

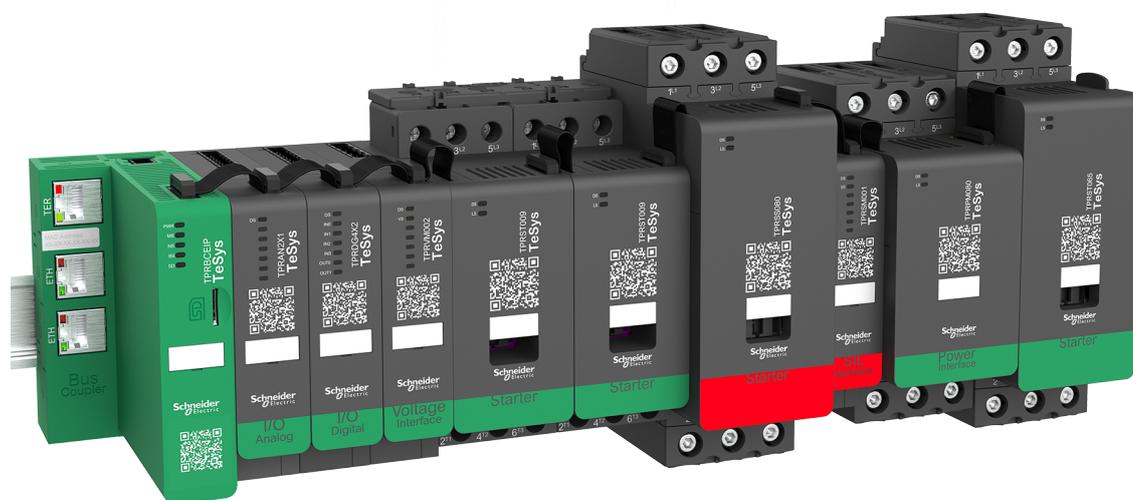
TeSys Active

TeSys™ island – Solución de gestión de motores digital

Guía de seguridad funcional

TeSys ofrece soluciones innovadoras y conectadas para arrancadores de motor.

85361B1904ES-04
08/2023



Información legal

La información proporcionada en este documento contiene descripciones generales, características técnicas o recomendaciones relacionadas con productos o soluciones.

Este documento no pretende sustituir a un estudio detallado o un plan de desarrollo o esquemático específico de operaciones o sitios. No debe usarse para determinar la adecuación o la fiabilidad de los productos o las soluciones para aplicaciones de usuario específicas. Es responsabilidad del usuario realizar o solicitar a un experto profesional (integrador, especificador, etc.) que realice análisis de riesgos, evaluación y pruebas adecuados y completos de los productos o las soluciones con respecto a la aplicación o el uso específicos de dichos productos o dichas soluciones.

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en este documento son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios.

Este documento y su contenido están protegidos por las leyes de copyright aplicables, y se proporcionan exclusivamente a título informativo. Ninguna parte de este documento puede ser reproducida o transmitida de cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otro), para ningún propósito, sin el permiso previo por escrito de Schneider Electric.

Schneider Electric no otorga ningún derecho o licencia para el uso comercial del documento o su contenido, excepto por una licencia no exclusiva y personal para consultarla "tal cual".

Schneider Electric se reserva el derecho de realizar cambios o actualizaciones con respecto a o en el contenido de este documento o con respecto a o en el formato de dicho documento en cualquier momento sin previo aviso.

En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este documento o por el uso no previsto o el mal uso del contenido de dicho documento.

Schneider Electric, Preventa y TeSys son marcas comerciales propiedad de Schneider Electric SE y sus filiales y empresas asociadas. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios.

Tabla de contenido

Información de seguridad	5
Acerca del manual	6
Alcance del documento	6
Campo de aplicación	6
Documentación relacionada	7
Terminología derivada de la normativa	8
Terminología de seguridad funcional	9
Declaración de conformidad CE	10
Precauciones	11
Personal cualificado	12
Uso previsto	12
Descripción general de seguridad funcional de TeSys™	
island	13
Rango maestro: TeSys	13
Concepto de TeSys island	13
Seguridad funcional en TeSys island	14
Características de seguridad funcional de TeSys island	15
Normas y características con certificación	15
Condiciones de funcionamiento	16
Arquitectura de canal único (ISO 13849)	16
Arquitectura de doble canal (ISO 13849)	16
Categorías de parada (EN/IEC 60204-1)	17
Categoría de cableado ¹	17
Categoría de cableado 1	17
Categoría de cableado 2	17
Categoría de cableado 3	18
Categoría de cableado 4	19
Ensayo de aceptación	19
Conceptos y componentes	20
Estructura típica de TeSys™ island	20
Grupo SIL	21
Avatares SIL	21
Módulo de interfaz SIL	22
Estado del contacto de los arrancadores SIL	22
Elemento sensor relacionado con la seguridad	24
Arrancadores SIL	25
Elemento externo relacionado con la seguridad	26
Parada SIL, Categoría de parada 0, Arquitectura categoría de cableado 1	27
Parada SIL, Categoría de parada 0, Arquitectura categoría de cableado 2	27
Parada SIL, Categoría de parada 1, Arquitectura categoría de cableado 2	31
Parada SIL, Categoría de parada 0, Arquitectura categoría de cableado 3/4	35
Parada SIL, Categoría de parada 1, Arquitectura categoría de cableado 3/4	37

Aislamiento de cable protegido	40
Arquitectura de conmutación de baja/alta frecuencia	41
Frecuencia de conmutación baja (< 15 ciclos por hora)	42
Frecuencia de conmutación alta (\geq 15 ciclos por hora)	43
Arquitecturas de muestra	46
Parada SIL, Categoría de parada 0, Categoría de cableado 1	47
Parada SIL, Categoría de parada 0, Categoría de cableado 2	48
Parada SIL, Categoría de parada 1, Categoría de cableado 2	50
Parada SIL, Categoría de parada 0, Categoría de cableado 3/4	52
Parada SIL, Categoría de parada 1, Categoría de cableado 3/4	54
Datos técnicos	56
Módulo de interfaz SIL	56
Arrancador SIL	56
Datos de fiabilidad	58
Cableado de avatares SIL	59
Puesta en marcha de la función de seguridad	66
Pruebas de instalación	66
Comprobación de la función de seguridad	66
Requisitos de mantenimiento de la función de seguridad	68
Programa de mantenimiento	68
Comprobaciones de mantenimiento	68
Comprobaciones de uso de un dispositivo	68
Comprobación de la función de seguridad	68
Apéndice: Arquitectura de canal único	69
Requisitos de la arquitectura para la Categoría de cableado 1	69
Requisitos de la arquitectura para la Categoría de cableado 2	70
Apéndice: Arquitectura de doble canal	71
Requisitos de la arquitectura para la Categoría de cableado 3	71
Requisitos de la arquitectura para la Categoría de cableado 4	71
Glosario	73

Información de seguridad

Información importante

Lea atentamente estas instrucciones y observe el equipo para familiarizarse con el dispositivo antes de instalarlo, utilizarlo, revisarlo o realizar su mantenimiento. Los mensajes especiales que se ofrecen a continuación pueden aparecer a lo largo de la documentación o en el equipo para advertir de peligros potenciales, o para ofrecer información que aclara o simplifica los distintos procedimientos.



La adición de uno de estos dos símbolos a una etiqueta de seguridad del tipo "Peligro" o "Advertencia" indica que existe un peligro eléctrico que causará lesiones si no se siguen las instrucciones.



Este es el símbolo de alerta de seguridad. Sirve para alertar de riesgos potenciales de lesiones. Siga las recomendaciones de todos los mensajes de seguridad precedidos por este símbolo para evitar lesiones potenciales e incluso la muerte.

⚠ PELIGRO
PELIGRO indica una situación de riesgo que, si no se evita, ocasionará la muerte o lesiones graves.
⚠ ADVERTENCIA
ADVERTENCIA indica una situación de riesgo que, si no se evita, puede ocasionar la muerte o lesiones graves.
⚠ PRECAUCIÓN
PRECAUCIÓN indica una situación de riesgo que, si no se evita, puede ocasionar lesiones moderadas o leves.
AVISO
AVISO sirve para indicar prácticas no relacionadas con lesiones físicas.

Tenga en cuenta

La instalación, el manejo y el mantenimiento de los equipos eléctricos deberán ser realizados solo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Un personal cualificado es aquel que posee habilidades y conocimientos relacionados con la construcción y el funcionamiento de los equipos eléctricos y su instalación, y que ha recibido formación en materia de seguridad para reconocer y evitar los peligros que conllevan.

Acerca del manual

Alcance del documento

Utilice este documento para obtener más información sobre las siguientes características de seguridad funcional de TeSys™ island:

- conocimientos generales
- aspectos clave a tener en cuenta
- rendimientos
- descripción del hardware
- configuraciones típicas
- arquitecturas de muestra
- referencias a la normativa

Campo de aplicación

Esta guía es válida para todas las configuraciones de TeSys island. La disponibilidad de algunas de las funciones descritas en esta guía depende del protocolo de comunicación utilizado y los módulos físicos instalados en la TeSys island.

Para obtener información sobre la conformidad de los productos con las directivas medioambientales como RoHS, REACH, PEP y EOL, visite www.se.com/green-premium.

Para conocer las características técnicas de los módulos físicos descritos en esta guía, visite www.se.com.

Las características técnicas que se describen en esta guía deben ser las mismas que las que aparecen en línea. Es posible que el contenido se revise con el tiempo a fin de mejorar su claridad y exactitud. Si observa una diferencia entre la información de esta guía y la información en línea, tenga en cuenta esta última.

Documentación relacionada

Título del documento	Descripción	Número del documento
TeSys island - Guía de sistema, instalación y funcionamiento de	La guía describe las funciones principales, la instalación mecánica, el cableado, la puesta en marcha, así como el funcionamiento y mantenimiento de TeSys island.	DOCA0270ES
TeSys island - EtherNet/IP™ - Guía de inicio rápido y biblioteca de bloques funcionales	Describe cómo integrar la TeSys island y la información de la TeSys island biblioteca utilizada en el entorno EtherNet/IP de Rockwell Software® Studio 5000®.	DOCA0271ES
TeSys island – Guía de seguridad de funcionamiento	Describe las características de seguridad de funcionamiento de TeSys island.	8536IB1904ES
TeSys island – Guía de bloques funcionales de terceros	Contiene la información necesaria para crear bloques funcionales para hardware de terceros.	8536IB1905ES
TeSys island - Guía de ayuda en línea de DTM	Describe cómo instalar y utilizar diversas funciones de software de configuración de TeSys island y cómo configurar los parámetros de TeSys island.	8536IB1907ES
TeSys island - Perfil ambiental del producto	Describe los materiales constituyentes, el potencial de reciclado y la información sobre el impacto ambiental de TeSys island.	ENVPEP1904009
TeSys island - Instrucciones para el final de la vida útil del producto	Contiene instrucciones para el final de la vida útil de TeSys island.	ENVEOLI1904009
TeSys island - Hoja de instrucciones, Acoplador de bus, TPRBCEIP	Describe cómo instalar el acoplador de bus Ethernet/IP de TeSys island.	MFR44097
TeSys island - Hoja de instrucciones, Acoplador de bus, TPRBCPFN	Describe cómo instalar el TeSys island Acoplador de bus PROFINET.	MFR44098
TeSys island - Hoja de instrucciones, acoplador de bus, TPRBCPFB	Describe cómo instalar el acoplador de bus PROFIBUS DP de TeSys island.	GDE55148
TeSys island - Hoja de instrucciones, arrancadores y módulos de interfaz de alimentación, tamaño 1 y 2	Describe cómo instalar los arrancadores y módulos de interfaz de alimentación de tamaño 1 y 2 de TeSys island.	MFR77070
TeSys island - Hoja de instrucciones, arrancadores y módulos de interfaz de alimentación, tamaño 3	Describe cómo instalar los arrancadores y módulos de interfaz de alimentación de tamaño 3 de TeSys island.	MFR77085
TeSys island - Hoja de instrucciones: Módulos de entrada/salida	Describe cómo instalar los módulos de E/S analógicas y digitales de TeSys island.	MFR44099
TeSys island - Hoja de instrucciones: Módulos de interfaz de tensión y de interfaz SIL	Describe cómo instalar los módulos de interfaz de tensión y SIL de TeSys island ¹ .	MFR44100

1. Nivel de integridad de seguridad según la norma IEC 61508.

Terminología derivada de la normativa

Los términos técnicos, la terminología y las descripciones correspondientes de esta guía normalmente utilizan los términos o las definiciones de las normas correspondientes. Entre otras, estas normas incluyen:

- **EN ISO 13849-1:** Seguridad de las máquinas – Piezas de sistemas de control relacionadas con la seguridad – Parte 1: Principios generales para el diseño
- **EN ISO 13849-2:** Seguridad de las máquinas – Piezas de sistemas de control relacionadas con la seguridad – Parte 2: Validación
- **IEC 61508:** Seguridad funcional de los sistemas relacionados con la seguridad eléctricos / electrónicos / electrónicos programables
- **EN 62061:** Seguridad de las máquinas – Seguridad funcional de los sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad
- **IEC 61511:** Seguridad funcional – Sistemas de seguridad instrumentados para el sector de la industria de procesos
- **EN/IEC 60204-1:** Seguridad de las máquinas – Equipos eléctricos de las máquinas – Parte 1: Requisitos generales
- **IEC 61000-6-7:** Compatibilidad electromagnética (CEM) – Parte 6-7: Normas genéricas – Requisitos de inmunidad para equipos concebidos para realizar funciones en un sistema relacionado con la seguridad (seguridad funcional) en ubicaciones industriales
- **IEC 60664-5:** Coordinación del aislamiento para equipos dentro de sistemas de baja tensión – Parte 5: Método exhaustivo para calcular los espacios y las distancias de fuga iguales o inferiores a 2 mm
- **IEC 60947-4-1:** Aparata de baja tensión – Parte 4-1: Contactores y arrancadores de motor – Contactores y arrancadores electromecánicos
- **IEC 60947-5-1:** Aparata de baja tensión – Parte 5-1: Aparatos y elementos de conmutación para circuitos de mando – Aparatos electromecánicos para circuitos de mando
- **IEC 60947-7-1:** Aparata de baja tensión – Parte 7-1: Equipamiento auxiliar – Bloques de conexión para conductores de cobre
- **IEC 60947-7-2:** Aparata de baja tensión – Parte 7-2: Equipamiento auxiliar – Bloques de conexión de conductores de protección para conductores de cobre
- **EN 50205:** Relés con contactos de guía forzada (enlazados mecánicamente)
- **IEC TR 62380:** Manual de datos de fiabilidad – Modelo universal para la predicción de la fiabilidad de los componentes electrónicos, tarjetas de circuito impreso y equipos

Terminología de seguridad funcional

ATTENTION

A continuación se define la terminología de seguridad funcional utilizada en esta guía.

Término	Estándar	Definición
Tolerancia a fallos	IEC 61511-1	Capacidad de un elemento funcional de seguir ejecutando una función requerida en presencia de fallos o errores
Seguridad funcional	IEC 61508-4	Parte de la seguridad general en relación con el equipo bajo control (EUC) y el sistema de control del EUC que depende del funcionamiento correcto de los sistemas eléctrico/electrónico/electrónico programable (E/E/PE) relacionados con la seguridad y otras medidas de reducción de riesgos
Fallo seguro	IEC 61508-4	El fallo de un elemento, subsistema y/o sistema que interviene en la implementación de la función de seguridad que: <ol style="list-style-type: none"> da lugar al accionamiento espurio de la función de seguridad encargada de establecer el EUC² (o una parte del mismo) en un estado seguro o mantenerlo en dicho estado; o aumenta la probabilidad de que se produzca un accionamiento espurio de la función de seguridad encargada de establecer el EUC² (o una parte del mismo) en un estado seguro o mantenerlo en dicho estado.
Fracción de fallo seguro	IEC 61508-4	La relación del índice de fallos seguros con el índice total de fallos del sistema.
Estado seguro	IEC 61511-1	Estado del proceso en el que se alcanza la seguridad
	IEC 61800-5-2	Estado de los PDS(SR) ³ una vez alcanzada la seguridad
Parada de emergencia	IEC 61800-5-2	Las funciones de parada de emergencia se definen como sigue: <ul style="list-style-type: none"> • Desconexión segura de par (STO) <ul style="list-style-type: none"> ◦ Esta función impide que se suministre potencia de producción de fuerza al motor. ◦ Esta <i>subfunción de seguridad</i> corresponde a una parada no controlada de conformidad con la categoría de parada 0 de IEC 60204-1. • Parada de emergencia 1 (SS1) <ul style="list-style-type: none"> ◦ Parada de emergencia 1 con deceleración controlada: SS1-d inicia y controla el índice de deceleración del motor dentro de límites seleccionados para parar el motor y ejecuta la función STO (véase 4.2.3.2) cuando la velocidad del motor es inferior a un límite especificado; o ◦ Parada de emergencia 1 con rampa supervisada: SS1-r inicia y supervisa el índice de deceleración del motor dentro de límites seleccionados para parar el motor y ejecuta la función STO cuando la velocidad del motor es inferior a un límite especificado; o ◦ La parada de emergencia 1 con control de tiempo SS1-t inicia la deceleración del motor y ejecuta la función STO tras un retardo de tiempo específico de la aplicación.
Función de seguridad	IEC 61800-5-2	Función que debe implementarse a través de un sistema relacionado con la seguridad u otras medidas de reducción de riesgos, y que tiene como propósito alcanzar o mantener un estado seguro para los equipos o la maquinaria accionados por los PDS(SR) ³ , en relación con un evento peligroso específico

2. EUC: equipo bajo control

3. Sistemas de control de potencia relacionados con la seguridad

Término	Estándar	Definición
Nivel de integridad de seguridad (SIL)	IEC 61508	La norma IEC 61508 define cuatro niveles de integridad de seguridad (SIL) para las funciones de seguridad. SIL 1 es el nivel de integridad más bajo y SIL 4 el más alto. Un análisis de peligros y una evaluación de riesgos sirven como base para determinar el nivel de integridad de seguridad requerido.
Sistema relacionado con la seguridad	IEC 61800-5-2	Sistema designado que <ul style="list-style-type: none"> • implementa las funciones de seguridad requeridas para alcanzar o mantener un estado seguro para los equipos o la maquinaria accionados por los PDS(SR)⁴; y • tiene como propósito alcanzar, por sí solo o junto con otras medidas de reducción de riesgos, la integridad de seguridad necesaria para las funciones de seguridad requeridas
Subsistema	IEC 61800-5-2	Parte del diseño arquitectónico de nivel superior de un sistema relacionado con la seguridad, cuyo fallo da lugar a un fallo de una función relacionada con la seguridad

Declaración de conformidad CE

Las Declaraciones de conformidad CE para la TeSys™ se pueden consultar en www.schneider-electric.com.

