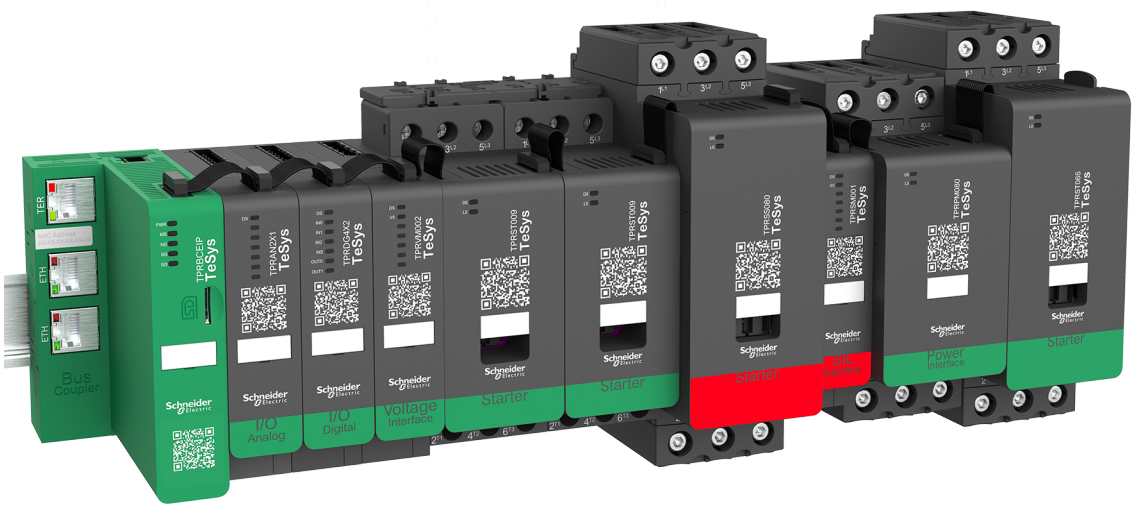
TeSys Active

TeSys™ island – 数字电机管理解决方案

功能安全指南

TeSys 为电机起动器提供了创新的互联解决方案。

8536IB1904ZH-04
08/2023



法律声明

本文档中提供的信息包含与产品/解决方案相关的一般说明、技术特性和/或建议。

本文档不应替代详细调研、或运营及场所特定的开发或平面示意图。它不用于判定产品/解决方案对于特定用户应用的适用性或可靠性。任何此类用户都有责任就相关特定应用场合或使用方面，对产品/解决方案执行或者由所选择的任何业内专家（集成师、规格指定者等）对产品/解决方案执行适当且全面的风险分析、评估和测试。

施耐德电气品牌以及本文档中涉及的施耐德电气及其附属公司的任何商标均是施耐德电气或其附属公司的财产。所有其他品牌均为其各自所有者的商标。

对于将本文档 或其内容用作商业用途的行为，施耐德电气未授予任何权利或许可，但以“原样”为基础进行咨询的非独占个人许可除外。

对于本文档或其内容或其格式，施耐德电气有权随时修改或更新，恕不另行通知。

在适用法律允许的范围内，对于本文档信息内容中的任何错误或遗漏，以及对本文档内容的任何非预期使用或误用，施耐德电气及其附属公司不会承担任何责任或义务。

目录

安全信息

重要信息

在尝试安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。 下述特别信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。

这两个符号中的任何一个与“危险”或“警告”安全标签一起使用，指示存在电击危险，若不遵循相关说明，可能会导致人身伤害。

这是安全警示符号。它用来提醒您可能存在的人身伤害危险。请遵守此符号后面提及的全部安全信息，以避免可能的人身伤害或死亡。

⚠ 危险

危险表示存在危险情况，如果不避免，**将导致**死亡或严重人身伤害。

⚠ 警告

警告表示存在潜在的危险情况，如果不避免，**可能导致**死亡或严重人身伤害。

⚠ 小心

小心表示存在潜在的危险情况，如果不避免，**可能导致**轻微或中度人身伤害。

注意

注意用于提请注意与人身伤害无关的事项。

请注意

电气设备的安装、操作、维修和维护工作仅限于合格人员执行。 Schneider Electric 不承担由于使用本资料所引起的任何后果。

有资质的人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

关于本手册

文档范围

使用此文档可了解更多有关以下 TeSys™ island 功能安全特征的信息：

- 一般性理解
- 要考虑的关键方面
- 性能
- 硬件描述
- 典型配置
- 示例架构
- 标准参考

有效性说明

本指南对所有 TeSys island 配置均有效。本指南中描述的某些功能的可用性取决于所使用的通讯协议和 TeSys island 上安装的物理模块。

有关产品在环境指令（比如 RoHS、REACH、PEP 和 EOLI）方面的合规性，请访问 www.se.com/green-premium。

欲了解有关本指南中描述的物理模块的技术特性，请转至 www.se.com。

本指南中提供的技术特性应该与在线内容相同。我们可能会随着时间的推移修改内容以提高清晰性和准确性。如果发现本指南中包含的信息与在线信息之间存在差异，请以在线信息为准。

相关的文件

文件名称	描述	文档编号
TeSys island — 系统、安装和操作指南	描述 TeSys island 的主要功能、机械安装、接线、调试，以及如何操作和维护 TeSys island。	DOCA0270ZH
TeSys island - EtherNet/IP™ — 快速入门和功能块库指南	介绍如何集成 TeSys island 以及有关 Rockwell Software® Studio 5000® EtherNet/IP 环境中使用的 TeSys island 库的信息。	DOCA0271ZH
TeSys island– 功能安全指南	描述 TeSys island 的功能安全功能。	8536IB1904ZH
TeSys island– 第三方功能块指南	包含为第三方硬件创建功能块所需的信息。	8536IB1905ZH
TeSys island - DTM 在线帮助指南	描述如何安装和使用 TeSys island 配置软件的各种功能以及如何配置 TeSys island 的参数。	8536IB1907ZH
TeSys island — 产品环境简介	描述了 TeSys island 的组成材料、可回收性和环境影响信息。	ENVPEP1904009
TeSys island – 产品生命周期结束说明	包含 TeSys island 的生命周期结束说明。	ENVEOLI1904009
TeSys island — 说明书，总线耦合器，TPRBCEIP	描述如何安装 TeSys island Ethernet/IP 总线耦合器。	MFR44097
TeSys island — 说明书，总线耦合器，TPRBCPFN	描述如何安装 TeSys island PROFINET 总线耦合器。	MFR44098
TeSys island — 说明书，总线耦合器，TPRBCPFB	描述如何安装 TeSys island PROFIBUS DP 总线耦合器。	GDE55148
TeSys island — 说明书，起动器和电源接口模块，尺寸 1 和 2	描述如何安装尺寸 1 和 2 TeSys island 起动器和电源接口模块。	MFR77070
TeSys island — 说明书，起动器和电源接口模块，尺寸 3	描述如何安装尺寸 3 TeSys island 起动器和电源接口模块。	MFR77085
TeSys island — 说明书：输入/输出模块	描述如何安装 TeSys island 模拟和数字 I/O 模块。	MFR44099
TeSys island — 说明书：SIL 接口和电压接口模块	描述如何安装 TeSys island 电压接口模块和 SIL[1] 接口模块。	MFR44100

1. 符合 IEC 61508 标准的安全完整性水平。

源自标准的术语

本指南中的技术术语、术语和相应描述通常使用相关标准中的术语或定义。其中，这些标准包括：

- **EN ISO 13849-1**：机械安全 - 控制系统的安全相关部件 - 第 1 部分：一般设计原则
- **EN ISO 13849-2**：机械安全 - 控制系统的安全相关部件 - 第 2 部分：验证
- **IEC 61508**：电气/电子/可编程电子安全相关系统的功能安全
- **EN 62061**：机械安全 - 与安全相关的电气、电子和可编程电子控制系统的功能安全
- **IEC 61511**：功能安全 - 工业生产行业的安全仪表系统
- **EN/IEC 60204-1**：机械安全 - 机械电气设备 - 第 1 部分：一般要求
- **IEC 61000-6-7**：电磁兼容性 (EMC) - 第 6-7 部分：通用标准 - 用于在工业场所执行安全相关系统（功能安全）功能的设备的抗扰度要求
- **IEC 60664-5**：低压系统内设备的绝缘配合 - 第 5 部分：确定间隙和沿面距离等于或小于 2 毫米的综合方法
- **IEC 60947-4-1**：低压开关设备和控制装置 - 第 4-1 部分：接触器和电动机起动器 - 机电接触器和电动机起动器
- **IEC 60947-5-1**：低压开关设备和控制装置 - 第 5-1 部分：控制电路装置和开关元件 – 机电控制电路装置
- **IEC 60947-7-1**：低压开关设备和控制装置 - 第 7-1 部分：辅助设备 - 铜导线的接线端子
- **IEC 60947-7-2**：低压开关设备和控制装置 - 第 7-2 部分：辅助设备 – 铜导线用保护导体端子块
- **EN 50205**：带有强制导向（机械连接）触点的继电器
- **IEC TR 62380**：可靠性数据手册 - 电子元件、PCB 和设备可靠性预测的通用模型

功能安全术语

ATTENTION

本指南中使用的功能安全术语定义如下。

术语	标准	定义
容错	IEC 61511-1	功能项在出现故障或错误时继续执行所需功能的能力
功能安全	IEC 61508-4	与受控设备 (EUC) 和 EUC 控制系统相关的整体安全的一部分，取决于电气/电子/可编程电子 (E/E/PE) 安全相关系统的正常运行以及其他风险降低措施
安全故障	IEC 61508-4	在实现安全功能中起作用的元件和/或子系统和/或系统发生故障将： 1. 导致安全功能产生虚假操作，使 EUC[2]（或其中的一部分）进入安全状态或维持安全状态；或者 2. 提高安全功能产生虚假操作的可能性，使 EUC[2]（或其中的一部分）进入安全状态或维持安全状态。
安全故障分数	IEC 61508-4	安全故障率与系统总故障率之比。
安全状态	IEC 61511-1	实现安全时的过程的状态
	IEC 61800-5-2	实现安全时的 PDS(SR) 状态[3]
安全停止	IEC 61800-5-2	安全停止功能定义为： • **安全扭矩关闭 (STO)** ◦ 此功能可防止将产生电磁力的电能提供给电机。 ◦ 根据 IEC 60204-1 的停止类别 0，此{18}安全子功能{19}对应于不受控停止。 • **安全停止 1 (SS1)** ◦ 安全停止 1 减速控制：当电机速度低于规定限值时，SS1-d 启动并将电机减速率控制在选定范围内以停止电机并执行 STO 功能（见 4.2.3.2）；或者 ◦ 监控的安全停止 1 渐变：当电机速度低于规定限值时，SS1-r 启动并将电机减速率控制在选定范围内以停止电机并执行 STO 功能；或者 ◦ 安全停止 1 时间控制的 SS1-t 启动电机减速并在特定时间延迟后执行 STO 功能。
安全功能	IEC 61800-5-2	针对特定危险事件，由安全相关系统或其他降低风险措施实施的功能，旨在实现或保持由 PDS (SR) [3]驱动的设备或机器的安全状态
安全完整性等级 (SIL)	IEC 61508	标准 IEC 61508 为安全功能定义了四种安全完整性等级 (SIL)：SIL 1 是最低的完整性等级，SIL 4 是最高等级。 危害分析和风险评估是确定所需安全完整性等级的基础。
安全相关系统	IEC 61800-5-2	同时满足以下条件的指定系统 • 实施实现或保持 PDS (SR) [3]驱动的设备或机械的安全状态所需的安全功能；和 • 旨在单独或与其他风险降低措施一起实现所需安全功能的必要安全完整性
子系统	IEC 61800-5-2	安全相关系统的顶级架构设计的一部分，其失效将导致安全相关功能的失效

EC 符合性声明

可以从 www.schneider-electric.com 获得 TeSys™ island 的 EC 符合性声明。

2. EUC：受控设备
3. 安全相关电源驱动系统

注意事项

在执行本指南中的任何步骤之前，请阅读并理解以下注意事项。

⚠⚠危险

电击、爆炸、电闪弧光危险

- 只能由具备资质的电工来安装和维修本设备。
- 在本设备上或设备内部进行操作之前，请关闭向本设备供电的所有电源。
- 操作本设备和任何相关产品时，请仅使用指定的电压。
- 务必使用额定值正确的电压传感设备来确认电源已关闭。
- 在对人员和/或设备有危险的地方使用适当的联锁装置。
- 电源电路必须按照当地和国家法规要求进行接线和保护。
- 使用适当的个人防护设备 (PPE)，并遵循 NFPA 70E、NOM-029-STPS 或 CSA Z462 或当地同等标准的安全电气操作规范。

未按说明操作将导致人身伤亡等严重后果。

⚠警告

意外的设备操作

- 有关功能性安全的完整说明，请参阅《TeSys™ island 功能性安全指南》，8536IB1904。
- 请勿拆卸、维修或改造此设备。其中没有可由用户维护保养的零件。
- 在适合其预期应用环境的外壳中安装和操作此设备。
- 在投入使用之前，必须对该设备的每个实施环节进行单独和彻底的测试，以确保其正常运行。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

⚠ **警告**：本产品可能会使您接触到化学物质，包括加利福尼亚州已公布的会导致癌症的氧化锑（三氧化二锑）。欲了解更多信息，请转至 www.P65Warnings.ca.gov。

合格人员

只有经过适当培训且熟悉并理解本指南内容和所有其他相关产品文档的人员才有权使用本产品。

合格人员必须能够检测可能由于修改参数值而产生的危险，这通常来自机械、电气或电子设备。合格人员必须熟悉工业事故预防的标准、预防措施和规定，在设计和实施系统时必须遵守这些标准、预防措施和规定。

使用和应用本指南中包含的信息时需要掌握自动化控制系统的设计和编程方面的专业知识。只有您、用户、机器制造商或集成商才了解机器或流程的安装、设置、操作和维护过程中出现的所有条件和因素，因此可以确定自动化及相关设备和相关安全设备和联锁装置，这样才可以有效和正确地使用。

在为特定应用选择自动化和控制设备（以及任何其他相关设备或软件）时，您还必须考虑适用的当地、地区或国家标准和/或法规。

在使用本设备时，请特别注意遵守适用于您的机器或流程的任何安全信息、电气要求和规范标准。

预期用途

本指南中描述的产品以及软件、配件和选件是低压电气负载的起动器，根据本文档以及其他支持文件中包含的说明、指示、示例和安全信息用于工业用途。

该产品只能在符合所有适用的安全法规和指令、规定的要求和技术数据的环境中使用。

在使用本产品之前，您必须对计划的应用进行危害分析和风险评估。根据结果，必须采取适当的安全相关措施。

由于产品属于机器或流程的组件，因此必须通过整个系统设计确保人员的安全。

仅使用指定的电缆和配件操作产品。仅使用原装配件和备件。

禁止将本产品用于明确允许使用以外的任何用途，否则可能导致意外危险。

TeSys™ island 功能安全概述

主要范围：TeSys

TeSys™ 是全球市场领先企业提供的创新型电机控制和管理解决方案。TeSys 提供了互联互通的、高效的产品和解决方案，用于符合所有全球主要电气标准的电机及气负载的控制与保护。

TeSys island 概念

TeSys island 是一款模块化的多功能系统，在自动化架构内提供集成的功能，主要用于直接控制和管理低压负载。TeSys island 能够开关、保护和管理电机和电气控制面板中安装的高达 80 A(AC1) 的其他电气负载。

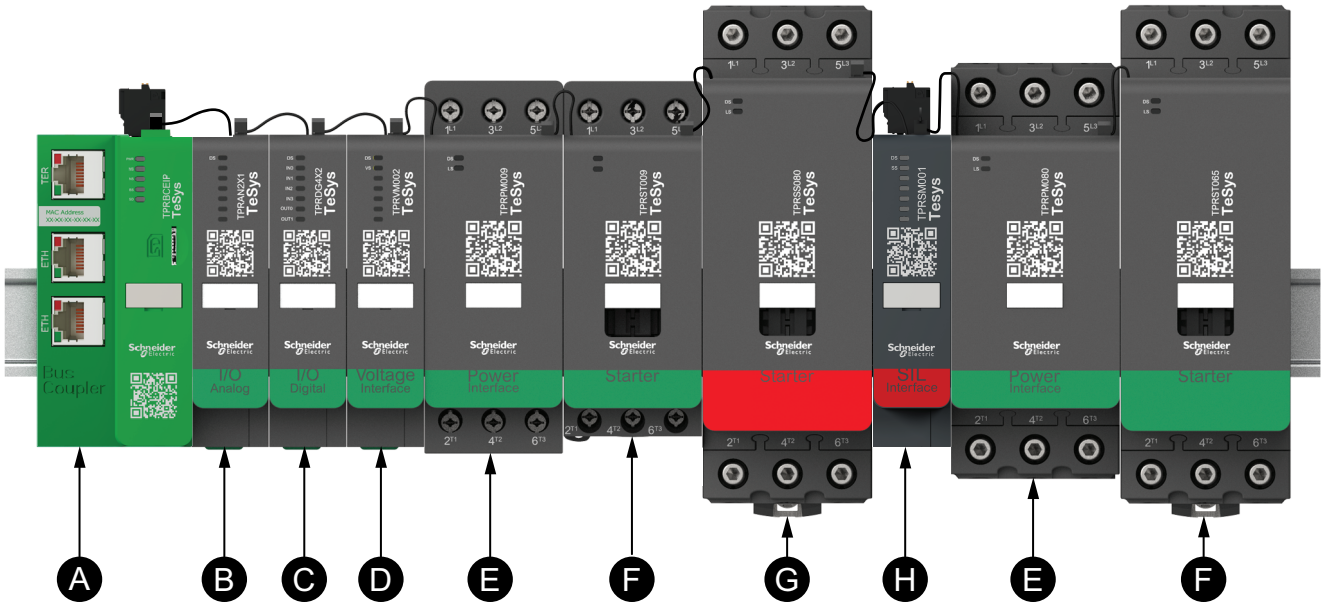
此系统围绕 TeSys avatars 的概念设计。这些 avatars：

- 表示自动化功能的逻辑和物理方面
- 决定 TeSys island 的配置

TeSys island 的逻辑方面由软件工具管理，覆盖产品和应用程序生命周期的所有阶段：设计、工程、调试、运行和维护。

物理 TeSys island 由安装在单个 DIN 轨道上的一套设备组成，并用扁平电缆连接在一起，从而在各模块之间实现通讯。与自动化环境的外部通讯是通过单个总线耦合器模块实现的，而 TeSys island 被视为网络上的单个节点。其他模块包括起动器、电源接口模块、模拟和数字 I/O 模块、电压接口模块以及 SIL（符合 IEC 61508 标准的安全完整性等级）接口模块，这些模块能提供广泛的操作功能。

图 1 - TeSys island 概述



A	总线耦合器	E	电源接口模块
B	模拟量 I/O 模块	F	标准起动器
C	数字量 I/O 模块	G	SIL 起动器
D	电压接口模块	H	SIL 接口模块

TeSys island 的功能安全

TeSys™ island 提供特定的 Avatar 和物理设备，可根据 EN/IEC 60204-1 构建停止类别 0 和停止类别 1 功能的配置。TeSys avatar 是阀岛上物理模块的数字表示，但 TeSys island 安全功能仅依赖于机电硬件组件。特定的设备为 SIL[4] 起动器和 SIL 接口模块。另一个重要的概念是 SIL 安全起动器组：一组与一个 SIL 接口模块相关联并遵循相同安全功能的 avatar。阀岛内可能有多个 SIL 安全起动器组。

TeSys island 必须与更广泛的安全相关系统中的其他安全相关元件集成，以帮助确保机器或系统/过程的功能安全。

4. 根据标准 IEC 61508 确定的安全完整性等级。

TeSys island 的功能安全特征

TeSys™ island 提供符合以下特定条件的功能安全特征：

标准和认证特征

TeSys island 遵循以下指令和标准：

- 机械指令 2006/42 / CE：
  - EN ISO 13849-1：2015
  - EN 62061：2016 或 IEC 62061：2015（第 1.2 版）
- 电气/电子/可编程电子安全相关系统的功能安全：IEC 61508 第 2 版：2010
- 功能安全 - 工业生产行业的安全仪表系统：IEC 61511 第 2 版：2016
- TeSys island 停止类别 0 和停止类别 1 功能符合 EN/IEC 60204-1 标准。

