# Technology CPU 317TF-2 DP：根据 IEC 62061 确定安全完整性等级 (SIL) 的示例

Technology CPU

应用说明 • 2012 年 1 月

应用与工具

工业解决之道！

SIEMENS

西门子工业自动化与驱动集团服务及支持门户

本文摘自西门子有限公司工业自动化与驱动集团的服务门户网站。通过以下链接，用户可以直接访问本文的下载页面：

http://support.automation.siemens.com/WW/view/en/47393794

注意

本文所述的功能与解决方案仅限于主要自动化任务的实现。此外，如需将设备连接至工厂其它部分、企业网络或者因特网，请务必考虑在工业安全的范围内采取必要的保护性措施。欲了解更多信息，请参考编号为 50203404 的文档。

http://support.automation.siemens.com/WW/view/en/50203404

关于本文档，如果存在任何疑问，请通过以下电子邮箱联系我们：

mailto:online-support.industry@siemens.com

您也可以主动使用服务和支持门户网站上关于本主题的技术论坛。添加您的问题、建议和问题并在我们强大的论坛社区中一起讨论它们：

http://www.siemens.com/forum-applications

西门子

# SIMATIC
# 根据 IEC 62061 确定安全完整性等级 (SIL)

Technology CPU 317TF-2 DP

# 担保与责任

请注意

应用示例并不完备，也不局限于所示的组态、设备以及任何突发事件。这些应用示例并不代表特定于客户的解决方案。它们仅为典型的应用提供支持。您有责任确保所述的产品得到正确的使用。这些应用示例并不会免除您安全而专业地使用、安装、操作以及维修本设备的责任。当实施这些应用示例时，您应当意识到，西门子并不会对超出本责任条款的任何损害/索赔负责。我们保留了随时对本应用示例作出更改而不作事先通知的权力。如果这些应用示例中所提供的建议与其它西门子出版物——比如产品目录——出现偏差的话，以其它文档中的内容为准。

我们不对本文档中所包含的信息承担任何责任。

无论根据任何合法原因，对于本应用示例中的例子、信息、程序、设计以及性能数据等的使用而引起的索赔，我们一概不予接受。此类除外责任不适用于强制责任，比如德国产品责任法的约束，在故意、重大过失的情况，或者导致生命、身体与健康受损，产品的质量保证，欺诈性隐瞒缺陷，以及违反合同根基的情况。然而，对于违反合同根基条件而引起的索赔，应当限制在合同固有的可预见的损失范围内，除非是索赔是由于故意重大过失，或者伤害生命、身体和健康等强制性责任而导致。上述规定并不意味着您的损害举证负担发生变化。

# 前言

### 本应用文档的目标

本文档将通过应用示例，介绍如何利用安全评估工具 (SET) 来确定 Technology CPU 317TF-2 DP 应用的安全完整性等级 (SIL) 是否符合 IEC 62061 的要求。

### 本应用文档的核心内容

以下是本应用文档所讨论的主要内容：

- 介绍用于确定安全完整性等级 (SIL) 的应用示例。
- 确认本应用示例所需的安全功能 (SRCF)。
- 利用安全评估工具 (SET) 来确定所要求的安全完整性等级 (SIL)。
- 设计并实现所开发的安全功能 (SRCF)。
- 利用安全评估工具 (SET) 来确定所达到的安全完整性等级 (SIL)。

**请注意**

安全完整性等级确定是基于下述关于使用 IEC 62061 标准的文档来执行的：

**应用示例**
“Practical application of the IEC 62061, illustrated using an application example with SIMATIC S7 Distributed Safety（通过 SIMATIC S7 Distributed Safety 应用示例来讲解 IEC 62061 的实际应用）”

互联网链接：http://support.automation.siemens.com/WW/view/en/23996473



### 适用范围

本文档主要介绍 Technology CPU 317TF-2 DP 的使用步骤，但也适用于一般的故障安全 SIMATIC-CPU。

### 安全评估工具 (SET) 的显示画面

本文档的 PDF 版本中示出了安全评估工具 (SET) 的显示画面（高分辨率）。 为了查看该显示画面的细节内容，请使用 PDF 阅读器的缩放功能。

对于本文档的印刷版本，可从本应用示例的下载页面上下载到可用的安全评估工具 (SET) 项目文件。 利用该项目文件，可以直接在安全评估工具 (SET) 中查看显示画面。

# 目录

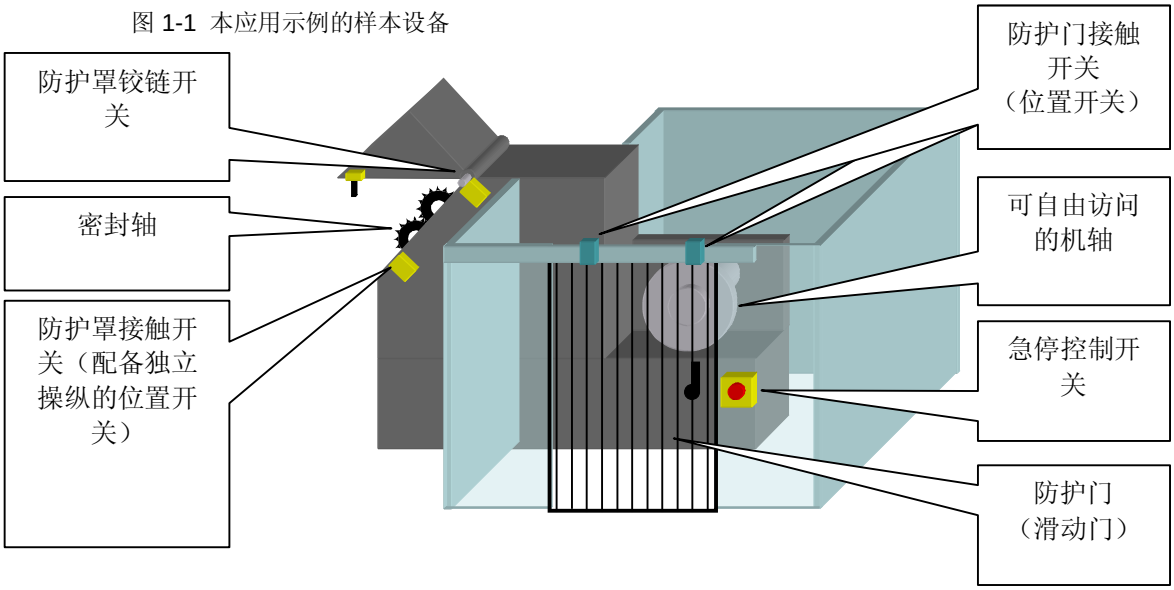
# 1 应用示例

## 1.1 本应用示例中的问题界定

设备器中包含有两根相互独立的机轴。 这些机轴可通过 Technology CPU 317TF-2 DP 进行控制。 其中的封闭机轴位于设备的防护罩下方。另一根暴露机轴则位于操作员可自由进入的位置。应当在设备的这一危险区域周围设置防护栏，工作人员须通过带有接触开关保护的防护门（滑动门）才能进入该区域。封闭机轴的防护罩可通过防护罩铰链开关以及防护罩接触开关来监测和控制。

利用防护栏外的急停控制开关，可安全地停止这两根机轴。

图 1-1 本应用示例的样本设备




下述是需要在该设备上实现的安全功能：

- **安全功能 1 (SF 1)：安全限制速度**
  如果防护门在设备运行过程中打开，那么暴露机轴必须运行在安全限制速度下。为此，须使用 SINAMICS S120 的 *Safely-Limited Speed（安全限制速度，SLS）*安全功能。
- **安全功能 2 (SF 2)：安全停止所有机轴**
  如果设备上的封闭机轴防护罩打开，则两根机轴都必须停止。为此，须使用 SINAMICS S120 的 *Safe Stop 1（安全停止 1，SS1）*安全功能。
- **安全功能 3 (SF 3)：紧急停止所有机轴**
  一旦按下紧急停止按钮，两根机轴均会停止工作。为此，须使用 SINAMICS S120 的 *Safe Torque Off （转矩安全关闭，STO）*安全功能。

**请注意**

急停控制开关是根据 2006/42/EG 设备指南 1.2.4.3 章节而提供的一项普遍要求的补充安全功能，这类常规要求并不包含在本文档所述的安全相关控制功能的讨论范围之内。

为了阐明安全等级的确定步骤，本文档会将急停控制开关的功能考虑在内。

## 1.2 本应用示例中的解决方案概览

以下是本应用示例任务的解决方案中所采用的假定：

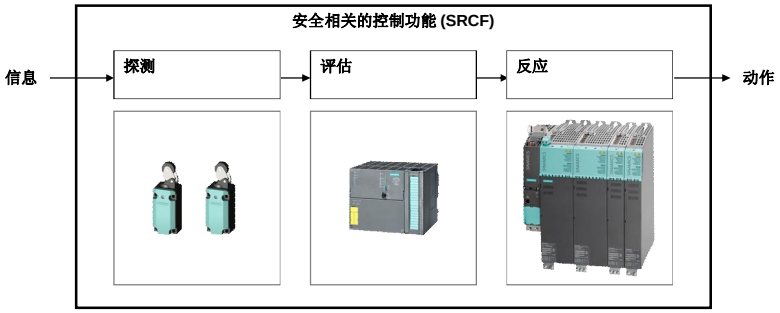
安全功能 (SF 1 / SF 2 / SF 3) 由安全相关的控制功能 (SRCF 1 / SRCF 2 / SRCF 3) 来实现。

### 1.2.1 安全相关的控制功能 1 (SRCF 1)

将暴露机轴转速降低为安全速度。

- 该 SRCF 的标识名称：
  “机轴速度的安全减速”
- 该 SRCF 的功能：
  当防护门打开时，设备上的暴露机轴转速将会降低至给定的安全速度，并可通过 SINAMICS S120 的 Safely-Limited Speed (安全限制速度，SLS) 安全功能来进行监测。
- 根据风险分析（参见章节 3.2.1 ），所要求的 SRCF 安全完整性等级 (SIL) 为：SIL 2

图 1-2 SRCF 1 可能的实现方法



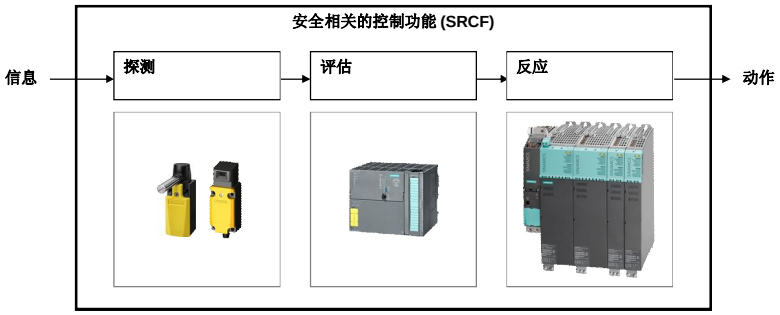

### 1.2.2 安全相关的控制功能 2 (SRCF 2)

当打开设备上的封闭机轴防护罩时，关停两根机轴：

- 该 SRCF 的标识名称：
  “机轴的安全停止”
- 该 SRCF 的功能：
  当打开防护罩时，利用 SINAMICS S120 的 *Safe Stop 1（安全停止 1，SS1）*，安全功能来停止两根机轴。

- 根据风险分析（参见章节 0），所要求的 SRCF 安全完整性等级 (SIL) 为：
  SIL 2

图 1-3 SRCF 2 可能的实现方法

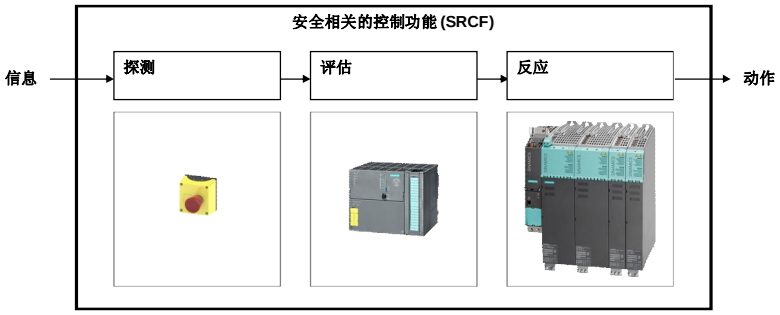



### 1.2.3 安全相关的控制功能 3 (SRCF 3)

当按下设备上的急停控制开关之后，两根机轴均会紧急停止：

- 该 SRCF 的标识名称：
  “机轴的紧急停止”
- 该 SRCF 的功能：
  按下急停控制开关之后，将利用 SINAMICS S120 的 *Safe Torque Off （转矩安全关闭，STO*）安全功能来停止两根机轴。
- 根据安全相关控制功能的评定（参见章节 0），所要求的 SRCF 安全完整性等级 (SIL) 为：
  SIL 2

图 1-4 SRCF 3 可能的实现方法



## 1.2.4 安全系统 (SRECS)

用于执行安全相关控制功能 (SRCF 1, SRCF 2 以及 SRCF 3) 的安全系统 (SRECS) 由五个子系统所组成：

表 1-1 安全系统 (SRECS) 的子系统

| 子系统 | 需要执行的功能 | 组件 |
|---|---|---|
| 子系统 1 | SRCF 1：“Detection（检测）”<br>利用两个位置开关开监测防护门的状态 | SIRIUS |
| 子系统 2 | SRCF 2：“Detection（检测）”<br>利用铰链开关和配备独立操纵的位置开关来监测防护罩的状态。 | SIRIUS |
| 子系统 3 | SRCF 3：“Detection（检测）”<br>监测用于停止所有机轴的急停控制开关的状态 | SIRIUS |
| 子系统 4 | SRCF 1 / SRCF 2 / SRCF 3：“评估”<br>处理故障安全控制器 (F-PLC) 中的信号 | SIMATIC S7 Distributed Safety |
| 子系统 5 | SRCF 1 / SRCF 2 / SRCF 3：“反应”<br>• 执行驱动器内部的 *Safely-Limited Speed（安全限制速度，SLS）* 安全功能。<br>• 执行驱动器内部的 *Safe Stop 1（安全停止，SS1）* 安全功能。 | SINAMICS |

图 1-5 安全系统 (SRECS)


子系统 1、2、3 为设计子系统；子系统 4 和 5 是预制子系统。

# 2 SET 的应用

## 2.1 基本介绍

### 2.1.1 安全评估工具 (SET)

安全评估工具 (SET) 是由西门子工业部门按照 IEC 62061 以及 ISO 13849-1 标准所开发的一款经过 TÜV 认证的在线工具，用于辅助评估设备上的安全功能。该工具的输出结果是符合标准的报告，可整合到设备文档中用作安全证明。

该安全评估工具 (SET) 可通过以下链接在线访问：

http://www.siemens.de/safety-evaluation-tool

此外还提供有“SET Getting Started（SET 入门）”以及“SET Tutorial（SET 教程）”（视频）。

### 2.1.2 安全评估工具 (SET) 所支持的评估对象

当按照 IEC 62061 来确定安全完整性等级 (SIL) 时，安全评估工具 (SET) 支持对下述活动进行评估：

- 安全系统 (SRECS) 架构的设计
- 安全系统 (SRECS) 子系统的实现
- 确定所实现的安全完整性等级 (SIL)

请注意

IEC 62061 的完整应用还附加要求更多的活动，而这些活动已超出安全评估工具 (SET) 的应用范围。 比如其中包括，生成额外的文档以及验证文件。

欲了解更多信息，请参考相应标准所给出的标准文件。

## 2.2 创建 SET 项目

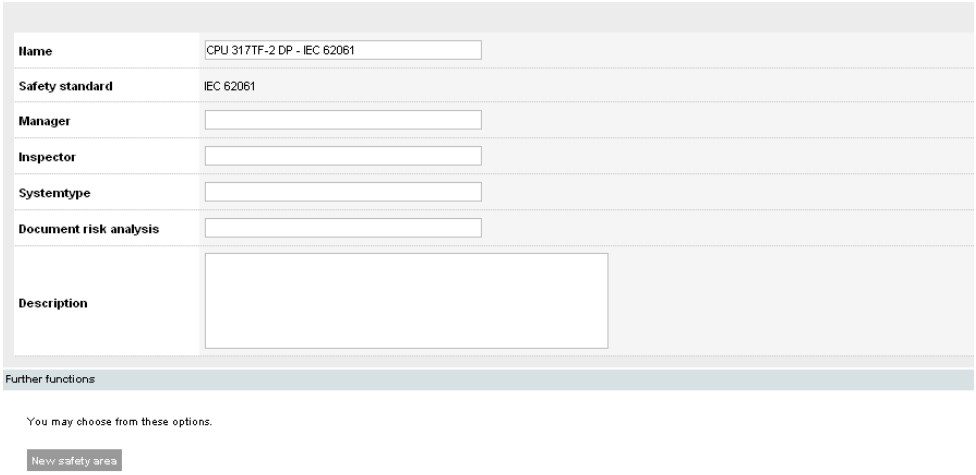
### 2.2.1 创建项目

当在安全评估工具 (SET) 中创建一个新项目时，必须决定该项目所适用的标准。本应用示例将会更为详尽地解释 IEC 62061 标准的应用。

图 2-1 创建一个 SET 项目 – 选择适用的标准

在接下来的画面中，可以设定项目名称并进一步输入该项目的详细信息。

图 2-2 创建一个 SET 项目




**请注意**

为了从安全评估工具 (SET) 上获得符合标准的报告作为安全证明，必须填写上述安全评估工具 (SET) 画面上的全部相关字段。

由于本文档所包含的显示画面源自一个应用示例，为了提供更简洁的概览，所以并未完整填写所有详细信息字段。

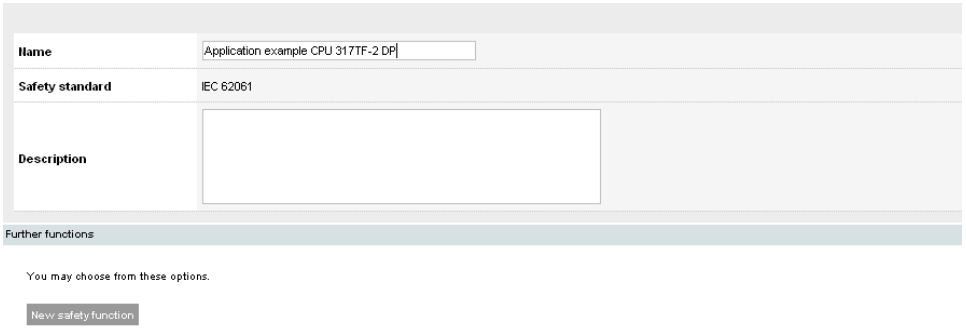


## 2.2.2 创建一个安全区域

可以将整个设备划分为不同的安全区域，然后向这些区域分配不同的安全功能或者安全相关控制功能 (SRCF)。

在本应用示例当中，将会创建一个替代的安全区域，并将需要演示的安全功能集成到该区域当中。

图 2-3 创建一个安全区域

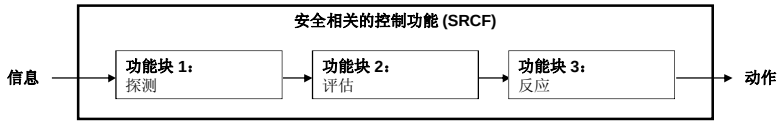


## 2.2.3 创建安全功能

现在，可以在安全区域内创建各种安全相关控制功能 (SRCF)。在此，必须对安全相关控制功能 (SRCF) 或者安全功能进行相应的设置。

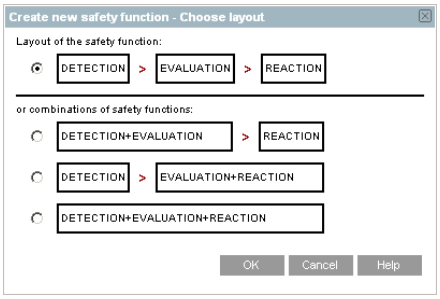
在本应用示例中，将使用三个功能块来实现安全相关控制功能 (SRCF) 的经典设置：