Precauciones

Lea y entienda las siguientes precauciones antes de llevar a cabo cualquiera de los procedimientos indicados en este manual.

PELIGRO

RIESGO DE DESCARGA ELÉCTRICA, EXPLOSIÓN O ARCO ELÉCTRICO

- Solo personal electricista cualificado deberá instalar y reparar este equipo.
- Apague todas las fuentes de alimentación del equipo antes de iniciar el trabajo, ya sea dentro o fuera de este equipo.
- Use únicamente la tensión indicada al usar el equipo y cualquier otro producto asociado.
- Utilice siempre un voltímetro de rango adecuado para confirmar que el equipo esté apagado por completo.
- Utilice enclavamientos adecuados cuando existan peligros para el personal y/o los equipos.
- Los circuitos eléctricos deben cablearse y protegerse conforme a los requisitos normativos locales y nacionales.
- Utilice equipos de protección individual (EPI) adecuados y siga las prácticas seguras para trabajos eléctricos contempladas en las normas NFPA 70E, NOM-029-STPS o CSA Z462 o sus equivalentes en la normativa local.

Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.

ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

- Para obtener instrucciones completas en relación con la seguridad funcional, consulte la Guía de seguridad funcional de TeSys™ island, 8536IB1904.
- No desmonte, repare ni modifique el equipo. Este no contiene piezas que el usuario pueda reparar.
- Instale y utilice este equipo dentro de un alojamiento adecuado cuyas características nominales se ajusten a las del entorno de aplicación previsto.
- Cada implantación de este equipo deberá comprobarse de forma individual y exhaustiva para garantizar su correcto funcionamiento antes de ponerse en marcha.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.



ADVERTENCIA: Este producto puede exponerle a sustancias químicas, incluido óxido de antimonio (trióxido de antimonio), el cual es cancerígeno según la normativa del Estado de California. Para obtener más información al respecto, visite www.P65Warnings.ca.gov.

Personal cualificado

Solo podrán trabajar en este producto o con él el personal debidamente formado que entienda y conozca los contenidos de esta guía y cualquier otra documentación de producto relacionada.

El personal cualificado deberá ser capaz de detectar posibles peligros que puedan presentarse como consecuencia de la modificación de los valores de los parámetros y, en general, del trabajo en equipos mecánicos, eléctricos o electrónicos. El personal cualificado deberá conocer las normas, las disposiciones y los reglamentos relativos a la prevención de accidentes industriales, los cuales deberá observar a la hora de diseñar e implantar el sistema.

El uso y la aplicación de la información contenida en esta guía requiere de conocimientos especializados en el diseño y la programación de sistemas de control automatizadas. Solamente el usuario, el fabricante de la máquina o el integrador saben cuáles son las condiciones y los factores presentes durante la instalación, la configuración, el funcionamiento y el mantenimiento de la máquina o el proceso, por lo que pueden determinar la automatización y el equipo asociado, así como las medidas de seguridad y los enclavamientos relacionados que se pueden utilizar de forma eficaz y correcta.

Al seleccionar el equipo de control y automatización (y cualquier otro equipo o software relacionado) para una determinada aplicación, también debe tener en cuenta las normativas o estándares locales, regionales o nacionales.

Preste especial atención al cumplimiento de la información de seguridad, los requisitos eléctricos y las normas que se apliquen a su máquina o proceso en el uso de este equipo.

Uso previsto

Los productos descritos en esta guía –junto con el software, los accesorios y las opciones– son arrancadores de cargas eléctricas de baja tensión destinados a utilizarse en entornos industriales de acuerdo con las instrucciones, direcciones, ejemplos e información de seguridad contenida en este documento y otros documentos de apoyo.

El producto únicamente puede utilizarse cumpliendo todos los reglamentos y las directivas de seguridad aplicables, los requisitos específicos y los datos técnicos.

Antes de utilizar el producto, deberá llevar a cabo un análisis de peligros y una evaluación de riesgos de la aplicación planificada. A partir de los resultados, deberán aplicarse medidas de seguridad adecuadas.

Puesto que el producto se utiliza como componente en una máquina o proceso, deberá garantizar la seguridad de las personas en virtud del diseño general del sistema.

Utilice el producto solo con los cables y accesorios especificados. Utilice únicamente accesorios y repuestos genuinos.

Queda terminantemente prohibido cualquier uso distinto de los usos explícitamente permitidos, ya que podrían dar lugar a peligros imprevistos.

Descripción general de seguridad funcional de TeSys™ island

Rango maestro: TeSys

TeSys™ es una innovadora solución de gestión y control de motores de un líder del mercado global. TeSys ofrece productos y soluciones eficientes y conectadas para la conmutación y protección de motores y cargas eléctricas cumpliendo todas las principales normas eléctricas internacionales.

Concepto de TeSys island

TeSys island es un sistema modular y multifuncional que proporciona funciones integradas dentro de una arquitectura de automatización, principalmente para el control directo y la gestión de cargas de baja tensión. TeSys island puede conmutar, ayudar a proteger y administrar motores y otras cargas eléctricas de hasta 80 A (AC1) instaladas en un cuadro de control eléctrico.

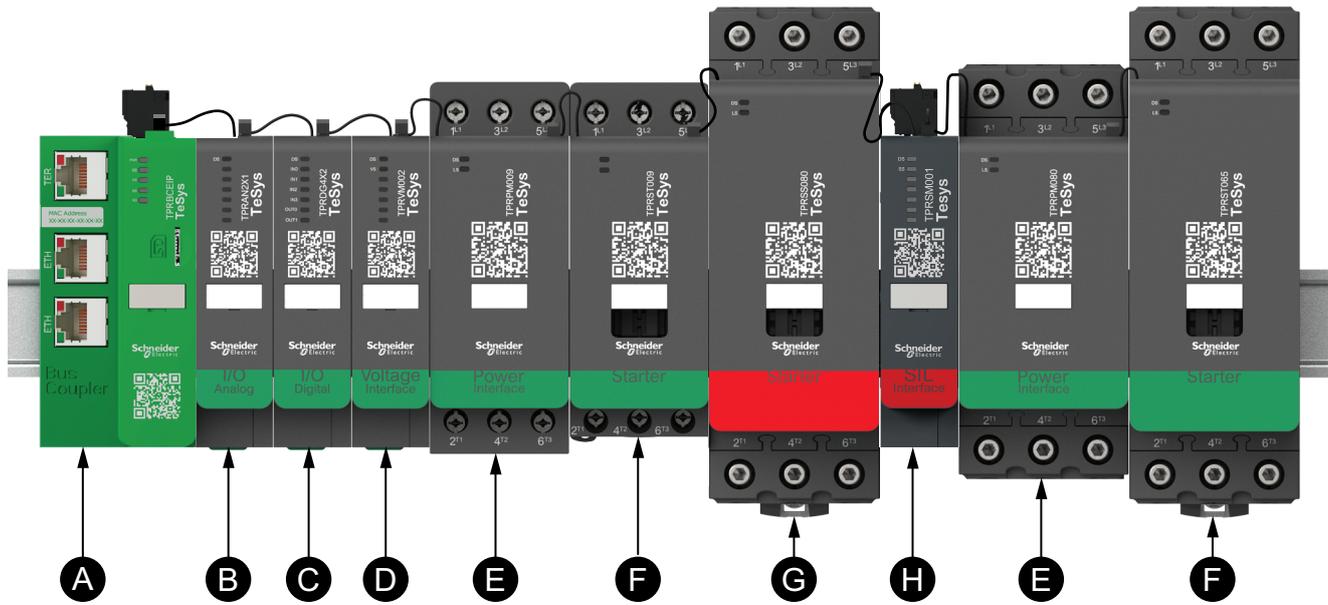
Este sistema se ha diseñado en torno al concepto de TeSys avatars. Estos avatars:

- Representan los aspectos tanto lógicos como físicos de las funciones de automatización
- Determinar la configuración de la TeSys island

Los aspectos lógicos de la TeSys island se gestionan mediante herramientas de software que cubren todas las fases del ciclo de vida de producto y aplicación: diseño, ingeniería, puesta en marcha, operación y mantenimiento. diseño, ingeniería, puesta en marcha, funcionamiento y mantenimiento.

La TeSys island física consta de un conjunto de dispositivos instalados en un solo carril DIN y conectados junto con cables planos que proporcionan la comunicación interna entre módulos. La comunicación externa con el entorno de automatización se realiza a través de un único módulo acoplador de bus, y la TeSys island aparece en la red como un único nodo. El resto de módulos incluyen arrancadores, módulos de interfaz de alimentación, módulos de E/S analógicas y digitales, módulos de interfaz de tensión y módulos de interfaz SIL (nivel de integridad de seguridad según la norma IEC 61508), que cubren una amplia gama de funciones operativas.

Figura 1 - Descripción general de TeSys island



A	Acoplador de bus	E	Módulo de interfaz de alimentación
B	Módulo de E/S analógicas	F	Arrancador estándar
C	Módulo de E/S digitales	G	Arrancador SIL
D	Módulo de interfaz de tensión	H	Módulo de interfaz SIL

Seguridad funcional en TeSys island

TeSys™ island ofrece avatares y dispositivos físicos para la configuración de funciones de Categoría de parada 0 y Categoría de parada 1 de acuerdo con la norma EN/IEC 60204-1. Los avatares de TeSys son representaciones digitales de los módulos físicos de la isla, si bien la función de seguridad de TeSys island se basa únicamente en los componentes de hardware electromecánicos. Los dispositivos específicos son el arrancador SIL⁵ y el módulo de interfaz SIL. Otro concepto importante es el grupo SIL: un conjunto de avatares asociados a un módulo de interfaz SIL y que siguen la misma función de seguridad. Puede haber varios grupos SIL dentro de una isla.

TeSys island debe integrarse con otros elementos relacionados con la seguridad en un sistema relacionado con la seguridad más amplio para ayudar a garantizar la seguridad funcional de una máquina o un sistema/proceso.

5. Nivel de integridad de la seguridad según la norma IEC 61508.

Características de seguridad funcional de TeSys island

TeSys™ island ofrece características de seguridad funcional conforme a las siguientes condiciones específicas:

- Normas y características con certificación, página 15
- Condiciones de funcionamiento, página 16
- Arquitectura de canal único (ISO 13849), página 16
- Arquitectura de doble canal (ISO 13849), página 16
- Categorías de parada (EN/IEC 60204-1), página 17
- Categorías de cableado (ISO 13849), página 17
- Ensayo de aceptación, página 19

Normas y características con certificación

TeSys island cumple las siguientes directivas y normas:

- Directiva sobre máquinas 2006/42/CE:
 - EN ISO 13849-1: 2015
 - EN 62061: 2016 o IEC 62061: 2015 (ed. 1.2)
- Seguridad funcional de los sistemas relacionados con la seguridad eléctricos / electrónicos / electrónicos programables: IEC 61508 ed. 2: 2010
- Seguridad funcional – Sistemas de seguridad instrumentados para el sector de la industria de procesos: IEC 61511 ed. 2: 2016
- Las funciones de Categoría de parada 0 y Categoría de parada 1 de TeSys island cumplen la norma EN/IEC 60204-1.

En canal único, los rendimientos más altos para esas funciones son:

- Nivel de rendimiento “d” Categoría 2 de conformidad con EN ISO 13849-1
- SIL⁶ Capacidad 2 de conformidad con las normas IEC 61508 Ed 2 e IEC 61511 Ed 2
- Capacidad SIL CL 2 de conformidad con EN 62061 Ed 1

En doble canal, los rendimientos más altos para esas funciones son:

- Nivel de rendimiento “e” Categoría 4 de conformidad con EN ISO 13849-1
- Capacidad SIL 3 de conformidad con IEC 61508 Ed 2 e IEC 61511 Ed 2
- Capacidad SIL CL 3 de conformidad con EN 62061: 2016 o IEC 62061: 2015 (ed. 1.2)

TeSys island está diseñada para admitir distintos niveles de rendimiento de seguridad funcional y niveles de integridad de la seguridad dependiendo de su arquitectura de cableado, y es conforme a las características de seguridad funcional descritas en la siguiente tabla.

Tabla 1 - Características de seguridad funcional

Función	Función de parada relacionada con la seguridad	
Posición de repliegue	Contactor abierto	
Tiempo de respuesta (peor caso)	145 ms	
Categoría de parada según la norma EN/IEC 60204-1	Cat. 0 / Cat. 1	
Directiva sobre máquinas	Sí	
Arquitectura del sistema de TeSys island	Canal único	Doble canal

6. Nivel de integridad de la seguridad según la norma IEC 61508.

Tabla 1 - Características de seguridad funcional (Continuación)

Nivel de rendimiento EN ISO 13849-1	PL c, d	PL c, d, e
Categoría de cableado según la norma ISO 13849-1	Cat. 1, 2	Cat. 3, 4
SIL CL EN 62061	SIL CL 2	SIL CL 3
SIL IEC 61508 / IEC 61511	SIL 2	SIL 3

El certificado de seguridad funcional puede consultarse en www.se.com/tesys/.

NOTA: Para la certificación relacionada con aspectos funcionales, solo se tendrá en cuenta una TeSys island adecuada para el uso en aplicaciones relacionadas con la seguridad, no el sistema completo en el que se integra para ayudar a garantizar la seguridad funcional de una máquina o un sistema/proceso.

Condiciones de funcionamiento

TeSys island ha sido diseñada para soportar de forma duradera las siguientes condiciones. Otras condiciones podrían ser aplicables a los módulos específicos, tal y como se describe en sus correspondientes fichas de datos, disponibles en www.se.com/tesys-island.

- Temperatura ambiente de 40 °C
- motor de 400 o 480 V
- Humedad del 50 %
- Carga del 80 %
- Orientación de montaje horizontal
- Todas las entradas activadas
- Todas las salidas activadas
- En funcionamiento las 24 horas/día, los 365 días del año

Arquitectura de canal único (ISO 13849)

TeSys island es aplicable a las arquitecturas de canal único en las que un fallo detectado puede dar lugar a la pérdida de la función de seguridad.

Arquitectura de doble canal (ISO 13849)

TeSys island es aplicable a las arquitecturas de doble canal en las que un fallo único detectado (incluidos los fallos de modo común) no da lugar a la pérdida de la función de seguridad.

Categorías de parada (EN/IEC 60204-1)

La categoría de parada hace referencia a la forma en la que se desconecta la carga impulsada y depende del subsistema externo relacionado con la seguridad que activa la función de parada. Es posible implementar un subsistema externo relacionado con la seguridad con dispositivos como el módulo Preventa™ XPS.

Categoría de parada 0

La Categoría de parada 0 se define como la detención del movimiento de la máquina mediante la eliminación inmediata de la alimentación eléctrica de los actuadores de la máquina. La Categoría de parada 0 es una parada no controlada.

Categoría de parada 1

La Categoría de parada 1 se define como la detención del movimiento de la máquina con la alimentación eléctrica mantenida en los actuadores de la máquina durante el proceso de parada. La alimentación se desconecta una vez completada la parada. La Categoría de parada 1 es una parada controlada.

Categoría de cableado⁷

Las categorías de cableado hacen referencia a la forma en que se cablea el módulo externo Preventa™ XPS (o equivalente), y al nivel de seguridad adicional correspondiente de la función de seguridad.

Categoría de cableado 1

Un fallo único detectado puede provocar la pérdida de la función de seguridad y no se requiere cobertura de diagnóstico.

El elemento sensor relacionado con la seguridad puede cablearse directamente a las entradas SIL-IN/SIL Common.⁸ No se utilizan las entradas Mirror In/Mirror Out. Para obtener más información sobre el cableado de las entradas SIL-IN/SIL Common, consulte Elemento sensor relacionado con la seguridad, página 24.

Categoría de cableado 2

El elemento sensor relacionado con la seguridad se cablea a un módulo Preventa XPS (o equivalente). Las salidas del módulo Preventa XPS (o equivalente) se cablean a las entradas SIL-IN/SIL Common del módulo de interfaz SIL⁸.

Para cumplir con el requisito de la Categoría 2, la retroalimentación del contacto de espejo (Mirror In/Mirror Out) debe ser supervisada por un módulo Preventa XPS (o equivalente) que realice una supervisión de diagnóstico externa del contacto de espejo. Si el contacto espejo no se cierra en parada, se impide el siguiente reinicio a todos los arrancadores SIL del grupo SIL.

Implementación de la supervisión indirecta para la Categoría 2

Para alcanzar los requisitos de la categoría 2 para la cobertura de diagnóstico (DC > 60 %), se debe implementar una supervisión externa del estado del grupo para activar un mecanismo secundario para parar la máquina (disyuntor con dispositivo de disparo, etc.) o para evitar el acceso a áreas peligrosas (bloqueo de protección).

7. Categorías de cableado según la norma ISO 13849.

8. Nivel de integridad de la seguridad según la norma IEC 61508.

Cada grupo SIL⁹ lleva asociados cinco estados que indican el estado operativo. El estado 0 indica que no hay ningún grupo SIL presente en esta ranura. TeSys island admite hasta 10 grupos SIL en la isla.

Estado de los grupos SIL para la función de parada SIL:

- 0 = grupo SIL no presente en la configuración del sistema
- 1 = grupo SIL afectado por evento de dispositivo avatar
- 2 = comando de parada SIL recibido, arrancadores SIL no abiertos aún
- 3 = comando de parada de emergencia enviado correctamente, todos los arrancadores SIL están abiertos
- 4 = comando de parada enviado a un solo canal de entrada del módulo de interfaz SIL (SIM) (el puente o el cableado de entrada SIM están causando un problema), pero los arrancadores SIL se han abierto correctamente
- 5 = funcionamiento normal, los arrancadores SIL se pueden abrir o cerrar

El estado 5 es el estado de funcionamiento normal, y el estado 3 es el estado de parada SIL normal. El estado 1 indica que existe un problema de firmware o comunicación con un arrancador SIL. Los estados 2 y 4 indican que hay problemas relacionados con la parada SIL en el SIM, los arrancadores SIL o el cableado de parada SIL. La supervisión indirecta debe determinar si los estados 2 o 4 persisten durante un periodo superior al tiempo de actuación de una parada SIL y utilizar la información de estado para activar un mecanismo secundario para parar la máquina (disyuntor con dispositivo de disparo, etc.).

Para la lectura del estado de los grupos SIL, la supervisión externa debe utilizar el bloque funcional SystemDiagnostics. Cada grupo SIL del sistema tiene una salida en este bloque funcional para su estado de grupo SIL, etiquetado en el bloque funcional como "SILStarterStopMsgGrp *n*", donde *n* es el número del grupo SIL en la isla. El estado del grupo SIL presenta la enumeración mostrada arriba.

