anwahl oder Abwahl
$t_{Dmin} = t_{PH} / t_P$ = 90 %	minimales Tastverhältnis der Anwahlsignale
$t_{Dmax} = t_{PH} / t_P$ = 100 %	maximales Tastverhältnis der Anwahlsignale
t_{Prell} = 400 ms	maximale Prelldauer bei einer An- oder Abwahl
φ [1)] = -	Phasenverschiebung der Testpulse auf beiden Kanälen: keine Anforderung

1) gilt nur bei zweikanaliger Anwahl

Tab. 5-1: Grenzwerte der Dynamisierungspulse der OSSD-Ausgänge

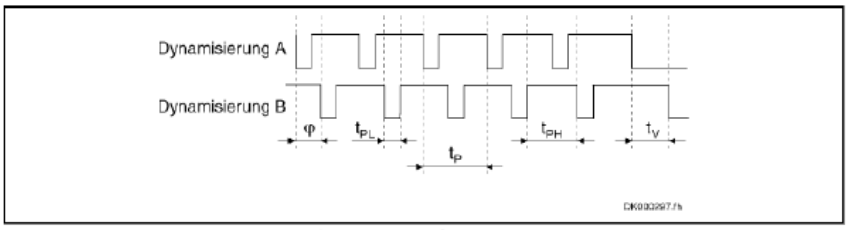


Abb. 5-1: Beispiel für dynamisierte Anwahlsignale

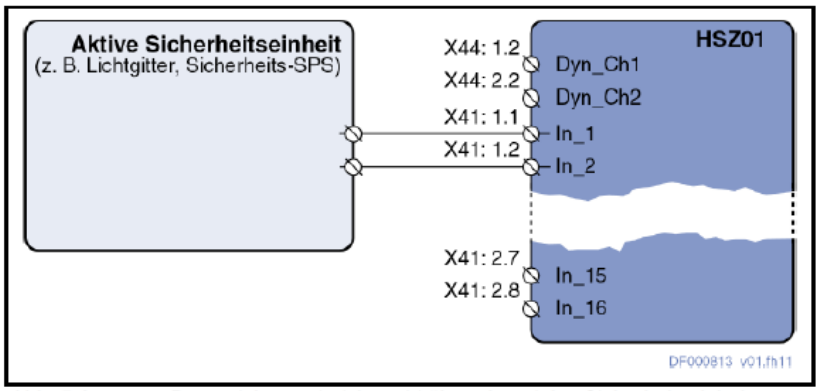


Abb. 5-2: Dynamisierung bei Anwahl über eine aktive Sicherheitseinheit

Diese Bestätigung gilt bis auf Widerruf.

Mit freundlichen Grüßen

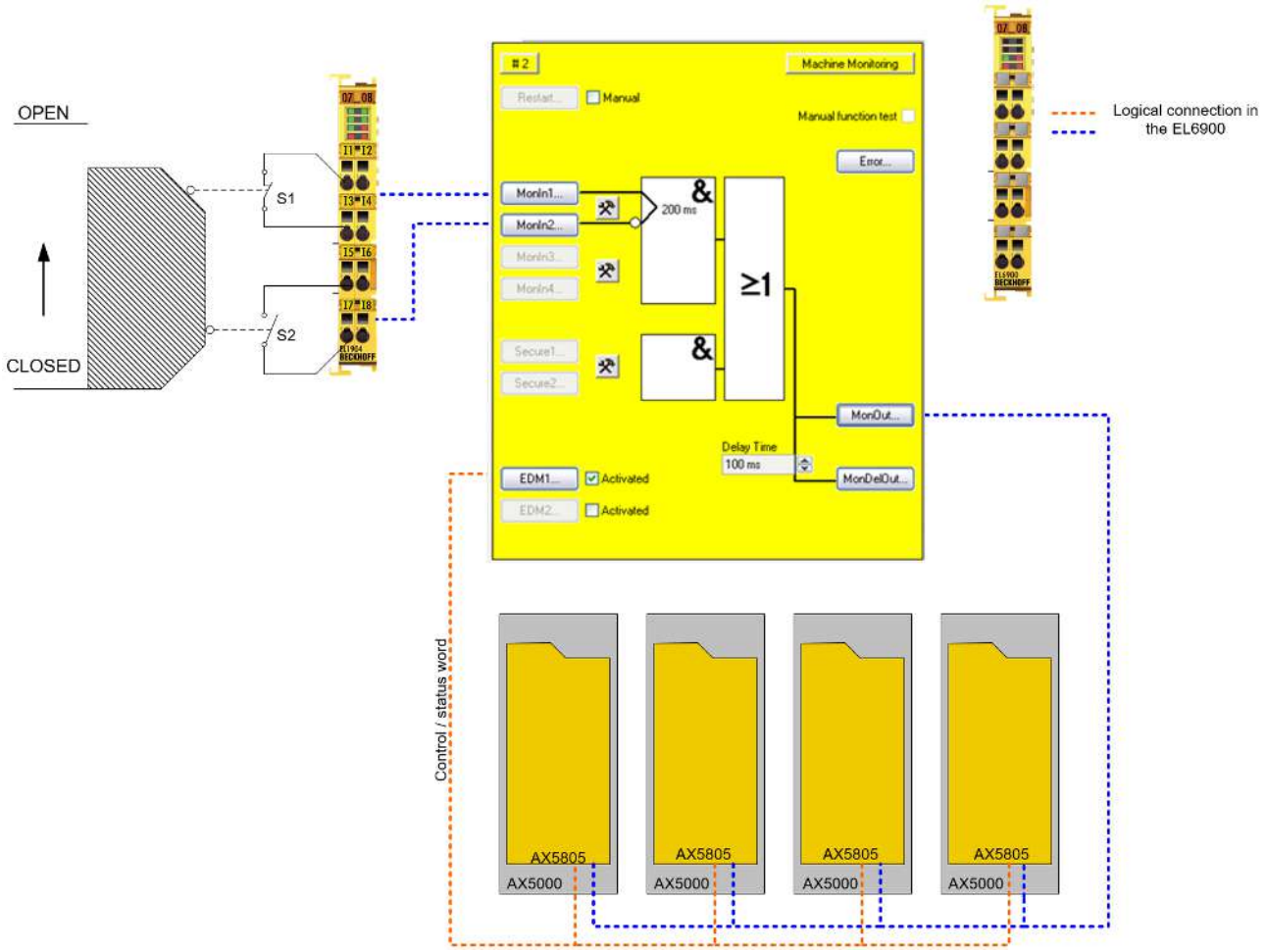
Bosch Rexroth AG (DC-IA/EDY)

7 安全运动功能

7.1 带 SS2 停止功能的 AX5805 驱动器选件（类别 4，PL e）

防护门通过常闭和常开触点组合连接至 EL1904 安全输入端子模块。启动了对输入信号的测试和差异检查。输出端在 AX5805 上连接。

反馈信号通过驱动器选件返回的控制字和状态字进行检查。



7.1.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

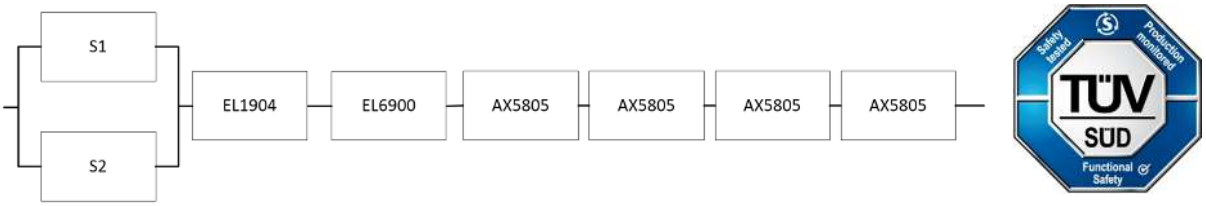
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

AX5805

参数	值
-	

7.1.2 功能块结构和安全回路

7.1.2.1 安全功能 1



7.1.3 计算

7.1.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL6900 – PFH_D	1.03E-09
AX5805 – PFH_D	5.15E-09（请参见经批准的电机列表）
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	60（每小时 1 次）
使用寿命（T1）	20 年 = 175200 小时

7.1.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1/S2	DC_{avg}=99%

7.1.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 1840} = 5434{,}8y = 47608848h$$

S2:

$$n_{op} = \frac{230 * 8 * 60}{60} = 1840$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 1840} = 10869{,}6y = 95217696h$$

并假设 S1 和 S2 均为单通道:

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1:

$$PFH = \frac{1 - 0{,}99}{5434{,}8 * 8760} = 2{,}10E - 10$$

S2:

$$PFH = \frac{1 - 0{,}99}{10869{,}6 * 8760} = 1{,}05E - 10$$

现在必须做出以下假设:

门开关 S1/S2 始终保持反向触发动作。由于两个开关具有不同的值，但完整的防护门开关由常闭和常开触点组合构成，且两个开关均须正常工作，因此可选取两个值中较差的值（S1）代表该组合!

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下:

$$PFH_{ges} = \beta * \frac{PFH_{(S1)} + PFH_{(S2)}}{2} + (1-\beta)^2 * (PFH_{(S1)} * PFH_{(S2)}) * T1 + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(AX5805)} + PFH_{(AX5805)} + PFH_{(AX5805)} + PFH_{(AX5805)}$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至:

$$PFH_{ges} = 10\% * \frac{2{,}10E-10 + 1{,}05E-10}{2} + 1{,}11E-09 + 1{,}03E-09 + 4 * 5{,}15E-09 = 2{,}28E-08$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）:

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为:

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}} + \frac{1}{MTTF_{D(AX5805)}}$$

及:

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0{,}1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

如果仅有 EL1904、AX5805 和 EL6900If 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,99)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1 - DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1 - 0,99)}{1,03E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(AX5805)} = \frac{(1 - DC_{(AX5805)})}{PFH_{(AX5805)}} = \frac{(1 - 0,99)}{5,15E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{4,51E-05\frac{1}{y}} = 221,7y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{5434,8y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y}} = 49,8y$$

$$DC_{avg} = \frac{\frac{99\%}{5434,8y} + \frac{99\%}{10869,6y} + \frac{99\%}{1028,8y} + \frac{99\%}{1108,6y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y} + \frac{99\%}{221,7y}}{\frac{1}{5434,8y} + \frac{1}{10869,6y} + \frac{1}{1028,8y} + \frac{1}{1108,6y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y} + \frac{1}{221,7y}} = 99,00\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年
中等	10 年 ≤ $MTTF_D$ < 30 年
高	**30 年 ≤ $MTTF_D$ ≤ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ≤ DC < 90%
中等	90% ≤ DC < 99%
高	**99% ≤ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

7.2 带集成 EnDat 3 编码器的 AdvPosMon

特定电机的限制条件

本章所述应用示例仅适用于最大速度为 0.44 转/毫秒的电机。

AX8000 的 AX8911 TwinSAFE 驱动器选件卡可通过集成编码器实现安全运动功能的安全参数 SIL 2 / PL d 类别 3。如果使用集成的 EnDat 3 编码器，还可以通过附加措施达到 SIL 3 / PL e 类别 4。为此，必须使用功能块“AdvPosMon”对位置和速度进行额外监控。

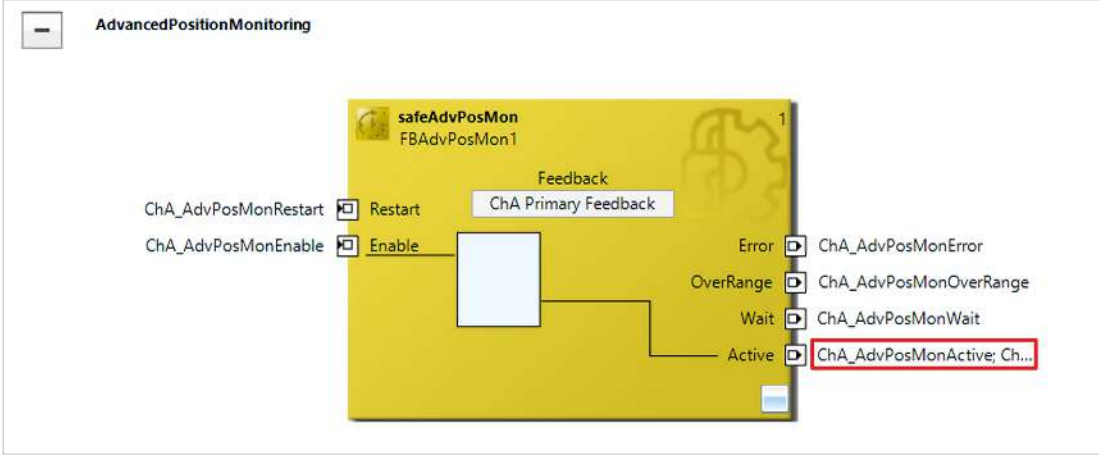
注意

集成到安全运动功能中

您必须将附加措施集成到每个要加载 SIL 3 / PL e 类别 4 的安全运动功能中。

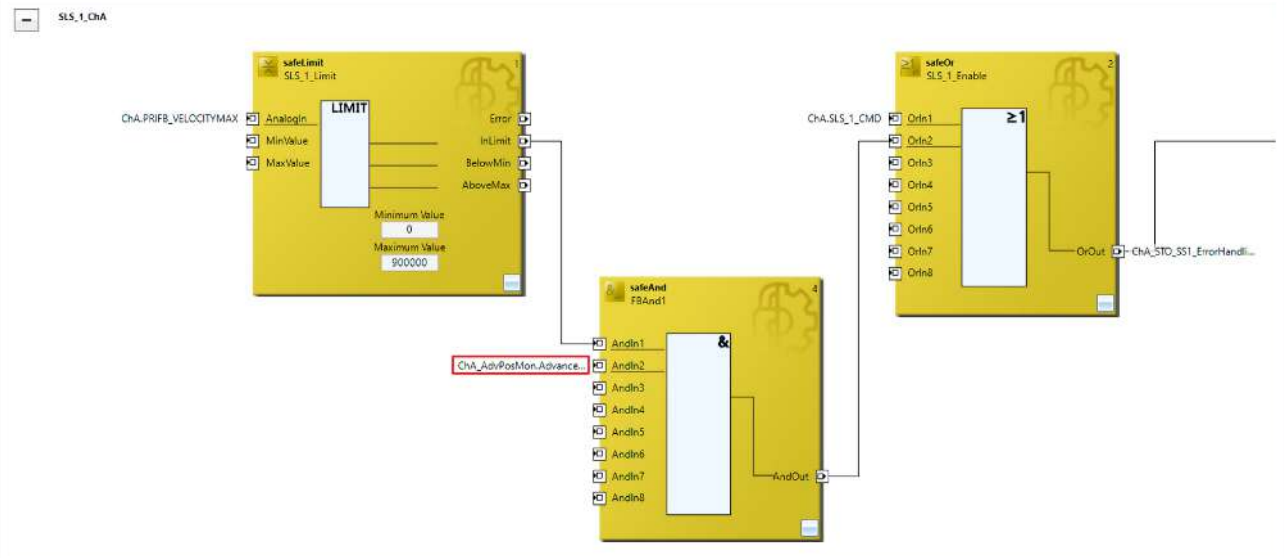
7.2.1 程序

本章介绍了如何在带有所需安全运动功能（例如 SLS1）的安全项目中使用功能块 AdvPosMon。

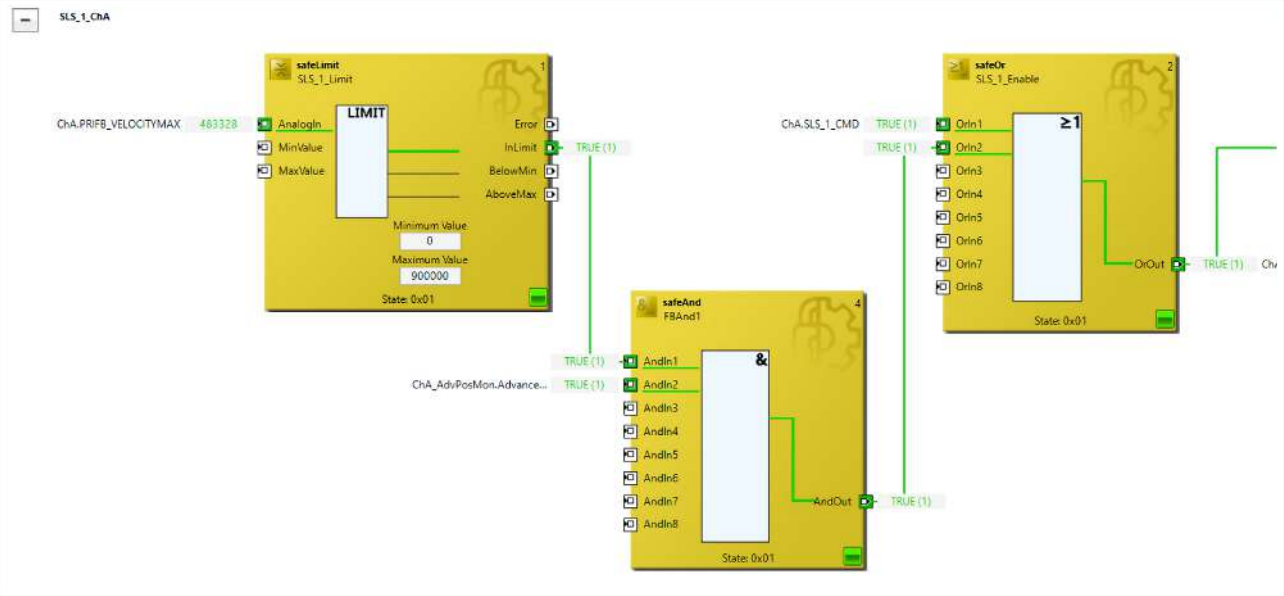


功能块 AdvPosMon 的有效输出信号（红色标记）指示了 EnDat 3 SIL 3 附加措施的活动。如果该信号用于启用诸如 SLS 或 SLP 等下游监控功能（如本应用示例中所述），那么考虑到上述功能限制，这些功能可达到 SIL 3/PL e 类别 4。

要使用功能块 AdvPosMon，必须将有效输出信号集成到所需的应用中。通过启用输入可以启用或禁用扩展监控。如果发生超量程错误，只要在应用中使用重启信号，即可通过重新启动来重置该错误。



上图显示了如何将有效输出信号（红色标记）集成到所需的应用中。有效输出信号连接至 SafeAnd 功能块，从而集成到 SLS1 配置中。



功能块 AdvPosMon 的有效信号活动和 SLS1 配置的状态均在安全编辑器的在线视图中显示。

8 使用 TwinSAFE SC 处理模拟量值

8.1 速度监测（类别 3，PL d）

要监控驱动器的速度。该驱动器具有安全功能（在本示例中以 STO 为例），可通过相应的输入激活。该输入通过两个接触器中各一个常开触点进行路由。位置和速度信号通过两条不同的通信路径传输到 EL6910 TwinSAFE 逻辑，并在那里按照图示逻辑进行处理。sin/cos编码器连接至 EL5021-0090，位置信息通过 TwinSAFE SC 通信和 EtherCAT 进行传输。通过标准 PROFINET 通信（也可使用任何其他现场总线）和标准 PLC，还可以将驱动器速度传输到 EL6910 TwinSAFE 逻辑。

通过安全相关的 EL6910 逻辑模块，基于位置值计算出速度（FB Speed）。驱动器的速度通过 FB 进行缩放，使其值与计算出的速度相匹配。这两个速度值通过 FB Compare 进行等值校验，并通过 FB Limit 监控其最大值。由于两个速度值（一个直接计算得出的，另一个在安全相关 EL6910 逻辑中计算得出）在任何时候都绝不会 100% 相等，因此两个速度值之间的差值必须在 10% 的容差范围内，这样才能满足等值条件。如果当前速度值低于 FB Limit 中指定的阈值，则 STO 输出将被设置为逻辑 1，驱动器可以转动。如果超过限值或比较无效，则输出将被设置为逻辑 0，驱动器将切换为无转矩状态，或集成在驱动器中的安全功能将被激活。整个计算和调整均在安全相关 EL6910 逻辑中的 SIL 3/PL e 安全水平上进行。使用这种方法，可以从两个非安全相关的信号中生成一个安全相关的结果。

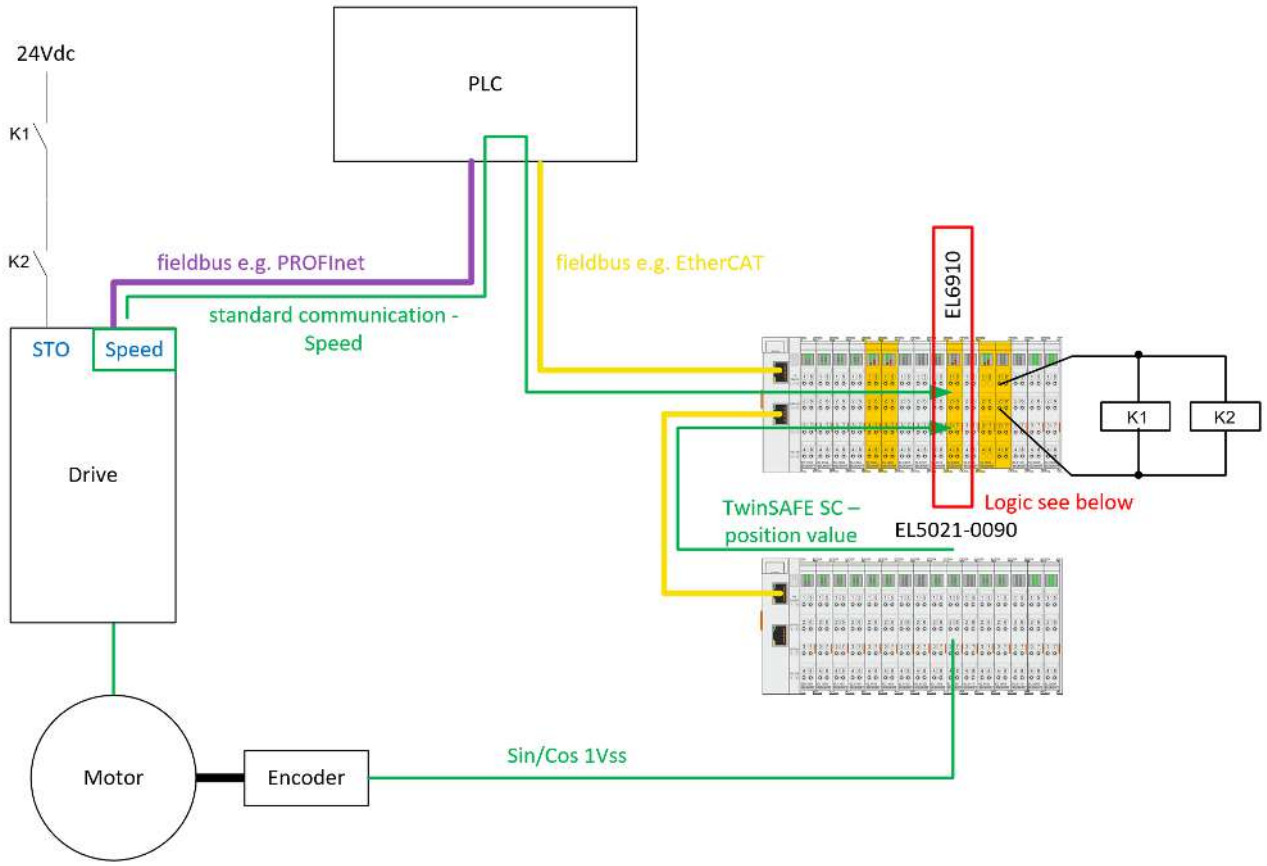
此外，还通过 ESTOP 功能块（为了清晰起见，未在图中显示）实现了急停功能，该功能块既能阻止重启，也能接管接触器 K1 和 K2 的控制。

在发生故障时，必须使用比较功能块的 IsValid 信号执行关断操作。

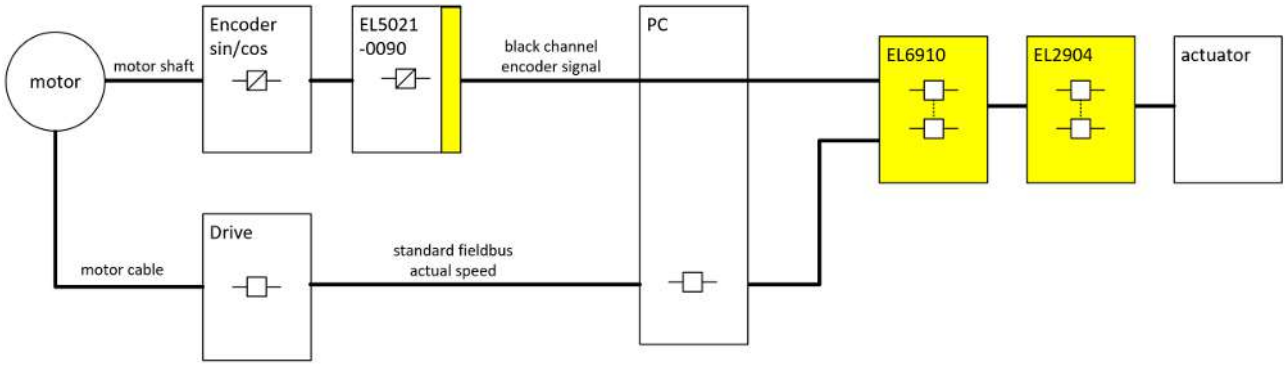
下表列出了可用于此应用示例的替代型 TwinSAFE SC 产品。在本例中描述的假设和论证仍需纳入考量。

速度监测示例：安全功能（如 STO）可用于驱动器，EL5021-0090 可用于连接sin/cos编码器		
用于位置、速度或频率传输的替代型 TwinSAFE SC 编码器端子模块	EL5001-0090	EtherCAT 端子模块，单通道编码器接口，SSI，TwinSAFE SC
	EL5101-0090	EtherCAT 端子模块，单通道编码器接口，增量式，5 V DC（DIFF RS422，TTL），1 MHz，TwinSAFE SC
	EL5151-0090	EtherCAT 端子模块，单通道编码器接口，增量式，24 V DC HTL，100 kHz，TwinSAFE SC
	EL5021-0090	EtherCAT 端子模块，单通道编码器接口，SinCos，1 Vpp，TwinSAFE SC
	EL5032-0090	EtherCAT 端子模块，双通道编码器接口，EnDat 2.2，TwinSAFE SC

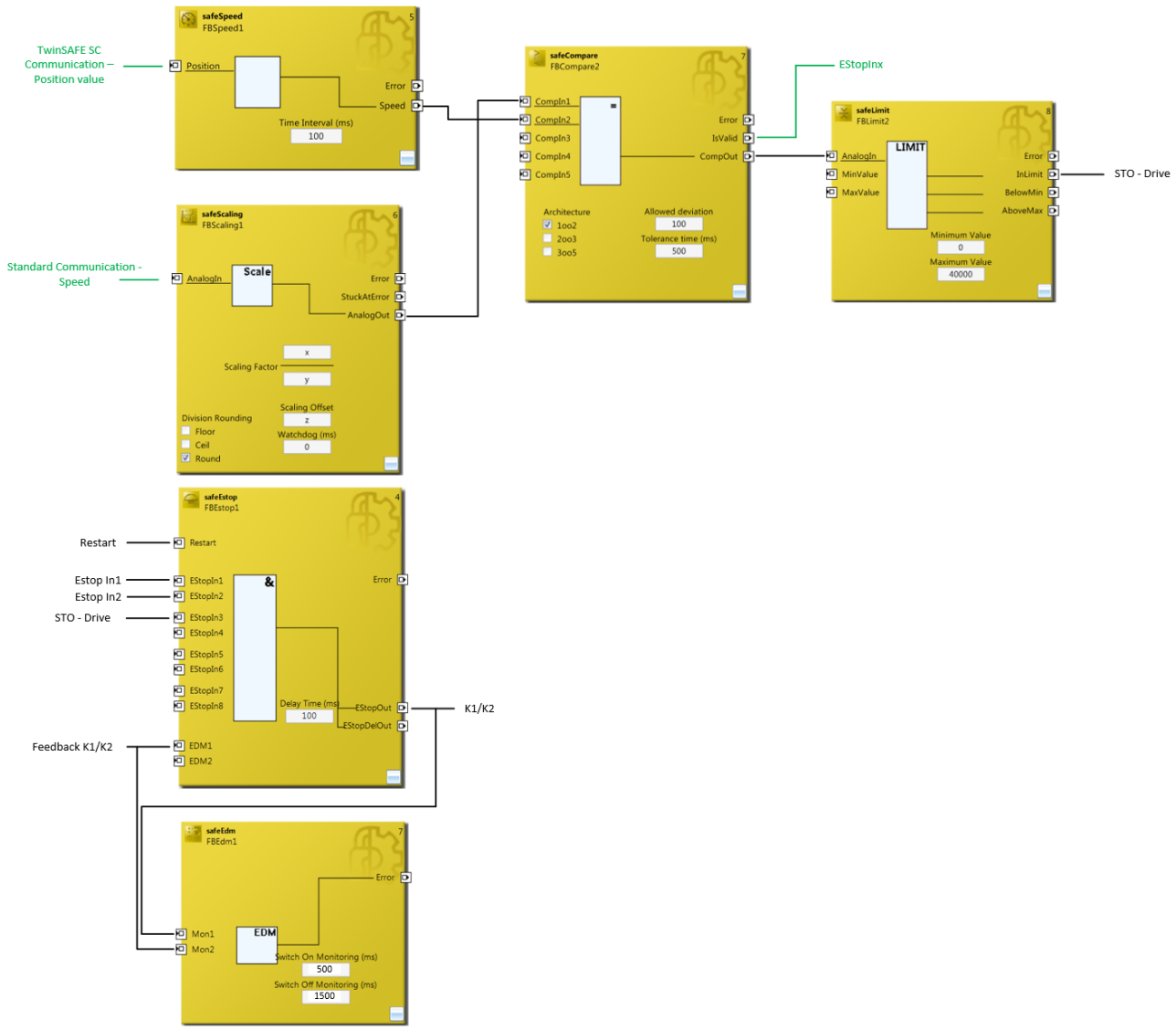
结构


24Vdc
K1
K2
PLC
fieldbus e.g. PROFInet
standard communication - Speed
fieldbus e.g. EtherCAT
EL6910
STO
Speed
Drive
K1
K2
TwinSAFE SC – position value
EL5021-0090
Logic see below
Motor
Encoder
Sin/Cos 1Vss

结构图配置


motor
motor shaft
Encoder sin/cos
EL5021 -0090
black channel encoder signal
PC
EL6910
EL2904
actuator
Drive
motor cable
standard fieldbus actual speed

逻辑



8.1.1 结构和诊断

来自驱动器和编码器的输入信号是动态且互不相同的标准信号。驱动器提供速度值，编码器提供sin/cos信号，该信号由标准端子模块进行评估，并打包成安全报文（带修正多项式的 FSoE - TwinSAFE SC）进行传输。

该端子模块（EL5021-0090）提供位置值，该位置值在安全逻辑中转换为速度值，然后进行缩放并与驱动器的速度值进行比较。在这种情况下，相等意味着差异信号位于 10% 的公差窗口之内。

编码器信号通过标准现场总线遵循黑色通道原理进行传输。该值会与通过标准现场总线传输的驱动器速度进行合理性校验。通过在安全逻辑内比较两个不同的速度和位置信号，可检测任一通道中的错误，并启动驱动器的 STO。

8.1.2 FMEA

错误假设	预期情况	已检查
速度值（例如通过 PROFINET 传输）停滞	通过第二个值以及 EL6910 中的合理性检查（其他现场总线以及 EL5021-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况。 此外，应为速度 0 启用标准通信 Watchdog（看门狗）。	

错误假设	预期情况	已检查
通过 EtherCAT 和 TwinSAFE SC 通信传输的速度值停滞	通过 TwinSAFE SC 通信中的 Watchdog（看门狗）检测到该情况。 合理性检查：当电机启动时，预期也会产生动态速度值。	
速度值在标准 PLC 中被连续复制	TwinSAFE SC 通信中的畸变值会导致报文中出现无效的 CRC，从而立即关闭组和输出。 两个速度值的数据类型长度不同（例如 4 字节和 11 字节）	
速度值发生畸变，例如通过 PROFINET	通过第二个值以及 EL6910 中的合理性检查（其他现场总线以及 EL5021-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况	
电机与编码器之间已完全失去连接	通过 EL6910 内驱动器速度值的合理性检查检测到该情况。 合理性检查：当电机启动时，预期也会产生动态速度值。	
编码器提供错误的位置值	通过 EL6910 内驱动器速度值的合理性检查检测到该情况	
驱动器提供错误的速度值	通过第二个值以及 EL6910 中的合理性检查（其他现场总线以及 EL5021-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误： 损坏	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 非预期重复	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况。此外，应为速度 0 启用标准通信 Watchdog（看门狗）。	
基于 61784-3 标准的通讯错误： 错误顺序	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 丢失	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 不可接受的延迟	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况。此外，应为速度 0 启用标准通信 Watchdog（看门狗）。	
基于 61784-3 标准的通讯错误： 插入	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 伪装	与标准无关，仅适用于安全通信。	
基于 61784-3 标准的通讯错误： 寻址	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
标准通信的通信错误： 交换机中的重复性内存错误	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

8.1.2.1 关于 TwinSAFE SC 通信的说明：

TwinSAFE SC 通信采用与 Saftey over EtherCAT 通信相同的错误检测机制，区别在于其使用不同的多项式计算校验和，且该多项式与之前 Safety over EtherCAT 所用的多项式具有充分的独立性。

这些相同的机制均处于激活状态，例如黑色通道原理（比特错误概率 10^{-2}）。

数据传输的质量并非关键因素，因为所有传输错误最终都会通过安全逻辑中的比较被检测出来，因为这类错误将导致数据不一致。

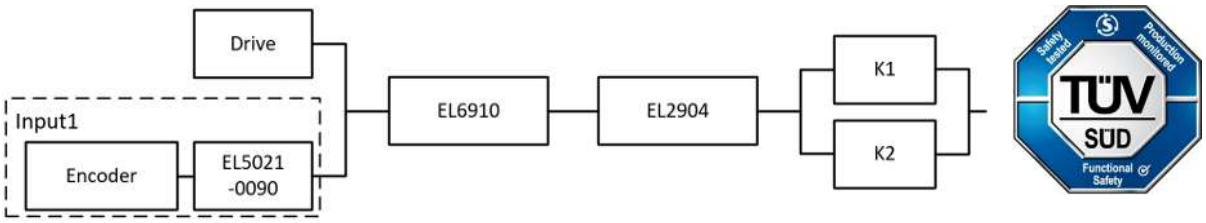
8.1.3 安全输出端子模块的参数

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

8.1.4 功能块结构和安全回路

8.1.4.1 安全功能 1



8.1.5 计算

8.1.5.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
驱动器 – MTBF	516,840（59a）
编码器 – MTTF	549,149
EL5021-0090 - MTBF	1,205,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

8.1.5.2 诊断覆盖率 DC

组件	值
采用 EL5021-0090 的驱动器与编码器及其逻辑内的合理性检查	DC_{avg}=90%（计算中替代值：99%）
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

8.1.5.3 安全功能 1 的计算

为了清晰起见，安全系数同时根据 EN 62061 和 EN 13849 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

根据 MTBF 值计算 PFH_D 和 $MTTF_D$ 值：

注：维修时间可以忽略不计，因此以下内容适用：

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

及

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

驱动器

$$MTTF_D = 2 * MTBF = 2 * 59y = 1.033.680h = 118y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.033.680h} = 9{,}67E - 08$$

编码器

$$MTTF_D = 2 * MTTF = 2 * 549149h = 1.098.298h = 125y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.098.298h} = 9{,}10E - 08$$

EL5021-0090

$$MTTF_D = 2 * MTBF = 2 * 1.205.000h = 2.410.000h = 275y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{2.410.000h} = 4{,}15E - 08$$

输入子系统 1

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL5021-0090)} = 9{,}10E - 08 + 4{,}15E - 08 = 13{,}25E - 08$$

K1/K2：

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1*21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接回读

$$PFH = \frac{1-0,99}{593607,3*8760} = 1,92E-12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

来自带 EL5021-0090 的编码器与驱动器的输入信号采用不同的测量程序，输出不同的标度值，且均参与安全功能的实现。通道故障不会导致危险情况，但会通过比较 TwinSAFE 逻辑中的两个值被检测到，并导致关断。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输入子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Drive)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Antrieb)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

$$PFH_{ges} = 10\% * \frac{13,25E-08 + 9,67E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,45E-08$$

注意

EN 62061

根据 EN 62061 标准，输入子系统需以 90% 的 SFF 或 DC 值进行评估。根据 EN 62061 表 5，这将系统可实现的最大 SIL 值限制为 2。

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值的替代计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

较低值取自输入子系统（在本示例中为编码器与 EL5021-0090 的组合）：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL5021-0090)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 69{,}9y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL5021-0090)}} + \frac{DC}{MTTF_{D(Drive)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL5021-0090)}} + \frac{1}{MTTF_{D(Drive)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{90\%}{125y} + \frac{90\%}{275y} + \frac{90\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 90{,}78\%$$

或采用 DC = 99% 进行计算

$$DC_{avg} = \frac{\frac{99\%}{125y} + \frac{99\%}{275y} + \frac{99\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{125y} + \frac{1}{275y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

⚠ 警告

停转

当电机处于停止状态时，仅当请求运动时才会检测到编码器信号停滞等错误。设备制造商或用户必须考虑到这一点。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

或输入子系统采用 DC=99% 进行计算：

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

8.2 速度监测（通过 IO-Link）（类别 3，PL d）

要监控驱动器的速度。该驱动器具有安全功能（在本示例中以 STO 为例），可通过相应的输入激活。该输入通过两个接触器中各一个常开触点进行路由。

速度信号以两种不同的方式传输到 EL6910 TwinSAFE 逻辑，并按照所示逻辑进行处理。IO-Link 编码器连接至 EL6224-0090，速度信息通过 TwinSAFE SC 通信进行传输。通过标准 PROFINET 通信（也可使用任何其他现场总线）和标准 PLC，还可以将驱动器速度传输到 EL6910 TwinSAFE 逻辑。

两个速度值通过安全相关 EL6910 逻辑内的 FB Scale 进行缩放，使值相互匹配。这两个速度值通过 FB Compare 进行等值校验，并通过 FB Limit 监控其最大值。由于两个速度值在任何时候都绝不会 100% 相等，因此两个速度值之间的差值必须在 10% 的容差范围内，这样才能满足等值条件。如果当前速度值低于 FB Limit 中指定的阈值，则 STO 输出将被设置为逻辑 1，驱动器可以转动。如果超过限值或比较无效，则输出将被设置为逻辑 0，驱动器将切换为无转矩状态，或集成在驱动器中的安全功能将被激活。整个计算和调整均在安全相关 EL6910 逻辑中的 SIL 3/PL e 安全水平上进行。使用这种方法，可以从两个非安全相关的信号中生成一个安全相关的结果。

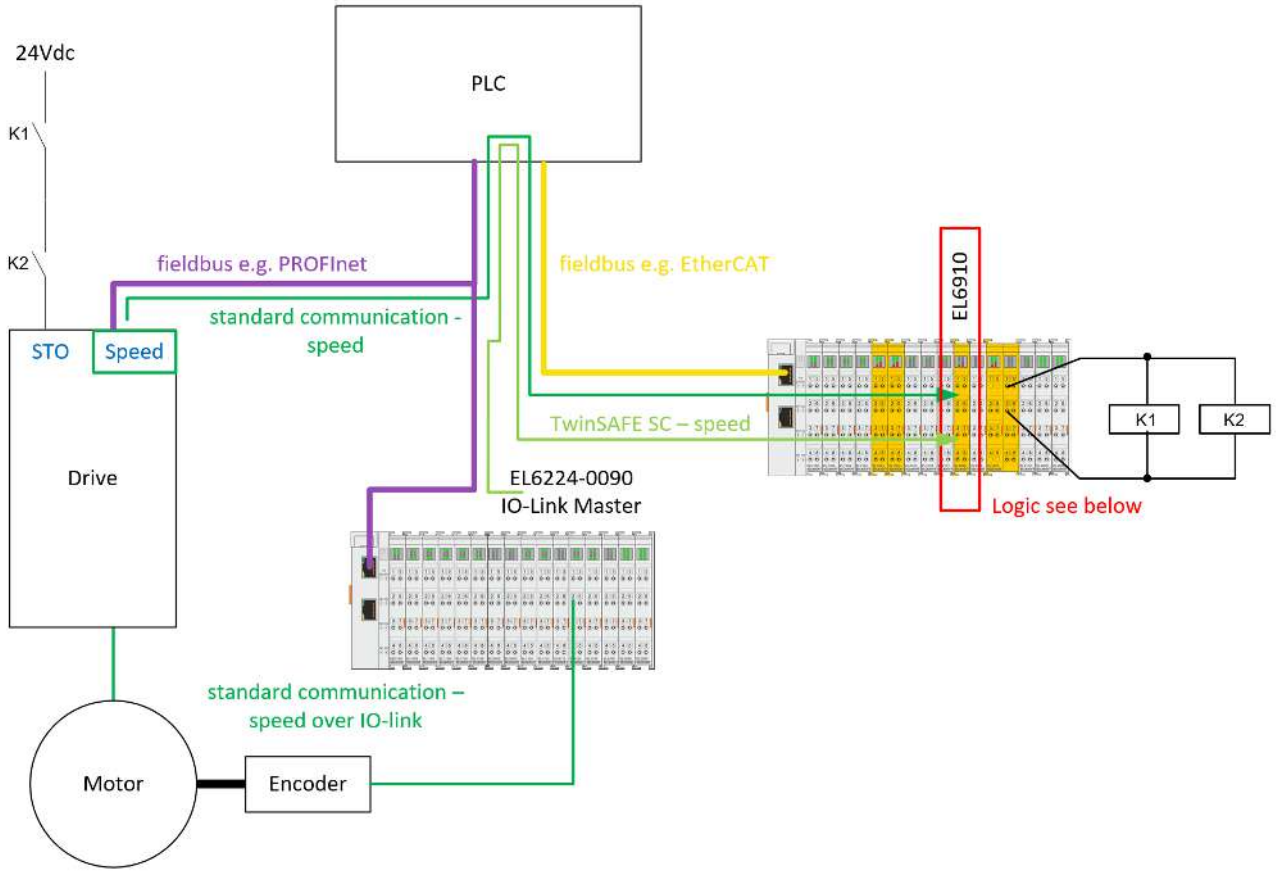
此外，还通过 ESTOP 功能块（为了清晰起见，未在图中显示）实现了急停功能，该功能块既能阻止重启，也能接管接触器 K1 和 K2 的控制。