图 2-4 安全相关控制功能 (SRCF) 的功能块



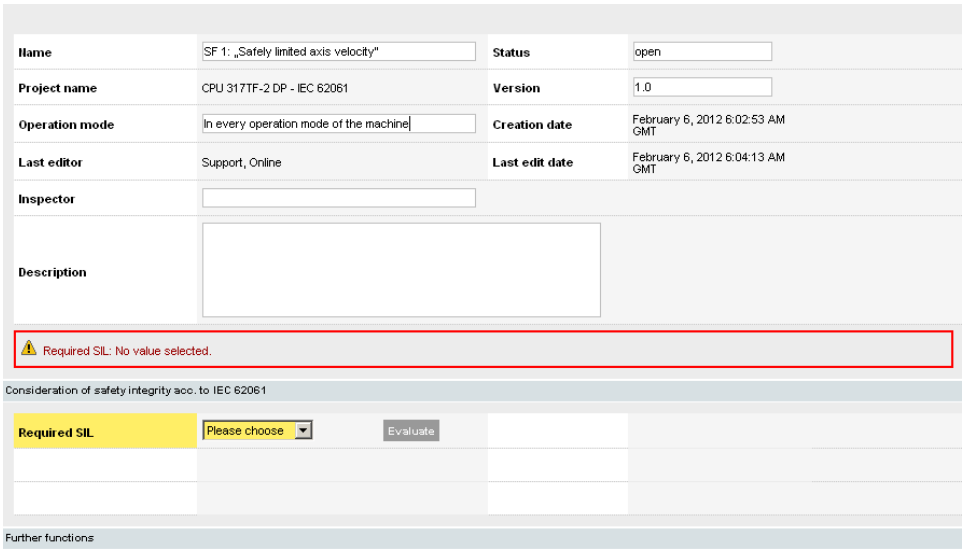

安全评估工具 (SET) 中的安全功能设置可通过以下的画面进行选择。

图 2-5 创建一个安全功能 – 选择子功能




这一个步骤将会在安全评估工具 (SET) 中创建三个子功能。 然后便可以在安全功能的画面中执行风险评估，如章节 3.2 所述。

图 2-6 创建安全功能

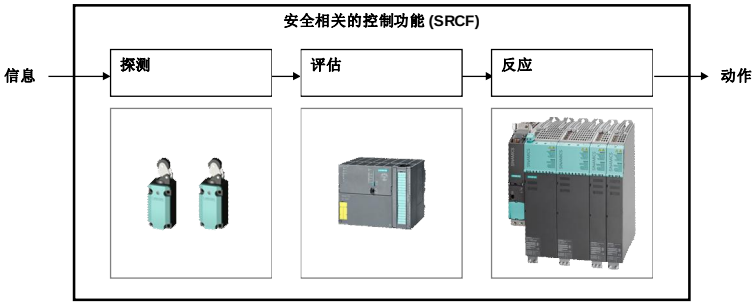


## 2.2 创建 SET 项目

利用三个对应的功能块来创建以下三个安全相关控制功能 (SRCF) 或者安全功能 (SF)：

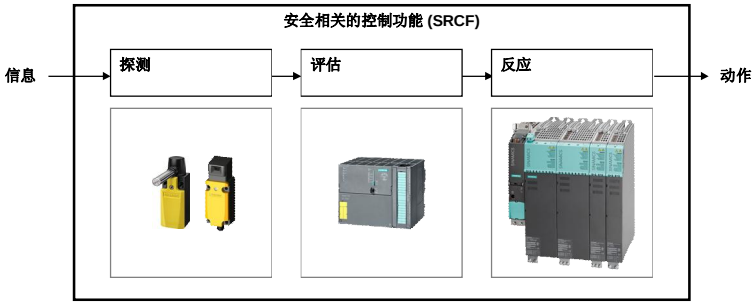
- **安全功能 1 (SF 1)**：“安全限制速度”

图 2-7 SRCF 1 可能的实现方法



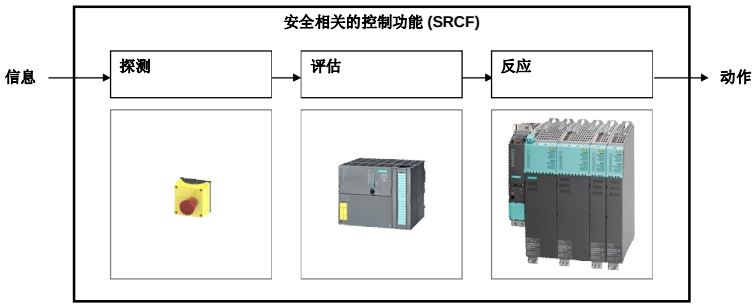

- **安全功能 2 (SF 2)**：“安全停止所有机轴”

图 2-8 SRCF 2 可能的实现方法




- **安全功能 3 (SF 3)**：“紧急停止所有机轴”

图 2-9 SRCF 3 可能的实现方法



# 3 风险分析与风险评估

## 3.1 风险分析的执行

在实际应用 IEC 62061 标准之前，必须对设备进行风险分析。 风险分析并未包含在 IEC 62061 之中。

该风险分析将会检查以下内容：

- 设备所带来的危险
- 为了降低出现危险的风险，需要采用哪些安全相关的控制功能

潜在的危险风险取决于以下两个因素：

- 由潜在危险所造成的伤害严重程度
- 伤害的发生率

**本应用示例的评估结果**

针对本应用示例的风险分析得出以下结果：

表 3-1

| 危险 | | 所要求的 SRCFs |
|---|---|---|
| 1 | 当通过安全门进入危险区域时，操作员可能会遭受暴露机轴的严重伤害。 | SRCF 1：将暴露机轴的转速降低至一个安全上限速度以内。 |
| 2 | 当打开设备的防护罩时，操作员可能会由于设备内连接至两根机轴的齿轮转动而遭受严重损伤。 | SRCF 2：立即停止设备上的两根机轴。 |

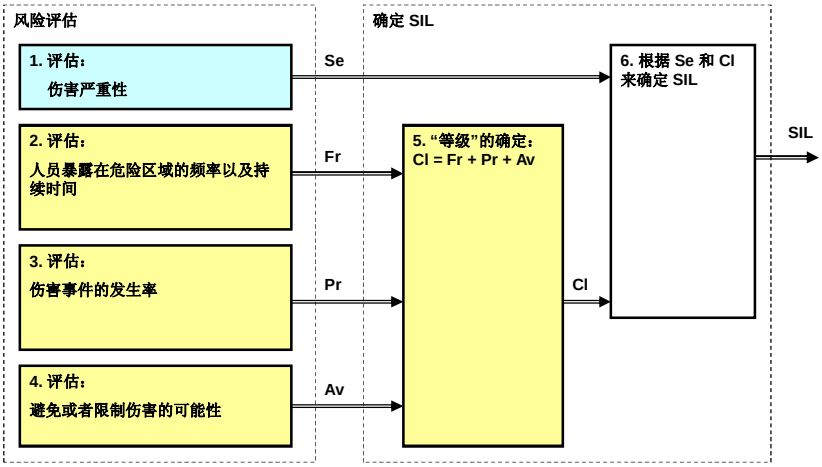
**请注意** 由于用户通常可以选择“紧急停止”类别，所以无须为 SRCF 3 “紧急停止”的实现进行风险分析，除非存在 C 类标准指定了类别的选择。

**请注意** SRCF 3 “紧急停止”是一项补充的安全功能，不可替代独立的安全功能。

## 3.2 风险评估的执行

经过分析之后，需要对所识别的每一项设备危险进行风险评估。与风险分析一样，风险评估也不包含在 IEC 62061 标准之内。

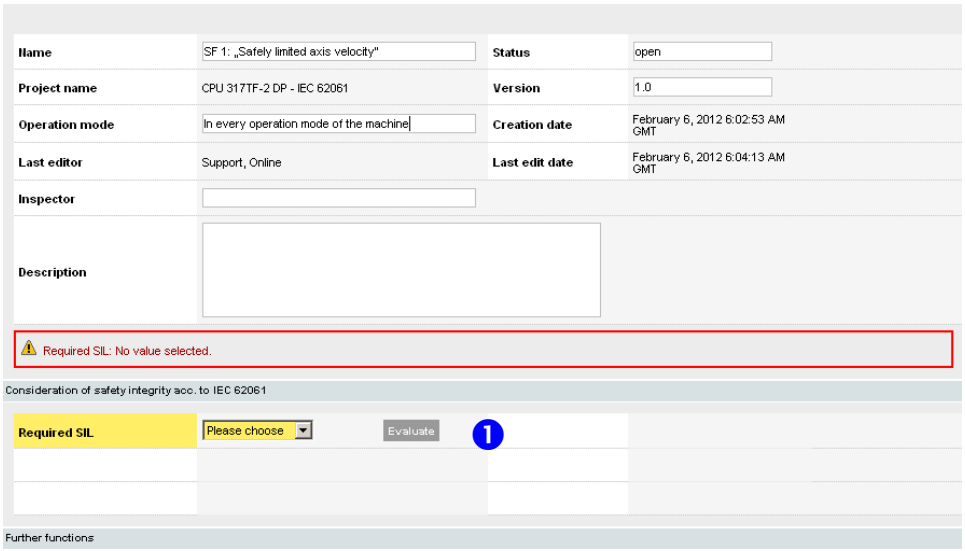
图 3-1 执行风险评估




风险评估会对每一项潜在危险进行检查，并确定采取何种措施可将风险降至最低。如果所需采取的措施是一项 SRCF，那么就必须确定该 SRCF 所要求的安全完整性等级 (SIL)。SIL 的确定方法是将潜在危险所残留的风险（剩余风险）降至可接受的低水平。

安全评估工具 (SET) 会在风险评估过程中为您提供支持，指导您确定各项安全功能或者安全相关控制功能 (SRCF) 所要求的安全完整性等级 (SIL)。

图 3-2 指导确定所要求的安全完整性等级 (SIL)



按下“Evaluate（评估）”按钮❶之后，工具便会指导您确定所要求的安全完整性等级 (SIL)，如以下章节所述。

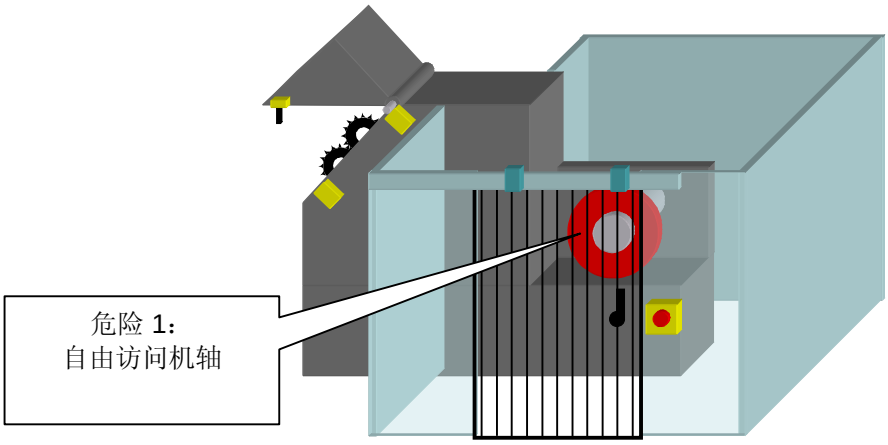
## 3.2.1 危险 1 的风险评估

对章节 3.1 的风险分析（参见 表 3-1）中所确定的危险 1 进行风险评估。

**危险情况**

暴露机轴对操作员造成严重损伤。

图 3-3 危险 1




**评估 1：伤害的严重程度**

表 3-2 风险评估 – 伤害的严重程度

| 伤害的严重程度 | Se |
|---|---|
| 不可挽回的：死亡，失去眼睛或者手臂 | 4 |
| 不可挽回的：造成肢体残缺，失去一只或者多只手指 | B |
| 可挽回的：需要医生治疗 | 2 |
| 可挽回的：需要急救 | 1 |
| **本应用示例的评估结果** | |
| 由该设备所弹射出的飞行部件可能会造成人员肢体残缺。 | 3 |

### 评估 2：人员暴露在危险中的频率以及持续时间

表 3-3 风险评估 – 暴露于危险的频率与时间

| 暴露情况 | | Fr |
|---|---|---|
| **频率** | **持续时间** | |
| ≤ 1h | 大于 10 min | 5 |
| | 达到 10min | 5 |
| > 1h，但 ≤ 1 天 | 大于 10 min | 5 |
| | 达到 10min | 4 |
| > 1 天，但 ≤ 2 周 | 大于 10 min | 4 |
| | 达到 10min | 3 |
| > 2 周，但 ≤ 1 年 | 大于 10 min | 3 |
| | 达到 10min | 2 |
| > 1 年 | 大于 10 min | 2 |
| | 达到 10min | 1 |
| **本应用示例的评估结果** | | |
| 操作员在一小时之内需要数次进入危险区域，每次持续时间最多 10 分钟。 | | 5 |

### 评估 3：危险事件的发生率

表 3-4 风险评估 – 伤害的发生率

| 发生率 | Pr |
|---|---|
| 非常高 | 5 |
| 较高 | 4 |
| 一般 | 3 |
| 较低 | 2 |
| 可忽略 | 1 |
| **本应用示例的评估结果** | |
| 站立在危险区域时，操作员很容易被设备所弹射出的飞行部件击中。 | 4 |

### 评估 4：避免或者限制伤害发生的可能性

表 3-5 风险评估 – 避免或者限制伤害的发生

| 避免或者限制伤害发生的可能性 | Av |
|---|---|
| 不可能 | 5 |
| 极少情况下可避免或者限制 | 3 |
| 很可能避免或者限制 | 1 |
| **本应用示例的评估结果** | |
| 操作员极少情况下可避免被设备弹射出的飞行部件击中。 | 3 |

### 风险评估的评价：确定 CI 等级

表 3-6 评价 – 确定 CI 等级

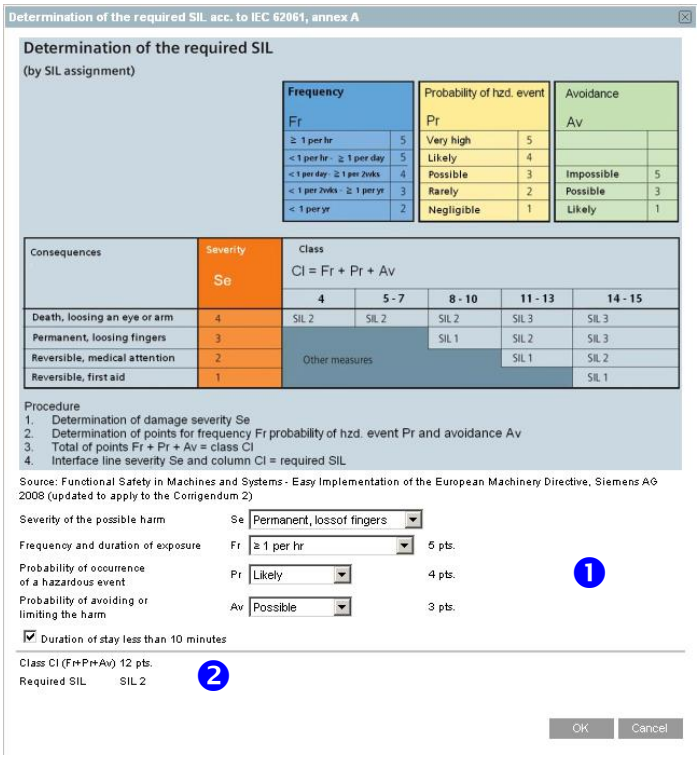
| 风险评估的评价 | CI |
|---|---|
| CI 等级的确定 | Fr + Pr + Av |
| **本应用示例的评估结果** | |
| 等级 CI = Fr + Pr + Av，其中 Fr=5，Pr=4，Av=3 | 12 |

### 风险评估的评价：根据 Se 和 CI 确定所要求的 SIL

表 3-7 评价 – 根据 Se 和 CI 确定所要求的 SIL

| 伤害的严重程度 Se | 等级 CI = Fr + Pr + Av | | | | |
|---|---|---|---|---|---|
| | 3 至 4 | 5 至 7 | 8 至 10 | 11 至 13 | 14 至 15 |
| 4 | SIL 2 | SIL 2 | SIL 2 | SIL 3 | SIL 3 |
| 3 | | | SIL 1 | SIL 2 | SIL 3 |
| 2 | | | | SIL 1 | SIL 2 |
| 1 | | | | | SIL 1 |
| **本应用示例的评估结果** | | | | | |
| 根据 Se 和 CI 来确定 SIL，其中 Se=3；CI=12 | | | | | SIL 2 |

图 3-4 评价 – 利用 SET 确定所要求的 SIL




选择了对应的评价项 ❶ 之后，安全评估工具 (SET) 的画面上便会输出所要求的安全完整性等级 (SIL) ❷。

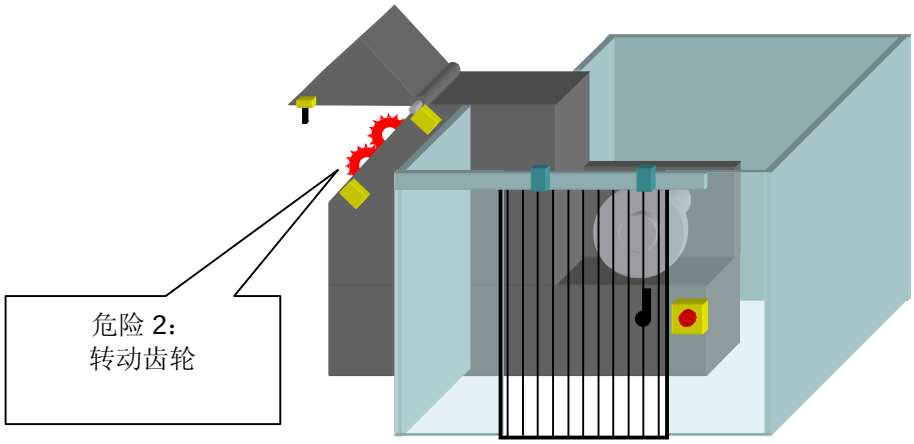
## 3.2.2 危险 2 的风险评估

对章节 3.1 的风险分析（参见表 3-1）中所确定的危险 2 进行风险评估。

**危险情况**

连接至两根机轴的转动齿轮对操作员所造成的严重伤害。

图 3-5 危险 2




**评估 1：伤害的严重程度**

表 3-8 风险评估 – 伤害的严重程度

| 伤害的严重程度 | Se |
|---|---|
| 不可挽回的：死亡，失去眼睛或者手臂 | 4 |
| 不可挽回的：造成肢体残缺，失去一只或者多只手指 | 3 |
| 可挽回的：需要医生治疗 | 2 |
| 可挽回的：需要急救 | 1 |
| **本应用示例的评估结果** | |
| 如果操作员接触设备上的转动齿轮，将可能导致断臂。 | 4 |

### 评估 2：人员暴露在危险中的频率以及持续时间

表 3-9 风险评估 – 暴露于危险的频率与时间

| 暴露情况 | | Fr |
|---|---|---|
| **频率** | **持续时间** | |
| ≤ 1h | 大于 10 min | 5 |
| | 达到 10min | 5 |
| > 1h，但 ≤ 1 天 | 大于 10 min | 5 |
| | 达到 10min | 4 |
| > 1 天，但 ≤ 2 周 | 大于 10 min | 4 |
| | 达到 10min | 3 |
| > 2 周，但 ≤ 1 年 | 大于 10 min | 3 |
| | 达到 10min | 2 |
| > 1 年 | 大于 10 min | 2 |
| | 达到 10min | 1 |
| **本应用示例的评估结果** | | |
| 操作员需要每隔两天打开设备齿轮的防护罩进行维护，该维护过程最长需要 15 分钟。 | | 4 |

### 评估 3：危险事件的发生率

表 3-10 风险评估 – 伤害的发生率

| 发生率 | Pr |
|---|---|
| 非常高 | 5 |
| 很可能避免或者限制 | 4 |
| 一般 | 3 |
| 极少情况下可避免或者限制 | 2 |
| 可忽略 | 1 |
| **本应用示例的评估结果** | |
| 在对设备的齿轮执行维护工作时，如果发生滑倒等意外事故，将使操作员与齿轮相接触。 | 3 |