Supervisión de diagnóstico

Dado que la supervisión de diagnóstico se realiza inmediatamente a petición de la función de seguridad, el tiempo total para detectar el fallo y llevar la máquina a un estado no peligroso debe ser más corto que el tiempo para alcanzar el área peligrosa.

De acuerdo con ISO 13849-2, 9.2.3, para la Categoría 2: El $MTTF_d^{10}$ del equipo de supervisión debe ser superior a la mitad del $MTTF_d$ de la lógica. La contribución de TeSys island al $MTTF_d$ de la supervisión de diagnóstico es de $MTTF_d > 100$ años.

Categoría de cableado 3

Un fallo único no dará lugar a la pérdida de la función de seguridad y, siempre que sea posible, el fallo único se detectará en o antes de la siguiente demanda de la función de seguridad.

Para cumplir con el requisito de la Categoría 3, la retroalimentación del contacto de espejo (Mirror In/Mirror Out) debe ser supervisada por un módulo Preventa XPS (o equivalente) que realice una supervisión de diagnóstico externa del contacto de espejo del arrancador SIL⁹. Si el contacto espejo no se abre en parada, se impide el siguiente reinicio a todos los arrancadores SIL del grupo SIL. El elemento sensor relacionado con la seguridad se cablea a un módulo Preventa XPS (o equivalente). Las salidas del módulo Preventa XPS (o equivalente) se cablean a las entradas SIL-IN/SIL Common del módulo de interfaz SIL.

En caso de supervisión indirecta, la supervisión externa del estado del grupo debe buscar que los estados 2 o 4 persistan por más tiempo que el tiempo de

9. Nivel de integridad de la seguridad según la norma IEC 61508.

10. Tiempo medio hasta fallo peligroso conforme a la definición de IEC 13849-1.

actuación de una parada SIL. Utilice la información de estado para impedir el siguiente reinicio de los arrancadores SIL del grupo.

Categoría de cableado 4

Un fallo único no dará lugar a la pérdida de la función de seguridad. El fallo único se detecta en o antes de la siguiente demanda de la función de seguridad. Si esta detección no es posible, una acumulación de fallos no detectados no dará lugar a la pérdida de la función de seguridad.

Para cumplir con el requisito de la Categoría 4, la retroalimentación del contacto de espejo (Mirror In/Mirror Out) debe ser supervisada por un módulo Preventa XPS (o equivalente) que realice una supervisión de diagnóstico externa del contacto de espejo del arrancador SIL¹¹. Si el contacto espejo no se abre en parada, se impide el siguiente reinicio a todos los arrancadores SIL del grupo SIL. El elemento sensor relacionado con la seguridad se cablea a un módulo Preventa XPS (o equivalente). Las salidas del módulo Preventa XPS (o equivalente) se cablean a las entradas SIL-IN/SIL Common del módulo de interfaz SIL.

Ensayo de aceptación

El integrador de sistemas / fabricante de la máquina debe realizar un ensayo de aceptación de la función de seguridad para verificar y documentar el correcto funcionamiento de la función de seguridad. El integrador de sistemas / fabricante de la máquina certifica que ha comprobado la eficacia de las funciones de seguridad utilizadas. El ensayo de aceptación debe realizarse basándose en el análisis de peligros y la evaluación de riesgos. En el caso del modo de baja demanda con categoría 4, la función de seguridad debe probarse al menos una vez al mes. Deben respetarse todas las normas y los reglamentos vigentes.

11. Nivel de integridad de la seguridad según la norma IEC 61508.

cableado 1/2" (Avatar A4), donde ambos están formados por un único arrancador SIL. Ambos avatares siguen la lógica de avatares y los comandos operativos procedentes del PLC a través del bus de campo. El Comando de parada SIL procede del módulo externo Preventa™ XPS (o equivalente) cableado al módulo de interfaz SIL, y provoca que los arrancadores SIL desconecten la carga y accedan al estado seguro (Categoría de cableado 2).

Grupo SIL

Un grupo SIL¹⁵ está formado por uno o más avatares SIL, todos ellos asignados a un único módulo de interfaz SIL. Todos los Avatares SIL del grupo SIL reaccionan ante un único comando de parada SIL. El módulo de interfaz SIL siempre se instala a la derecha del último arrancador SIL incluido en el grupo SIL (en el extremo más alejado del módulo de interfaz de bus).

Una isla puede incluir varios grupos SIL.

Avatares SIL

Los Avatares SIL¹⁵ disponibles para funciones de Parada SIL son:

- Conmutador - Parada SIL, Cat. cableado 1/2
- Conmutador - Parada SIL, Cat. cableado 3/4
- Motor de una dirección - Parada SIL, Cat. cableado 1/2
- Motor de una dirección - Parada SIL, Cat. cableado 3/4
- Motor de dos direcciones - Parada de SIL, Cat. cableado 1/2
- Motor de dos direcciones - Parada de SIL, Cat. cableado 3/4
- Motor de dos velocidades - Parada de SIL, Cat. cableado 1/2
- Motor de dos velocidades - Parada de SIL, Cat. cableado 3/4
- Motor de dos velocidades y dos direcciones - Parada SIL, Cat. cableado 1/2
- Motor de dos velocidades y dos direcciones - Parada SIL, Cat. cableado 3/4
- Cinta transportadora de una dirección - Parada SIL, Cat. cableado 1/2
- Cinta transportadora de dos direcciones - Parada SIL, Cat. cableado 3/4

Los avatares SIL están formados por dispositivos de hardware específicos, que incluyen los arrancadores SIL, los arrancadores estándar y el módulo de interfaz SIL necesario que gestiona el grupo SIL asignado a los avatares SIL.

NOTA: Los avatares SIL están diseñados para aplicaciones con comandos operativos de baja frecuencia (inferior a una media anual de 15 ciclos de inicio/parada por hora).

Arrancador SIL



Arrancador estándar



Módulo de interfaz SIL



15. Nivel de integridad de la seguridad según la norma IEC 61508.

Módulo de interfaz SIL

El módulo de interfaz SIL¹⁶ (SIM) de TeSys™ island es un módulo complementario necesario para habilitar la característica de Seguridad funcional de la isla.

La función de Parada SIL se consigue a través de medios puramente electromecánicos sin necesidad de módulos de interfaz de bus ni de comunicación digitales.

El SIM:

- se conecta a un módulo externo Preventa™ XPS (o equivalente)
- controla la función de parada de su grupo SIL
- intercambia datos de funcionamiento con el módulo de interfaz de bus
- indica la información de funcionamiento a través de los LED frontales

Estado del contacto de los arrancadores SIL

El estado de los arrancadores SIL¹⁶ pertenecientes al grupo SIL se indica a través de las conexiones SIM Mirror In/Out. Esto permite la implementación de arquitecturas de la Categoría de cableado 2¹⁷ en las que los contactos de espejo se conectan al módulo Preventa XPS (o equivalente). Estas configuraciones ofrecen capacidad de supervisión directa de los dispositivos electromecánicos a través de un elemento de contacto enlazado mecánicamente, lo que proporciona una cobertura de diagnóstico de hasta el 99 %. Consulte EN ISO 13849-1, Tabla E.1 – Estimaciones para la cobertura de diagnóstico (DC).

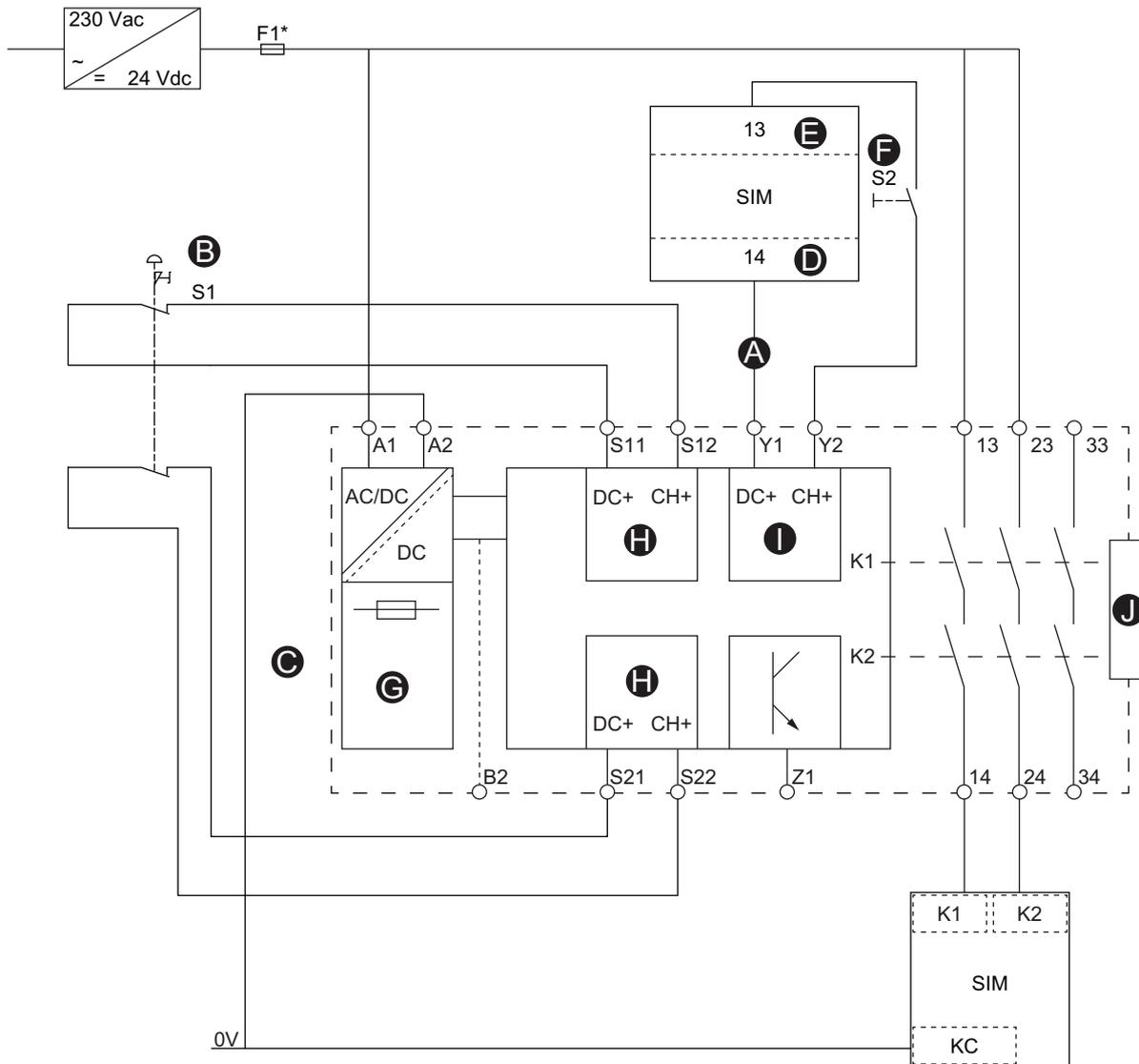
Tabla 2 - Estado del contacto de los arrancadores SIL

Estado de grupo SIL	Estado de Mirror In/Out
Todos los arrancadores SIL están abiertos	El contacto Mirror In/Out está cerrado
Al menos un arrancador SIL está cerrado	El contacto Mirror In/Out está abierto
TeSys island desconectada, o la función de seguridad ha detectado un fallo	El contacto Mirror In/Out está abierto

16. Nivel de integridad de la seguridad según la norma IEC 61508.

17. Categoría de cableado de cableado 2 según la norma ISO 13849.

Figura 3 - Cableado de SIM a módulo Preventa XPS-AF



A	Condiciones de inicio externas (ESC)	F	Botón Inicio (S2)
B	Pulsador de parada de emergencia (S1)	G	Fuente de alimentación
C	Módulo Preventa XPS-UAF	H	Entrada
D	SIM mirror out	I	Inicio
E	SIM mirror in	J	Extensión

Elemento sensor relacionado con la seguridad

El módulo SIM está conectado aguas arriba:

- a la fuente de 24 V CC
- al elemento sensor relacionado con la seguridad o a un módulo Preventa XPS (o equivalente).

El módulo SIM está diseñado con dos canales de entrada para alojar elementos sensores relacionados con la seguridad de doble canal. Para un nivel superior de tolerancia a fallos, se recomienda la arquitectura de canal de dos entradas.

Para ver los diagramas de cableado de abajo, consulte la Leyenda para los diagramas de cableado de canal SIM, página 24.

Figura 4 - SIM — Cableado de un canal

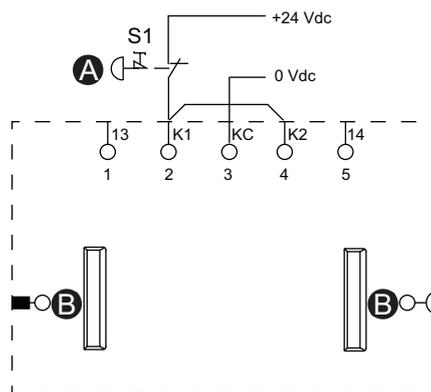


Figura 5 - SIM — Cableado de dos canales

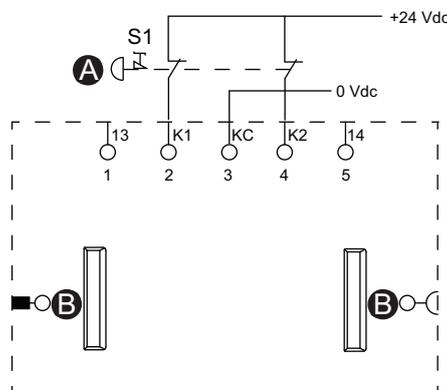


Tabla 3 - Leyenda para los diagramas de cableado de canal SIM

A	Pulsador de parada de emergencia (S1)
B	Conector de cable plano

Arrancadores SIL

⚠ ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

Para obtener instrucciones completas en relación con la seguridad funcional, consulte la Guía de seguridad funcional de TeSys™ island, 8536IB1904.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Los arrancadores SIL¹⁸ proporcionan funciones similares a las de los arrancadores estándar, pero se asocian con un módulo de interfaz SIL.

Las principales funciones de los arrancadores SIL son las siguientes:

- Proporcionar funcionalidades de Categoría de parada 0 y Categoría de parada 1¹⁹
- Permitir el control de funcionamiento de las cargas
- Medir datos eléctricos relacionados con la carga
- Proporcionar datos de supervisión de energía cuando se instala un módulo de interfaz de tensión en la TeSys island

Podrían ser necesarios varios SIL arrancadores para una única función de un TeSys avatar. Por ejemplo, el avatar Motor de dos direcciones - SIL Parada, categoría de cableado 1/2²⁰ incluye dos arrancadores SIL. Además, los avatars que utilizan arrancadores SIL siempre incluyen un módulo de interfaz SIL.

Los arrancadores SIL se conectan:

- Aguas arriba con un disyuntor
- Aguas abajo con la carga

Los arrancadores SIL se comunican con el acoplador de bus mediante el envío de datos de funcionamiento y la recepción de comandos.

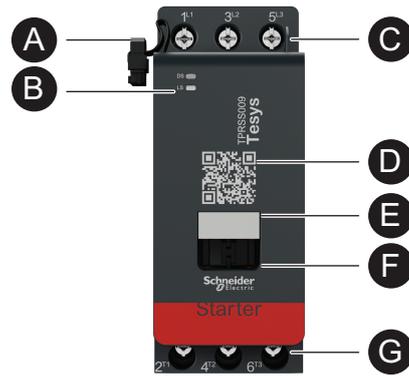
Tabla 4 - Valores nominales de los arrancadores SIL

Valores nominales de potencia		Amperaje	Referencia
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

18. Nivel de integridad de la seguridad según la norma IEC 61508

19. Categoría de parada 0 y Categoría de parada 1 según la norma EN/IEC 60204-1.

20. categoría de cableado 1 y categoría de cableado 2 según la norma ISO 13849.

Figura 6 - Características de los arrancadores SIL

A	Cable plano (para la conexión con el módulo de la izquierda)	E	Etiqueta de nombre
B	Indicadores de estado LED	F	Puente móvil
C	Conexiones de alimentación aguas arriba	G	Conexiones de alimentación aguas abajo
D	Código QR		

Elemento externo relacionado con la seguridad

TeSys™ island debe integrarse con otros elementos relacionados con la seguridad en un sistema relacionado con la seguridad más amplio para ayudar a garantizar la seguridad funcional de una máquina o un sistema/proceso.

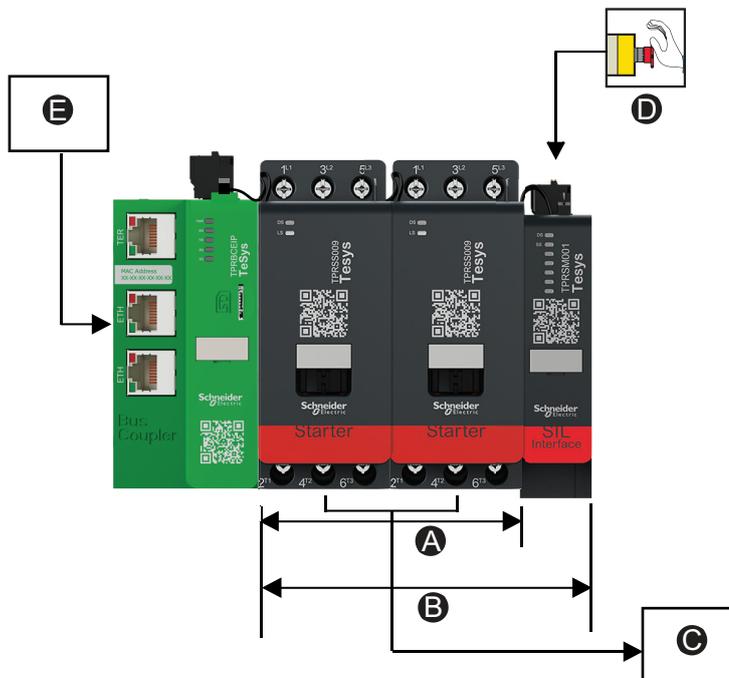
Las siguientes configuraciones ilustran los dispositivos típicos.

Parada SIL, Categoría de parada 0, Arquitectura categoría de cableado 1

NOTA: Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado de cableado 1 según la norma ISO 13849. Categoría de parada 0 según la norma EN/IEC 60204-1.

La parada SIL del motor se controla directamente mediante la apertura del contacto del pulsador de parada de emergencia.