在发生故障时，必须使用比较功能块的 IsValid 信号执行关断操作。

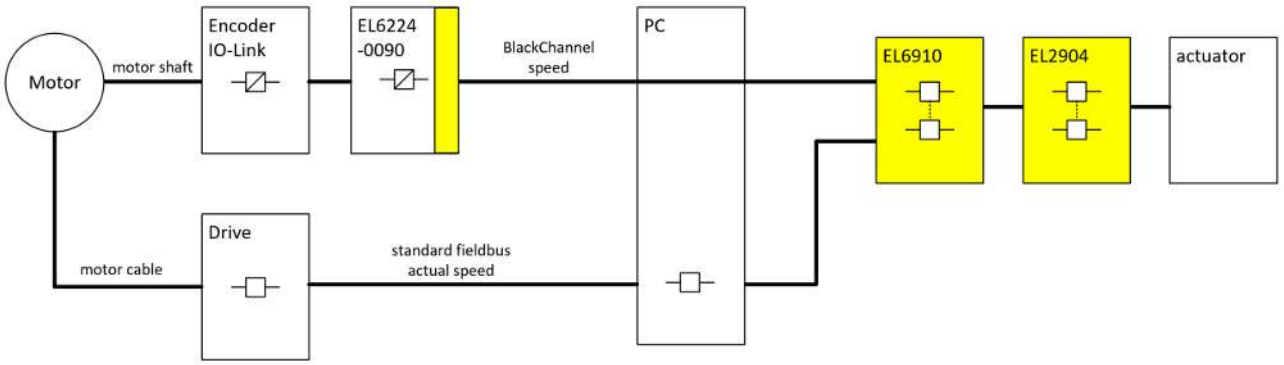
下表列出了可用于此应用示例的替代型 TwinSAFE SC 产品。在本例中描述的假设和论证仍需纳入考量。

速度监测示例：安全功能（如 STO）可用于驱动器，EL6224-0090 可用于连接 IO-Link 编码器		
用于位置、速度或频率传输的替代型 TwinSAFE SC 编码器端子模块	EL5001-0090	EtherCAT 端子模块，单通道编码器接口，SSI，TwinSAFE SC
	EL5101-0090	EtherCAT 端子模块，单通道编码器接口，增量式，5 V DC（DIFF RS422，TTL），1 MHz，TwinSAFE SC
	EL5151-0090	EtherCAT 端子模块，单通道编码器接口，增量式，24 V DC HTL，100 kHz，TwinSAFE SC
	EL5021-0090	EtherCAT 端子模块，单通道编码器接口，SinCos，1 Vpp，TwinSAFE SC
	EL5032-0090	EtherCAT 端子模块，双通道编码器接口，EnDat 2.2，TwinSAFE SC

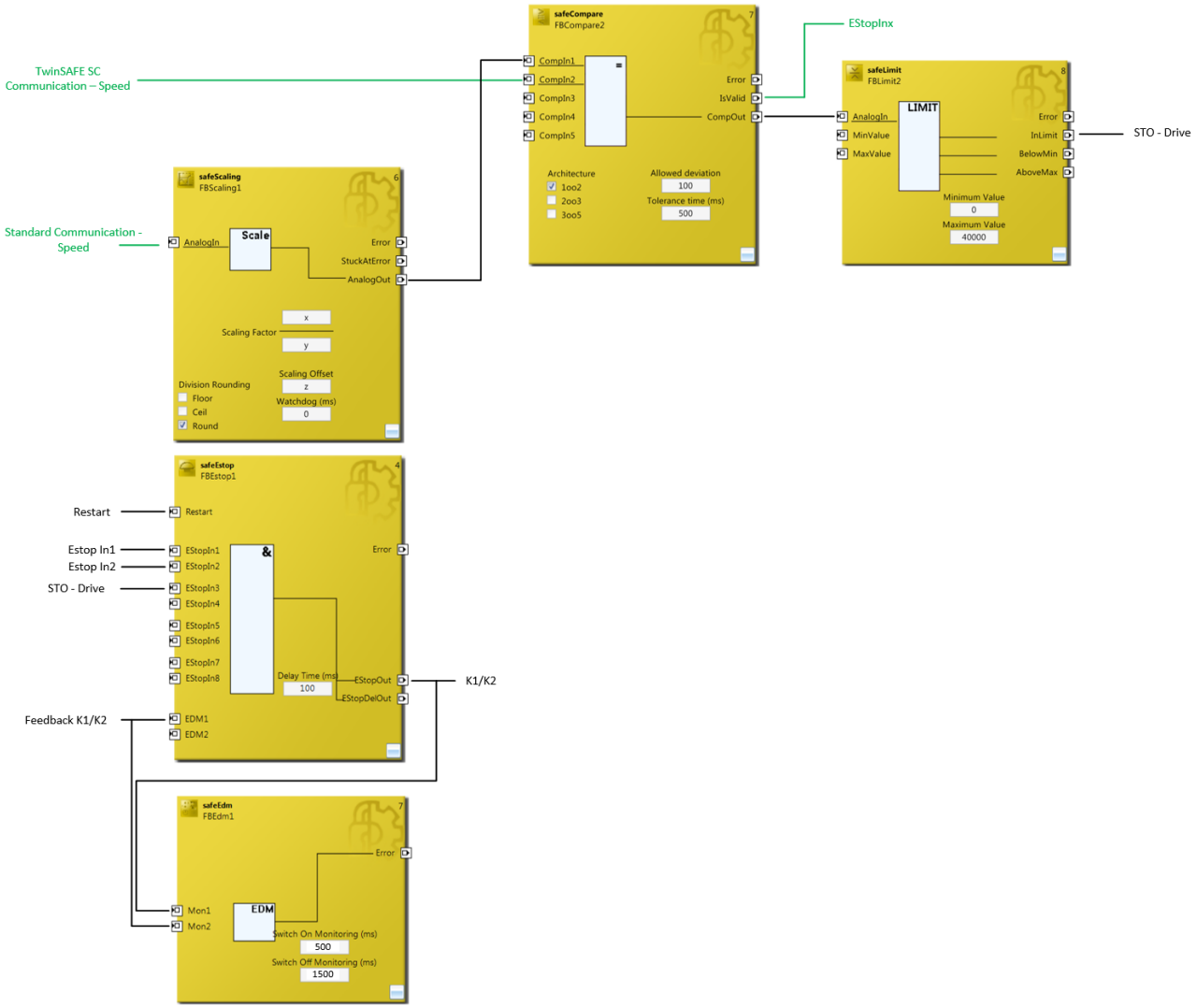
IO-Link 结构



结构图配置



逻辑



8.2.1 结构和诊断

从驱动器和编码器读取的输入信号是互不相同的标准信号。驱动器提供速度值，编码器提供 IO-Link 信号，该信号由标准端子模块进行评估，并打包成安全报文（带修正多项式的 FSoE - TwinSAFE SC）进行传输。该端子模块（EL6224-0090）提供速度值，该速度值在安全逻辑中进行缩放，并与驱动器的速度值进行比较。在这种情况下，相等意味着差异信号位于 10% 的公差窗口之内。

IO-link 编码器信号通过标准现场总线遵循黑色通道原理进行传输。该值会与通过标准现场总线传输的驱动器速度进行合理性校验。通过在安全逻辑内比较两个不同的速度信号，可检测任一通道中的错误，并启动驱动器的 STO。

8.2.2 FMEA

错误假设	预期情况	已检查
速度值（例如通过 PROFINET 传输）停滞	通过第二个值以及 EL6910 中的合理性检查（EL6224-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况。 此外，应为速度 0 启用标准通信 Watchdog（看门狗）。	
通过 EtherCAT 和 TwinSAFE SC 通信传输的速度值停滞	通过 TwinSAFE SC 通信中的 Watchdog（看门狗）检测到该情况。 合理性检查：当电机启动时，预期也会产生动态速度值。	

错误假设	预期情况	已检查
速度值在标准 PLC 中被连续复制	TwinSAFE SC 通信中的畸变值会导致报文中出现无效的 CRC，从而立即关闭组和输出 两个速度值的数据类型长度不同（例如 4 字节和 11 字节）	
速度值发生畸变，例如通过 PROFINET	通过第二个值以及 EL6910 中的合理性检查（EL6224-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况	
电机与编码器之间已完全失去连接	通过 EL6910 内驱动器速度值的合理性检查检测到该情况 合理性检查：当电机启动时，预期也会产生动态速度值。	
编码器提供错误的位置值	通过 EL6910 内驱动器速度值的合理性检查检测到该情况	
驱动器提供错误的速度值	通过第二个值以及 EL6910 中的合理性检查（EL6224-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误： 损坏	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 非预期重复	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况。此外，应为速度 0 启用标准通信 Watchdog（看门狗）。	
基于 61784-3 标准的通讯错误： 错误顺序	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 丢失	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 不可接受的延迟	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况。此外，应为速度 0 启用标准通信 Watchdog（看门狗）。	
基于 61784-3 标准的通讯错误： 插入	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 伪装	与标准无关，仅适用于安全通信。	
基于 61784-3 标准的通讯错误： 寻址	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
标准通信的通信错误： 交换机中的重复性内存错误	通过速度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

8.2.2.1 关于 TwinSAFE SC 通信的说明：

TwinSAFE SC 通信采用与 Saftey over EtherCAT 通信相同的错误检测机制，区别在于其使用不同的多项式计算校验和，且该多项式与之前 Safety over EtherCAT 所用的多项式具有充分的独立性。

这些相同的机制均处于激活状态，例如黑色通道原理（比特错误概率 10^{-2}）。

数据传输的质量并非关键因素，因为所有传输错误最终都会通过安全逻辑中的比较被检测出来，因为这类错误将导致数据不一致。

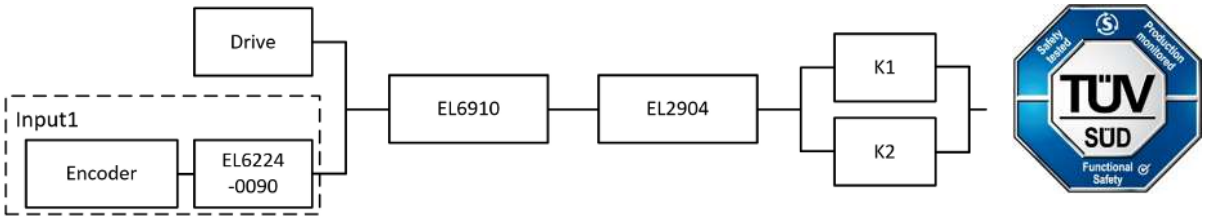
8.2.3 安全输出端子模块的参数

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

8.2.4 功能块结构和安全回路

8.2.4.1 安全功能 1



8.2.5 计算

8.2.5.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
驱动器 – MTBF	516,840（59y）
编码器 – MTTF	1,208,880（138y）
EL6224-0090 - MTBF	1,200,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

8.2.5.2 诊断覆盖率 DC

组件	值
采用 EL6224-0090 的驱动器与编码器及其逻辑内的合理性检查	DC_{avg}=90%（计算中替代值：99%）
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

8.2.5.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN 13849 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

根据 MTBF 值计算 PFH_D 和 $MTTF_D$ 值：

注：维修时间可以忽略不计，因此以下内容适用：

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

及

$$\lambda_D \approx \frac{0,1}{T_{10D}} = \frac{0,1 * n_{op}}{B10_D}$$

得出

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

驱动器

$$MTTF_D = 2 * MTBF = 2 * 59y = 1.033.680h = 118y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{1.033.680h} = 9,67E - 08$$

编码器

$$MTTF_D = 2 * MTTF = 2 * 1.208.880h = 2.417.760h = 276y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.417.760h} = 4,13E - 08$$

EL6224-0090

$$MTTF_D = 2 * MTBF = 2 * 1.200.000h = 2.400.000h = 273y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0,9}{2.400.000h} = 4,17E - 08$$

输入系统 1

$$PFH_{(Input1)} = PFH_{(Encoder)} + PFH_{(EL6224-0090)} = 4,13E - 08 + 4,17E - 08 = 8,30E - 08$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接反馈

$$PFH = \frac{1 - 0,99}{593607,3 * 8760} = 1,92E - 12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

来自带 EL6224-0090 的编码器与驱动器的输入信号采用不同的测量程序，输出不同的标度值，且均参与安全功能的实现。通道故障不会导致危险情况，但会通过比较 TwinSAFE 逻辑中的两个值被检测到，并导致关断。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输入子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。
此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Drive)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Drive)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Antrieb)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

$$PFH_{ges} = 10\% * \frac{8,30E-08 + 9,67E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,2E-08$$

注意

EN 62061

根据 EN 62061 标准，输入子系统需以 90% 的 SFF 或 DC 值进行评估。根据 EN 62061 表 5，这将系统可实现的最大 SIL 值限制为 2。

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值的替代计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

较低值取自输入子系统（在本示例中为驱动器）：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Antrieb)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 89,7y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6244-0090)}} + \frac{DC}{MTTF_{D(Antrieb)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6224-0090)}} + \frac{1}{MTTF_{D(Antrieb)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{90\%}{276y} + \frac{90\%}{273y} + \frac{90\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{276y} + \frac{1}{273y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91{,}30\%$$

或采用 DC = 99% 进行计算

$$DC_{avg} = \frac{\frac{99\%}{276y} + \frac{99\%}{273y} + \frac{99\%}{118y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{276y} + \frac{1}{273y} + \frac{1}{118y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

⚠ 警告

停转

当电机处于停止状态时，仅当请求运动时才会检测到编码器信号停滞等错误。设备制造商或用户必须考虑到这一点。

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

或输入子系统采用 DC = 99% 进行计算：

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

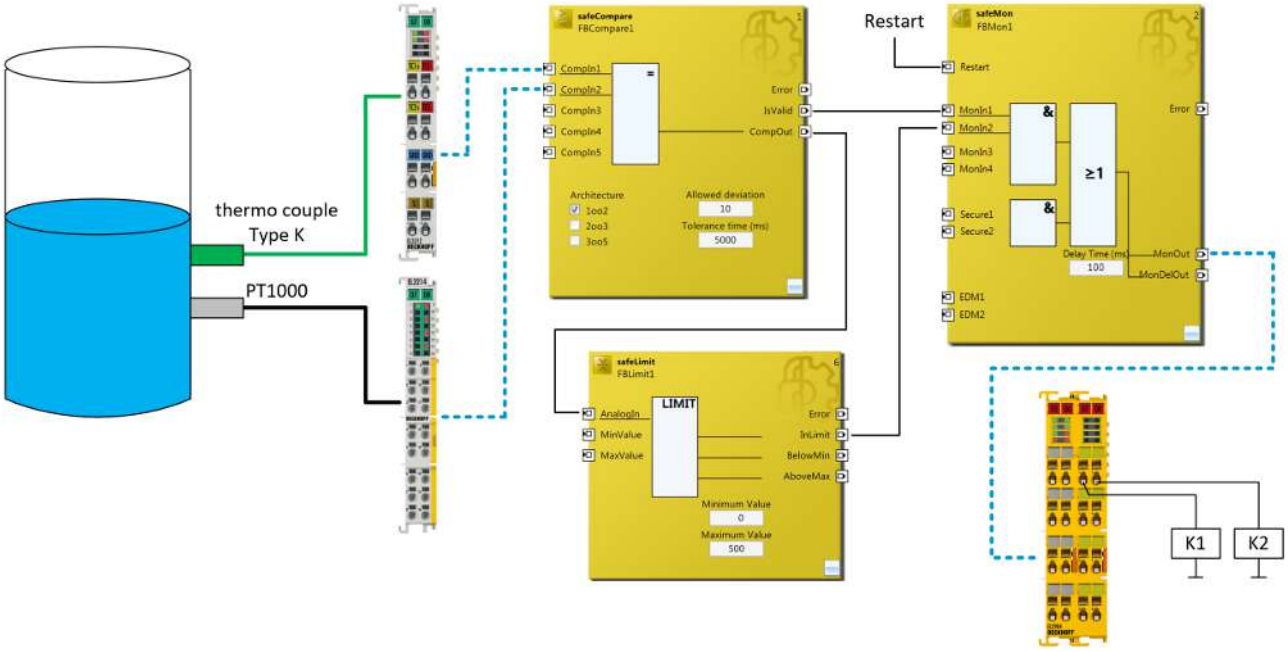
根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

8.3 采用 TwinSAFE SC 进行温度测量（类别 3，PL d）

本示例说明了如何使用 TwinSAFE SC 技术实现温度测量。为此，两个测量点都配有温度传感器，其中一个带 K 型热电偶（连接到标准 EtherCAT 端子模块 EL3312），另一个带 PT1000 测量电阻（连接到 TwinSAFE SC EtherCAT 端子模块 EL3214-0090）。

通过安全 TwinSAFE 逻辑 EL6910 内的 Compare 功能块对这两个信号进行比较或校验。然后，信号通过 *Limit* 功能块进行检查。*Limit* 功能块的结果和 Compare 功能块的 *IsValid* 输出通过 *Mon* 功能块使用，以切断接触器 K1 和 K2。

说的更明白一点，在本例中并未显示接触器控制，但用户应牢记在心。



⚠ 谨慎

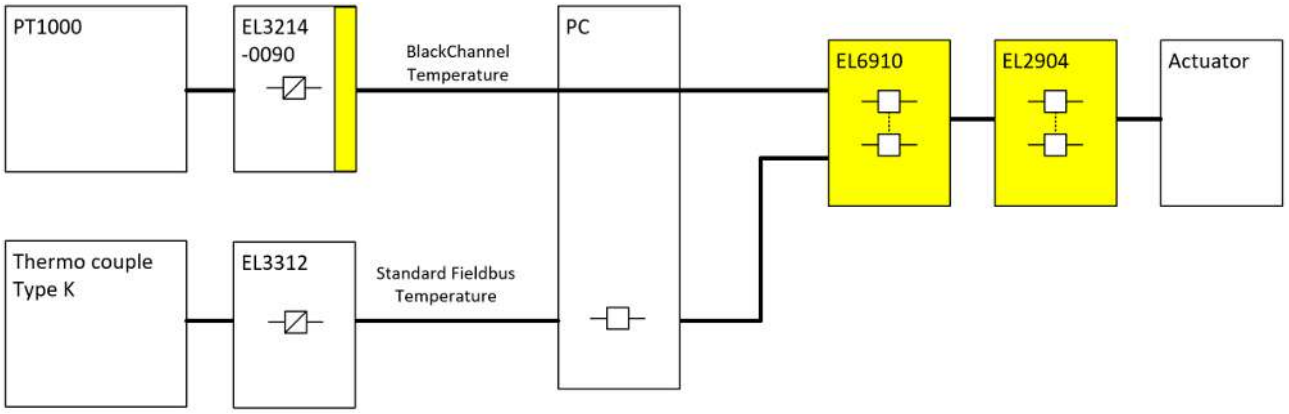
急停/接触器监控！

除上述功能外，用户必须额外实现接触器监控（例如通过 EDM 功能块监控 K1 和 K2），并视需要配置急停功能！

下表列出了可用于此应用示例的替代型 TwinSAFE SC 产品。在本例中描述的假设和论证仍需纳入考量。

温度测量示例：EL3312 可用于 K 型热电偶，EL3214-0090 可用于 Pt100 测量电阻
无替代型 TwinSAFE SC 产品可用。

8.3.1 配置示意图



8.3.2 结构和诊断

在两个测量点读取的信号是采用不同技术的标准信号。至少有一个信号通过 TwinSAFE SC 技术传输至安全的 TwinSAFE 逻辑，从而可以在 PC 中或通信路径上检测到该信号的畸变。在允许的公差范围内，在安全的 TwinSAFE 逻辑中对这两个信号进行等值测试。

各项错误假设及相应的预期情况列于下方的 FMEA 表格中。

8.3.3 FMEA

错误假设	预期情况	已检查
通过标准现场总线传输的温度值停滞	通过第二个值以及 EL6910 中的合理性检查检测到该值。	
通过 TwinSAFE SC 通信传输的温度值停滞	通过 TwinSAFE SC 通信中的 Watchdog（看门狗）以及 EL6910 中的合理性检查检测到该情况。	
温度值在标准 PLC 中相互复制	TwinSAFE SC 通信中的畸变值会导致报文中出现无效的 CRC，从而立即关闭组和输出。	
通过标准现场总线传输的温度值发生畸变	通过第二个值以及 EL6910 中的合理性检查检测到该值。	
传感器与 EtherCAT 端子模块之间的连接已断开	通过采用 EL6910 中第二个温度值的合理性检查检测到该情况。	
PT1000 提供错误的温度值	通过采用 EL6910 中第二个温度值的合理性检查检测到该情况。	
热电偶提供的错误的温度值	通过采用 EL6910 中第二个温度值的合理性检查检测到该情况。	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误：损坏	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：非预期重复	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：错误顺序	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：丢失	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：不可接受的延迟	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误： 插入	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 伪装	与标准无关，仅适用于安全通信。	
基于 61784-3 标准的通讯错误： 寻址	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
标准通信的通信错误： 交换机中的重复性内存错误	通过温度值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

8.3.3.1 关于 TwinSAFE SC 通信的说明：

TwinSAFE SC 通信采用与 Saftey over EtherCAT 通信相同的错误检测机制，区别在于其使用不同的多项式计算校验和，且该多项式与之前 Safety over EtherCAT 所用的多项式具有充分的独立性。

这些相同的机制均处于激活状态，例如黑色通道原理（比特错误概率 10^{-2}）。

数据传输的质量并非关键因素，因为所有传输错误最终都会通过安全的 TwinSAFE 逻辑中的比较被检测出来，因为这类错误将导致数据不一致。

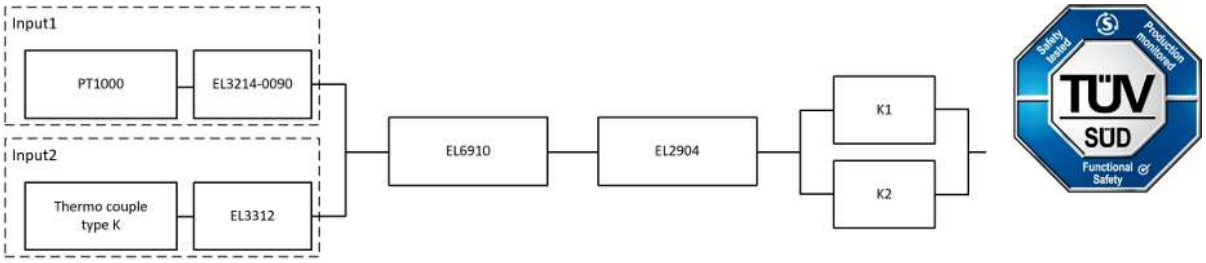
8.3.4 安全输出端子模块的参数

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

8.3.5 功能块结构和安全回路

8.3.5.1 安全功能 1



8.3.6 计算

8.3.6.1 PFHD / MTTFD / B10D – 值

组件	值
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
PT1000 – $MTTF_D$	7,618 a（根据 EN ISO 13849-1:2015 表 C.5）
K 型热电偶 – FIT	1900（10^9 小时中的错误数）

组件	值
EL3214-0090 - MTBF	890,000
EL3312 - MTBF	1,661,253
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

8.3.6.2 诊断覆盖率 DC

组件	值
通过 TwinSAFE SC 传输的温度值以及逻辑内的合理性检查	DC_{avg}=90%（计算中替代值：99%）
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

8.3.6.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN 13849 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

根据 MTBF 值计算 PFH_D 和 $MTTF_D$ 值：

注：维修时间可以忽略不计，因此以下内容适用：

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

及

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

PT1000

$$MTTF_D = 7618y = 66.733.680h$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{66.733.680h} = 1,50E-09$$

EL3214-0090

$$MTTF_D = 2 * MTBF = 2 * 890.000h = 1.780.000h = 203y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{1.780.000h} = 5,62E-08$$

输入系统 1

$$PFH_{(Input1)} = PFH_{(PT1000)} + PFH_{(EL3214-0090)} = 1,50E-09 + 5,62E-08 = 5,77E-08$$

热电偶

$$MTTF_D = \frac{1}{\lambda_D} = \frac{1}{1900FIT} * 10^9 h = 526.315h = 60y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{526.315h} = 19,0E-08$$

EL3312

$$MTTF_D = 2 * MTBF = 2 * 1.661.253h = 3.322.506h = 379y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{3.322.506h} = 3,0E-08$$

输入系统 2

$$PFH_{(Input2)} = PFH_{(ThermoCouple)} + PFH_{(EL3312)} = 19,0E-08 + 3,0E-08 = 22,0E-08$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接反馈

$$PFH = \frac{1-0,99}{593607,3 * 8760} = 1,92E-12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

来自带 EL3214-0090 的 PT1000 和带 EL3312 的热电偶的输入信号采用不同的测量程序。两者都提供温度值，且均参与安全功能的实现。通道故障不会导致危险情况，但会通过比较 TwinSAFE 逻辑中的两个值被检测到，并导致关断。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输入子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{5,77E-08 + 22,0E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,693E-08$$

注意

EN 62061

根据 EN 62061 标准，输入子系统需以 90% 的 SFF 或 DC 值进行评估。根据 EN 62061 表 5，这将系统可实现的最大 SIL 值限制为 2。

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值的替代计算（在相同假设条件下）

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

较低值取自输入子系统：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(ThermoCouple)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 45,5y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(PT1000)}} + \frac{DC}{MTTF_{D(EL3214)}} + \frac{DC}{MTTF_{D(Thermocouple)}} + \frac{DC}{MTTF_{D(EL3312)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(PT1000)}} + \frac{1}{MTTF_{D(EL3214)}} + \frac{1}{MTTF_{D(Thermocouple)}} + \frac{1}{MTTF_{D(EL3312)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

采用 DC=90% 进行计算

$$DC_{avg} = \frac{\frac{90\%}{7618y} + \frac{90\%}{203y} + \frac{90\%}{60y} + \frac{90\%}{379y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{7618y} + \frac{1}{203y} + \frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,11\%$$

或采用 DC = 99% 进行计算

$$DC_{avg} = \frac{\frac{99\%}{7618y} + \frac{99\%}{203y} + \frac{99\%}{60y} + \frac{99\%}{379y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{7618y} + \frac{1}{203y} + \frac{1}{60y} + \frac{1}{379y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

输入子系统采用 DC = 90% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

或输入子系统采用 DC = 99% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%

DC	
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

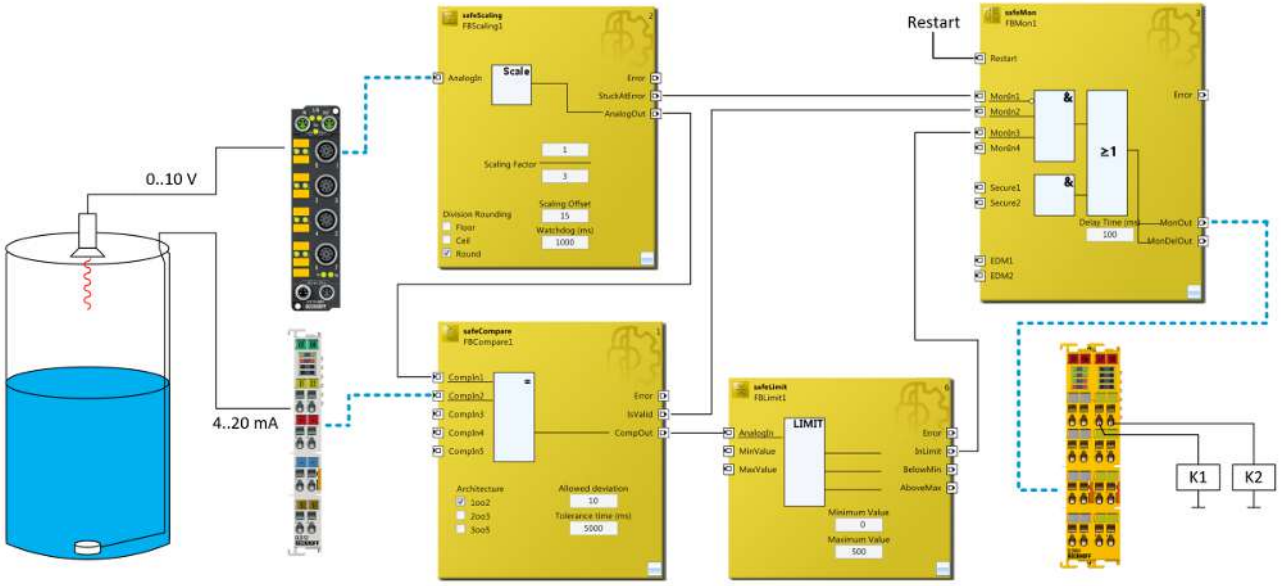
根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

8.4 采用 TwinSAFE SC 进行液位测量（类别 3，PL d）

本示例说明了如何使用 TwinSAFE SC 技术实现容器的液位测量。为此，采用了两种不同的测量方法。一种方法是使用一个带 0 - 10 V 接口的超声波传感器（连接到 TwinSAFE SC EtherCAT 端子盒 EP3174-0092），另一种方法是使用一个带 4-20 mA 接口的液位探针（连接到标准 EtherCAT 端子模块 EL3152）。

通过安全 TwinSAFE 逻辑 EL6910 内的 Compare 功能块对这两个信号进行比较或校验。EP3174-0092 中的信号首先通过 Scale 功能块缩放，使得两个信号具有相同的值范围。然后，信号通过 *Limit* 功能块进行检查。*Limit* 功能块的结果和 Compare 功能块的 *IsValid* 输出通过 *Mon* 功能块使用，以切断接触器 K1 和 K2。另外，Scale 功能块的 StuckAtError 输出可以连接到 Mon 输入。通过这种配置可以检测信号停滞现象。

说的更明白一点，在本例中并未显示接触器控制，但用户应牢记在心。



⚠ 谨慎

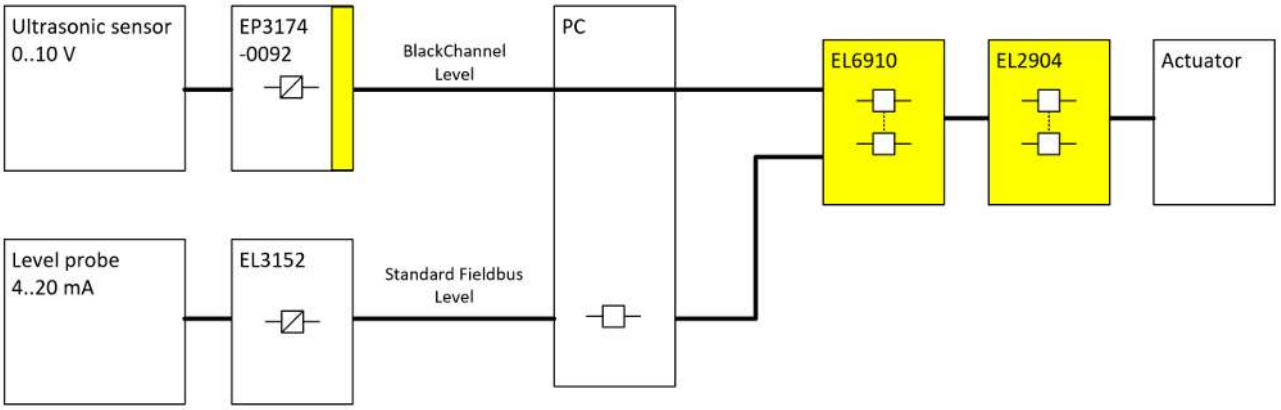
急停/接触器监控

除上述功能外，用户必须额外实现接触器监控（例如通过 EDM 功能块监控 K1 和 K2），并视需要配置急停功能！

下表列出了可用于此应用示例的替代型 TwinSAFE SC 产品。在本例中描述的假设和论证仍需纳入考量。

液位测量示例：EP3174-0092 端子盒可用于超声波传感器（0–10 V），EL3152 端子模块可用于液位探针（4–20 mA）		
带 0 - 10 V 和/或 +/- 10 V 模拟量输入或带 IO-Link 接口传感器的替代型 TwinSAFE SC 产品	EL3174-0090	EtherCAT 端子模块，4 通道模拟量输入，多功能，±10 V，±20 mA，16 位，TwinSAFE SC
	EL6224-0090	EtherCAT 端子模块，4 通道通信接口，IO-Link，主站，TwinSAFE SC
	EJ6224-0090	EtherCAT 插拔式模块，4 通道通信接口，IO-Link，主站，TwinSAFE SC
	EP6224-0092	EtherCAT 端子盒，4 通道通信接口 + 4 通道数字量输入，IO-Link，主站，Class A，M12，TwinSAFE SC

8.4.1 配置示意图



8.4.2 结构和诊断

在两个测量点读取的信号是采用不同技术的标准信号。至少有一个信号通过 TwinSAFE SC 技术传输至安全的 TwinSAFE 逻辑，从而可以在 PC 中或通信路径上检测到该信号的畸变。在允许的公差范围内，在安全的 TwinSAFE 逻辑中对这两个信号进行等值测试。

各项错误假设及相应的预期情况列于下方的 FMEA 表格中。

8.4.3 FMEA

错误假设	预期情况	已检查
通过标准现场总线传输的液位数值停滞	通过第二个值以及 EL6910 中的合理性检查检测到该值。	
通过 TwinSAFE SC 通信传输的液位数值停滞	通过 TwinSAFE SC 通信中的 Watchdog（看门狗）以及 EL6910 中的合理性检查检测到该情况。	
液位数值在标准 PLC 中相互复制	TwinSAFE SC 通信中的畸变值会导致报文中出现无效的 CRC，从而立即关闭组和输出。	
通过标准现场总线传输的液位数值发生畸变	通过第二个值以及 EL6910 中的合理性检查检测到该值。	
传感器与 EtherCAT 端子模块之间的连接已断开	通过采用 EL6910 中第二个液位数值的合理性检查检测到该情况。	
超声波传感器提供错误的液位数值	通过采用 EL6910 中第二个液位数值的合理性检查检测到该情况。	
液位探针提供错误的液位数值	通过采用 EL6910 中第二个液位数值的合理性检查检测到该情况。	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误：损坏	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：非预期重复	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：错误顺序	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：丢失	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：不可接受的延迟	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误： 插入	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 伪装	与标准无关，仅适用于安全通信。	
基于 61784-3 标准的通讯错误： 寻址	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
标准通信的通信错误： 交换机中的重复性内存错误	通过液位数值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

8.4.3.1 关于 TwinSAFE SC 通信的说明：

TwinSAFE SC 通信采用与 Saftey over EtherCAT 通信相同的错误检测机制，区别在于其使用不同的多项式计算校验和，且该多项式与之前 Safety over EtherCAT 所用的多项式具有充分的独立性。

这些相同的机制均处于激活状态，例如黑色通道原理（比特错误概率 10^{-2}）。

数据传输的质量并非关键因素，因为所有传输错误最终都会通过安全的 TwinSAFE 逻辑中的比较被检测出来，因为这类错误将导致数据不一致。

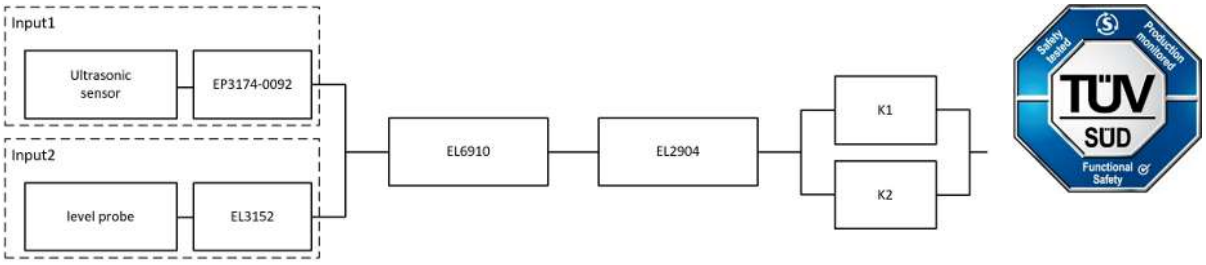
8.4.4 安全输出端子模块的参数

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

8.4.5 功能块结构和安全回路

8.4.5.1 安全功能 1



8.4.6 计算

8.4.6.1 PFHD / MTTFD / B10D – 值

组件	值
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
超声波传感器 – MTBF	195 a（1,708,200 h）
液位探针 – MTTF	732 a（6,412,320 h）

组件	值
EP3174-0092 - MTBF	600,000 h
EL3152 - MTBF	2,507,303 h
K1 – $B10_D$	1,300,000 h
K2 – $B10_D$	1,300,000 h
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

8.4.6.2 诊断覆盖率 DC

组件	值
通过 TwinSAFE SC 传输的液位数值以及逻辑内的合理性检查	DC_{avg}=90%（计算中替代值：99%）
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

8.4.6.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN 13849 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

根据 MTBF 值计算 PFH_D 和 $MTTF_D$ 值：

注：维修时间可以忽略不计，因此以下内容适用：

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

及

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

超声波传感器

$$MTTF_D = 2 * MTBF = 2 * 195y = 390y = 3.416.400h$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{3.416.400h} = 2,93E-08$$

EP3174-0092

$$MTTF_D = 2 * MTBF = 2 * 600.000h = 1.200.000h = 136y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{1.200.000h} = 8,33E-08$$

输入系统 1

$$PFH_{(Input1)} = PFH_{(Ultrasonic)} + PFH_{(EP3174-0092)} = 2,93E-08 + 8,33E-08 = 11,26E-08$$

液位探针

$$MTTF_D = 2 * MTTF = 2 * 732y = 1.464y = 12.824.640h$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{12.824.640h} = 7,79E-09$$

EL3152

$$MTTF_D = 2 * MTBF = 2 * 2.507.303h = 5.014.606h = 572y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{5.014.606h} = 1,99E-08$$

输入系统 2

$$PFH_{(Input2)} = PFH_{(Level\,Probe)} + PFH_{(EL3152)} = 7,79E-09 + 1,99E-08 = 2,77E-08$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接反馈

$$PFH = \frac{1-0,99}{593607,3 * 8760} = 1,92E-12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

来自带 EP3174-0092 的超声波传感器和带 EL3152 的液位探针的输入信号采用不同的测量程序。两者都提供液位数值，且均参与安全功能的实现。通道故障不会导致危险情况，但会通过比较 TwinSAFE 逻辑中的两个值被检测到，并导致关断。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输入子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{11,26E-08 + 2,77E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,005E-08$$

注意

EN 62061

根据 EN 62061 标准，输入子系统需以 90% 的 SFF 或 DC 值进行评估。根据 EN 62061 表 5，这将系统可实现的最大 SIL 值限制为 2。

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值的替代计算（在相同假设条件下）

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

较低值取自输入子系统：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(UltraSonicSensor)}} + \frac{1}{MTTF_{D(EP3174-0092)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 79,46y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(UltraSonic)}} + \frac{DC}{MTTF_{D(EP3174-0092)}} + \frac{DC}{MTTF_{D(Level\,Probe)}} + \frac{DC}{MTTF_{D(EL3152)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(UltraSonic)}} + \frac{1}{MTTF_{D(EP3174-0092)}} + \frac{1}{MTTF_{D(Level\,Probe)}} + \frac{1}{MTTF_{D(EL3152)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

采用 DC=90% 进行计算

$$DC_{avg} = \frac{\frac{90\%}{390y} + \frac{90\%}{136y} + \frac{90\%}{1464y} + \frac{90\%}{572y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{1464y} + \frac{1}{572y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,33\%$$

或采用 DC = 99% 进行计算

$$DC_{avg} = \frac{\frac{99\%}{390y} + \frac{99\%}{136y} + \frac{99\%}{1464y} + \frac{99\%}{572y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{390y} + \frac{1}{136y} + \frac{1}{1464y} + \frac{1}{572y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99,00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

输入子系统采用 DC = 90% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

或输入子系统采用 DC = 99% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%

DC	
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

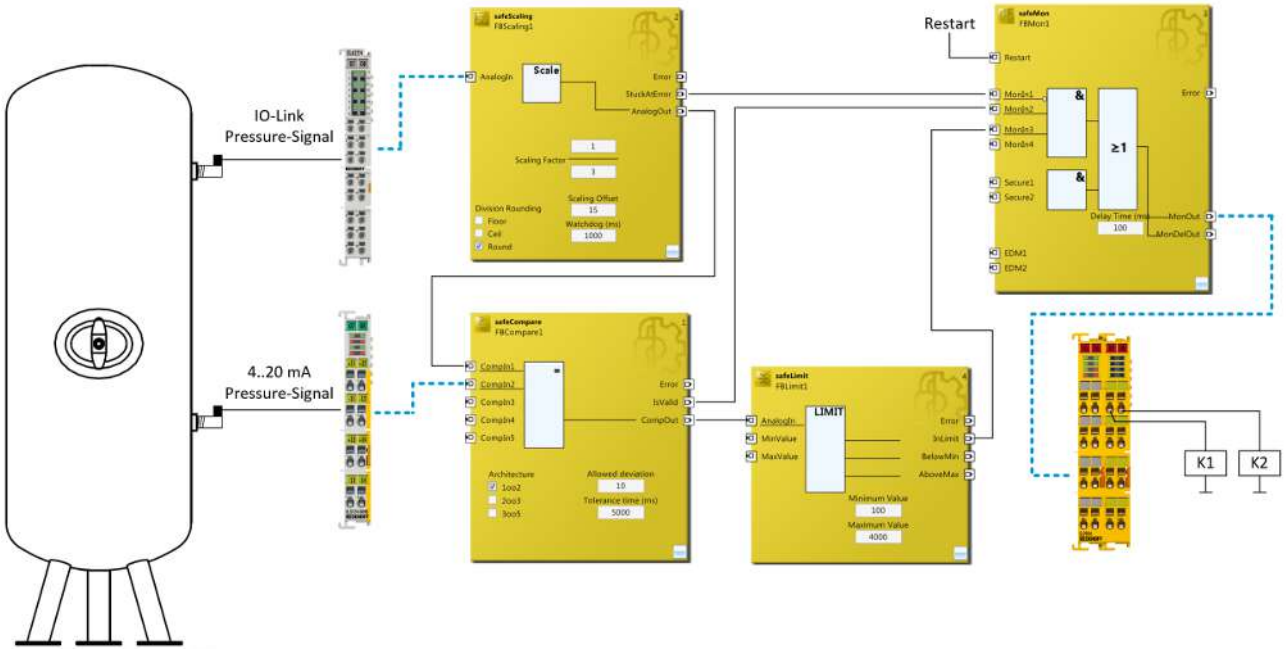
根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

8.5 采用 TwinSAFE SC 进行压力测量（类别 3，PL d）

本示例说明了如何使用 TwinSAFE SC 技术实现容器的压力测量。为此，两个测量点都配有压力传感器，其中一个压力传感器带 IO-Link 接口（连接到标准 EtherCAT 端子模块 EL6224），另一个压力传感器带 4-20 mA 接口（连接到 TwinSAFE SC EtherCAT 端子模块 EL3124-0090）。

通过安全 TwinSAFE 逻辑 EL6910 内的 Compare 功能块对这两个信号进行比较或校验。EL6224 中的信号首先通过 Scale 功能块缩放，使得两个信号具有相同的值范围。然后，信号通过 *Limit* 功能块进行检查。*Limit* 功能块的结果和 Compare 功能块的 *IsValid* 输出通过 *Mon* 功能块使用，以切断接触器 K1 和 K2。另外，Scale 功能块的 StuckAtError 输出可以连接到 Mon 输入。通过这种配置可以检测信号停滞现象。