### 评估 4：避免或者限制伤害发生的可能性

表 3-11 风险评估 – 避免或者限制伤害的发生

| 避免或者限制伤害发生的可能性 | Av |
|---|---|
| 不可能 | 5 |
| 极少情况下可避免或者限制 | 3 |
| 很可能避免或者限制 | 1 |
| **本应用示例的评估结果** | |
| 如果操作员在维护过程中滑倒，将很难避免与齿轮相接触。 | 3 |

### 风险评估的评价：确定 CI 等级

表 3-12 评价 – 确定 CI 等级

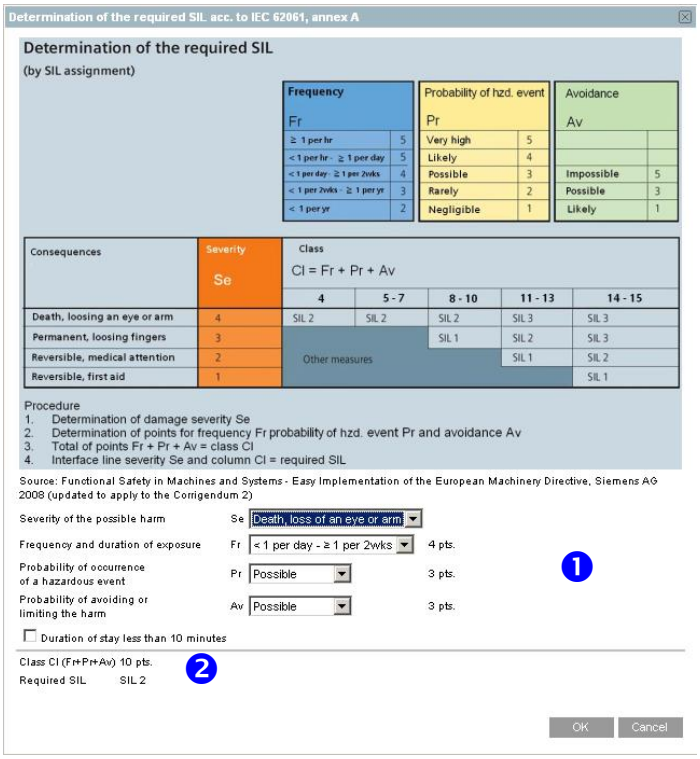
| 风险评估的评价 | CI |
|---|---|
| CI 等级的确定 | Fr + Pr + Av |
| **本应用示例的评估结果** | |
| 等级 CI = Fr + Pr + Av，其中 Fr=4，Pr=3，Av=3 | 10 |

### 风险评估的评价：根据 Se 和 CI 来确定 SIL

表 3-13 评价 – 根据 Se 和 CI 来确定 SIL

| 伤害的严重程度 Se | 等级 CI = Fr + Pr + Av | | | | |
|---|---|---|---|---|---|
| | 3 至 4 | 5 至 7 | 8 至 10 | 11 至 13 | 14 至 15 |
| 4 | SIL 2 | SIL 2 | SIL 2 | SIL 3 | SIL 3 |
| 3 | | | SIL 1 | SIL 2 | SIL 3 |
| 2 | | | | SIL 1 | SIL 2 |
| 1 | | | | | SIL 1 |
| 本应用示例的评估结果 | | | | | |
| 根据 Se 和 CI 来确定 SIL，其中 Se=4；CI=10 | | | | | SIL 2 |

图 3-6 评价 – 利用 SET，根据 Se 和 CI 来确定 SIL

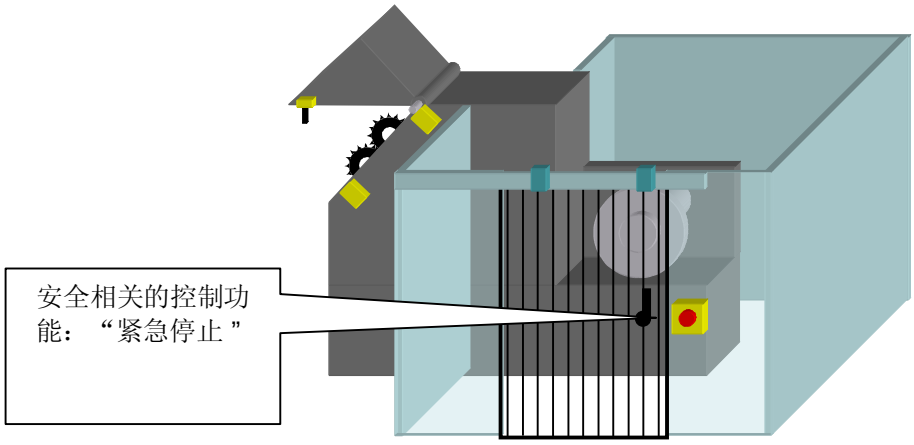



选择了对应的评价项 ❶ 之后，安全评估工具 (SET) 的画面上便会输出所要求的安全完整性等级 (SIL) ❷。

### 3.2.3 安全相关控制功能 3 的分类

安全相关的“机轴紧急停止”控制功能 (SRCF 3) 是一项根据设备指南 2006/42/EG 章节 1.2.4.3 所普遍要求的补充安全功能。 因此并不会对 SRCF 3 进行风险评估。

图 3-7 安全相关的控制功能 3 – “紧急停止”



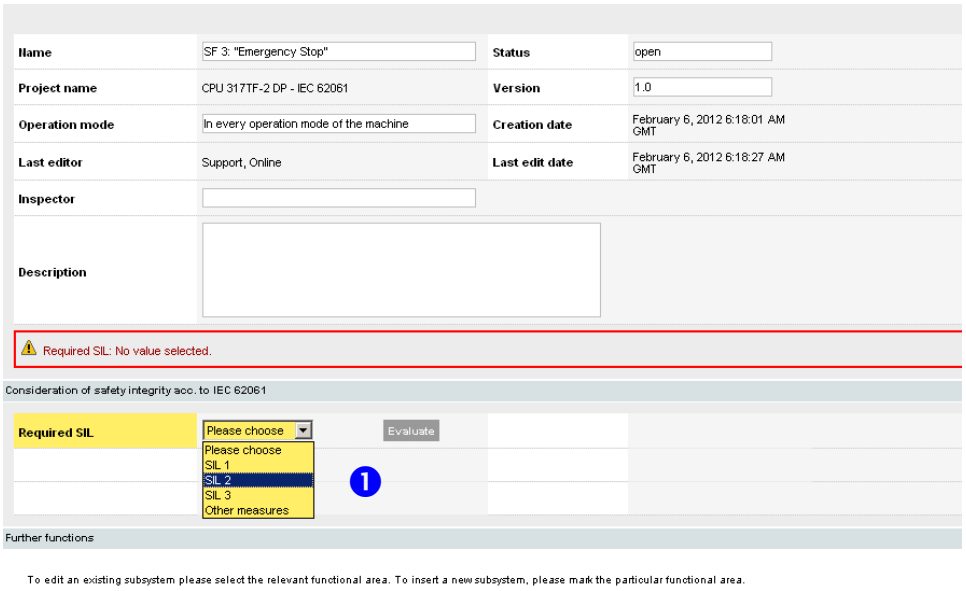

经过对另外两个安全相关的控制功能（SRCF 1 和 SRCF 2）执行示例风险评估之后，本应用示例所要求的安全完整性等级 (SIL) 为 SIL 2。

表 3-14 风险评估 – 小结

| 安全相关的控制功能 (SRCF) | | 所要求的 SIL |
|---|---|---|
| **SRCF 3** | “机轴紧急停止” | SIL 2 |

该 SIL 可通过安全功能的画面 ❶ 在安全评估工具 (SET) 中直接设置。

图 3-8 利用已完成的风险分类，设定所要求的 SIL



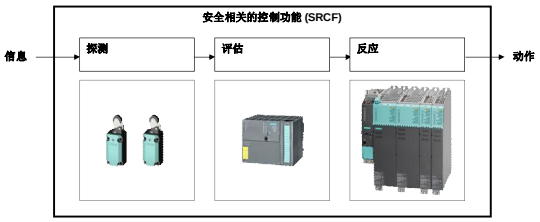

请注意

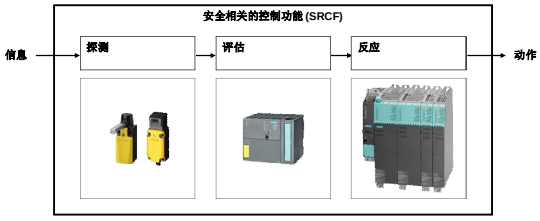
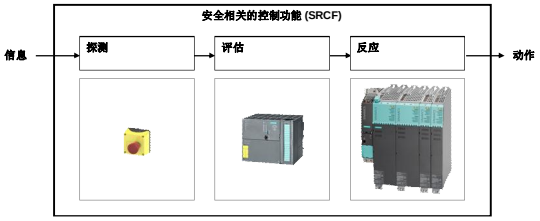
实际上，设备中其它安全相关的控制功能 (SRCF) 的最高安全完整性等级 (SIL)（由风险评估所确定的）均应用在“紧急停止”分类当中。

## 3.2.4 风险评估的总结

各项安全完整性等级 (SIL) 彼此相互独立，是在风险分析过程中根据各项潜在危险以及所分别要求的安全相关控制功能 (SRCF) 来设定或者确定的。

表 3-15 风险评估 – 总结

| 所要求的安全相关控制功能 (SRCF) | | 所要求的 SIL |
|---|---|---|
| SRCF 1 | “机轴速度的安全减速”  | SIL 2 |

| 所要求的安全相关控制功能 (SRCF) | | 所要求的 SIL |
|---|---|---|
| **SRCF 2** | “机轴安全停止”<br>  | SIL 2 |
| **SRCF 3** | “机轴紧急停止”<br>  | SIL 2 |

现在，必须指定并实现安全相关控制功能 SRCF 1，SRCF 2 以及 SRCF 3。每项安全相关控制功能 (SRCF) 都必须满足所要求的安全完整性等级 (SIL) 。

# 4 规范与实现

## 4.1 制定 SRCF 规范

安全相关控制功能 (SRCF) 的规范基本由以下几个部分组成：

- SRCF 上的信息
- SRCF 功能性的要求
- SRCF 的安全完整性要求

必须为每个安全相关控制功能 (SRCF) 制定单独的规范。

### 4.1.1 SRCF 1 的规范

表 4-1

| SRCF | 具体的 SRCF |
|---|---|
| 1 | 将暴露机轴的转速降低至安全上限速度以内。 |



**SRCF 上的信息**

表 4-2

| 主题 | 信息 |
|---|---|
| SRCF 应当避免的设备危险 | 当进入安全区域之后，操作员可能会遭受到来自设备弹射出来的飞行部件的严重伤害。 |
| 设备中的人员 | 操作人员，维护人员 |
| 启用 SRCF 的设备模式 | 设备的每个操作模式 |

**SRCF 功能性的要求**

表 4-3

| 主题 | 要求 |
|---|---|
| SRCF 的功能 | 当打开保护区的防护门时，暴露机轴的轴转速必须降低至安全上限速度以内。 |
| SRFC 必须被启用或者禁用的条件 | SRCF 必须在设备上一直保持启用状态 |
| 反应时间要求 | 一旦开启保护区的防护门，轴转速便需要在 200ms 以内降低至安全速度上限以下。 |

| 主题 | 要求 |
|---|---|
| 故障反应 | 一旦出现故障，必须采取以下的反应措施：<br>• 立即停止机轴<br>• 打开“Disturbance（干扰）”指示灯 |
| | 仅当满足以下条件之后，才能重新运行机轴：<br>• 故障已经得到纠正<br>• 防护门已关闭<br>• 操作员通过设备上的按钮确认了该故障 |
| 机电组件的工作周期率 | 保护区防护门上的位置开关：<br>• 操作员在一小时之内须数次进入危险区域，每次持续时间大约 10 分钟。<br>⇨ 每小时最多进入 6 次 |

**请注意**

**反应时间要求**取决于设备的状态。该要求的设置不应对操作员造成任何伤害。

需要确定反应时间的话，可利用 S7FCOTIA.XLS 表格或者 S7FCOTIB.XLS 表格（请参见 \E\）。

**请注意**

**故障反应**之后，重新开启机轴的条件序列可确保操作员已离开危险区域。



**SRCF 的安全完整性要求**

表 4-4

| 主题 | 要求 |
|---|---|
| SRCF 的安全完整性等级 (SIL) | 根据风险评估（参见章节 3.2.1 ），可得到以下的安全完整性等级：<br>SIL 2 |
| SRCF 的 $PFH_D$ 值 ($PFH_D$) | 利用所要求的安全完整性等级，可得到以下的 $PFH_D$ 值：<br>$PFH_D < 10^{-6}$ |

## 4.1.2 SRCF 2 的规范

表 4-5

| SRCF | 具体的 SRCF |
|---|---|
| 2 | 立即停止设备上的两根机轴。 |

**SRCF 上的信息**

表 4-6

| 主题 | 信息 |
|---|---|
| SRCF 应当避免的设备危险 | 当打开设备上的防护罩时，操作员可能会由于设备内连接至两根机轴的齿轮转动而遭受严重伤害。 |
| 设备中的人员 | 操作人员，维护人员 |
| 启用 SRCF 的设备模式 | 设备的每个操作模式 |

**SRCF 功能性的要求**

表 4-7

| 主题 | 要求 |
|---|---|
| SRCF 的功能 | 一旦打开设备上的防护罩，所有机轴必须立即停止。 |
| SRFC 必须被启用或者禁用的条件 | SRCF 必须在设备上一直保持启用状态 |
| 反应时间要求 | 一旦打开防护罩，叶片必须在 150ms 之内停止。 |
| 故障反应 | 一旦发生故障，必须采取以下的反应措施：<br>• 立即停止所有机轴<br>• 打开“Disturbance（干扰）”指示灯 |
| | 仅当满足以下条件之后，才能重新运行机轴：<br>• 故障已经得到纠正<br>• 防护罩已关闭<br>• 操作员通过设备上的按钮确认了该故障 |
| 机电组件的工作周期率 | 防护罩上的铰接开关与位置开关：<br>• 操作员需要每隔两天打开设备齿轮的防护罩进行维护，维护过程需要 15 分钟。<br>⇨ 每月 10 次 |

**请注意** **反应时间要求**取决于设备的状态。 该要求的设置不应对操作员造成任何伤害。

需要确定反应时间的话，可利用 S7FCOTIA.XLS 表格或者 S7FCOTIB.XLS 表格（请参见 \E\）。

**请注意** **故障反应**之后，重新开启机轴的条件序列可确保操作员已离开危险区域。

**SRCF 的安全完整性要求**

表 4-8

| 主题 | 要求 |
|---|---|
| SRCF 的安全完整性等级 (SIL) | 根据风险评估（参见章节 0），可得到以下的安全完整性等级：<br>SIL 2 |
| SRCF 的 $PFH_D$ 值 ($PFH_D$) | 利用所要求的安全完整性等级，可得到以下的 $PFH_D$ 值：<br>$PFH_D < 10^{-6}$ |

## 4.1.3 SRCF 3 的规范

表 4-9

| SRCF | 具体的 SRCF |
|---|---|
| 3 | 紧急停止设备上的所有机轴。 |



**SRCF 上的信息**

表 4-10

| 主题 | 信息 |
|---|---|
| SRCF 应当避免的设备危险 | 无。<br><br>SRCF 3 “紧急停止”是一项补充的安全功能，不可替代独立的安全功能。 因此，无法为该 SRCF 设定对应危险情况。 |
| 设备中的人员 | 全部 |
| 启用 SRCF 的设备模式 | 设备的每个操作模式 |

**SRCF 功能性的要求**

表 4-11

| 主题 | 要求 |
|---|---|
| SRCF 的功能 | 操作了急停控制开关之后，设备的所有机轴将会马上停止。 |
| SRFC 必须被启用或者禁用的条件 | SRCF 必须在设备上一直保持启用状态 |
| 反应时间要求 | 操作了急停控制开关之后，叶片必须在 150ms 之内停止。 |

| 主题 | 要求 |
|---|---|
| 故障反应 | 一旦发生故障，必须采取以下的反应措施：<br>• 立即停止所有机轴<br>• 打开“Disturbance（干扰）”指示灯 |
| | 仅当满足以下条件之后，才能重新运行机轴：<br>• 故障已经得到纠正<br>• 紧急停止按钮已解锁<br>• 操作员通过设备上的按钮确认了该故障 |
| 机电组件的工作周期率 | 急停控制开关：<br>• 操作员每周至少需要操作一次急停控制开关。<br>⇨ 每周 1 次 |

**请注意** **反应时间要求**取决于设备的状态。 该要求的设置不应对操作员造成任何伤害。

需要确定反应时间的话，可利用 S7FCOTIA.XLS 表格或者 S7FCOTIB.XLS 表格（请参见 \E\）。

**请注意** **故障反应**之后，重新开启机轴的条件序列可确保机轴不会在出现故障之后自动启动。



**SRCF 的安全完整性要求**

表 4-12

| 主题 | 要求 |
|---|---|
| SRCF 的安全完整性等级 (SIL) | 根据风险评估（参见章节 0），可得到以下的安全完整性等级：<br>SIL 2 |
| SRCF 的 $PFH_D$ 值 ($PFH_D$) | 利用所要求的安全完整性等级，可得到以下的 $PFH_D$ 值：<br>$PFH_D < 10^{-6}$ |

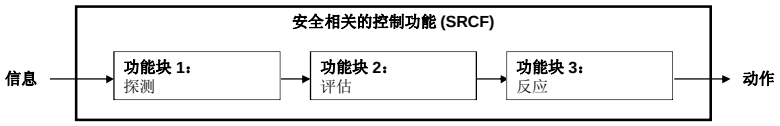
# 4.2 设计 SRECS 架构

## 4.2.1 将 SRCF 划分为功能块

在章节 2.2.3 中利用安全评估工具 (SET) 创建安全功能时，便已将 SRCF 划分为功能块。

SRCF 功能块的划分，使得 SRCF 的各项功能可以在单独的功能块中实现，一旦某个 SRCF 功能块出现故障，便会导致整个 SRCF 失效（“功能块的串联”）。

图 4-1 将 SRCF 划分为功能块




**安全相关控制功能 1 (SRCF 1)**

图 4-2 安全相关的控制功能 1 (SRCF 1)

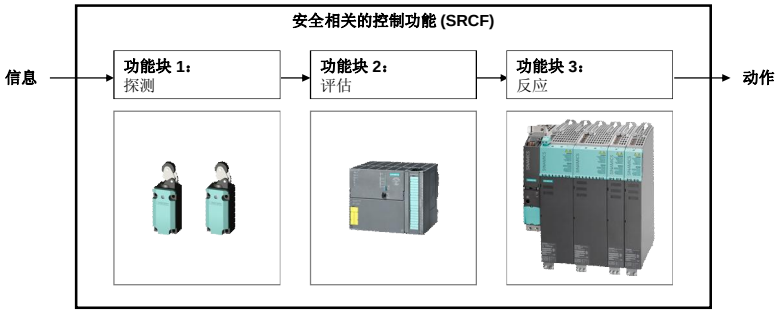



表 4-13 功能块的作用 - SRCF 1

| 功能块 | 作用 |
|---|---|
| 1：检测 | 检测保护区防护门的位置 |
| 2：评估 | 评估所检测到的保护区防护门位置，然后触发相应的动作（控制 SINAMICS S120 驱动器） |
| 3：反应 | 触发 SINAMICS S120 驱动器的安全功能 |

### 安全相关控制功能 2 (SRCF 2)

图 4-3 安全相关的控制功能 2 (SRCF 2)

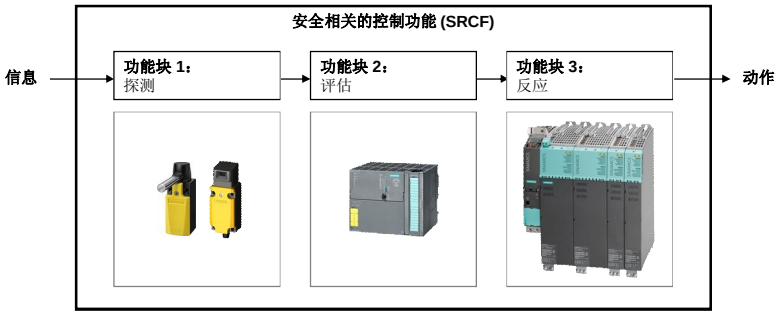



表 4-14 功能块的作用 - SRCF 2

| 功能块 | 作用 |
|---|---|
| 1：检测 | 检测防护罩的位置 |
| 2：评估 | 评估所检测到的保护区防护罩位置，然后触发相应的动作（控制 SINAMICS S120 驱动器） |
| 3：反应 | 触发 SINAMICS S120 驱动器的安全功能 |