Figura 7 - Parada SIL



A	Avatar A1	D	Categoría de cableado 1, Categoría de parada 0
B	Grupo SIL 1	E	PLC
C	Motor		

Parada SIL, Categoría de parada 0, Arquitectura categoría de cableado 2

NOTA: Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado de cableado 2 según la norma ISO 13849. Categoría de parada 0 según la norma EN/IEC 60204-1.

Figura 8 - Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 1/2 — Categoría de parada 0, Arquitectura categoría de cableado 2 (supervisión indirecta)

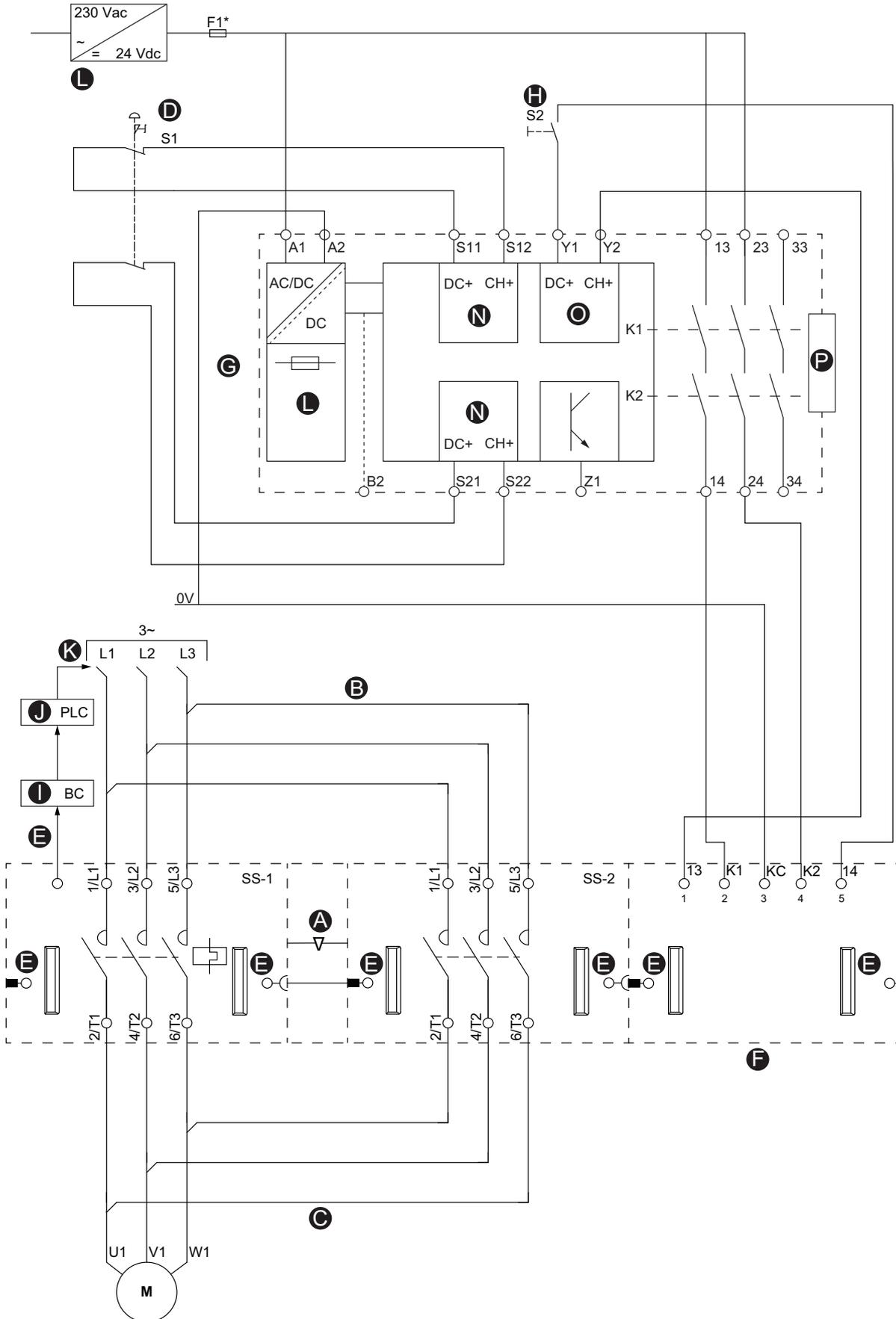
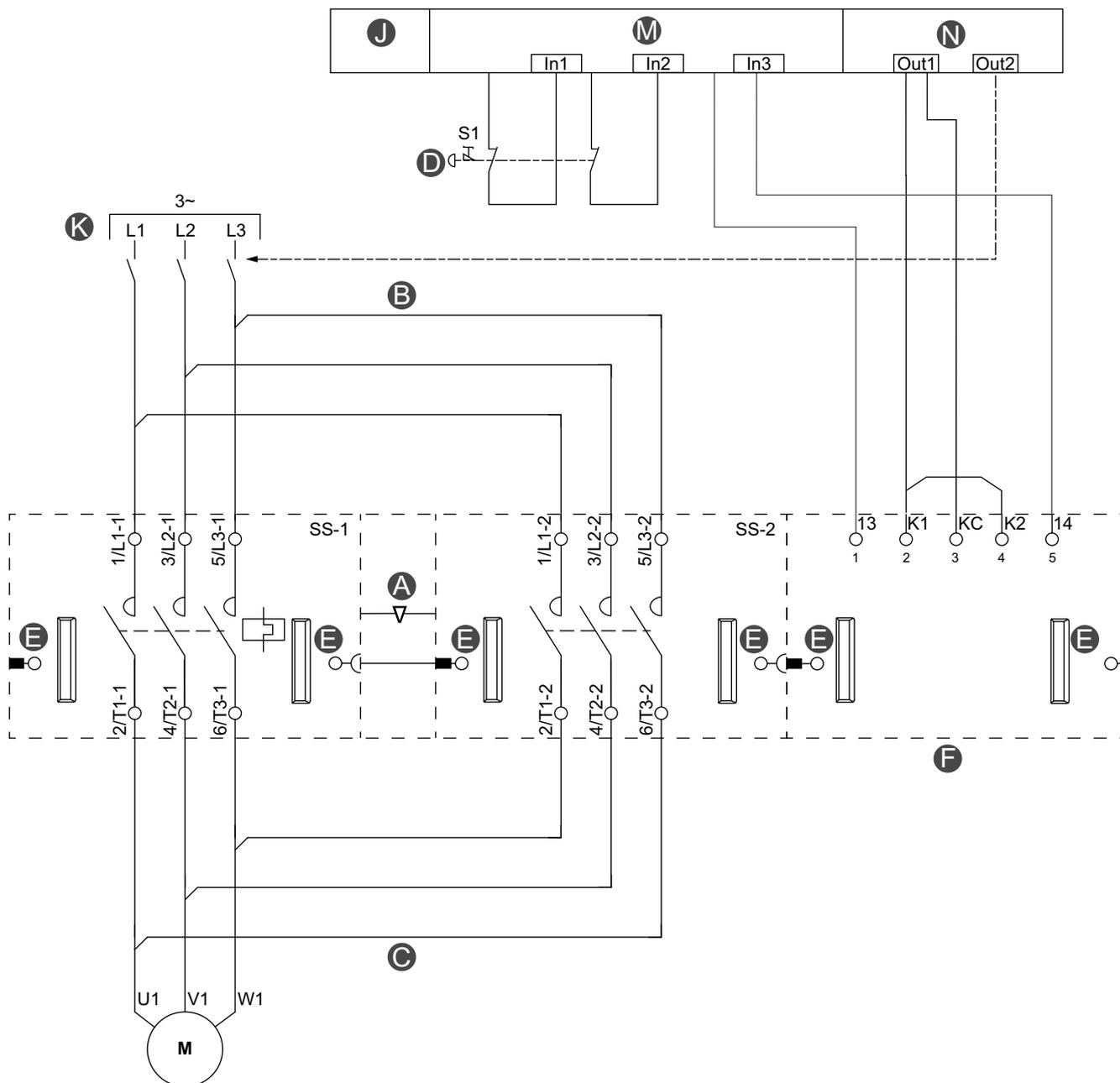


Tabla 5 - Leyenda de Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 1/2 — Categoría de parada 0, Arquitectura categoría de cableado 2 (supervisión indirecta), página 28

A	Enclavamiento mecánico	I	Modulo de interfaz de bus
B	Conexión paralela	J	PLC
C	Conexión de inversión	K	Disyuntor aguas arriba
D	Pulsador de parada de emergencia (S1)	L	Fuente de alimentación
E	Conector de cable plano	N	Entrada
F	Módulo de interfaz SIL (SIM)	O	Inicio
G	Módulo Preventa XPS-UAF	P	Extensión
H	Botón Inicio (S2)		

Figura 9 - Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 1/2 — Categoría de parada 0, Arquitectura categoría de cableado 2 (supervisión directa)



A	Enclavamiento mecánico	F	Módulo de interfaz SIL (SIM)
B	Conexión paralela	J	PLC función de seguridad
C	Conexión de inversión	K	Disyuntor aguas arriba
D	Pulsador de parada de emergencia (S1)	M	Entrada digital
E	Conector de cable plano	N	Salida digital

Parada SIL, Categoría de parada 1, Arquitectura categoría de cableado 2

NOTA: Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado de cableado 2 según la norma ISO 13849. Categoría de parada 1 según la norma EN/IEC 60204-1.

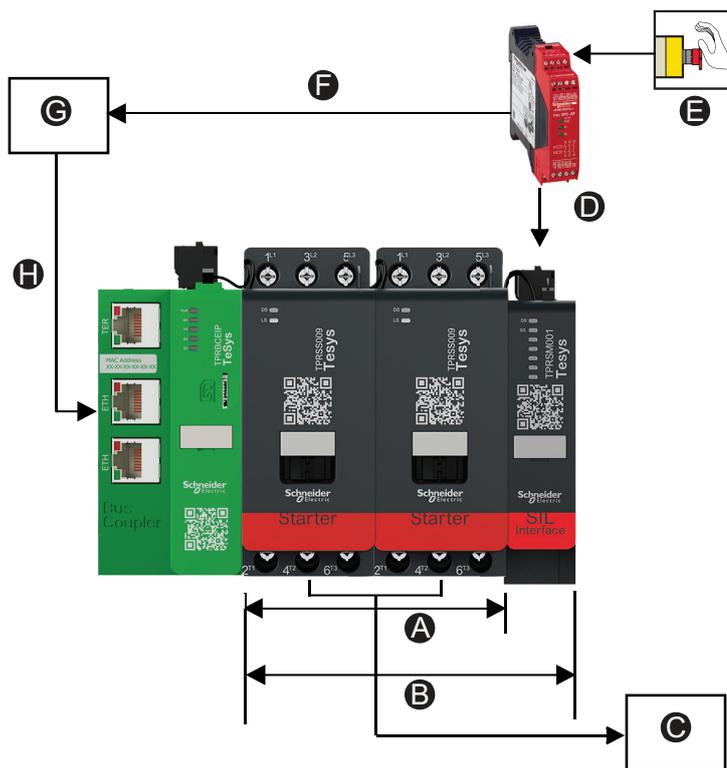
La Categoría de parada 1 se define como “una parada controlada con potencia disponible para que los actuadores de la máquina alcancen la parada y a continuación eliminen la potencia una vez alcanzada la parada”.

Cuando se activa una parada de emergencia, el comando de parada primero se envía a un dispositivo externo (por ejemplo, un PLC o un accionamiento). De esta forma, el proceso se detiene de forma controlada y no a través de una eliminación inmediata de la potencia. Tras un periodo de tiempo predefinido, el Comando de parada SIL se envía al SIM para la desconexión de las cargas de los avatares SIL del grupo SIL correspondiente.

La configuración recomendada consiste en utilizar un PLC para ayudar a garantizar la detención correcta del proceso antes de que se produzca la parada SIL.

El comando de parada se puede enrutar directamente a una entrada digital del PLC, o a un avatar de módulo E/S digital de TeSys™ island, utilizando una de sus entradas digitales leídas por el PLC. Una vez recibida la entrada de comando de parada, el PLC inicia una parada controlada mediante el envío de un comando de parada operativa al avatar objetivo de TeSys island.

Figura 10 - Comando de parada



A	Avatar A1	E	Categoría de cableado 2, Categoría de parada 1
B	Grupo SIL 1	F	Comando de parada controlada de Categoría 1

C	Motor	G	PLC
D	Parada no controlada	H	Comando de parada operativa

Figura 11 - Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 1/2 — Categoría de parada 1, Arquitectura categoría de cableado 2

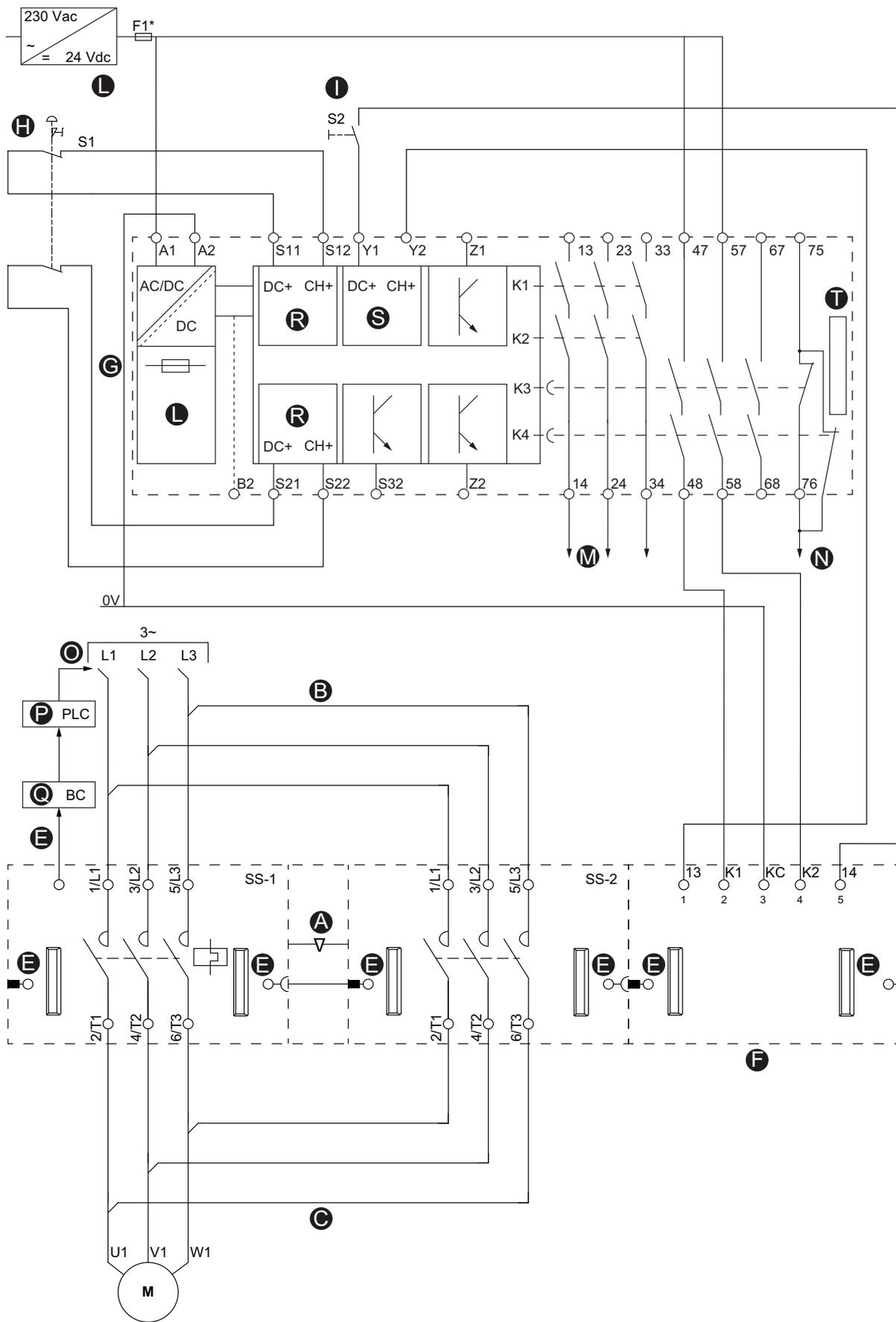


Tabla 6 - Leyenda de Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 1/2 — Categoría de parada 1, Arquitectura categoría de cableado 2, página 33

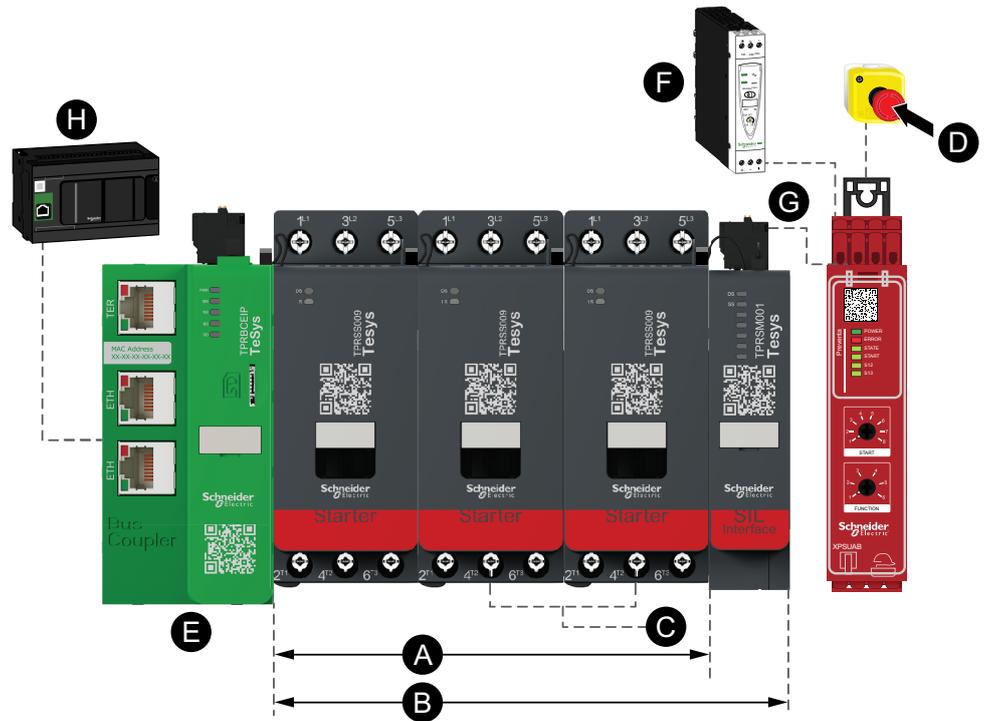
A	Enclavamiento mecánico	M	Parada controlada
B	Conexión paralela	N	Categoría de parada 1
C	Conexión de inversión	O	Disyuntor aguas arriba
E	Conector de cable plano	P	PLC
F	Módulo de interfaz SIL (SIM)	Q	Modulo de interfaz de bus
G	Módulo Preventa XPS-UAF	R	Entrada
H	Pulsador de parada de emergencia	S	Inicio
I	Botón Inicio S2	T	Extensión
L	Fuente de alimentación		

Parada SIL, Categoría de parada 0, Arquitectura categoría de cableado 3/4

NOTA: Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado 3/4 según la norma ISO 13849. Categoría de parada 0 según la norma EN/IEC 60204-1.