说的更明白一点，在本例中并未显示接触器控制，但用户应牢记在心。



⚠ 警告

压力安全阀（PSV）！

根据 EC 压力设备指令，上述应用不能用作压力安全阀的替代方案。

⚠ 谨慎

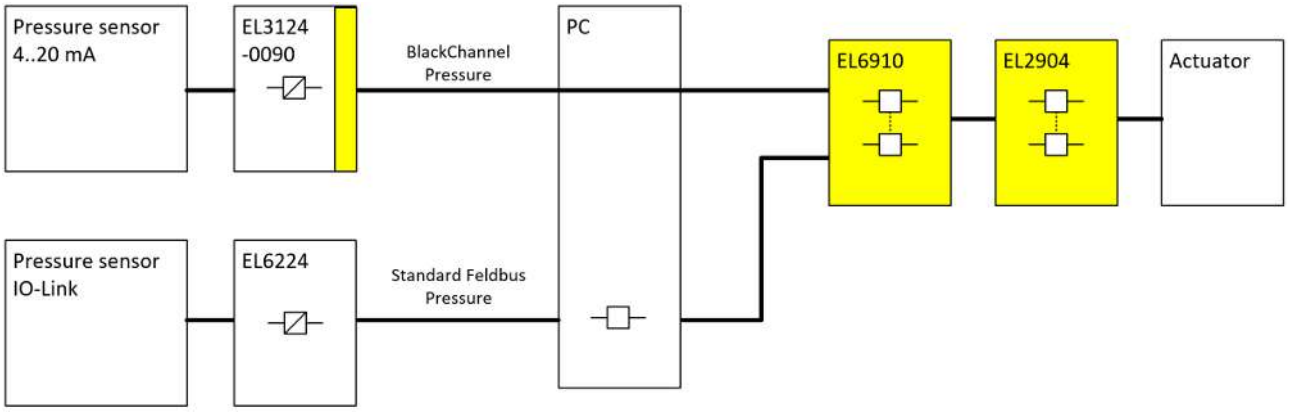
急停/接触器监控！

除上述功能外，用户必须额外实现接触器监控（例如通过 EDM 功能块监控 K1 和 K2），并视需要配置急停功能！

下表列出了可用于此应用示例的替代型 TwinSAFE SC 产品。在本例中描述的假设和论证仍需纳入考量。

压力测量示例：EL6224 可用于压力传感器（IO-Link 接口），EL3124-0090 可用于压力传感器（4…20 mA）		
带 4–20mA 模拟量输入的可选 TwinSAFE SC 产品	EL3174-0090	EtherCAT 端子模块，4 通道模拟量输入，多功能，±10 V，±20 mA，16 位，TwinSAFE SC
	EP3174-0092	EtherCAT 端子盒，4 通道模拟量输入，多功能，±10 V，0/4…20 mA，16 位，差分，M12，TwinSAFE SC

8.5.1 配置示意图



8.5.2 结构和诊断

在两个测量点读取的信号是采用不同技术的标准信号。至少有一个信号通过 TwinSAFE SC 技术传输至安全的 TwinSAFE 逻辑，从而可以在 PC 中或通信路径上检测到该信号的畸变。在允许的公差范围内，在安全的 TwinSAFE 逻辑中对这两个信号进行等值测试。

各项错误假设及相应的预期情况列于下方的 FMEA 表格中。

8.5.3 FMEA

错误假设	预期情况	已检查
通过标准现场总线传输的压力值停滞	通过第二个值以及 EL6910 中的合理性检查检测到该值。	
通过 TwinSAFE SC 通信传输的压力值停滞	通过 TwinSAFE SC 通信中的 Watchdog（看门狗）以及 EL6910 中的合理性检查检测到该情况。	
压力值在标准 PLC 中相互复制	TwinSAFE SC 通信中的畸变值会导致报文中出现无效的 CRC，从而立即关闭组和输出。	
通过标准现场总线传输的压力值发生畸变	通过第二个值以及 EL6910 中的合理性检查检测到该值。	
传感器与 EtherCAT 端子模块之间的连接已断开	通过采用 EL6910 中第二个压力值的合理性检查检测到该情况。	
压力传感器（4..20 mA）提供错误的压力值	通过采用 EL6910 中第二个压力值的合理性检查检测到该情况。	
压力传感器（IO-Link）提供错误的压力值	通过采用 EL6910 中第二个压力值的合理性检查检测到该情况。	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误：损坏	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：非预期重复	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：错误顺序	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：丢失	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误：不可接受的延迟	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误： 插入	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 伪装	与标准无关，仅适用于安全通信。	
基于 61784-3 标准的通讯错误： 寻址	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
标准通信的通信错误： 交换机中的重复性内存错误	通过压力值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

8.5.3.1 关于 TwinSAFE SC 通信的说明：

TwinSAFE SC 通信采用与 Saftey over EtherCAT 通信相同的错误检测机制，区别在于其使用不同的多项式计算校验和，且该多项式与之前 Safety over EtherCAT 所用的多项式具有充分的独立性。

这些相同的机制均处于激活状态，例如黑色通道原理（比特错误概率 10^{-2}）。

数据传输的质量并非关键因素，因为所有传输错误最终都会通过安全的 TwinSAFE 逻辑中的比较被检测出来，因为这类错误将导致数据不一致。

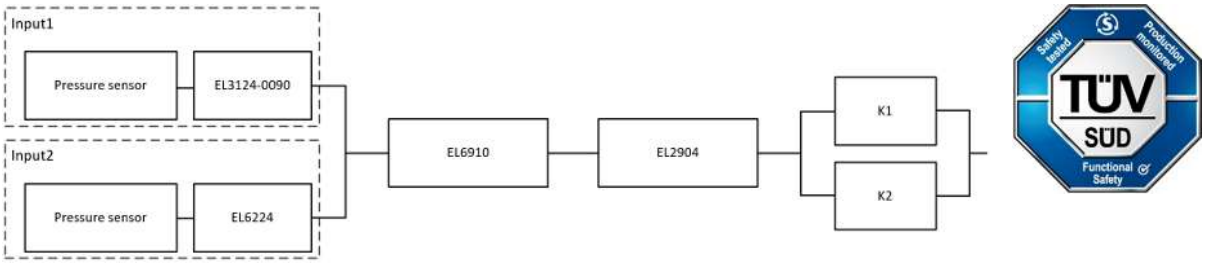
8.5.4 安全输出端子模块的参数

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

8.5.5 功能块结构和安全回路

8.5.5.1 安全功能 1



8.5.6 计算

8.5.6.1 PFHD / MTTFD / B10D – 值

组件	值
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
压力传感器 1（4-20 mA） – MTTF	124 a（1,086,240 h）
压力传感器 2 IO-Link – MTTF	201 a（1,760,760 h）

组件	值
EL3124-0090 - MTBF	950,000 h
EL6224 - MTBF	1,607,919 h
K1 – $B10_D$	1,300,000 h
K2 – $B10_D$	1,300,000 h
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

8.5.6.2 诊断覆盖率 DC

组件	值
通过 TwinSAFE SC 传输的压力值以及逻辑内的合理性检查	DC_{avg}=90%（计算中替代值：99%）
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

8.5.6.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN 13849 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

根据 MTBF 值计算 PFH_D 和 $MTTF_D$ 值：

注：维修时间可以忽略不计，因此以下内容适用：

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

及

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

压力传感器 1（4-20 mA）

$$MTTF_D = 2 * MTTF = 2 * 124y = 248y = 2.172.480h$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{2.172.480h} = 4,60E-08$$

EL3124-0090

$$MTTF_D = 2 * MTBF = 2 * 950.000h = 1.900.000h = 216y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{1.900.000h} = 5,26E-08$$

输入系统 1

$$PFH_{(Input1)} = PFH_{(PressureSensor1)} + PFH_{(EL3124-0090)} = 4,60E-08 + 5,26E-08 = 9,86E-08$$

压力传感器 2（IO-Link）

$$MTTF_D = 2 * MTBF = 2 * 1.760.760h = 3.521.520h = 402y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{3.521.520h} = 2,84E-08$$

EL6224

$$MTTF_D = 2 * MTBF = 2 * 1.607.919h = 3.215.838h = 367y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{3.215.838h} = 3,11E-08$$

输入系统 2

$$PFH_{(Input2)} = PFH_{(PressureSensor2)} + PFH_{(EL6224)} = 2,84E-08 + 3,11E-08 = 5,95E-08$$

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1 * 21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接反馈

$$PFH = \frac{1-0,99}{593607,3 * 8760} = 1,92E-12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

来自带 EL3124-0090 的压力传感器 1 和带 EL6224 的压力传感器 2 的输入信号采用不同的测量程序。两者都提供压力值，且均参与安全功能的实现。通道故障不会导致危险情况，但会通过比较 TwinSAFE 逻辑中的两个值被检测到，并导致关断。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输入子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1 + PFH_{(EL6910)} + PFH_{(EL2904)}$$
$$+\beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 和 $(1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 10\% * \frac{9,86E-08 + 5,95E-08}{2} + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,92E-12 + 1,92E-12}{2}$$
$$= 1,094E-08$$

注意

EN 62061

根据 EN 62061 标准，输入子系统需以 90% 的 SFF 或 DC 值进行评估。根据 EN 62061 表 5，这将系统可实现的最大 SIL 值限制为 2。

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值的替代计算（在相同假设条件下）

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

较低值取自输入子系统：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(PressureSensor)}} + \frac{1}{MTTF_{D(EL3124-0090)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 88,27y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Pressure1)}} + \frac{DC}{MTTF_{D(EL3124-0090)}} + \frac{DC}{MTTF_{D(Pressure2)}} + \frac{DC}{MTTF_{D(EL6224)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Pressure1)}} + \frac{1}{MTTF_{D(EL3124-0090)}} + \frac{1}{MTTF_{D(Pressure2)}} + \frac{1}{MTTF_{D(EL6224)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

采用 DC=90% 进行计算

$$DC_{avg} = \frac{\frac{90\%}{248y} + \frac{90\%}{216y} + \frac{90\%}{402y} + \frac{90\%}{367y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{402y} + \frac{1}{367y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 91,41\%$$

或采用 DC = 99% 进行计算

$$DC_{avg} = \frac{\frac{99\%}{248y} + \frac{99\%}{216y} + \frac{99\%}{402y} + \frac{99\%}{367y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{248y} + \frac{1}{216y} + \frac{1}{402y} + \frac{1}{367y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}} = 99{,}00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

输入子系统采用 DC = 90% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

或输入子系统采用 DC = 99% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%

DC	
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

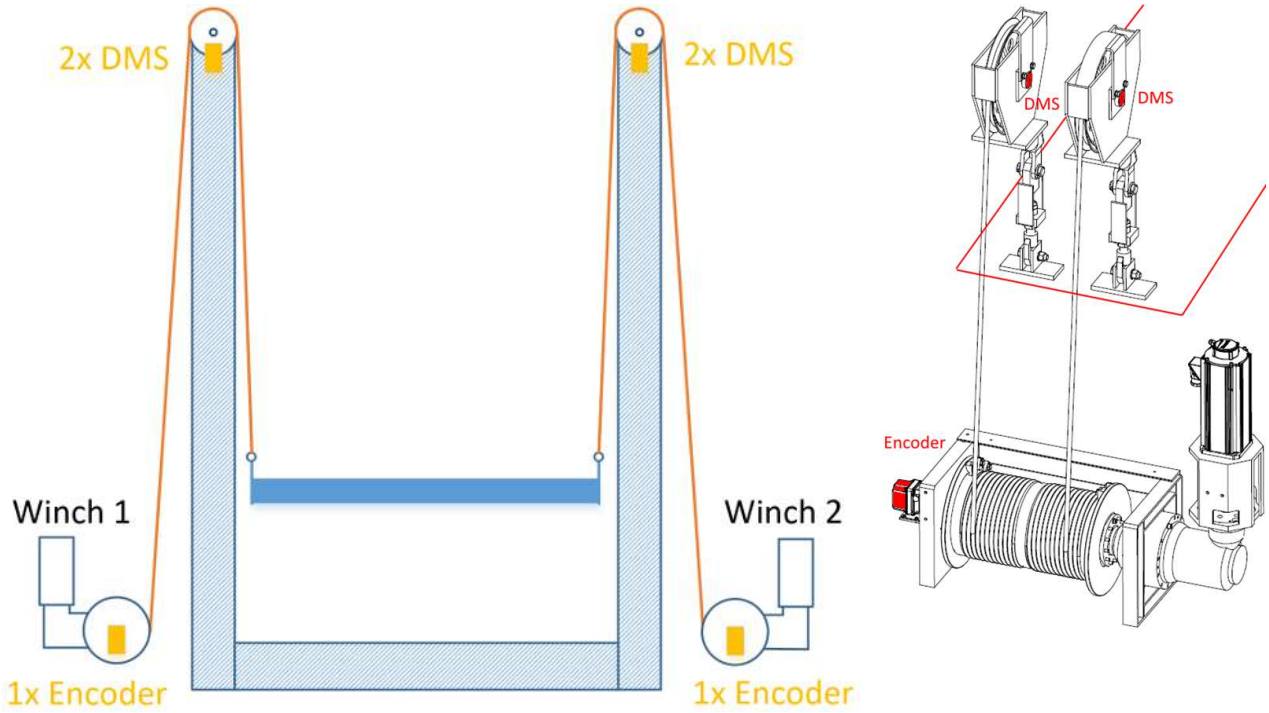
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

根据 EN62061 表 3 确定的安全完整性等级	
安全完整性等级	每小时发生危险故障的概率（PFH_D）
3	⩾ 10^{-8} 至 < 10^{-7}
2	**⩾ 10^{-7} 至 < 10^{-6}**
1	⩾ 10^{-6} 至 < 10^{-5}

8.6 升降设备的监测（类别 3，PL d）

从安全角度出发，需要对一个升降设备进行监测，该设备由两个带导向滑轮的绞盘组成，用于驱动升降台。需实现“松绳检测”与“过载”功能。两侧立柱顶端各安装两个带 SG 传感器的导向滑轮，即一共配备四个 SG 传感器。其中一侧的两个传感器之一通过 TwinSAFE SC 端子模块 EL3356-0090 进行读入。另一个 SG 传感器连接至 EL3751。这提供了一个 SG mV/V 信号，需在安全逻辑中转换为重量值，以便与 EL3356-0090 的值进行比较。



安全功能 1 – 过载

升降设备规定了最大允许有效载荷。此项必须进行监测。完成 EL3751 和 EL3356-0090 信号的合理性检查后，通过 EL6910 中的 Limit 功能块对结果进行限值处理。

根据客户的风险与危害分析，该安全功能必须按照 EN 13849-1:2023 标准被评定为 PL c。

该安全功能被设置为类别 3 结构。

安全功能 2 – 松绳检测

松绳检测用于判断升降滑块是否因机械卡阻或触底而停滞。在上述任一情况下，均须立即关闭系统。此外，该功能还能检测到绳索是否被卡住。

根据客户的风险与危害分析，该安全功能必须按照 EN 13849-1:2023 标准被评定为 PL c。

该安全功能被设置为类别 3 结构。

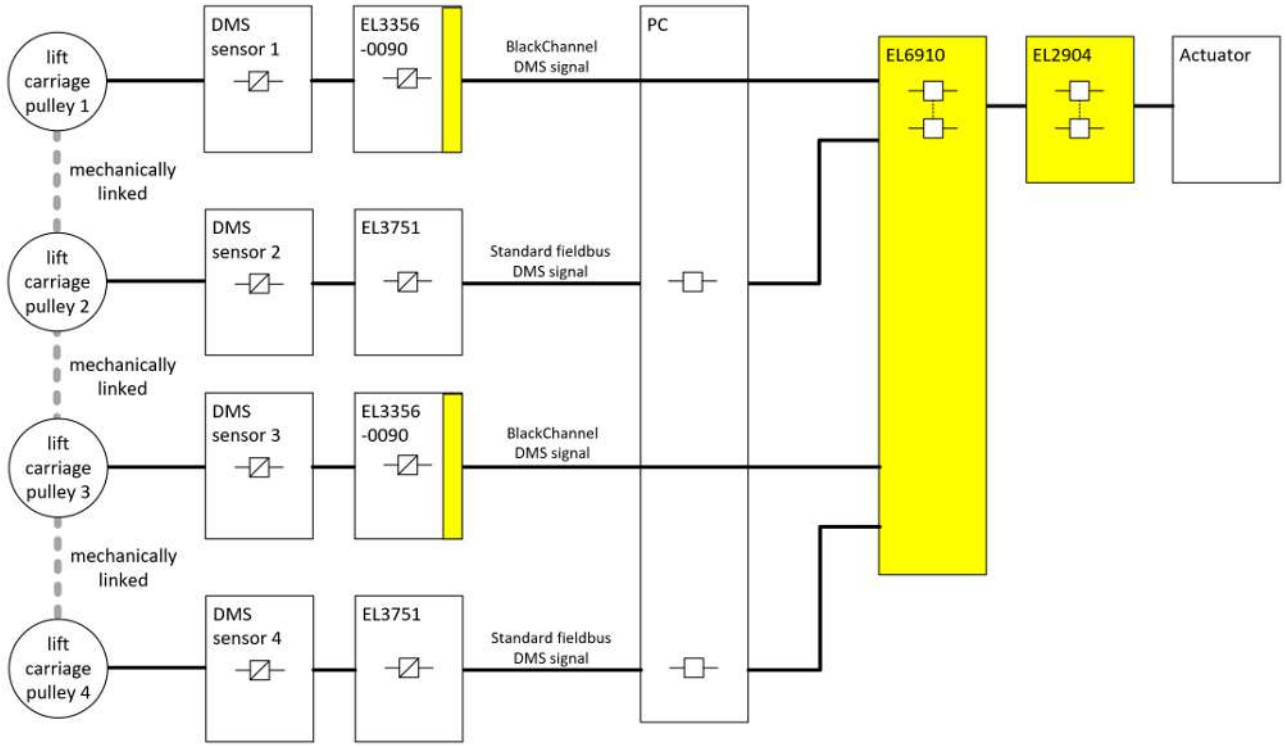
附加功能 – 无安全要求

通过对比绞盘 1 与绞盘 2 的编码器值进行增量检查，可实现同步性监测。这能防止升降滑块因两个绞盘牵引角度偏差而在早期阶段发生倾斜。

下表列出了可用于此应用示例的替代型 TwinSAFE SC 产品。在本例中描述的假设和论证仍需纳入考量。

示例：监测升降设备、松绳检测和过载：导向滑轮上安装的 SG 传感器（EL3356-0090 和 EL3751）
无替代型 TwinSAFE SC 产品可用。

8.6.1 结构图架构



8.6.2 结构和诊断

SG 传感器的读入信号是标准信号，两侧的记录方式各不相同。第一个 SG 传感器连接至 EL3356-0090 SG 端子模块，该端子模块将确定的重量值打包成安全报文（带修正多项式的 FSoE - TwinSAFE SC）并传输至 EL6910。第二个 SG 传感器连接至 EL3751 端子模块，该端子模块执行 SG mV/V 测量。该信号通过标准通信路径发送至 EL6910。在执行合理性检查之前，该信号会被转换为安全逻辑中的重量值。

带有 SG 传感器 3 和 4 的升降装置的第二侧采用相同的流程。与第一侧相比，第二个 EL3356-0090 的 TwinSAFE SC 通信使用不同的多项式。这样可以检测到两个 TwinSAFE SC 连接数据相互复制的情况。

8.6.3 FMEA

错误假设	预期情况	已检查
通过标准现场总线传输的 SG 信号停滞	通过第二个值以及 EL6910 中的合理性检查（EL3356-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况。	
通过 TwinSAFE SC 通信传输的 SG 信号停滞	通过第二个值和 EL6910 中的合理性检查以及 TwinSAFE SC 通信中的 Watchdog（看门狗）检测到该情况。	
SG 值在标准 PLC 中相互复制	TwinSAFE SC 通信中的畸变值会导致报文中出现无效的 CRC，从而立即关闭组和输出。 两个 SG 值的数据类型长度不同，因为其中一个打包在 TwinSAFE SC 报文中（例如 4 字节和 11 字节）	
通过标准现场总线传输的 SG 信号发生畸变	通过第二个值以及 EL6910 中的合理性检查（EL3356-0090 与 EL6910 之间的 TwinSAFE SC 通信）检测到该情况	
升降滑块与绞盘之间不再存在机械连接	通过采用 EL6910 中第二个 SG 信号的合理性检查检测到该情况。	
EL3356-0090 提供错误的 SG 值	通过采用 EL6910 中 EL3751 SG 值的合理性检查检测到该情况	
EL3751 返回错误的 SG 值	通过采用 EL6910 中 EL3356-0090 SG 值的合理性检查检测到该情况	

错误假设	预期情况	已检查
基于 61784-3 标准的通讯错误： 损坏	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 非预期重复	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 错误顺序	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 丢失	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 不可接受的延迟	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 插入	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
基于 61784-3 标准的通讯错误： 伪装	与标准无关，仅适用于安全通信。	
基于 61784-3 标准的通讯错误： 寻址	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	
标准通信的通信错误： 交换机中的重复性内存错误	通过 SG 值的合理性检查以及 EL6910 内的 TwinSAFE SC 通信检测到该情况	

8.6.3.1 关于 TwinSAFE SC 通信的说明：

TwinSAFE SC 通信采用与 Saftey over EtherCAT 通信相同的错误检测机制，区别在于其使用不同的多项式计算校验和，且该多项式与之前 Safety over EtherCAT 所用的多项式具有充分的独立性。

这些相同的机制均处于激活状态，例如黑色通道原理（比特错误概率 10^{-2}）。

数据传输的质量并非关键因素，因为所有传输错误最终都会通过安全逻辑中的比较被检测出来，因为这类错误将导致数据不一致。

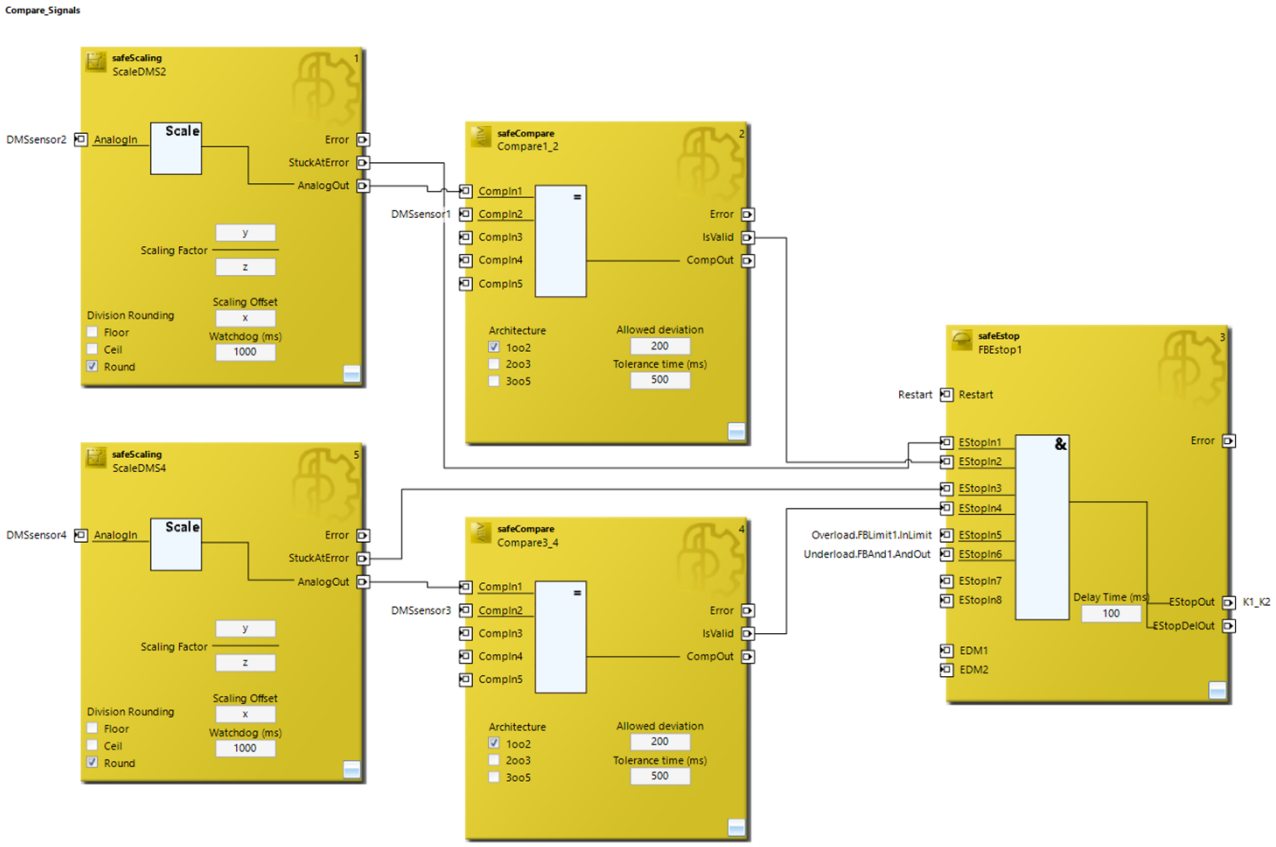
8.6.4 逻辑内部结构

EL6910 中的逻辑分为三个部分。在第一部分中，对 SG 值进行缩放和验证。该部分还包含通过 ESTOP 功能块实现的重启锁定及接触器 K1 与 K2 的关断控制。

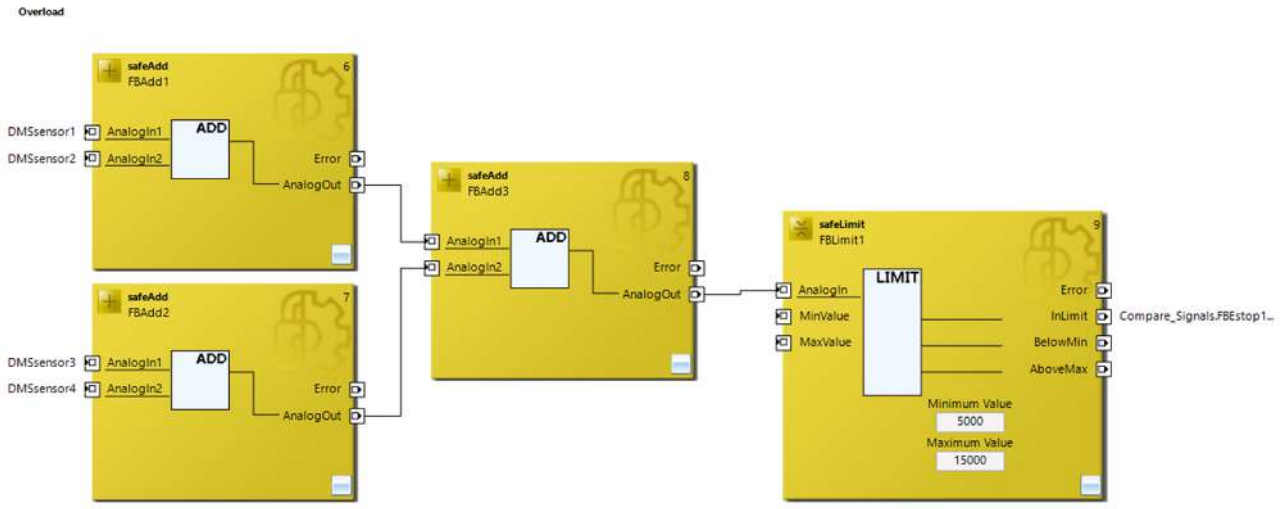
在第二部分中，通过 Limit 功能块计算总负载并监控其是否符合最大值与最小值要求。结果将被传送至第一部分的 ESTOP 功能块。

在第三部分中，监控每个独立信号是否符合最小值要求。这四个信号通过“与”运算后，连接至第一部分的 ESTOP 功能块。

第一部分


Compare_Signals
safeScaling
ScaleDMS2
1
DMSsensor2
AnalogIn
Scale
Error
StuckAtError
AnalogOut
Scaling Factor
y
z
Scaling Offset
x
Division Rounding
Floor
Ceil
Round
Watchdog (ms)
1000
safeCompare
Compare1_2
2
DMSsensor1
CompIn1
CompIn2
CompIn3
CompIn4
CompIn5
=
Error
IsValid
CompOut
Architecture
1oo2
2oo3
3oo5
Allowed deviation
200
Tolerance time (ms)
500
safeEstop
FBEstop1
3
Restart
EStopIn1
EStopIn2
EStopIn3
EStopIn4
EStopIn5
EStopIn6
EStopIn7
EStopIn8
&
Error
Overload.FBLimit1.InLimit
Underload.FBAnd1.AndOut
Delay Time (ms)
100
EStopOut
EStopDelOut
K1_K2
EDM1
EDM2
safeScaling
ScaleDMS4
5
DMSsensor4
safeCompare
Compare3_4
4
DMSsensor3

第二部分


Overload
safeAdd
FBAdd1
6
DMSsensor1
DMSsensor2
AnalogIn1
AnalogIn2
ADD
Error
AnalogOut
safeAdd
FBAdd2
7
DMSsensor3
DMSsensor4
safeAdd
FBAdd3
8
safeLimit
FBLimit1
9
AnalogIn
MinValue
MaxValue
LIMIT
InLimit
BelowMin
AboveMax
Minimum Value
5000
Maximum Value
15000
Compare_Signals.FBEstop1...

第三部分

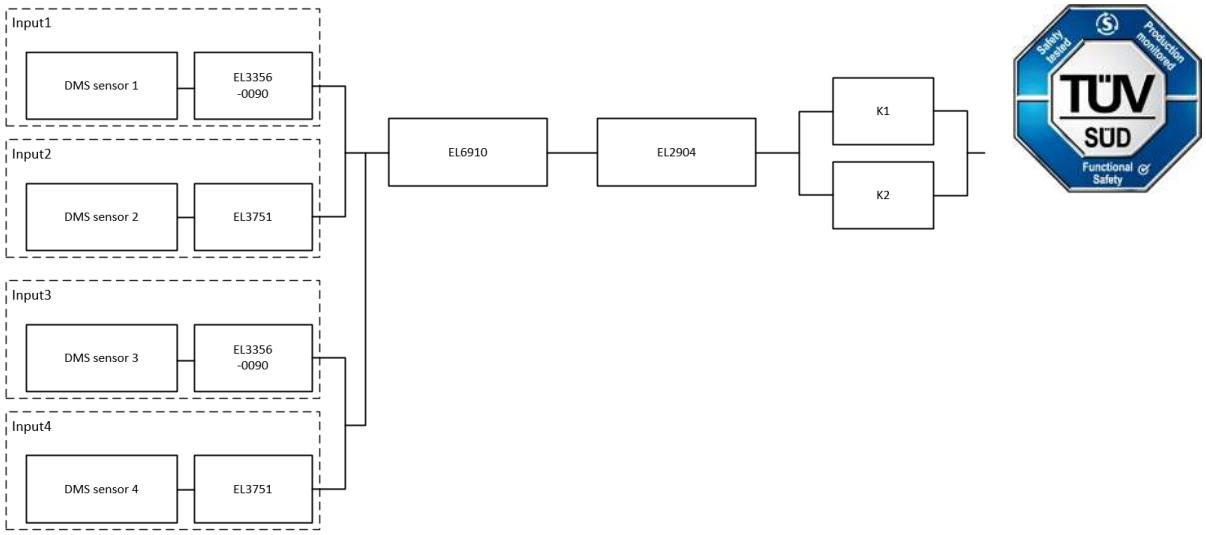
8.6.5 安全输出端子模块的参数

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	是

8.6.6 功能块结构和安全回路

8.6.6.1 安全功能 1/2



8.6.7 计算

8.6.7.1 PFHD / MTTFD / B10D – 值

组件	值
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
SG 传感器 1-4 – $MTTF_D$ （AST 3570951.1 CAL/10t/D50d11/L205/1.5 mV/V）	160 y（1,401,600 h）
EL3356-0090 - MTBF	780,733 h
EL3751 - MTBF	513,333 h
K1 – $B10_D$	1,300,000 h
K2 – $B10_D$	1,300,000 h
编码器 MTBF	107.5 y（914,700 h）
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

8.6.7.2 诊断覆盖率 DC

组件	值
通过 TwinSAFE SC 传输的 SG 值以及逻辑内的合理性检查	DC_{avg}=90%（计算中替代值：99%）
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

8.6.7.3 安全功能 1/2 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN 13849 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

根据 MTBF 值计算 PFH_D 和 $MTTF_D$ 值：

注：维修时间可以忽略不计，因此以下内容适用：

$$MTTF_D = 2 * MTBF$$

$$MTTF_D = \frac{1}{\lambda_D}$$

及

$$\lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

SG 传感器 1

$$MTTF_D = 1.401.600h = 160y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.401.600h} = 7{,}13E - 08$$

EL3356-0090

$$MTTF_D = 2 * MTBF = 2 * 780.733h = 1.561.466h = 178y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.561.466h} = 6{,}40E - 08$$

输入系统 1

$$PFH_{(Input1)} = PFH_{(DMS1)} + PFH_{(EL3356-0090)} = 7{,}13E - 08 + 6{,}40E - 08 = 13{,}53E - 08$$

SG 传感器 2

$$MTTF_D = 1.401.600h = 160y$$

$$PFH = \frac{1 - DC}{MTTF_D} = \frac{1 - 0{,}9}{1.401.600h} = 7{,}13E - 08$$

EL3751

$$MTTF_D = 2 * MTBF = 2 * 513.333h = 1.026.666h = 117y$$

$$PFH = \frac{1-DC}{MTTF_D} = \frac{1-0,9}{1.026.666h} = 9,74E-08$$

输入系统 2

$$PFH_{(Input2)} = PFH_{(DMS2)} + PFH_{(EL3751)} = 7,13E-08 + 9,74E-08 = 16,87E-08$$

对于输入系统 3，输入系统 1 的计算值适用。对于输入系统 4，输入系统 2 的计算值适用。

K1/K2：

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1*21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接反馈

$$PFH = \frac{1-0,99}{593607,3*8760} = 1,92E-12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

来自带 EL3356-0090 的 SG 传感器 1 与带 EL3751 的 SG 传感器 2 的输入信号采用不同的内部结构，提供不同的值（重量值和 mV/V 值），且均参与安全功能的实现。通道故障不会导致危险情况，但会通过比较 TwinSAFE 逻辑中的两个值被检测到，并导致关断。SG 传感器 3 和 4 采用相同的配置。四个传感器的数值总和为触发过载关停的重量值。如果任一 SG 传感器的值低于最小负载值，则会触发松绳关停功能。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输入子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 / 2 的 PFH_D 值计算如下

$$PFH_{(DMS1/2)} = \beta * \frac{PFH_{(Input1)} + PFH_{(Input2)}}{2} + (1-\beta)^2 * (PFH_{(Input1)} * PFH_{(Input2)}) * T1$$

$$= 10\% * \frac{13,53E-08 + 16,87E-08}{2} = 1,52E-08$$

$$PFH_{(DMS3/4)} = \beta * \frac{PFH_{(Input3)} + PFH_{(Input4)}}{2} + (1-\beta)^2 * (PFH_{(Input3)} * PFH_{(Input4)}) * T1$$

$$= 10\% * \frac{13,53E-08 + 16,87E-08}{2} = 1,52E-08$$

$$PFH_{(K1/K2)} = \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

$$= 10\% * \frac{1,92E-12 + 1,92E-12}{2} = 1,92E-13$$

由于 $(1-\beta)^2 * (PFH_{(x)} * PFH_{(y)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

$$PFH_{ges} = PFH_{(DMS1/2)} + PFH_{(DMS3/4)} + PFH_{(EL6910)} + PFH_{(EL2904)} + PFH_{(K1/K2)}$$
$$= 1,52E-08 + 1,52E-08 + 1,79E-09 + 1,25E-09 + 1,92E-13$$
$$= 3,344E-08$$

注意

EN 62061

根据 EN 62061 标准，输入子系统需以 90% 的 SFF 或 DC 值进行评估。根据 EN 62061 表 5，这将系统可实现的最大 SIL 值限制为 2。

根据 EN 13849 标准，安全功能 1 / 2 的 $MTTF_D$ 值的替代计算（在相同假设条件下）

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

较低值取自输入子系统：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(DMSsensor2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0,99)}{1,79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,99)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593.607y}} = 57,26y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}} + \frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(DMS1)}} + \frac{DC}{MTTF_{D(EL3356)}} + \frac{DC}{MTTF_{D(DMS2)}} + \frac{DC}{MTTF_{D(EL3751)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}} + \frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(DMS1)}} + \frac{1}{MTTF_{D(EL3356)}} + \frac{1}{MTTF_{D(DMS2)}} + \frac{1}{MTTF_{D(EL3751)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

采用 DC=90% 进行计算

$$DC_{avg} = \frac{\frac{90\%}{160y} + \frac{90\%}{178y} + \frac{90\%}{160y} + \frac{90\%}{117y} + \frac{90\%}{160y} + \frac{90\%}{178y} + \frac{90\%}{160y} + \frac{90\%}{117y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}}$$
$$= 90,42\%$$

或采用 DC = 99% 进行计算

$$DC_{avg} = \frac{\frac{99\%}{160y} + \frac{99\%}{178y} + \frac{99\%}{160y} + \frac{99\%}{117y} + \frac{99\%}{160y} + \frac{99\%}{178y} + \frac{99\%}{160y} + \frac{99\%}{117y} + \frac{99\%}{637y} + \frac{99\%}{913y} + \frac{99\%}{593607y} + \frac{99\%}{593607y}}{\frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{160y} + \frac{1}{178y} + \frac{1}{160y} + \frac{1}{117y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y} + \frac{1}{593607y}}$$
$$= 99,00\%$$

⚠ 谨慎

类别

这种结构最多能达到类别 3。

输入子系统采用 DC = 90% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

或输入子系统采用 DC = 99% 进行计算

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

注意

结果

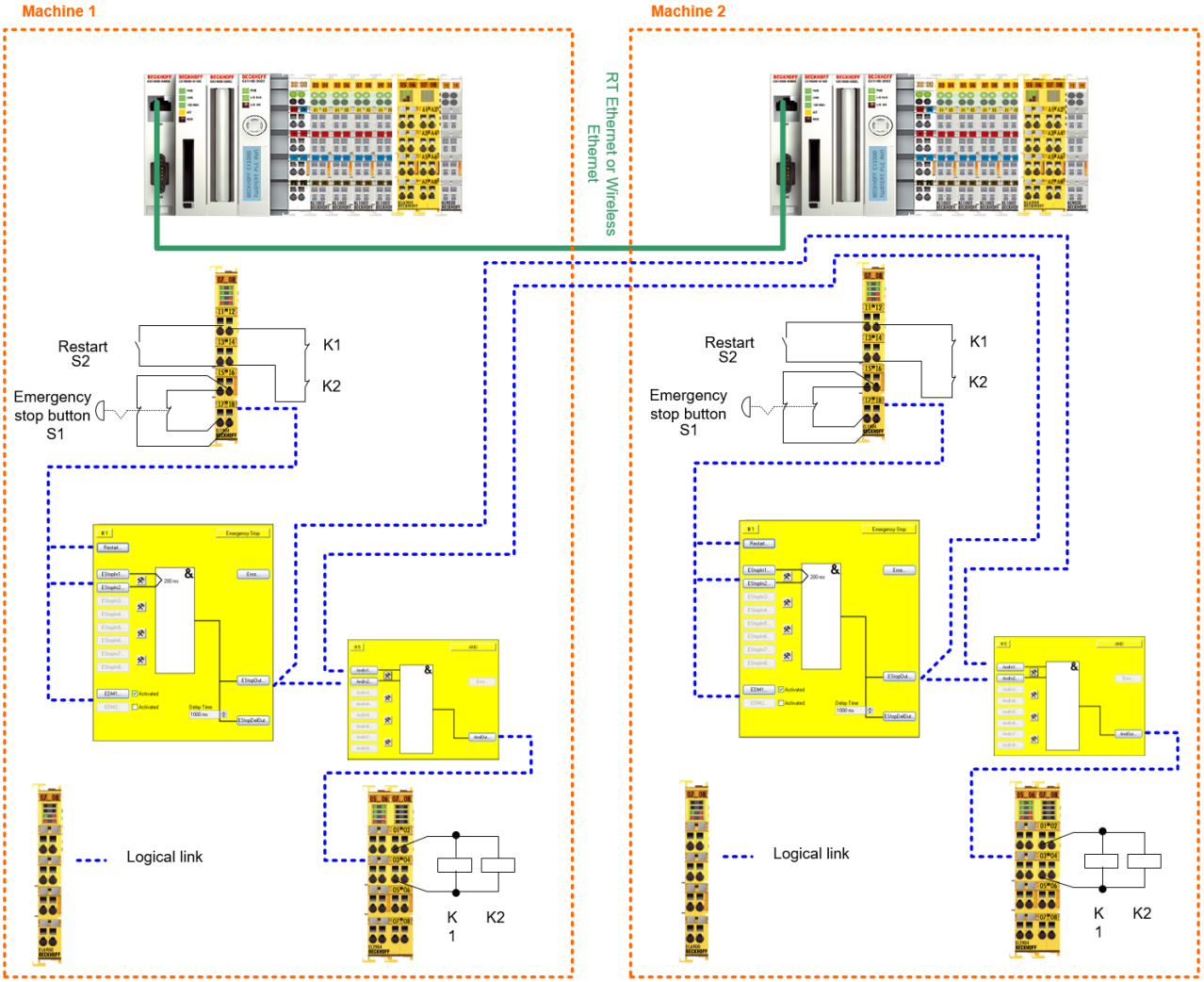
类别 3，PL d 的结果达到或超过了风险与危害分析的要求（PL c）。

9 特定应用场景

9.1 网络化系统（类别 4，PL e）

此处有 2 台设备通过以太网连接。该路径也可以通过无线以太网连接实现。只有在另一台设备未发出急停信号时，每个站点才会接通输出 K1 / K2。来自急停按钮、重启和反馈回路的信号连接至安全输入。ESTOP 功能块的输出连接至 AND 功能块，并通过网络向相应的其他设备发出信号。相应的其他设备的 ESTOP 输出连接至 AND 功能块，AND 门的输出随后会切换安全输出端子模块上的接触器。

启动了对输入信号的测试和差异检查。输出测试也已激活。



注意

启动/重启

如果一台设备配备多个操作站，必须采取相应措施，确保不同操作站发出的指令不会引发危险情况。

注意

接触器监控

如果风险与危害分析结果表明，在切换相应远程控制器的接触器时需要进行接触器检查，则应使用 EDM 功能块进行检查。

9.1.1 安全输入和输出端子模块的参数

EL1904（适用于所有使用的 EL1904）

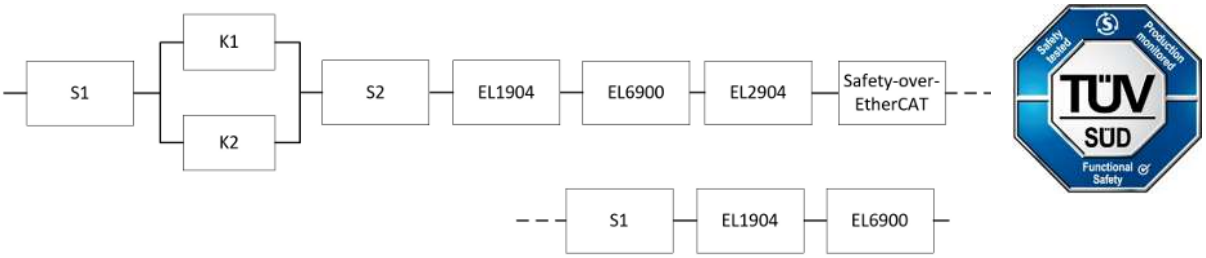
参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

9.1.2 功能块结构和安全回路

9.1.2.1 安全功能 1



9.1.3 计算

9.1.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
EL6900 – PFH_D	1.03E-09
Safety over EtherCAT（FSoE） – PFH_D	1.00E-09
S1 – $B10_D$	1,000,000
S2 – $B10_D$	2,000,000
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	15（每小时 4 次）
使用寿命（T1）	20 年 = 175200 小时

9.1.3.2 诊断覆盖率 DC

组件	值
带测试/合理性检查的 S1	DC_{avg}=99%
带合理性检查的 S2	DC_{avg}=90%
带测试和 EDM 的 K1/K2 （每班次执行 1 次）	DC_{avg}=99%

9.1.3.3 安全功能 1 的计算

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.000.000}{0{,}1 * 7360} = 1358{,}7y = 11902212h$$