在单通道中，这些功能的最高性能是：

- 性能等级“d”类别 2 符合 EN ISO 13849-1 标准
- SIL[5]2 功能符合 IEC 61508 标准第 2 版和 IEC 61511 标准第 2 版
- SIL CL 2 功能符合 EN 62061 标准第 1 版

在双通道中，这些功能的最高性能是：

- 性能等级 “e” 类别 4 符合 EN ISO 13849-1 标准
- SIL 3 功能符合 IEC 61508 标准第 2 版和 IEC 61511 标准第 2 版
- SIL CL 3 功能符合 EN 62061 标准：2016 或 IEC 62061：2015（第 1.2 版）

TeSys island 旨在根据其接线架构支持不同的功能安全性能等级和安全完整性等级，并符合下表中所述的功能安全特征。

表 1 - 功能安全特征

功能	安全相关的停止功能	
故障预置位置	打开接触器	
响应时间（最坏情况）	145 毫秒	
停止类别 EN/IEC 60204-1	类别0 / 类别1	
机械指令	是	
TeSys island 系统架构	单通道	双通道
性能级别 EN ISO 13849-1	PL c, d	PL c, d, e
接线类别 ISO 13849-1	类别 1、2	类别 3、4
SIL CL EN 62061	SIL CL 2	SIL CL 3
SIL IEC 61508/IEC 61511	SIL 2	SIL 3

www.se.com/tesys/ 网站中提供了有关功能安全证书。

5. 根据标准 IEC 61508 确定的安全完整性等级。

注: 对于与功能方面相关的认证，仅考虑适用于安全相关应用的 TeSys island，而不是集成到其中的完整系统，这可确保机器或系统/过程的功能安全。

运行条件

TeSys island 设计用于长期在以下条件下工作。其他条件可能适用于特定模块，如 www.se.com/tesys-island 上提供的相应产品手册所述。

- 环境温度 40 °C (104 °F)
- 400 或 480 V 电机
- 湿度 50%
- 80% 负载
- 水平安装方向
- 所有输入已激活
- 所有输出已激活
- 运行时间为 24 小时/天，365 天/年

单通道架构 (ISO 13849)

TeSys island 适用于单通道架构，其中检测到的故障可能导致安全功能的丧失。

双通道架构 (ISO 13849)

TeSys island 适用于双通道架构，其中单个检测到的故障（包括共模故障）不会导致安全功能的丧失。

停止类别 (EN/IEC 60204-1)

停止类别与驱动负载断电的方式有关，还取决于触发停止功能的外部安全相关子系统。可以使用诸如 Preventa™ XPS 模块之类的设备实现外部安全相关的子系统。

停止类别 0

停止类别 0 定义为通过立即断开机器执行器的电源来停止机器运动。停止类别 0 是一种不受控制的停止。

停止类别 1

停止类别 1 定义为停止机器运动并在停止过程中保持对机器执行器的供电。停止完成后，电源将完全断开。停止类别 1 是受控制的停止。

接线类别[6]

接线类别涉及外部 Preventa™ XPS 模块（或等效模块）的接线方式，以及与安全功能相关的附加控制级别。

接线类别 1

即使检测到一个故障也可能导致安全功能丧失，无需诊断覆盖信息。

6. 根据标准 ISO 13849 确定的接线类别。

安全相关的传感器元件可以直接连接到 SIL-IN / SIL 通用输入。[7]不使用镜像进/镜像出输入。有关连接 SIL-IN / SIL 通用输入的更多信息，请参阅安全相关的传感器元件, 22 页。

接线类别 2

安全相关的传感器元件连接到 Preventa XPS 模块（或等效模块）。Preventa XPS 模块（或等效模块）输出连接到 SIL[7] 接口模块的 SIL-IN / SIL 通用输入。

为了满足类别 2 的要求，镜像接触反馈（镜像进/镜像出）必须由 Preventa XPS 模块（或等效模块）监测，该模块执行镜像接触器的外部诊断监测。如果镜像触点在停止时未关闭，则会阻止 SIL 安全起动器组中的所有 SIL 起动器重新起动。

实施类别 2 间接监测

为了达到诊断覆盖范围的类别 2 要求 (DC>60%)，应实施对组状态的外部监测，以触发停止机器的辅助机制（断路器分励脱扣等）或防止进入危险区域（安全锁）。

每个 SIL[7] 安全起动器组都有五个与之关联的状态，以指示运行状态。状态 0 表示此插槽中不存在 SIL 安全起动器组。TeSys island 支持阀岛上多达 10 个 SIL 安全起动器组。

SIL 停止功能的 SIL 安全起动器组状态：

- 0 = 系统配置中不存在 SIL 安全起动器组
- 1 = 受 avatar 设备事件影响的 SIL 安全起动器组
- 2 = 停止命令已接收，SIL 起动器尚未打开
- 3 = 停止命令成功发出，所有 SIL 起动器都打开
- 4 = 仅向一个 SIL 接口模块 (SIM) 输入通道发出停止命令（跳线或 SIM 输入接线导致问题），但 SIL 起动器确实成功打开
- 5 = 正常操作，SIL 起动器可以为打开或关闭

状态 5 是正常运行状态，状态 3 是正常的 SIL 停止状态。状态 1 表示 SIL 起动器的固件或通信有问题。状态 2 和 4 表示 SIM、SIL 起动器或 SIL 停止接线的 SIL 停止相关问题。间接监控应查找状态 2 或 4 持续时间超过 SIL 停止的启动时间的情况，并使用状态信息触发辅助机制来停止机器（断路器旁路脱扣等）。

要读取 SIL 安全起动器组状态，外部监视必须使用系统诊断功能块。系统中的每个 SIL 安全起动器组在此功能块上都有一个输出，用于其 SIL 安全起动器组状态，在功能块上标记为 “SILStarterStopMsgGrp *n*”，其中 *n* 是阀岛中 SIL 安全起动器组的编号。SIL 安全起动器组状态遵循上面显示的类型。

诊断监测

由于根据安全功能的要求立即进行诊断监测，其检测故障并使机器处于非危险状态的总时间应短于到达危险区域的时间。

根据 ISO 13849-2,9.2.3，类别 2：监测设备的 $MTTF_d$[8] 应大于逻辑 $MTTF_d$ 的一半。TeSys island 对诊断监测的 $MTTF_d$ 的影响是 $MTTF_d$ > 100 年。

接线类别 3

单个故障不会导致安全功能的丧失，在可行的情况下，应在安全功能的下一个需求之时或之前检测到单个故障。

为了满足类别 3 的要求，镜像接触器反馈（镜像进/镜像出）必须由 Preventa XPS 模块（或等效模块）监测，该模块执行 SIL[7] 起动器镜像接触器的外部诊断监测。如果镜像接触器在停止时未打开，则会阻止 SIL 安全起动器组中的所有 SIL 起动器

7. 根据标准 IEC 61508 确定的安全完整性等级。
8. 平均危险失效时间如 ISO 13849-1 中所定义。

重新起动。安全相关的传感器元件连接到 Preventa XPS 模块（或等效模块）。Preventa XPS 模块（或等效模块）输出连接到 SIL 接口模块的 SIL-IN / SIL 公共输入。

在间接监测的情况下，组状态的外部监测应查找状态 2 或 4 以确保持续时间长度超过 SIL 停止的起动时间。使用状态信息可阻止 SIL 安全起动器组重新起动。

接线类别 4

单个故障不会导致安全功能的丧失。在安全功能的下一个需求之时或之前检测到单个故障。如果无法进行此检测，则未检测到的故障的累积不应导致安全功能的丧失。

为了满足类别 4 的要求，镜像接触器反馈（镜像进/镜像出）必须由 Preventa XPS 模块（或等效模块）监测，该模块执行 SIL[9] 起动器镜像接触器的外部诊断监测。如果镜像接触器在停止时未打开，则会阻止 SIL 安全起动器组中的所有 SIL 起动器重新起动。安全相关的传感器元件连接到 Preventa XPS 模块（或等效模块）。Preventa XPS 模块（或等效模块）输出连接到 SIL 接口模块的 SIL-IN / SIL 公共输入。

验收测试

系统集成商/机器制造商必须执行安全功能的验收测试，以验证和记录安全功能的正确性。系统集成商/机器制造商由此证明已经测试了所使用的安全功能的有效性。必须根据危害分析和风险评估进行验收测试。在类别 4 低需求模式的情况下，应每月至少测试一次安全功能。必须遵守所有适用的标准和规定。

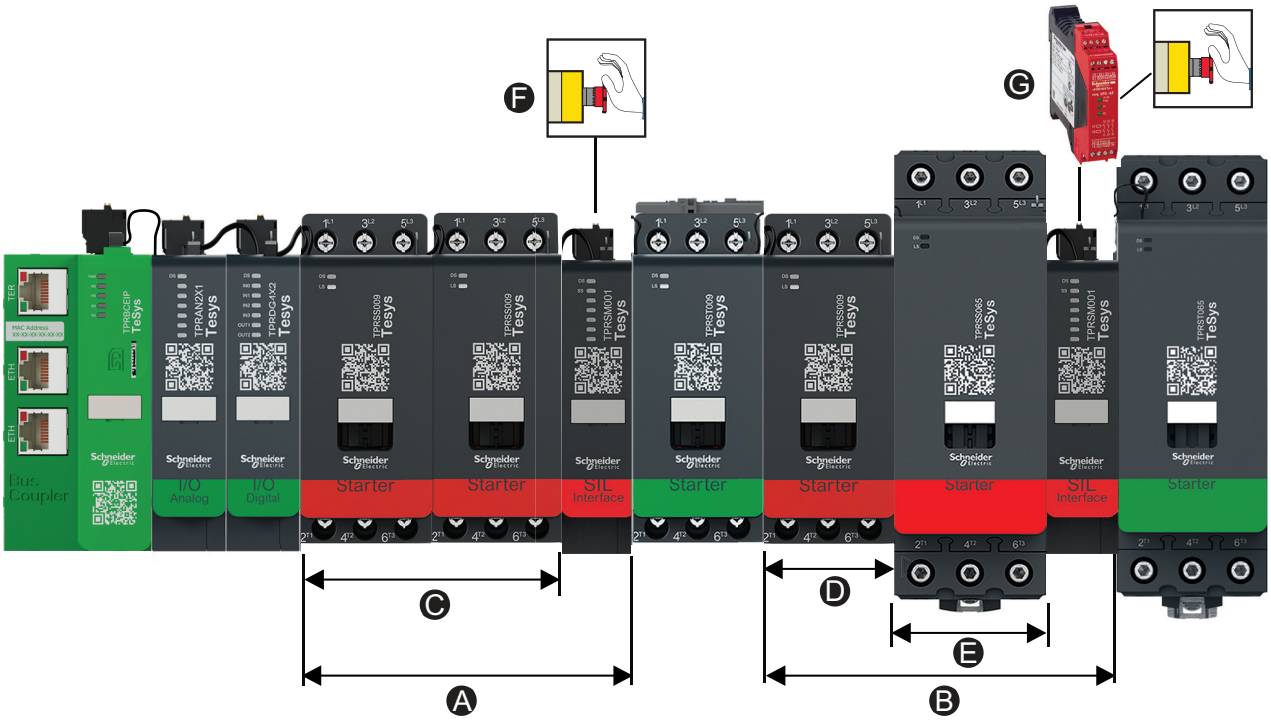
9. 根据标准 IEC 61508 确定的安全完整性等级。

概念和组件

典型的 TeSys™ island 结构

下图显示了由两个 SIL[10] 安全起动器组组成的 TeSys™ island 的示例。根据用户表达的功能需求使用 TeSys island 数字工具定义阀岛的组成。

图 2 - 有两个 SIL 安全起动器组的 TeSys island



A	SIL 安全起动器组 1	E	Avatar A4
B	SIL 安全起动器组 2	F	接线类别 1，停止类别 0[11]
C	Avatar A1	G	接线类别 2，停止类别 1[12]
D	Avatar A3		

SIL 安全起动器组 1：包括一个由两个 SIL 起动器组成的 Avatar：例如，“电机双向 - SIL 停止，接线类别 1/2” avatar (Avatar A1)。实际电机连接到这些 SIL 起动器，并通过现场总线跟踪 avatar 逻辑和来自 PLC 的操作命令。SIL 停止命令来自连接到 SIL 接口模块的紧急停止按钮（接线类别 1），从而使 SIL 起动器断开负载并进入安全状态（接触器打开，电机断电）。

SIL 安全起动器组 2：包括两个 Avatar，例如“开关 - SIL 停止，接线类别 1/2”（Avatar A3）和“电机单向 - SIL 停止，接线类别 1/2”（Avatar A4），每个都由一个 SIL 起动器组成。两个 avatar 都通过现场总线跟踪来自 PLC 的 avatar 逻辑和操作命令。SIL 停止命令来自连接到 SIL 接口模块的外部 Preventa™ XPS 模块（或等效模块），从而使 SIL 起动器断开负载并进入安全状态（接线类别 2）。

10. 根据标准 IEC 61508 确定的安全完整性等级。
11. 根据标准 ISO 13849 确定的接线类别 1。根据标准 EN/IEC 60204-1 确定的停止类别 0。
12. 根据标准 ISO 13849 确定的接线类别 2。根据标准 EN/IEC 60204-1 确定的停止类别 1。

SIL 安全起动器组

SIL[13] 安全起动器组由一个或多个 SIL Avatar 组成，全部分配到单个 SIL 接口模块。SIL 安全起动器组中的所有 SIL Avatar 都对单个 SIL 停止命令作出反应。SIL 接口模块始终安装在 SIL 安全起动器组中包含的最后一个 SIL 起动器的右侧（总线耦合器的远侧）。

一个阀岛可能包括几个 SIL 安全起动器组。

SIL Avatar

适用于 SIL 停止功能的 SIL[13] Avatar 包括：

- 开关 — SIL 停止，接线类别 1/2
- 开关 — SIL 停止，接线类别 3/4
- 电机单向 — SIL 停止，接线类别 1/2
- 电机单向 — SIL 停止，接线类别 3/4
- 电机双向 — SIL 停止，接线类别 1/2
- 电机双向 — SIL 停止，接线类别 3/4
- 电机双速 — SIL 停止，接线类别 1/2
- 电机双速 — SIL 停止，接线类别 3/4
- 电机双速双向 — SIL 停止，接线类别 1/2
- 电机双速双向 — SIL 停止，接线类别 3/4
- 输送机单向 — SIL 停止，接线类别 1/2
- 输送机双向 — SIL 停止，接线类别 3/4

SIL avatar 由特定的硬件设备组成，包括 SIL 起动器、标准起动器以及管理 SIL avatar 所分配的 SIL 安全起动器组所需的 SIL 接口模块。

注: SIL avatar 设计用于具有低频率操作命令的应用 - 年平均值低于每小时 15 个开始起动/停止循环。

SIL 起动器

标准起动器

SIL 接口模块

13. 根据标准 IEC 61508 确定的安全完整性等级。

SIL 接口模块

TeSys™ island SIL[14] 接口模块 (SIM) 是启用阀岛功能安全特征所需的附件模块。

SIL 停止功能是通过纯机电装置实现的，无需任何数字通信或总线耦合器。

SIM：

- 连接外部 Preventa™ XPS 模块（或等效模块）的接口
- 发出其 SIL 安全起动器组的停止功能命令
- 与总线耦合器交换运行数据
- 通过前面的 LED 报告运行信息

SIL 起动器接触器状态

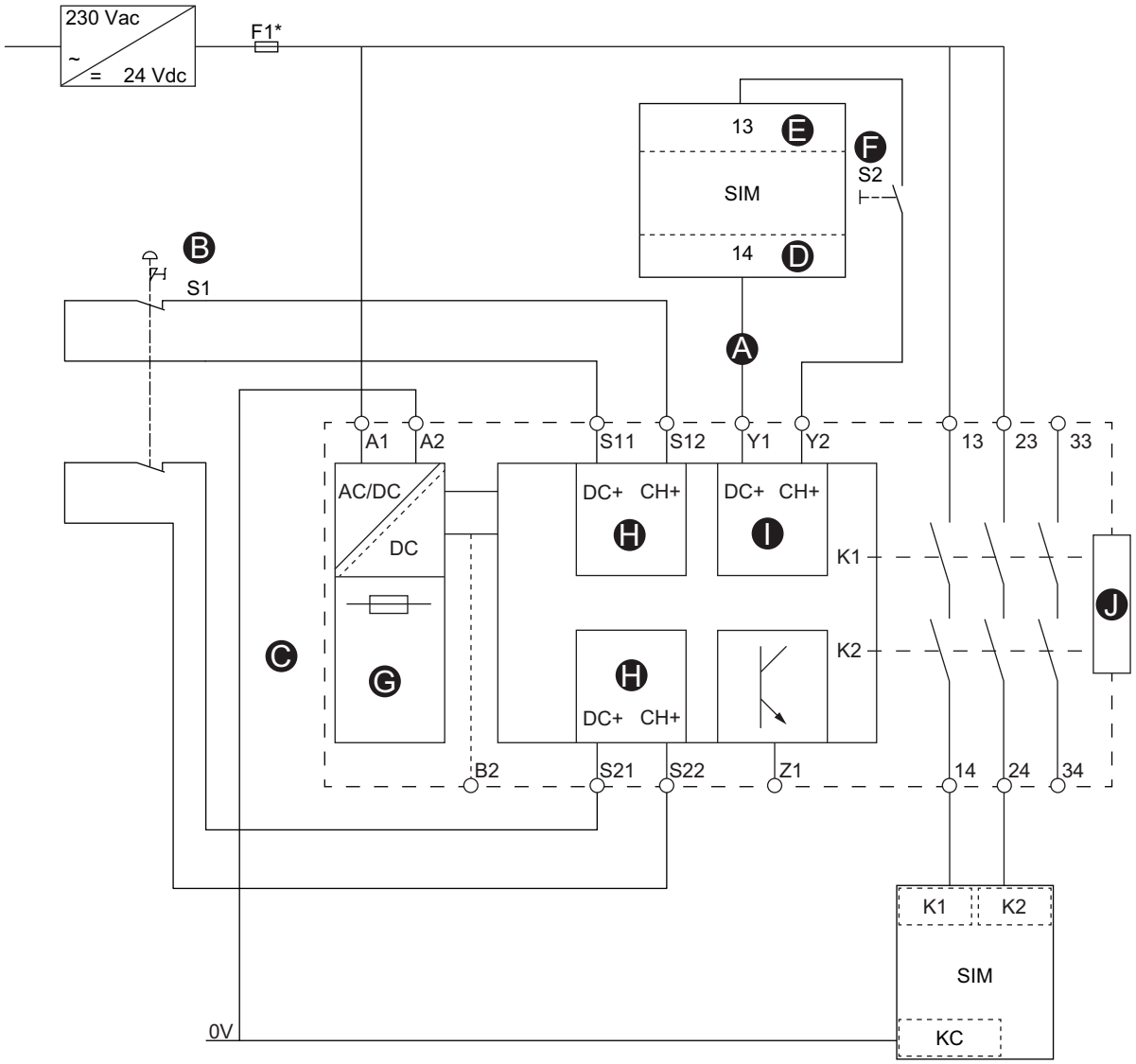
通过 SIM 镜像进/出连接报告属于 SIL 安全起动器组的 SIL[14] 起动器的状态。这样将可实现接线类别 2[15] 架构，其中镜像接触器连接到 Preventa XPS 模块（或等效模块）。这些配置通过机械连接的接触元件提供机电设备的直接监控功能，诊断覆盖率高达 99%。参见 EN ISO 13849-1，表 E.1 - 诊断覆盖率 (DC) 的估计值。

表 2 - SIL 起动器接触器状态

SIL 安全起动器组状态	镜像进/出状态
所有 SIL 起动器都是开启的	镜像进/出触点已闭合
至少有一个 SIL 起动器关闭	镜像进/出触点已开启
TeSys island 未通电或安全功能检测到故障	镜像进/出触点已开启