### 安全相关控制功能 3 (SRCF 3)

图 4-4 安全相关的控制功能 3 (SRCF 3)

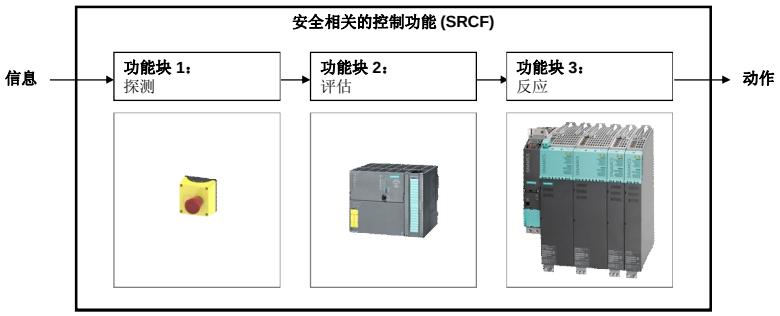



表 4-15 功能块的作用 - SRCF 3

| 功能块 | 作用 |
|---|---|
| 1：检测 | 检测急停控制开关的状态 |
| 2：评估 | 评估所检测到的急停控制开关状态，然后触发相应的动作（控制 SINAMICS S120 驱动器） |
| 3：反应 | 触发 SINAMICS S120 驱动器的安全功能 |

## 4.2.2 功能块的详细要求

以下的表格将对各个 SRCF 功能块的要求进行说明。

### 安全相关的控制功能 1 (SRCF 1)

表 4-16 功能块的详细作用 - SRCF 1

| 功能块 | | 作用 |
|---|---|---|
| **1：检测** | | |
| | 输入 | 保护区防护门的位置：<br>“open（打开）”或“closed（关闭）” |
| | 输出 | 保护区防护门的位置信息：<br>• 保护区防护门处于打开状态<br>• 保护区防护门处于关闭状态 |
| | 作用 | 在设备的所有操作模式下检测保护区防护门的位置 |
| **2：评估** | | |
| | 输入 | 保护区防护门的位置信息（功能块 1 的输出） |
| | 输出 | 用于控制 SINAMICS S120 驱动器的命令：<br>• 通过触发 PLCopen 功能，使得故障安全 Technology CPU 集成技术中的机轴转速降低。<br>• 触发 SINAMICS S120 驱动器中的“*Safely-Limited Speed （安全限制速度”* ***(SLS)*** 安全功能，监测机轴的减速情况。<br>为了实现安全性，用于控制 SINAMICS S120 的单一命令中组合了两个动作。 |
| | 作用 | 在设备的全部操作模式下评估保护区防护门的位置检测情况，并适当控制故障安全 Technology CPU 中的集成技术以及 SINAMICS S120 驱动器。 |
| **3：反应** | | |
| | 输入 | 用于控制 SINAMICS S120 驱动器的命令<br>（功能块 2 的输出） |
| | 输出 | --- |
| | 作用 | 将机轴转速降至安全的速度上限以内：<br>• 降低机轴转速<br>• 利用 SINAMICS S120 的“*Safely-Limited Speed （安全限制速度”* ***(SLS)*** 安全功能监测机轴是否在设定的延迟时间内减速。<br>为了实现高安全性，SINAMICS S120 的单一功能中组合了两个动作。 |

### 安全相关的控制功能 2 (SRCF 2)

表 4-17 功能块的详细作用 - SRCF 2

| 功能块 | | 作用 |
|---|---|---|
| **1：检测** | | |
| | 输入 | 防护罩的位置：“open（打开）”或者“closed（关闭）” |
| | 输出 | 防护罩位置信息：<br>• 防护罩处于打开状态<br>• 防护罩处于关闭状态 |

| 功能块 | | 作用 |
|---|---|---|
| | 作用 | 在设备的全部操作模式下检测防护罩的位置。 |
| **2：评估** | | |
| | 输入 | 防护罩位置的信息<br>（功能块 1 的输出） |
| | 输出 | 用于控制 SINAMICS S120 驱动器的命令：<br>• 触发 SINAMICS S120 驱动器的“*Safe Stop 1（安全停止）”(SS1)* 安全功能。 |
| | 作用 | 在设备的全部操作模式下评估防护罩的位置检测，然后合理控制 SINAMICS S120 驱动器。 |
| **3：反应** | | |
| | 输入 | 用于控制 SINAMICS S120 驱动器的命令<br>（功能块 2 的输出） |
| | 输出 | --- |
| | 作用 | 安全停止驱动器的所有机轴：<br>• 激活 SINAMICS S120 所有机轴的“*Safe Stop 1（安全停止）”(SS1)* 安全功能。 |



**安全相关的控制功能 3 (SRCF 3)**

表 4-18 功能块的详细作用 - SRCF 2

| 功能块 | | 作用 |
|---|---|---|
| **1：检测** | | |
| | 输入 | 急停控制开关的状态：<br>“triggered（触发）”或者“not triggered（为触发）” |
| | 输出 | 急停控制开关的状态信息：<br>• 急停控制开关已触发（已执行操作）：<br>• 急停控制开关为触发（未执行操作）： |
| | 作用 | 在设备的所有操作模式下检测急停控制开关的状态。 |
| **2：评估** | | |
| | 输入 | 急停控制开关的状态信息<br>（功能块 1 的输出） |
| | 输出 | 用于控制 SINAMICS S120 驱动器的命令：<br>• 触发 SINAMICS S120 驱动器的“*Safe Stop 1（安全停止）”(SS1)* 安全功能。 |
| | 作用 | 在设备的全部操作模式下评估急停控制开关的状态，然后合理控制 SINAMICS S120 驱动器。 |
| **3：反应** | | |
| | 输入 | 用于控制 SINAMICS S120 驱动器的命令<br>（功能块 2 的输出） |
| | 输出 | --- |
| | 作用 | 安全停止驱动器的所有机轴：<br>• 激活 SINAMICS S120 所有机轴的“*Safe Stop 1（安全停止）”(SS1)* 安全功能。 |

### 4.2.3 硬件组件的规范

为了验证利用安全评估工具 (SET) 实现各个功能块的可能性以及计算 SIL 要求限制 (SIL CL)，必须为用于验证的各个功能块指定硬件组件。

如果指定的硬件组件未能满足所需的 SIL 要求限制 (SIL CL)，便可在后续交互步骤中相应地调整硬件组件清单。

表 4-19 硬件组件清单

| SRCF | 硬件组件 | 订单号 | 制造商 |
|---|---|---|---|
| **功能块：检测** | | | |
| 1 | 位置开关<br>触头：1 NO + 1 NC | 3SE5 232-0HE10 | 西门子有限公司 |
| 1 | 位置开关<br>触头：1 NO + 1 NC | 3SE5 232-0HE10 | |
| 2 | 铰接开关<br>触头：1 NO + 1 NC<br>开关角度：10° | 3SE5 232-0HU22 | |
| 2 | 配备独立操纵的位置开关，<br>触头：1 NO + 2 NC | 3SE5 232-0QV40 | |
| | 标准执行器 | 3SE5 000-0AV01 | |
| 3 | 配备执行器的急停控制开关盒：<br>触头：2 NC | 3SB3801-0EG3 | |
| **功能块：评估** | | | |
| 1/2/3 | CPU 317TF-2 DP | 6ES7317-6TF14-0AB0 | 西门子有限公司 |
| | SM 326 – DI 24xDC24V | 6ES7326-1BK02-0AB0 | |
| **功能块：反应** | | | |
| 1/2/3 | SINAMICS S120 | 取决于版本 | 西门子有限公司 |
| | 控制单元<br>CU 320 | 6SL3040-0MA00-0AA1 | |
| | 整流器/发电设备<br>智能线路模块 | 6SL3430-6TE21-6AA0 | |
| | 动力单元<br>双电机模块 | 6SL3420-2TE11-7AA0 | |
| | 伺服电机<br>1FK7 电机 | 1FK7022-5AK71-1DG0 | |

## 4.2.4 将功能块分配至子系统

接下来，会将安全相关控制功能的功能块（SRCF 1，SRCF 2 以及 SRCF 3）分配至安全相关的电气、电子以及可编程电子控制系统 (SRECS)。

本文档将在接下来的章节中更为详尽地说明子系统的分配与实现。 可通过用于确定 SIL 要求限制 (SIL CL) 的表格来确定实现选件。

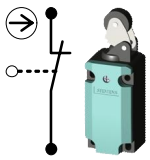
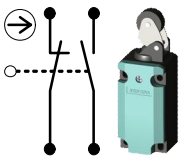
表 4-20 SIL 要求限制 (SIL Cl) 的评估

| | | 硬件故障容差 (HFT) | | |
|---|---|---|---|---|
| | | **0** | **1** | **2** |
| **安全失效分数 (SFF)** | **< 60%** | 不允许 | SIL CL 1 | SIL CL 2 |
| | **60% 至 < 90%** | SIL CL 1 | SIL CL 2 | SIL CL 3 |
| | **90% 至 < 99%** | SIL CL 2 | SIL CL 3 | SIL CL 3 |
| | **≥ 99%** | SIL CL 3 | SIL CL 3 | SIL CL 3 |

## 4.2.5 功能块子系统 1：“防护门的位置”

对于用来监测保护区防护门的子系统，根据表格所示，有三个选件可用于实现 SIL CL 2 的要求限制。 然而出于经济方面的原因，将不再考虑 HFT = 2 的选件。

表 4-21 子系统 1 的实现选件

| **实现选件 1** | **实现选件 2** | **实现选件 3** |
|---|---|---|
| 该子系统由一个子系统元件所组成 | 该子系统由一个子系统元件所组成 | 该子系统由两个子系统元件所组成 |
|  |  |  |
| • 单通道结构<br>⇨ 硬件故障容差 HFT = 0<br>• 所要求的安全失效分数：<br>90% ≤ SFF < 99% | • 机械单通道结构 / 电气双通道结构<br>⇨ 硬件故障容差 HFT = 0<br>• 所要求的安全失效分数：<br>90% ≤ SFF < 99% | • 双通道结构<br>⇨ 硬件故障容差 HFT = 1<br>• 所要求的安全失效分数：<br>60% ≤ SFF < 90% |

**实现选件 2 的显著特点：**
由于该位置开关的驱动头为机械结构，经受损伤的过程无法得到有效保护，因此所谓的故障排除不适用于此位置开关。

因此，其硬件故障容差不会增加至 HFT = 1，而是保持在 HFT = 0。该位置开关的两个触头无法相互独立地进行观察，因此无法检测驱动头的故障情况。不考虑这两个经过评估的触头，该子系统元件就像是一个单通道结构。由此，其诊断覆盖系数 (DC) < 60% （无）。

根据章节 4.1.1 所提到的安全相关控制功能 1 (SRCF 1) 的要求，可以得到下述的执行次数以及测试间隔：

表 4-22

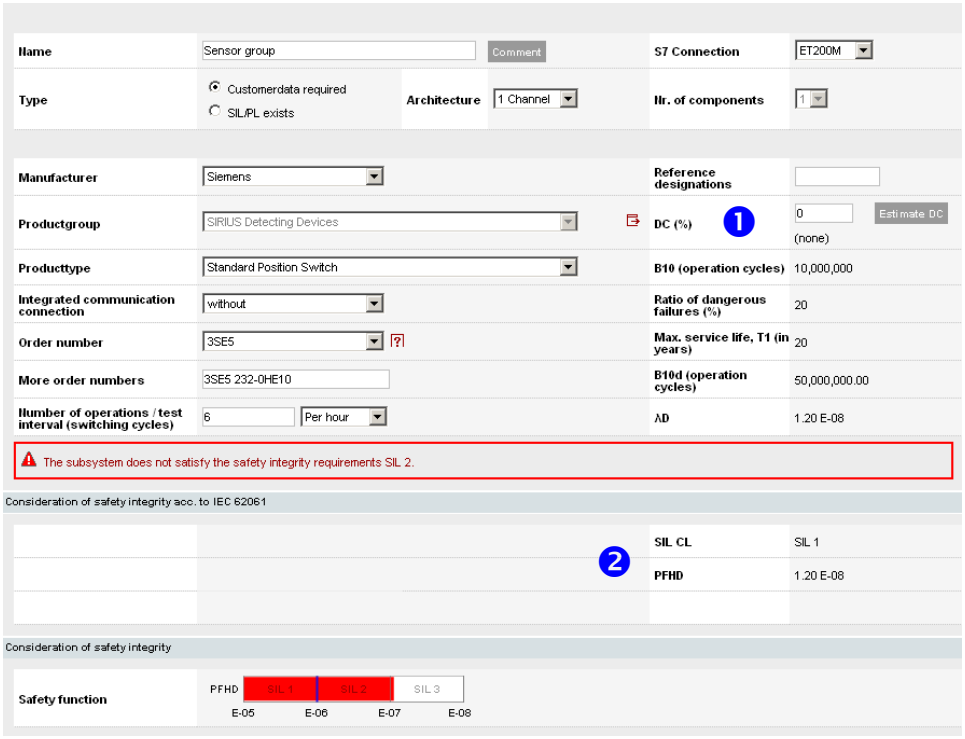
| SRCF 的要求 | 执行次数 / 测试间隔 |
|---|---|
| 操作员在一小时内须数次进入该危险区域，每次持续时间约 10 分钟。<br>⇨ 每小时最多 6 次进入 | 每小时 6.0 次 |

利用手头上的这些信息，可通过安全评估工具 (SET) 来确定适用于各种实现选件的切实可行的安全完整性等级 (SIL)。

**实现选件 1**

配备一个子系统元件的单通道结构。由于这是一个单通道结构，因此无法对子系统进行诊断。结果 ❶ 得到 < 60%（无）的诊断覆盖系数 (DC)，该系数会直接输入到安全评估工具 (SET) 的画面中。

图 4-5 在 SET 中查看实现选件 1




在安全评估工具 (SET) 中输入所有必要的数值与参数，立即可得 SIL 要求限制结果 (SIL CL) 以及相应的 $PFH_D$ 数值 ❷ 。

**实现选件 2**

配备一个子系统元件的双通道结构。由于缺少故障排除信号，所以该结构就像是一个单通道结构。因此无法对子系统进行诊断，并且会直接输入 < 60%（无）的诊断覆盖结果 (DC) ❶。

图 4-6 在 SET 中查看实现选件 2（通道 1）

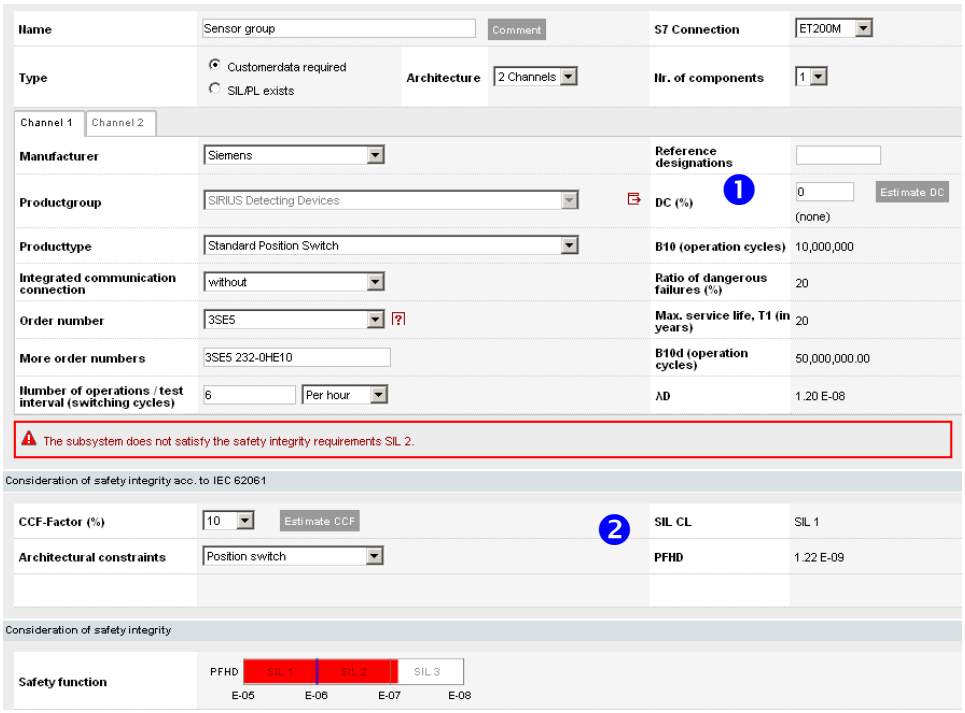
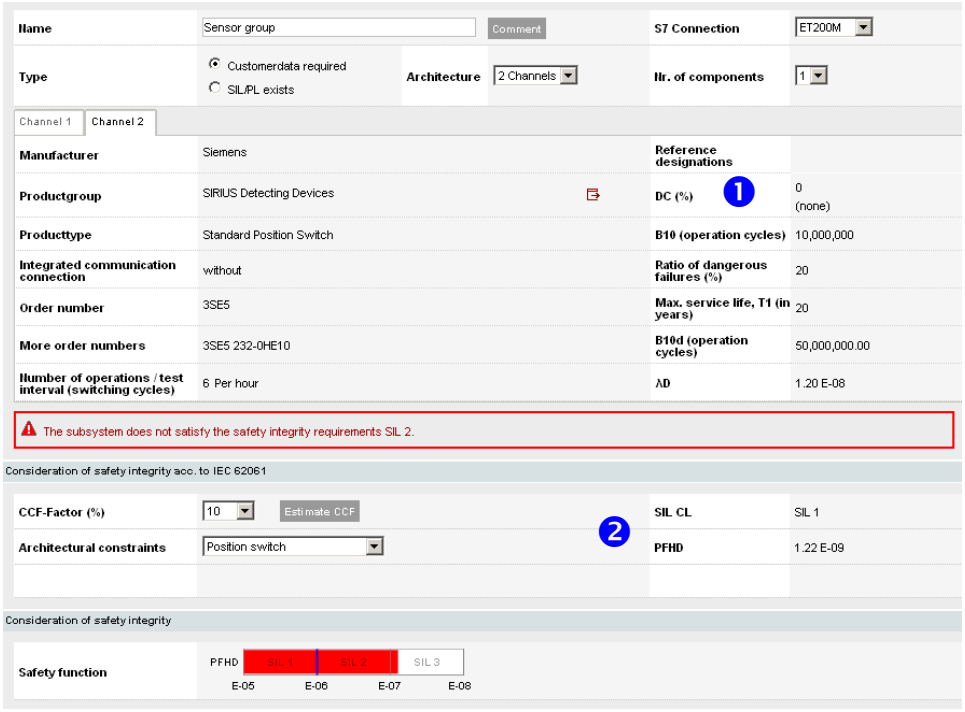



图 4-7 在 SET 中查看实现选件 2（通道 2）



**实现选件 3**

配备两个子系统元件的双通道结构。可以对逻辑上的输入信号进行交叉比较 ❶（SIMATIC F CPU 的原理），因此可达到 99% （高）的诊断覆盖系数 (DC) ❷。