S2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{2.000.000}{0{,}1 * 7360} = 2717{,}4y = 23804424h$$

K1/K2：

$$n_{op} = \frac{230 * 8 * 60}{15} = 7360$$

$$MTTF_D = \frac{1.300.000}{0{,}1 * 7360} = 1766{,}3y = 15472788h$$

并假设 S1、S2、K1 和 K2 均为单通道：

$$MTTF_D = \frac{1}{\lambda_D}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

S1：

$$PFH = \frac{1 - 0{,}99}{1358{,}7 * 8760} = 8{,}40E - 10$$

S2：

$$PFH = \frac{1-0,90}{2717,4*8760} = 4,20E-09$$

K1/K2：每班次执行 1 次，直接反馈

$$PFH = \frac{1-0,99}{1766,3*8760} = 6,46E-10$$

现在必须做出以下假设：

安全开关 S1：根据 BGIA 报告 2/2008，如果制造商已确认，则可排除高达 100000 次循环的故障。如果没有确认，则 S1 需按以下方式纳入计算。

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(S1)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1 + PFH_{(S2)} + PFH_{(EL1904)} + PFH_{(EL6900)} + PFH_{(EL2904)} + PFH_{(FSoE)} + PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6900)}$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

至：

$$PFH_{ges} = 8,40E-10 + 10\% * \frac{6,46E-10 + 6,46E-10}{2} + 4,20E-09 + 1,11E-09 + 1,03E-09 + 1,25E-09 + 1,00E-09 + 8,40E-10 + 1,11E-09 + 1,03E-09 = 1,25E-08$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(S2)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(FSoE)}} + \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6900)}}$$

及：

$$MTTF_{D(S1)} = \frac{B10_{D(S1)}}{0,1 * n_{op}}$$

$$MTTF_{D(S2)} = \frac{B10_{D(S2)}}{0,1 * n_{op}}$$

$$MTTF_{D(K1)} = \frac{B10_{D(K1)}}{0,1 * n_{op}}$$

如果仅有 EL1904、EL2904 和 EL6900 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1-DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6900)} = \frac{(1-DC_{(EL6900)})}{PFH_{(EL6900)}} = \frac{(1-0,99)}{1,03E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,02E-06\frac{1}{y}} = 1108,6y$$

$$MTTF_{D(EL2904)} = \frac{(1-DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1-0,99)}{1,25E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{1,1E-05\frac{1}{y}} = 913,2y$$

$$MTTF_{D(FSoE)} = \frac{(1-DC_{(FSoE)})}{PFH_{(FSoE)}} = \frac{(1-0,99)}{1,00E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{8,76E-06\frac{1}{y}} = 1141,6y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{1358,7y}+\frac{1}{1766,3y}+\frac{1}{2717,4y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{1141,6y}+\frac{1}{1358,7y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}} = 123,1y$$

$$DC_{avg} = \frac{\frac{99\%}{1358,7y}+\frac{99\%}{1766,3y}+\frac{99\%}{1766,3y}+\frac{90\%}{2717,4y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}+\frac{99\%}{913,2y}+\frac{99\%}{1141,6y}+\frac{99\%}{1358,7y}+\frac{99\%}{1028,8y}+\frac{99\%}{1108,6y}}{\frac{1}{1358,7y}+\frac{1}{1766,3y}+\frac{1}{1766,3y}+\frac{1}{2717,4y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}+\frac{1}{913,2y}+\frac{1}{1141,6y}+\frac{1}{1358,7y}+\frac{1}{1028,8y}+\frac{1}{1108,6y}} = 98,99\%$$

注意

类别

这种结构最多能达到类别 4。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

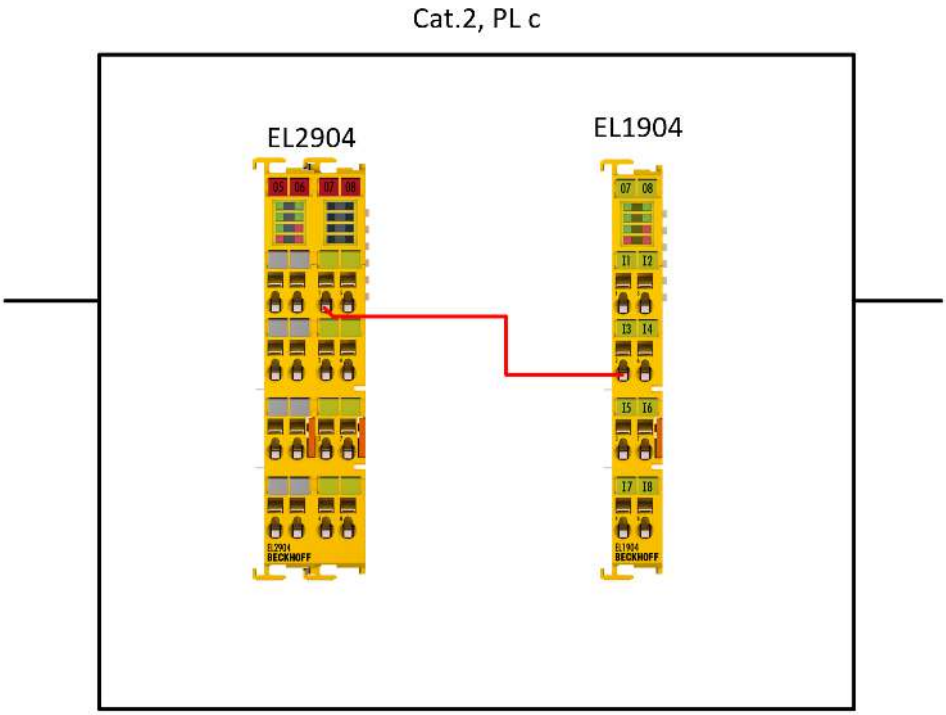
Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.2 TwinSAFE 输出与 TwinSAFE 输入的直接接线（单通道）（类别 2，PL c）

EL2904 的输出直接连接至 EL1904 的安全输入；这将禁用输出的测试脉冲和电流测量以及输入的传感器测试。这意味着线路上的交叉短路与外部馈电无法进行周期性测试。

鉴于 EL2904 和 EL1904 具备高级内部诊断功能，在外部仅采用单通道结构的情况下，两者应作为独立组件被评定为类别 2、SIL2 和 PL d。根据 DIN EN ISO 13849-1:2016-06 标准第 6.2.5 章，输出与输入的整体性能等级最高应评定为 PL c。

类别 2 所需的测试设置已集成在 EL2904 中。当 EL2904 输出接通时，系统会执行检测，以确认是否实际读回 24 V 电压。当断开输出时，系统会执行检测，以确认是否实际读回 0 V 电压。如果检测到错误，EL2904 将会进入错误状态，并向上级安全控制器发送信号。EL2904 的这种模块错误必须在设备控制器中进行评估。为此，在与 EL2904 的连接中必须启用 *ModuleFault is ComError* 参数，因此，如果发生模块错误，TwinSAFE 组将会切换至安全状态，并发出 ComError 信号。



9.2.1 安全输入和输出端子模块的参数

EL1904

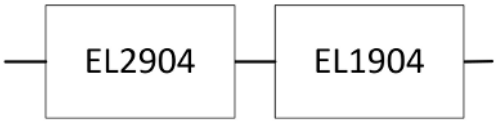
参数	值
传感器测试通道 1 激活	否
传感器测试通道 2 激活	否
传感器测试通道 3 激活	否
传感器测试通道 4 激活	否
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	否

9.2.2 功能块结构和安全回路

9.2.2.1 安全功能 1



9.2.3 计算

9.2.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	60（每小时 1 次）
使用寿命（T1）	20 年 = 175200 小时

9.2.3.2 诊断覆盖率 DC

组件	值
EL1904/EL2904 由于端子模块具备内部诊断功能（例如监测现场电压、温度等），并且 EL2904 在每次信号状态变化时都会检查切换输出的正确性	DC_{avg}=60%

9.2.3.3 安全功能 1 的计算

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(EL1904)} + PFH_{(EL2904)}$$

至：

$$PFH_{ges} = 1{,}11E-09 + 1{,}25E-09 = 2{,}36E-09$$

安全功能 1 的 $MTTF_D$ 值计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL2904)}}$$

如果仅有 EL1904 和 EL2904 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0,60)}{1,11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,4}{9,72E-06\frac{1}{y}} = 41152y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0,60)}{1,25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0,4}{1,1E-05\frac{1}{y}} = 36364y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{41152y} + \frac{1}{36364y}} = 19305y$$

$$DC_{avg} = \frac{\frac{60\%}{41152y} + \frac{60\%}{36364y}}{\frac{1}{41152y} + \frac{1}{36364y}} = 60\%$$

注意

类别

这种结构最多能达到类别 2。

⚠ 谨慎

实现安全等级

为了实现安全等级，用户必须确保在其应用中执行接线测试，且该测试的频率需达到安全功能调用次数的 100 倍以上。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	**60% ⩽ DC < 90%**
中等	90% ⩽ DC < 99%
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.3 TwinSAFE 输出与 TwinSAFE 输入的直接接线（双通道）（类别 3，PL d）

EL2904 的两个输出直接连接至 EL1904 的两个安全输入；这将禁用输出的测试脉冲和电流测量以及输入的传感器测试。在输入侧，两个信号在 TwinSAFE 逻辑中进行差异检查。因此，系统会检查两个信号的值，但在电缆上没有激活测试功能，这样在切换输出时能够检测到可能的外部馈电。

9.3.1 安全输入和输出端子模块的参数

EL1904

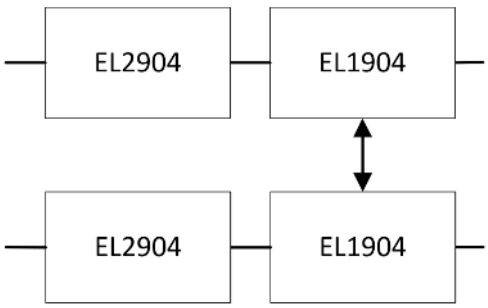
参数	值
传感器测试通道 1 激活	否
传感器测试通道 2 激活	否
传感器测试通道 3 激活	否
传感器测试通道 4 激活	否
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

EL2904

参数	值
电流测量激活	否
输出测试脉冲激活	否

9.3.2 功能块结构和安全回路

9.3.2.1 安全功能 1



9.3.3 计算

9.3.3.1 PFHD / MTTFD / B10D – 值

组件	值
EL1904 – PFH_D	1.11E-09
EL2904 – PFH_D	1.25E-09
运行天数（d_{op}）	230

组件	值
运行小时数/天（h_{op}）	8
循环时间（分钟）（T_{cycle}）	60（每小时 1 次）
使用寿命（T1）	20 年 = 175200 小时

9.3.3.2 诊断覆盖率 DC

组件	值
EL1904/EL2904	DC_{avg}=90%

9.3.3.3 安全功能 1 的计算

由此，安全功能 1 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(EL1904)} + PFH_{(EL2904)}$$

至：

$$PFH_{ges} = 1{,}11E-09 + 1{,}25E-09 = 2{,}36E-09$$

安全功能 1 的 $MTTF_D$ 值计算（在相同假设条件下）：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

公式为：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL2904)}}$$

如果仅有 EL1904 和 EL2904 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{D(ELxxxx)} = \frac{(1 - DC_{(ELxxxx)})}{PFH_{(ELxxxx)}}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1 - DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1 - 0{,}90)}{1{,}11E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{9{,}72E-06\frac{1}{y}} = 10288{,}1y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}90)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}1}{1{,}1E-05\frac{1}{y}} = 9090{,}9y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{10288{,}1y} + \frac{1}{9090{,}9y}} = 4826{,}3y$$

$$DC_{avg} = \frac{\frac{90\%}{10288{,}1y} + \frac{90\%}{10288{,}1y} + \frac{90\%}{9090{,}9y} + \frac{90\%}{9090{,}9y}}{\frac{1}{10288{,}1y} + \frac{1}{10288{,}1y} + \frac{1}{9090{,}9y} + \frac{1}{9090{,}9y}} = 90\%$$

注意

类别

这种结构最多能达到类别 3。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

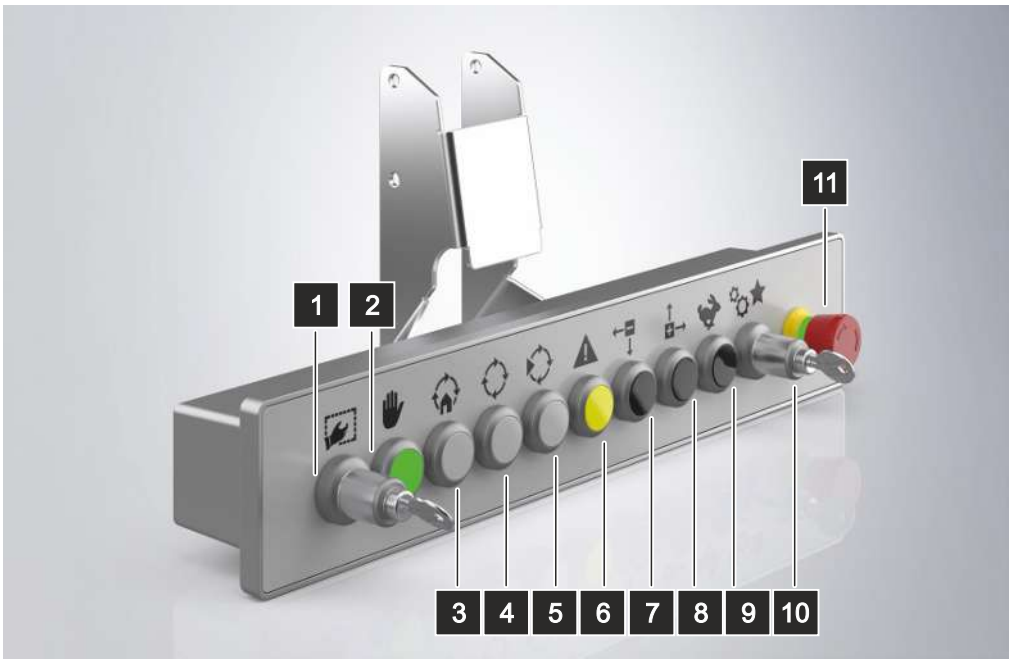
为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.4 应用示例 C9900-M800

9.4.1 描述 C9900-M800

C9900-M800 产品是倍福控制面板的按钮扩展单元。相关按钮（请参见下表）通过安全组件（FB6901-1918，请参见 Z10 62386 037 修订版 1）进行读入。然后，这些信号由 FB6901-1918 安全组件打包成 PROFIsafe 报文，并通过按钮扩展单元上的标准控制器传输到 PROFINET 接口。



按钮	描述	PROFIsafe 信号	信号 FB6901-1918
1（SW700）	标准	-	-
2（SW701）	标准	-	-
3（SW702）	标准	-	-
4（SW703）	标准	-	-
5（SW704）	标准	-	-
6（SW705.2）	黄色带灯按钮 （1 个常开触点）	PROFIsafe_2B[0].4	SW705_SafeIn2
7（SW706）	标准	-	-
8（SW707）	标准	-	-
9（SW708）	标准	-	-
10 （SW709.1/.2）	钥匙开关 SSG10， 左侧非锁定，右侧 锁定 （2 个常开触点）	PROFIsafe_2B[0].2 PROFIsafe_2B[0].3	SW709_SafeIn4 SW709_SafeIn3
11 （SW710.1/.2）	急停按钮 （2 个常闭触点）	PROFIsafe_2B[0].0 PROFIsafe_2B[0].1	SW710_SafeIn1 SW710_SafeIn5

	其他 PROFIsafe 信号		
	ModuleFault_SafeIn1_2	PROFIsafe_2B[0].5	FSIN Module1.Module Fault
	ModuleFault_SafeIn3_4	PROFIsafe_2B[0].6	FSIN Module2.Module Fault
	ModuleFault_SafeIn5	PROFIsafe_2B[0].7	FSIN Module3.Module Fault
	ModuleFault_ErrAck	PROFIsafe_1B[0].0	FSIN Module1.Err Ack FSIN Module2.Err Ack

	其他 PROFIsafe 信号		
			FSIN Module3.Err Ack

9.4.2 计算

9.4.2.1 基本信息

按钮和开关信号由 FB6901-1918 作为单通道信号读入，在通过 SIL 3 认证的 FB6901-1918 内部进行处理，并传输到 PROFIsafe 报文中。因此，安全相关参数的计算从按钮开始，一直到传输至安全协议。为了在上级安全控制器中执行进一步评估，需建立假设条件并基于这些条件开展替代计算。因此，除安全子功能 3 外，所有示例均为 Cat.2 功能。

9.4.2.2 参数 FB6901-1918

参数	值
使用寿命 [a]	20
验证测试间隔 [a]	无需配置
PFHD	3.4 E-09
PFDavg	5.1E-05
MTTFD	1780 a
DC	97.5%（CAT4）
性能等级	PL e
类别	4
SFF	>99%
HFT	1
元件分类	B 型
总线通信残余错误率	1E-09

总线通信的残余错误率 1E-09（SIL 3 的 1%）已在 FB6901-1918 的特性中予以考虑，因此无需在后续计算中再次纳入。

9.4.2.3 按钮 SW710 参数

参数	操作元件	开关元件
使用寿命	50,000 次循环	1,000,000 次循环
B10	65,000 次循环	1,300,000 次循环
$B10_D$	130,000 次循环	2,600,000 次循环
操作频次 / [a] (n_{op})	12	
版本	2 个常闭触点	

开关元件的关键数据远大于操作元件的关键数据，因此这里使用较差的值进行计算。

⚠ 警告

验证值

操作频次是基于客户侧所做的假设。该值必须进行验证，并由客户在安全功能的最终计算阶段做出必要调整。

9.4.2.4 按钮 SW709 参数

参数	操作元件	开关元件
使用寿命	50,000 次循环	1,000,000 次循环
B10	71,660 次循环	1,300,000 次循环
$B10_D$	-	-
操作频次 / [a] (n_{op})	52	
版本	2 个常开触点	

开关元件的关键数据远大于操作元件的关键数据，因此这里使用较差的值进行计算。

⚠ 警告

验证值

操作频次是基于客户侧所做的假设。该值必须进行验证，并由客户在安全功能的最终计算阶段做出必要调整。

9.4.2.5 按钮 SW705 参数

参数	操作元件	开关元件
使用寿命	1,000,000 次循环	1,000,000 次循环
B10	1,300,000 次循环	1,300,000 次循环
$B10_D$	-	-
操作频次 / [a] (n_{op})	8760	
版本	1 个常开触点	

开关元件的关键数据均相同，因此采用哪个值并无影响。

⚠ 警告

验证值

操作频次是基于客户侧所做的假设。该值必须进行验证，并由客户在安全功能的最终计算阶段做出必要调整。

9.4.2.6 FB6910-1918 的参数

索引	描述	值
80x0:01	诊断测试脉冲模数	0x00
80x0:02	诊断测试脉冲倍数	0x01
80x0:04	诊断测试脉冲激活	TRUE
80x0:05	模块故障链路激活	TRUE
80x1:01	通道 1. 输入滤波时间	0x0014 (20) x 0.1 毫秒
80x1:02	通道 1. 诊断测试脉冲滤波时间	0x0002 (2) x 0.1 毫秒
80x1:04	通道 2. 输入滤波时间	0x0014 (20) x 0.1 毫秒
80x1:05	通道 2. 诊断测试脉冲滤波时间	0x0002 (2) x 0.1 毫秒

FB6901-1918 的参数保持默认设置。

所有通道的测试脉冲均处于启用状态，在发生故障时，通过模块故障链接激活参数将所有输入模块设置为模块故障状态。

9.4.2.7 诊断覆盖率 DC 的假设

组件	DC 值
SW710.1 通过测试脉冲对急停信号进行单通道评估 （类别 2 结构） 急停按钮被设计为常闭触点，因此可以通过周期性测试进行检查。因此，测试频率比安全功能的要求高出 100 倍以上。	90%
SW710.2 通过测试脉冲对急停信号进行单通道评估 （类别 2 结构） 说明详见 SW710.1	90%

急停按钮的替代方案	DC 值
对于 SW710.1 和 SW710.2，在上级安全控制器中执行带合理性检查的双通道评估 （类别 4 结构）	99%

单通道组件	DC 值
SW709.1 通过测试脉冲对按键开关（位置 1）进行单通道评估 （类别 2 结构） 在动作状态下，仅可通过测试脉冲检测常开触点的接线。在外壳内部可以实现开关与安全输入之间的连接，因此不会因外部影响而发生短路。由于 FB6901-1918 具备高级诊断功能，因此可以对电压、温度等环境条件进行监测，从而可以假定 DC 的值为 60%。 **警告 安全功能必须由用户进行定义，确保未接通状态为安全状态。**	60%
SW709.2 通过测试脉冲对按键开关（位置 2）进行单通道评估 （类别 2 结构） 原因和警告详见 SW709.1	60%
SW705.2 通过测试脉冲对复位按钮进行单通道评估 （类别 2 结构） 原因和警告详见 SW709.1 **注意 如果在上级控制器中对复位按钮的上升沿、下降沿及时间特性进行监控（上升沿和下降沿之间的间隔范围为 0.5 s - 5 s），则可假定 DC 值为 90%，而非 60%。**	60%

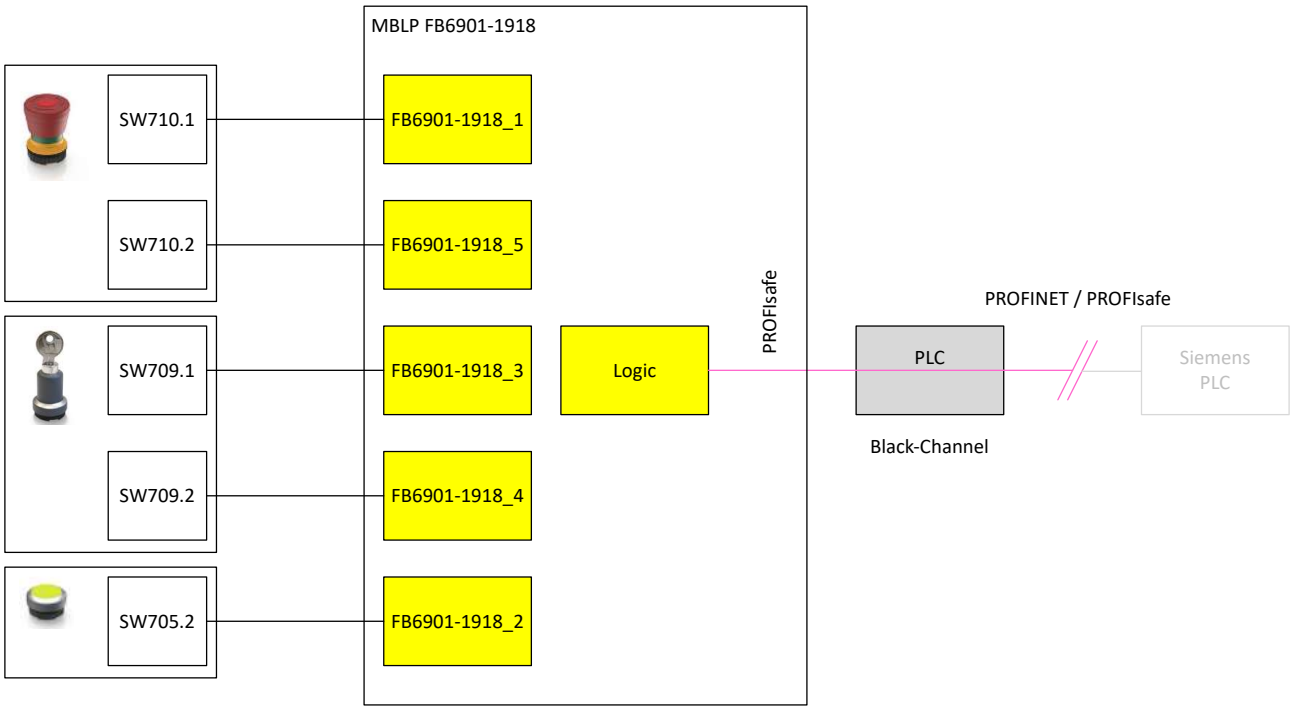
⚠ 警告

执行合理性检查和交叉比较

对于假定 DC 为 99% 的急停按钮替代计算，必须对上级安全控制器中 SW710 开关的两个信号执行合理性检查/交叉比较。

9.4.2.8 功能块结构和安全回路

9.4.2.8.1 概述



9.4.2.8.2 计算 MTTFD 和 PFHD 的通用公式

如果仅有一个 B10 值可用时的估算方法（请参见 DIN EN ISO 13849-1 表 C.1）：

$$B10_D = 2 * B10$$

每年操作频次：

$$n_{op} = Betätigungen\ pro\ Jahr$$

根据 B10D 推导 MTTFD：

$$MTTF_D = \frac{1}{\lambda_D}\ mit\ \lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 * n_{op}}{B10_D}$$

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

总 MTTFD 计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

$$MTTF_D = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}}$$

总 DC 计算：

$$DC_{avg} = \frac{\frac{DC_{SW7xx}}{MTTF_{D(SW7xx)}} + \frac{DC_{FB6901-1918}}{MTTF_{D(FB6901-1918)}}}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}}$$

根据 MTTFD 和 DC 计算 PFHD：

$$PFH_D = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

总 PFHD 计算（针对单通道结构）：

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)}$$

总 PFHD 计算（针对双通道结构）：

$$PFH_{Dges} = \beta * \frac{PFH_{D(SW710.1)} + PFH_{D(SW710.2)}}{2} + (1 - \beta)^2 * \left(PFH_{D(SW710.1)} * PFH_{D(SW710.2)}\right) * T_1 + PFH_{D(FB6901-1918)}$$

9.4.2.8.3 安全子功能 1/2（SW710.1 / SW710.2）

安全子功能 1/2 由急停按钮的单个通道（此处为 SW710.1 或 SW710.2）、FB6901-1918 以及 PROFIsafe 报文中的信号共同构成。

两个独立通道的计算方法相同，因此在此处只计算一次。

⚠ 警告

实施措施

客户必须对该框图进行扩展，以包括上级控制器和开关式执行器系统，以及反馈回路的监控和重启锁定的实施。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

计算 MTTFD 和 DC：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{130.000}{0{,}1 * 12} = 108.000\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{108.000} + \frac{1}{1.780}} = 1.751\ a$$

$$DC_{avg} = \frac{\frac{0{,}9}{108.000} + \frac{0{,}975}{1.780}}{\frac{1}{108.000} + \frac{1}{1.780}} = 0{,}973 = 97{,}3\%$$

计算 PFH：

$$PFH_D = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}9}{108.000} = 9{,}26E - 07$$

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)} = 9{,}26E - 07 + 3{,}4E - 09 = 9{,}30E - 07$$

⚠ 警告

在类别 2 中使用

该安全子功能的结构可在类别 2 中使用。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC_{avg}	
名称	**范围**

DC_{avg}	
无	DC < 60%
低	60% ⩽ DC < 90%
中	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.4.2.8.4 安全子功能 3（SW710.1 和 SW710.2）

安全子功能 3 由急停按钮的两个通道（此处为 SW710.1 和 SW710.2）、FB6901-1918 以及 PROFIsafe 报文中的 2 个信号共同构成。

⚠ 警告

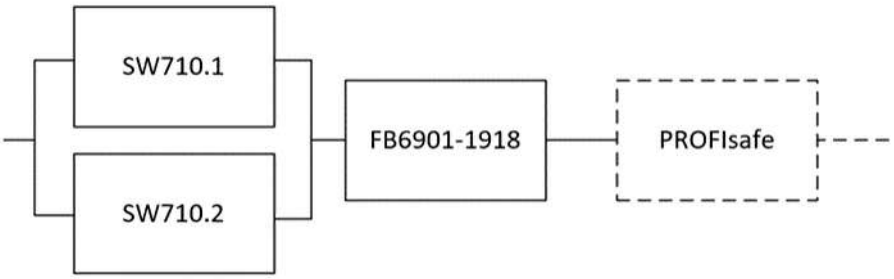
执行合理性检查并设置重启锁定

客户必须在上级安全控制器中对两个信号执行合理性检查，还须实现重启锁定功能

⚠ 警告

实施措施

客户必须对该框图进行扩展，以包括上级控制器和开关式执行器系统，以及反馈回路的监控和重启锁定的实施。



急停按钮的两个通道被设计为常闭触点，并通过测试脉冲进行测试。在上级控制器中对两个信号执行合理性检查。为了简化计算，两个值中的较差值可以用于该组合（另请参见 DIN EN ISO 13849-1:2016 的 D.2）。此处，本示例中的两个值相同。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

计算 MTTFD 和 DC：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{130.000}{0{,}1 * 12} = 108.000\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{108.000} + \frac{1}{1.780}} = 1.751\ a$$

$$DC_{avg} = \frac{\frac{0{,}99}{108.000} + \frac{0{,}975}{1.780}}{\frac{1}{108.000} + \frac{1}{1.780}} = 0{,}975 = 97{,}5\%$$

计算 PFH：

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 ß =10%。EN 62061 包含一个表格，可用于精确确定该 β 系数。此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

$$PFH_{D(SW710.1)} = \frac{(1-DC)}{MTTF_D} = \frac{1-0{,}99}{108.000} = 9{,}26E-08$$

$$PFH_{D(SW710.2)} = \frac{(1-DC)}{MTTF_D} = \frac{1-0{,}99}{108.000} = 9{,}26E-08$$

$$PFH_{Dges} = \beta * \frac{PFH_{D(SW710.1)} + PFH_{D(SW710.2)}}{2} + (1-\beta)^2 * \left(PFH_{D(SW710.1)} * PFH_{D(SW710.2)}\right) * T_1 + PFH_{D(FB6901-1918)}$$

由于 $(1-\beta)^2 * \left(PFH_{D(SW710.1)} * PFH_{D(SW710.2)}\right) * T_1$ 部分比其余部分小 10 倍，为了简化计算，在此项计算中均予以忽略。

$$PFH_{Dges} = \beta * \frac{PFH_{D(SW710.1)} + PFH_{D(SW710.2)}}{2} + PFH_{D(FB6901-1918)}$$

$$PFH_{Dges} = 10\% * \frac{9{,}26E-08 + 9{,}26E-08}{2} + 3{,}4E-09 = 12{,}66E-09 = 1{,}27E-08$$

⚠ 警告

最高适用至类别 4

该安全子功能的结构可在类别 4 中使用。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC_{avg}	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.4.2.8.5 安全子功能 4/5（SW709.1 和 SW709.2）

安全子功能 4 和 5 由钥匙开关的单个通道（此处为 SW709.1 或 SW709.2）、FB6901-1918 以及 PROFIsafe 报文中的信号共同构成。

两个独立通道的计算方法相同，因此在此处只计算一次。

⚠ 警告

实施措施

客户必须对该框图进行扩展，以包括上级控制器和开关式执行器系统，以及反馈回路的监控和重启锁定的实施。

⚠ 警告

保持安全状态

安全功能必须由用户进行定义，确保未接通状态为安全状态。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

计算 B10D：

$$B10_D = 2 * B10 = 2 * 71.660 = 143.320$$

计算 MTTFD 和 DC：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{143.320}{0{,}1 * 52} = 27.561\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{27.561} + \frac{1}{1.780}} = 1.672\ a$$

$$DC_{avg} = \frac{\frac{0{,}6}{27.561} + \frac{0{,}975}{1.780}}{\frac{1}{27.561} + \frac{1}{1.780}} = 0{,}9523 = 95{,}2\%$$

计算 PFH：

$$PFH_D = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}6}{27.561} = 1{,}45E-05$$

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)} = 1{,}45E-05 + 3{,}4E-09 = 1{,}45E-05$$

⚠ 警告

在类别 2 中使用

该安全子功能的结构可在类别 2 中使用。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ≤ $MTTF_D$ < 10 年

$MTTF_D$	
中	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC_{avg}	
名称	**范围**
无	DC < 60%
低	60% ⩽ DC < 90%
中	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

9.4.2.8.6 安全子功能 6（SW705.2）

安全子功能 6 由复位按钮的单个通道（此处为 SW705.2）、FB6901-1918 以及 PROFIsafe 报文中的信号共同构成。

⚠ 警告

实施措施

客户必须对该框图进行扩展，以包括上级控制器和开关式执行器系统，以及反馈回路的监控和重启锁定的实施。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

计算 B10D：

$$B10_D = 2 * B10 = 2 * 1.300.000 = 2.600.000$$

计算 MTTFD 和 DC：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}} = \frac{2.600.000}{0{,}1 * 8760} = 2.968\ a$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{MTTF_{D(SW7xx)}} + \frac{1}{MTTF_{D(FB6901-1918)}}} = \frac{1}{\frac{1}{2.968} + \frac{1}{1.780}} = 1.112\ a$$

注意

DC 值

如果在上级控制器中对复位按钮的上升沿、下降沿及时间特性进行监控（上升沿和下降沿之间的间隔范围为 0.5 s - 5 s），则可假定 DC 值为 90%，而非 60%。

$$DC_{avg} = \frac{\frac{0{,}6}{1.112} + \frac{0{,}975}{1.780}}{\frac{1}{1.112} + \frac{1}{1.780}} = 0{,}744 = 74{,}4\%$$

计算 PFH：

$$PFH_D = \frac{(1 - DC)}{MTTF_D} = \frac{1 - 0{,}6}{1.112} = 3{,}60E-04$$

$$PFH_{Dges} = PFH_{D(SW7xx)} + PFH_{D(FB6901-1918)} = 3{,}60E-04 + 3{,}4E-09 = 3{,}60E-04$$

⚠ 警告

在类别 2 中使用

该安全子功能的结构可在类别 2 中使用。

$MTTF_D$	
每个通道的标识	**每个通道的范围**

$MTTF_D$	
低	3 年 ⩽ $MTTF_D$ < 10 年
中	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC_{avg}	
名称	**范围**
无	DC < 60%
低	**60% ⩽ DC < 90%**
中	90% ⩽ DC < 99%
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

1 PROFIsafe 的连接
0

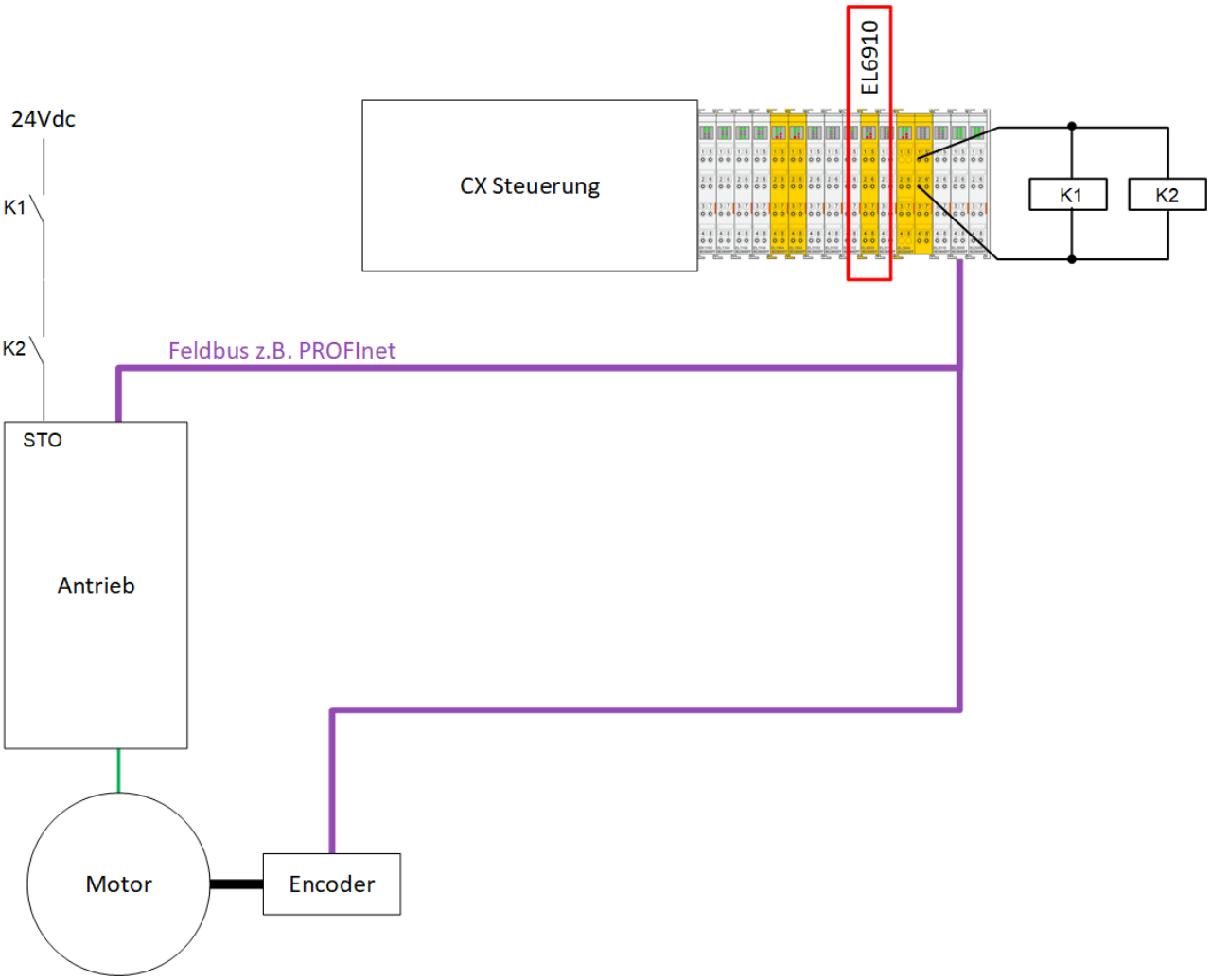
10.1 采用 PROFIsafe 编码器的安全速度监控（类别 4，PL e）

要监控驱动器的速度。该驱动器具有安全功能（在本示例中以 STO 为例），可通过相应的输入激活。该输入/这些输入通过两个接触器的常开触点进行连接。TR-Electronic 的安全型绝对值旋转编码器可用于安全测量速度。它已获得认证，适用于最高性能等级 e 的应用场景。借助于 PROFIsafe，安全相关数据通过 PROFInet 进行传输。速度数据通过安全相关协议 PROFIsafe 传输至作为 PROFIsafe 主站的 EL6910，并借助于可用的预认证模拟量值处理功能块在那里进行监控。

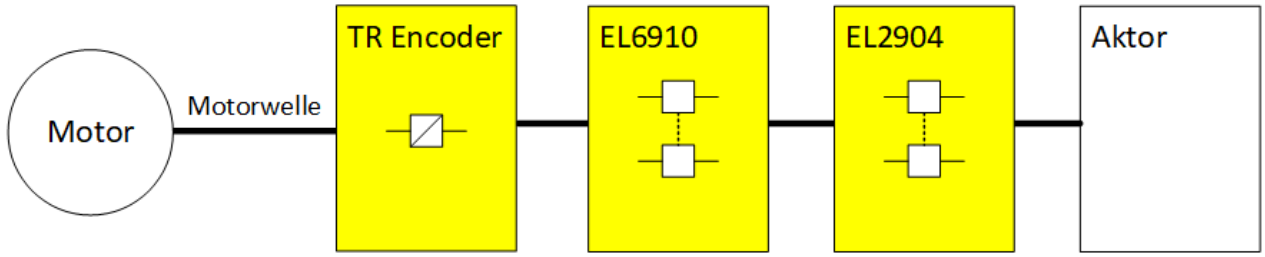
如果当前速度值低于 Limit FB 中指定的阈值，则 STO 输出将被设置为逻辑 1，驱动器可以运转。如果超过限值，则输出将被设置为逻辑 0，驱动器将切换为无转矩状态，或集成在驱动器中的安全功能将被激活。整个计算和调整均在安全相关 EL6910 逻辑中的安全水平 SIL3/PL e 上进行。

此外，ESTOP 功能块还实现了急停功能（为了降低复杂程度，未在图中显示），该功能块既能阻止重启，也能接管接触器 K1 和 K2 的控制。

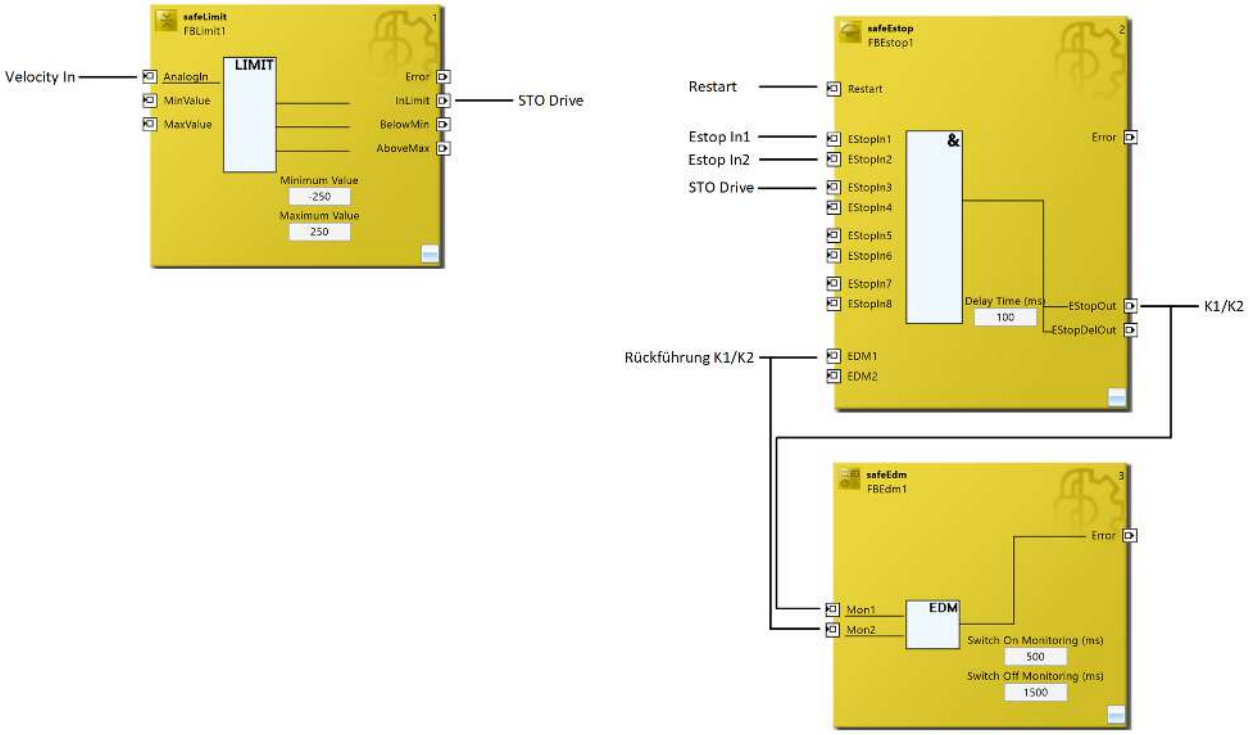
结构



结构图配置



逻辑



整个系统的正确配置

在 EtherCAT 内部传输 PROFIsafe 时需遵循以下限制。

PROFIsafe 报文仅通过 E-bus 和 PROFINET/PROFIBUS 传输

根据 PROFIsafe 规范，仅允许通过 PROFIBUS 和 PROFINET 现场总线或背板总线（例如，在本示例中为 E-bus）使用 PROFIsafe。由于专利法相关原因，禁止通过其他现场总线使用 PROFIsafe。