14. 根据标准 IEC 61508 确定的安全完整性等级。
15. 根据标准 ISO 13849 确定的接线类别 2。

图 3 - SIM 到 Preventa 模块 XPS-AF 的接线



A	外部起动条件 (ESC)	F	起动按钮 (S2)
B	紧急停止按钮 (S1)	G	电源
C	Preventa XPS-UAF 模块	H	输入
D	SIM 镜像出	I	起动
E	SIM 镜像进	J	扩展

安全相关传感器元件

SIM 模块连接上游：

- 至 24 Vdc 电源
- 至安全相关的传感器元件或 Preventa XPS 模块（或等效模块）。

SIM 模块设计有两个输入通道，以适应双通道安全相关的传感器元件。为了获得更高级别的容错，建议使用双输入通道架构。

有关下面的接线图的说明，请参阅 SIM 通道接线图图例, 22 页。

图 4 - SIM — 单通道接线

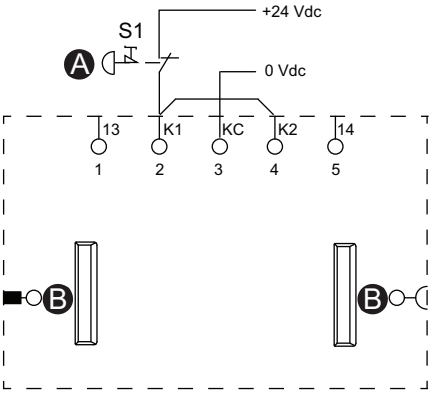


图 5 - SIM — 双通道接线

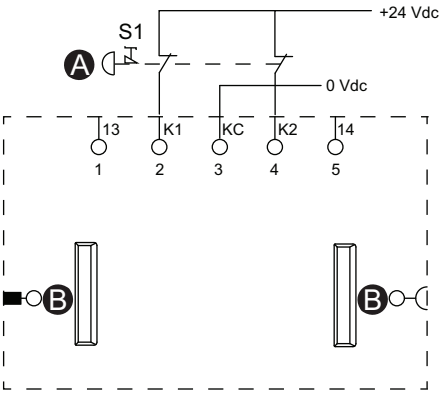


表 3 - SIM 通道接线图图例

A	紧急停止按钮 (S1)
B	扁平电缆连接器

SIL 起动器

⚠警告

意外的设备运行

有关功能性安全的完整说明，请参阅《TeSys™ island 功能性安全指南》，8536IB1904。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

SIL [16]起动器提供与标准起动器类似的功能，但与 SIL 接口模块相关联。

SIL 起动器的主要功能如下：

- 提供停止类别 0 和停止类别 1[17] 功能
- 为负载提供操作控制
- 测量与负载相关的电气数据
- 当 TeSys island 上安装了电压接口模块时提供电能监测数据

单个 TeSys avatar 功能可能需要多个 SIL 起动器。例如，avatar 电机双向 - SIL 停止，接线类别 1/2[18] 包括两个 SIL 起动器。此外，使用 SIL 起动器的 avatars 始终包含 SIL 接口模块。

SIL 起动器实现以下连接：

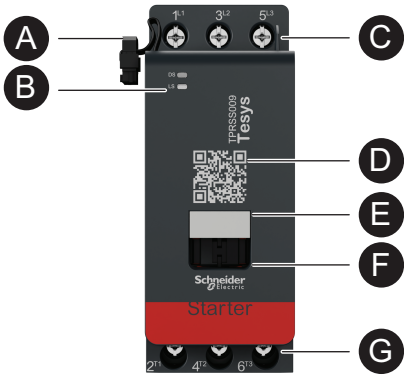
- 断路器上游
- 下游到负载

SIL 起动器与总线耦合器通讯，发送运行数据和接收命令。

表 4 - SIL 起动器额定值

功率额定值		安培	参考
kW	hp		
4	5	0.18–9	TPRSS009
11	15	0.5-25	TPRSS025
18.5	20	0.76-38	TPRSS038
30	40	3.25-65	TPRSS065
37	40	4-80	TPRSS080

图 6 - SIL 起动器功能



A	扁平电缆（用于连接左侧模块）	E	铭牌
B	LED 状态指示灯	F	移动桥接
C	上游电源连接	G	下游电源连接
D	二维码		

16. 符合 IEC 61508 标准的安全完整性等级。
17. 符合 EN/IEC 60204-1 标准的停止类别 0 停止类别 1。
18. 符合 ISO 13849 标准的接线类别 1 和类别 2。

外部安全相关元件

TeSys™ island 必须与更广泛的安全相关系统中的其他安全相关元件集成，以有助于确保机器或系统/过程的功能安全。

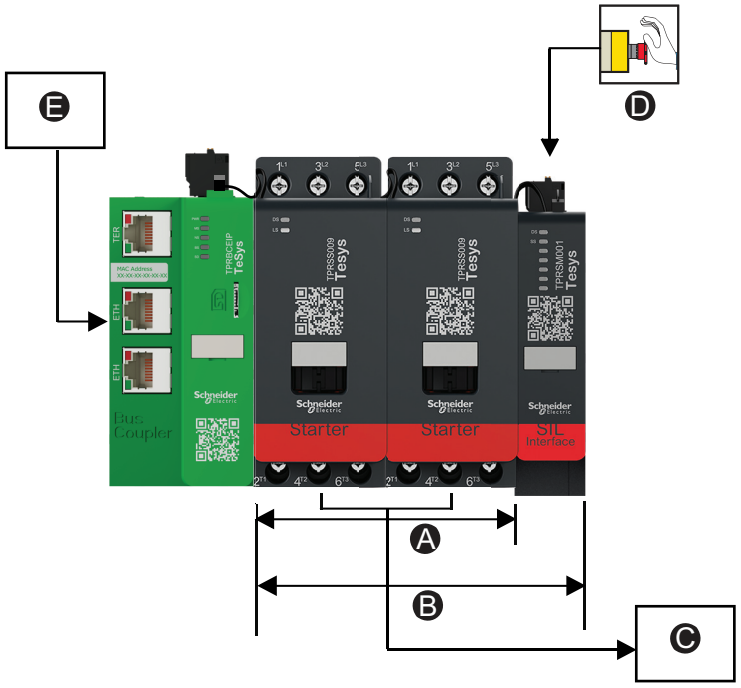
以下配置说明了典型的设备。

SIL 停止，停止类别 0，接线类别 1 配置

注: 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 1。根据标准 EN/IEC 60204-1 确定的停止类别 0。

通过断开紧急停止按钮的接触器直接控制电机的 SIL 停止。

图 7 - SIL 停止



A	Avatar A1	D	接线类别 1，停止类别 0
B	SIL 安全起动器组 1	E	PLC
C	电机		

SIL 停止，停止类别 0，接线类别 2 配置

注: 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 2。根据标准 EN/IEC 60204-1 确定的停止类别 0。

图 8 - 示例：电机双向 - SIL 停止，接线类别 1/2 — 停止类别 0，接线类别 2 配置（间接监测）

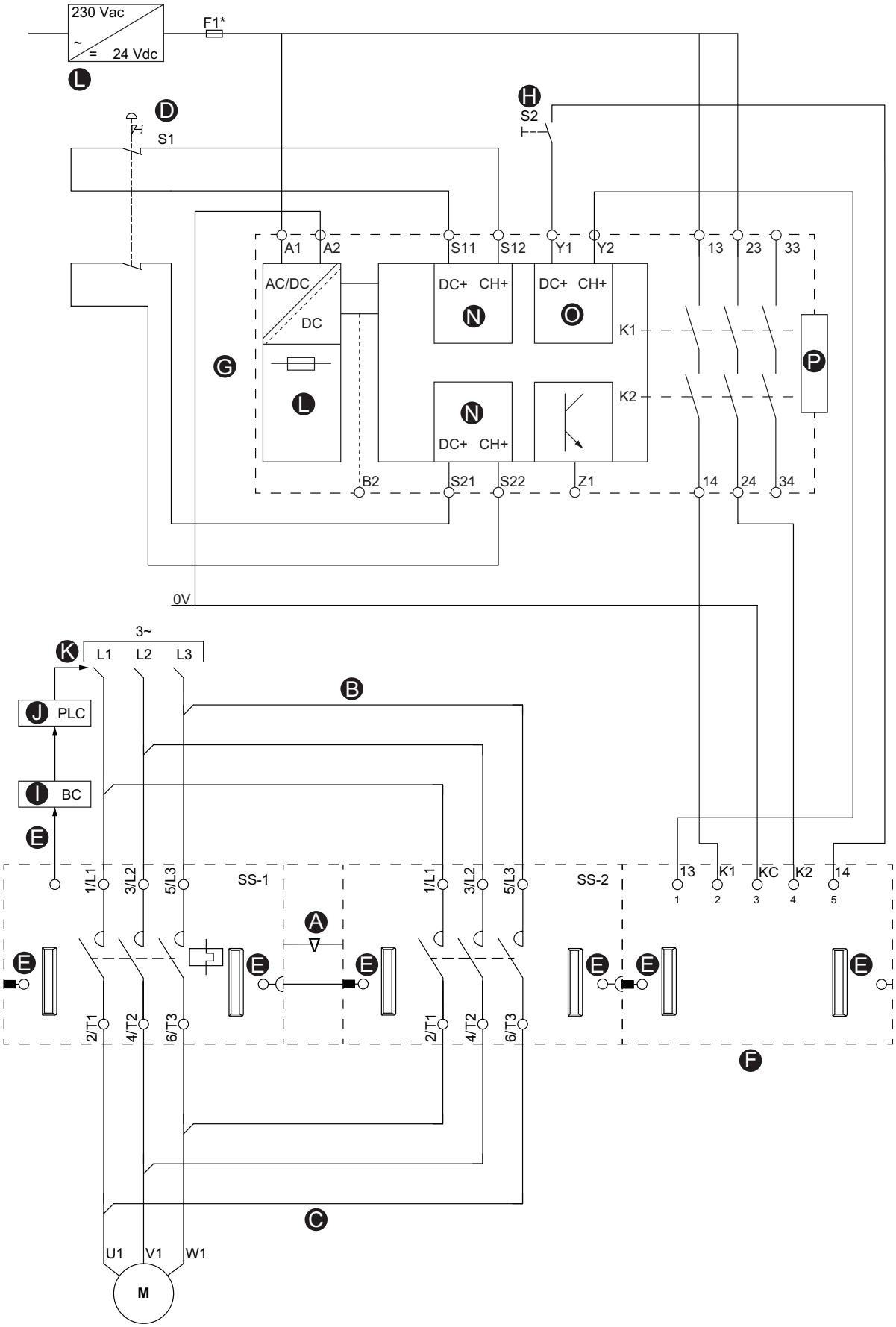
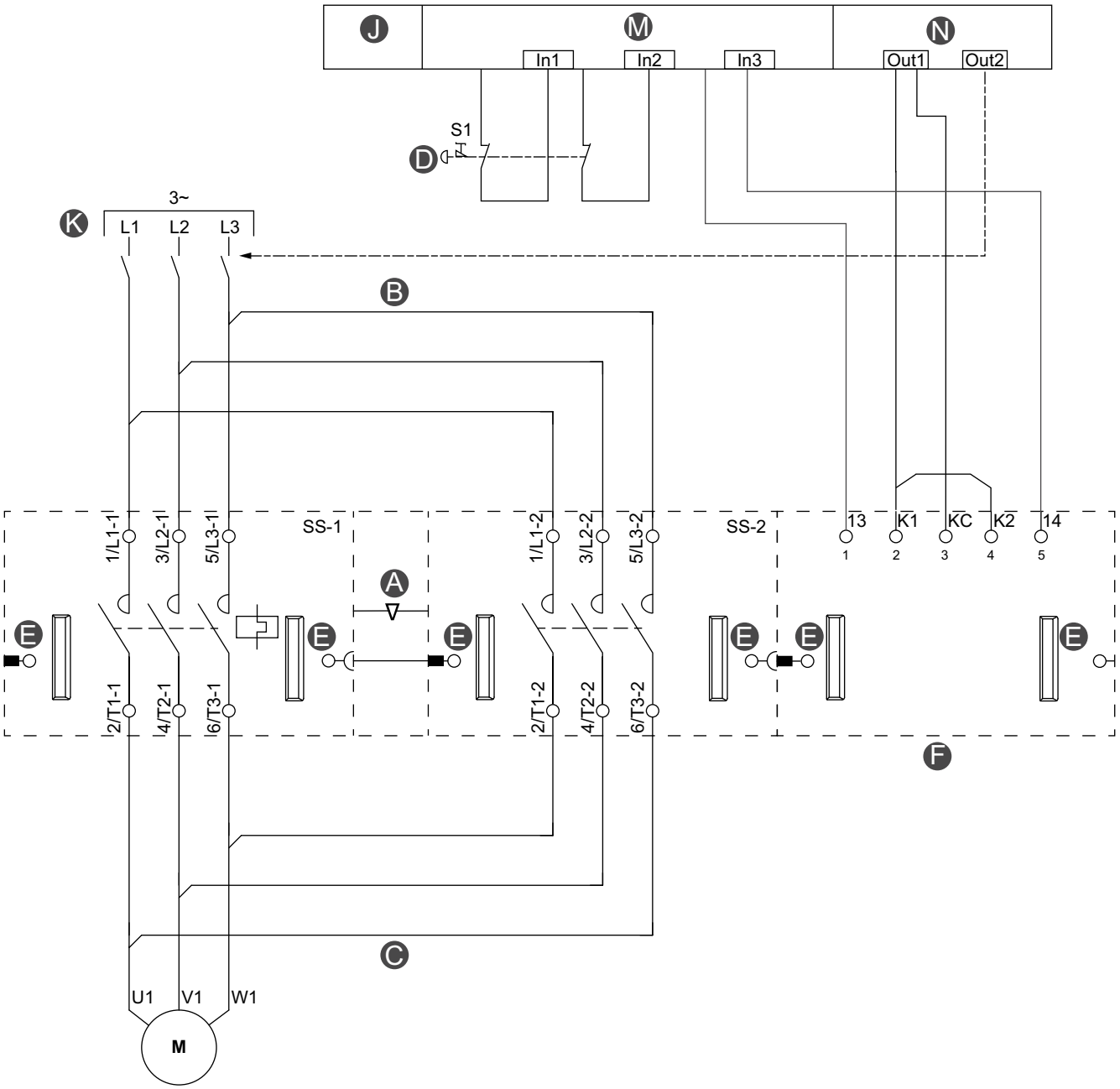


表 5 - 图例 示例：电机双向 - SIL 停止，接线类别 1/2 — 停止类别 0，接线类别 2 配置（间接监测）, 25 页

A	机械联锁	I	总线耦合器
B	并联链路	J	PLC
C	反向链路	K	上游电路断路器
D	紧急停止按钮 (S1)	L	电源
E	扁平电缆连接器	N	输入
F	SIL 接口模块 (SIM)	O	起动
G	Preventa XPS-UAF 模块	P	扩展
H	起动按钮 (S2)		

图 9 - 示例：电机双向 - SIL 停止，接线类别 1/2 — 停止类别 0，接线类别 2 配置（直接监测）



A	机械联锁	F	SIL 接口模块 (SIM)
B	并联链路	J	安全功能 PLC
C	反向链路	K	上游电路断路器
D	紧急停止按钮 (S1)	M	数字量输入
E	扁平电缆连接器	N	数字量输出

SIL 停止，停止类别 1，接线类别 2 配置

注: 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 2。根据标准 EN/IEC 60204-1 确定的停止类别 1。

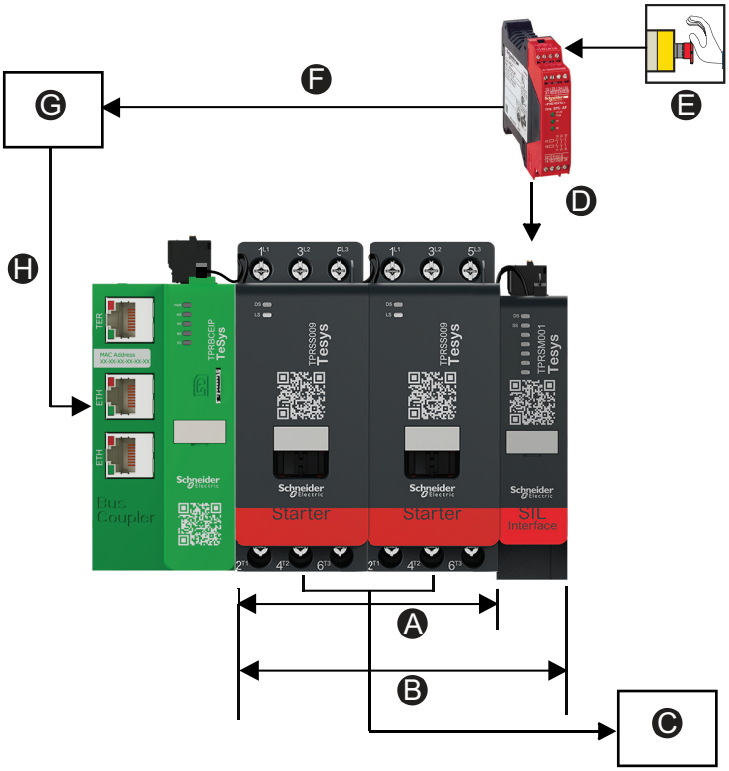
停止类别 1 被定义为“受控停止，机器执行器可以使用电源来实现停止，然后在停止后断开电源”。

触发紧急停止时，首先将停止命令发送到外部设备（例如，PLC 或驱动器）。以这种方式，该过程以受控方式而不是通过立即断电来停止。在预定义的时间之后，SIL 停止命令随后被发送到 SIM 以断开相关 SIL 安全起动器组中的 SIL Avatar 上的负载。

建议的设置是使用 PLC 来确保在 SIL 停止发生之前正确地停止流程。

停止命令可以使用其中一个 PLC 读取的数字量输入直接传递到 PLC 的数字量输入或 TeSys™ island 数字量 I/O 模块 avatar。在接收到停止命令输入时，PLC 通过向目标 TeSys island avatar 发出操作停止命令来启动受控停止。

图 10 - 停止命令



A	Avatar A1	E	接线类别 2，停止类别 1
B	SIL 安全起动器组 1	F	受控停止类别 1 命令
C	电机	G	PLC
D	不受控停止	H	运行停止命令