图 4-8 在 SET 中确定诊断覆盖 DC

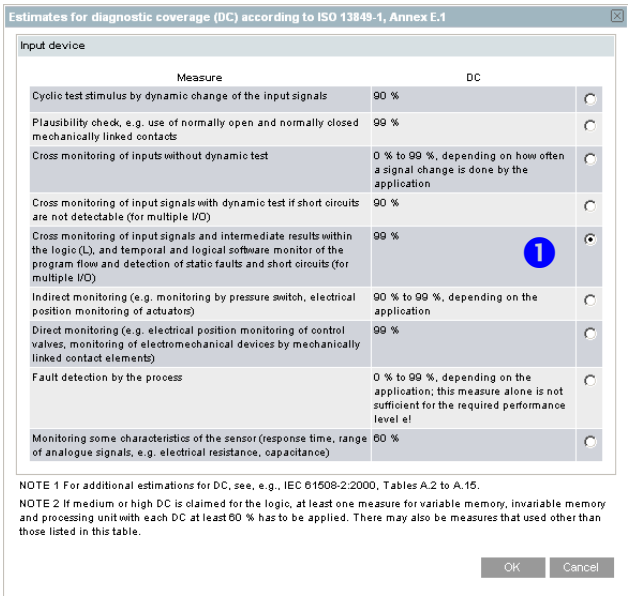



图 4-9 在 SET 中查看实现选件 2（通道 1）

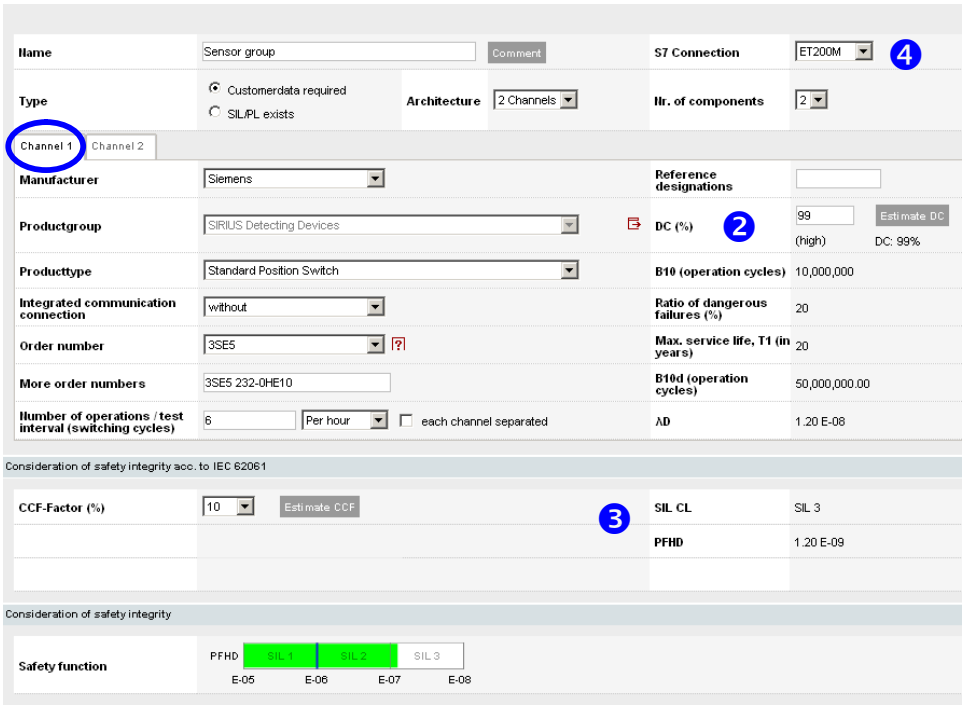
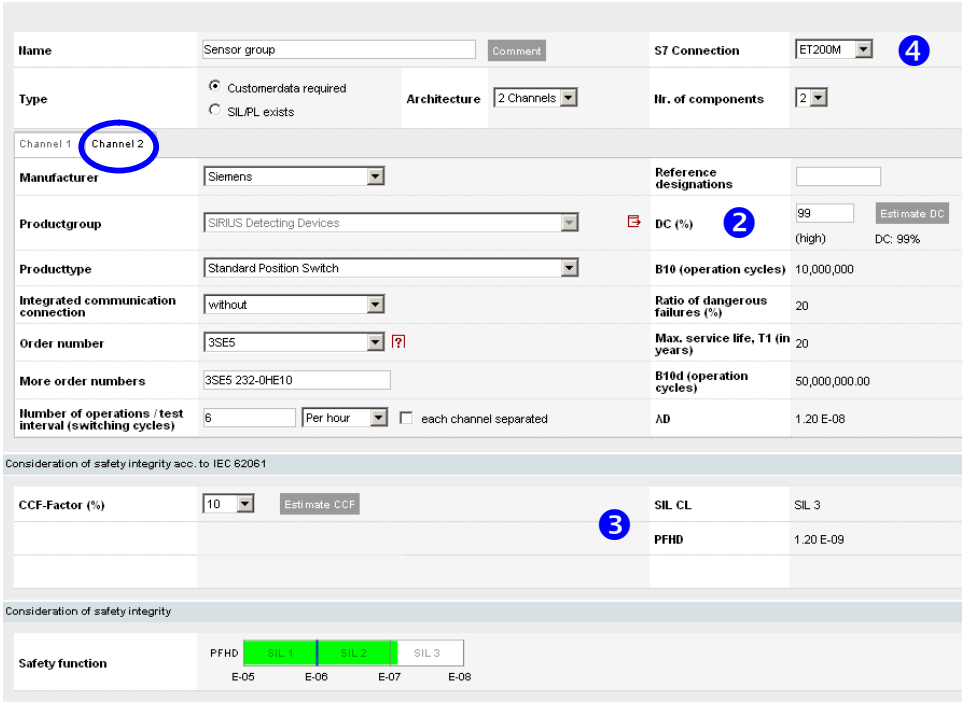


图 4-10 在 SET 中查看实现选件 2（通道 2）




在安全评估工具 (SET) 中输入所有必要的数值与参数，便可立即读取 SIL 要求限制结果 (SIL CL) 以及相应的 $PFH_D$ 数值 ❸ 。

**实现选件的评价**

对于**实现选件 1 和 2**，其所能实现的最高安全完整性等级为 SIL CL 1，因此本应用中不考虑采用这些实现选件。

利用**实现选件 3** 可达到 SIL CL 3 的安全完整性等级，而且不存在任何问题。因此，安全相关控制功能 (SRCF) 的子系统 1 必须配备带有这些位置开关类型的双通道结构。

**请注意**

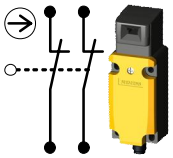
如果在安全评估工具 (SET) 中选择通过 ET 200 M 连接至 S7 ❹，即直接通过 S7-300 控制器系列的故障安全 I/O 模块进行连接，那么“S7 传感器组”便会自动插入到安全评估工具 (SET) 的“Evaluate（评估）”子系统当中，并且可以为计算提供所要求的参数。

如果在未指定连接的情况下需要连接至传感器组，也可以在“Evaluation（评估）”子系统中手动插入 S7 传感器组。

## 4.2.6 功能块子系统 2：“防护罩的位置”

对于用来监测防护罩的子系统，根据表格所示，有三个选件可用于实现 SIL CL 2 的要求限制。然而出于经济方面的原因，将不再考虑 HFT = 2 的选件。

表 4-23 子系统 2 的实现选件

| 实现选件 1 | 实现选件 2 | 实现选件 3 |
|---|---|---|
| 该子系统由一个子系统元件所组成 | 该子系统由一个子系统元件所组成 | 该子系统由两个子系统元件所组成 |
|  |  |  |
| • 单通道结构<br>⇨ 硬件故障容差 HFT = 0<br>• 所要求的安全失效分数：<br>90% ≤ SFF < 99% | • 机械单通道结构 / 电气双通道结构<br>⇨ 硬件故障容差 HFT = 0<br>• 所要求的安全失效分数：<br>90% ≤ SFF < 99% | • 双通道结构<br>⇨ 硬件故障容差 HFT = 1<br>• 所要求的安全失效分数：<br>60% ≤ SFF < 90% |

**请注意** 断线和短路已经在考虑范围之内，但并未包括在诊断能力当中，因为这些故障只会造成系统误差。

**实现选件 2 的显著特点：**

该解决方案中的机械单通道机构可通过所谓的故障排除功能来进行补偿：

- 分离执行器上的保护能够避免该位置开关的执行器出现破损。

因此，这种装置可以认为是双通道结构。 其子系统硬件故障容差可达到 HFT = 1
因此，达到 SIL CL 2 的安全失效分数将降低至 60% ≤ SFF < 90%。 通过双通道电气结构可进行诊断。
在这种情况下，实现选件 2 的功能就和该子系统中的实现选件 3 类似。

**请注意** 根据 IEC 62061，当使用故障排除功能时，对于硬件故障容差为 HFT = 0 的系统，可达到 SIL CL 2 的最大 SIL 要求限制。

根据章节 4.1.2 所提到的安全相关控制功能 2 (SRCF 2) 的要求，可以得到下述的执行次数以及测试间隔：

表 4-24

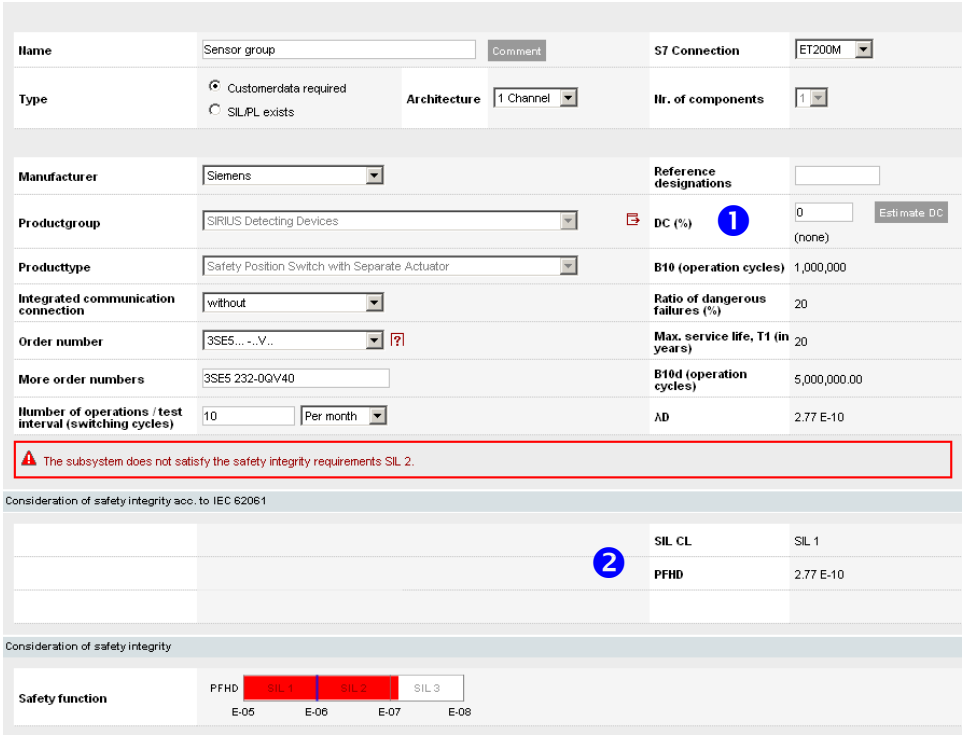
| SRCF 的要求 | 执行次数 / 测试间隔 |
|---|---|
| 操作员需要每隔两天打开设备齿轮的防护罩进行维护，该维护过程最长需要 15 分钟。<br>⇨ 每月 10 次 | 每月 10.0 次<br><br>对应于：每小时 0.014 次<br>(= 10/(30·24) = 0.014 $h^{-1}$) |

利用手头上的这些信息，可通过安全评估工具 (SET) 来确定适用于各种实现选件的切实可行的安全完整性等级 (SIL)。

**实现选件 1**

配备一个子系统元件的单通道结构。 由于这是一个单通道结构，因此无法对子系统进行诊断。 结果 ❶ 得到 < 60%（无）的诊断覆盖系数 (DC)，该系数会直接输入到安全评估工具 (SET) 的画面中。

图 4-11 在 SET 中查看实现选件 1




在安全评估工具 (SET) 中输入所有必须的数值与参数，立即可得 SIL 要求限制 (SIL CL) 结果以及相应的 $PFH_D$ 数值 ❷ 。

**实现选件 2**

配备一个子系统元件的双通道结构。 可以对逻辑上的输入信号进行交叉比较，因此可达到 99% （高）的诊断覆盖系数 (DC) ❶。

图 4-12 在 SET 中查看实现选件 2（通道 1）

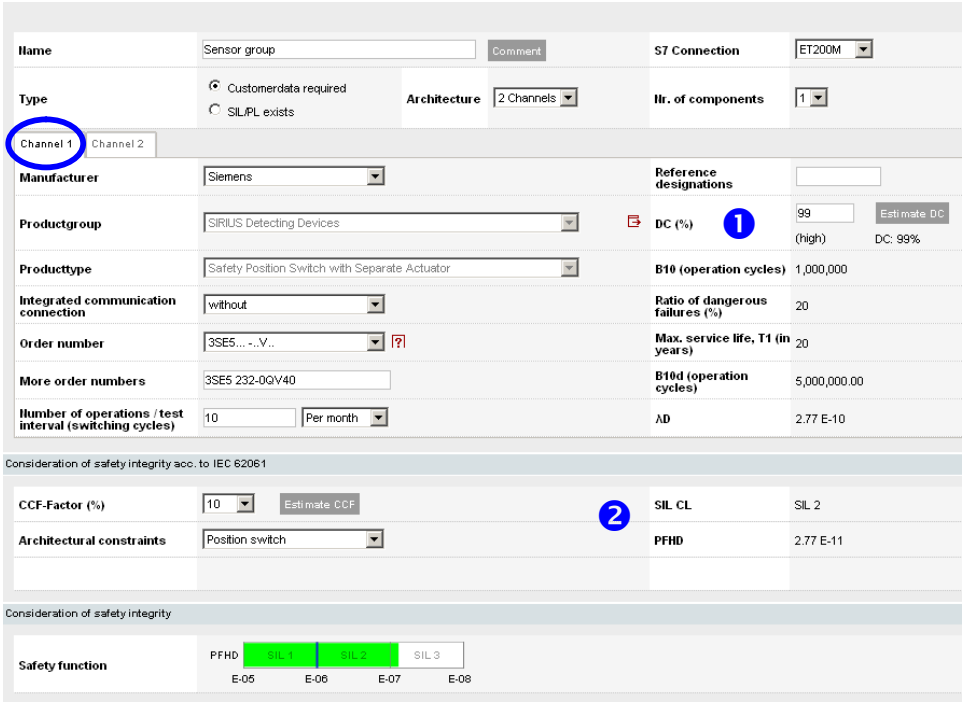
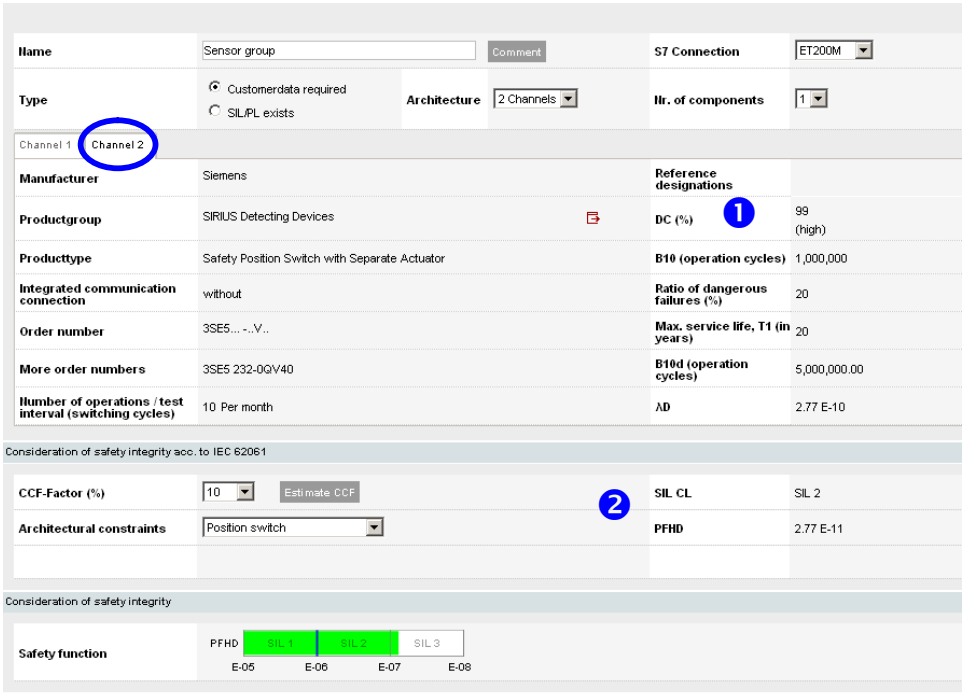



图 4-13 在 SET 中查看实现选件 2（通道 2）



**实现选件 3**

配备两个子系统元件的双通道结构。 可以对逻辑上的输入信号进行交叉比较，因此可达到 99% （高）的诊断覆盖系数 (DC) ❶。

图 4-14 在 SET 中查看实现选件 3（通道 1）

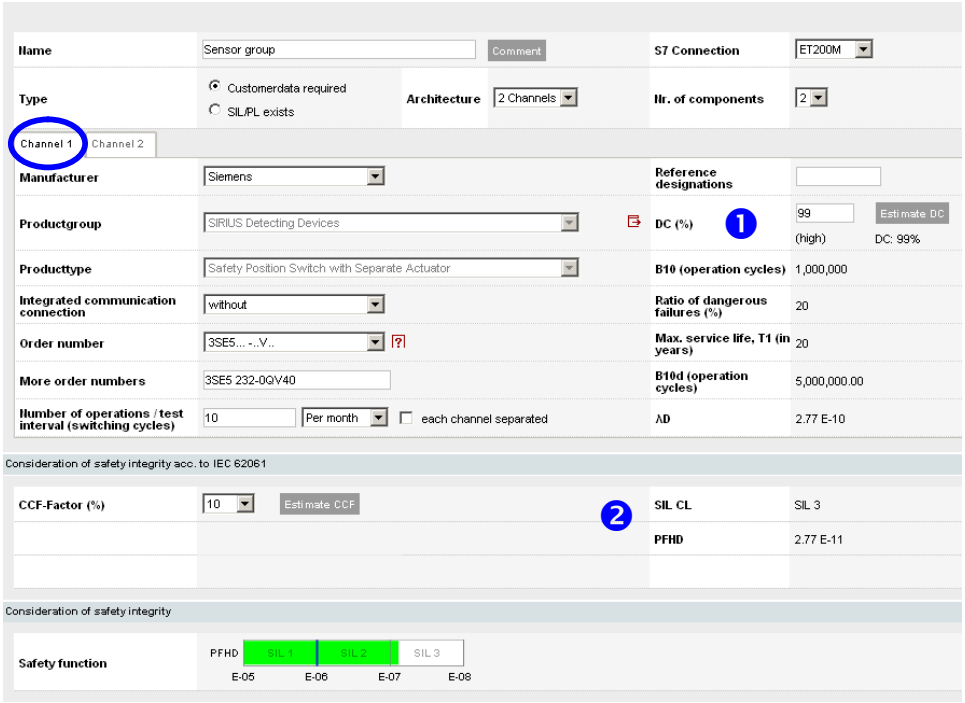
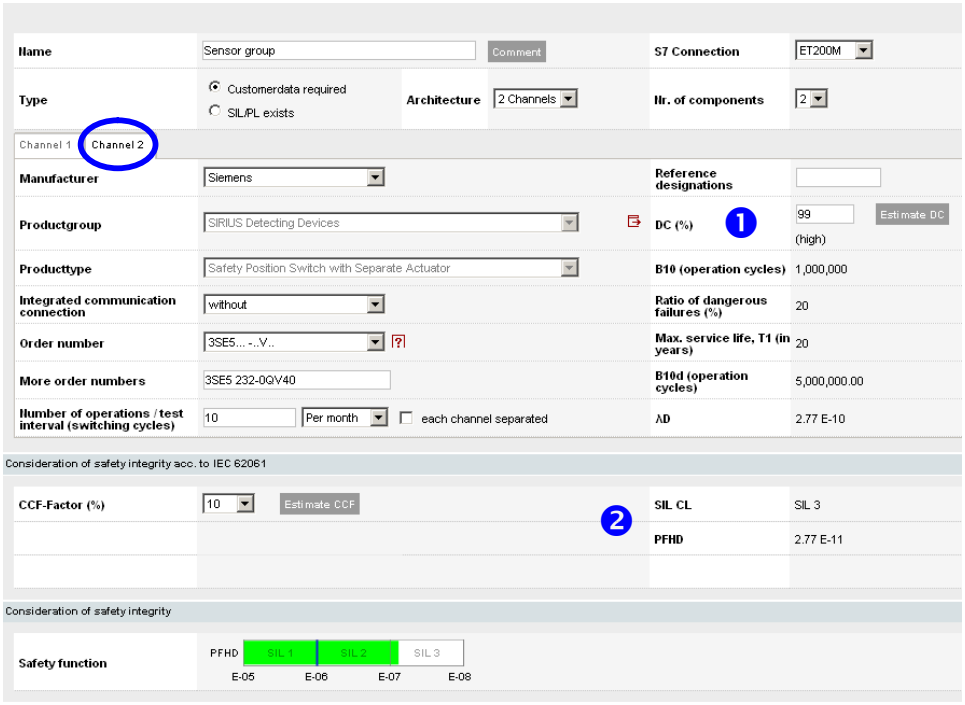