La parada SIL del motor se controla directamente mediante la apertura del contacto del pulsador de parada de emergencia.

Figura 12 - Parada SIL, Categoría de cableado 3/4



A	Avatar A1	E	Modulo de interfaz de bus
B	Grupo SIL 1	F	24 VCC
C	Motor	G	Módulo Preventa XPS-UAF
D	Categoría de cableado 3/4, Categoría de parada 0	H	PLC

Tabla 7 - Leyenda de Ejemplo: Motor de una dirección - Parada SIL, Cat. cableado 1/4 — Categoría de parada 0, Arquitectura categoría de cableado 3/4, página 36

C	Fuente de alimentación	H	Botón Inicio (S2)
D	Pulsador de parada de emergencia (S1)	I	Entrada
E	Conector de cable plano	J	Inicio
F	Módulo de interfaz SIL (SIM)	K	Extensión
G	Módulo Preventa XPS-UAF		

Parada SIL, Categoría de parada 1, Arquitectura categoría de cableado 3/4

NOTA: Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado 3/4 según la norma ISO 13849. Categoría de parada 1 según la norma EN/IEC 60204.

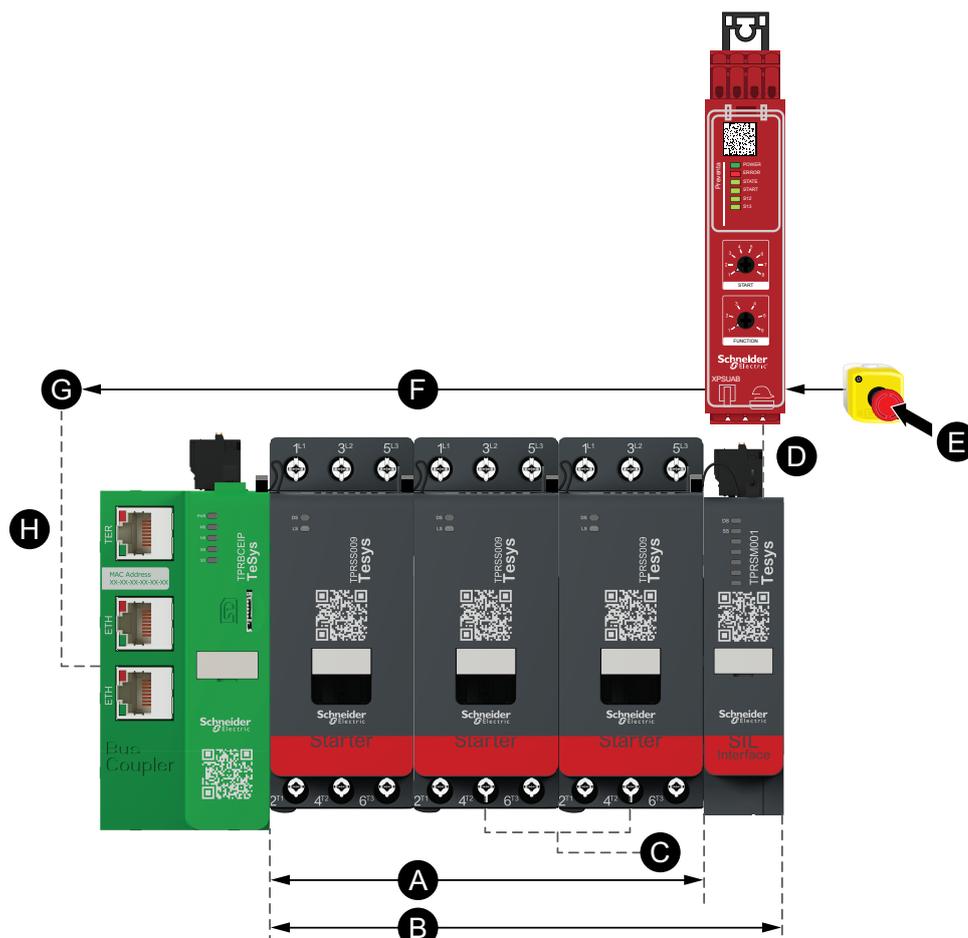
La Categoría de parada 1 se define como “una parada controlada con potencia disponible para que los actuadores de la máquina alcancen la parada y a continuación eliminen la potencia una vez alcanzada la parada”.

Cuando se activa una parada de emergencia, el comando de parada primero se envía a un dispositivo externo (por ejemplo, un PLC o un accionamiento). De esta forma, el proceso se detiene de forma controlada y no a través de una eliminación inmediata de la potencia. Tras un periodo de tiempo predefinido, el Comando de parada SIL se envía al SIM para la desconexión de las cargas de los avatares SIL del grupo SIL correspondiente.

Para la configuración, se recomienda utilizar un PLC para ayudar a garantizar la detención correcta del proceso antes de que se produzca la parada SIL.

El comando de parada se puede enrutar directamente a una entrada digital del PLC, o a un avatar de módulo E/S digital de TeSys™ island, utilizando una de sus entradas digitales leídas por el PLC. Una vez recibida la entrada de comando de parada, el PLC inicia una parada controlada mediante el envío de un comando de parada operativa al avatar objetivo de TeSys island.

Figura 14 - Comando de parada, Categoría de cableado 3/4



A	Avatar A1	E	Categoría de cableado 3/4, Categoría de parada 1
B	Grupo SIL 1	F	Comando de parada controlada de Categoría 1
C	Motor	G	PLC
D	Parada no controlada	H	Comando de parada operativa

Figura 15 - Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 3/4 — Categoría de parada 1, Arquitectura categoría de cableado 3/4

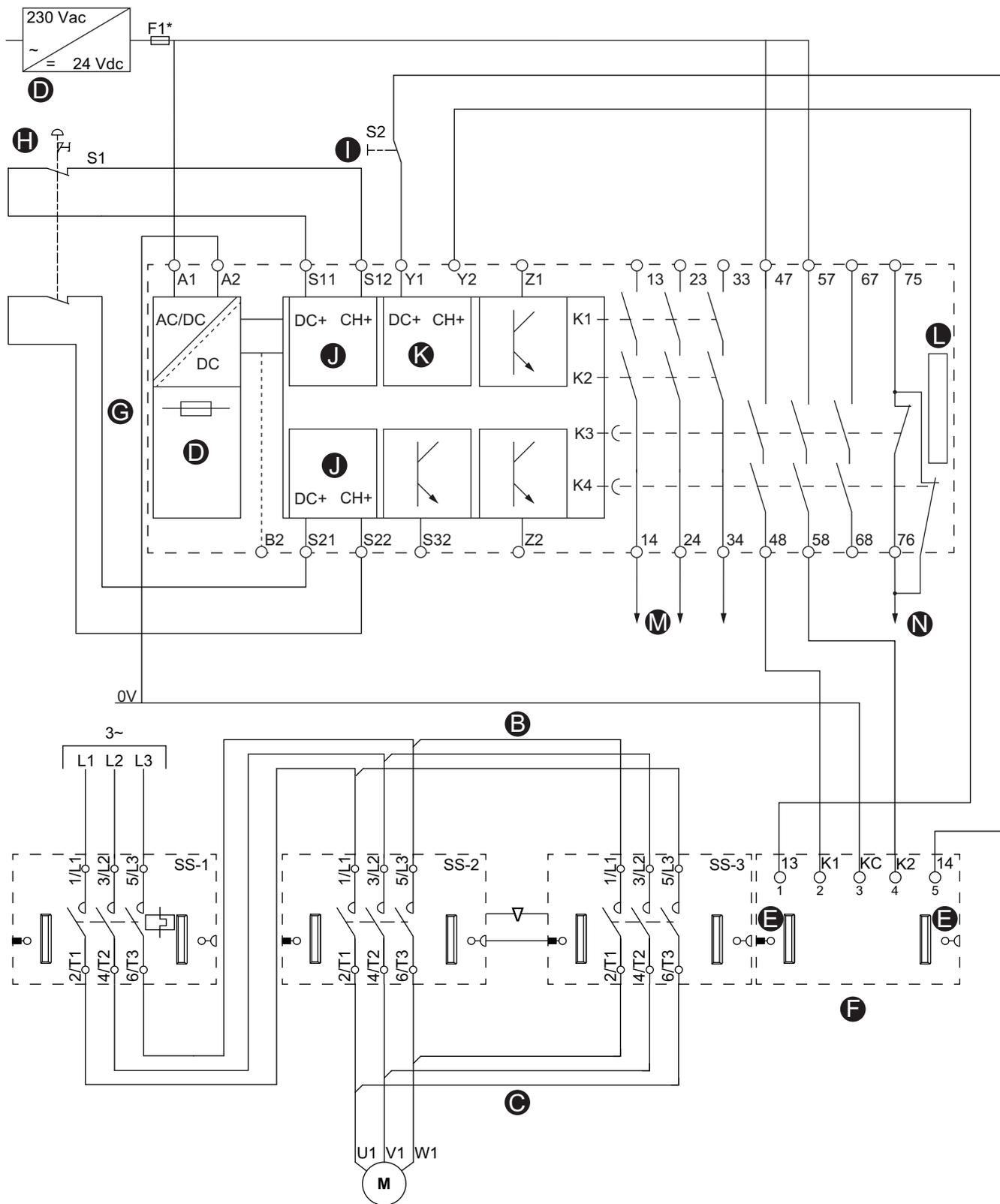


Tabla 8 - Leyenda de Ejemplo: Motor de dos direcciones - Parada SIL, Cat. cableado 3/4 — Categoría de parada 1, Arquitectura categoría de cableado 3/4, página 39

B	Conexión paralela	I	Botón Inicio S2
C	Conexión de inversión	J	Entrada
D	Fuente de alimentación	K	Inicio
E	Conector de cable plano	L	Extensión
F	Módulo de interfaz SIL (SIM)	M	Parada controlada
G	Módulo Preventa XPS-UAF	N	Categoría de parada 1
H	Pulsador de parada de emergencia (S1)		

Aislamiento de cable protegido

⚠ PELIGRO

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

Asegúrese de instalar los cables del sistema relacionado con la seguridad de conformidad con la norma ISO 13849-2.

Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.

Si se pueden producir cortocircuitos y circuitos cruzados con los cables del sistema relacionado con la seguridad y si los dispositivos anteriores no los detectan, se requiere la instalación de cables protegidos de acuerdo con la norma ISO 13849-2.

En el caso de una instalación con cables sin protección, las dos señales (ambos canales) de una función de seguridad en estado de cortocircuito pueden conectarse a tensión externa si un cable está dañado. En este caso, la función de seguridad dejará de estar operativa.

Arquitectura de conmutación de baja/alta frecuencia

Es posible utilizar la información incluida en esta sección para determinar si el funcionamiento se lleva a cabo en una arquitectura de frecuencia baja o alta.

La parte electromecánica del arrancador SIL²¹ posee características B10d.

Para calcular el $MTTF_d$ (de acuerdo con ISO 13849-1) o λ_d (de acuerdo con IEC 62061), se aplica la siguiente fórmula:

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

$$\text{con } \lambda_d = 1 / MTTF_d$$

Nop: Número medio de operaciones anuales

De acuerdo con la norma ISO 13849, el tiempo de funcionamiento de un componente electromecánico está limitado a T10d (el tiempo medio hasta que el 10 % de los componentes falla peligrosamente²²).

En consecuencia, el tiempo de funcionamiento de un arrancador SIL está limitado a:

$$T10d = B10d / Nop$$

El B10d de un arrancador SIL es $B10d = 1.369.863$ y, suponiendo un T10d de 10 años, el número de ciclos para un arrancador SIL de la TeSys está limitado a $Nop = B10d / T10 = 131.400/\text{año}$ (o una media anual de 15 ciclos/h).

Si la aplicación exige un Nop inferior a ese valor, queda dentro de la categoría de frecuencia de conmutación baja (donde los avatares SIL pueden utilizarse tal cual). De lo contrario, queda dentro de la categoría de frecuencia de conmutación alta (donde la función de seguridad debe implementarse con un avatar SIL específico como se describe abajo).

21. Nivel de integridad de la seguridad según la norma IEC 61508.

22. Falla peligrosamente de acuerdo con la norma ISO 13849

Frecuencia de conmutación baja (< 15 ciclos por hora)

Con una frecuencia de conmutación baja, las funciones de parada SIL²³ y de encendido/apagado se pueden conseguir conjuntamente con un Avatar SIL.

Figura 16 - Ejemplo de Avatar con arrancador SIL



Tabla 9 - Frecuencia de conmutación baja — Funciones operativa y de seguridad

Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5
Conmutador - Parada SIL, Cat. cableado 1/2 ²⁴	Arrancador SIL	SIM	—	—	—
Conmutador - Parada SIL, Cat. cableado 3/4 ²⁵	Arrancador SIL	Arrancador SIL	SIM	—	—
Motor de una dirección - Parada SIL, Cat. cableado 1/2	Arrancador SIL	SIM	—	—	—
Motor de una dirección - Parada SIL, Cat. cableado 3/4	Arrancador SIL	Arrancador SIL	SIM	—	—
Motor de dos direcciones - Parada de SIL, Cat. cableado 1/2	Arrancador SIL	Arrancador SIL	SIM	—	—
Motor de dos direcciones - Parada de SIL, Cat. cableado 3/4	Arrancador SIL	Arrancador SIL	Arrancador SIL	SIM	—
Motor de dos velocidades - Parada de SIL, Cat. cableado 1/2	Arrancador SIL	Arrancador SIL	SIM	—	—
Motor de dos velocidades - Parada de SIL, Cat. cableado 3/4	Arrancador SIL	Arrancador SIL	Arrancador SIL	SIM	—
Motor de dos velocidades y dos direcciones - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM
Motor de dos velocidades y dos direcciones - Parada SIL, Cat. cableado 3/4	Arrancador SIL	Arrancador SIL	Arrancador SIL	Arrancador SIL	SIM
Transportador de una dirección - Parada SIL, Cat. cableado 1/2	Arrancador SIL	SIM	—	—	—
Transportador de dos direcciones - Parada SIL, Cat. cableado 1/2	Arrancador SIL	Arrancador SIL	SIM	—	—

23. Nivel de integridad de la seguridad según la norma IEC 61508.

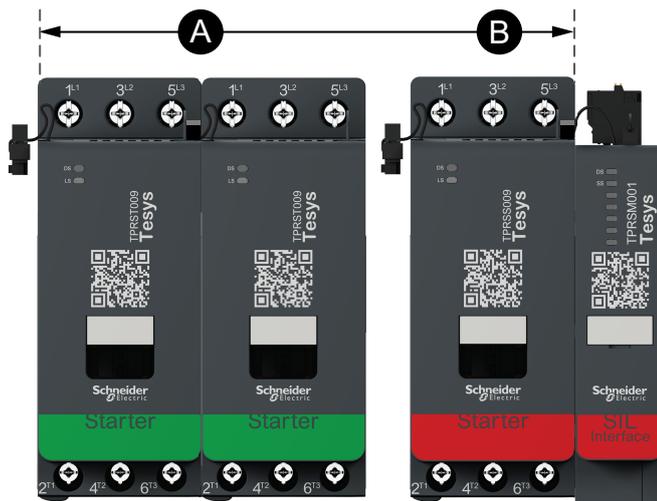
24. Categoría de cableado 1 y Categoría de cableado 2 según la norma ISO 13849.

25. Categoría de cableado 3 y Categoría de cableado 4 según la norma ISO 13849.

Frecuencia de conmutación alta (≥ 15 ciclos por hora)

Para un uso de alta frecuencia, la función de seguridad debe aislarse de la función operativa utilizando un Avatar SIL²⁶ para la función de seguridad y un Avatar estándar para la función operativa. Los siguientes arrancadores estándar se cablean en series aguas abajo de los arrancadores SIL. Frecuencia de conmutación alta - La tabla Funciones operativas y de seguridad muestra ejemplos de avatares estándar utilizados aguas abajo del/de los arrancador(es) SIL para arquitecturas de parada SIL, Cat. cableado 1/2²⁷ y Parada SIL, Cat. cableado 3/4²⁸.