图 11 - 示例：电机双向 - SIL 停止，接线类别 1/2 — 停止类别 1，接线类别 2 配置

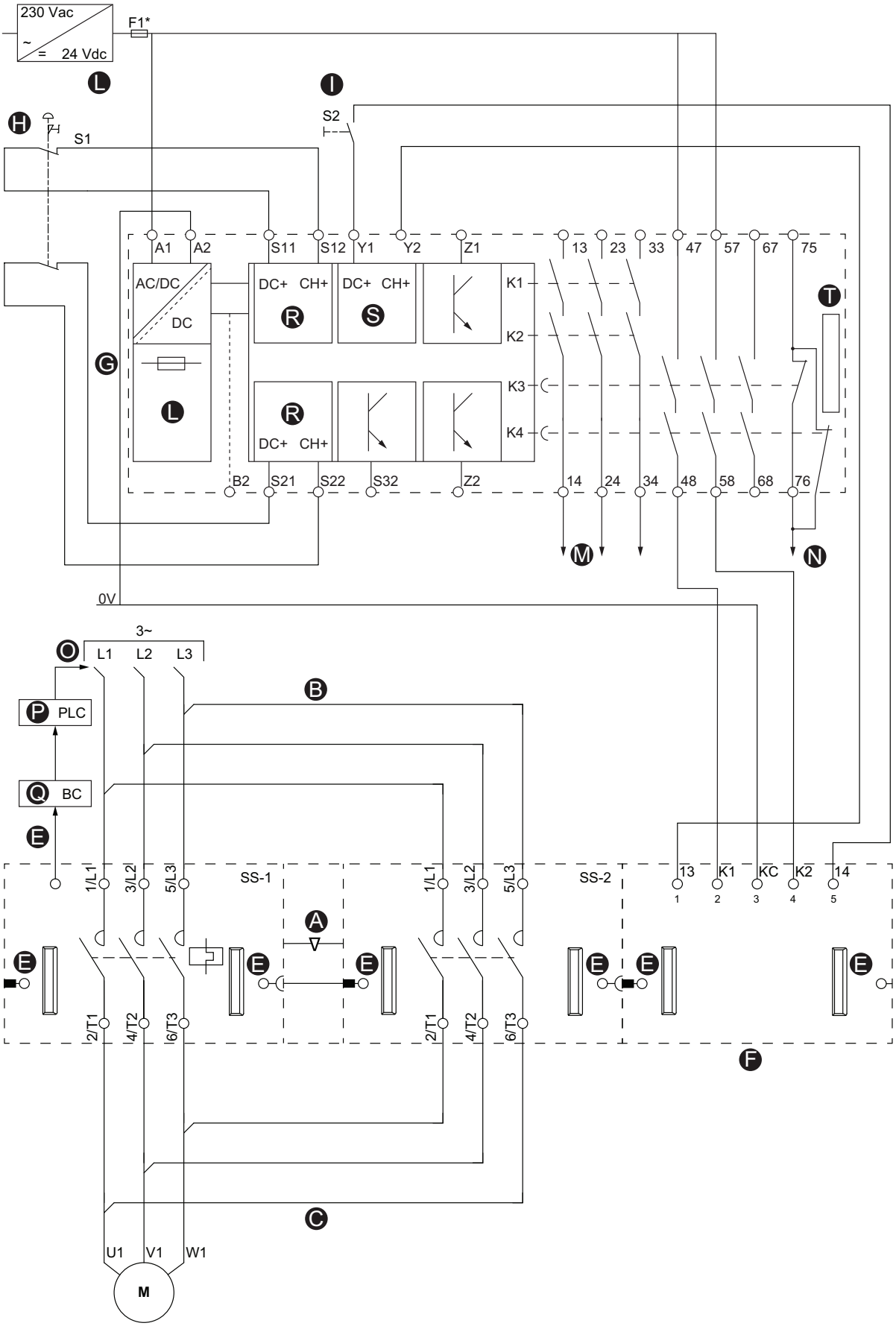


表 6 - 图例 示例：电机双向 - SIL 停止，接线类别 1/2 — 停止类别 1，接线类别 2 配置, 29 页

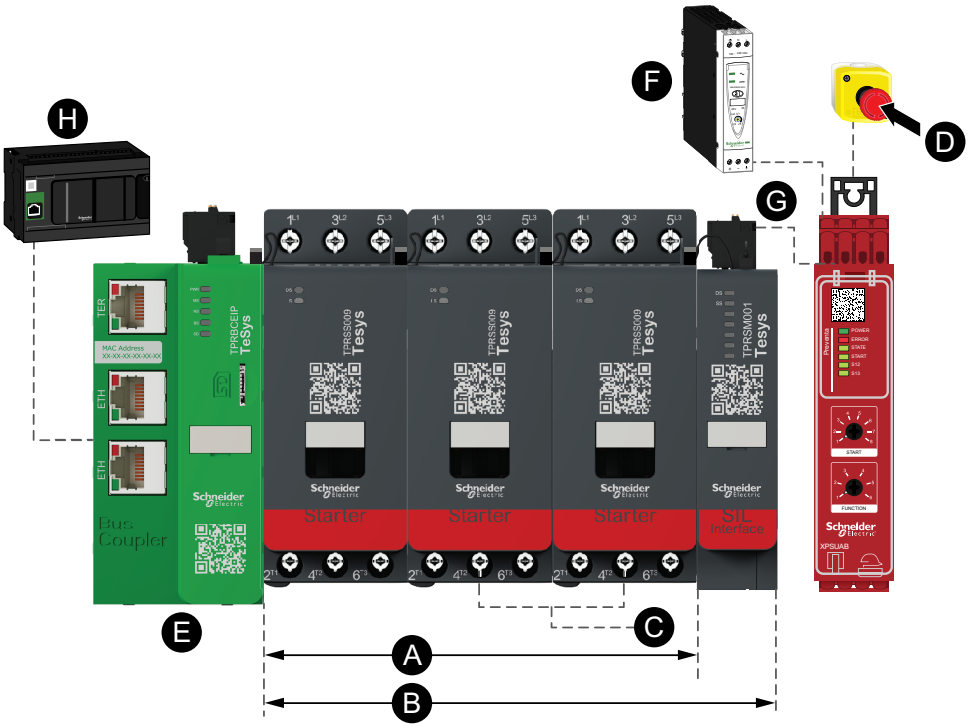
A	机械联锁	M	受控的停止
B	并联链路	N	停止类别 1
C	反向链路	O	上游电路断路器
E	扁平电缆连接器	P	PLC
F	SIL 接口模块 (SIM)	Q	总线耦合器
G	Preventa XPS-UAF 模块	R	输入
H	紧急停止按钮	S	起动
I	S2 起动按钮	T	扩展
L	电源		

SIL 停止，停止类别 0，接线类别 3/4 配置

注: 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 3/4。根据标准 EN/IEC 60204-1 确定的停止类别 0。

通过断开紧急停止按钮的触点直接控制电机的 SIL 停止。

图 12 - SIL 停止，接线类别 3/4



A	Avatar A1	E	总线耦合器
B	SIL 安全起动器组 1	F	24 VDC
C	电机	G	Preventa XPS-UAF 模块
D	接线类别 3/4，停止类别 0	H	PLC

图 13 - 示例：电机单向 - SIL 停止，接线类别 3/4 — 停止类别 0，接线类别 3/4 配置

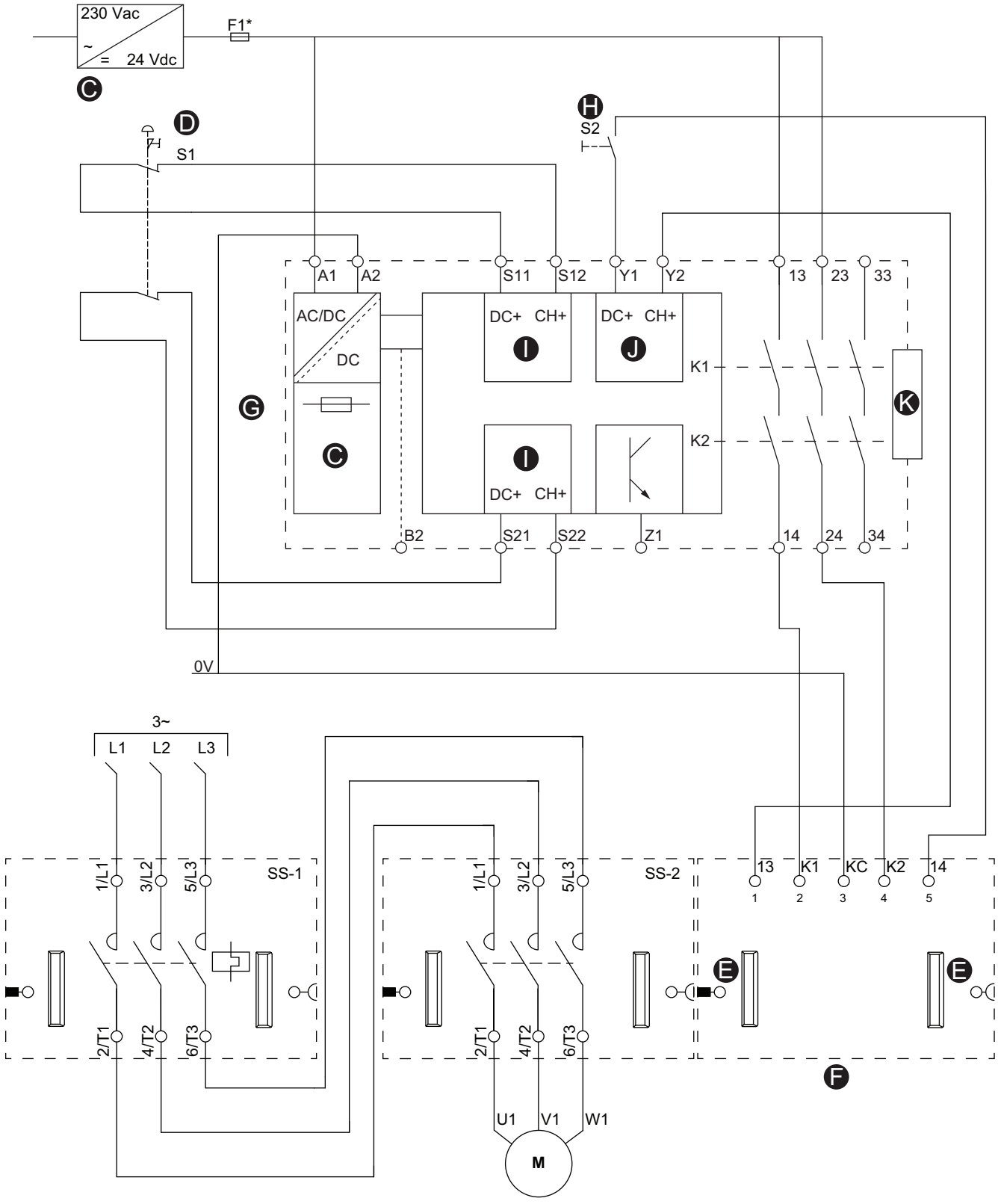


表 7 - 图例 示例：电机单向 - SIL 停止，接线类别 3/4 — 停止类别 0，接线类别 3/4 配置, 32 页

C	电源	H	起动按钮 (S2)
D	紧急停止按钮 (S1)	I	输入
E	扁平电缆连接器	J	起动
F	SIL 接口模块 (SIM)	K	扩展
G	Preventa XPS-UAF 模块		

SIL 停止，停止类别 1，接线类别 3/4 配置

注: 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 3/4。根据标准 EN/IEC 60204 确定的停止类别 1。

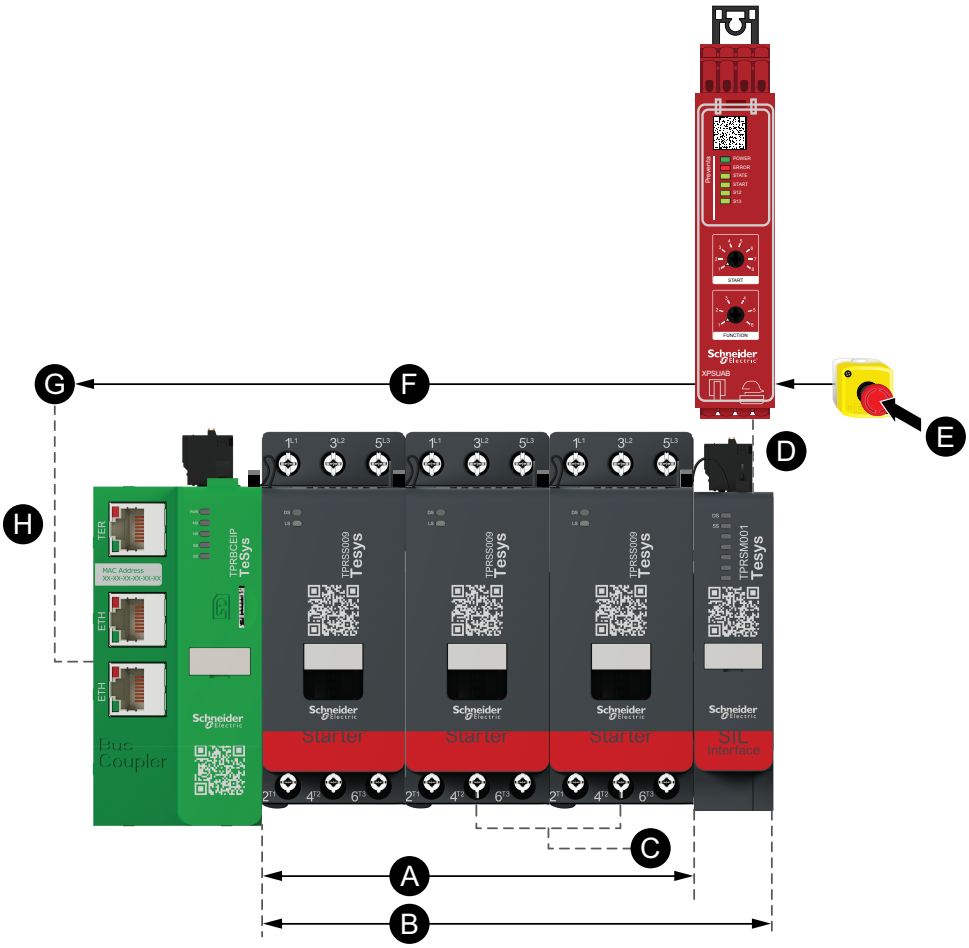
停止类别 1 被定义为“受控停止，机器执行器可以使用电源来实现停止，然后在停止后断开电源”。

触发紧急停止时，首先将停止命令发送到外部设备（例如，PLC 或驱动器）。以这种方式，该过程以受控方式而不是通过立即断电来停止。在预定义的时间之后，SIL 停止命令被发送到 SIM 以断开相关 SIL 安全起动器组中的 SIL Avatar 上的负载。

对于设置，建议使用 PLC 来确保在 SIL 停止发生之前正确地终止过程。

停止命令可以使用其中一个 PLC 读取的数字量输入直接传递到 PLC 的数字量输入或 TeSys™ island 数字量 I/O 模块 avatar。在接收到停止命令输入时，PLC 通过向目标 TeSys island avatar 发出操作停止命令来启动受控停止。

图 14 - 停止命令，接线类别 3/4



A	Avatar A1	E	接线类别 3/4，停止类别 1
B	SIL 安全起动器组 1	F	受控停止类别 1 命令
C	电机	G	PLC
D	不受控停止	H	运行停止命令

图 15 - 示例：电机双向 - SIL 停止，接线类别 3/4 — 停止类别 1，接线类别 3/4 配置

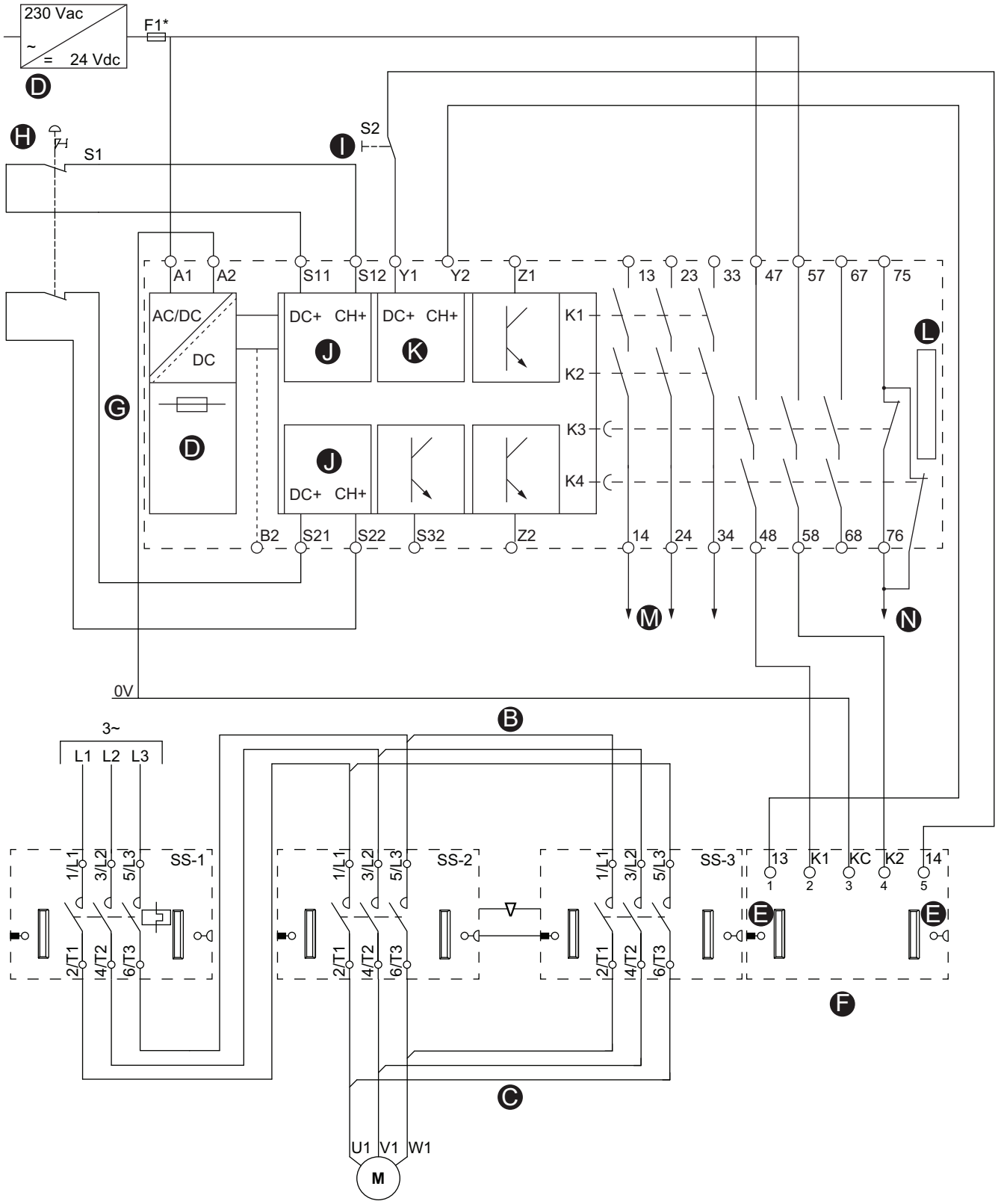


表 8 - 图例 示例：电机双向 - SIL 停止，接线类别 3/4 — 停止类别 1，接线类别 3/4 配置, 35 页

B	并联链路	I	S2 起动按钮
C	反向链路	J	输入
D	电源	K	起动
E	扁平电缆连接器	L	扩展
F	SIL 接口模块 (SIM)	M	受控的停止
G	Preventa XPS-UAF 模块	N	停止类别 1
H	紧急停止按钮 (S1)		

受保护电缆绝缘

⚠危险

意外的设备操作

确保按照 ISO 13849-2 标准安装安全相关系统的电缆。

未按说明操作将导致人身伤亡等严重后果。

如果安全相关系统的电缆可能发生短路和交叉电路，并且上游设备未检测到，则需要根据 ISO 13849-2 标准安装受保护的电缆。

在安装未受保护的电缆的情况下，如果电缆损坏，则短路状态下的安全功能的两个信号（两个通道）可能会连接到外部电压。在这种情况下，安全功能不再有效。

低/高频开关架构

本节中的信息可用于确定您是在低频还是高频架构中运行。

SIL[19] 起动器的机电部分具有 B10d 特征。

可以使用下列公式计算 $MTTF_d$（根据 ISO 13849-1）或 λd（根据 IEC 62061）：

$$MTTF_d=B10d/(0,1*Nop)$$

而 $\lambda d=1/MTTF_d$

Nop：年度操作的平均次数

根据 ISO 13849，机电组件的运行时间限于 T10d（平均时间，直到 10% 的组件危险地失效[20]）。

因此，SIL 起动器的运行时间限于：

$$T10d=B10d/Nop$$

SIL 起动器的 B10d 为 B10d = 1,369,863，假设 T10d 为 10 年，TeSys island SIL 起动器的循环次数限制为 Nop = B10d / T10 = 131,400 /年（或每年平均 15 次循环/小时）。

如果应用要求 Nop 低于该值，则它属于低开关频率类别（可以按原样使用 SIL avatar）。否则，它属于高开关频率类别（其中安全功能必须使用如下所述的专用 SIL avatar 来实现）。