根据 PROFIsafe 规范，以下 Siemens AG 专利具有相关性：
- EP1267270-A2 数据传输方法
- WO00/045562-A1 确定数据载体可靠性的方法和设备
- WO99/049373-A1 自动化系统的短数据报文
- EP1686732 传输协议数据单元的方法和系统
- EP1802019 识别数据传输中的错误
- EP1921525-A1 安全相关系统的操作方法
- EP13172092.2 错误检测方法和系统

因此，必须根据应用程序的架构采取适当的措施。有关 PROFIsafe 的整个系统的正确配置详情，请参阅 EL6910 和 EL9930 的文档。

使用外部安全编码器

在使用外部编码器时，还必须满足其他要求。

⚠ 谨慎

使用外部安全编码器

在使用外部安全编码器时，必须始终遵循当前版本的文档说明。此处列出了所有关于装配、操作和维修的要求，您必须满足这些条件，才能在安全相关应用中正确使用编码器。

10.1.1 FMEA

错误假设	预期情况	已检查
速度值停滞	编码器中的速度经安全方式确定（性能等级 e），并通过 PROFIsafe 安全传输。通过安全通信协议的 Watchdog（看门狗）可检测到报文的停滞情况。	
速度值被伪造	编码器中的速度经安全方式确定（性能等级 e），并通过 PROFIsafe 安全传输。通过安全通信协议可检测到报文的伪造情况。	
电机与编码器之间已完全失去连接	可通过采用标准驱动信号的合理性检查检测到。因此，既可利用驱动器的标准速度进行合理性检查，也可借助驱动器是否应处于旋转状态的布尔信息进行验证。另外，也可将安全报文的位置信号用作功能块 safeScaling 的输入信号，以便借助输出 *StuckAtError* 来检测这种错误情况（例如，结合驱动器是否正在主动减速的信息）。 合理性检查：当电机启动时，预期也会产生动态速度值。	

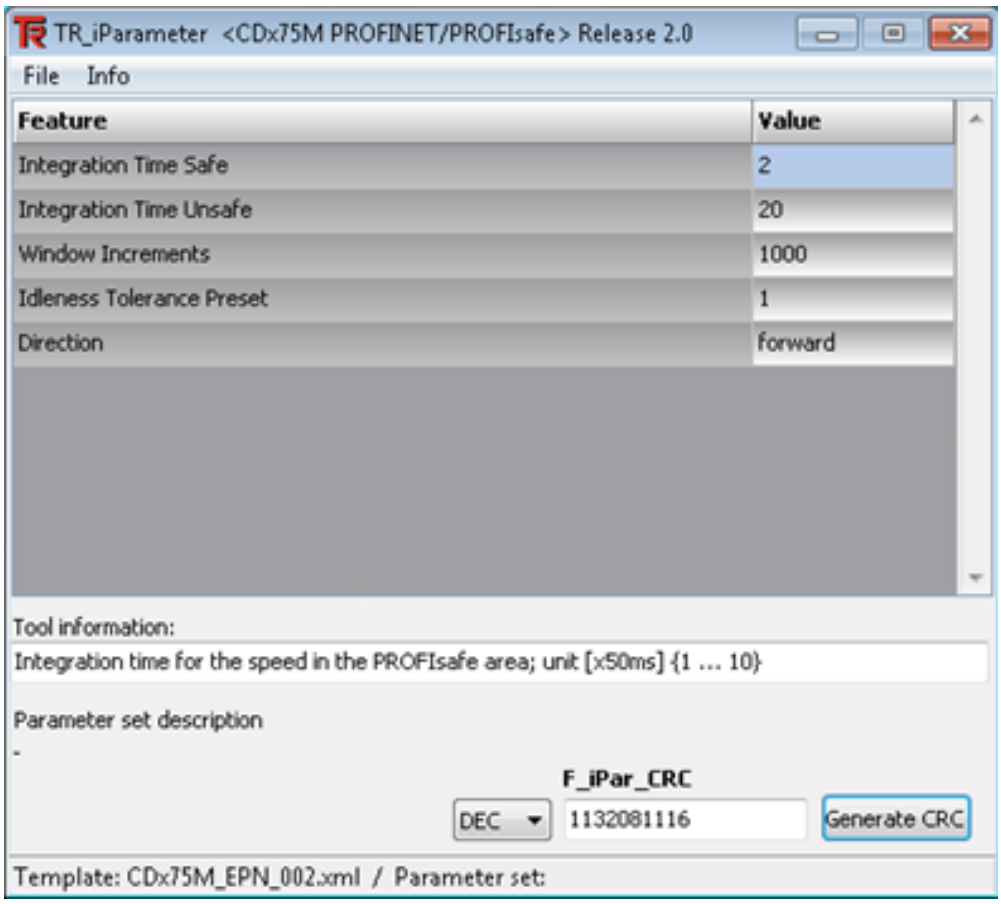
10.1.2 工程环境中的配置

除了连接 TwinSAFE 组件外，本应用示例还考虑了通过 PROFIsafe/PROFInet 连接编码器的附加方案。下文将详细介绍实施过程中所有必要的配置步骤。

为了配置编码器的安全相关参数，需要借助额外的应用程序对设备进行参数设置，并确定 iParameters 的 CRC 校验和，该校验和最终必须在 TwinCAT 中进行额外配置。

10.1.2.1 编码器配置

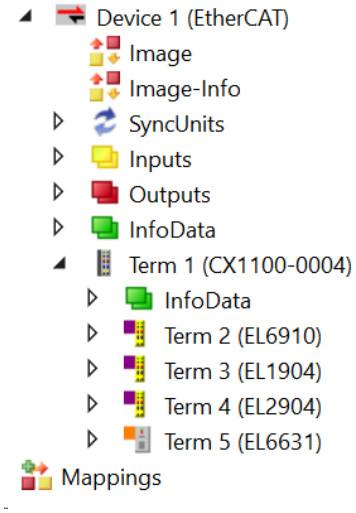
编码器的参数设置需要借助额外的应用程序。可从制造商网站获取当前版本。



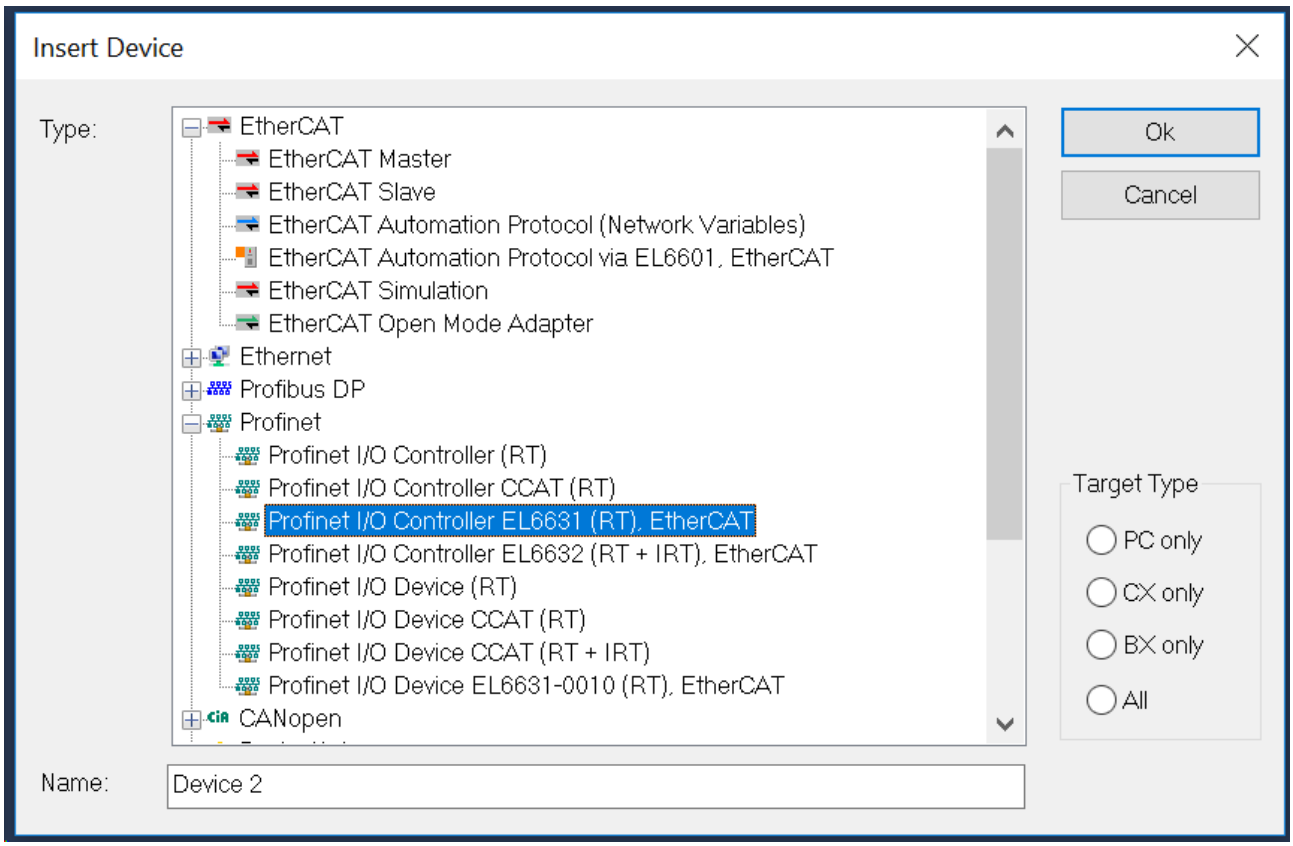
此处必须根据应用配置必要的参数，以便能够正确计算 CRC 校验和（图中为 **F_iPar_CRC** ）。

10.1.2.2 TwinCAT I/O 的配置

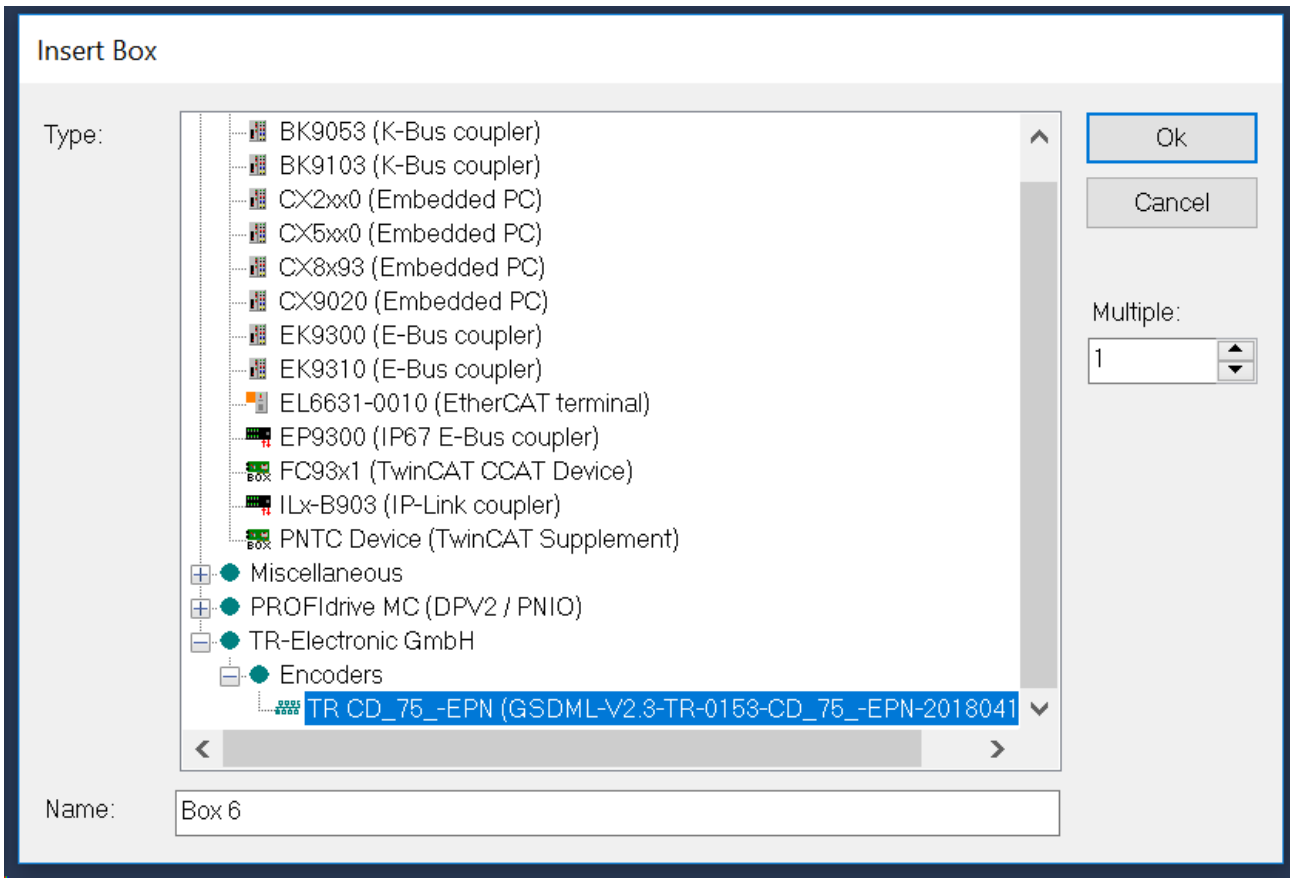
首先，创建一个新的 TwinCAT 项目并配置 EtherCAT 网段。



此外，通过添加一个 PROFInet I/O 控制器，可生成 PROFInet 网段的配置。



与 EtherCAT 网段的配置方式相同，PROFInet 控制器同样支持自动扫描或手动生成配置。通过这种方式，也可以手动添加编码器。



要通过 PROFIsafe 成功使用编码器，必须遵循以下信息说明。

⚠ 谨慎

数据类型 WORD!

当在过程映像中使用 WORD 数据类型时，可能需要进行额外配置。

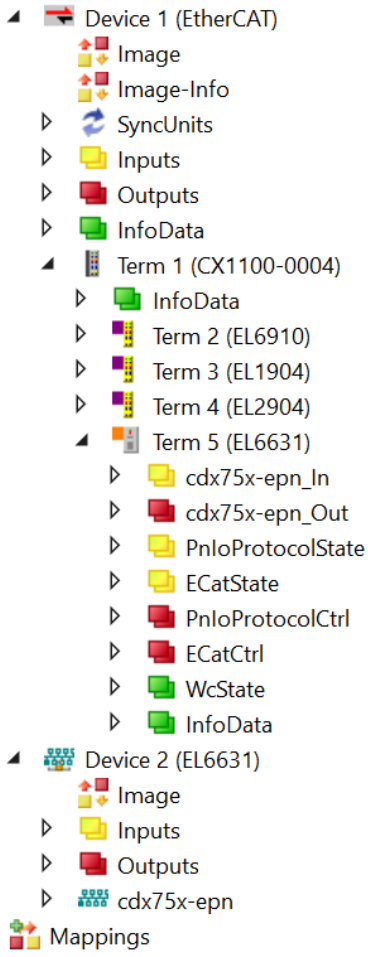
如果在配置中没有使用 EL9930 来限制 PROFIsafe 网段，则必须针对过程映像中包含 WORD 数据类型的信号，在 PROFIsafe 设备的 I/O 配置中配置高字节和低字节部分的交换。此操作可通过直接在数据值（在 *Flags*（标志）选项卡上）勾选 *Swap LOBYTE and HIBYTE*（交换 LOBYTE 和 HIBYTE）复选框来完成。

⚠ 谨慎

iParameters

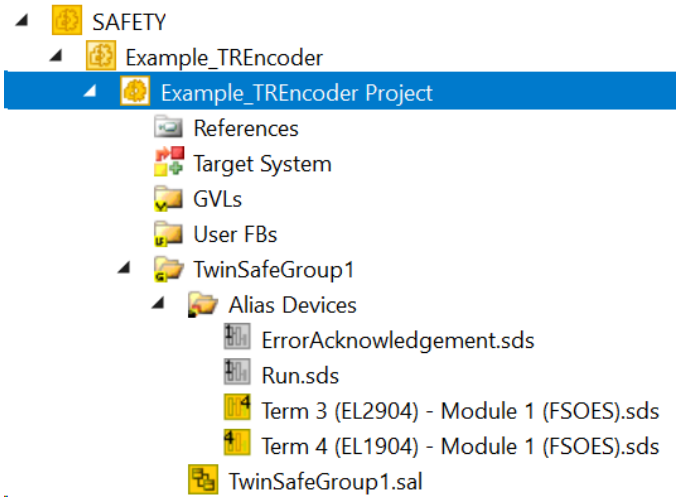
务必在 PROFIsafe I/O 设备上配置与 *Alias Device*（别名设备）完全相同的 iParameters，以便正确启动通信。

然后，您可以继续配置安全项目。此时，假定存在如下初始状况。

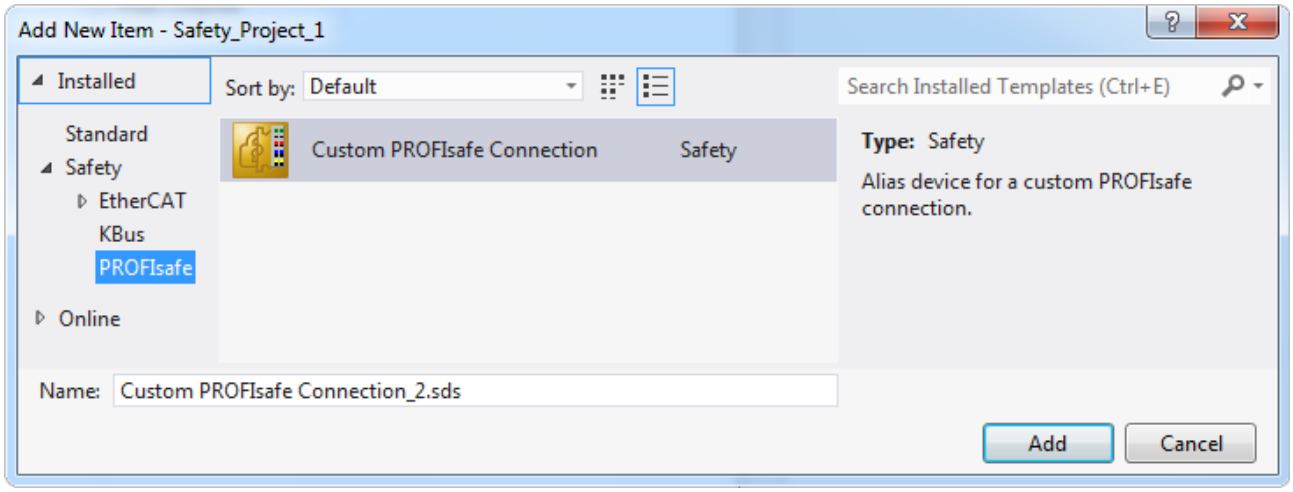


10.1.2.3 TwinCAT 安全项目连接的配置

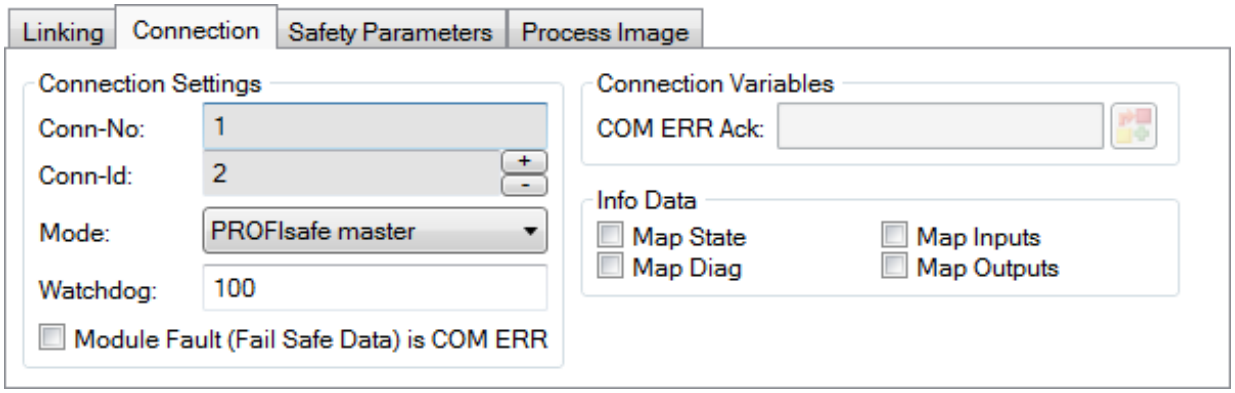
在配置 PROFIsafe 连接之前，首先要创建一个安全项目，并为可用的 EtherCAT 组件导入所需的别名设备。此外，目标系统还映射到 EtherCAT 网段的 EL6910（通过 *Target System*（目标系统）节点）。



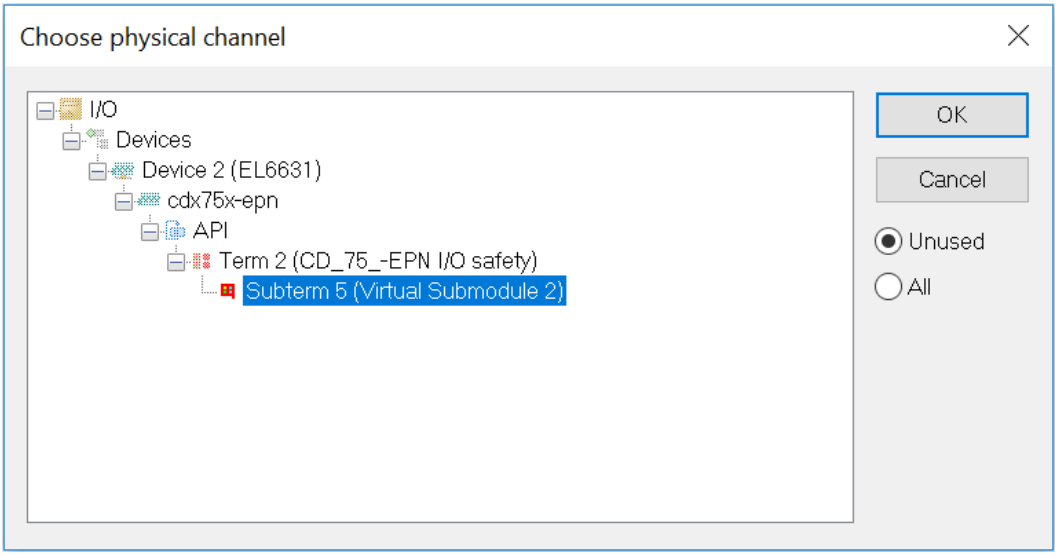
然后，您可以继续配置与 TR 编码器的 PROFIsafe 连接。这种连接通常通过 *Alias Device*（别名设备）来实现。通过在 *Alias Devices*（别名设备）节点的上下文菜单中选择 *Add*（添加）和 New item…（新项目…），可以创建 *Custom PROFIsafe Connection*（自定义 PROFIsafe 连接）。



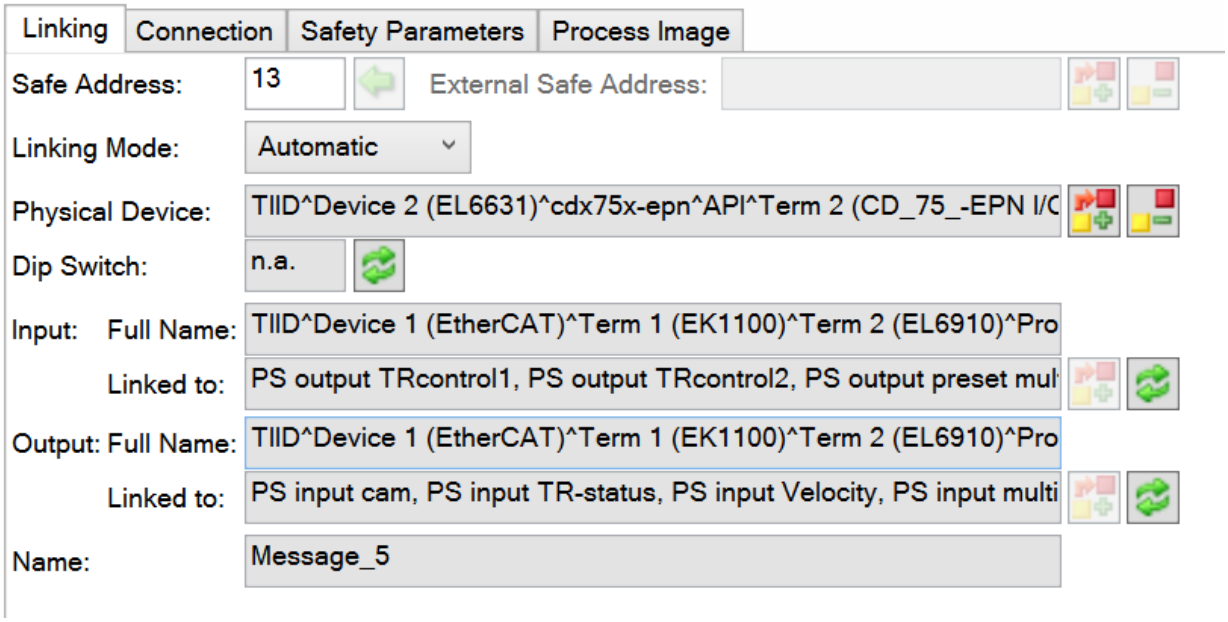
打开别名设备后，首先必须在 *Connection*（连接）选项卡上将 *PROFIsafe Master*（PROFIsafe 主站）选为连接模式。



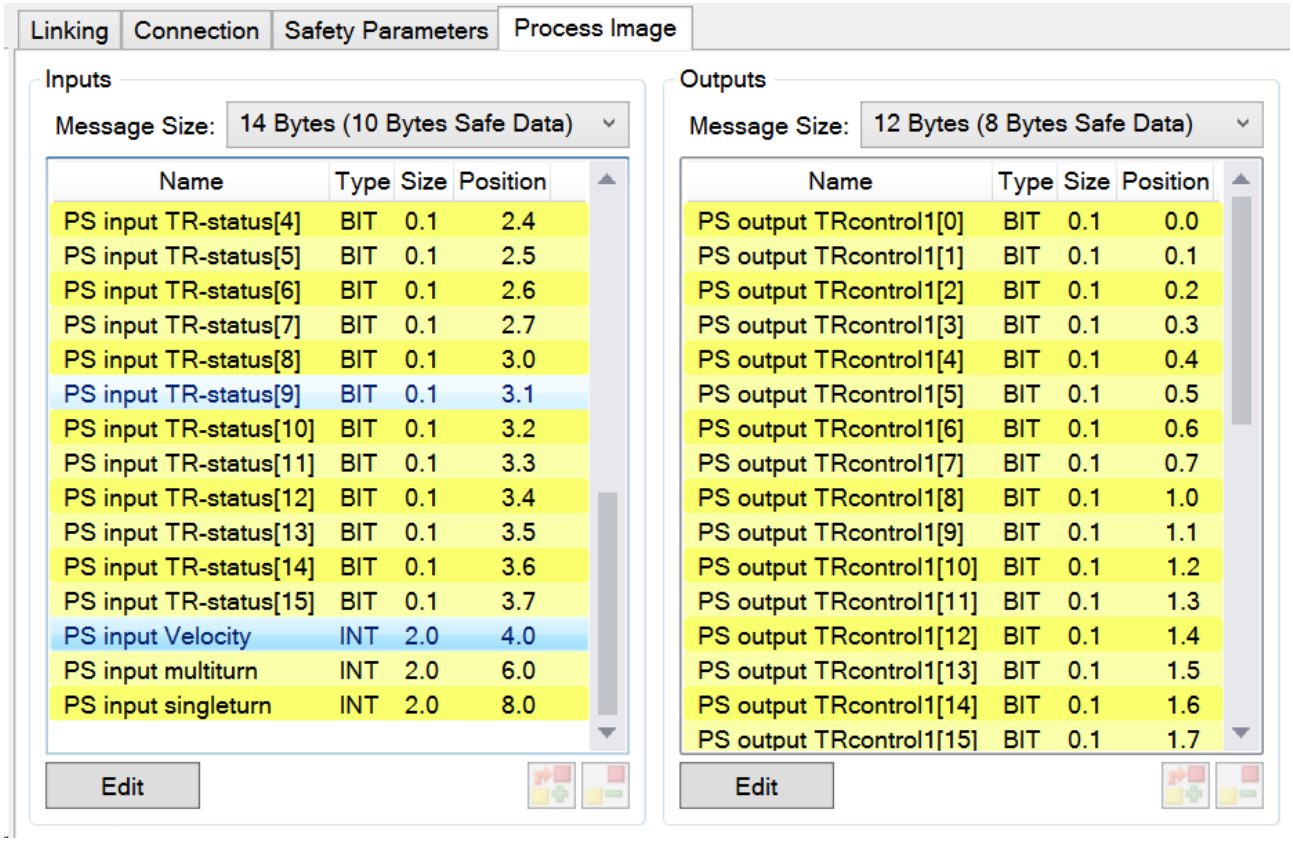
在 *Linking*（链接）选项卡上，链接模式必须被设置为 *Automatic*（自动），以便能够通过 *Map to Physical Device*（映射到物理设备）按钮选择此处考虑的 TR 编码器。



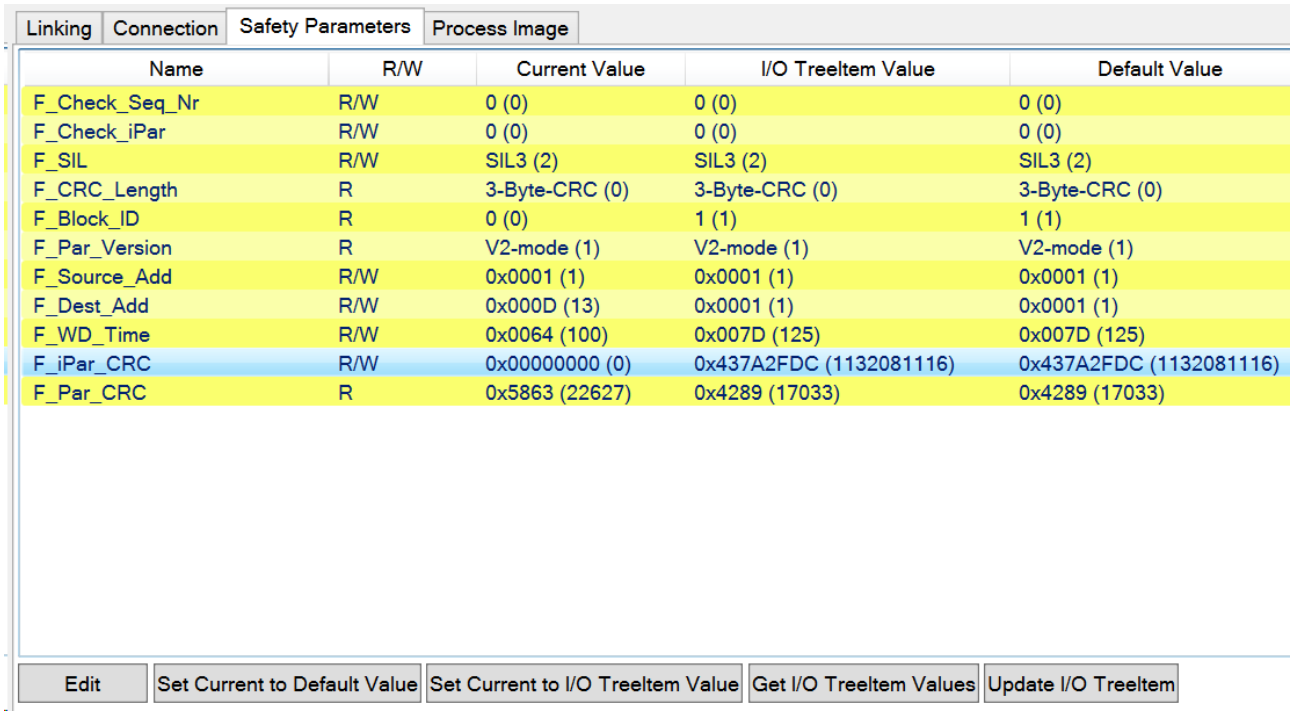
除了映射到物理设备外，还必须在 *Linking*（链接）选项卡上输入编码器的安全地址（在本例中为 13）。



如果所有设置均正确无误，则可在 *Process Image*（过程映像）选项卡上查看编码器的安全过程映像（在本例中涉及的条目为 *Velocity*（速度））。



Safety Parameters（安全参数）选项卡提供了 PROFIsafe 主站连接的相关参数。



附图 1: 安全参数编码器

在此处必须正确设置 PROFIsafe 连接的所有参数。其中包括两个地址 F_Source_Add（目标系统）和 F_Dest_Add（PROFIsafe 设备的安全地址）。此外，还必须配置 *iParameters* 的 CRC。这可以从配置编码器的附加应用程序中获取（请参见*编码器配置*一节）

对于 PROFIsafe 设备，必须在别名设备内部和 I/O 配置中直接为设备设置参数。通过 *Safety Parameters*（安全参数）选项卡上的相应按钮可以启动从 I/O 设备读取数据和向 I/O 设备传输数据的操作。两处的数据必须一致，才能成功建立 PROFIsafe 连接。

参数	描述
F_Check_Seq_Nr	设置（0/1）以指示是否应检查连接的序列号。
F_Check_iPar	设置（0/1）以指示是否应通过 iPar 服务器执行参数设置。
F_SIL	选择所需的 SIL 等级（SIL1、SIL2、SIL3、NoSIL）
F_CRC_Length	CRC 长度显示
F_Block_ID	始终为 0
F_Par_Version	使用的 PROFIsafe 版本（通常为 V2 模式）
F_Source_Add	设置 PROFIsafe 源地址
F_Dest_Add	设置 PROFIsafe 目标地址
F_WD_Time	设置 Watchdog（看门狗）时间
F_iPar_CRC	PROFIsafe 从站的 i-parameter(s)
F_Par_CRC	对所有参数计算得出的 CRC

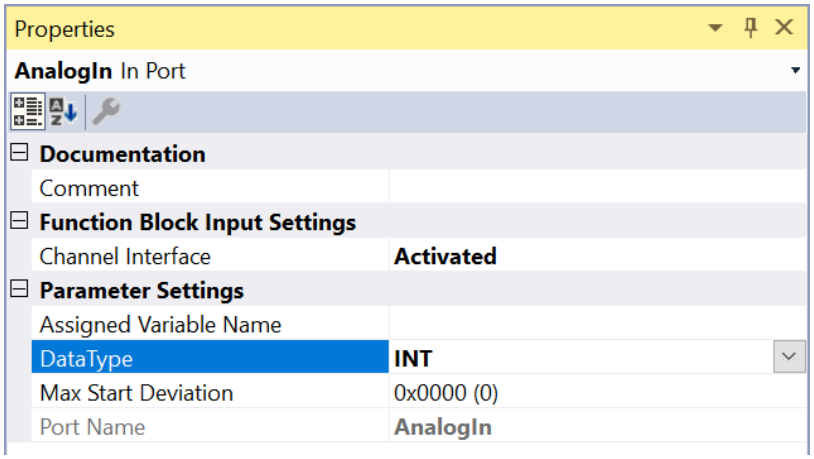
完成参数配置后，必须点击 *Update IO TreeItem*（更新 IO 树项）按钮，最终将参数传输至 I/O 配置中。

完成连接配置后，您可以继续实施实际的安全功能。

10.1.2.4 实施 TwinCAT 安全项目

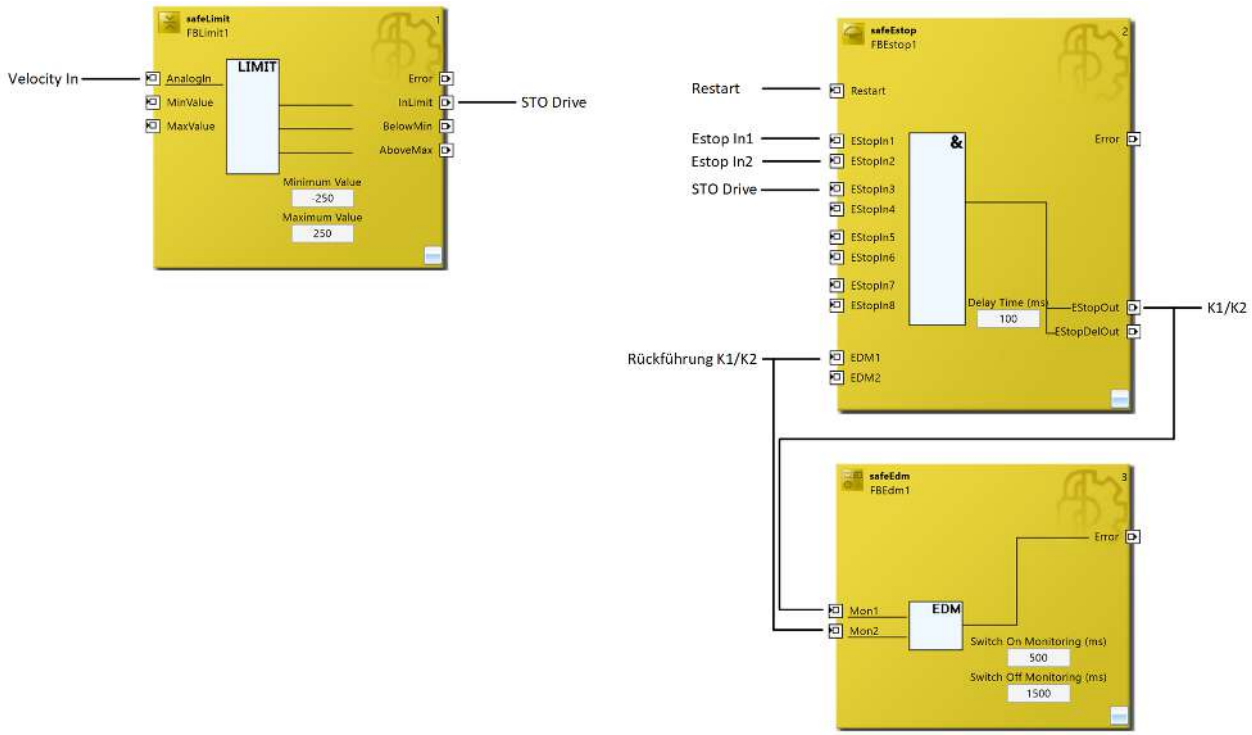
在本例所考虑的监控驱动器速度的安全功能中，通过 PROFIsafe 接收的安全速度值用于将其与指定的限值进行比较，并在超过该限值时采取适当的措施。

safeLimit 功能块用于检查速度值。通过 PROFIsafe 接收的速度值是一个 16 位整数值（请参见 PROFIsafe 连接的 *Alias Device*（别名设备）的 *Process Image*（过程映像）选项卡）。因此，对于插入的 safeLimit 功能块，必须将输入 *AnalogIn* 的数据类型配置为 *INT*。



然后，可将该输入与 PROFIsafe 连接的 *Velocity*（速度）信号相关联。

safeLimit 功能块生成的 *InLimit* 信号可指示速度是否低于配置的最大限值。例如，它还可用于通过 *safeEstop* 功能块对可能存在的急停开关进行额外评估。



如图所示，*safeEstop* 功能块的 *EstopOut* 输出可切换两个接触器 *K1* 和 *K2*，进而控制驱动器的 *STO* 安全功能。接触器的反馈信号可用作 safeEstop 功能块的 *EDM* 输入。

除了已提及的功能块外，还使用 *safeEdm* 功能块检查接触器 K1 和 K2 的动作是否正确。在这里，根据所使用的接触器，对接通和断开检查的时间间隔进行配置。

10.1.3 安全输出端子模块的参数

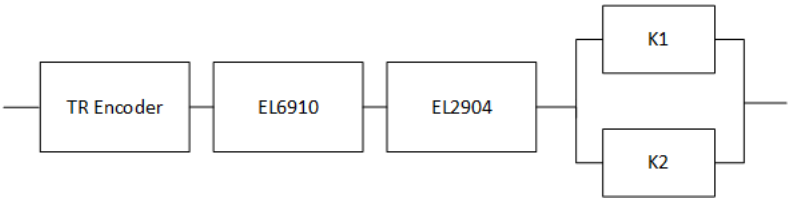
EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

10.1.4 功能块结构和安全回路

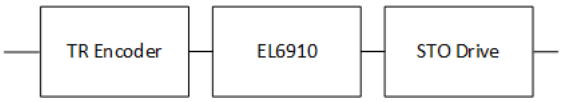
10.1.4.1 安全功能 1（不带驱动器）

就目前所述的应用示例而言，安全功能 1 考虑了从 TR 编码器到接触器 K1/K2 的安全回路。在该安全功能中，未将下游 STO 输入纳入考量范围。



10.1.4.2 安全功能 2（带驱动器）

就目前所述的应用示例而言，安全功能 2 考虑了从 TR 编码器开始的安全回路。STO 安全功能通过安全通信进行控制。为此，在计算中假定驱动器具有相应的特性安全值。



10.1.5 安全功能 1 的计算（不带驱动器）

10.1.5.1 PFHD / MTTFD / B10D – 值

组件	值
TR 编码器[1] – PFH_D	1.46E-09
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

[1] 请注意当前用户文档中提供的信息

10.1.5.2 诊断覆盖率 DC

组件	值
TR 编码器[1]	DC_{avg}=95%
带 EDM 监控（每周执行 1 次，并对所有上升沿和下降沿进行评估和持续监控）的 K1/K2，各个通道均带测试	DC_{avg}=99%

[1] 请注意当前用户文档中提供的信息

10.1.5.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN ISO 13849-1 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

K1/K2：

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{1.300.000}{0,1*21,90} = 593607,3y = 5199997320h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每周执行 1 次，直接回读

$$PFH = \frac{1-0,99}{593607,3*8760} = 1,92E-12$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输出子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = PFH_{(Encoder)} + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1-\beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

$$PFH_{ges} = 1,46E-09 + 1,79E-09 + 1,25E-09 + 10\% * \frac{1,94E-09 + 1,94E-09}{2}$$

$$PFH_{ges} = 4,69E-09$$

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值按以下公式计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

至：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTFD_{(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

如果仅有 EL2904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{d(x)} = \frac{(1-DC(x))}{PFH(x)}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

编码器的值可从当前用户文档中获取：

$$MTTF_{d(Encoder)} = 421y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{421y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{593607y}} = 198y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{95\%}{421} + \frac{99\%}{637} + \frac{99\%}{913} + \frac{99\%}{593607} + \frac{99\%}{593607}}{\frac{1}{421} + \frac{1}{637} + \frac{1}{913} + \frac{1}{593607} + \frac{1}{593607}} = 97{,}12\%$$

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**区域**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

10.1.6 安全功能 2 的计算（带驱动器）

10.1.6.1 PFHD / MTTFD / B10D – 值

组件	值
TR 编码器[1] – PFH_D	1.46E-09
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
AX8xxx-x1xx – PFH_D	3.04E-09
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

[1] 请注意当前用户文档中提供的信息

10.1.6.2 诊断覆盖率 DC

组件	值
TR 编码器[1]	DC_{avg}=95%
AX8xxx-x1xx STO 功能	DC_{avg}>99%

[1] 请注意当前用户文档中提供的信息

10.1.6.3 安全功能 2 的计算

由此，安全功能 2 的 PFH_D 值计算如下：

$$PFH_{ges} = PFH_{(Encoder)} + PFH_{(EL6910)} + PFH_{(AX8xxx-x1xx)}$$

$$PFH_{ges} = 1,46E-09 + 1,79E-09 + 3,04E-09$$
$$PFH_{ges} = 6,29E-09$$

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值按以下公式计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

至：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTFD_{(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}$$