图 4-15 在 SET 中查看实现选件 3（通道 2）



通过安全评估工具 (SET) 在实现选件 2 和 3 中输入所有必要的数值与参数，便可立即读取 SIL 要求限制结果 (SIL CL) 以及相应的 $PFH_D$ 数值 ❷ 。

**实现选件的评价**

对于**实现选件 1**，其所能实现的最高安全完整性等级为 SIL CL 1，因此本应用中不考虑采用这种实现方式。

利用**实现选件 2** 和**实现选件 3** 可达到 SIL CL 2 的安全完整性等级，而且不存在任何问题。 因此，安全相关控制功能 (SRCF) 的子系统 2 要求这些开关类型具备双通道结构，或者是配备故障排除功能的机械单通道和电气双通道结构。

**请注意** 为了达到所需的 SIL 要求限制，必须一直完整记录所应用的故障排除。

**请注意** 为了进一步阐明安全完整性等级 (SIL) 的计算，本示例出于教学目的，将采用**实现选件 3** 来对防护罩的状态进行监测。

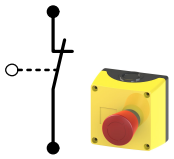
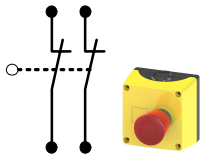
对于实现选件 2，也可以利用相似的方法来计算安全完整性等级 (SIL)。



## 4.2.7 功能块子系统 3：“紧急停止”

对于用来监测急停控制开关状态的子系统，根据表格所示，有两个选件可用于确定达到 SIL CL 2 的要求限制。

表 4-25 子系统 1 的实现选件

| **实现选件 1** | **实现选件 2** |
|---|---|
| 该子系统由一个子系统元件所组成 | 该子系统由一个子系统元件所组成 |
|  |  |
| • 单通道结构<br>⇨ 硬件故障容差 HFT = 0<br>• 所要求的安全失效分数：<br>90% ≤ SFF < 99% | • 双通道结构<br>⇨ 硬件故障容差 HFT = 0<br>• 所要求的安全失效分数：<br>90% ≤ SFF < 99% |

**请注意** 利用**实现选件 2** 的双通道结构，仅可实现 HFT = 0 的硬件故障容差，因为用于驱动两个触点的急停控制开关仅有一个。

根据章节 4.1.1 所提到的安全相关控制功能 1 (SRCF 1) 的要求，可以得到下述的执行次数以及测试间隔：

表 4-26

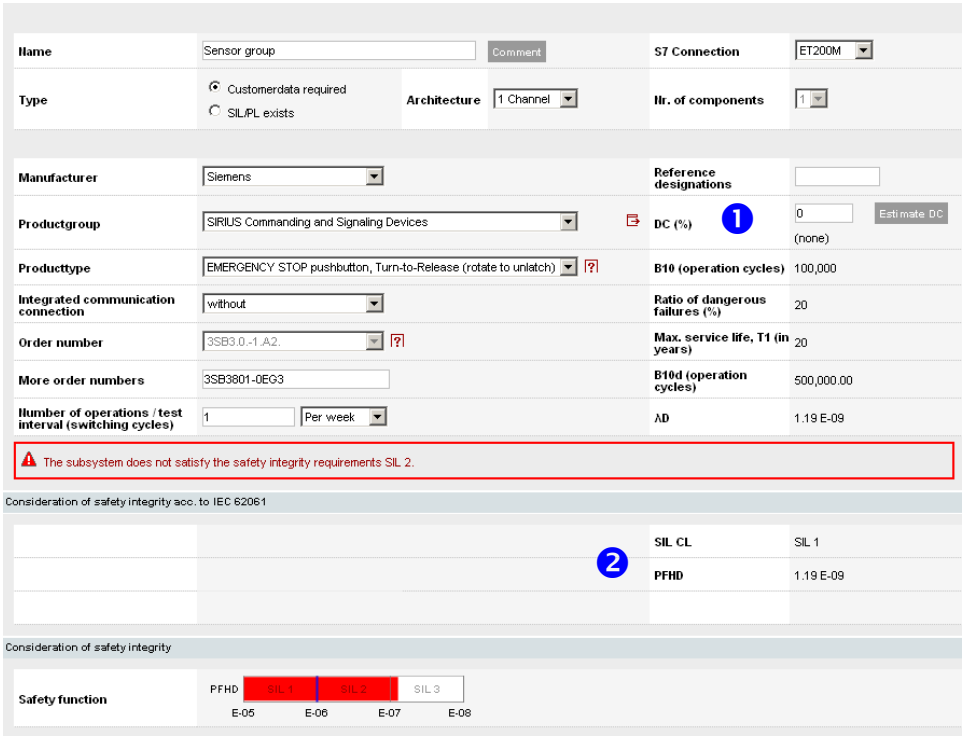
| SRCF 的要求 | 执行次数 / 测试间隔 |
|---|---|
| 操作员每周至少需要操作一次急停控制开关。<br>⇨ 每周 1 次 | 每周 1 次 |

利用手头上的这些信息，可通过安全评估工具 (SET) 来确定适用于各种实现选件的切实可行的安全完整性等级 (SIL)。

**实现选件 1**

配备一个子系统元件的单通道结构。由于这是一个单通道结构，因此无法对子系统进行诊断。结果 ❶ 得到 < 60%（无）的诊断覆盖系数 (DC)，该系数会直接输入到安全评估工具 (SET) 的画面中。

图 4-16 在 SET 中查看实现选件 1



**实现选件 2**

配备一个子系统元件的双通道结构。 可以对逻辑上的输入信号进行交叉比较，因此可达到 99% （高）的诊断覆盖系数 (DC) ❶。

图 4-17 在 SET 中查看实现选件 2（通道 1）

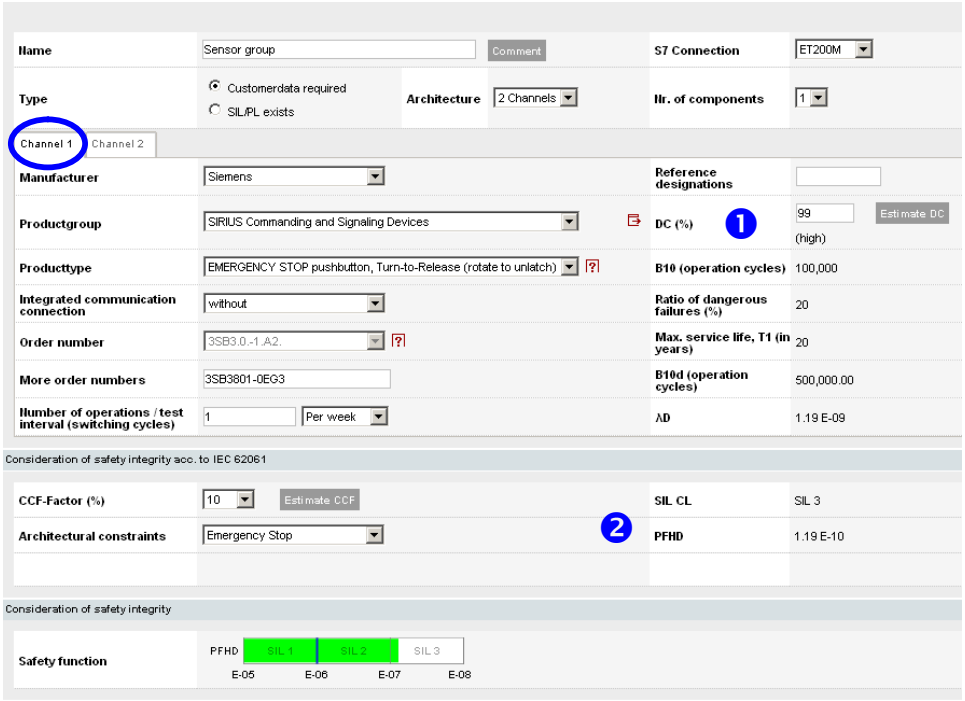
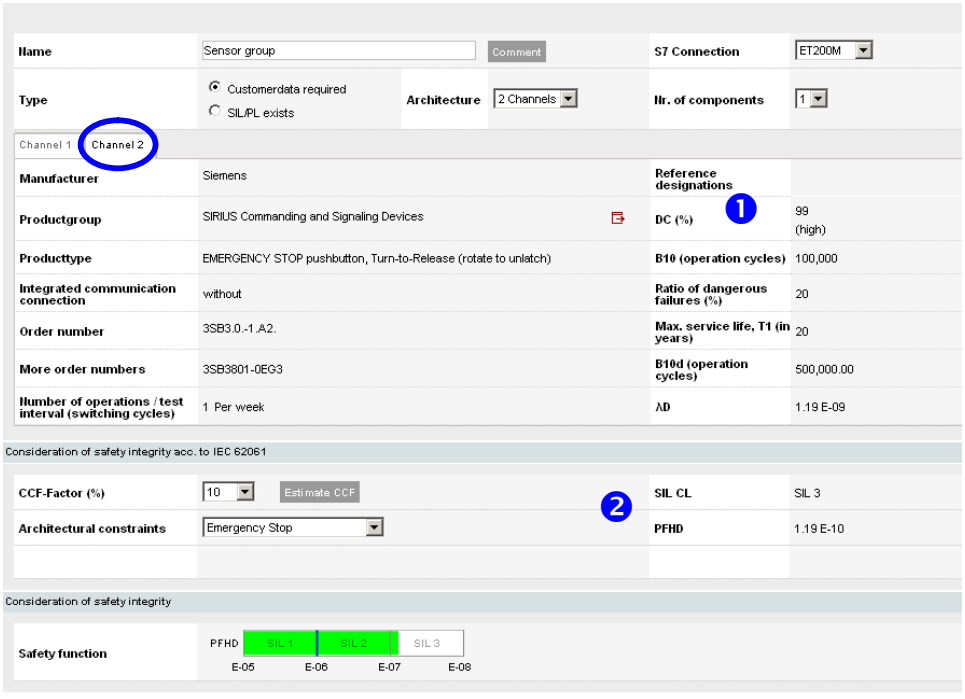



图 4-18 在 SET 中查看实现选件 2（通道 2）



**实现选件的评价**

对于实现选件 1，其所能实现的最高安全完整性等级为 SIL CL 1 ❷，因此本应用中不考虑采用这种实现方式。

利用实现选件 2 可达到 SIL CL 2 的安全完整性等级，而且不存在任何问题 ❷。因此，安全相关控制功能 (SRCF) 的子系统 3 必须配备带有这些位置开关类型的双通道结构。

## 4.2.8 功能块子系统 4

对于子系统 4，将结合使用故障安全 Technology CPU 317TF-2 DP 以及故障安全输入模块 SM 326 – DI 24xDC24V。根据制造商所提供的数据，这两个模块可实现 SIL CL 3 的安全完整性等级。

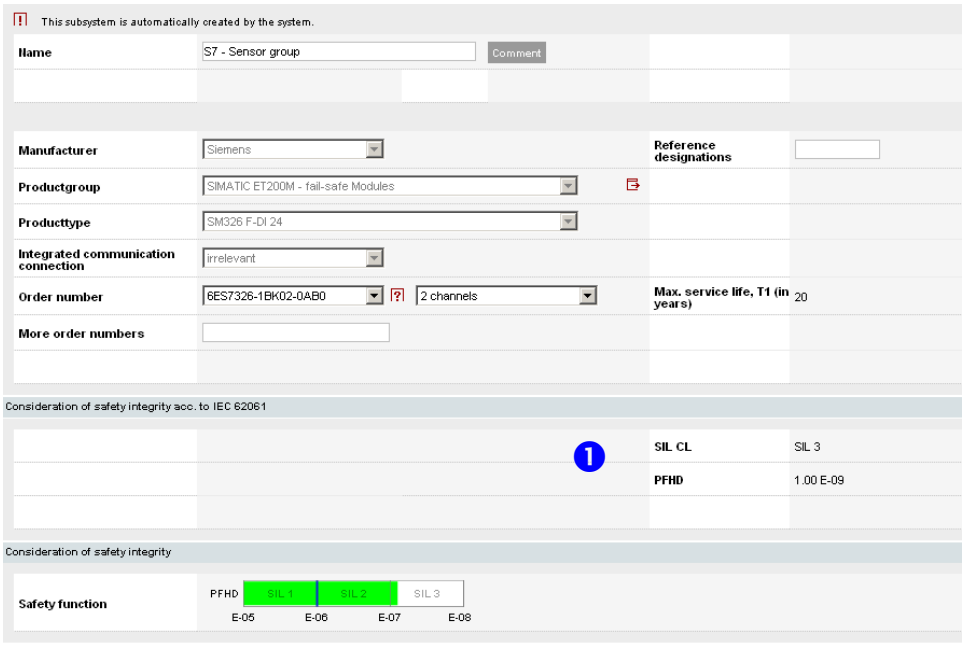
在安全评估工具 (SET) 中，必须相互独立地输入以及评估这两个模块：

- 将 Technology CPU 317T-2 DP 创建为“Logic group”（逻辑组）
- 故障安全输入模块 SM 326 – DI 24xDC24V 创建为“S7 sensor group(S7 传感器组)”。

**请注意** 如果在安全评估工具 (SET) 的“Detection（检测）”功能块中为传感器的 S7 连接分别选择了“ET200M”设置，那么 S7 传感器组将会自动插入到安全评估工具 (SET) 的“Evaluate（评估）”子系统当中。

图 4-19 在 SET 中查看逻辑组

图 4-20 在 SET 中查看 S7 传感器组




在安全评估工具 (SET) 中选择所使用的硬件组件，便直接可得 SIL 要求限制 (SIL CL) 结果以及相应的 $PFH_D$ 数值 ❶ 。

## 4.2.9 功能块子系统 5

子系统 5 使用了故障安全 SINAMICS S120 驱动器，根据制造上所提供的数据，该驱动器最高可实现 SIL CL 2。

必须在安全评估工具 (SET) 中输入 SINAMICS S120 的各个组件（包括所使用的电机以及编码器）的驱动。执行这一步骤有两种不同的方式：

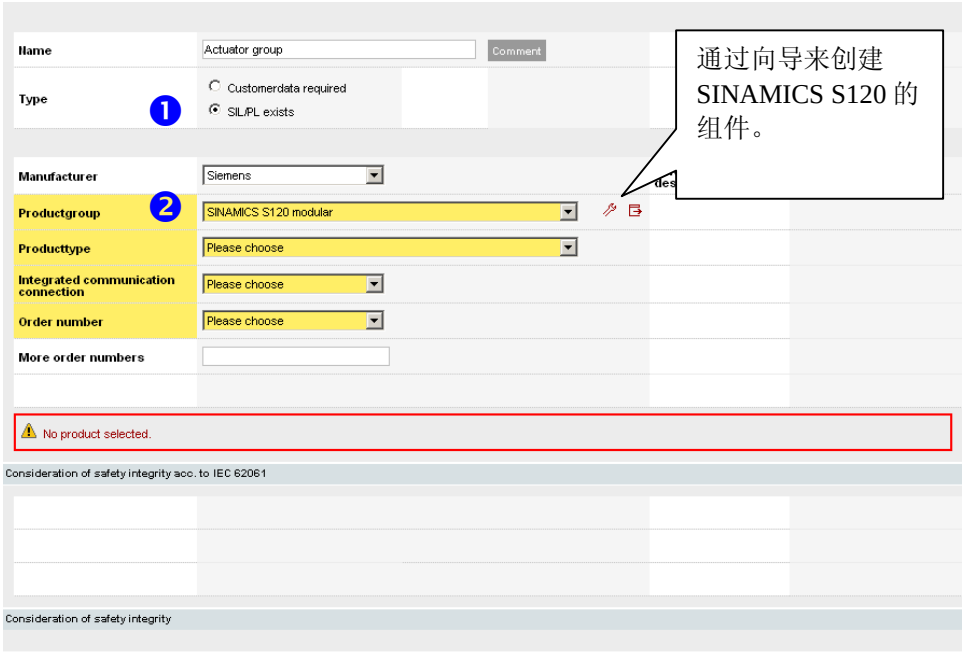
- 使用向导来输入 SINAMICS S120 的各个组件
- 手动输入 SINAMICS S120 的各个组件

### 使用向导来输入 SINAMICS S120 的各个组件

对于利用向导来输入 SINAMICS S120 组件的方式，必须先在“Reaction（反应）”功能块中创建一个执行器组作为新的子系统。

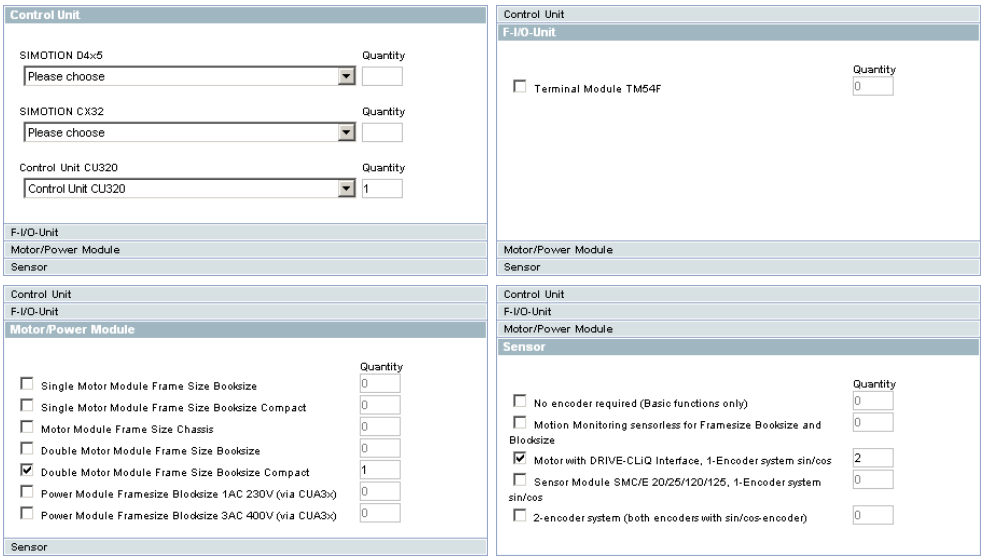
相应地，将所创建的执行器组选为“SIL/PL exists”类型 ❶，并输入为“SINAMICS S120 modular”产品组 ❷。然后，便可通过安全评估工具 (SET) 上的螺丝刀图标来访问用于输入 SINAMICS S120 组件的向导。

图 4-21 在 SET 中调用向导




现在需要填写向导各个画面中的信息，然后便会在安全评估工具 (SET) 中创建 SINAMICS S120 的各个组件。

图 4-22 用于选择子系统 5 的子结构的向导 (SINAMICS S120)




**请注意**

在安全评估工具 (SET) 的驱动系统所选结构中，无须查看 SINAMICS S120 的 “Smart Line Module（智能线路模块）”整流器/发电设备，因为这一操作与该配置的计算无关。