19. 根据标准 IEC 61508 确定的安全完整性等级。
20. 由 ISO 13849 标准规定的危险失效

低开关频率（每小时 < 15 次循环）

低开关频率中，SIL[21]可以使用一个 SIL Avatar 同时实现安全停止和操作开/关控制功能。

图 16 - 使用 SIL 起动器的 Avatar 示例

表 9 - 低开关频率 - 运行和安全功能

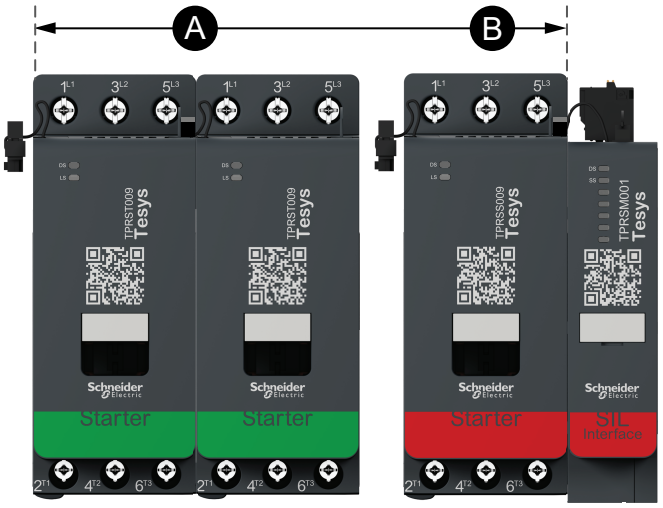
SIL Avatar	模块 1	模块 2	模块 3	模块 4	模块 5
开关 - SIL 停止，接线类别 1/2[22]	SIL 起动器	SIM	—	—	—
开关 - SIL 停止，接线类别 3/4[23]	SIL 起动器	SIL 起动器	SIM	—	—
电机单向 — SIL 停止，接线类别 1/2	SIL 起动器	SIM		—	—
电机单向 — SIL 停止，接线类别 3/4	SIL 起动器	SIL 起动器	SIM	—	—
电机双向 — SIL 停止，接线类别 1/2	SIL 起动器	SIL 起动器	SIM	—	—
电机双向 — SIL 停止，接线类别 3/4	SIL 起动器	SIL 起动器	SIL 起动器	SIM	—
电机双速 — SIL 停止，接线类别 1/2	SIL 起动器	SIL 起动器	SIM	—	—
电机双速 — SIL 停止，接线类别 3/4	SIL 起动器	SIL 起动器	SIL 起动器	SIM	—
电机双速双向 — SIL 停止，接线类别 1/2	标准起动器	标准起动器	SIL 起动器	SIL 起动器	SIM
电机双速双向 — SIL 停止，接线类别 3/4	SIL 起动器	SIL 起动器	SIL 起动器	SIL 起动器	SIM
输送机单向 — SIL 停止，接线类别 1/2	SIL 起动器	SIM	—	—	—
输送机双向 — SIL 停止，接线类别 1/2	SIL 起动器	SIL 起动器	SIM	—	—

21. 根据标准 IEC 61508 确定的安全完整性等级。
22. 根据标准 ISO 13849 确定的接线类别 1 和类别 2。
23. 根据标准 ISO 13849 确定的接线类别 3 和类别 4。

高开关频率（每小时 ≥ 15 次循环）

对于高频使用，安全功能必须与操作功能隔离，使用 SIL[24] Avatar 作为安全功能，并使用标准 Avatar 作为操作功能。然后将标准起动器串联在 SIL 起动器下游。高开关频率 – 运行和安全功能表显示了在 SIL 起动器下游用于 SIL 停止，接线类别 1/2[25] 和 SIL 停止，接线类别 3/4[26] 的标准 Avatar 架构的示例。

图 17 - 运行功能的标准 Avatar + 用于安全功能的 SIL Avatar — SIL 停止，接线类别 1/2



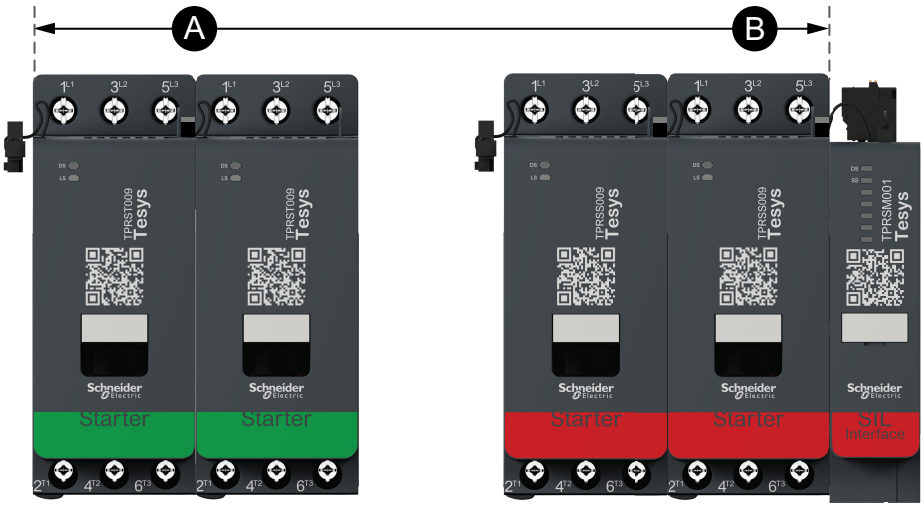
A	标准 avatar
B	SIL avatar

表 10 - 高开关频率 - SIL 停止，接线类别 1/2 — 运行和安全功能

标准 Avatar	SIL Avatar	模块 1	模块 2	模块 3	模块 4	模块 5	模块 6
开关	开关 - SIL 停止，接线类别 1/2	标准起动器	SIL 起动器	SIM	—	—	—
电机单向	开关 - SIL 停止，接线类别 1/2	标准起动器	SIL 起动器	SIM	—	—	—
电机双向	开关 - SIL 停止，接线类别 1/2	标准起动器	标准起动器	SIL 起动器	SIM	—	—
电机双速	开关 - SIL 停止，接线类别 1/2	标准起动器	标准起动器	SIL 起动器	SIM	—	—
电机双速双向	开关 - SIL 停止，接线类别 1/2	标准起动器	标准起动器	标准起动器	标准起动器	SIL 起动器	SIM
输送机单向	开关 - SIL 停止，接线类别 1/2	标准起动器	SIL 起动器	SIM	—	—	—
输送机双向	开关 - SIL 停止，接线类别 1/2	标准起动器	标准起动器	SIL 起动器	SIM	—	—
电机 Y/D 单向	开关 - SIL 停止，接线类别 1/2	标准起动器	标准起动器	标准起动器	SIL 起动器	SIM	—
电机 Y/D 双向	开关 - SIL 停止，接线类别 1/2	标准起动器	标准起动器	标准起动器	标准起动器	SIL 起动器	SIM

24. 根据标准 IEC 61508 确定的安全完整性等级。
25. 根据标准 ISO 13849 确定的接线类别 1 和类别 2。
26. 根据标准 ISO 13849 确定的接线类别 3 和类别 4。

图 18 - 用于操作功能的标准 Avatar + 用于安全功能的 SIL Avatar — SIL 停止，接线类别 3/4



A	标准 avatar
B	SIL avatar

表 11 - 高开关频率 - SIL 停止，接线类别 3/4 — 运行和安全功能

标准 Avatar	SIL Avatar	模块 1	模块 2	模块 3	模块 4	模块 5	模块 6	模块 7
开关	开关 - SIL 停止，接线类别 3/4	标准起动器	SIL 起动器	SIL 起动器	SIM	—	—	—
电机单向	开关 - SIL 停止，接线类别 3/4	标准起动器	SIL 起动器	SIL 起动器	SIM	—	—	—
电机双向	开关 - SIL 停止，接线类别 3/4	标准起动器	标准起动器	SIL 起动器	SIL 起动器	SIM	—	—
电机双速	开关 - SIL 停止，接线类别 3/4	标准起动器	标准起动器	SIL 起动器	SIL 起动器	SIM	—	—
电机双速双向	开关 - SIL 停止，接线类别 3/4	标准起动器	标准起动器	标准起动器	标准起动器	SIL 起动器	SIL 起动器	SIM
电机 Y/D 单向	开关 - SIL 停止，接线类别 3/4	标准起动器	标准起动器	标准起动器	标准起动器	SIL 起动器	SIL 起动器	SIM
电机 Y/D 双向	开关 - SIL 停止，接线类别 3/4	标准起动器	标准起动器	标准起动器	标准起动器	SIL 起动器	SIL 起动器	SIM

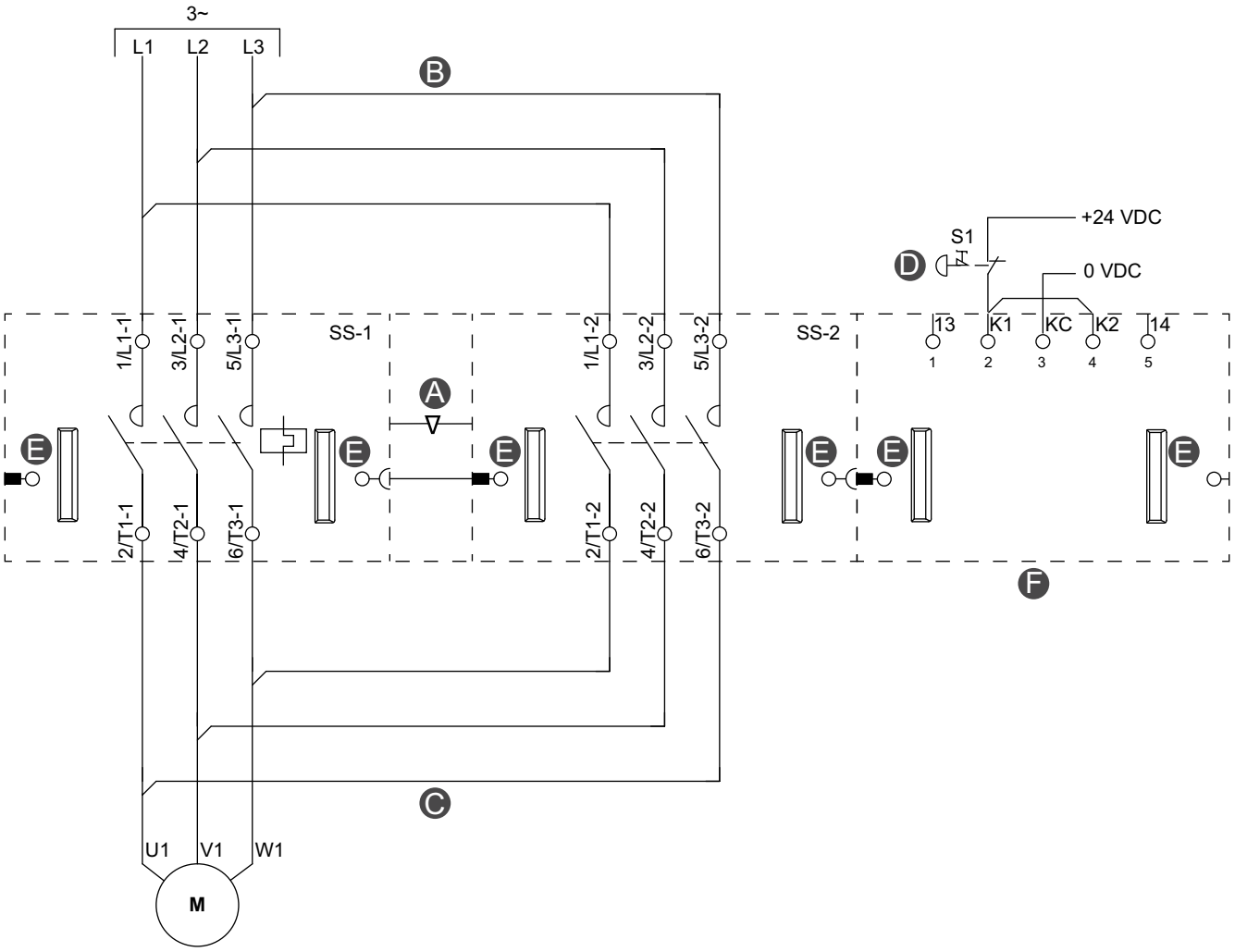
示例架构

以下架构可用于 TeSys™ island 的功能安全：

- SIL 停止，停止类别 0，接线类别 1[27]
- SIL 停止，停止类别 0，接线类别 2
- SIL 停止，停止类别 1，接线类别 2
- SIL 停止，停止类别 0，接线类别 3/4
- SIL 停止，停止类别 1，接线类别 3/4

SIL 停止，停止类别 0，接线类别 1

图 19 - 示例：SIL 停止，停止类别 0，接线类别 1[28]

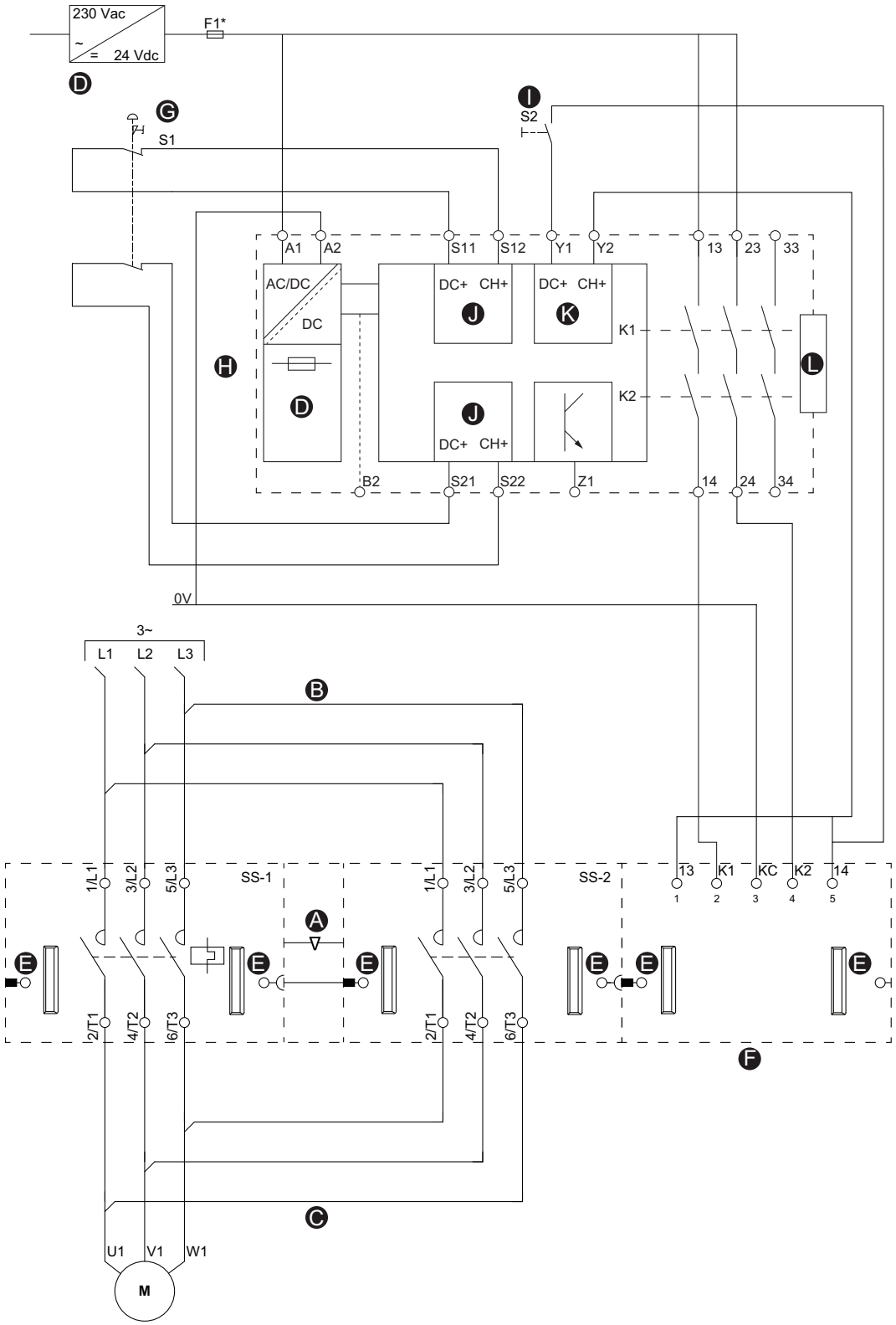


A	机械联锁	D	紧急停止按钮 (S1)
B	并联链路	E	扁平电缆连接器
C	反向链路	F	SIL 接口模块 (SIM)

27. 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 1、类别 2 和类别 3/4。根据标准 EN/IEC 60204-1 确定的停止类别 0 和类别 1。
28. 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 1。根据标准 EN/IEC 60204-1 确定的停止类别 0。

SIL 停止，停止类别 0，接线类别 2

图 20 - 示例：SIL 停止，停止类别 0，接线类别 2[29]



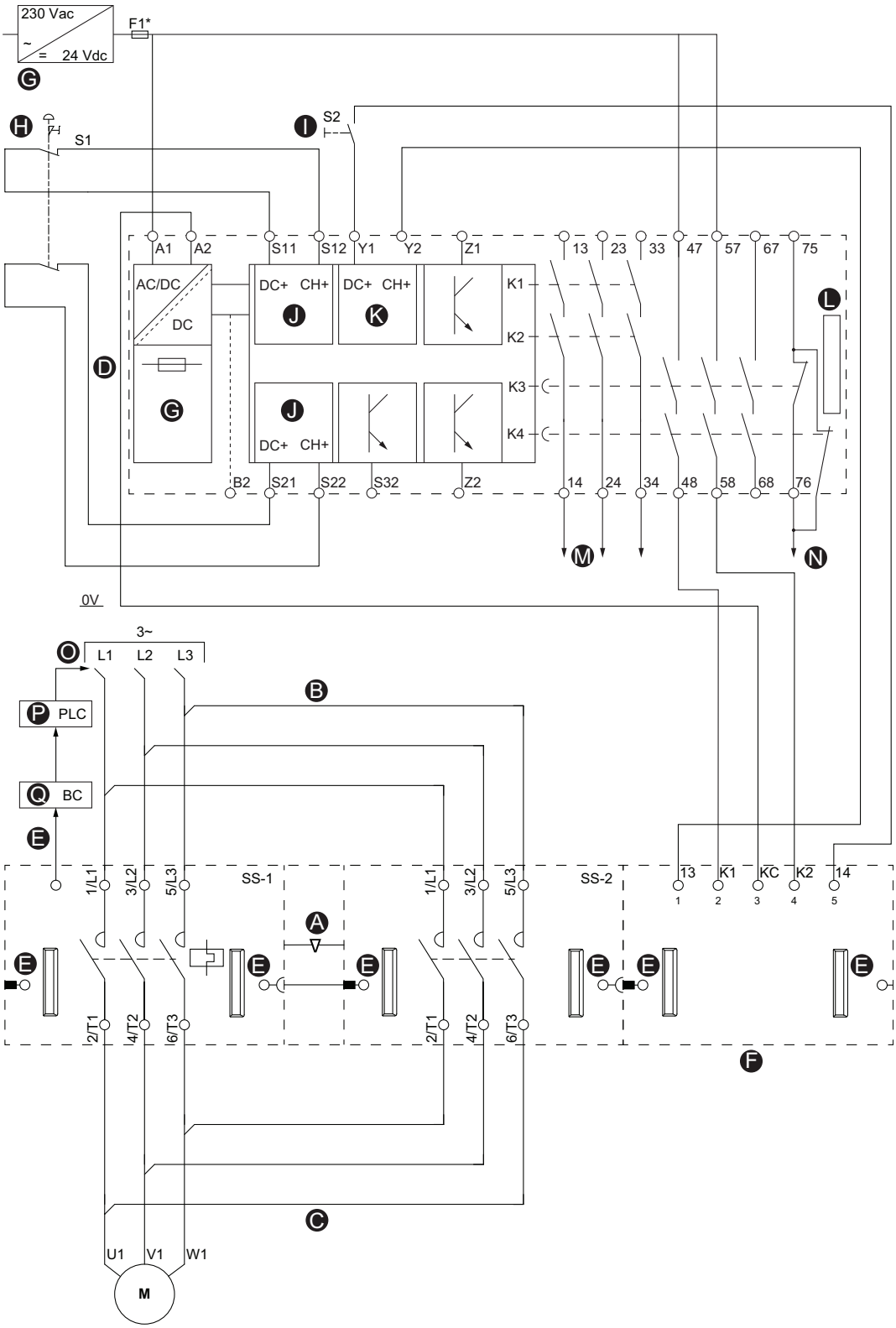
29. 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 2。根据标准 EN/IEC 60204-1 确定的停止类别 0。