及：

如果仅存在 AX8xxx-x1xx 和 EL6910 的 PFH_D 值，则适用以下估算方法：

$$MTTF_{d(x)} = \frac{(1-DC(x))}{PFH(x)}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(AX8xxx-x1xx)} = \frac{(1-DC_{(AX8xxx-x1xx)})}{PFH_{D(AX8xxx-x1xx)}} = \frac{(1-0,99)}{3,04E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{2,66E-05\frac{1}{y}} = 375y$$

附图 2:

编码器的值可从当前用户文档中获取：

$$MTTF_{d(Encoder)} = 421y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{421y} + \frac{1}{637y} + \frac{1}{375y}} = 151y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Encoder)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(AX8xxx-x1xx)}}}{\frac{1}{MTTF_{D(Encoder)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(AX8xxx-x1xx)}}}$$

$$DC_{avg} = \frac{\frac{95\%}{421} + \frac{99\%}{637} + \frac{99\%}{375}}{\frac{1}{421} + \frac{1}{637} + \frac{1}{375}} = 97,56\%$$

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**区域**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	90% ⩽ DC < 99%
高	**99% ⩽ DC**

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

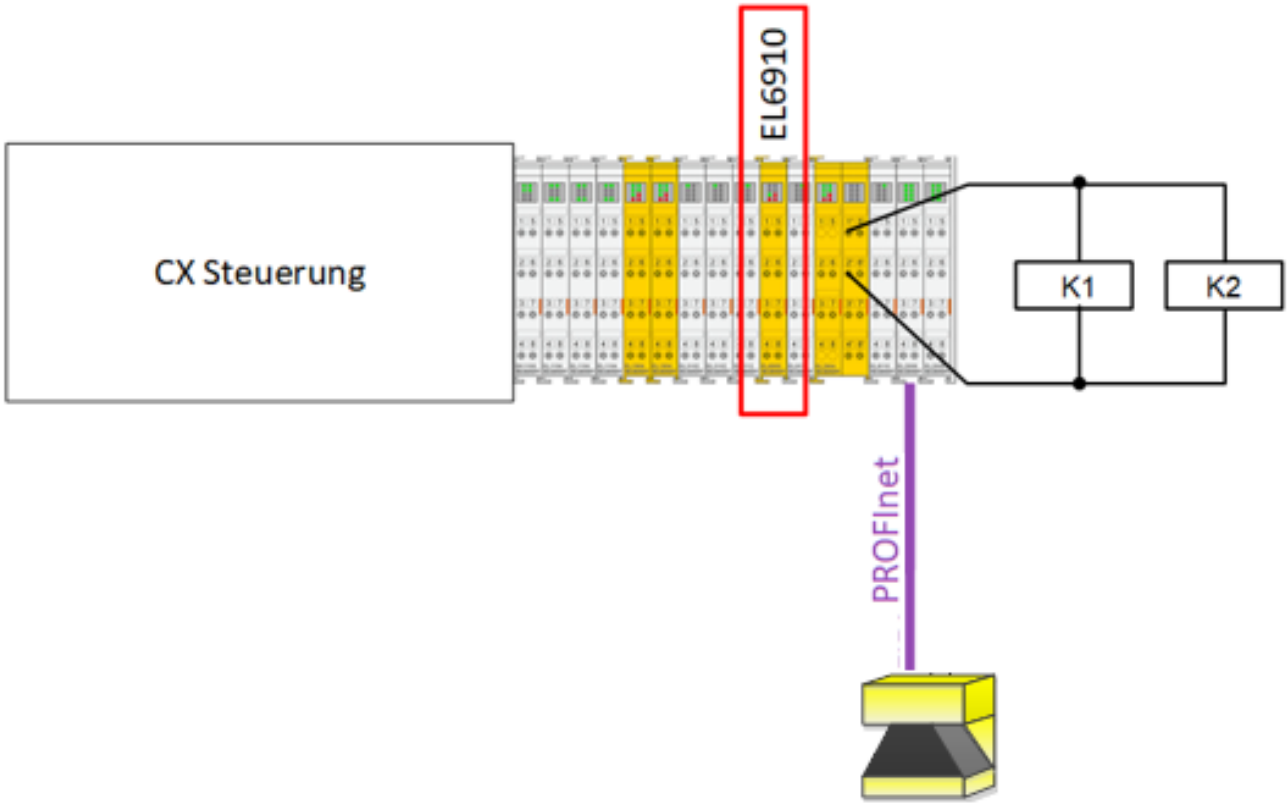
10.2 采用 PROFIsafe 激光扫描器的安全区域监控（类别 3，PL d）

通过安全激光扫描器对设备的危险区进行监控。该危险源可以通过两个接触器实现关断。接触器连接至 EL2904 的输出。SICK 的 microScan3 安全激光扫描器可用于安全区域监控。它已获得认证，适用于最高性能等级 d 的应用场景。相关数据通过安全相关协议 PROFIsafe 传输至作为 PROFIsafe 主站的 EL6910，并借助于可用的预认证功能块在那里进行监控。

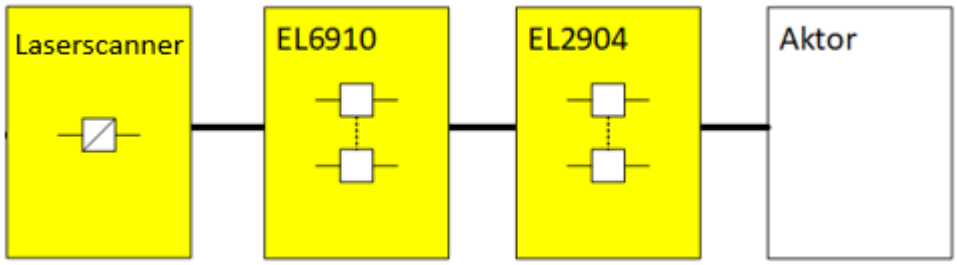
如果设定的监控案例中的两个关断路径（PROFIsafe 协议中的两个信号）发出逻辑 1 信号，则防护区域处于空闲状态，并且两个接触器保持接通。如果防护区域被占用，则两个关断路径发出逻辑 0 信号，接触器断开。整个评估在安全相关逻辑 EL6910 中的安全水平 SIL3 / PL e 上进行。

任何必要的重启锁定均可通过 fbMon 的复位输入来实现。通过安全输入读入反馈回路。该输入测试已激活。

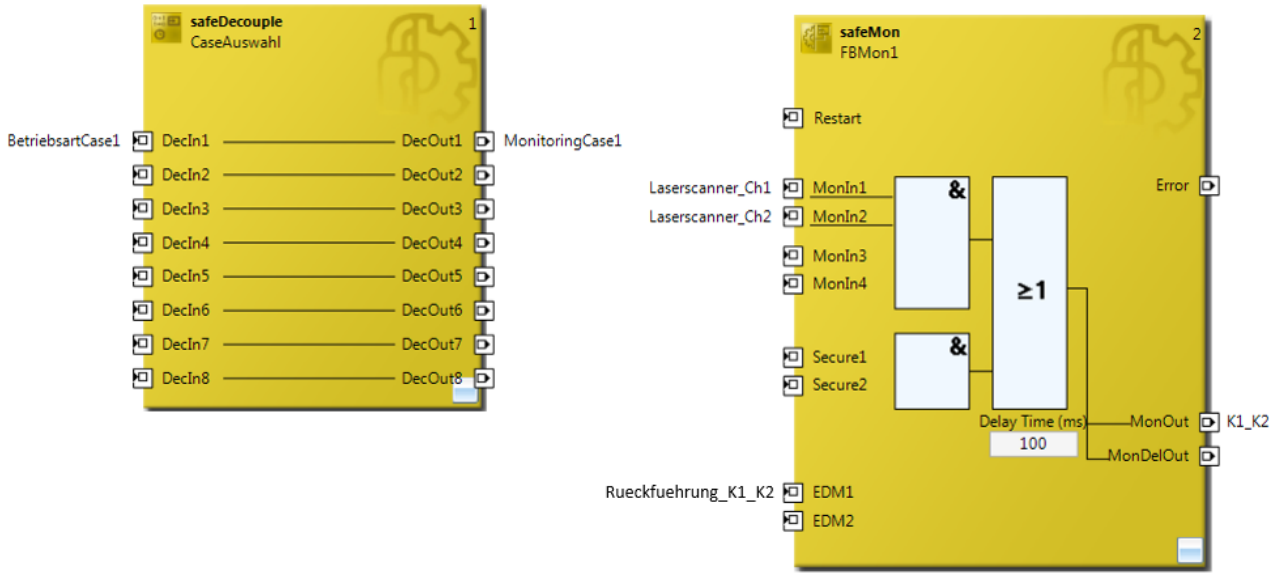
结构



结构图配置



逻辑



整个系统的正确配置

在 EtherCAT 内部传输 PROFIsafe 时需遵循以下限制。

PROFIsafe 报文仅通过 E-bus 和 PROFINET/PROFIBUS 传输

根据 PROFIsafe 规范，仅允许通过 PROFIBUS 和 PROFINET 现场总线或背板总线（例如，在本示例中为 E-bus）使用 PROFIsafe。由于专利法相关原因，禁止通过其他现场总线使用 PROFIsafe。

根据 PROFIsafe 规范，以下 Siemens AG 专利具有相关性：
- EP1267270-A2 数据传输方法
- WO00/045562-A1 确定数据载体可靠性的方法和设备
- WO99/049373-A1 自动化系统的短数据报文
- EP1686732 传输协议数据单元的方法和系统
- EP1802019 识别数据传输中的错误
- EP1921525-A1 安全相关系统的操作方法
- EP13172092.2 错误检测方法和系统

因此，必须根据应用程序的架构采取适当的措施。有关 PROFIsafe 的整个系统的正确配置详情，请参阅 EL6910 和 EL9930 的文档。

使用外部安全传感器

在使用外部安全传感器时，还必须遵循其他要求。

⚠ 谨慎

使用外部安全传感器

在使用外部安全传感器时，必须始终遵循当前版本的文档说明。此处列出了所有关于装配、操作和维修的要求，您必须满足这些条件，才能在安全相关应用中正确使用传感器。

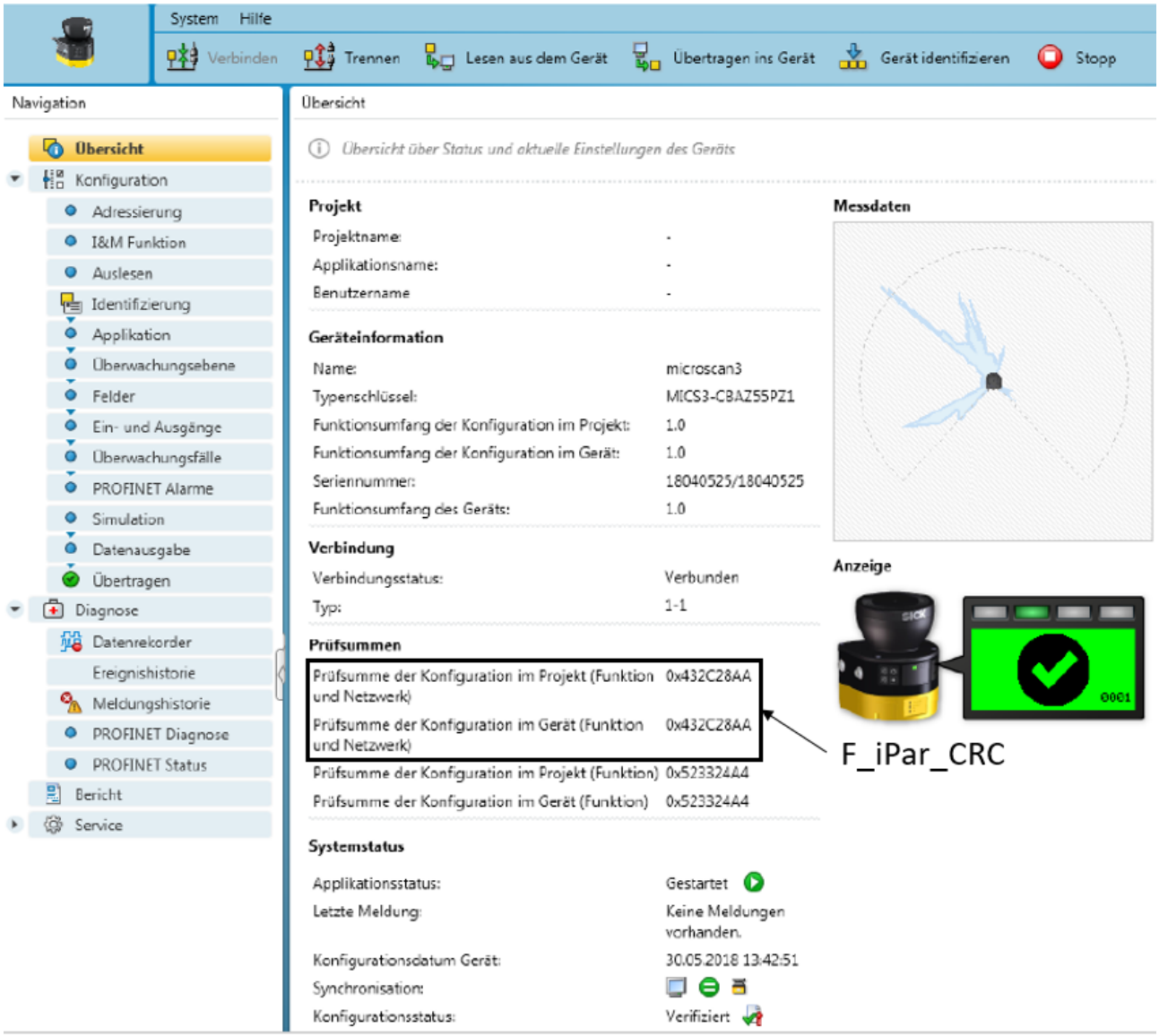
10.2.1 工程环境中的配置

除了连接 TwinSAFE 组件外，本应用示例还考虑了通过 PROFIsafe/PROFInet 连接安全激光扫描器的附加方案。下文将详细介绍实施过程中所有必要的配置步骤。

安全激光扫描器的配置需要借助额外的应用程序。这可以确定安全激光扫描器的功能范围、PROFInet/PROFIsafe 中的通信设置以及 iParameters 的 CRC 校验和，这些参数最终均需在 TwinCAT 中进行额外配置。

10.2.1.1 安全激光扫描器的配置

安全激光扫描器的配置需要借助额外的应用程序。可从制造商网站获取当前版本。

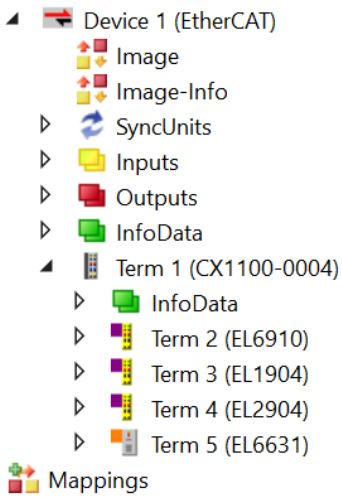


此处必须根据应用配置必要的功能和参数，以便能够正确计算 CRC 校验和（图中为 **F_iPar_CRC**）。

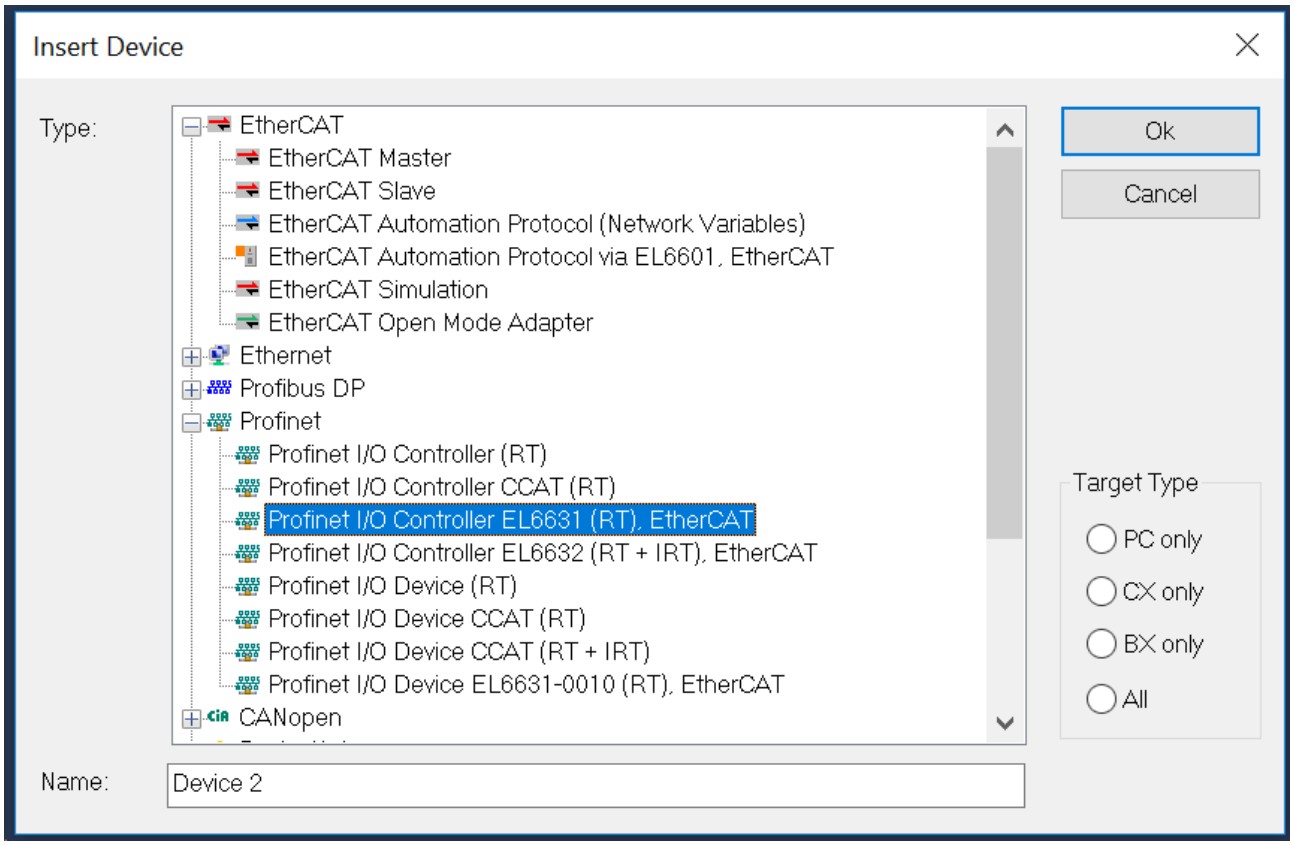
10.2.1.2 TwinCAT I/O 的配置

在开始 TwinCAT 配置之前，必须将安全激光扫描器的当前 GSDML 文件插入以下路径的 Profinet 设备目录中：TwinCAT\3.1\Config\Io\Profinet。

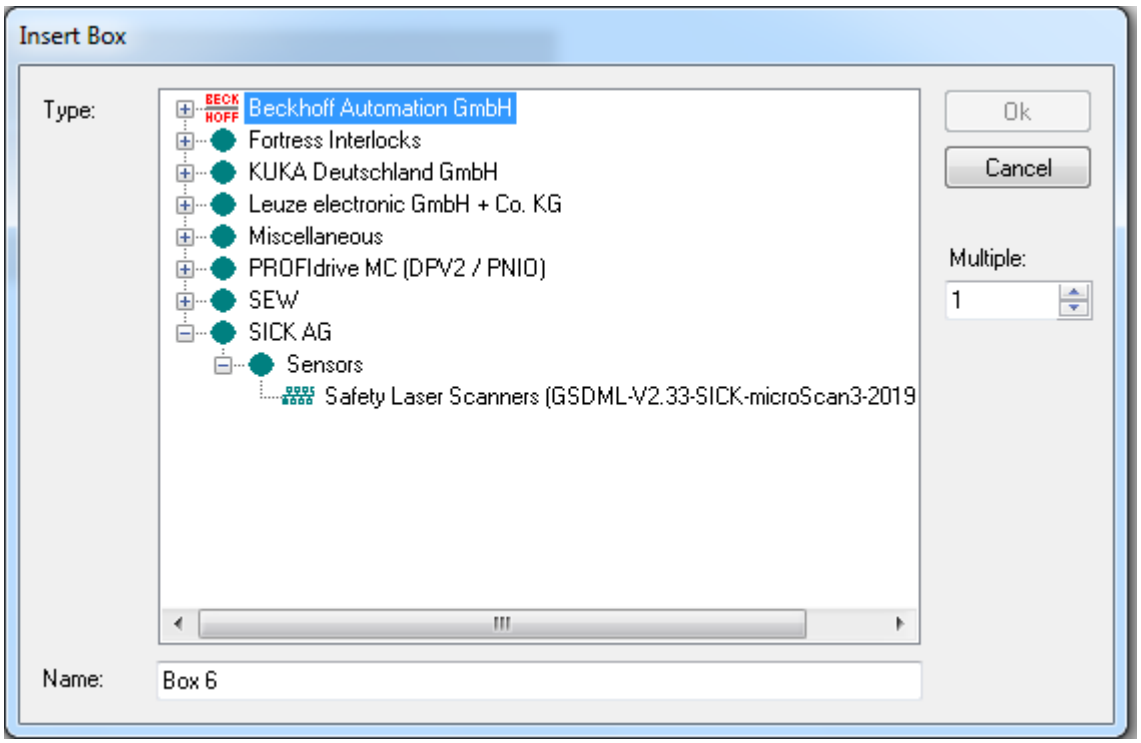
随后，创建一个新的 TwinCAT 项目并配置 EtherCAT 网段。



此外，通过添加一个 PROFInet I/O 控制器，可生成 PROFInet 网段的配置。



与 EtherCAT 网段的配置方式相同，PROFInet 控制器同样支持自动扫描或手动生成配置。通过这种方式，也可以手动添加 Sick 激光扫描器。



要通过 PROFIsafe 成功使用 Sick 激光扫描器，必须遵循以下信息说明。

⚠ 谨慎

数据类型 WORD!

当在过程映像中使用 WORD 数据类型时，可能需要进行额外配置。

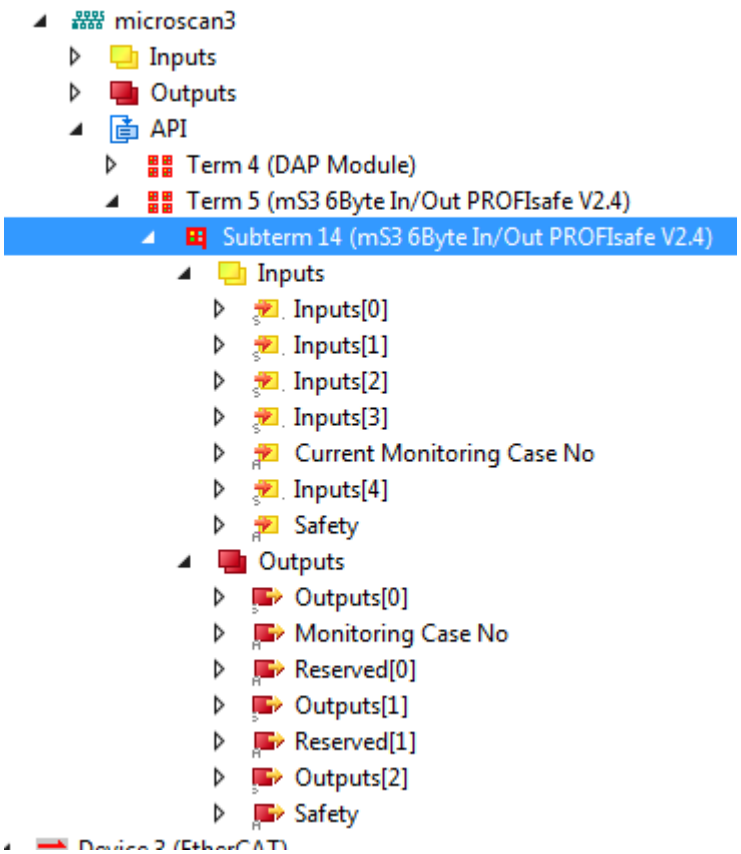
如果在配置中没有使用 EL9930 来限制 PROFIsafe 网段，则必须针对过程映像中包含 WORD 数据类型的信号，在 PROFIsafe 设备的 I/O 配置中配置高字节和低字节部分的交换。此操作可通过直接在数据值（在 *Flags*（标志）选项卡上）勾选 *Swap LOBYTE and HIBYTE*（交换 LOBYTE 和 HIBYTE）复选框来完成。

⚠ 谨慎

iParameter

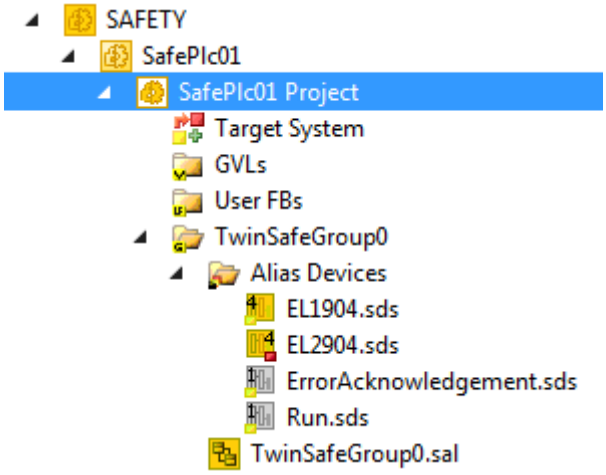
务必在 PROFIsafe I/O 设备上配置与 *Alias Device*（别名设备）完全相同的 iParameters，以便正确启动通信。

然后，您可以继续配置安全项目。此时，假定存在如下初始状况。

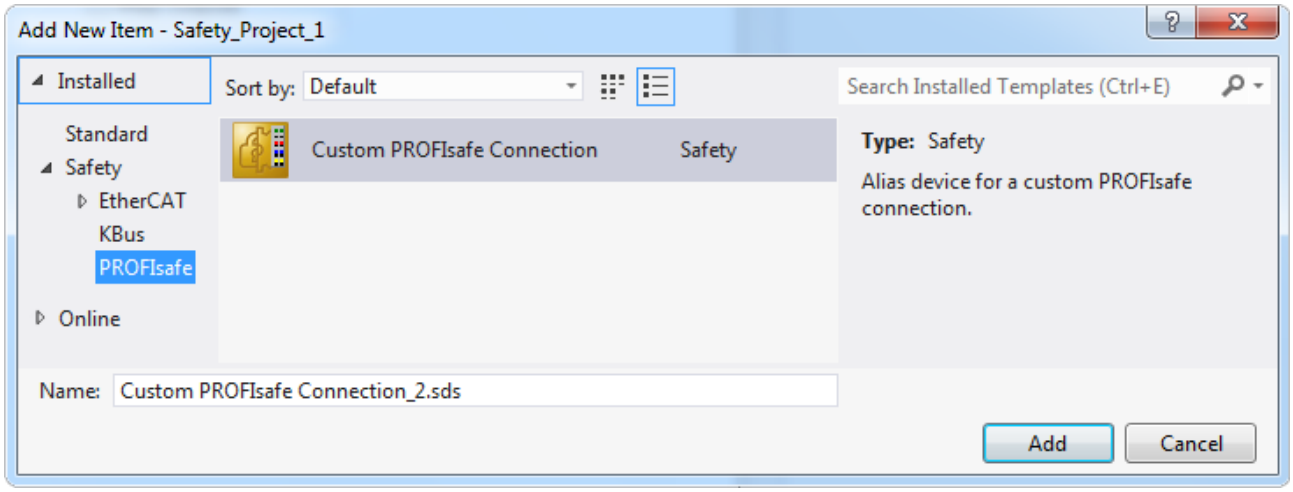


10.2.1.3 TwinCAT 安全项目连接的配置

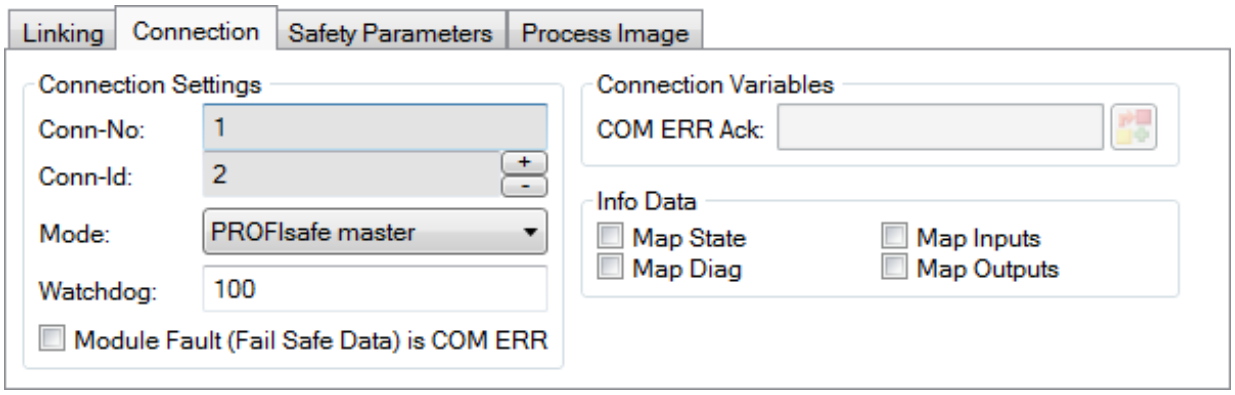
在配置 PROFIsafe 连接之前，首先要创建一个安全项目，并为可用的 EtherCAT 组件导入所需的别名设备。此外，目标系统还映射到 EtherCAT 网段的 EL6910（通过 *Target System*（目标系统）节点）。



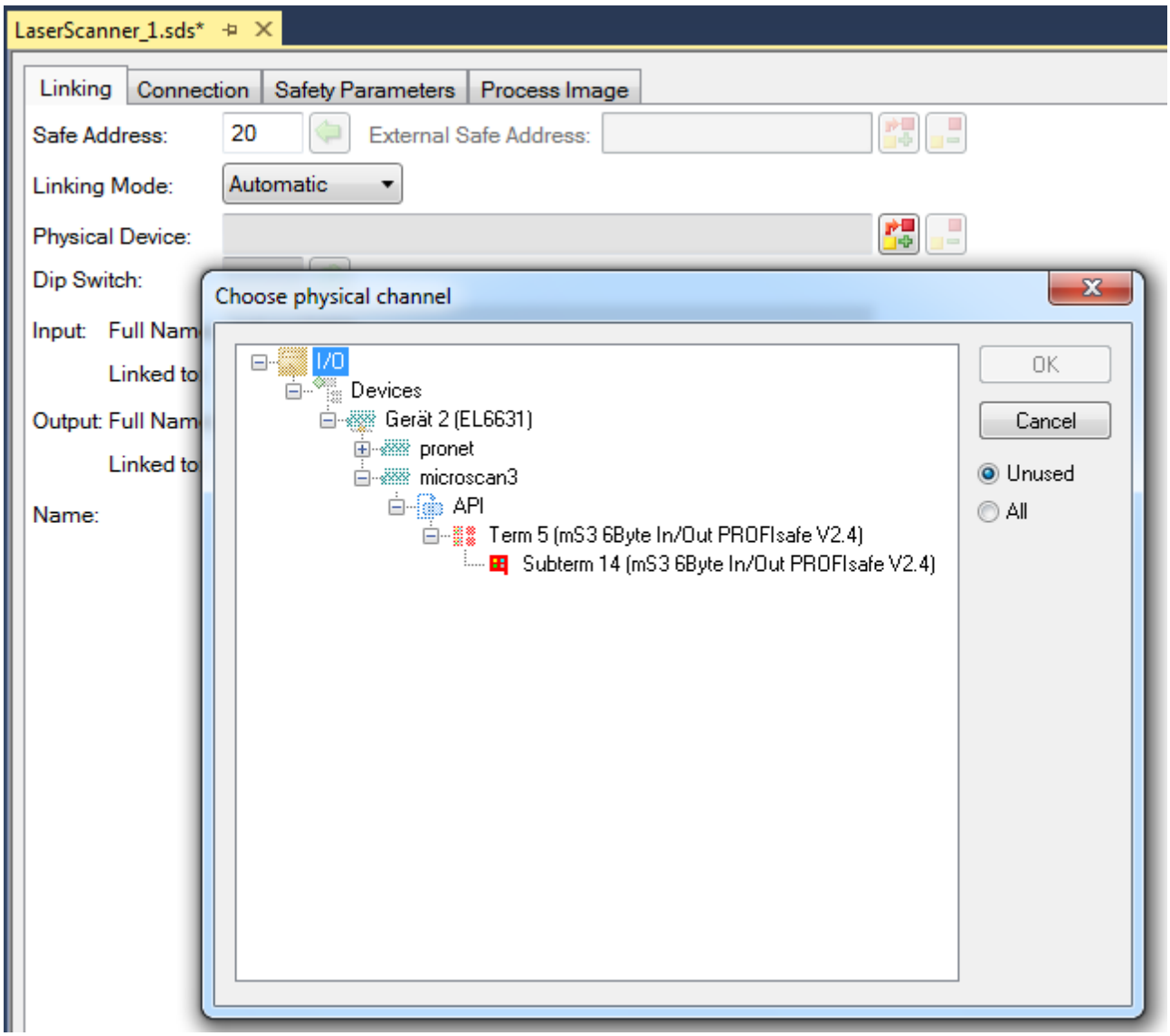
然后，您可以继续配置与安全激光扫描器的 PROFIsafe 连接。这种连接通常通过 *Alias Device*（别名设备）来实现。通过在 *Alias Devices*（别名设备）节点的上下文菜单中选择 *Add*（添加）和 New item…（新项目…），可以创建 *Custom PROFIsafe Connection*（自定义 PROFIsafe 连接）。



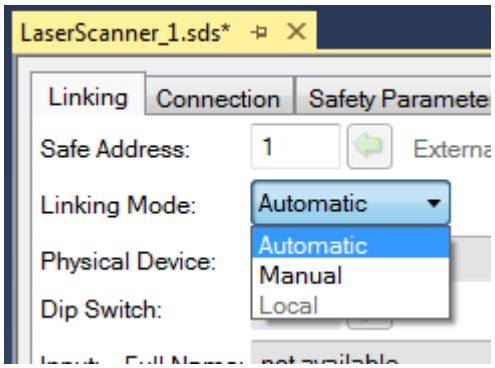
打开别名设备后，首先必须在 *Connection*（连接）选项卡上将 *PROFIsafe Master*（PROFIsafe 主站）选为连接模式。



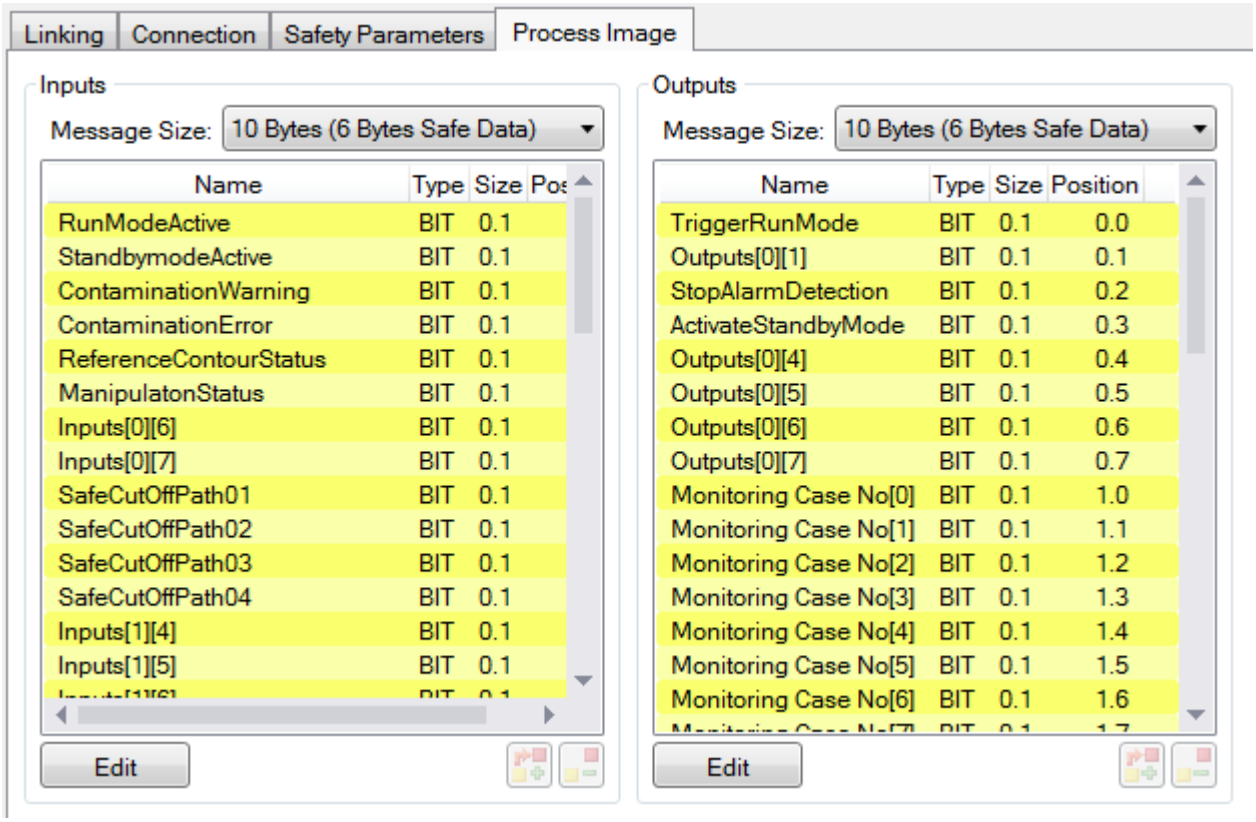
在 *Linking*（链接）选项卡上，链接模式必须被设置为 *Automatic*（自动），以便能够通过 *Map to Physical Device*（映射到物理设备）按钮选择此处考虑的 Sick 安全激光扫描器。



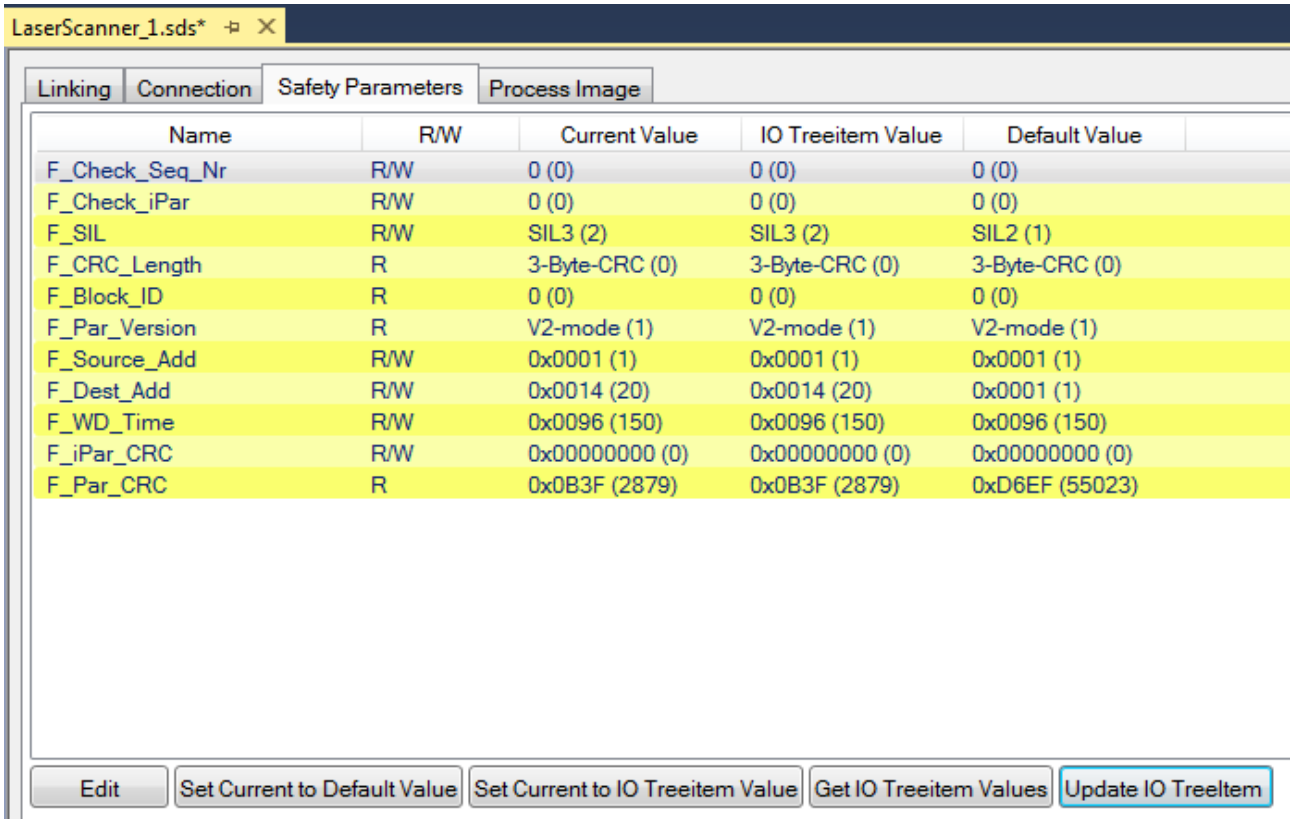
除了映射到物理设备外，还必须在 *Linking*（链接）选项卡上输入安全激光扫描器的安全地址（在本例中为 20）。



如果所有设置均正确无误，则可在 *Process Image*（过程映像）选项卡上查看安全激光扫描器的安全过程映像。通过 Edit（编辑）按钮可以调整名称。务必从制造商的最新文档中获取接口的分配以及各个信号的说明。



Safety Parameters（安全参数）选项卡提供了 PROFIsafe 主站连接的相关参数。



在此处必须正确设置 PROFIsafe 连接的所有参数。其中包括两个地址 F_Source_Add（目标系统）和 F_Dest_Add（PROFIsafe 设备的安全地址）。此外，还必须配置 *iParameters* 的 CRC。这可以从配置安全激光扫描器的附加应用程序中获取（请参见*编码器配置*一节）。

对于 PROFIsafe 设备，必须在别名设备内部和 I/O 配置中直接为设备设置参数。通过 *Safety Parameters*（安全参数）选项卡上的相应按钮可以启动从 I/O 设备读取数据和向 I/O 设备传输数据的操作。两处的数据必须一致，才能成功建立 PROFIsafe 连接。

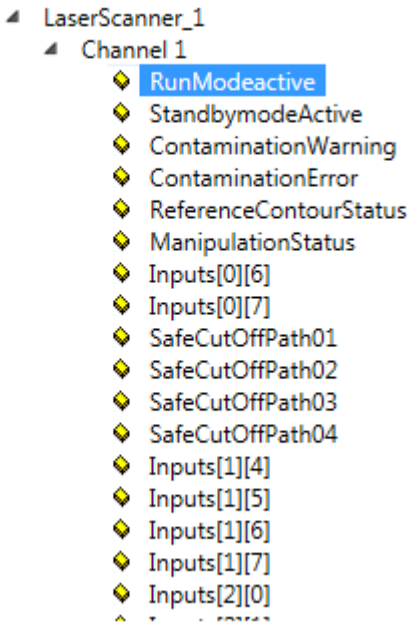
参数	描述
F_Check_Seq_Nr	设置（0/1）以指示是否应检查连接的序列号。
F_Check_iPar	设置（0/1）以指示是否应通过 iPar 服务器执行参数设置。
F_SIL	选择所需的 SIL 等级（SIL1、SIL2、SIL3、NoSIL）
F_CRC_Length	CRC 长度显示
F_Block_ID	始终为 0
F_Par_Version	使用的 PROFIsafe 版本（通常为 V2 模式）
F_Source_Add	设置 PROFIsafe 源地址
F_Dest_Add	设置 PROFIsafe 目标地址
F_WD_Time	设置 Watchdog（看门狗）时间
F_iPar_CRC	PROFIsafe 从站的 i-parameter(s)
F_Par_CRC	对所有参数计算得出的 CRC