Figura 17 - Avatar estándar para función operativa + Avatar SIL para función de seguridad — Parada SIL, Cat. cableado 1/2



A	Avatar estándar
B	Avatar SIL

Tabla 10 - Frecuencia de conmutación alta - Parada SIL, Cat. cableado 1/2 — Funciones operativa y de seguridad

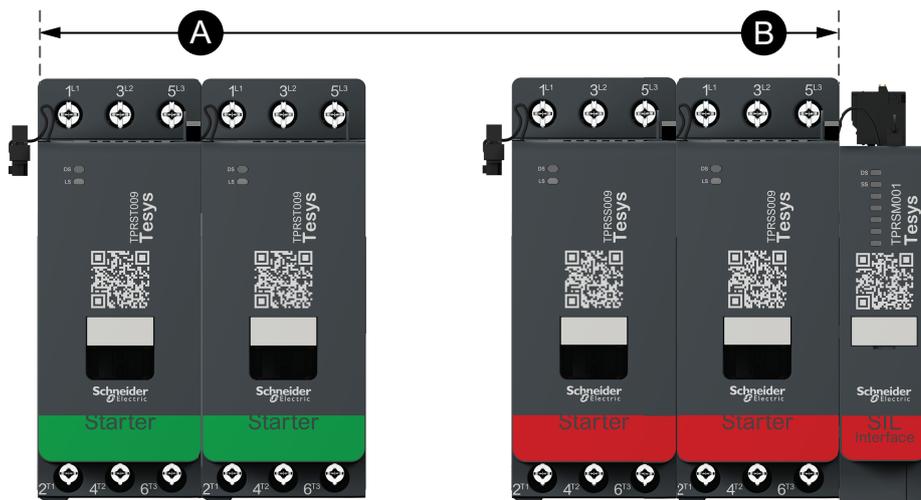
Avatar estándar	Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5	Módulo 6
Conmutador	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador SIL	SIM	—	—	—
Motor de una dirección	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador SIL	SIM	—	—	—
Motor de dos direcciones	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador SIL	SIM	—	—
Motor de dos velocidades	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador SIL	SIM	—	—
Motor de dos velocidades y dos direcciones	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador SIL	SIM
Cinta transportadora de una dirección	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador SIL	SIM	—	—	—
Cinta transportadora de dos direcciones	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador SIL	SIM	—	—

26. Nivel de integridad de la seguridad según la norma IEC 61508.
 27. Categoría de cableado 1 y Categoría de cableado 2 según la norma ISO 13849.
 28. Categoría de cableado 3 y Categoría de cableado 4 según la norma ISO 13849

Tabla 10 - Frecuencia de conmutación alta - Parada SIL, Cat. cableado 1/2 — Funciones operativa y de seguridad (Continuación)

Avatar estándar	Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5	Módulo 6
Motor estrella/triángulo de una dirección	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador SIL	SIM	—
Motor estrella/triángulo de dos direcciones	Conmutador - Parada SIL, Cat. cableado 1/2	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador SIL	SIM

Figura 18 - Avatar estándar para función operativa + Avatar SIL para función de seguridad — Parada SIL, Cat. cableado 3/4



A	Avatar estándar
B	Avatar SIL

Tabla 11 - Frecuencia de conmutación alta - Parada SIL, Cat. cableado 3/4 — Funciones operativa y de seguridad

Avatar estándar	Avatar SIL	Módulo 1	Módulo 2	Módulo 3	Módulo 4	Módulo 5	Módulo 6	Módulo 7
Conmutador	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM	—	—	—
Motor de una dirección	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM	—	—	—
Motor de dos direcciones	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM	—	—
Motor de dos velocidades	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM	—	—
Motor de dos velocidades y dos direcciones	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM
Motor estrella/triángulo de una dirección	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM
Motor estrella/triángulo de dos direcciones	Conmutador - Parada SIL, Cat. cableado 3/4	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador estándar	Arrancador SIL	Arrancador SIL	SIM

Arquitecturas de muestra

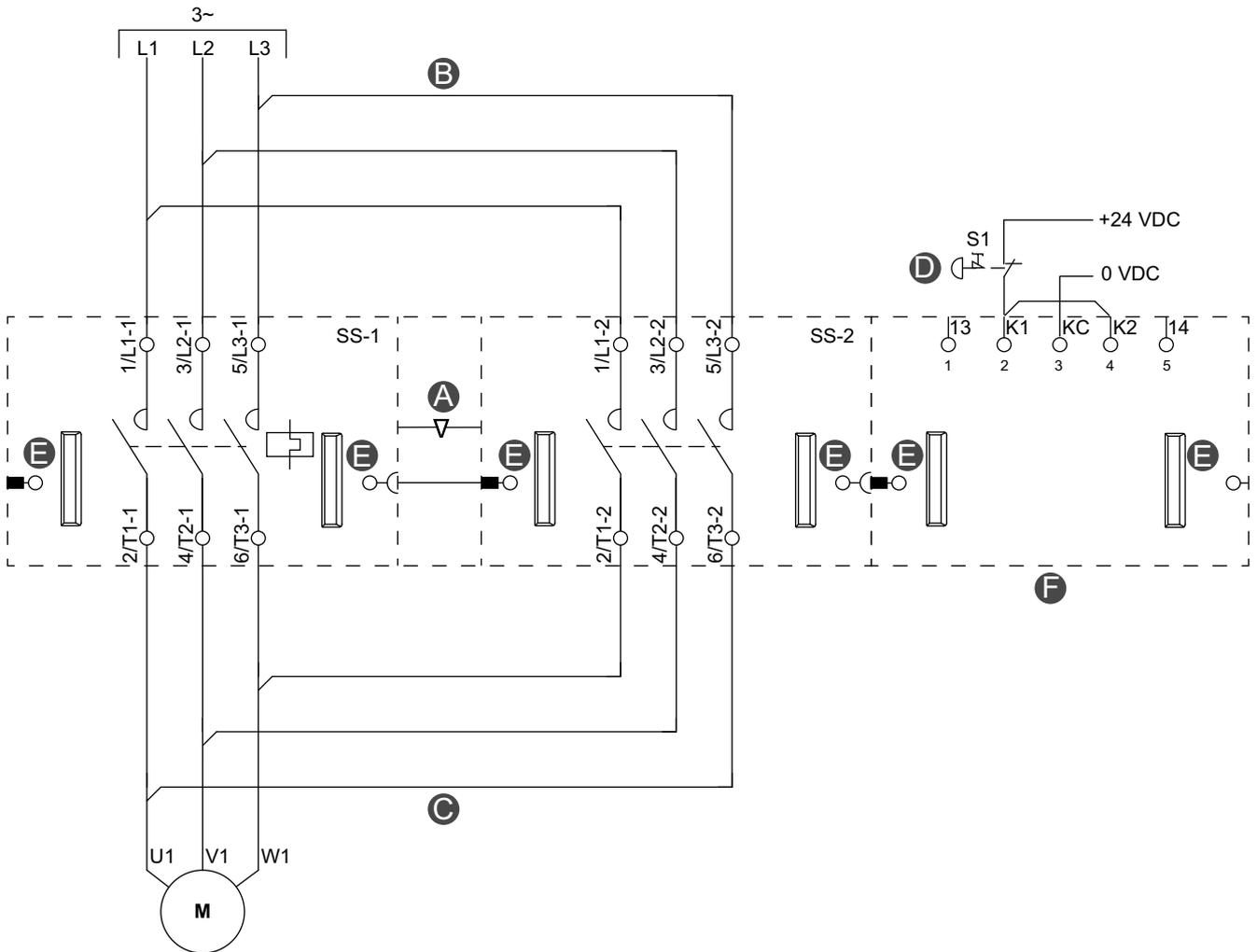
Las siguientes arquitecturas están disponibles para la seguridad funcional de TeSys™ island:

- Parada SIL, Categoría de parada 0, Categoría de cableado 1²⁹
- Parada SIL, Categoría de parada 0, Categoría de cableado 2
- Parada SIL, Categoría de parada 1, Categoría de cableado 2
- Parada SIL, Categoría de parada 0, Categoría de cableado 3/4
- Parada SIL, Categoría de parada 1, Categoría de cableado 3/4

29. Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado 1, Categoría de cableado 2 y Categoría de cableado 3/4 según la norma ISO 13849. Categoría de parada 0 y Categoría de parada 1 según la norma EN/IEC 60204-1.

Parada SIL, Categoría de parada 0, Categoría de cableado 1

Figura 19 - Ejemplo: Parada SIL, Categoría de parada 0, Categoría de cableado 1³⁰

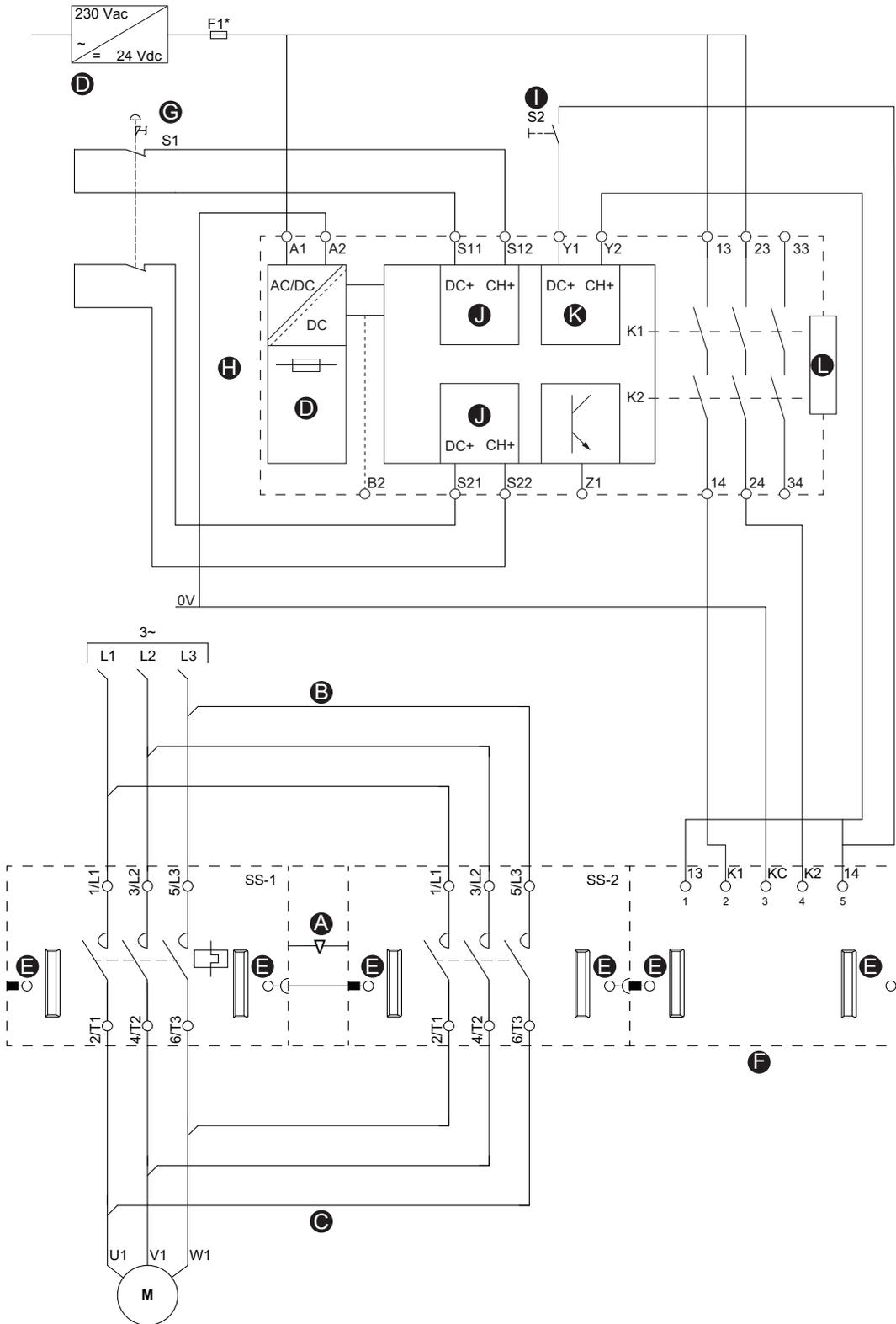


A	Enclavamiento mecánico	D	Pulsador de parada de emergencia (S1)
B	Conexión paralela	E	Conector de cable plano
C	Conexión de inversión	F	Módulo de interfaz SIL (SIM)

30. Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado de cableado 1 según la norma ISO 13849. Categoría de parada 0 según la norma EN/IEC 60204-1.

Parada SIL, Categoría de parada 0, Categoría de cableado 2

Figura 20 - Ejemplo: Parada SIL, Categoría de parada 0, Categoría de cableado 2³¹



31. Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado 2 según la norma ISO 13849. Categoría de parada 0 según la norma EN/IEC 60204-1.

Tabla 12 - Leyenda de Ejemplo: Parada SIL, Categoría de parada 0, Categoría de cableado 2, página 48

A	Bloqueo mecánico	G	Pulsador de parada de emergencia (S1)
B	Conexión paralela	H	Módulo Preventa XPS-UAF
C	Conexión de inversión	I	Botón Inicio (S2)
D	Alimentación	J	Entrada
E	Conector de cable plano	K	Iniciar
F	Módulo de interfaz SIL (SIM)	L	Extensión

Tabla 13 - Leyenda de Ejemplo: Parada SIL, Categoría de parada 1, Categoría de cableado 2, página 50

A	Bloqueo mecánico	J	Entrada
B	Conexión paralela	K	Iniciar
C	Conexión de inversión	L	Extensión
E	Conector de cable plano	M	Parada controlada
F	Módulo de interfaz SIL (SIM)	N	Categoría de parada 1
G	Alimentación	O	Interruptor automático aguas arriba
H	Pulsador de parada de emergencia (S1)	P	PLC
I	Botón Inicio S2	Q	Acoplador de bus

Tabla 14 - Leyenda de Ejemplo: Parada SIL, Categoría de parada 0, Categoría de cableado 3/4 (Continuación)

F	Módulo de interfaz SIL (SIM)	K	Extensión
G	Módulo Preventa XPS-UAF		

Parada SIL, Categoría de parada 1, Categoría de cableado 3/4

Figura 23 - Ejemplo: Parada SIL, Categoría de parada 1, Categoría de cableado 3/4³⁴

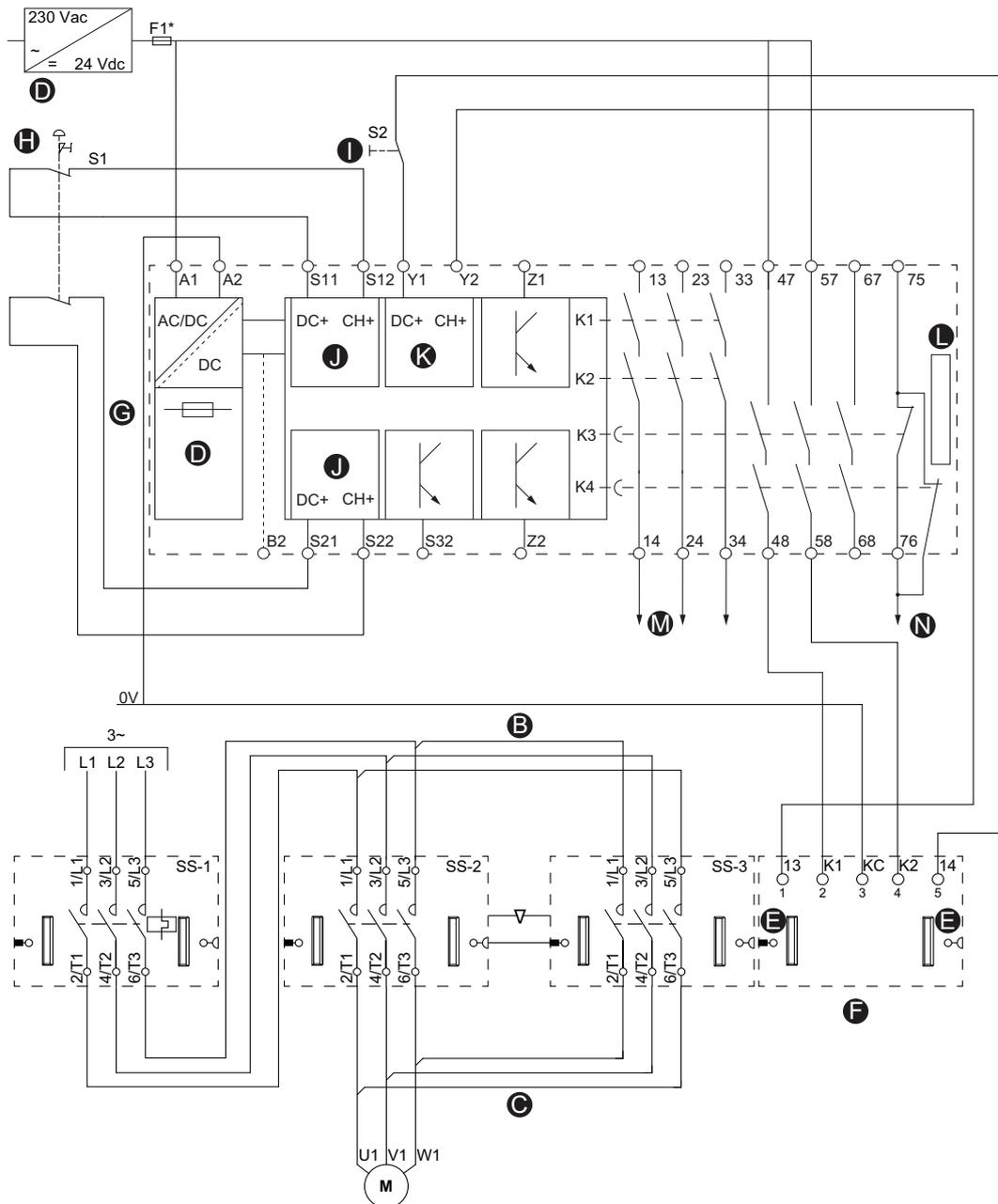


Tabla 15 - Leyenda de Ejemplo: Parada SIL, Categoría de parada 1, Categoría de cableado 3/4, página 54

B	Conexión paralela	I	Botón Inicio S2
C	Conexión de inversión	J	Entrada
D	Alimentación	K	Iniciar

34. Nivel de integridad de la seguridad según la norma IEC 61508. Categoría de cableado 3/4 según la norma ISO 13849. Categoría de parada 1 según la norma EN/IEC 60204-1.

Tabla 15 - Leyenda de Ejemplo: Parada SIL, Categoría de parada 1, Categoría de cableado 3/4 (Continuación)

E	Conector de cable plano	L	Extensión
F	Módulo de interfaz SIL (SIM)	M	Parada controlada
G	Módulo Preventa XPS-UAF	N	Categoría de parada 1
H	Pulsador de parada de emergencia (S1)		

Datos técnicos

Módulo de interfaz SIL

Tabla 16 - Valores calculados del módulo de interfaz SIL³⁵ (SIM)

Arquitectura	SIM					
	PFH ³⁶	PFD ³⁷	SFF ³⁸	HFT ³⁹	MTTF _d (años)	DC ⁴⁰
Categoría de cableado 1 ⁴¹	2.10 ⁻¹⁰	2.10 ⁻⁵	>90 %	1	17.459	No pertinente
Categoría de cableado 2			>99%			90%
Categoría de cableado 3			>99%			90%
Categoría de cableado 4			99%			99%

NOTA: Los valores PFD y PFH se calculan con lo siguiente:

- Intervalo de prueba = 20 años
- MTTR⁴²=MRT⁴³= 24 horas

Los requisitos arquitectónicos definidos en la Tabla 3 de la norma IEC 61508-2 y la Tabla 5 de la norma EN 62061 se cumplen hasta los niveles SIL 3.

Arrancador SIL

Los siguientes datos contribuyen a definir el nivel de funcionamiento de los arrancadores SIL³⁵.