表 12 - 示例图例：SIL 停止，停止类别 0，接线类别 2, 42 页

A	机械联锁	G	紧急停止按钮 (S1)
B	并联链路	H	Preventa XPS-UAF 模块
C	反向链路	I	起动按钮 (S2)
D	电源	J	输入
E	扁平电缆连接器	K	启动
F	SIL 接口模块 (SIM)	L	扩展

SIL 停止，停止类别 1，接线类别 2

图 21 - 示例：SIL 停止，停止类别 1，接线类别 2[30]



30. 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 2。根据标准 EN/IEC 60204-1 确定的停止类别 1。

表 13 - 示例图例：SIL 停止，停止类别 1，接线类别 2, 44 页

A	机械联锁	J	输入
B	并联链路	K	启动
C	反向链路	L	扩展
E	扁平电缆连接器	M	受控的停止
F	SIL 接口模块 (SIM)	N	停止类别 1
G	电源	O	上游断路器
H	紧急停止按钮 (S1)	P	PLC
I	S2 起动按钮	Q	总线耦合器

SIL 停止，停止类别 0，接线类别 3/4

图 22 - 示例：SIL 停止，停止类别 0，接线类别 3/4[31]

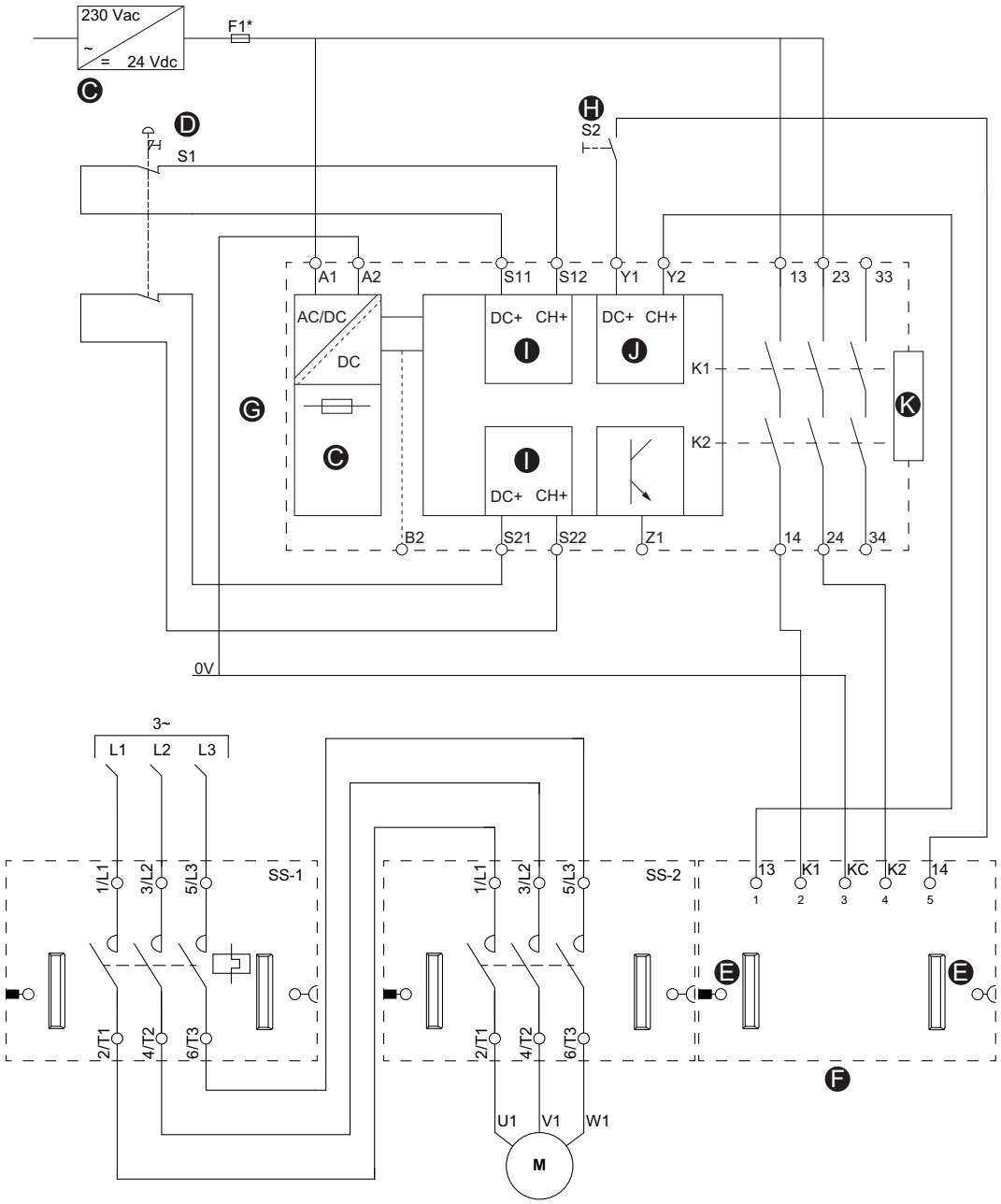


表 14 - 示例图例：SIL 停止，停止类别 0，接线类别 3/4, 46 页

C	电源	H	起动按钮 (S2)
D	紧急停止按钮 (S1)	I	输入
E	扁平电缆连接器	J	启动

31. 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 3/4。根据标准 EN/IEC 60204-1 确定的停止类别 0。

表 14 - 示例图例：SIL 停止，停止类别 0，接线类别 3/4 (持续)

F	SIL 接口模块 (SIM)	K	扩展
G	Preventa XPS-UAF 模块		

SIL 停止，停止类别 1，接线类别 3/4

图 23 - 示例：SIL 停止，停止类别 1，接线类别 3/4[32]

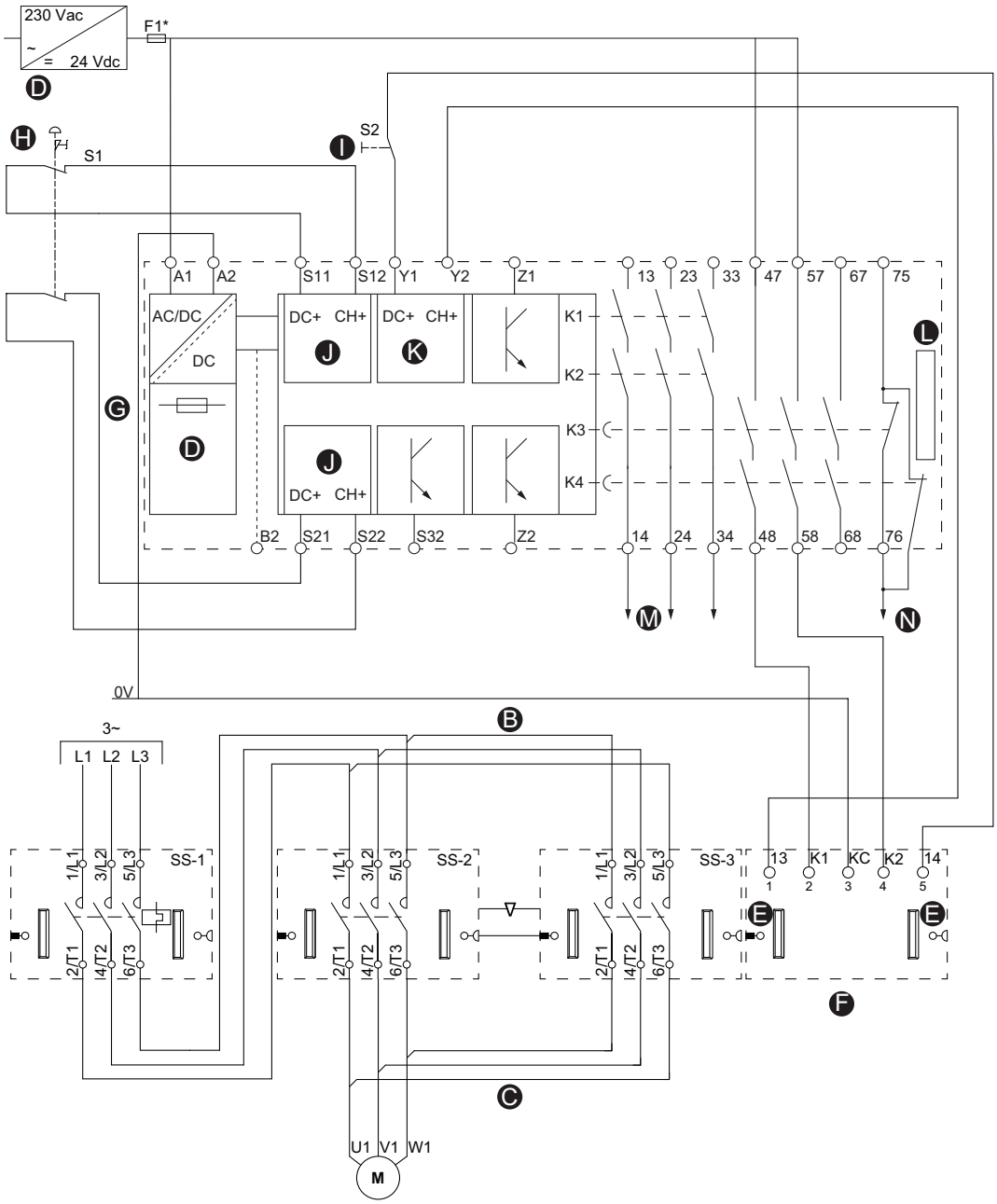


表 15 - 示例图例：SIL 停止，停止类别 1，接线类别 3/4, 48 页

B	并联链路	I	S2 起动按钮
C	反向链路	J	输入
D	电源	K	启动
E	扁平电缆连接器	L	扩展

32. 根据标准 IEC 61508 确定的安全完整性等级。根据标准 ISO 13849 确定的接线类别 3/4。根据标准 EN/IEC 60204-1 确定的停止类别 1。

表 15 - 示例图例：SIL 停止，停止类别 1，接线类别 3/4 (持续)

F	SIL 接口模块 (SIM)	M	受控的停止
G	Preventa XPS-UAF 模块	N	停止类别 1
H	紧急停止按钮 (S1)		

技术数据

SIL 接口模块

表 16 - SIL[33] 的计算值接口模块 (SIM)

架构	SIM					
	PFH[34]	PFD[35]	SFF[36]	HFT[37]	$MTTF_d$（年）	DC[38]
接线类别 1[39]	2.10^{-10}	2.10^{-5}	>90%	1	17,459	不相关
接线类别 2			>99%			90%
接线类别 3			>99%			90%
接线类别 4			99%			99%

注: PFD 和 PFH 值的计算如下：

- 测试间隔 = 20 年
- MTTR[40]=MRT[40]= 24 小时

IEC 61508-2 表 3 和 EN 62061 表 5 中定义的架构要求最高符合 SIL 3 级。

SIL 起动器

以下数据有助于定义 SIL[33] 起动器的性能级别。

B10：**1,000,000**

危险故障的百分比[41]：**73%**

$B10_d$：**1,369,863**

假设操作次数 = 131,400 次循环/年（平均 15 次循环/小时）

SIL 起动器的计算值如下表所示：

表 17 - 单通道中的 SIL 起动器

接线类别[39]	SFF	HFT	$MTTF_d$（年）	直流
类别 1	27%	0	100 年	不相关
类别 2 - 直接监控	90%	0	100 年	≥ 90%

表 18 - 双通道中的 SIL 起动器

接线类别	SFF	HFT	$MTTF_d$（年）	直流
类别 3	27%	0	100 年	≥ 90%
类别 4	90%	0	100 年	≥ 99%

根据架构和测试间隔，SIL 起动器的 PFH_d 和 PFD 之间的关系如下表所示：

33. 根据标准 IEC 61508 确定的安全完整性等级。
34. 危险故障的平均频率 [h-1]，如 IEC 61508-4 中所定义
35. 按需发生危险故障的概率，如 IEC 61509-4 中所定义。
36. 安全故障分数，如 IEC 61509-4 中所定义。
37. 硬件容错，如 IEC 61509-4 中所定义。
38. 诊断覆盖，如 IEC 61509-4 中所定义。
39. 根据标准 ISO 13849 确定的接线类别 1、2、3 和 4。
40. 平均维修时间，如 IEC 61509-4 中所定义
41. 危险故障如 IEC 61508-4 中所定义

表 19 - SIL 起动器 — PFH_d 和 PFD

接线类别	PFH (IEC 61508)	PFD (IEC 61508) Ti=10 年[42]	PFD (IEC 61508) Ti=5 年[42]
类别 1	1.10E-06	4.80E-02	4.82E-03
类别 2 - 直接监控	1.10E-06	4.82E-03	5.06E-04
类别 3	4.5E-09	—	1.30E-04
类别 4	2.5E-10	—	2.5E-06

IEC 61508-2 表 3 和 EN 62061 表 5 中定义的架构要求最高符合 SIL 2 级。

需要类别 2 架构来满足 SIL 2 架构约束（使用直接监控镜像输入/镜像输出完成）。

注: 必须在安全相关控制功能解决的危险情况发生之前执行故障检测和指定的故障响应。

可靠性数据

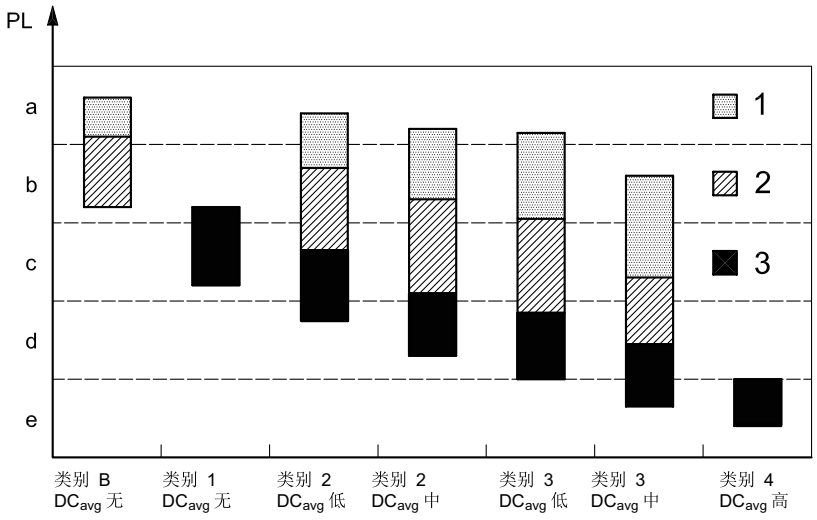
安全功能标准参考

SIL[43]停止功能优先于因操作原因触发的停止 (EN ISO 13849-1, 5.2.1)。

性能水平取决于接线类别[44]、$MTTF_d$ 和 DC_{avg}。

下图显示了根据类别要求的 TeSys™ island 定位。

图 24 - 按类别要求进行的 TeSys island 定位



按键

PL - 性能等级

1 每个通道的 $MTTF_d$ = 低

2 每个通道的 $MTTF_d$ = 中

3 每个通道的 $MTTF_d$ = 高

42. 测试间隔
43. 根据标准 IEC 61508 确定的安全完整性等级。
44. 根据标准 ISO 13849 确定的接线类别。

表 20 - 通过控制系统安全相关部件实现 PL 评估的简化程序 (SRP/CS)

类别	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**无**	**无**	**低**	**中**	**低**	**中**	**高**
每个通道的 $MTTF_d$							
低	a	未覆盖	a	b	b	c	未覆盖
中	b	未覆盖	b	c	c	d	未覆盖
高	未覆盖	c	v	d	d	d	e

根据 TeSys island 的架构和接线类别，TeSys island 应符合的关键指标值（DC_{avg}、$MTTF_d$、PL）显示在下表中。

表 21 - 单通道和双通道架构的关键指标值

TeSys island 系统架构	**类别**	**单一容错[45]**	**DC_{avg}**	**每个通道的 $MTTF_d$**	**目标 PL**
单通道	1	否	无	高（≥ 30 年）	c
	2	否	低 (≥ 60%) 至中 (≥ 90%)	低（≥ 3 年）至高（≥ 30 年）	c、d
双通道	3	是			c、d、e
	4	是	高 (≥ 99%)	高（≥ 30 年）	e

45. 单一容错系指单个故障（包括共模事件）不得导致安全功能丧失。

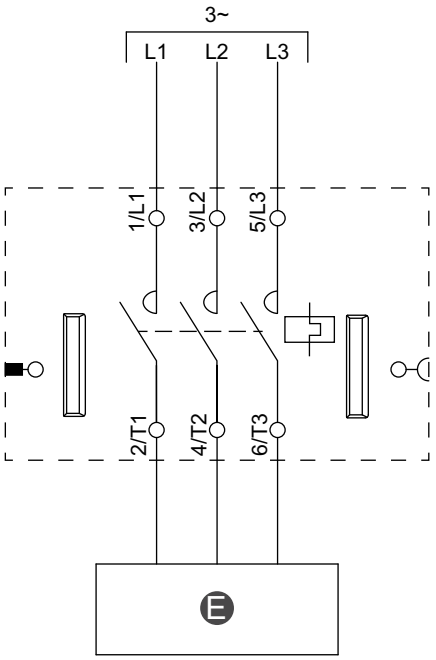
SIL Avatar 接线

本节的接线图适用于 SIL[46] Avatar。下表是本节中接线图的图例。

表 22 - 接线图图例

A	机械联锁
B	并联链路
C	反向链路
E	电路

图 25 - 开关 - SIL 停止，接线类别 1/2[47]