然后，需要在安全评估工具 (SET) 中完整填写各个组件的数据，如下图所示。

**手动输入 SINAMICS S120 的各个组件**

图 4-23 在 SET 中查看控制单元

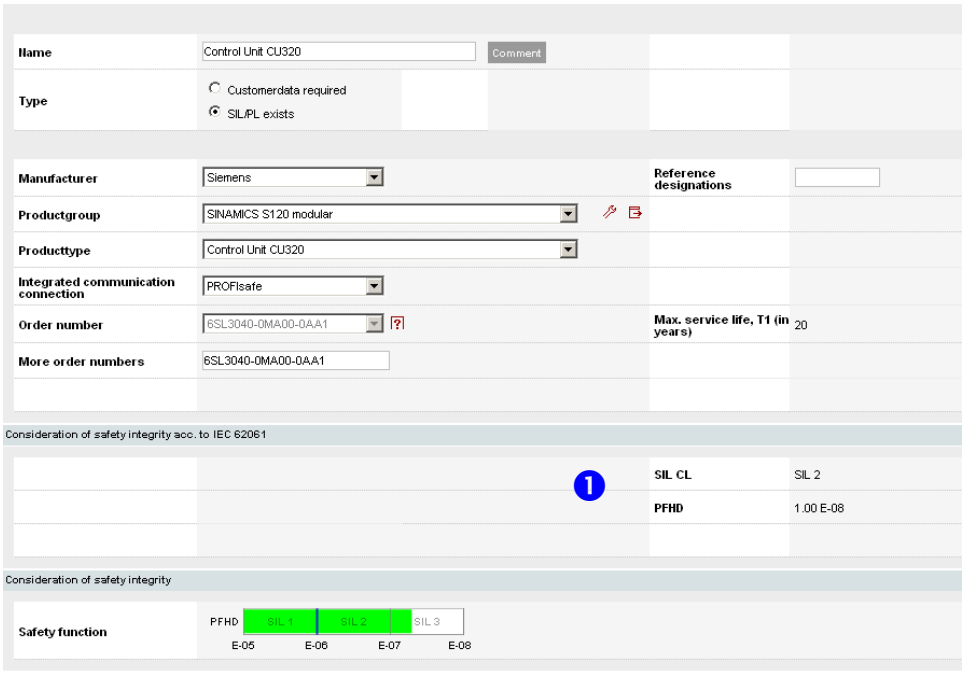



图 4-24 在 SET 中查看双电机模块

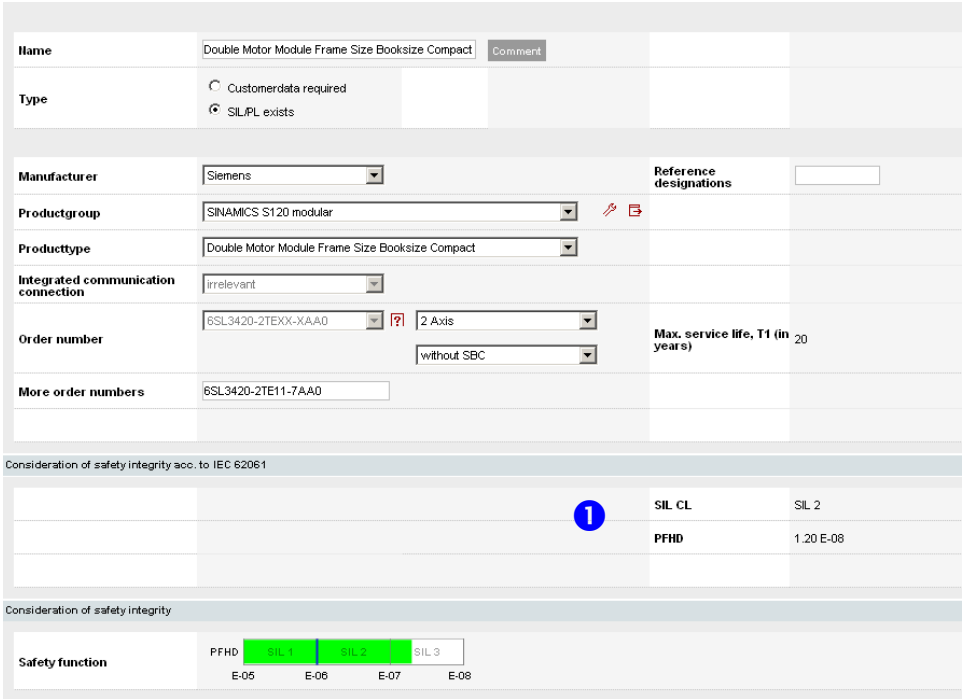


图 4-25 在 SET 中查看电机 1（暴露机轴）

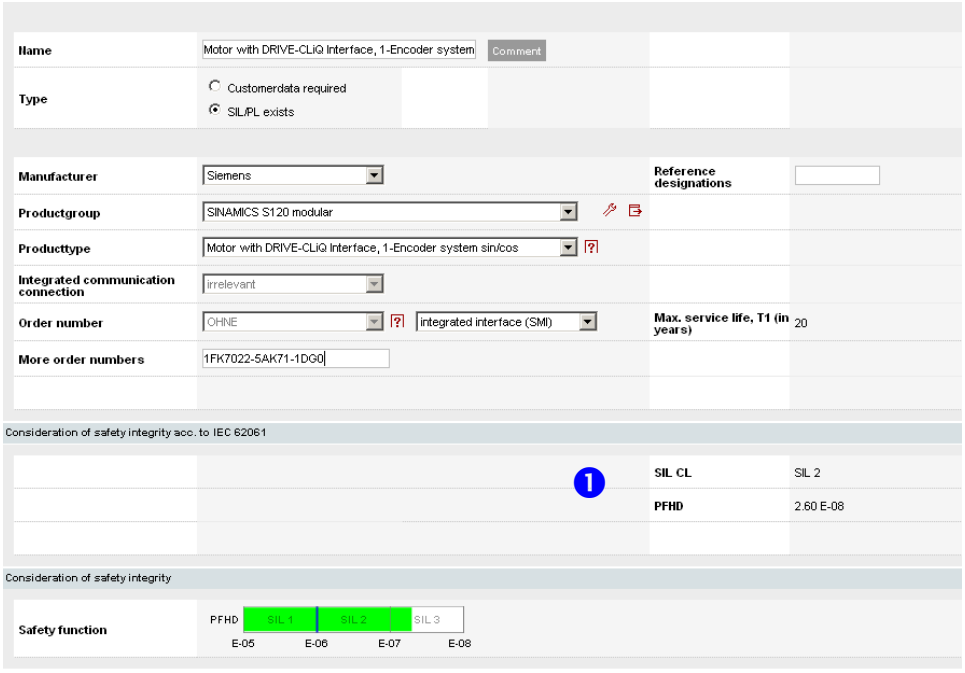
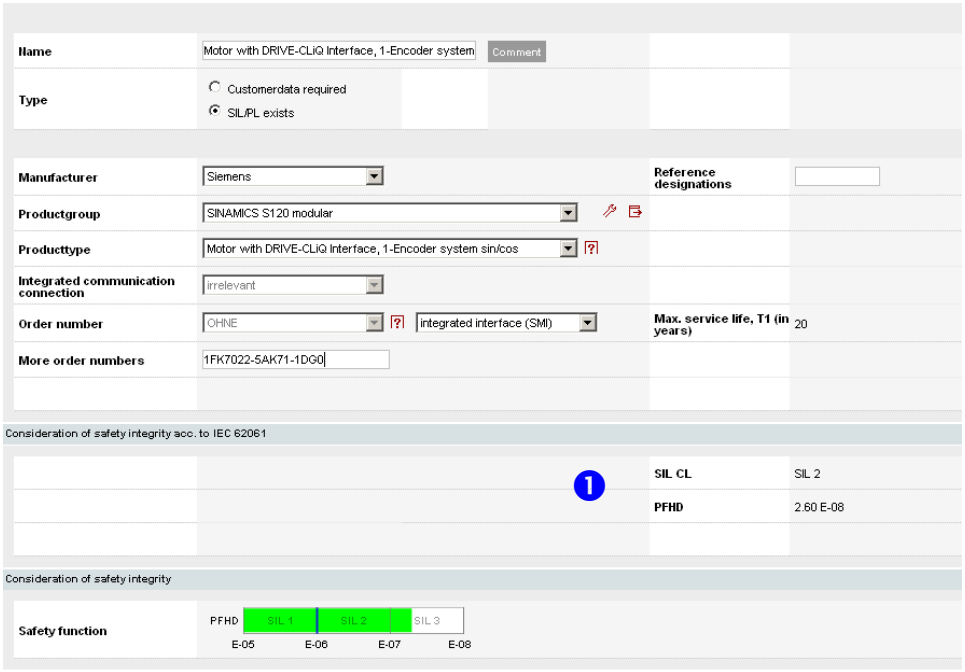



图 4-26 在 SET 中查看电机 2（封闭机轴）




在安全评估工具 (SET) 中为子系统 5 选择所使用的硬件组件并指定 SINAMICS S120 的子结构，便直接可得 SIL 要求限制 (SIL CL) 结果以及相应的 $PFH_D$ 数值 ❶ 。

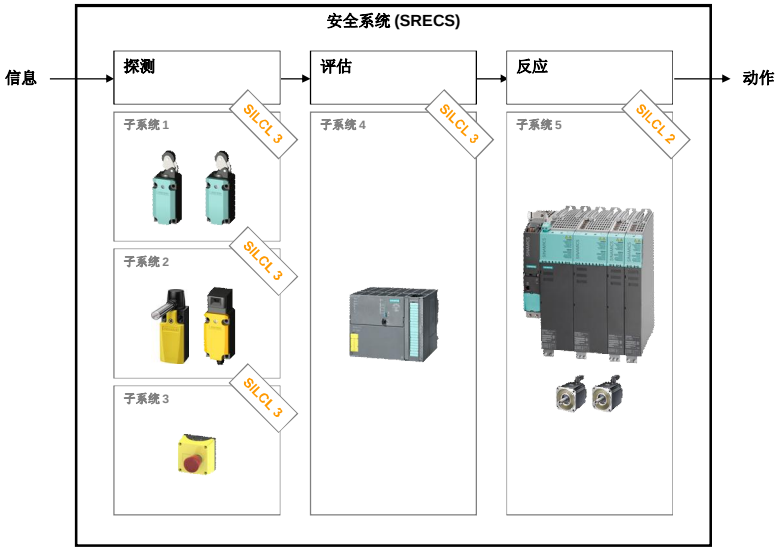
### 4.2.10 总结

下表列出了安全相关控制功能 (SRECS) 的各个功能块分配到安全系统 (SRECS) 子系统的情况。

表 4-27 安全系统 (SRECS) 的子系统

| 子系统 | 作用 | 组件 |
|---|---|---|
| 子系统 1 | 检测防护门的位置<br>(SRCF 1) | SIRIUS |
| 子系统 2 | 检测防护罩的位置。<br>(SRCF 2) | SIRIUS |
| 子系统 3 | 检测急停控制开关的状态。<br>(SRCF 3) | SIRIUS |
| 子系统 4 | 信号评估<br>(SRCF 1 / SRCF 2 / SRCF 3) | SIMATIC S7<br>Distributed Safety |
| 子系统 5 | 根据评估信号作出反应<br>(SRCF 1 / SRCF 2 / SRCF 3) | SINAMICS |

图 4-27 安全系统 (SRECS)




## 4.3 子系统的实现

完成了安全系统 (SRECS) 的架构设计之后，最后一步便是 SRECS 子系统的实现。

SRECS 安全系统的实现必须满足所需 SIL 的全部要求。其目标在于充分降低发生故障的概率，避免设备造成危险。

以下是子系统实现所需要考虑的因素：

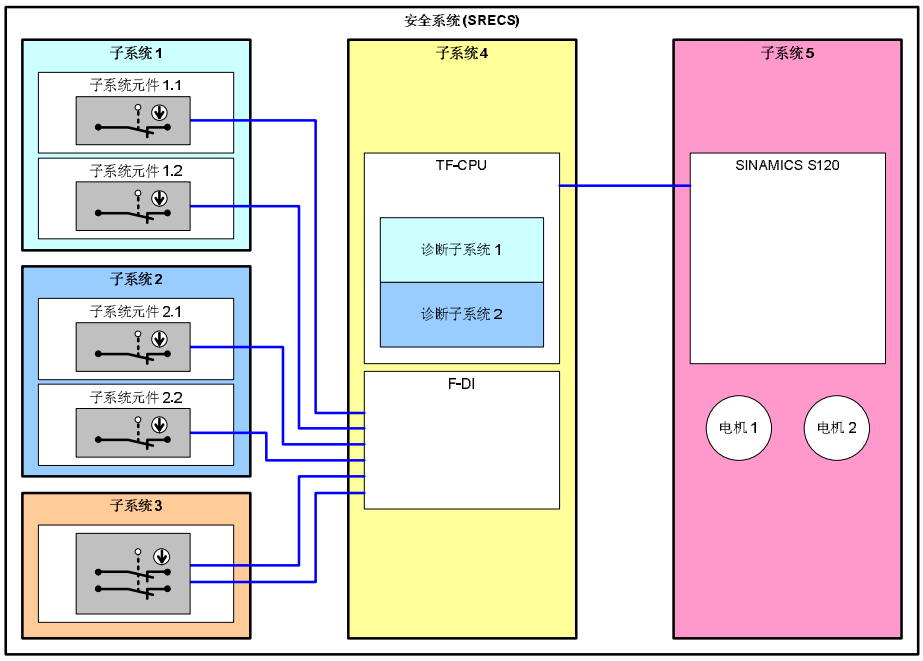
- 结构限制的考虑
  子系统的结构（架构）实现必须使得子系统的 SIL 要求限制至少与安全相关控制功能 (SRCF) 的安全完整性等级 (SIL) 相等。

- $PFH_D$ 值 ($PFH_D$) 的考虑
  安全相关控制功能 (SRCF) 的 $PFH_D$ 值 ($PFH_D$) 等于子系统 $PFH_D$ 值 ($PFH_D$) 的总和。 因此，子系统的实现必须使该值不超过 SRCF 总的 $PFH_D$ 值 ($PFH_D$)。
- 诊断方面的考虑
  附加的诊断功能可以让子系统设计的 SIL 要求限制 (SILCL) 得到提高。
  - 增强的诊断功能提升了安全失效分数 (SFF)
    （获得更好的故障检测性能）
  - 增强的诊断功能改善了 $PFH_D$ 值 ($PFH_D$)
    （$PFH_D$ 得到降低）

  所关注的子系统并不需要对其本身执行诊断功能。 比如，子系统 1 的诊断可以在子系统 4 中执行。
- 系统化安全完整性等级的考虑
  在子系统中，必须采取措施来实现系统化的安全完整性 以下是可分别采取的措施（按照 \5\）：
  - 避免系统故障
  - 控制系统故障（比如通过诊断的方式）

本应用示例的子系统实现概览如下图所示：

图 4-28 安全系统 (SRECS) 的结构概览



下表列出了用于最终实现安全系统 (SRECS) 的硬件组件。

表 4-28 硬件组件清单

| 硬件组件 | | 订单号 | 制造商 |
|---|---|---|---|
| 1.1 | 位置开关<br>触头：1 NO + 1 NC | 3SE5 232-0HE10 | 西门子有限公司 |
| 1.2 | 位置开关<br>触头：1 NO + 1 NC | 3SE5 232-0HE10 | |
| 2.1 | 铰接开关<br>触头：1 NO + 1 NC<br>开关角度：10° | 3SE5 232-0HU22 | |
| 2.2 | 配备独立操纵的位置开关<br>触头：1 NO + 2 NC | 3SE5 232-0QV40 | |
| | 标准执行器 | 3SE5 000-0AV01 | |
| 3 | 配备执行器的急停控制开关盒：<br>触头：2 NC | 3SB3801-0EG3 | |
| 4 | CPU 317TF-2 DP | 6ES7317-6TF14-0AB0 | 西门子有限公司 |
| | SM 326 – DI 24xDC24V | 6ES7326-1BK02-0AB0 | |
| 5 | SINAMICS S120 | 取决于版本 | 西门子有限公司 |
| | 控制单元<br>CU 320 | 6SL3040-0MA00-0AA1 | |
| | 整流器/发电设备<br>智能线路模块 | 6SL3430-6TE21-6AA0 | |
| | 动力单元<br>双电机模块 | 6SL3420-2TE11-7AA0 | |
| | 伺服电机<br>1FK7 电机 | 1FK7022-5AK71-1DG0 | |

# 5 确定由 SRECS 所实现的 SIL

## 5.1 利用安全评估工具 (SET) 进行评估

### 5.1.1 所要求的 SIL 条件

本章节内容将会检查所实现的安全系统 (SRECS) 的每项安全相关控制功能 (SRCF) 是否达到要求的安全完整性等级 (SIL)。

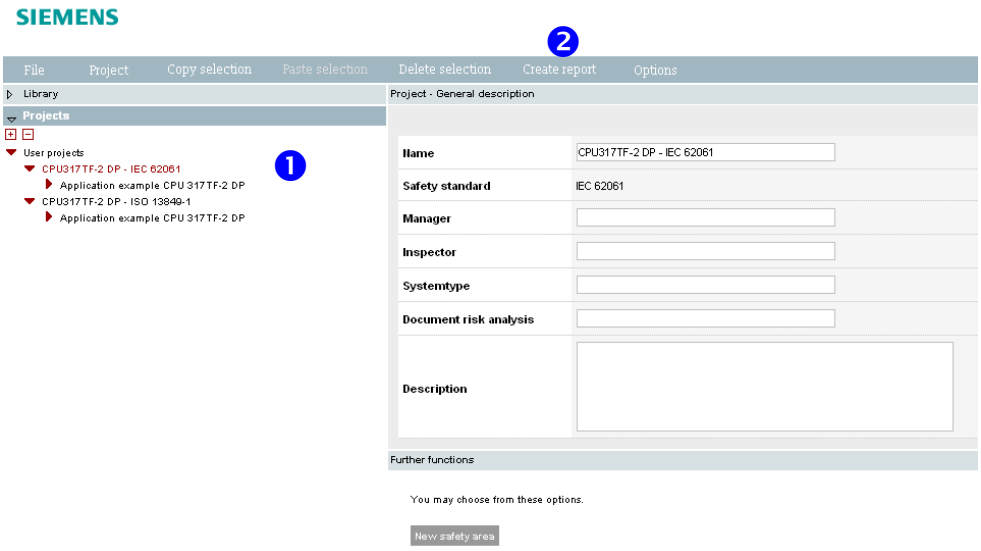
必须实现以下的条件：

- 每个 SRCF 子系统的 SIL 要求限制 (SILCL) 必须至少对应于 SRCF 的安全完整性等级 (SIL) 。
- 所有 SRCF 子系统的 $PFH_D$ 值 ($PFH_D$) 总和不应超过由 SRCF 的安全完整性等级 (SIL) 所规定的 $PFH_D$ 值 ($PFH_D$)。
- 如果某个子系统被不同的 SRCF 所使用，那么该子系统的 SIL 要求限制 (SILCL) 必须符合 SRCF 的最高安全完整性等级 (SIL)。

### 5.1.2 安全评价工具 (SET) 的结果报告

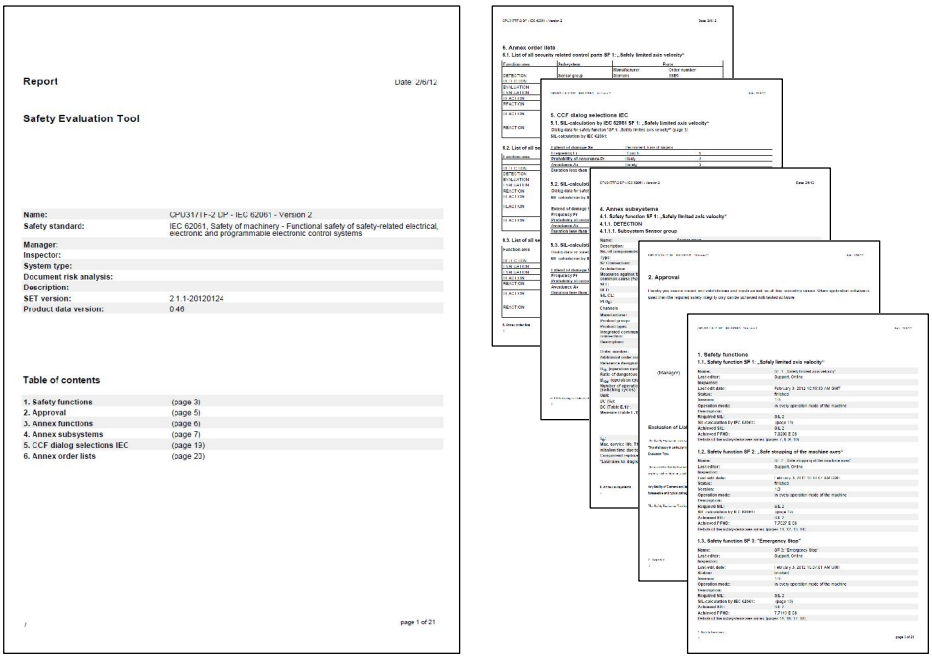
上述条件可以在给定的安全评估工具 (SET) 中通过结果报告进行评价和应用。

图 5-1 在 SET 中创建报告




要在安全评估工具 (SET) 中创建报告，首先应在项目树 ❶ 中选择所需的项目，然后点击工具栏上的“Create report（创建报告）”按钮 ❷。然后便可下载 PDF 格式的报告文件。