B10: 1.000.000

% de fallos peligrosos⁴⁴: 73%

B10_d: 1.369.863

Suponiendo un número de operaciones = 131.400 ciclos/año (media de 15 ciclos/hora)

Los valores calculados del arrancador SIL se exponen en las siguientes tablas:

Tabla 17 - Arrancador SIL en monocanal

Categoría de cableado ⁴¹	SFF	HFT	MTTF _d (años)	DC
Categoría 1	27%	0	100 años	No pertinente
Categoría 2 – Supervisión directa	90%	0	100 años	≥ 90%

35. Nivel de integridad de la seguridad según la norma IEC 61508.

36. Frecuencia media de fallo peligroso [h⁻¹], conforme a la definición de IEC 61508-4

37. Probabilidad de fallo peligroso en demanda, conforme a la definición de IEC 61509-4.

38. Fracción de fallo seguro, conforme a la definición de IEC 61509-4.

39. Tolerancia de fallo de hardware, conforme a la definición de IEC 61509-4.

40. Cobertura de diagnóstico, conforme a la definición de IEC 61509-4.

41. Categorías de cableado 1, 2, 3 y 4 según la norma ISO 13849.

42. Tiempo medio hasta reparación, conforme a la definición de IEC 61509-4

43. Tiempo medio de reparación, conforme a la definición de IEC 61509-4

44. Fallo peligroso conforme a la definición de IEC 61508-4

Tabla 18 - Arrancador SIL en doble canal

Categoría de cableado	SFF	HFT	MTTF _d (años)	DC
Categoría 3	27%	0	100 años	≥ 90%
Categoría 4	90%	0	100 años	≥ 99 %

La relación entre PFH_d y PFD de los arrancadores SIL, dependiendo de la arquitectura y el intervalo de prueba, se indica en la siguiente tabla:

Tabla 19 - Arrancadores SIL — PFH_d y PFD

Categoría de cableado	PFH (IEC 61508)	PFD (IEC 61508) Ti=10 años ⁴⁵	PFD (IEC 61508) Ti=5 años ⁴⁵
Categoría 1	1.10E-06	4.80E-02	4.82E-03
Categoría 2 – Supervisión directa	1.10E-06	4.82E-03	5.06E-04
Categoría 3	4.5E-09	—	1.30E-04
Categoría 4	2.5E-10	—	2.5E-06

Los requisitos arquitectónicos definidos en la Tabla 3 de la norma IEC 61508-2 y la Tabla 5 de la norma EN 62061 se cumplen hasta los niveles SIL 2.

Es necesaria una arquitectura de categoría 2 para cumplir las limitaciones arquitectónicas SIL 2 (obtenida utilizando la supervisión directa Mirror In/Mirror Out).

NOTA: La detección de fallos y la reacción al fallo específico deben tener lugar antes de que pueda producirse la situación peligrosa abordada por la función de control relacionada con la seguridad.

45. Intervalo de prueba

Datos de fiabilidad

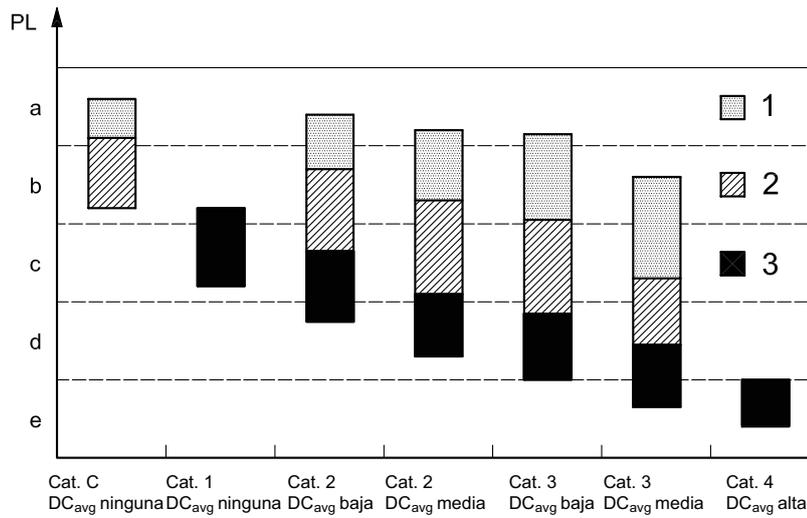
Referencias a la normativa sobre la función de seguridad

La función de Parada SIL⁴⁶ tiene prioridad sobre una parada activada por motivos operativos (EN ISO 13849-1, 5.2.1).

El nivel de funcionamiento depende de la categoría de cableado⁴⁷, el $MTTF_d$ y el DC_{avg} .

El siguiente diagrama muestra el posicionamiento de TeSys™ island de acuerdo con el requisito de categoría.

Figura 24 - Posicionamiento de TeSys island según el requisito de categoría



Clave

PL - Nivel de rendimiento

- 1 $MTTF_d$ de cada canal = baja
- 2 $MTTF_d$ de cada canal = media
- 3 $MTTF_d$ de cada canal = alta

Tabla 20 - Procedimiento simplificado para la evaluación del PL alcanzado por las piezas de sistemas de control relacionadas con la seguridad (SRP/CS)

Categoría	B	1	2	2	3	3	4
DC _{avg}	Ninguna	Ninguna	baja	media	baja	media	alta
MTTF_d de cada canal							
Baja	a	No cubierto	a	b	b	c	No cubierto
Media	b	No cubierto	b	c	c	d	No cubierto
Alta	No cubierto	c	v	d	d	d	e

De acuerdo con la arquitectura y la categoría de cableado de TeSys island, los indicadores clave (DC_{avg} , $MTTF_d$, PL) para TeSys island cumplen con los valores mostrados en la tabla de abajo.

46. Nivel de integridad de la seguridad según la norma IEC 61508.

47. Categorías de cableado según la norma ISO 13849.

Tabla 21 - Valores de los indicadores clave para arquitecturas de canal único y doble

Arquitectura del sistema de TeSys island	Categoría	Tolerancia a fallo único ⁴⁸	DC _{avg}	MTTF _d de cada canal	PL objetivo
Canal único	1	No	Ninguno	Alta (≥ 30 años)	c
	2	No	Baja (≥ 60 %) a media (≥ 90 %)	Baja (≥ 3 años) a alta (≥ 30 años)	c, d
Doble canal	3	Sí			c, d, e
	4	Sí	Alta (≥ 99 %)	Alta (≥ 30 años)	e

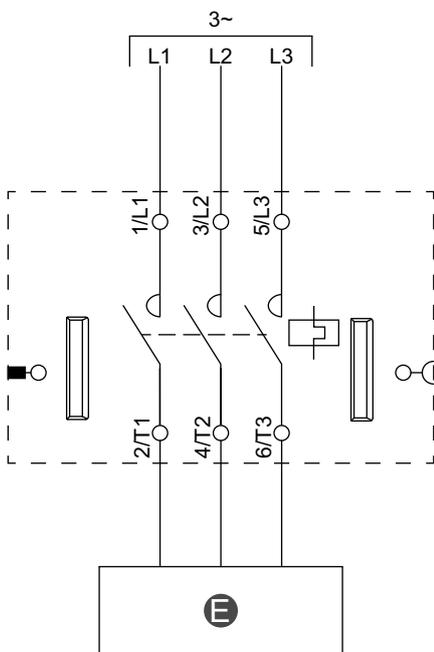
Cableado de avatares SIL

Los diagramas de cableado de esta sección corresponden a los avatares SIL⁴⁹. La siguiente tabla es una leyenda para los diagramas de esta sección.

Tabla 22 - Leyenda para los diagramas de cableado

A	Enclavamiento mecánico
B	Conexión paralela
C	Conexión de inversión
E	Circuito eléctrico

Figura 25 - Conmutador - Parada SIL, Cat. cableado 1/2⁵⁰



48. Tolerancia a fallo único significa que un único fallo (incluidos los eventos en modo común) no deben dar lugar a la pérdida de la función de seguridad.

49. Nivel de integridad de la seguridad según la norma IEC 61508.

50. Categoría de cableado 1 y Categoría de cableado 2 según la norma ISO 13849.

Figura 26 - Motor de una dirección - Parada SIL, Cat. cableado 1/2

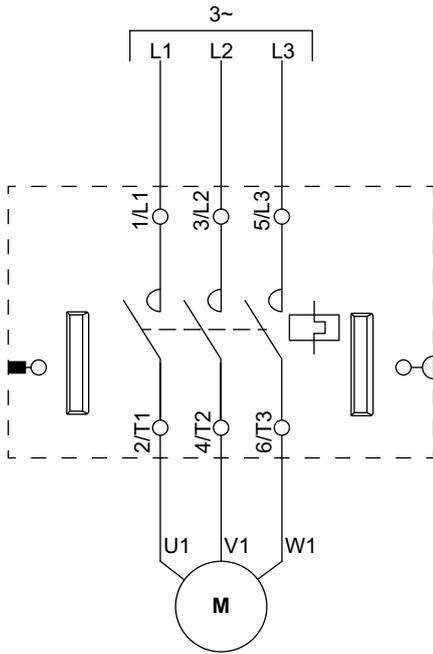


Figura 27 - Motor de dos direcciones - Parada de SIL, Cat. cableado 1/2

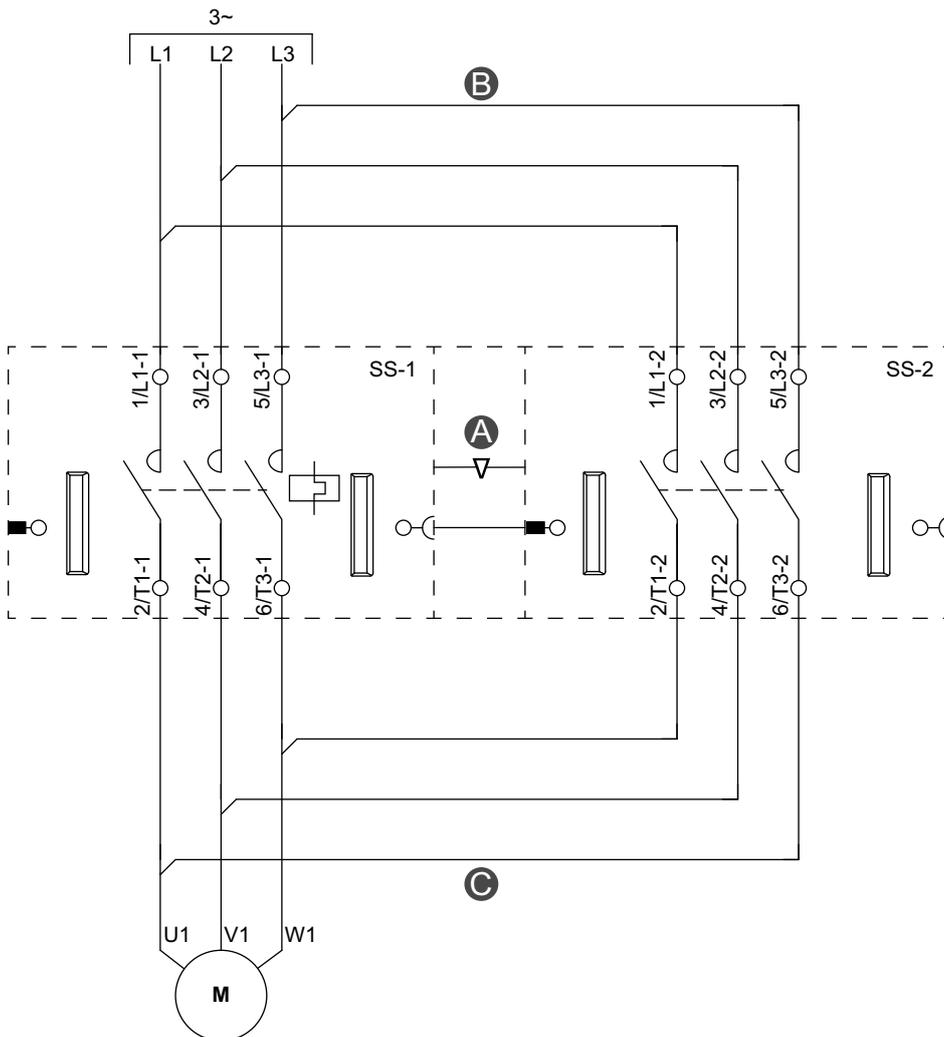


Figura 28 - Motor de dos velocidades - Parada de SIL, Cat. cableado 1/2

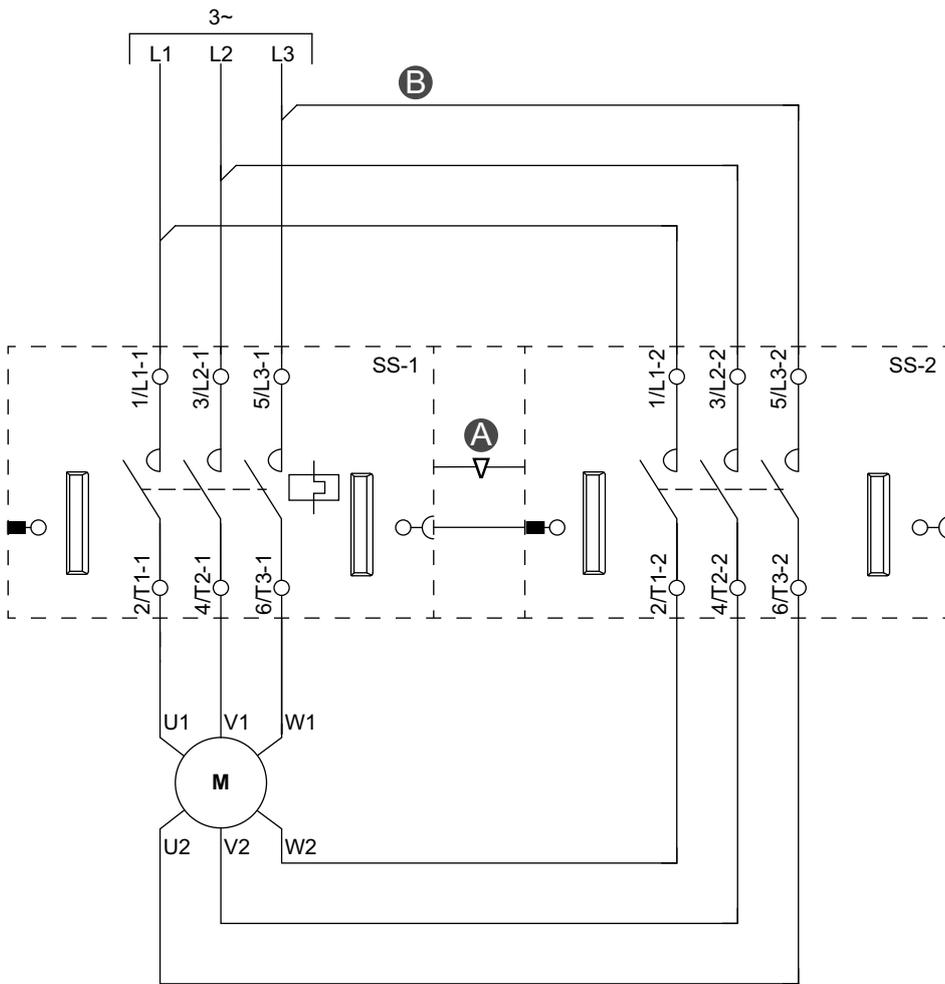


Figura 29 - Motor de dos velocidades y dos direcciones - Parada SIL, Cat. cableado 1/2

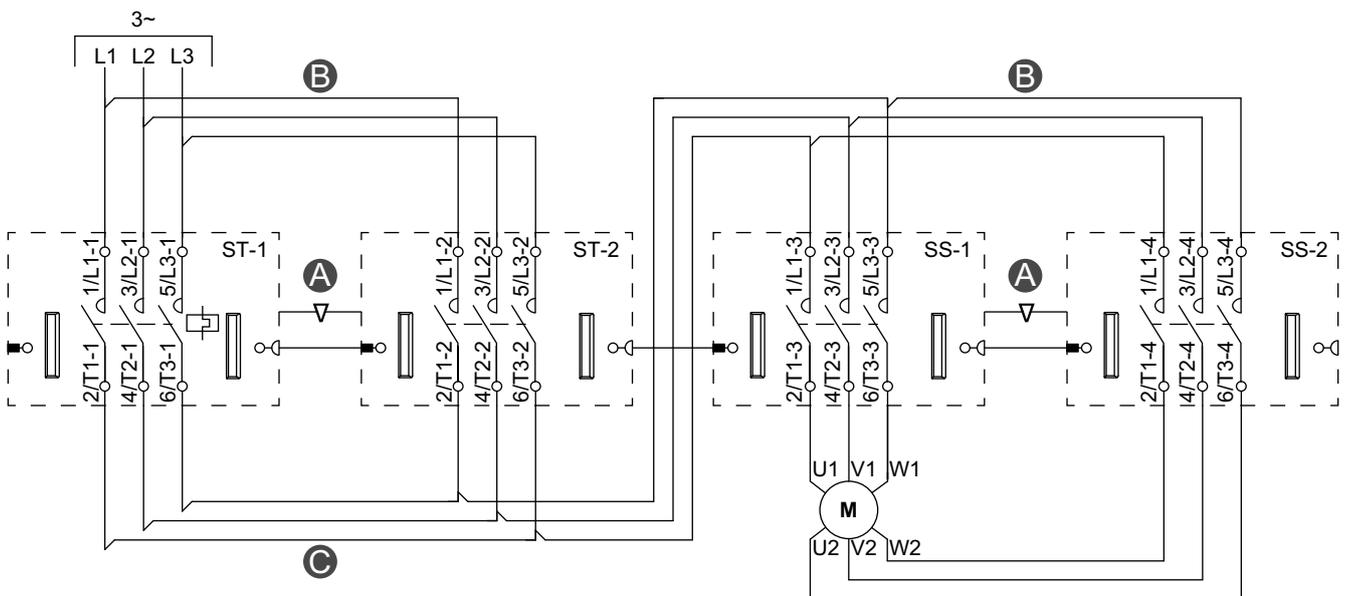
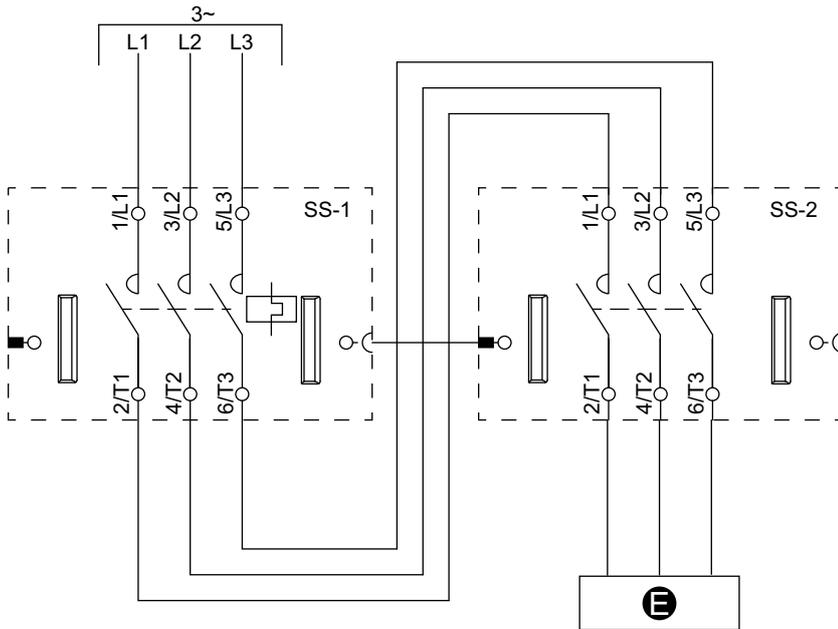
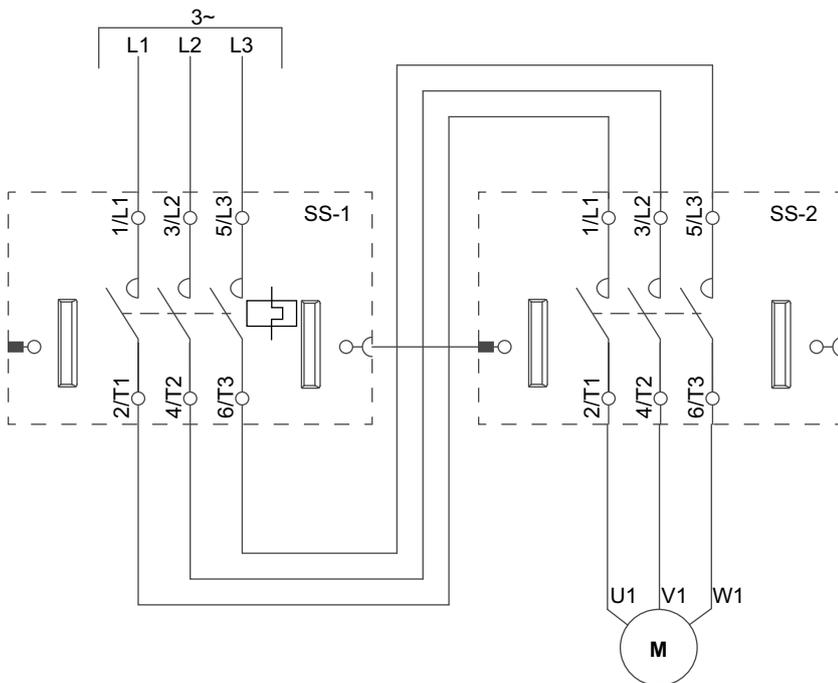