46. 根据标准 IEC 61508 确定的安全完整性等级。
47. 根据标准 ISO 13849 确定的接线类别 1 和类别 2。

图 26 - 电机单向 — SIL 停止，接线类别 1/2

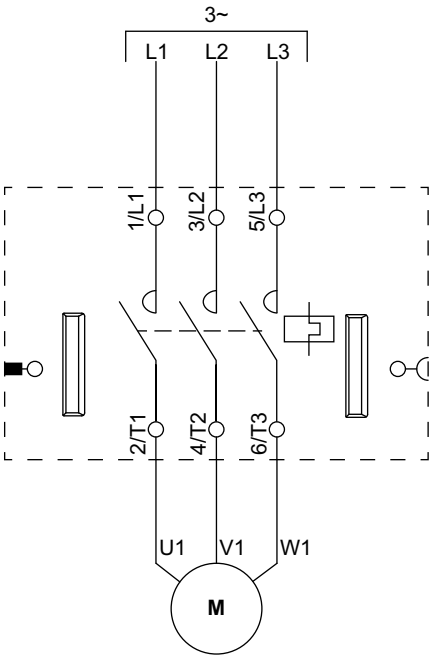


图 27 - 电机双向 — SIL 停止，接线类别 1/2

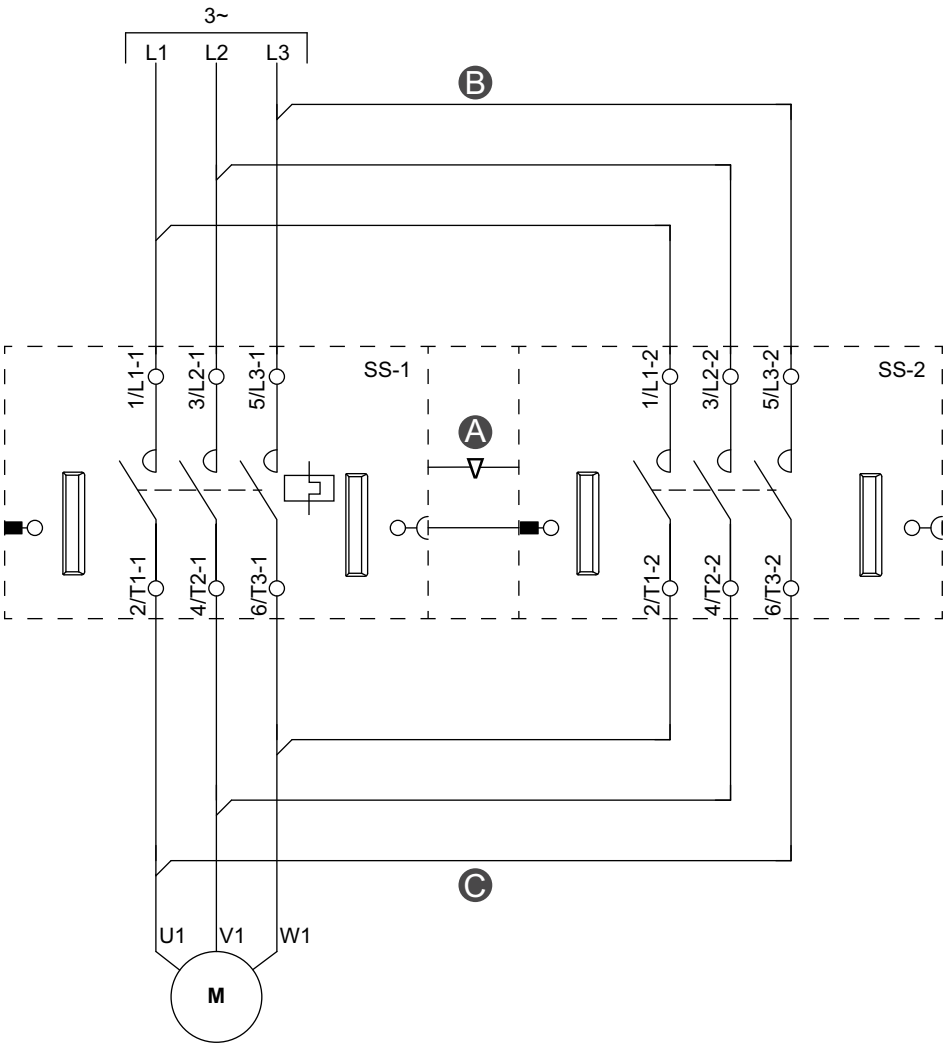


图 28 - 电机双速 — SIL 停止，接线类别 1/2

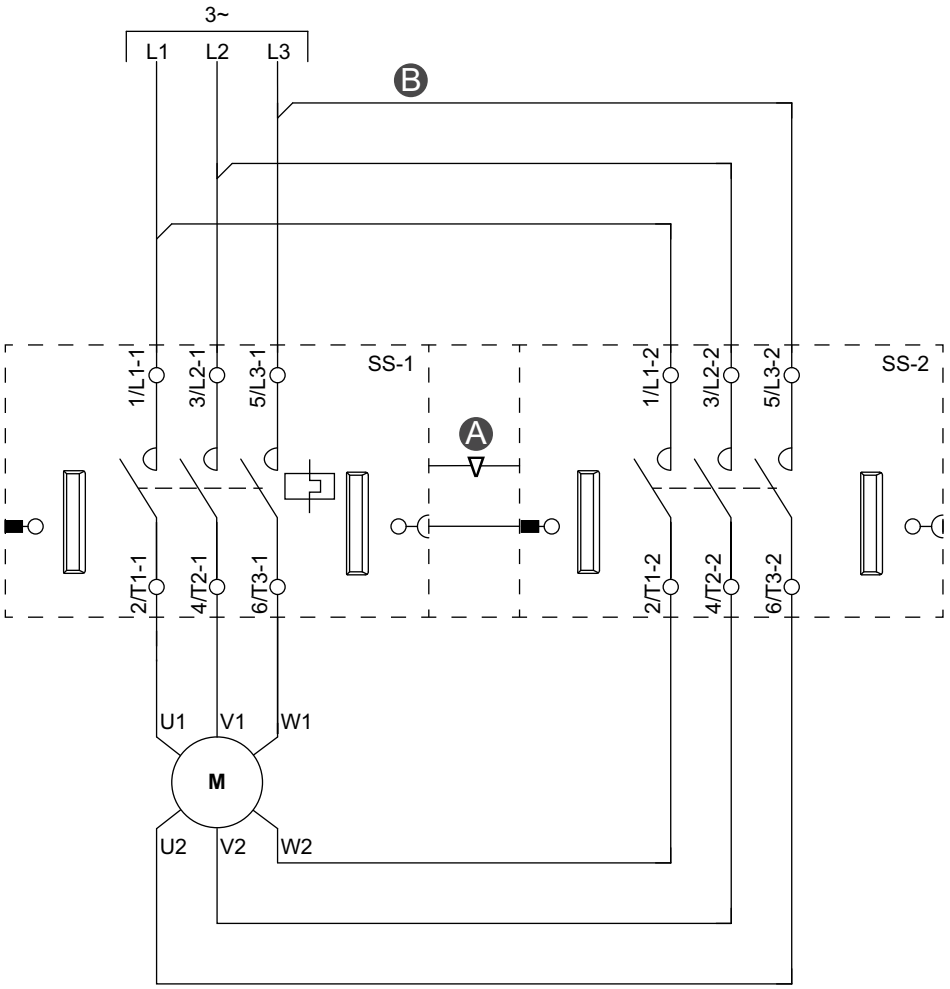


图 29 - 电机双速双向 — SIL 停止，接线类别 1/2

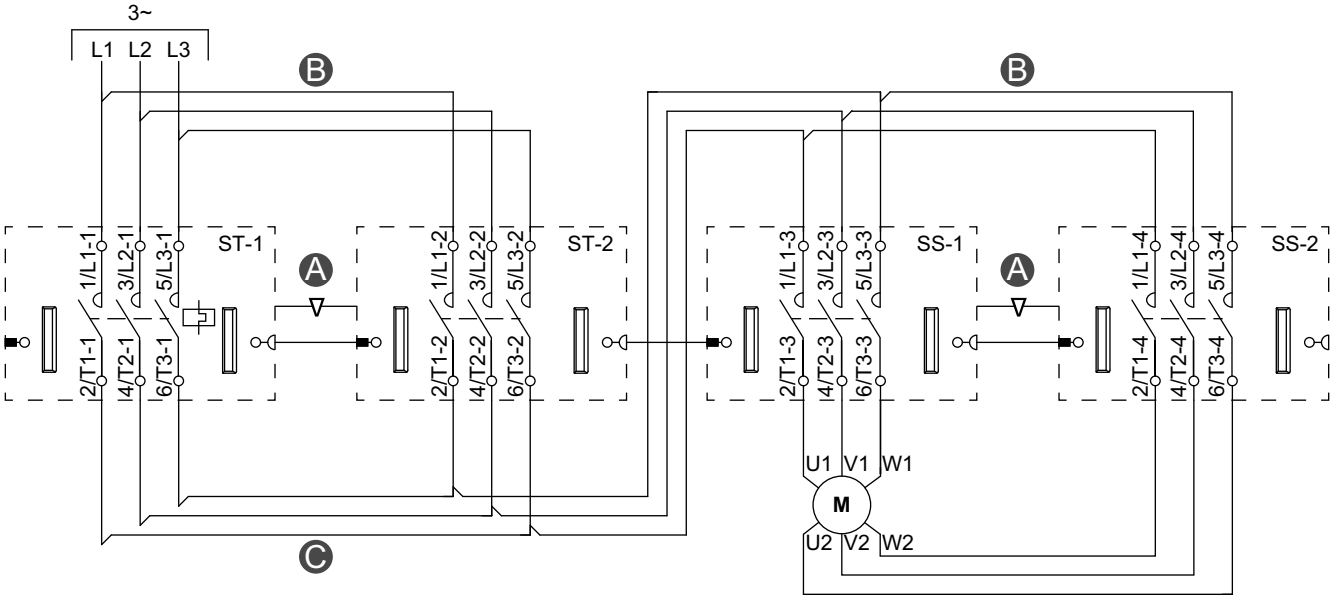


图 30 - 开关 - SIL 停止，接线类别 3/4[48]

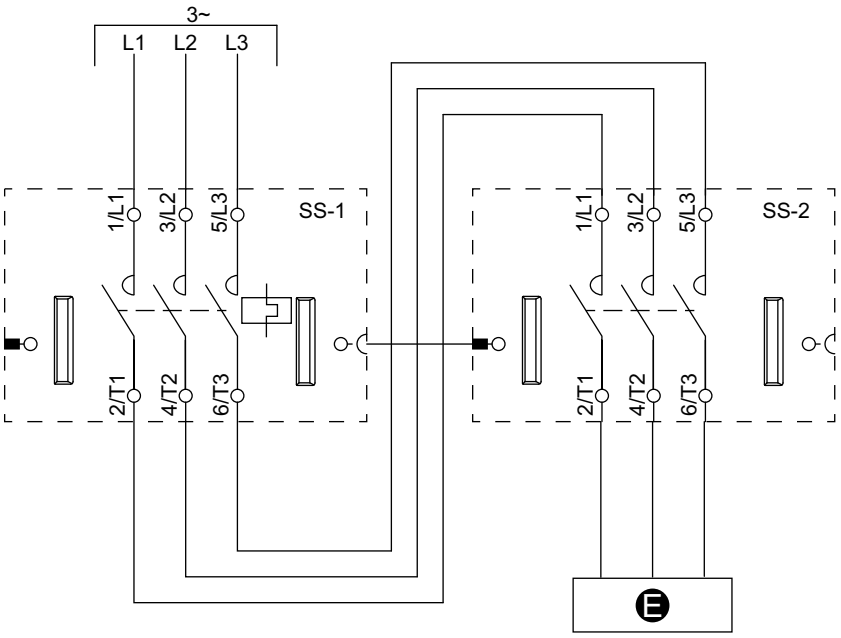
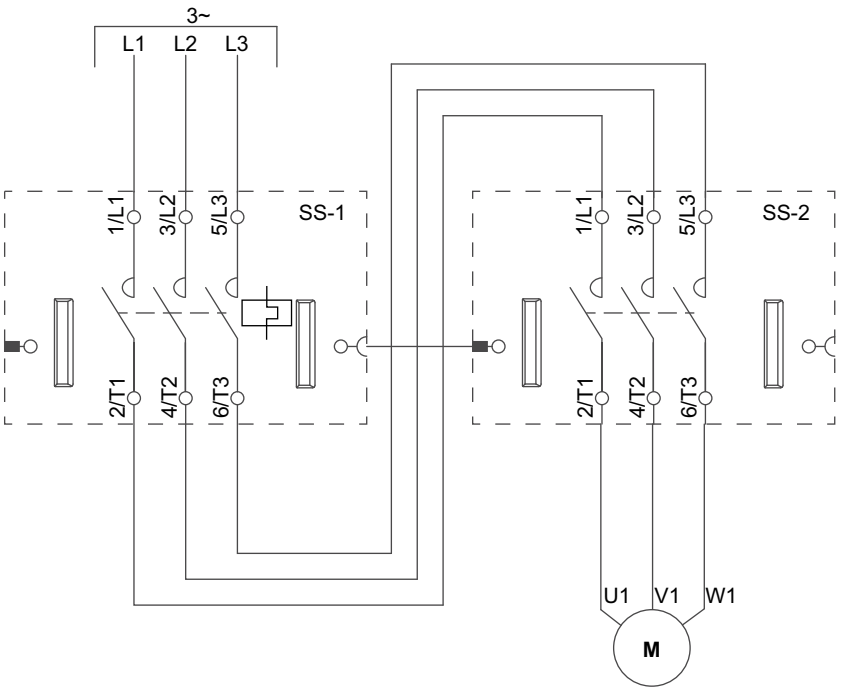