图 5-2 PDF 报告文件


Report

Date 2/9/12

Safety Evaluation Tool

| | |
|---|---|
| Name: | CPU317T-2 DP - IEC 62061 - Version 2 |
| Safety standard: | IEC 62061, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems |
| Manager: | |
| Inspector: | |
| System type: | |
| Document risk analysis: | |
| Description: | |
| SET version: | 2.1.1-20120124 |
| Product data version: | 0.46 |

Table of contents



page 1 of 21

## 5.2 安全相关的控制功能 1 (SRCF 1)

表 5-1

| SRCF | 具体的 SRCF |
|---|---|
| 1 | 将暴露机轴的转速降低至安全上限速度以内。 |

图 5-3 SRECS 的安全相关控制功能 1 (SRCF 1)

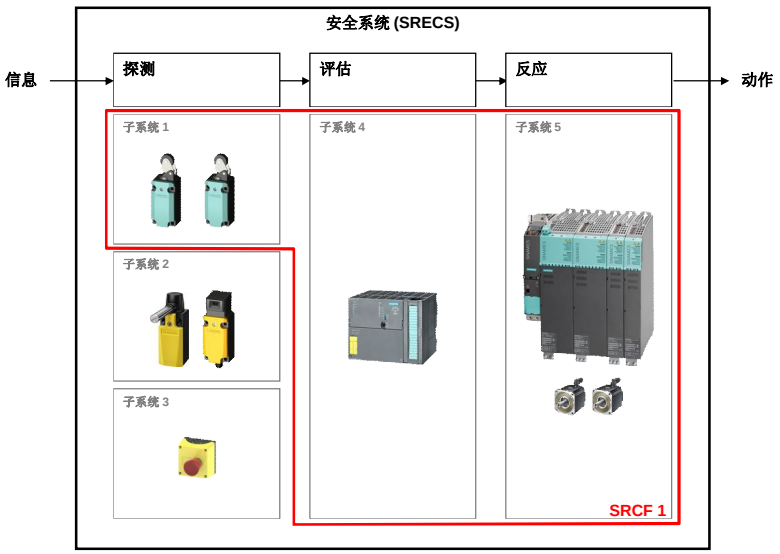


图 5-4 安全相关控制功能 1 (SRCF 1) 的结果报告

| | |
|---|---|
| **Name:** | SF 1: „Safely limited axis velocity“ |
| **Last editor:** | Support, Online |
| **Inspector:** | |
| **Last edit date:** | February 3, 2012 10:15:30 AM GMT |
| **Status:** | finished |
| **Version:** | 1.0 |
| **Operation mode:** | In every operation mode of the machine |
| **Description:** | |
| **Required SIL:** | SIL 2 |
| **SIL-calculation by IEC 62061:** | (page 19) |
| **Achieved SIL:** | SIL 2 |
| **Achieved PFHD:** | 7.8200 E-08 |
| Details of the subsystems see annex (pages 7, 8, 9, 10) | |

**结果**

安全相关控制功能 1 (SRCF 1) 达到了所要求的安全完整性等级 SIL 2。

**请注意**

根据 $PFH_D$ 值，该安全相关控制功能 (SRCF 1) 甚至还能满足 SIL 3 的安全完整性等级。由于子系统 5 的 SIL CL 最小值限制，所以安全相关控制功能 1 (SRCF 1) 仅可达到 SIL 2 的等级水平。



## 5.3 安全相关的控制功能 2 (SRCF 2)

表 5-2

| SRCF | 具体的 SRCF |
|---|---|
| 2 | 立即停止设备上的两根机轴。 |

图 5-5 SRECS 的安全相关控制功能 2 (SRCF 2)

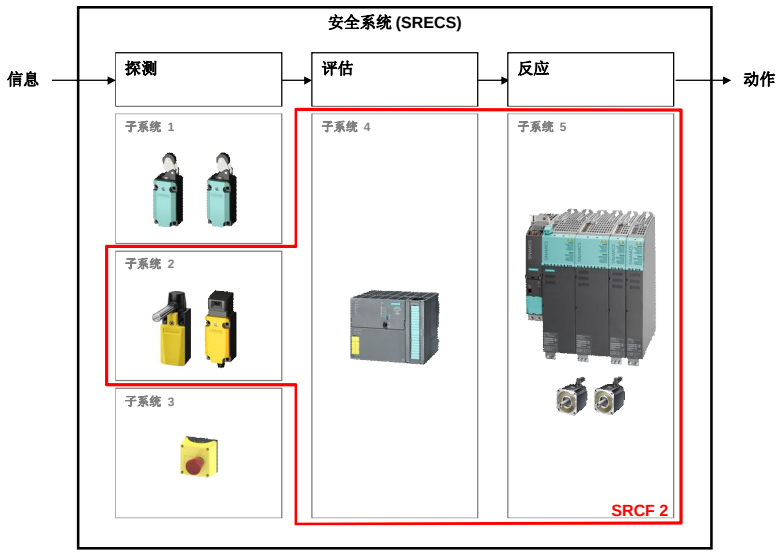


图 5-6 安全相关控制功能 2 (SRCF 2) 的结果报告

| | |
|---|---|
| **Name:** | SF 2: „Safe stopping of the machine axes“ |
| **Last editor:** | Support, Online |
| **Inspector:** | |
| **Last edit date:** | February 3, 2012 10:14:07 AM GMT |
| **Status:** | finished |
| **Version:** | 1.0 |
| **Operation mode:** | In every operation mode of the machine |
| **Description:** | |
| **Required SIL:** | SIL 2 |
| **SIL-calculation by IEC 62061:** | (page 19) |
| **Achieved SIL:** | SIL 2 |
| **Achieved PFHD:** | 7.7027 E-08 |
| Details of the subsystems see annex (pages 11, 12, 13, 14) | |

**结果**

安全相关控制功能 2 (SRCF 2) 达到了所要求的安全完整性等级 SIL 2。

**请注意**

根据 $PFH_D$ 值，该安全相关控制功能 (SRCF 2) 甚至还能满足 SIL 3 的安全完整性等级。由于子系统 5 的 SIL CL 最小值限制，所以安全相关控制功能 2 (SRCF 1) 仅可达到 SIL 2 的等级水平。



## 5.4 安全相关的控制功能 3 (SRCF 3)

表 5-3

| SRCF | 具体的 SRCF |
|---|---|
| 3 | 紧急停止设备上的所有机轴。 |

图 5-7 SRECS 的安全相关控制功能 3 (SRCF 3)

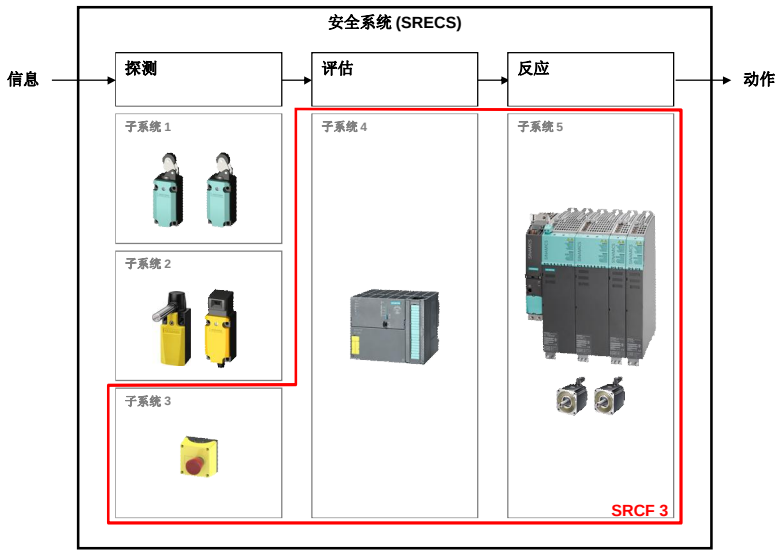


图 5-8 安全相关控制功能 3 (SRCF 3) 的结果报告

| | |
|---|---|
| **Name:** | SF 3: "Emergency Stop" |
| **Last editor:** | Support, Online |
| **Inspector:** | |
| **Last edit date:** | February 3, 2012 10:07:01 AM GMT |
| **Status:** | finished |
| **Version:** | 1.0 |
| **Operation mode:** | In every operation mode of the machine |
| **Description:** | |
| **Required SIL:** | SIL 2 |
| **SIL-calculation by IEC 62061:** | (page 19) |
| **Achieved SIL:** | SIL 2 |
| **Achieved PFHD:** | 7.7119 E-08 |
| Details of the subsystems see annex (pages 15, 16, 17, 18) | |

**结果**

安全相关控制功能 3 (SRCF 3) 达到了所要求的安全完整性等级 SIL 2。

**请注意**

根据 $PFH_D$ 值，该安全相关控制功能 (SRCF 3) 甚至还能满足 SIL 3 的安全完整性等级。由于子系统 5 的 SIL CL 最小值限制，所以安全相关控制功能 3 (SRCF 1) 仅可达到 SIL 2 的等级水平。



## 5.5 SRECS 的执行

安全系统 (SRECS) 将按照以下步骤来执行：

**硬件的实现**

安全系统 (SRECS) 必须按照 SRECS 的文档设计来实现。

**指定软件**

在该应用中，需要通过应用软件来实现安全相关控制功能 (SRCF)。该应用软件将由子系统 4 的故障安全 CPU 来执行。

根据 IEC 62061，必须为该软件制订一个规范。

**软件的设计与开发**

根据 IEC 62061，章节 6.10 所指定的应用软件，必须根据 IEC 62061 的要求来实现。这些都是在 IEC 61508 的基础上提出的要求。

**整合与测试**

安全系统 (SRECS) 必须根据 IEC 62061 的要求来进行整合。而且还必须经过测试，审查所有子系统与子系统元件（包括应用软件）之间是否能够正确地进行交互。 这些测试必须在安全计划（测试案例）中定义，然后相应地执行。

**安装**

安装完毕之后，该安全系统 (SRECS) 便等待进行验证。

# 6 用户信息与验证

## 6.1 生成用户信息

为了确保 SRECS 在使用和维护过程中能够实现功能化的安全性，必须创建包含有以下元素的用户信息，比如：

- 设备、安装以及固定的说明
- 电路图
- 验证试验时间间隔或者生命周期
- SRECS 与设备之间的交互说明
- SRECS 的维护要求说明

## 6.2 执行验证

验证过程将会在安全计划的基础上检查安全系统 (SRECS) 是否满足“Specification of the safety function （安全功能规范，SRCF）”中所述的要求。

以下是验证的要求：

- 必须记录所有的测试
- 必须通过测试和/或分析来验证每项 SRCF。
- 必须验证 SRECS 的系统化安全完整性。

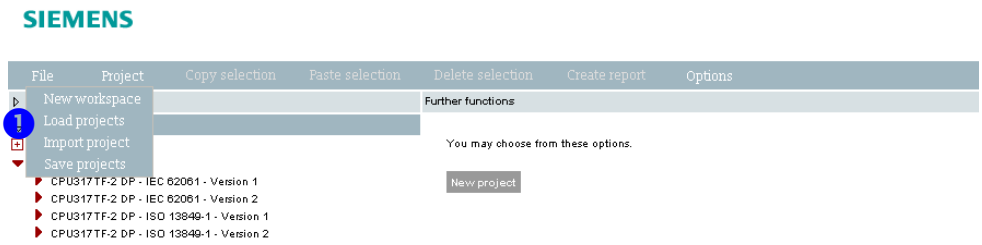
执行验证之后，便完成了满足 IEC 62061 要求的安全系统 (SRECS) 生成过程。

# 7 本应用示例的项目文件

## 7.1 下载项目文件

关于本应用示例，安全评估工具 (SET) 的项目文件可通过下载获得。

图 7-1 下载项目文件




利用 “File （文件）” > “Load projects （下载项目）” ❶，可将本应用示例的项目文件下载至安全评估工具 (SET) 当中。

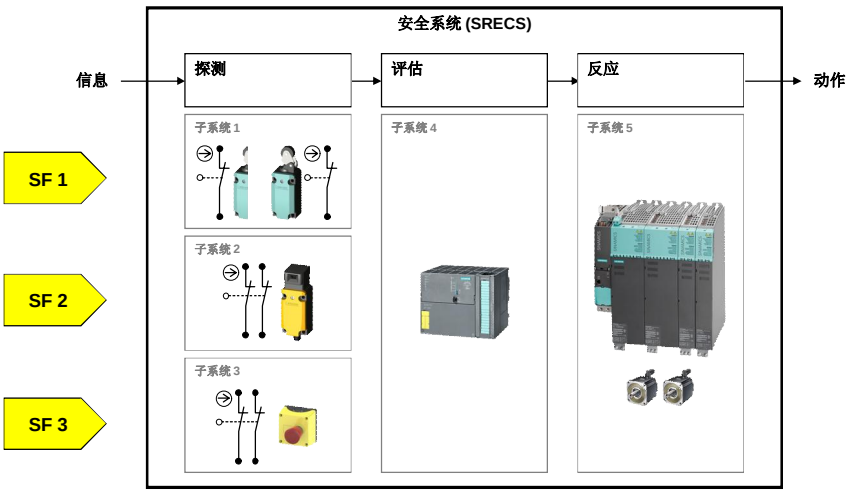
## 7.2 项目文件的内容

项目文件中包含有符合 IEC 62061 要求的安全完整性等级 (SIL) 计算或者符合 ISO 13849-1 的性能等级 (PL)，分别对应于本文档所述的两种安全系统 (SRECS) 变体。

### 7.2.1 安全系统 (SRECS) 的变体 1

项目文件中所包含的安全系统 (SRECS) 变体 1 如下所示：

图 7-2 安全系统 (SRECS) 的变体 1

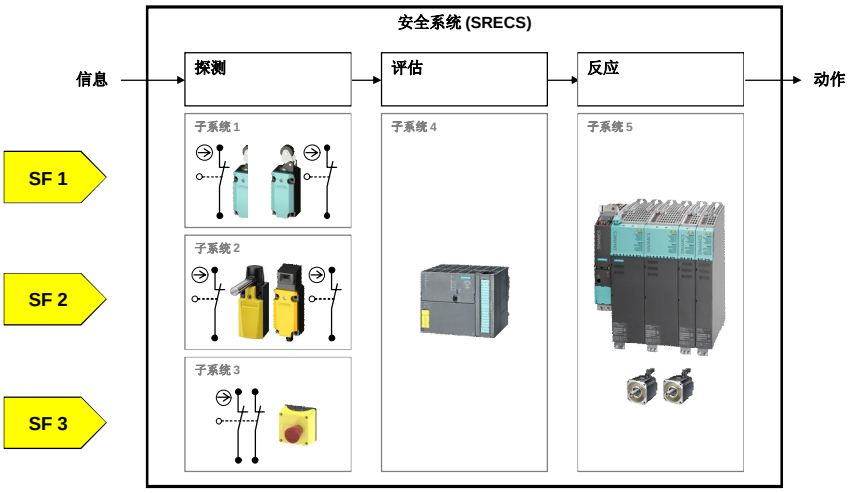


安全系统 (SRECS) 的子系统 2 将根据本文档所述的实现选件 2 来实现。根据本文档所述的实现选件，所有其它子系统均包含在内。

### 7.2.2 安全系统 (SRECS) 的变体 2

项目文件中所包含的安全系统 (SRECS) 变体 2 如下所示：

图 7-3 安全系统 (SRECS) 的变体 2




安全系统 (SRECS) 的子系统 2 将根据本文档所述的实现选件 3 来实现。根据本文档所述的实现选件，所有其它子系统均包含在内。

# 8 链接与文献

## 8.1 其它文献

下述列表中的内容并不完整，仅提供一部分相关文献以供参考。

表 8-1

| | 主题 | 标题 |
|---|---|---|
| /1/ | 安全性<br>功能示例 | 适用于工厂自动化的 SIMATIC 安全性集成<br>通过 SIMATIC S7 Distributed Safety 的应用示例来解释 IEC 62061 的实际应用<br>（功能示例：AS-FE-I-013-V12-DE）<br>西门子有限公司<br>订单号 6ZB5310-0NM01-0BA0 |

## 8.2 Internet 链接

本列表所列出的文献内容并不完备，仅提供部分相关信息以供参考。

表 8-2

| | 主题 | 标题 |
|---|---|---|
| \1\ | 本文档的引用链接 | http://support.automation.siemens.com/WW/view/en/47393794 |
| \2\ | 西门子 I IA/DT 客户支持 | http://support.automation.siemens.com |
| \3\ | 安全评估工具 | http://www.siemens.de/safety-evaluation-tool |
| \4\ | 标准 | 标准的订购<br>http://www.iec-normen.de<br>标准的官方状态：<br>http://www.dke.de<br>欧盟官方公报上的统一标准清单<br>http://www.newapproach.org/ |
| \5\ | 西门子<br>安全性集成 | 西门子的安全性集成<br>http://www.automation.siemens.com/mcms/safety-integrated/de/Seiten/funktionale-sicherheit.aspx<br>安全性集成的系统手册<br>http://support.automation.siemens.com/WW/view/de/12490443 |
| \6\ | 西门子<br>安全性集成<br>功能示例 | 适用于工厂自动化的 SIMATIC 安全性集成<br>通过 SIMATIC S7 Distributed Safety 的应用示例来解释 IEC 62061 的实际应用<br>（功能示例：AS-FE-I-013-V12-DE）<br>http://support.automation.siemens.com/WW/view/en/23996473<br><br>安全性集成的功能示例<br>http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&siteid=csius&aktprim=4&extranet=standard&viewreg=WW&objid=20810941&treeLang=en<br>手册和 CD 的订单号<br>6ZB5310-0MK01-0BA0 |

下表所列出的 Internet 文档链接可提供计算所要求的信息和数值：

表 8-3

| | 主题 | 标题 |
|---|---|---|
| \A\ | SIMATIC<br>$PFH_D$ 值 | FAQ：<br>F-CPU 和 ET 200 系列产品的 PFD, PFH 和验证测试时间间隔都是哪些数值?<br>http://support.automation.siemens.com/WW/view/en/27832836 |
| \B\ | SINAMICS S/G<br>$PFH_D$ 值 | FAQ：<br>配备集成安全功能的驱动系统 SINAMICS S120、SINAMICS S150、SINAMICS G130 以及 SINAMICS G150 的 PFH 值。<br>http://support.automation.siemens.com/WW/view/en/28556736<br><br>**请注意：**<br>相应的文档仅可从西门子内部网络中获取 请联系您的销售代表、技术顾问或者 SINAMICS 热线。本文档正准备发布到因特网上。 |
| \C\ | SINAMICS G<br>$PFH_D$ 值 | FAQ：<br>SINAMICS G120，G120D，SIMATIC ET200S：用于确定所达到的安全完整性的安全值 (PFHD, PFD, PFH)<br>http://support.automation.siemens.com/WW/view/en/31593618 |
| \D\ | SIRIUS<br>B10 值 | 技术援助的建议：<br>关于 DIN EN 62061 应用中的标准 B10 值建议。<br>请通过邮件发送技术援助请求：<br><br>**请注意：**<br>相应的文档现在可从西门子有限公司的技术援助页面上直接请求获得。<br>电子邮件： technical-assistance@siemens.com |
| \E\ | 表格<br>S7FCOTIA.XLS<br>S7FCOTIB.XLS | **下载：**<br>S7 Distributed Safety：F 执行时间，F 运行时，F 监测与反应时间<br>http://support.automation.siemens.com/WW/view/en/25412441 |



# 9 版本历史

表 9-1

| 版本 | 日期 | 修订 |
|---|---|---|
| V1.0 | 02/2012 | 首次发布 |
| | | |
| | | |