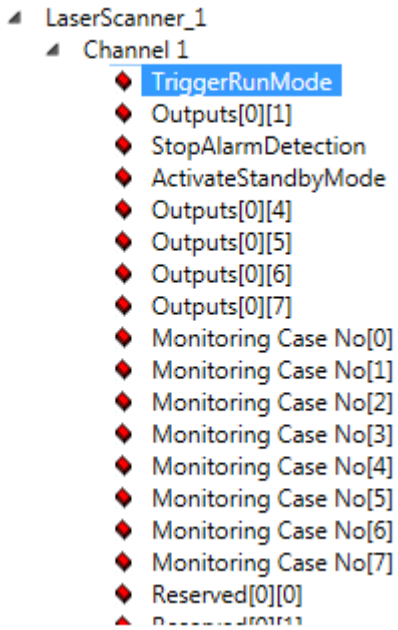
完成参数配置后，必须点击 *Update IO TreeItem*（更新 IO 树项）按钮，最终将参数传输至 I/O 配置中。

完成连接配置后，您可以继续实施实际的安全功能。

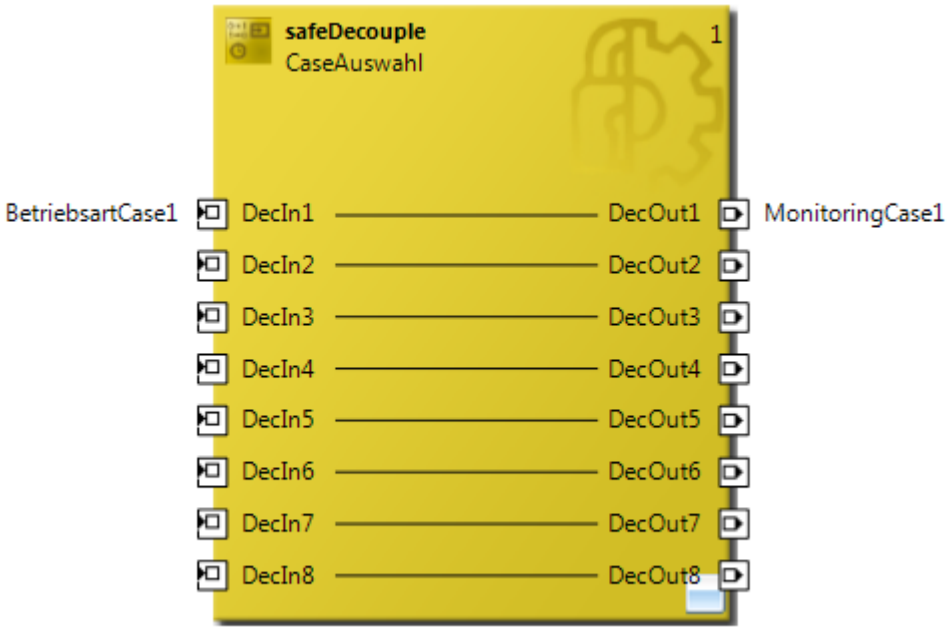
10.2.1.4 实施 TwinCAT 安全项目

通过 PROFIsafe 接收的安全过程映像可在安全功能范围内使用，通过本例所考虑的安全激光扫描器进行区域监控。安全激光扫描器的配置决定了必须评估的输入和必须接通的输出。

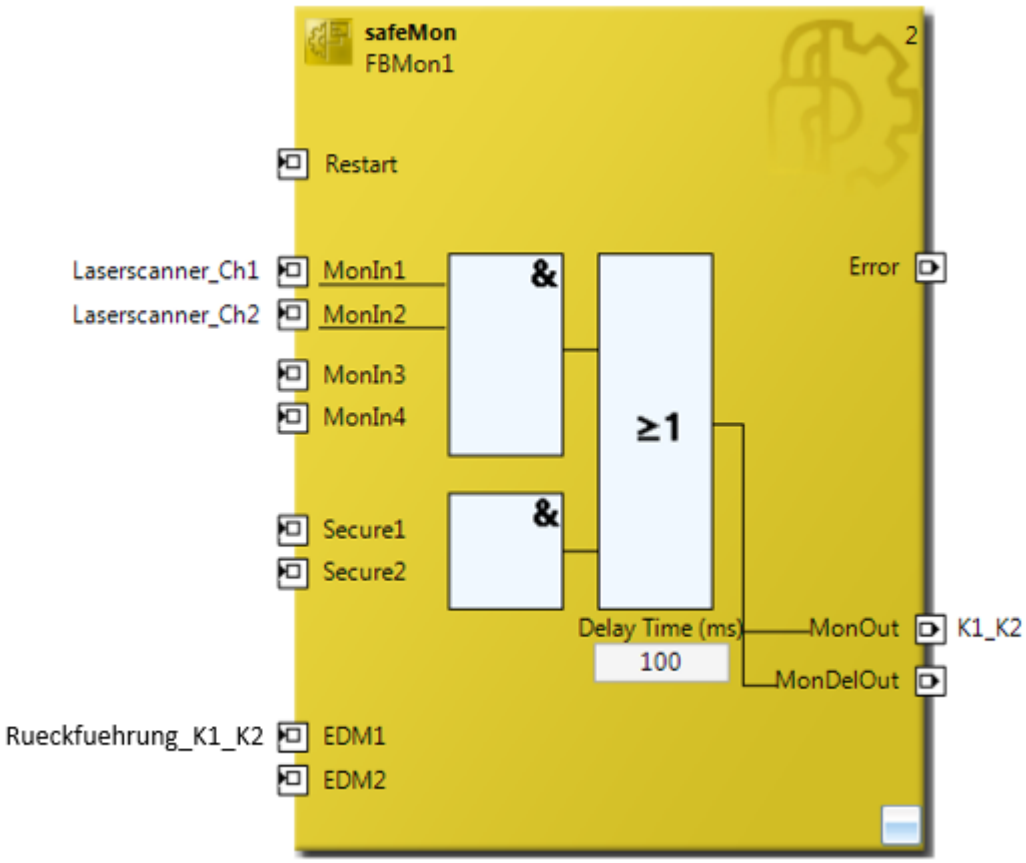




在本示例中，监控案例 1 通过 *safeDecoupler* 功能块无条件激活。



安全激光扫描器将监控设备中已参数设置的危险区，并通过关断路径 01 和 02 的信号发送监控结果。这两个信号均通过 *safeMon* 功能块进行评估。如果危险区处于空闲状态并以安全为导向进行监控，则关断路径为逻辑 1。



如图所示，当输入 *MonIn1*、*MonIn2* 和 *EDM1* 均为逻辑 1 时，两个执行安全功能的接触器 *K1* 和 *K2* 将通过 *safeMon* 功能块的输出 *MonOut* 进行切换。接触器的反馈信号可用作功能块 *safeMon* 的 *EDM1* 输入。

任何必要的重启锁定均可通过功能块 *safeMon* 的复位输入来实现。

10.2.2 安全输入和输出端子模块的参数

EL2904

参数	值
电流测量激活	是
输出测试脉冲激活	是

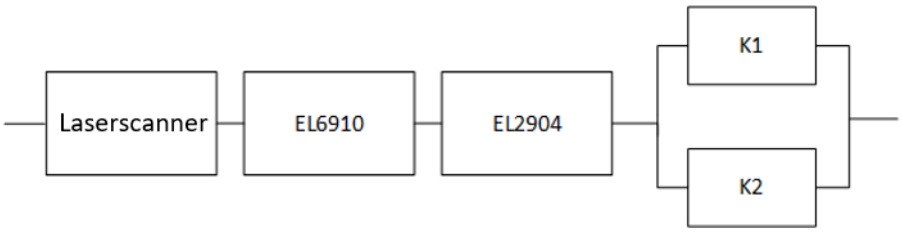
EL1904

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

10.2.3 功能块结构和安全回路

10.2.3.1 安全功能 1

就目前所述的应用示例而言，安全功能 1 考虑了从安全激光扫描器到接触器 K1/K2 的安全回路。



10.2.4 安全功能 1 的计算

10.2.4.1 PFHD / MTTFD / B10D – 值

组件	值
激光扫描器[1] – PFH_D、SIL、Cat、PL	8E-08、SIL 2、Cat. 3、PL d
EL2904 – PFH_D	1.25E-09
EL6910 – PFH_D	1.79E-09
K1 – $B10_D$	1,300,000
K2 – $B10_D$	1,300,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10（每小时 6 次）
使用寿命（T1）	20 年 = 175200 小时

[1] 请注意当前用户文档中提供的信息

10.2.4.2 诊断覆盖率 DC

组件	值
带测试（通过扫描器）[1] 的激光扫描器	DC_{avg}=90%
带 EDM 监控的 K1/K2，含各个通道的测试	DC_{avg}=99%

[1] 请注意当前用户文档中提供的信息

10.2.4.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN ISO 13849-1 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0,1 * n_{op}}$$

得出

$$PFH = \frac{0,1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

K1/K2：

$$n_{op} = \frac{230 * 16 * 60}{10} = 22.080$$

$$MTTF_D = \frac{1.300.000}{0,1 * 22.080} = 588,7y = 5.157.012h$$

并假设 K1 和 K2 均为单通道：

K1/K2：每小时执行 10 次，直接回读

$$PFH = \frac{1 - 0,99}{588,7y * 8760} = 1,94E - 09$$

现在必须做出以下假设：

继电器 K1 和 K2 均连接至安全功能。继电器故障不会导致危险情况，但反馈信号可检测到该情况。此外，K1 和 K2 的 $B10_D$ 值相同。

通过两个通道连接的组件之间存在一个耦合系数。例如温度、EMC、电压峰值或这些组件之间的信号。这被假定为最坏情况估计，其中 β =10%。EN 62061 包含相关表格（表 F.1：确定 CCF 的准则，表 F.2：CCF 系数（β）的估算），可用于精确确定 β 系数。对于输出子系统，如果对计算 β 系数的表格进行相应修改，估计值可达到 2%。在后续计算中，将采用 10% 作为最坏情况假设值。

此外，假定已采取所有常规措施，以防止因错误导致两个通道同时发生危险故障（例如：继电器触点过流、控制柜内超温）。

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = PFH_{(Scanner)} + PFH_{(EL6910)} + PFH_{(EL2904)} + \beta * \frac{PFH_{(K1)} + PFH_{(K2)}}{2} + (1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$$

由于 $(1 - \beta)^2 * (PFH_{(K1)} * PFH_{(K2)}) * T1$ 部分比其余部分小 10 倍，为了简化计算，在此处及后续所有计算中均予以忽略。

$$PFH_{ges} = 8E - 08 + 1,79E - 09 + 1,25E - 09 + 10\% * \frac{1,94E-09 + 1,94E-09}{2} = 8,32E - 08$$

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值按以下公式计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

至：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}}$$

及：

如果仅存在扫描器、EL2904 和 EL6910 的 PFH_D 值，则适用以下估算方法：

$$MTTF_{d(x)} = \frac{(1 - DC(x))}{PFH(x)}$$

因此：

$$MTTF_{D(EL6910)} = \frac{(1 - DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1 - 0{,}99)}{1{,}79E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{15{,}68E-06\frac{1}{y}} = 637y$$

$$MTTF_{D(EL2904)} = \frac{(1 - DC_{(EL2904)})}{PFH_{(EL2904)}} = \frac{(1 - 0{,}99)}{1{,}25E-09\frac{1}{h} * 8760\frac{h}{y}} = \frac{0{,}01}{1{,}1E-05\frac{1}{y}} = 913{,}2y$$

$$MTTF_{D(Scanner)} = \frac{(1-DC_{(Scanner)})}{PFH_{(Scanner)}} = \frac{(1-0{,}90)}{8E-08\frac{1}{h} * 8760\frac{h}{y}} = 142y$$

根据 EN ISO 13849-1 标准中引入的类别 3 结构组件的 $MTTF_D$ 限值为 100 年（类别 4 的限值为 2500 年），在进一步处理扫描器的 $MTTF_D$ 时，限值为 100 年。

$$MTTF_{D(Scanner)} = 100y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{100y} + \frac{1}{637y} + \frac{1}{913y} + \frac{1}{588y}} = 69{,}6y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(Scanner)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(EL2904)}} + \frac{DC}{MTTF_{D(K1)}} + \frac{DC}{MTTF_{D(K2)}}}{\frac{1}{MTTF_{D(Scanner)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(EL2904)}} + \frac{1}{MTTF_{D(K1)}} + \frac{1}{MTTF_{D(K2)}}}$$

$$DC_{avg} = \frac{\frac{90\%}{100} + \frac{99\%}{637} + \frac{99\%}{913} + \frac{99\%}{588} + \frac{99\%}{588}}{\frac{1}{100} + \frac{1}{637} + \frac{1}{913} + \frac{1}{588} + \frac{1}{588}} = 93{,}4\%$$

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

注意

类别

通过使用 3 类（类别 3）激光扫描器，这种结构最多能达到类别 3。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**区域**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

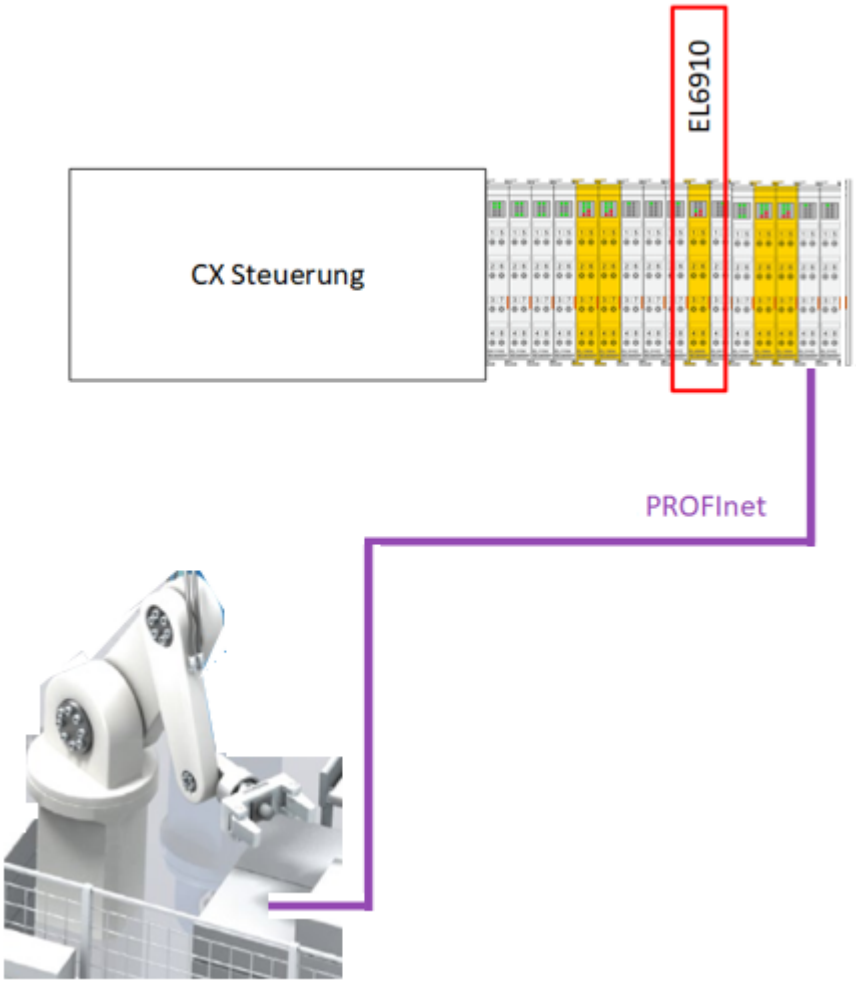
Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

10.3 通过 PROFIsafe 安全控制 ABB 机器人（类别 3，PL d）

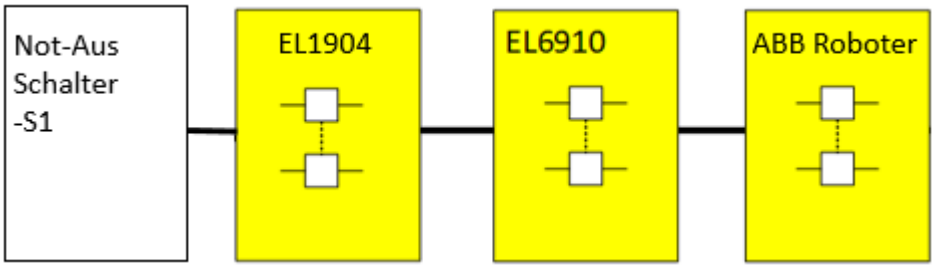
ABB 机器人可作为 PROFIsafe 设备连接至 TwinSAFE 控制器。具有 *SafeMove* 功能的 ABB 机器人已获得认证，适用于最高性能等级 d 的应用场景。借助于 PROFIsafe，安全相关数据通过 PROFInet 进行传输。急停信号通过安全协议 PROFIsafe 由作为 PROFIsafe 主站的 EL6910 传输至机器人。机器人已被配置为执行类别 0 停止。安全状态信号通过 PROFIsafe 连接传回 EL6910，并由可用的预认证功能块进行进一步处理。

该示例考虑了急停安全功能。急停开关采用双通道配置，通过两个常闭触点连接至 EL1904。启动了对信号的测试。对输入信号进行差异监控。整个评估在安全相关逻辑 EL6910 中的 SIL 3 / PL e 安全水平上进行。

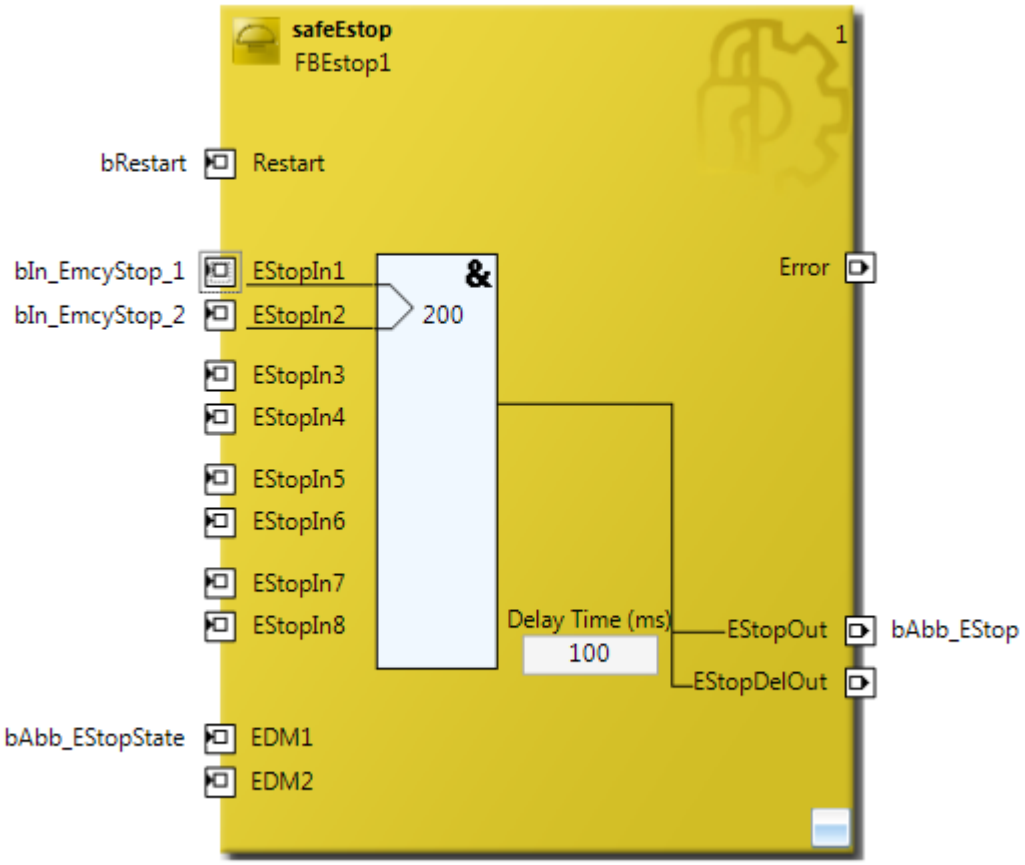
结构



结构图配置



逻辑



整个系统的正确配置

在 EtherCAT 内部传输 PROFIsafe 时需遵循以下限制。

PROFIsafe 报文仅通过 E-bus 和 PROFINET/PROFIBUS 传输

根据 PROFIsafe 规范，仅允许通过 PROFIBUS 和 PROFINET 现场总线或背板总线（例如，在本示例中为 E-bus）使用 PROFIsafe。由于专利法相关原因，禁止通过其他现场总线使用 PROFIsafe。

根据 PROFIsafe 规范，以下 Siemens AG 专利具有相关性：
- EP1267270-A2 数据传输方法
- WO00/045562-A1 确定数据载体可靠性的方法和设备
- WO99/049373-A1 自动化系统的短数据报文
- EP1686732 传输协议数据单元的方法和系统
- EP1802019 识别数据传输中的错误
- EP1921525-A1 安全相关系统的操作方法
- EP13172092.2 错误检测方法和系统

因此，必须根据应用程序的架构采取适当的措施。有关 PROFIsafe 的整个系统的正确配置详情，请参阅 EL6910 和 EL9930 的文档。

使用外部 PROFIsafe 机器人

在使用外部 PROFIsafe 机器人时，还必须遵循其他要求。

⚠ 谨慎

使用外部 PROFIsafe 机器人

在使用外部 PROFIsafe 机器人时，必须始终遵循当前版本的文档说明。此处列出了所有关于装配、操作和维修的要求，您必须满足这些条件，才能在安全相关应用中正确使用机器人。

10.3.1 FMEA

使用外部 PROFIsafe 机器人

在使用外部 PROFIsafe 机器人时，还必须遵循有关 FMEA 的其他要求。

⚠ 谨慎

使用外部 PROFIsafe 机器人

在使用外部 PROFIsafe 机器人时，必须始终遵循当前版本的文档说明。此处列出了所有关于装配、操作和维修的要求，您必须满足这些条件，才能在安全相关应用中正确使用机器人。

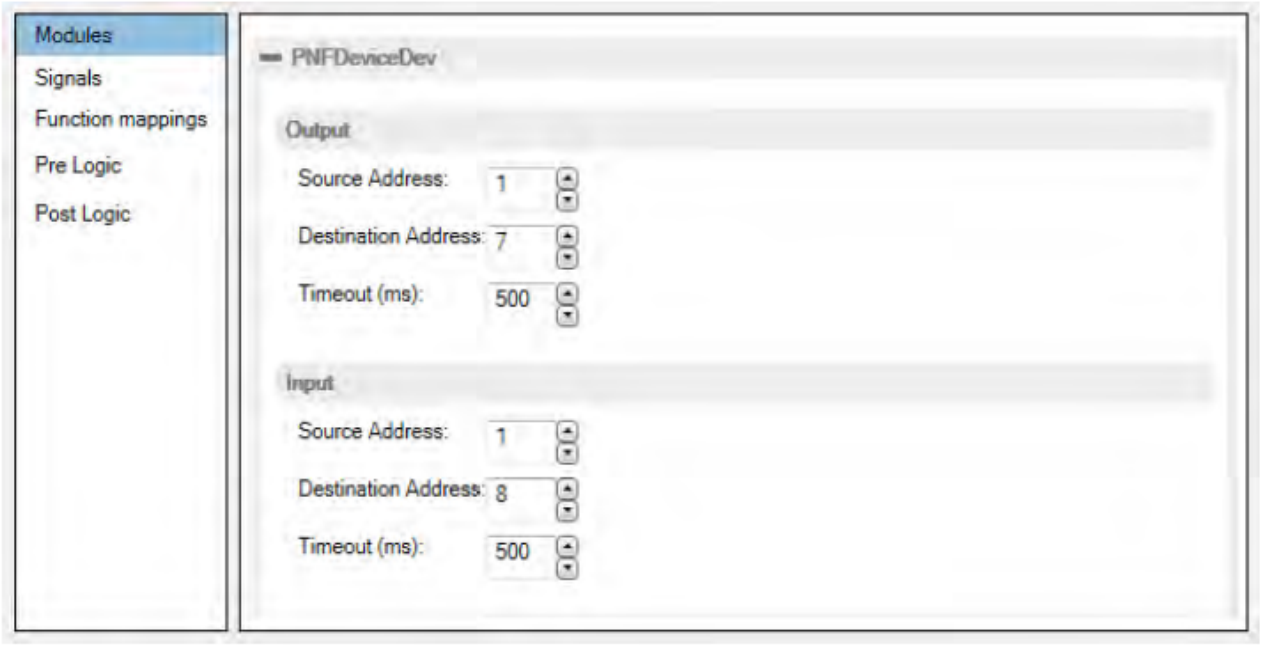
10.3.2 工程环境中的配置

除了连接 TwinSAFE 组件外，本应用示例还考虑了通过 PROFIsafe/PROFInet 连接编码器的附加方案。下文将详细介绍实施过程中所有必要的配置步骤。

为了配置编码器的安全相关参数，需要借助额外的应用程序对设备进行参数设置，并确定 iParameters 的 CRC 校验和，该校验和最终必须在 TwinCAT 中进行额外配置。

10.3.2.1 机器人配置

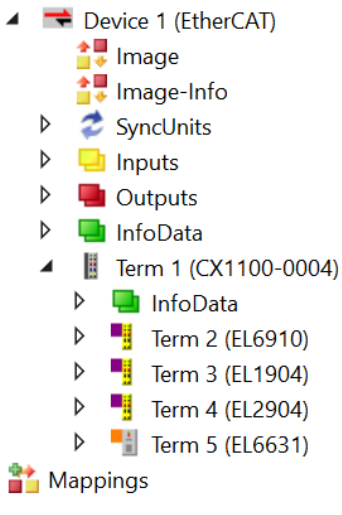
机器人的配置需要借助额外的应用程序。可从制造商网站获取当前版本。



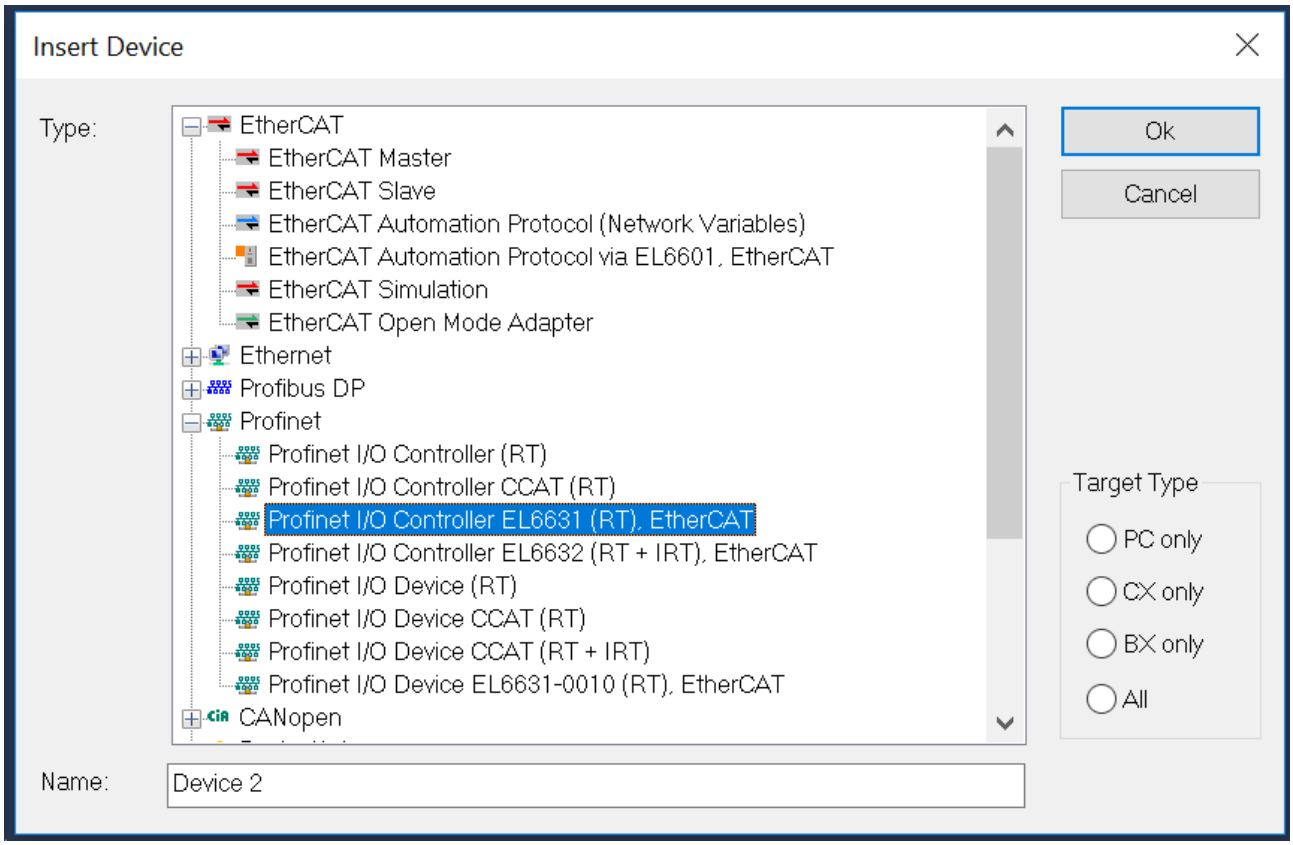
此处必须根据应用配置必要的功能和参数，以便能够正确计算 CRC 校验和等参数。只有在安全过程映像的设置相匹配的情况下，才能实现安全导向的通信。

10.3.2.2 TwinCAT I/O 的配置

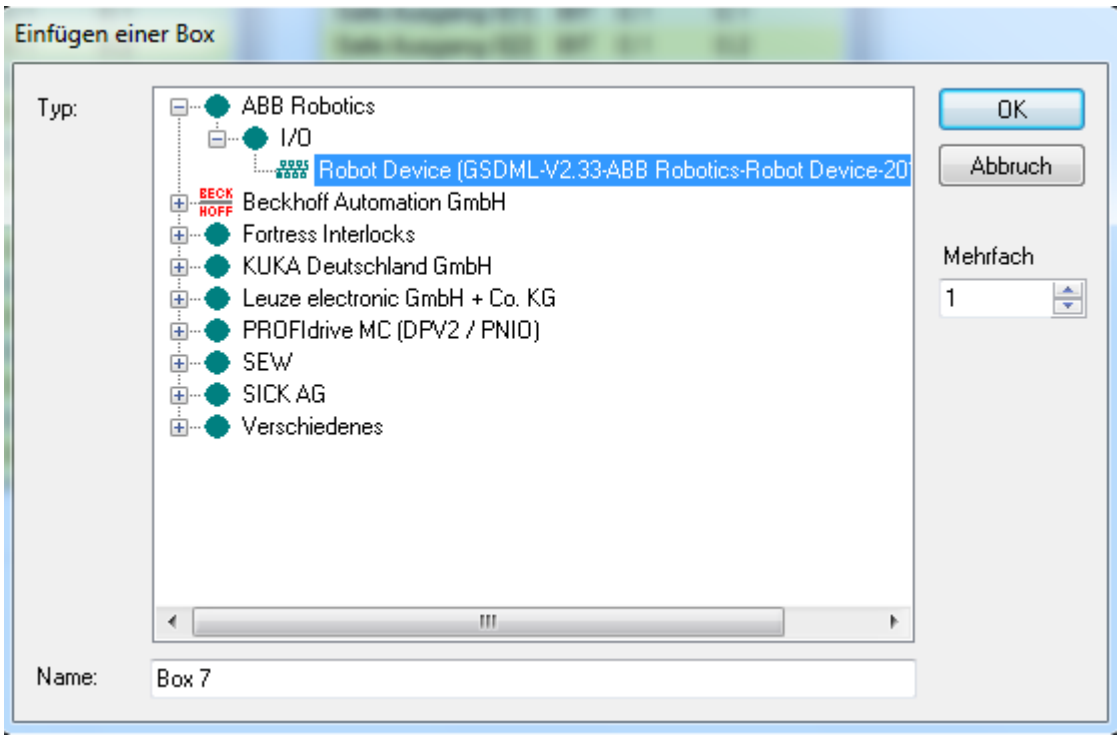
首先，创建一个新的 TwinCAT 项目并配置 EtherCAT 网段。



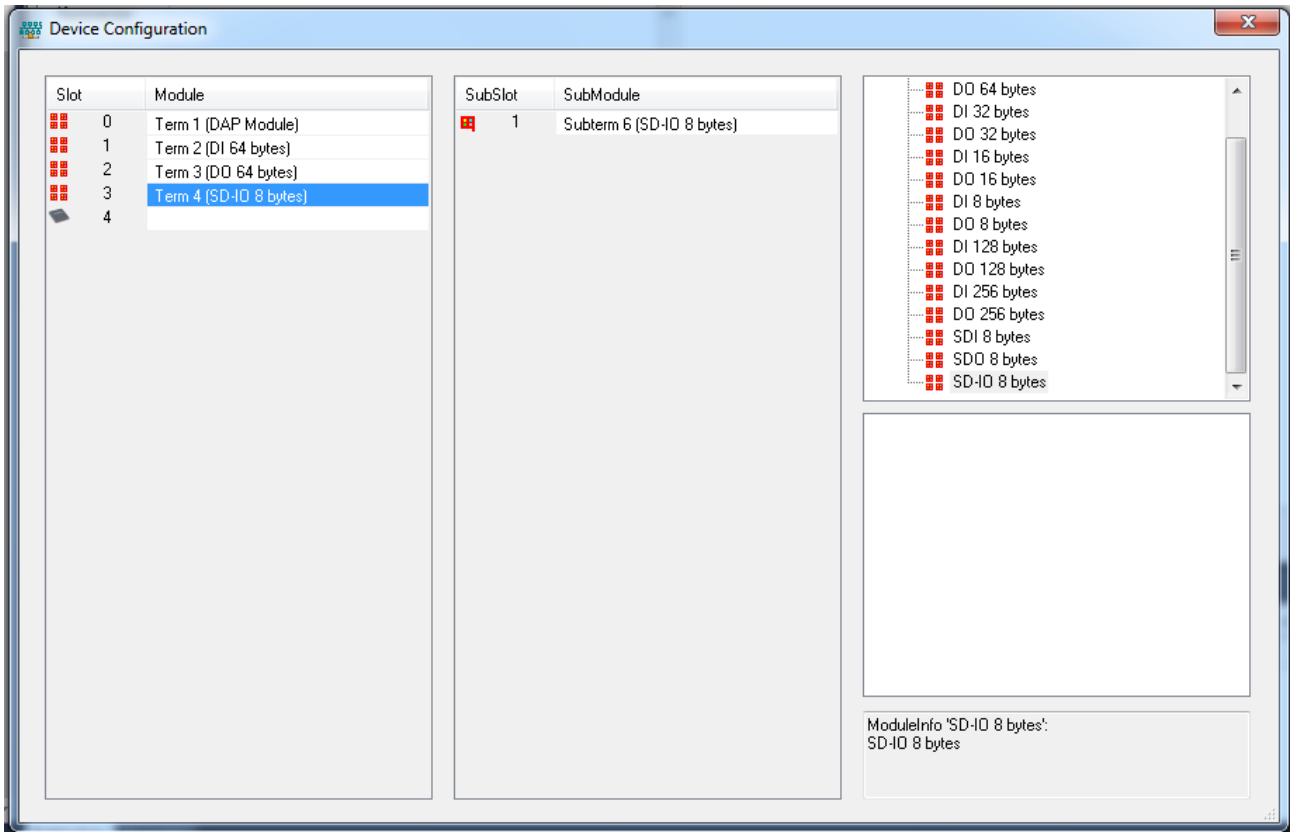
此外，通过添加一个 PROFInet I/O 控制器，可生成 PROFInet 网段的配置。



与 EtherCAT 网段的配置方式相同，PROFInet 控制器同样支持自动扫描或手动生成配置。通过这种方式，也可以手动添加 ABB 机器人。



设备配置必须通过 PROFIsafe 安全模块进行扩展。



要通过 PROFIsafe 成功使用 ABB 机器人，必须遵循以下信息说明。

⚠ 谨慎

数据类型 WORD!

当在过程映像中使用 WORD 数据类型时，可能需要进行额外配置。

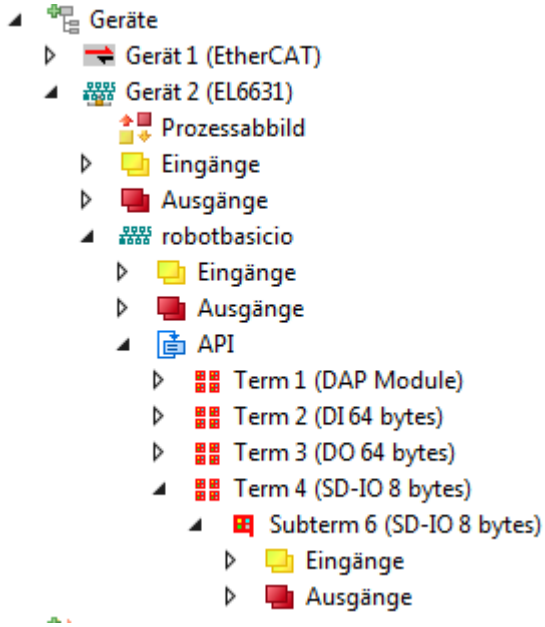
如果在配置中没有使用 EL9930 来限制 PROFIsafe 网段，则必须针对过程映像中包含 WORD 数据类型的信号，在 PROFIsafe 设备的 I/O 配置中配置高字节和低字节部分的交换。此操作可通过直接在数据值（在 *Flags*（标志）选项卡上）勾选 *Swap LOBYTE and HIBYTE*（交换 LOBYTE 和 HIBYTE）复选框来完成。

⚠ 谨慎

iParameters

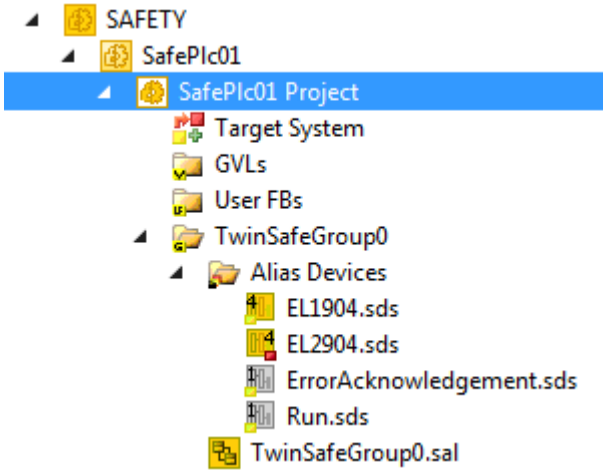
务必在 PROFIsafe I/O 设备上配置与 *Alias Device*（别名设备）完全相同的 iParameters，以便正确启动通信。

然后，您可以继续配置安全项目。此时，假定存在如下初始状况。

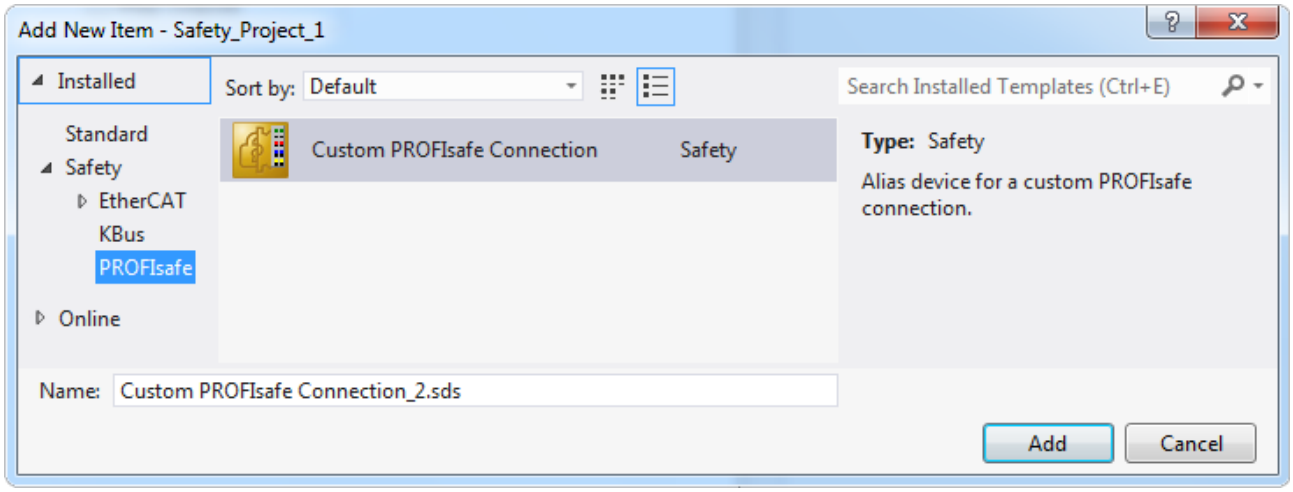


10.3.2.3 TwinCAT 安全项目连接的配置

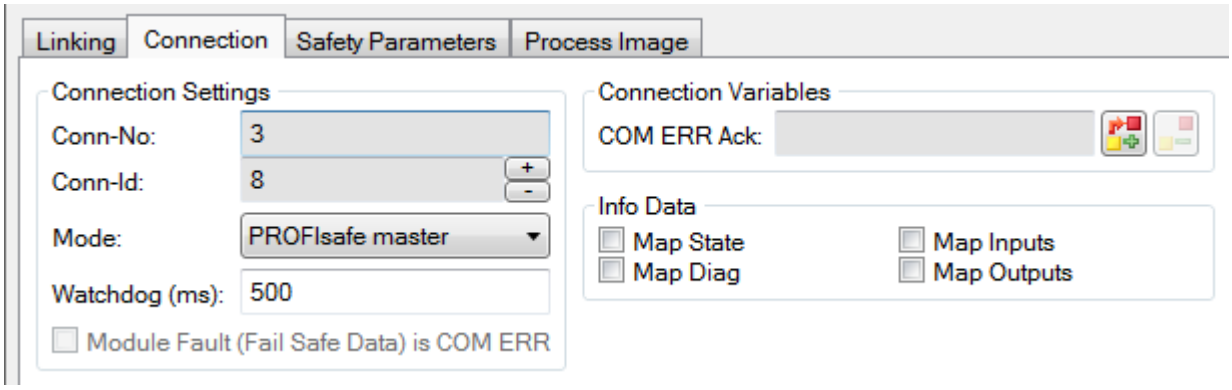
在配置 PROFIsafe 连接之前，首先要创建一个安全项目，并为可用的 EtherCAT 组件导入所需的别名设备。此外，目标系统还映射到 EtherCAT 网段的 EL6910（通过 *Target System*（目标系统）节点）。