图 31 - 电机单向 — SIL 停止，接线类别 3/4



48. 根据标准 ISO 13849 确定的接线类别 3 和类别 4。

图 32 - 电机双向 — SIL 停止，接线类别 3/4

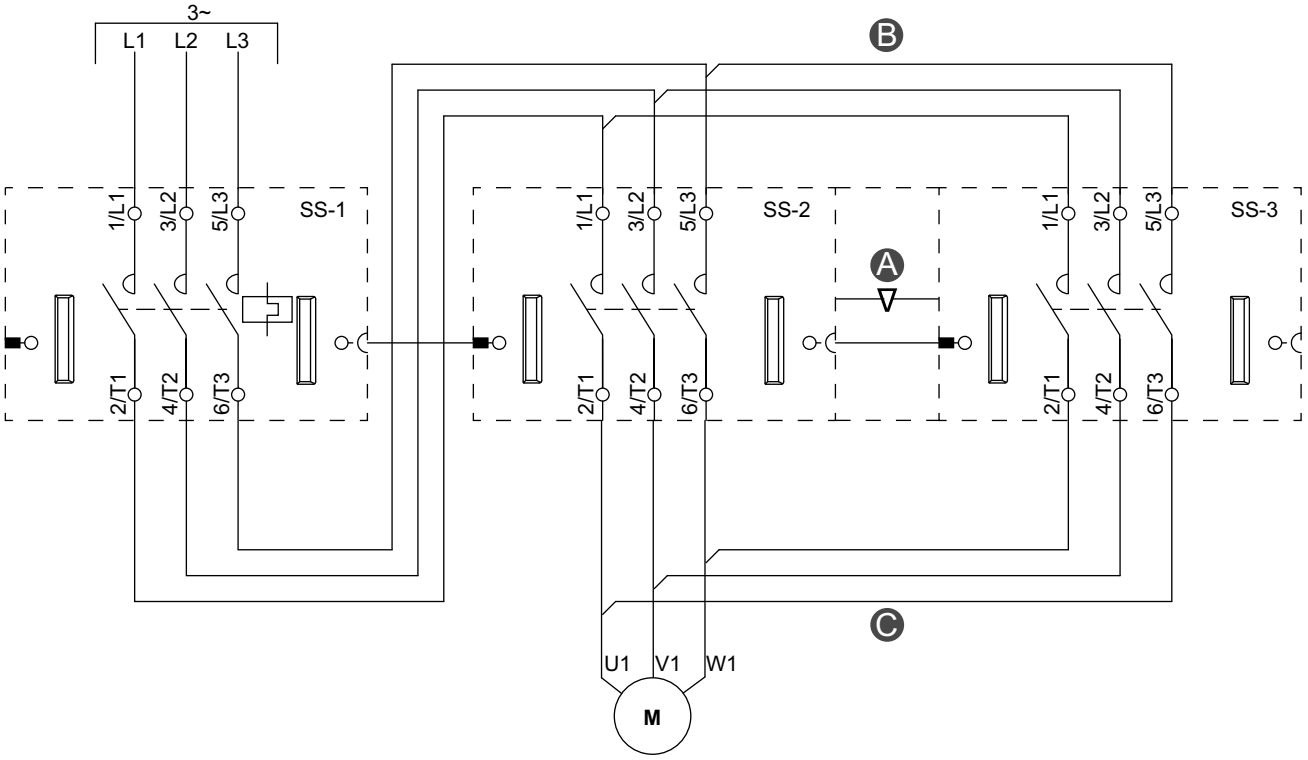


图 33 - 电机双速 — SIL 停止，接线类别 3/4

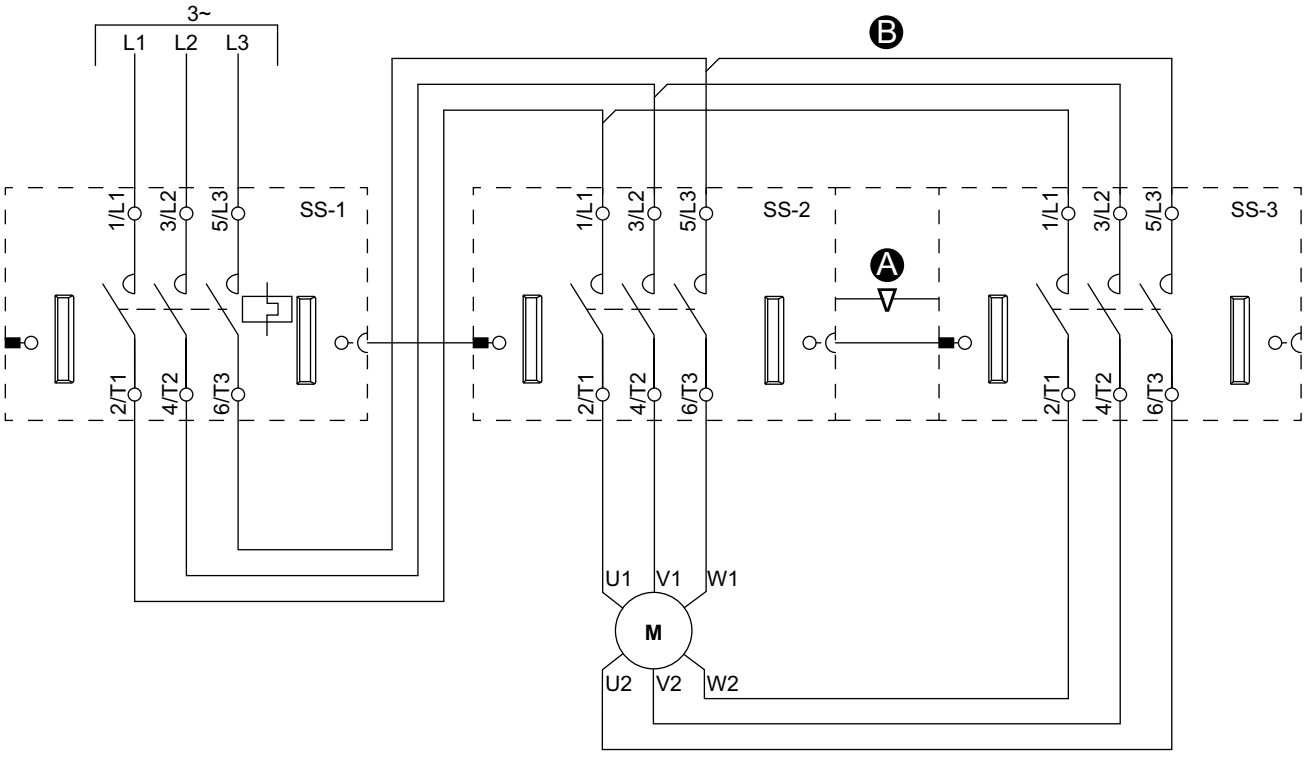


图 34 - 电机双速双向 — SIL 停止，接线类别 3/4

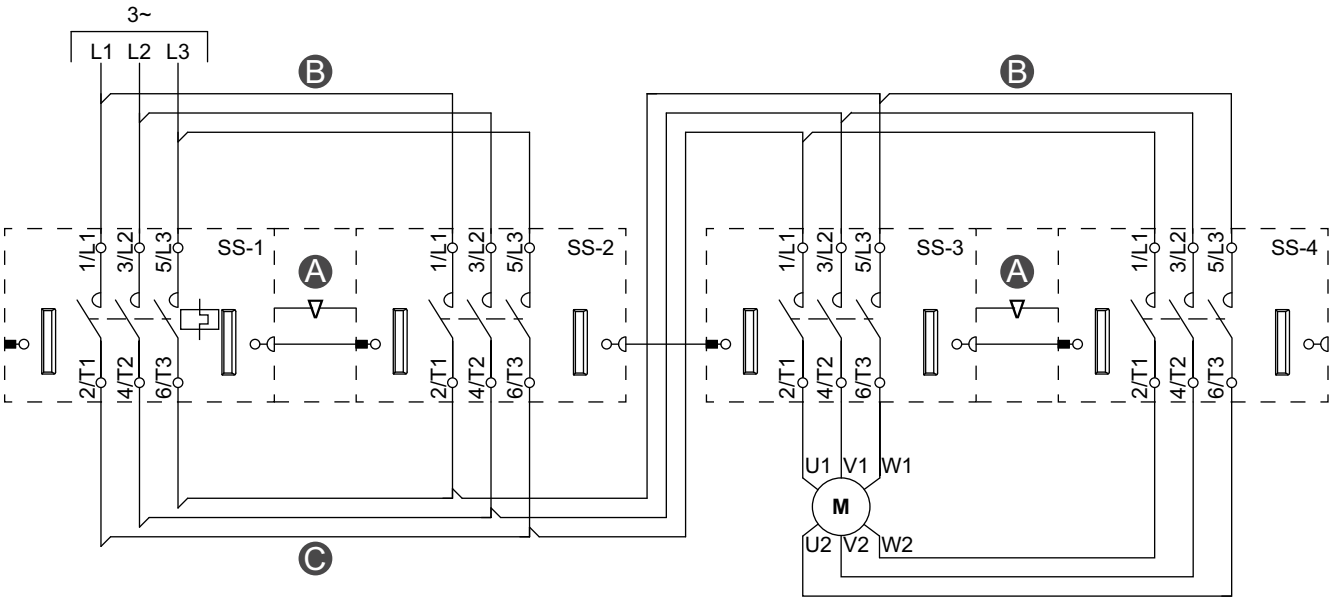


图 35 - 输送机单向 — SIL 停止，接线类别 1/2

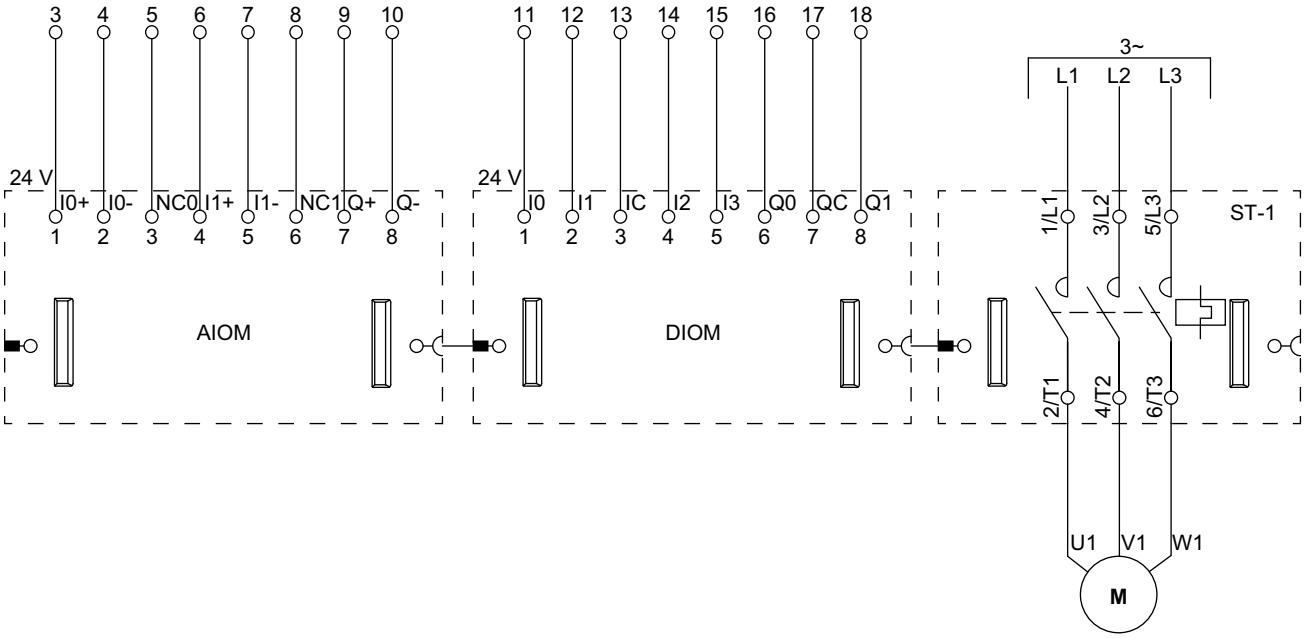
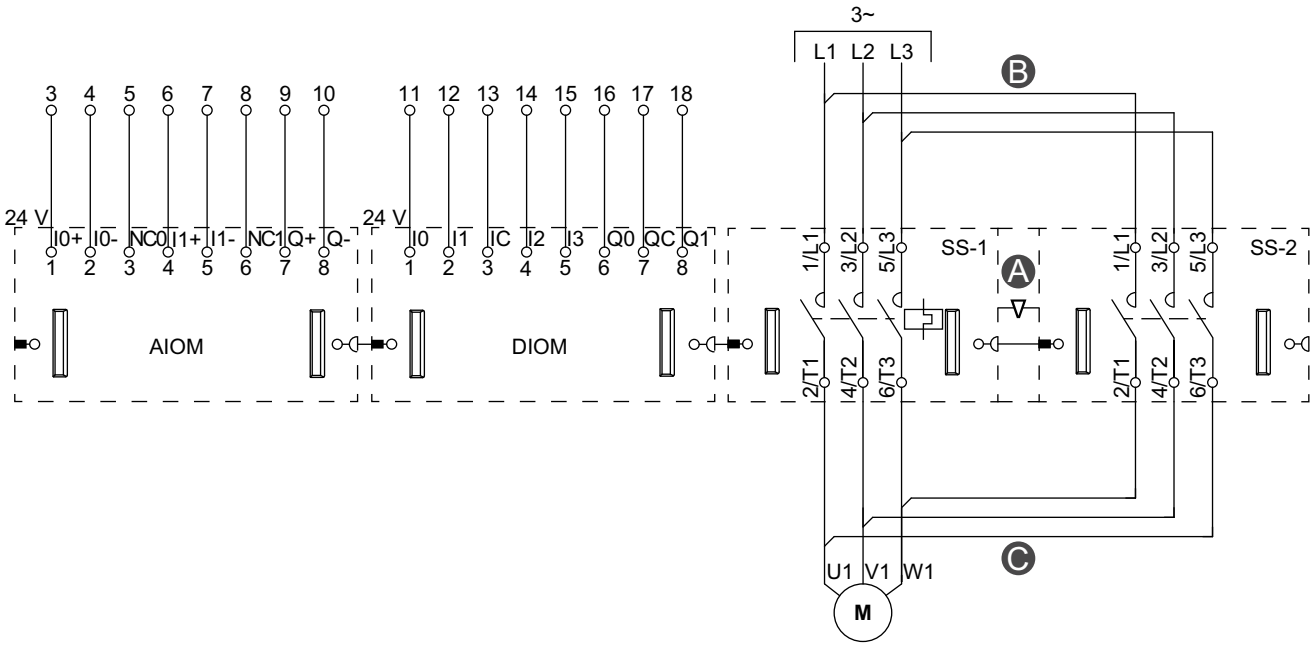


图 36 - 输送机双向 — SIL 停止，接线类别 1/2



调试安全功能

使用此程序调试安全功能。该程序包括两个步骤：

- 安装测试
- 安全功能验证测试 [49]

安装测试

执行下表中的步骤以测试安全功能的安装。

表 23 - 安装测试

1	使用 TeSys™ island DTM 中的**诊断**面板，验证物理拓扑是否与逻辑拓扑匹配。
2	使用 TeSys island DTM 中的**我的 AVATAR** 面板，验证在 **AVATAR 参数**中 SIL[50] Avatar 是否已经与正确的 SIL 相关联。

安全功能验证测试

对阀岛上的每个 SIL[50] 安全起动器组进行安全功能验证测试。SIL 安全起动器组可以包括由一个 SIL 接口模块 (SIM) 管理的多个 SIL avatar。

如果在激活与 SIL 安全起动器组相关联的紧急停止装置时，属于该 SIL 安全起动器组的所有 SIL 起动器都进入安全状态（负载断电），则安全功能验证测试成功。

注: 对于停止类别 0（非受控的停止），应立即停止。对于停止类别 1（受控的停止），停止在延迟后生效。[51]

对阀岛上的每个 SIL 安全起动器组执行下表中的步骤，以执行安全功能验证测试。

表 24 - 安全功能验证测试

1	激活与 SIL 安全起动器组关联的紧急停止设备，并检查属于该组的所有 SIL 起动器是否都进入安全状态（负载断电）。 **注:** SIL 起动器上的设备状态 (DS) LED 将闪烁红色，表示设备处于小事件状态。 如果未通过测试： • 紧急停止装置可能连接到错误的 SIM。检查这些连接。 • 紧急停止设备可能未正确接线到 SIM。检查这些连接。 • 某些 SIL avatar 可能不会连接到预期的 SIL 安全起动器组。检查配置。
2	在 TeSys™ island DTM 或 OMT **AVATARS** 面板上的**诊断**部分，检查**状态**和**事件日志**，确认 **SIL 安全起动器组状态**是否等于“**停止命令**”。在事件日志中将显示“SIL 安全起动器组停止命令，实现安全状态”。 如果未通过测试： • 某些 SIL avatar 可能不会连接到预期的 SIL 安全起动器组。检查配置。
3	在**诊断**面板的**设备**部分，验证 **SIL 接口模块 (SIM) 状态**是否等于“**停止命令**”。在事件日志中将显示“SIL 安全起动器组停止命令，实现安全状态”。 如果未通过测试： • 紧急停止装置可能连接到错误的 SIM。检查这些连接。 • 紧急停止设备可能未正确接线到 SIM。检查这些连接。

49. IEC 62061 中定义的验证测试
50. 根据标准 IEC 61508 确定的安全完整性等级。
51. 根据标准 EN/IEC 60204-1 确定的停止类别 0 和类别 1。

表 24 - 安全功能验证测试 (持续)

4	将起动命令应用到属于 SIL 安全起动器组的 SIL avatar，并验证起动是否成功：起动器应保持打开状态，并且应忽略起动命令，直到紧急停止设备被复位。 如果未通过测试： • 某些 SIL avatar 可能不会连接到预期的 SIL 安全起动器组。检查配置。 如果采取纠正措施后这些测试中的任何一项未通过，请不要继续操作该阀岛。请更换未通过测试的设备。
5	安全功能验证测试完成后，复位紧急停止设备并验证所有 SIL 起动器和 SIL 接口模块是否处于就绪状态（DS LED 呈绿色稳定亮起）。

安全功能维护要求

本节介绍了维护 TeSys™ island 上功能安全所需的日常维护。

维护计划

维护间隔取决于频率模式。

- 对于低频模式（每年平均接触器操作循环次数小于 15 次循环/小时），每 12 个月进行一次维护。
- 对于高频模式（每年平均接触器操作循环次数大于 15 次循环/小时或 136,986 次循环/年），请按照设备估计寿命 1/10 的间隔执行维护。

该设备估计寿命（年）= B10d（= 1,369,863）/年平均接触器操作循环次数

维护检查

设备使用检查

执行下表中描述的检查以验证 SIL[52] 起动器接触器操作循环是否在可接受的寿命值内。

1	使用 TeSys™ island DTM 或 OMT 的设备**诊断**功能，访问每个 SIL 起动器的设备资产信息。
2	如果**接触器操作循环次数**大于 B10d (=1,369,863)，则更换 SIL 起动器。
3	否则，使用**接触器操作循环次数**值计划下一次维护。请参阅 维护计划, 62 页。

安全功能验证测试

对每个 SIL[52]安全起动器组执行安全功能验证测试。请参阅 安全功能验证测试, 60 页。

52. 根据标准 IEC 61508 确定的安全完整性等级。

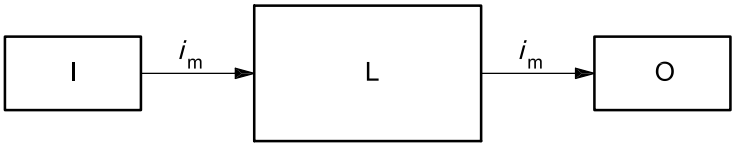
附录：单通道架构

这种单通道架构包含接线类别 1 和 2。

接线类别 1 的架构要求

类别 1 的指定架构在 EN ISO 13849-1, 6.2.4 中定义。

图 37 - 类别 1 指定架构 (EN ISO 13849-1)



I：输入设备

L：逻辑

O：输出设备

im：互连方式

SRP/CS 是接线类别 1 的控制系统的安全相关部分，必须使用经过**良好验证的组件**设计和构造。

安全相关应用的“经过良好验证的组件”是以下任一组件：

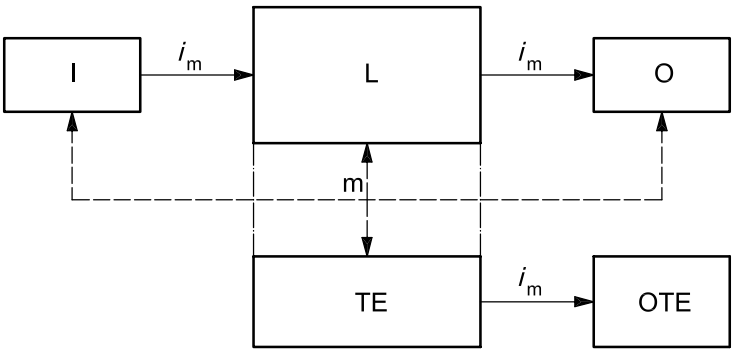
- 过去广泛使用，并在类似应用中获得成功结果，或
- 使用证明其安全相关应用的适用性和可靠性的原则制造和验证。

类别 1 系统中**没有诊断覆盖**（DC_{avg} = 无）。

接线类别 2 的架构要求

类别 2 的指定架构在 EN ISO 13849-1, 6.2.5 中定义。

图 38 - 类别 2 指定架构 (EN ISO 13849-1)



I：输入设备

L：逻辑

O：输出设备

im：互连方式

m：监测

TE：测试设备

OTE：测试设备输出

必须正确设计接线类别 2 控制系统的安全相关部分 SRP/CS，以便机器控制系统以适当的间隔检查其功能。

在单通道架构中，SIM 与 SIL[53] 起动器相关联。

具体而言，对于接线类别 2，镜像接触器连接到 Prevent™ XPS 模块（或等效模块）。如果镜像接触器反馈线的状态不等于 Preventa XPS 模块（或等效模块）的输出状态，则 Preventa XPS 模块（或等效模块）会阻止第二次起动。

注: 镜像接触器反馈仅传递诊断信息。

53. 根据标准 IEC 61508 确定的安全完整性等级。

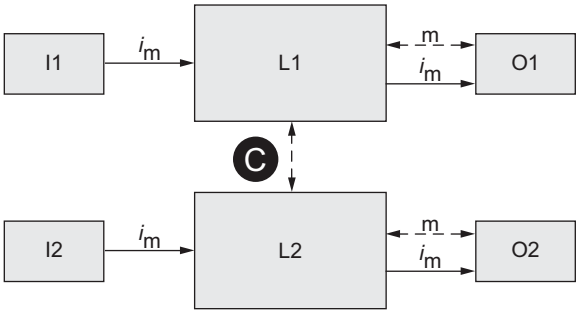
附录：双通道架构

这种双通道架构包含接线类别 3 和 4。

接线类别 3 的架构要求

类别 3 的指定架构在 EN ISO 13849–1, 6.2.6 中定义。

图 39 - 类别 3 指定架构 (EN ISO 13849-1)



im：互连方式

c：交叉监测

I1、**I2**：输入设备，例如传感器

L1、**L2**：逻辑

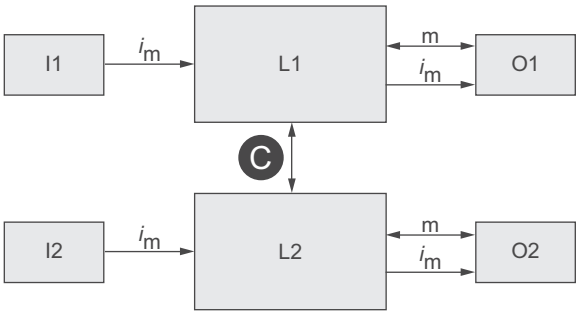
m：监测

O1、**O2**：输出设备，例如主接触器

接线类别 4 的架构要求

类别 4 的指定架构在 EN ISO 13849–1, 6.2.7 中定义。

图 40 - 类别 4 指定架构 (EN ISO 13849-1)



im：互连方式

c：交叉监测

I1、**I2**：输入设备，例如传感器

L1、**L2**：逻辑

m：监测

O1、**O2**：输出设备，例如主接触器

用于监测的实线表示诊断覆盖高于类别 3 的指定架构。

术语

A

危险故障的平均频率 [h^{-1}] (PFH)。（危险故障如 IEC 61508-4 中所定义）

为了保证安全功能，IEC 61508 标准要求采用各种级别的措施来避免和控制检测到的错误，具体取决于所需的 SIL[54]。

必须对安全功能的所有组件进行概率评估，以评估为控制检测到的故障而实施的措施的有效性。

该评估确定了安全相关系统的 PFH（危险故障的平均频率[55] [h^{-1}]）。这是安全相关系统以危险方式发生故障并且无法正确执行安全功能的每小时概率。

根据 SIL，PFH 不得超过整个安全相关系统的某些值。

添加了功能链的各个 PFH 值。结果不得超过标准中规定的最大值。

安全完整性等级	高需求或持续需求下危险故障的平均频率[55] [h^{-1}] (PFH)
4	$10^{-9} \leq — < 10^{-8}$
3	$10^{-8} \leq — < 10^{-7}$
2	$10^{-7} \leq — < 10^{-6}$
1	$10^{-6} \leq — < 10^{-5}$

E

EN ISO 13849 标准

本欧洲标准规定了控制系统安全相关部件的安全功能和类别的验证过程，包括危险分析、风险评估和测试。ISO 13849-1 中给出了安全功能的描述和类别的要求，其中包括一般设计原则。某些验证要求是通用的，某些要求特定于所使用的技术。EN ISO 13849-2 还规定了通过测试控制系统的安全相关部分进行验证的条件。

EN/IEC 60204-1 标准

停止类别 0 被定义为“通过立即切断机器执行器的电源而停止的功能（即非受控的停止）”。

停止类别 1 被定义为“受控停止，机器执行器可以使用电源来实现停止，然后在停止后断开电源”。

F

避免故障的措施

必须尽可能避免规格、硬件和软件中的系统错误，以及安全相关系统中的使用故障和维护故障。为了满足这些要求，IEC 61508 规定了许多必须根据所需 SIL[54] 实施的避免故障的措施。这些用于避免故障的措施必须涵盖安全相关系统的整个生命周期，即从设计到系统停止使用。

54. 根据标准 IEC 61508 确定的安全完整性等级。
55. 危险故障如 IEC 61508-4 中所定义

功能安全

自动化和功能安全工程在过去是完全独立的两个领域，但最近变得更加集成。

集成的安全功能简化了复杂自动化解决方案的工程和安装。

通常，功能安全工程要求取决于应用。

需求水平源于特定应用产生的风险和潜在危险。

H

硬件容错 (HFT) 和安全故障分数 (SFF)

根据安全相关系统的 SIL[56]，IEC 61508 标准要求特定硬件容错 (HFT) 与特定比例的安全故障相关，由安全故障分数 (SFF) 表示。

HFT 是系统执行所需安全功能的能力，不管存在一个还是多个硬件故障。

系统的 SFF 定义为安全故障率与系统总故障率之比。

根据 IEC 61508 标准，系统可达到的最大 SIL 部分取决于系统的 HFT 和 SFF。

这些类型是根据标准指定的，这些标准适用于安全相关元件。

SFF	**HFT A 类子系统**			**HFT B 类子系统**		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	—	SIL 1	SIL 2
60% – < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% – < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

I

IEC 61508 标准

标准 IEC 61508 涵盖电气/电子/可编程电子安全相关系统的功能安全性。

整个功能链（例如，从传感器通过逻辑处理单元到致动器）被视为一个单元，而不是单个组件。

该功能链必须满足特定安全完整性等级的要求。

L

低/高需求模式

IEC 61508 定义了安全功能需求操作模式：

- 高需求或连续模式 (PFH)
- 低需求模式（PFDavg，PTI）

M

56. 根据标准 IEC 61508 确定的安全完整性等级。

平均危险失效时间 ($MTTF_d$)

标准 ISO 13849-1 将 $MTTF_d$ 定义为预期的平均危险失效时间。

P

性能等级 (PL)

标准 IEC 13849-1 定义了安全功能的五个性能等级 (PL)。

等级 a 是最低等级，e 是最高等级。

五个等级（a、b、c、d 和 e）对应于每小时危险故障[57]的平均概率的不同值。

性能等级	**每小时危险故障的概率[57]**
e	≥ 10^{-8} 至 < 10^{-7}
d	≥ 10^{-7} 至 < 10^{-6}
c	≥ 10^{-6} 至 < 3 x 10^{-6}
b	≥ 3 x 10^{-6} 至 < 10^{-5}
a	≥ 10^{-5} 至 < 10^{-4}

S

安全完整性等级 (SIL)

标准 IEC 61508 为安全功能定义了四个安全完整性等级 (SIL)。

SIL 1 是最低的完整性等级，SIL 4 是最高等级。

危害分析和风险评估是确定所需安全完整性等级的基础。

这用于决定相关功能链是否被视为安全功能，以及它必须涵盖哪种潜在危险。

57. 危险故障如 IEC 61508-4 中所定义

Schneider Electric
800 Federal Street
01810 Andover, MA
美国

https://www.schneider-electric.com/en/work/support/

www.schneider-electric.com

由于各种标准、规范和设计不时变更，请索取对本出版物中给出的信息的确认。

8536IB1904ZH-04