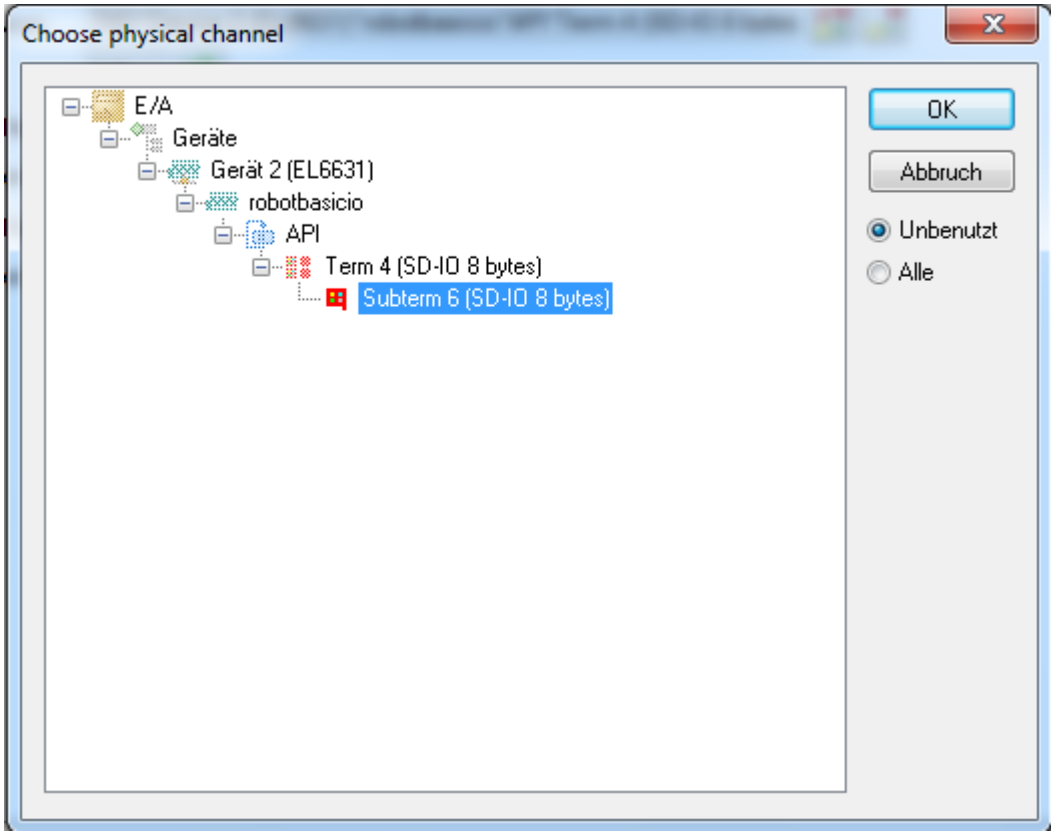
然后，您可以继续配置与 ABB 机器人的 PROFIsafe 连接。这种连接通常通过 *Alias Device*（别名设备）来实现。通过在 *Alias Devices*（别名设备）节点的上下文菜单中选择 *Add*（添加）和 New item…（新项目…），可以创建 *Custom PROFIsafe Connection*（自定义 PROFIsafe 连接）。



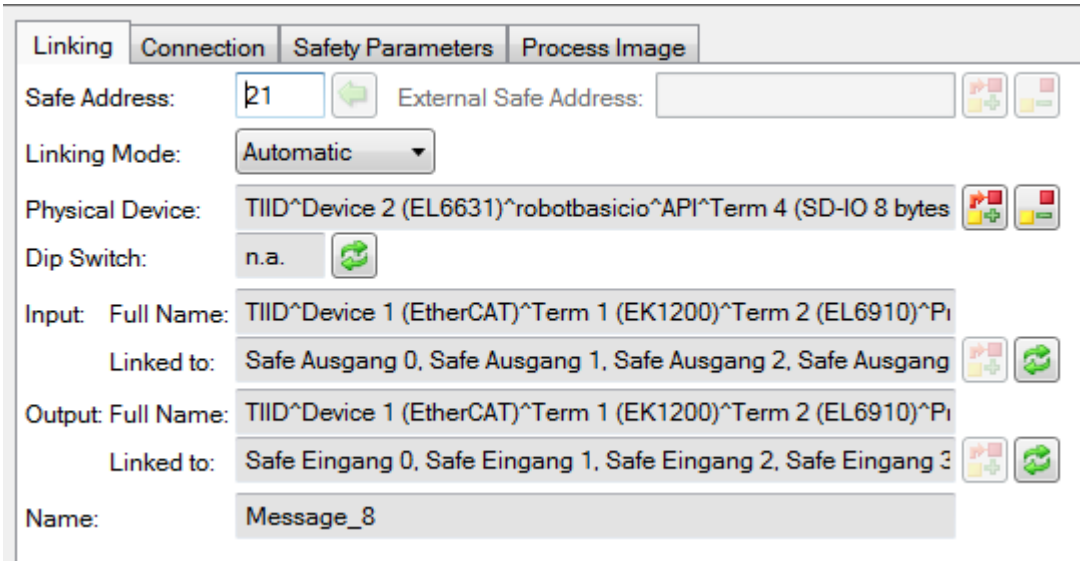
打开别名设备后，首先必须在 *Connection*（连接）选项卡上将 *PROFIsafe Master*（PROFIsafe 主站）选为连接模式和通信 Watchdog（看门狗）。



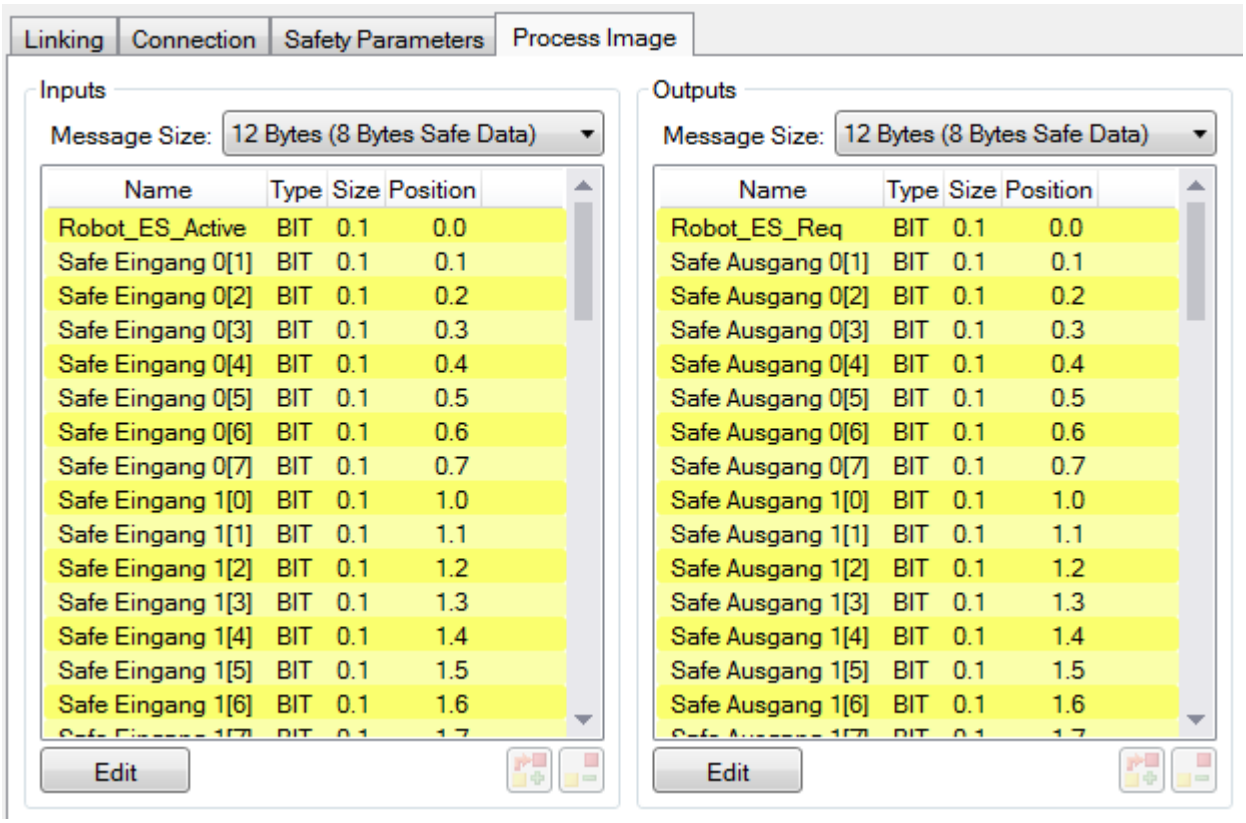
在 *Linking*（链接）选项卡上，链接模式必须被设置为 *Automatic*（自动），以便能够通过 *Map to Physical Device*（映射到物理设备）按钮选择此处考虑的 ABB 机器人。



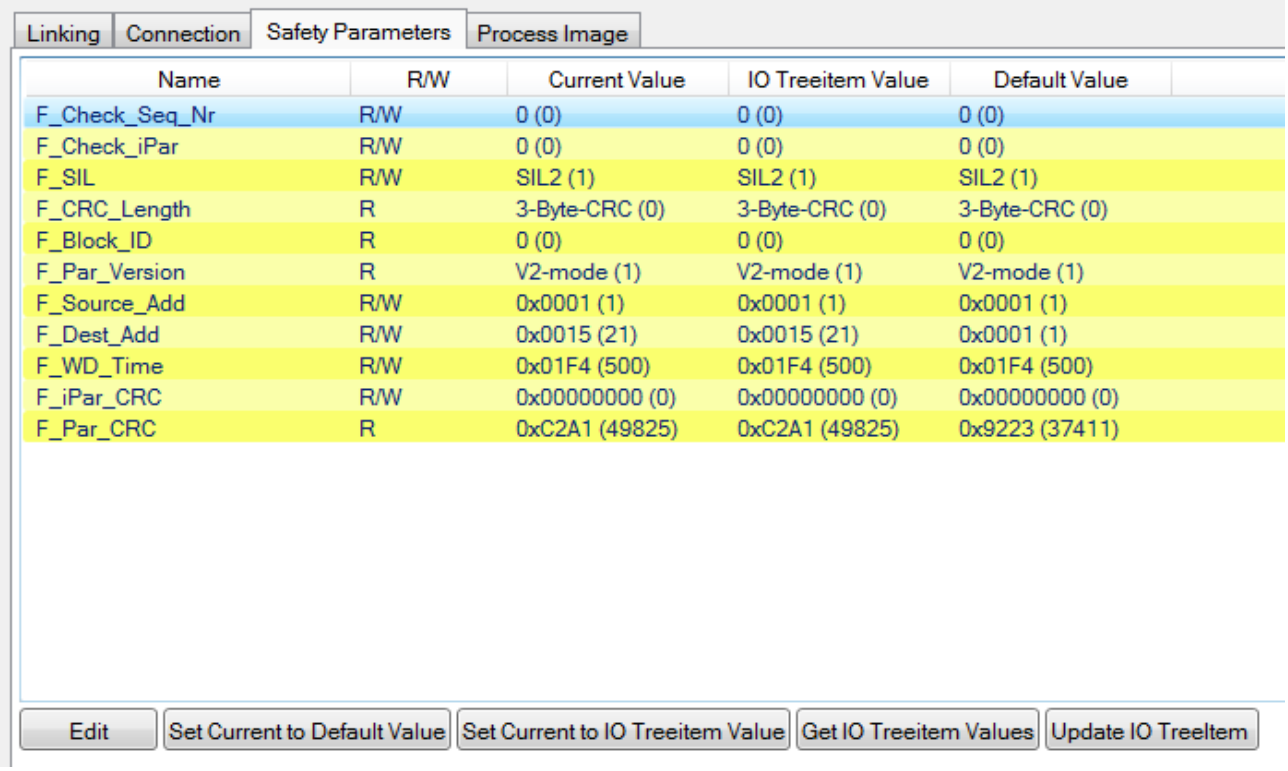
除了映射到物理设备外，还必须在 *Linking*（链接）选项卡上输入编码器的安全地址（在本例中为 21）。



如果所有设置均正确无误，则可在 *Process Image*（过程映像）选项卡上设置 ABB 机器人的安全过程映像，并根据机器人的应用工具中的设置进行编辑。



Safety Parameters（安全参数）选项卡提供了 PROFIsafe 主站连接的相关参数。如有必要，可通过 Edit（编辑）按钮根据具体应用调整相关值。



在此处必须正确设置 PROFIsafe 连接的所有参数。其中包括两个地址 F_Source_Add（目标系统）和 F_Dest_Add（PROFIsafe 设备的安全地址）。此外，还必须配置 *iParameters* 的 CRC。这可以从配置机器人的附加应用程序中获取（请参见*机器人配置*一节）

对于 PROFIsafe 设备，必须在别名设备内部和 I/O 配置中直接为设备设置参数。通过 *Safety Parameters*（安全参数）选项卡上的相应按钮可以启动从 I/O 设备读取数据和向 I/O 设备传输数据的操作。两处的数据必须一致，才能成功建立 PROFIsafe 连接。

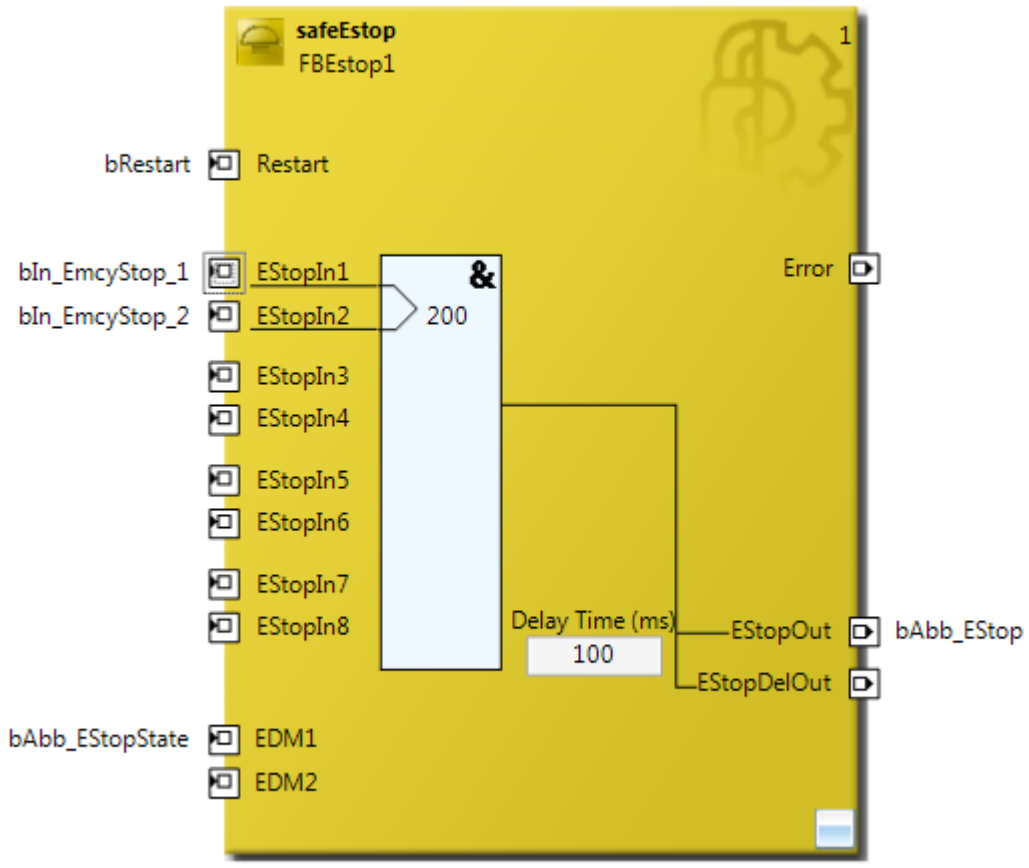
参数	描述
F_Check_Seq_Nr	设置（0/1）以指示是否应检查连接的序列号。
F_Check_iPar	设置（0/1）以指示是否应通过 iPar 服务器执行参数设置。
F_SIL	选择所需的 SIL 等级（SIL1、SIL2、SIL3、NoSIL）
F_CRC_Length	CRC 长度显示
F_Block_ID	始终为 0
F_Par_Version	使用的 PROFIsafe 版本（通常为 V2 模式）
F_Source_Add	设置 PROFIsafe 源地址
F_Dest_Add	设置 PROFIsafe 目标地址
F_WD_Time	设置 Watchdog（看门狗）时间
F_iPar_CRC	PROFIsafe 从站的 i-parameter(s)
F_Par_CRC	对所有参数计算得出的 CRC

完成参数配置后，必须点击 *Update IO TreeItem*（更新 IO 树项）按钮，最终将参数传输至 I/O 配置中。

完成连接配置后，您可以继续实施实际的安全功能。

10.3.2.4 实施 TwinCAT 安全项目

在本例所考虑的安全功能中，一个带有 2 个常闭触点的急停开关通过 EL1904 以双通道配置方式被安全读入。启动了对输入的测试。通过已启动差异监控的 safeEstop 功能块对输入进行评估。



如图所示，通过 PROFIsafe 控制 ABB 机器人的信号经由 *safeEstop* 功能块的 *EStopOut* 输出进行切换。ABB 机器人的反馈信号可用作 safeEstop 功能块的 *EDM* 输入。

10.3.3 安全输入端子模块的参数

EL1904

参数	值
传感器测试通道 1 激活	是
传感器测试通道 2 激活	是
传感器测试通道 3 激活	是
传感器测试通道 4 激活	是
逻辑通道 1 和 2	单逻辑
逻辑通道 3 和 4	单逻辑

10.3.4 功能块结构和安全回路

10.3.4.1 安全功能 1

就目前所述的应用示例而言，安全功能 1 考虑了从急停开关 S1 到 ABB 机器人的安全回路。

10.3.5 安全功能 1 的计算

10.3.5.1 PFHD / MTTFD / B10D – 值

组件	值
ABB 机器人，SafeMove 功能[1] – PFH_D、PL、$MTTF_D$、DC_{avg}	1.19E-07、PL d、52y、中等
EL1904 – PFH_D	1.11E-09
EL6910 – PFH_D	1.79E-09
S1 – $B10_D$	100,000
运行天数（d_{op}）	230
运行小时数/天（h_{op}）	16
循环时间（分钟）（T_{cycle}）	10080（每周 1 次）
使用寿命（T1）	20 年 = 175200 小时

[1] 请注意当前用户文档中提供的信息

10.3.5.2 诊断覆盖率 DC

组件	值
ABB 机器人，SAFEMove 功能[1]	DC_{avg}=90%
带测试/合理性检查的 S1	DC_{avg}=99%

[1] 请注意当前用户文档中提供的信息

10.3.5.3 安全功能 1 的计算

为了清晰起见，安全系数根据 EN 62061 和 EN ISO 13849-1 标准进行计算。在实际应用中，根据其中一项标准进行计算已足够。

根据 $B10_D$ 值计算 PFH_D 和 $MTTF_D$ 值：

从：

$$n_{op} = \frac{d_{op} * h_{op} * 60}{T_{Zyklus}}$$

和：

$$MTTF_D = \frac{B10_D}{0{,}1 * n_{op}}$$

得出

$$PFH = \frac{0{,}1 * n_{op} * (1 - DC)}{B10_D} = \frac{1 - DC}{MTTF_D}$$

插入值后，可得：

S1：

$$n_{op} = \frac{230*16*60}{10080} = 21,90$$

$$MTTF_D = \frac{100.000}{0,1*21,90} = 45662,1y = 399999120h$$

并假设 S1 为单通道：

S1：每周执行 1 次，直接回读

$$PFH = \frac{1-0,99}{45662,1*8760} = 2,50E-11$$

由此，安全功能 1 的 PFH_D 值计算如下

$$PFH_{ges} = PFH_{(S1)} + PFH_{(EL1904)} + PFH_{(EL6910)} + PFH_{(Roboter)}$$

$$PFH_{ges} = 2,5E-11+1,11E-9+1,79E-9+1,19E-7 = 1,22E-7$$

根据 EN 13849 标准，安全功能 1 的 $MTTF_D$ 值按以下公式计算：

$$\frac{1}{MTTF_{Dges}} = \sum_{i=1}^{n} \frac{1}{MTTF_{Dn}}$$

至：

$$\frac{1}{MTTF_{Dges}} = \frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(Roboter)}}$$

及：

如果仅有 EL1904 和 EL6910 的 PFH_D 值可用，则适用以下估算方法：

$$MTTF_{d(x)} = \frac{(1-DC(x))}{PFH(x)}$$

因此：

$$MTTF_{D(EL1904)} = \frac{(1-DC_{(EL1904)})}{PFH_{(EL1904)}} = \frac{(1-0,99)}{1,11E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{9,72E-06\frac{1}{y}} = 1028,8y$$

$$MTTF_{D(EL6910)} = \frac{(1-DC_{(EL6910)})}{PFH_{(EL6910)}} = \frac{(1-0,99)}{1,79E-09\frac{1}{h}*8760\frac{h}{y}} = \frac{0,01}{15,68E-06\frac{1}{y}} = 637y$$

机器人的值可从当前用户文档中获取：

$$MTTF_{D(Roboter)} = 52y$$

$$MTTF_{Dges} = \frac{1}{\frac{1}{45662,1y} + \frac{1}{1028,8y} + \frac{1}{637y} + \frac{1}{52y}} = 45,88y$$

$$DC_{avg} = \frac{\frac{DC}{MTTF_{D(S1)}} + \frac{DC}{MTTF_{D(EL1904)}} + \frac{DC}{MTTF_{D(EL6910)}} + \frac{DC}{MTTF_{D(Roboter)}}}{\frac{1}{MTTF_{D(S1)}} + \frac{1}{MTTF_{D(EL1904)}} + \frac{1}{MTTF_{D(EL6910)}} + \frac{1}{MTTF_{D(Roboter)}}}$$

$$DC_{avg} = \frac{\frac{99\%}{45662{,}1y} + \frac{99\%}{1028{,}8y} + \frac{99\%}{637y} + \frac{90\%}{52y}}{\frac{1}{45662{,}1y} + \frac{1}{1028{,}8y} + \frac{1}{637y} + \frac{1}{52y}} = 91\%$$

⚠ 谨慎

在设备中实施重启锁定功能！

重启锁定功能不属于安全链的组成部分，必须在设备中独立实施！

注意

类别

根据所使用机器人的安全数据，这种结构最多能达到类别 3。

$MTTF_D$	
每个通道的标识	**每个通道的范围**
低	3 年 ⩽ $MTTF_D$ < 10 年
中等	10 年 ⩽ $MTTF_D$ < 30 年
高	**30 年 ⩽ $MTTF_D$ ⩽ 100 年**

DC	
名称	**区域**
无	DC < 60%
低	60% ⩽ DC < 90%
中等	**90% ⩽ DC < 99%**
高	99% ⩽ DC

注意

诊断覆盖率

为了确保实际可用性，范围的数量被限制为 4 个。假定本表格中所示限值的精度为 5%。

Category	B	1	2	2	3	3	4
DC / $MTTF_D$	none	none	low	medium	low	medium	high
low	a	-	a	b	b	c	-
medium	b	-	b	c	c	d	-
high	-	c	c	d	d	d	e

1 使用 TwinSAFE 组件规划安全项目

1

本章概述了使用 TwinSAFE 组件进行安全项目规划的一般流程。

⚠ 谨慎

机械指令

本说明仅适用于机械指令所定义的设备。

⚠ 谨慎

标准

用户必须能够获取相关标准。以下说明不能取代标准。通常情况下，至少应提供当前版本的 EN ISO 13849-1 和 EN ISO 13849-2 或 EN 62061 标准。有关更多有用信息，请参见 IFA 报告 2/2017。

注意

C 类标准

在启动后续流程前，您应该检查是否存在适用于您的设备的 C 类标准。如果存在此类标准，请遵循其中规定的步骤和说明进行操作。如果没有适用的 C 类标准，您可以将下文所述流程用作操作步骤指南。

11.1 识别风险和危害

DIN EN ISO 12100 标准定义了一套*迭代流程，旨在最大限度降低风险*、消除危害或减少设备风险。它通过三步法阐述了最大限度降低风险的流程。第一步，设备应通过设计实现本质安全。如果做不到这一点，可以采取技术防护措施将风险降到最低。最后一步，可以提供有关残余风险的用户信息。

第一步，必须识别风险、危害以及相应的安全功能。设备制造商需要精确了解其设备的运行情况，以便识别各种风险和危害。为此，请参考 EN ISO 12100:2010 标准的附录 B。

此类风险和危害分析应由具备不同领域知识（机械、电气、液压、软件、维护.....）的人员共同完成。务必考虑到所有运行模式和条件，包括调试、维护/保养、正常运行以及拆卸和报废。支持或反对某项决定的理由也应记录在案。确保您的论点和理由清晰易懂且具有说服力。

在这种情况下，尤其需要注意的是，在评估风险时不得预先考虑安全措施。

当所有参与流程的人员对分析结果达成一致后，全体相关人员应签名。

11.2 确定 PLr / SIL

对于风险和危害分析中识别出的每项设备安全功能（SF），设备制造商或用户必须确定所需的性能等级或 SIL 等级。
SIL 等级根据 EN 62061 标准附录 A 中的描述进行确定
性能等级根据 EN ISO 13849-1 标准中用于确定 PL_r 的风险图进行确定。有关风险图的信息，请参见 EN ISO 13849-1:2015 标准的附录 A。

11.3 安全功能的规范

对于已识别的每项安全功能，必须根据 EN ISO 12100 标准的*风险降低策略*明确降低风险的具体实施方式。

务必明确需通过本质安全设计或用户信息来降低残余风险的风险和危害，但此类措施不属本文档描述范畴。以下说明仅涉及安全功能，应通过技术防护措施来降低其残余风险。

对于这些安全功能，将根据 EN ISO 13849-1:2015 标准执行*控制系统的安全相关部分（SRP/CS）的迭代设计流程*。

11.4 措施的规范

设备制造商应详细描述每项已识别的安全功能（SF），并通过技术防护措施降低其残余风险。该说明包含有关危害、为减少危害而采取的措施类型以及该安全功能所需的性能等级或 SIL 等级的信息。

对于每项 SF，措施说明必须包含根据 EN ISO 13849-1 标准确定的类别、要使用的组件，以及它们的安全参数（$MTTF_D$、DC、CCF、SFF）。

需要提供关于运行状态与特性的信息。其中包括运行模式、循环时间、响应时间或过程安全时间、环境条件、执行频率、运行时间、失能情况下的设备行为以及其他相关参数。有关这方面的更多详细信息，请参见 EN 62061 标准第 5.2 章以及 EN ISO 13849-1:2015 标准第 5 章。

设备制造商必须对 TwinSAFE 逻辑中的安全相关程序进行明确规定并记录在案，因为这是实现安全功能的基础。除了选择 TwinSAFE 组件、要使用的功能块以及传感器和执行器之外，还必须规定组件的参数设置，因为这可能会影响可达到的最高性能等级。

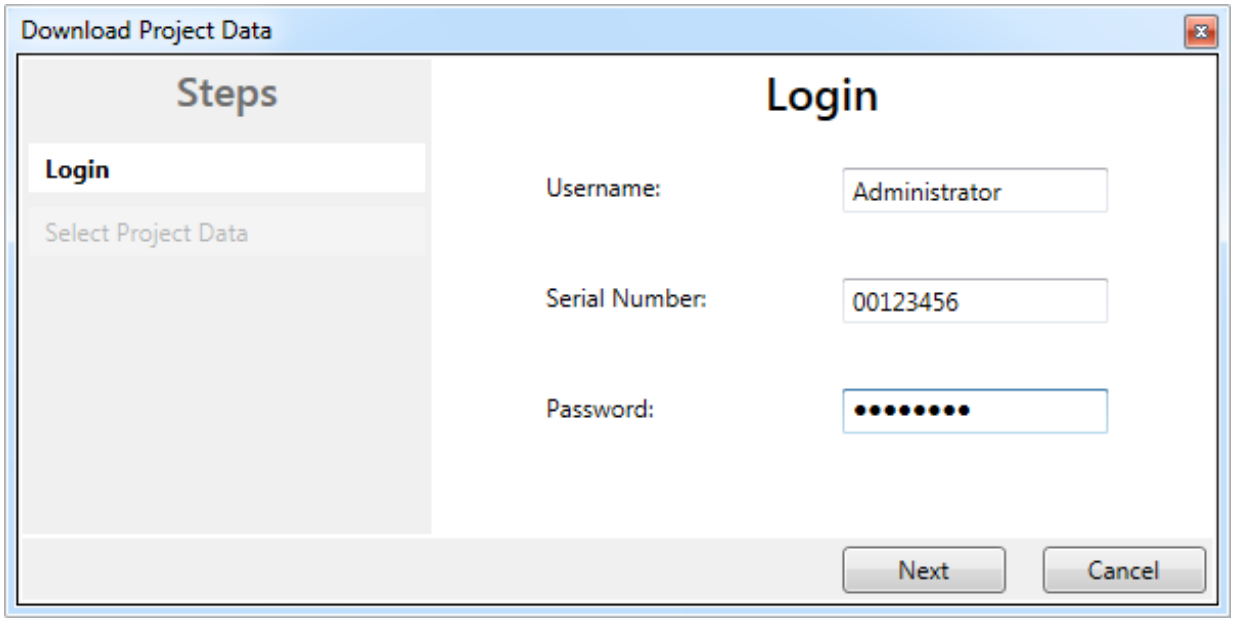
有关安全功能的实施示例和 TwinSAFE 组件的参数设置示例，请参见本手册。

11.5 安全功能的实施

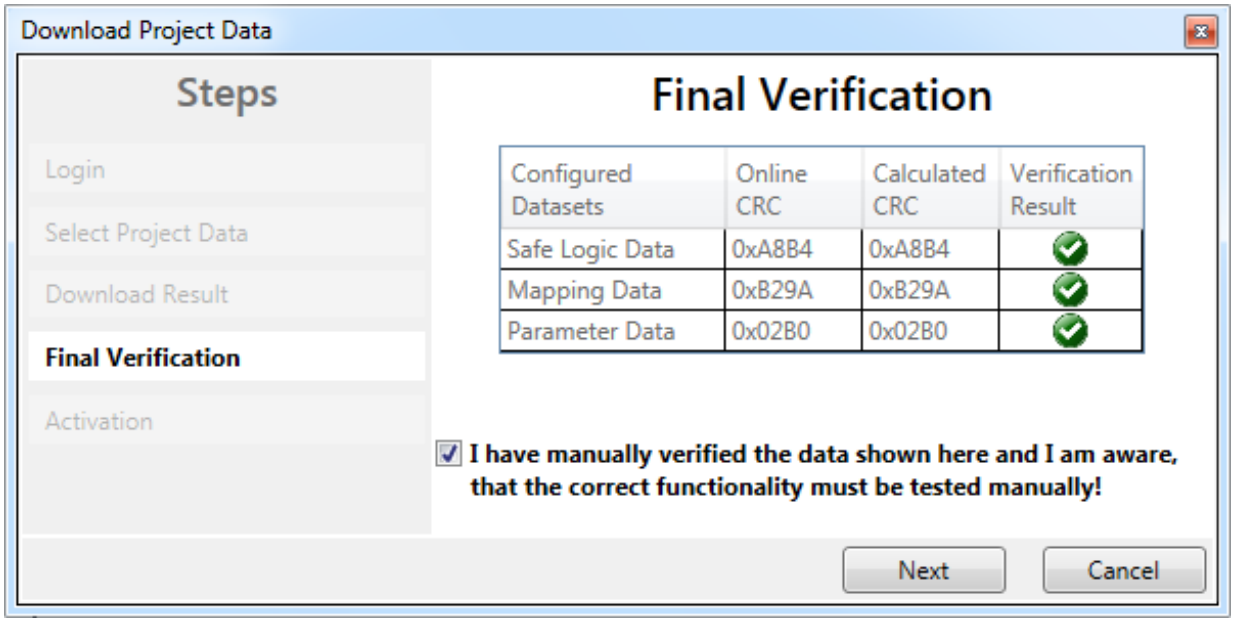
功能块在 TwinCAT 中根据已明确规定的安全功能进行配置。预定义功能块可用于典型的安全功能，用户可以在图形编辑器中对其进行互联配置。安全输入和输出组件为传感器和执行器提供接口。

当完整的安全逻辑以及安全输入和输出的参数设置全部实现后，即可将程序下载至 TwinSAFE 逻辑。

下载时必须提供有效的用户名和密码，以及设备的序列号。



通过比较加载项目的 CRC（在线 CRC）和安全编辑器计算出的 CRC（离线 CRC）可以验证安全程序的下载情况。一方面由 TwinCAT 进行比较，另一方面由用户进行比较。用户通过勾选复选框并重新输入密码来确认比较结果。



用户可以随时使用 TwinCAT 中的安全 CRC 工具栏来检查在线 CRC 是否与离线 CRC 相匹配，即在编辑器中或在 TwinSAFE 逻辑上是否已更改数据。下表摘自 EL6910 文档。

Icon	Name	Description
CRCs:	CRC Toolbar	Left-click on the toolbar to initiate an update of the CRCs by the user. Red icon: CRCs are different
CRCs:	CRC Toolbar	Green icon: All CRCs are identical
0x9135 | 0x9135 | 0x9135	Online CRC	CRC of the safety project on the EL6910. This value is read online by the terminal. In the absence of an ADS connection to the EL6910, this value is displayed with 0x---- .
0x9135 | 0x9135 | 0x9135	Downloaded CRC	CRC of the safety project that was loaded last. If no safety project is loaded when the TwinCAT project is opened, the value is displayed with 0x---- .
0x9135 | 0x9135 | 0x9135	Offline CRC	CRC of the current safety project, as stored in the safety editor. A CRC is displayed, if the stored project is valid. If the project is invalid, 0x---- is displayed as CRC.

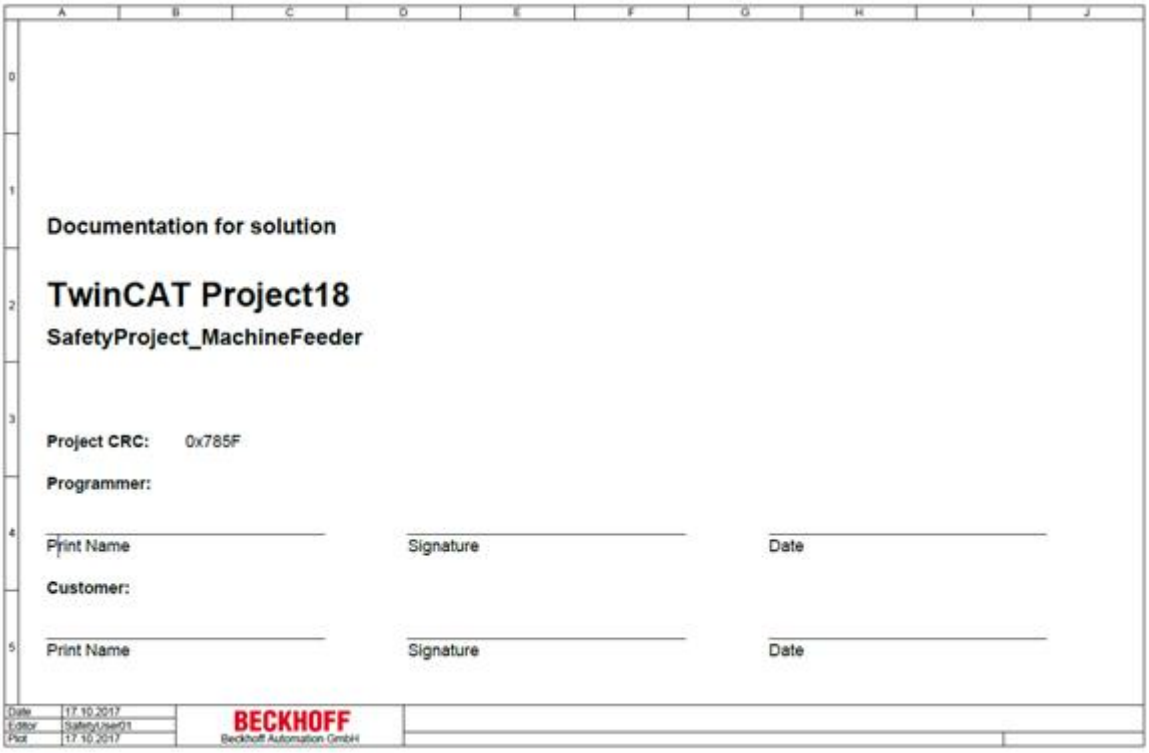
⚠ 谨慎

检查校验和

用户必须验证在线 CRC 和离线 CRC 是否相匹配。这是确保在创建或修改项目后进行下载的唯一方法。

当所有指定的安全功能均在 TwinSAFE 逻辑中实现后，需将已实现的逻辑打印输出。

除了完整的逻辑、参数以及所有已用安全组件的安全地址之外，打印文件还包含计算得出的项目校验和，该校验和在封面页显示。程序员和客户可以在封面页上记录安全功能的验收日期和签名。


Documentation for solution

TwinCAT Project18

SafetyProject_MachineFeeder

Project CRC: 0x785F

Programmer:

Print Name Signature Date

Customer:

Print Name Signature Date

BECKHOFF

11.6 达到性能等级的证明

当针对已识别安全功能（SF）的安全项目实现后，需计算并验证这些安全功能所达到的性能等级。有关此类计算和验证的示例，请参见本手册第 2 章。

11.7 安全功能的验证

摘自 EN ISO 13849-2:2013 标准，第 4.1 章：验证指南。

尽管 EN ISO 13849-2:2013 中仍引用 EN ISO 13849-1:2006，但引用的章节已更改为 EN ISO 13849-1:2015 的章节编号。

验证程序的目的是确认控制系统的安全相关部分（SRP/CS）的设计支持设备安全要求的规范。

验证工作必须证明每个 SRP/CS 均符合 EN ISO 13849-1:2015 标准的要求，特别在以下方面：

a) 安全功能的特定安全特性，符合设计预期；
b) 特定性能等级的要求（请参见 EN ISO 13849-1:2015 标准，第 4.5 章）：
   1. 特定类别的要求（请参见 EN ISO 13849-1:2015 标准，第 6.2 章），
   2. 控制和避免系统故障的措施（请参见 EN ISO 13849-1:2015 标准，附录 G），
   3. 软件要求（如适用）（请参见 EN ISO 13849-1:2015 标准，第 4.6 章），以及
   4. 在预期条件下提供安全功能的能力；
c) 用户界面的人体工学设计，例如阻止用户通过规避 SRP/CS 以危险的方式行事（请参见 EN ISO 13849-1:2015 标准，第 4.8 章）。

验证工作应由未参与 SRP/CS 设计的人员执行。

注意 “独立人员”并不一定指必须由第三方进行测试。

有关验证的更多信息，请参见 EN ISO 13849-2:2013 标准（例如图 1，*验证程序概述*）和 EN ISO 13849-1:2015 标准。

11.8 检查 SF 的说明

所有已实现的安全功能（SF）均须进行正确性检查。这包括正常运行状态及故障发生时的功能表现。其中一些测试用例可从已定义的安全功能及其所述的最大限度降低风险的措施中读取。对于每项功能，必须定义可能出现的故障情况，并进行相应的检查。此类信息必须记录在测试规范或验收规程中。

- 下文列出了一些需要考虑的故障情况：
- 两个安全输入的差异错误
- 所用现场总线的线路中断
- 执行器的反馈（EDM）错误
- 电源故障
- 接线中的交叉回路/外部馈电/线路中断
- 超出定义的限值（例如：轴功能的速度限值），并检查定义的错误行为
- ...

验证工作还须确保风险评估已识别的所有危害都有适当的措施加以应对，而且这些措施已得到切实执行。

这尤其适用于安装/装配和维护等生命周期阶段。务必确保只有在通知设计工程师（设备制造商）并由制造商更改安全规范后，才能对安全项目进行任何必要的更改或扩展。此外，还必须进行检查，以确认测试规范是否需要扩展。这尤其适用于在最终客户处装配并投入使用的设备。

测试必须至少涵盖以下几个要点：

- 安全输入和输出的 I/O 检查
- 验证所有安全组件的参数设置（Watchdog（看门狗）时间、传感器测试、FSoE 地址等）
- 检查正常运行时的安全功能
- 检查发生错误时的安全功能
- 检查正常运行时的安全驱动功能

- 在规定的安全限值之外，检查安全驱动功能
- 检查发生断电时的安全驱动功能
- ...

11.9 接受

以下列表包含安全项目验收所需的要点。但无法详尽无遗地列举。这些要点必须在 TwinSAFE 项目首次启动后以及每次软件修改后进行检查。

- 只能由具备相应资质的人员实施或更改
- TwinSAFE 项目的打印输出
- 根据前一章的内容，对整个安全项目进行正确性检查
- 比较 TwinSAFE 项目的在线 CRC 与离线 CRC，以确保在修改安全项目后已执行下载
- 打印验收规程的实施和打印输出
- 程序员和客户签名
- 这些信息应添加到设备文档中
- ...

1 技术报告 – TÜV SÜD
2

KONFORMITÄTSBESTÄTIGUNG
LETTER OF CONFIRMATION

Rail

BV89987T

Applikationshandbuch TwinSAFE
(Application guide TwinSAFE)

Hersteller: Manufacturer:	Prüfstelle: Test body:
Beckhoff Automation GmbH & Co. KG Huelshorstweg 20 D-33415 Verl	TÜV SÜD RAIL GmbH Rail Automation Barthstr. 16 D-80339 München

1. Allgemein / General

Das **"Applikationshandbuch TwinSAFE"** zeigt die Berechnungen der sicherheitsrelevanten Kennwerte bezüglich der Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle (MTTFd und PFH) nach EN 61508 bzw. EN ISO 13849-1.

The **"Application guide TwinSAFE"** shows calculations of the safety relevant parameters of the probability of dangerous random hardware failures (MTTFd and PFH) according to EN 61508 respectively EN ISO 13849-1.

2. Prüfgrundlagen / Test bases

Berechnung des $MTTF_d$ und DC entsprechend EN ISO 13849-1:2015 Calculation of $MTTF_d$ and DC in accordance with EN ISO 13849-1:2015
Berechnung des PFH entsprechend EN 61508:2010 Calculation of PFH in accordance with EN 61508:2010
Applikationshandbuch TwinSAFE Version 3.5.0 Application guide TwinSAFE version 3.5.0

3. Zusammenfassung / Summary

Die Applikationsbeispiele des "Applikationshandbuch TwinSAFE" der Firma Beckhoff Automation GmbH & Co. KG wurden von der TÜV SÜD Rail GmbH, Rail Automation, überprüft und bestätigt.

The application examples in the "Application guide TwinSAFE" were checked and confirmed by TÜV SÜD Rail GmbH, Rail Automation.

TÜV SÜD Rail GmbH
2024-12-06
1093478910
2024.12.09
09:38:02
+01'00'

G. Greil
Technical Certifier

Digital unterschrieben von Franz Seika
Datum: 2024.12.06
14:59:57 +01'00'

F. Seika
Project Leader

Diese Bestätigung wurde auf Grundlage einer TÜV-internen technischen Beurteilung erstellt.
Diese enthält das Ergebnis einer einmaligen Untersuchung an dem zur Prüfung vorgelegten Erzeugnis.

This confirmation was created on basis of a TÜV internal technical review report.
It includes the result of a one-time examination of the product submitted for examination.

附图 3: TÜV SÜD 确认函

Trademark statements

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® and XTS® are registered and licensed trademarks of Beckhoff Automation GmbH.

Third-party trademark statements

EnDat is a trademark of Dr. Johannes Heidenhain GmbH.

IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.

更多信息:
www.beckhoff.com/TwinSAFE

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
电话号码: +49 5246 9630
info@beckhoff.com
www.beckhoff.com