Figura 30 - Conmutador - Parada SIL, Cat. cableado 3/4⁵¹**Figura 31 - Motor de una dirección - Parada SIL, Cat. cableado 3/4**

51. Categoría de cableado 3 y Categoría de cableado 4 según la norma ISO 13849.

Figura 32 - Motor de dos direcciones - Parada de SIL, Cat. cableado 3/4

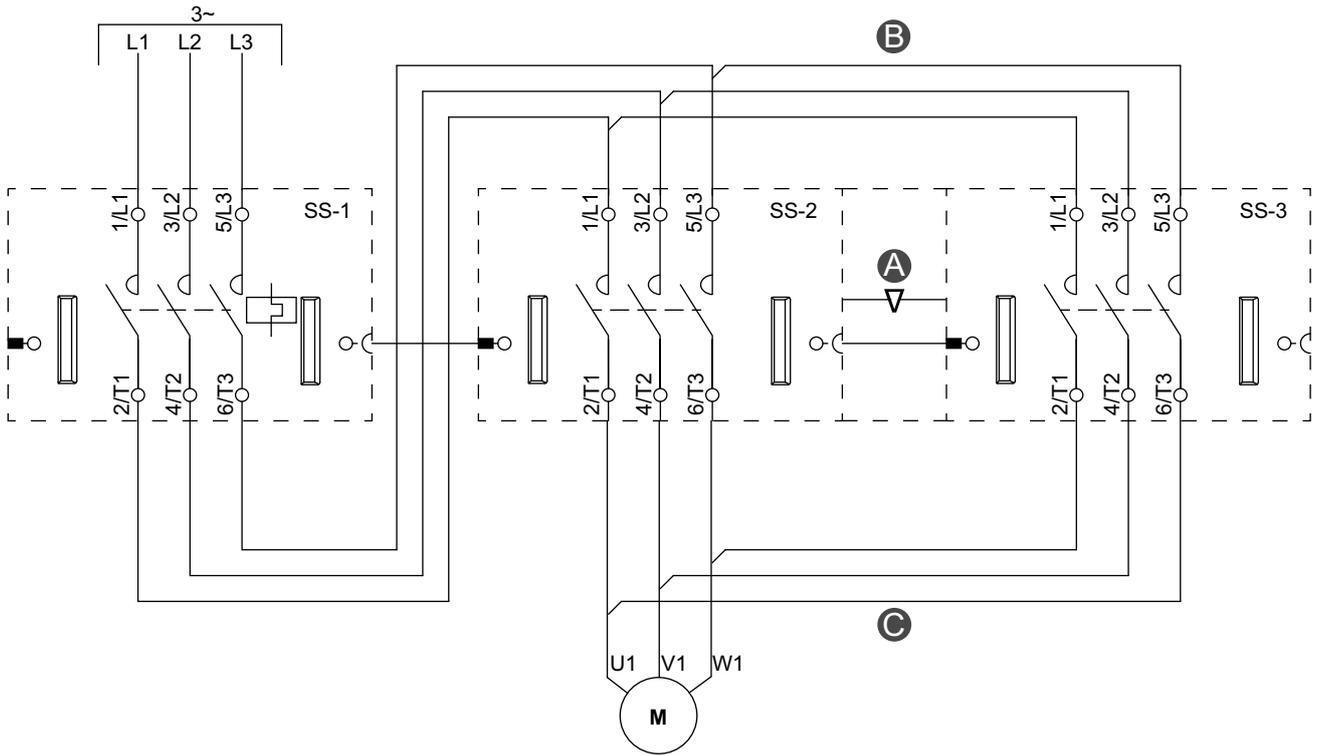


Figura 33 - Motor de dos velocidades— Parada de SIL, Cat. cableado 3/4

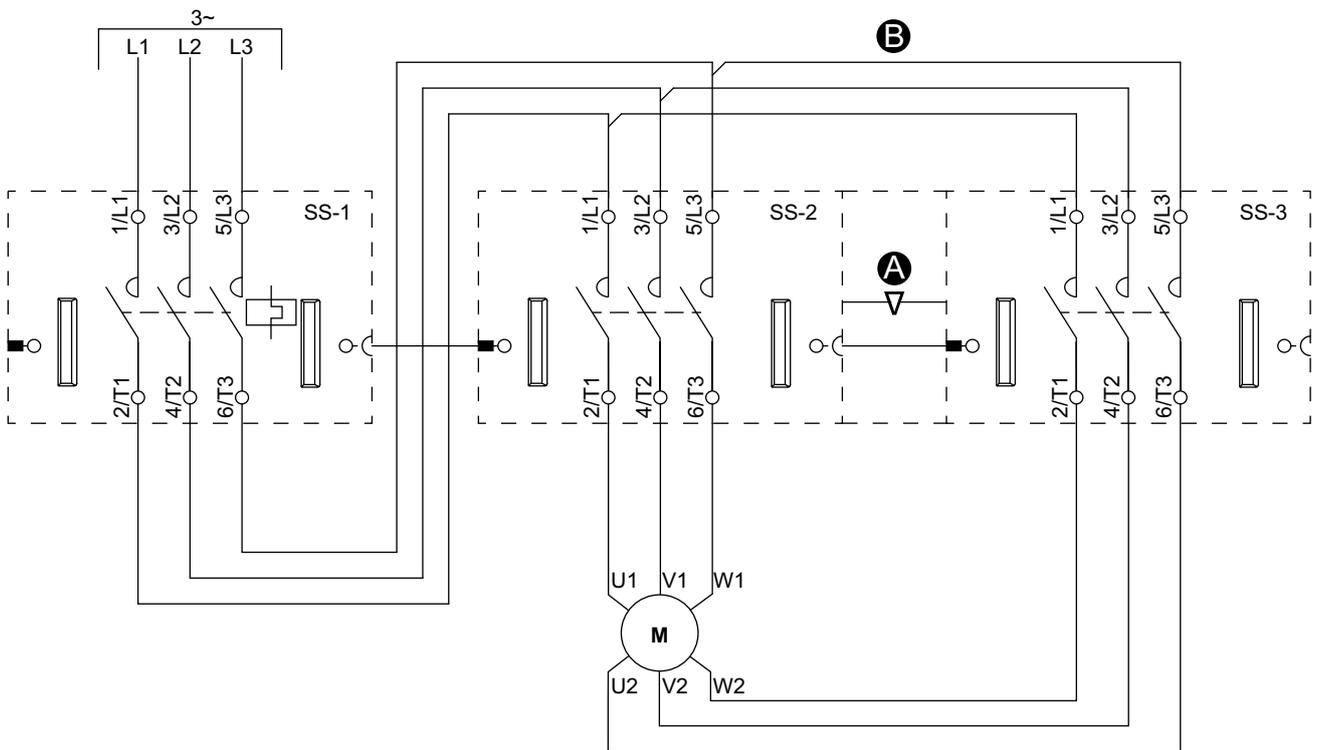


Figura 34 - Motor de dos velocidades y dos direcciones - Parada SIL, Cat. cableado 3/4

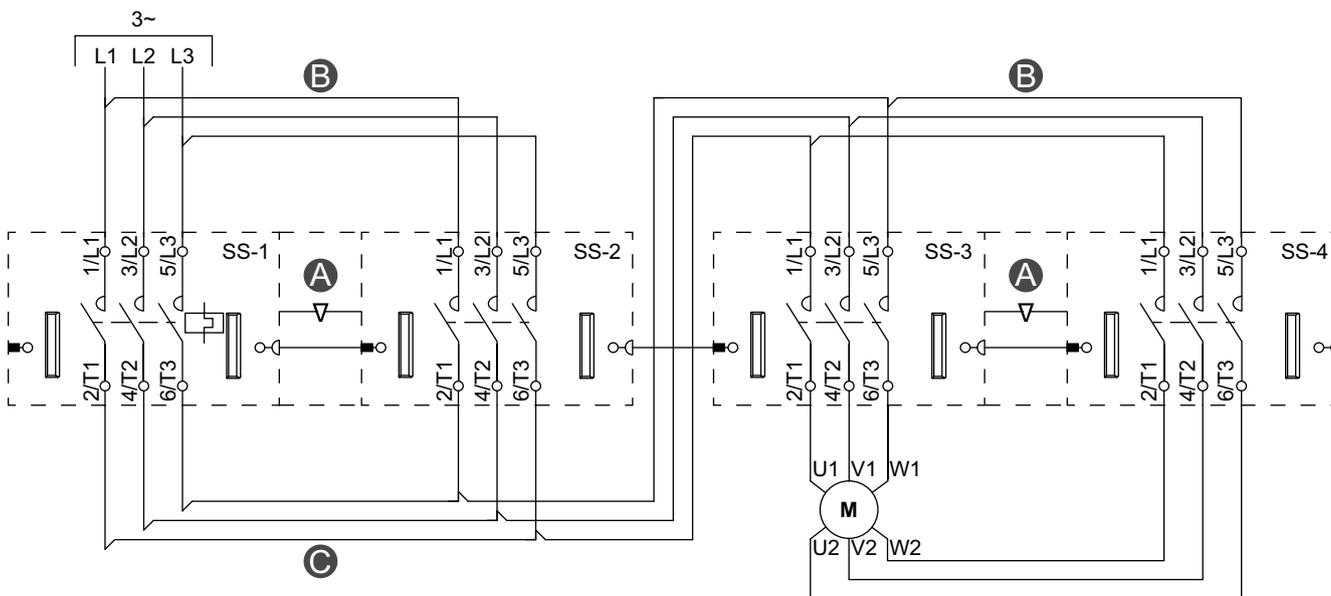


Figura 35 - Cinta transportadora de una dirección - Parada SIL, Cat. cableado 1/2

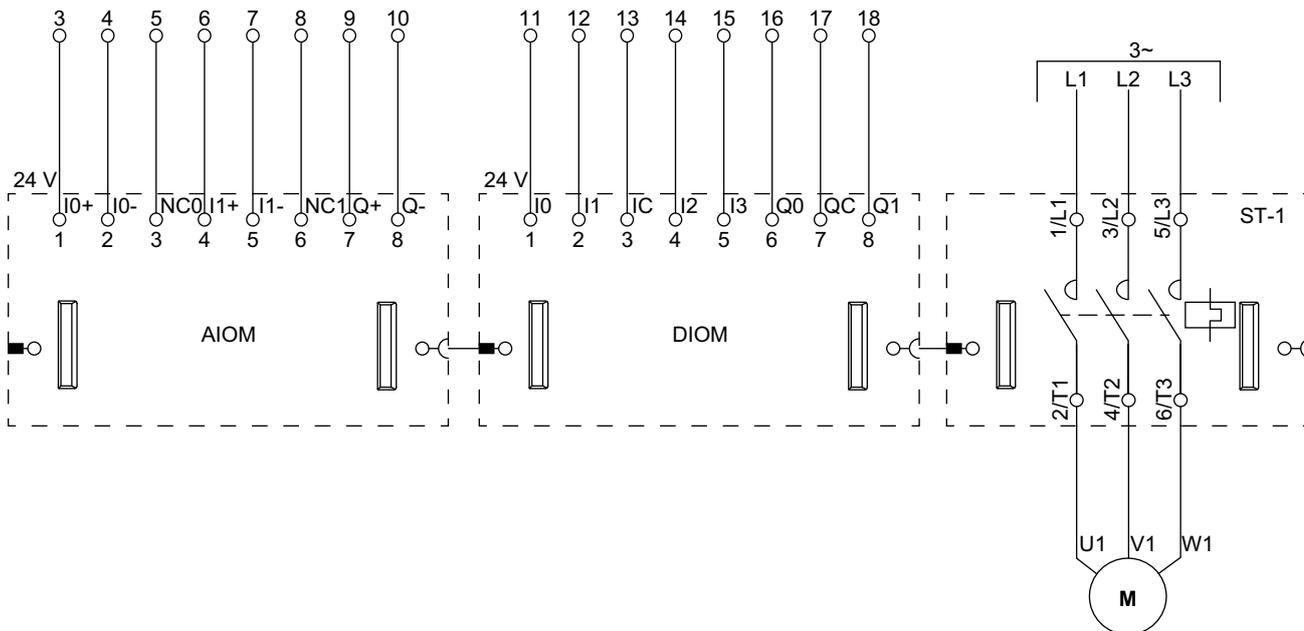
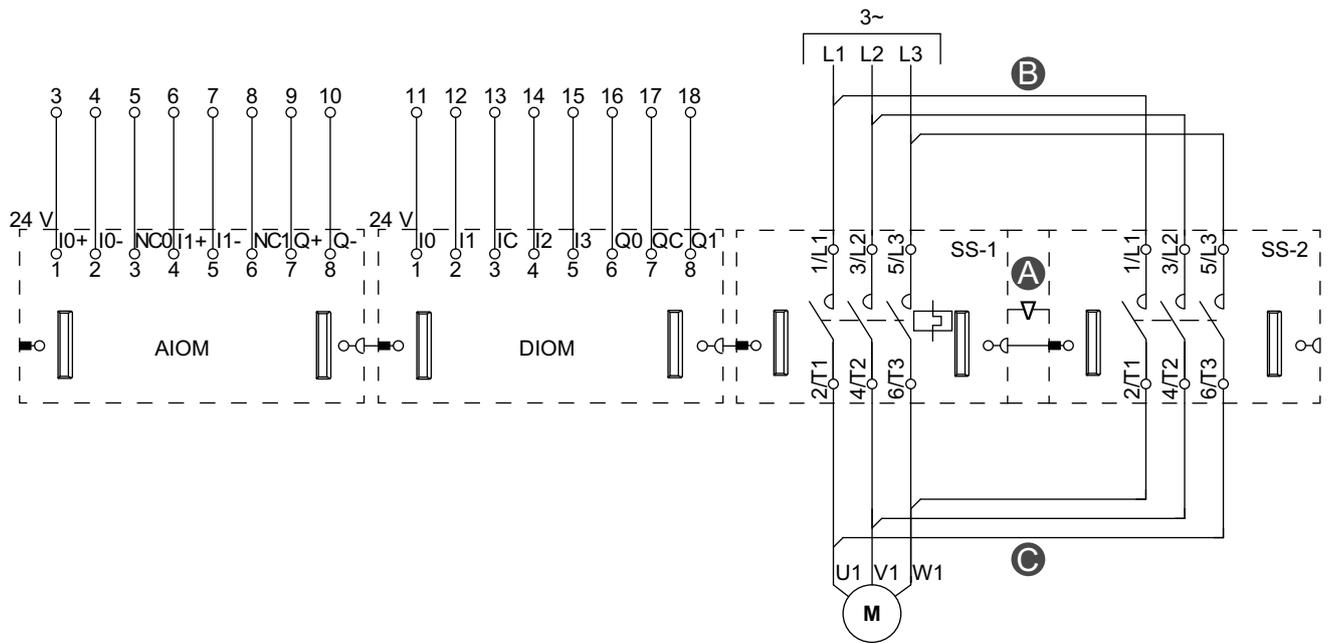


Figura 36 - Cinta transportadora de dos direcciones - Parada SIL, Cat. cableado 1/2



Puesta en marcha de la función de seguridad

Utilice este procedimiento para la puesta en marcha de la función de seguridad. El procedimiento incluye dos pasos:

- Pruebas de instalación
- Comprobaciones de la función de seguridad⁵²

Pruebas de instalación

Siga los pasos de la siguiente tabla para probar la instalación de la función de seguridad.

Tabla 23 - Prueba de instalación

1	Utilizando el panel DIAGNÓSTICO de TeSys™ island DTM, verifique que la topología física coincide con la topología lógica.
2	Utilizando el panel MI AVATAR de TeSys island DTM, verifique en los PARÁMETROS DE AVATAR que todos los Avatares SIL ⁵³ están asociados al grupo SIL correcto.

Comprobación de la función de seguridad

La comprobación de la función de seguridad se lleva a cabo en cada grupo SIL⁵³ de la isla. Un grupo SIL puede estar formado por varios avatares SIL gestionados por un módulo de interfaz SIL (SIM).

La comprobación de la función de seguridad tiene un resultado positivo si al activar el dispositivo de parada de emergencia asociado a un grupo SIL todos los arrancadores SIL pertenecientes a ese grupo SIL acceden al estado seguro (la carga se desconecta).

NOTA: Para la Categoría de parada 0 (parada no controlada), la parada debe ser inmediata. En la Categoría de parada 1 (parada controlada), la parada se hace efectiva tras un retardo.⁵⁴

Siga los pasos indicados en la siguiente tabla para cada grupo SIL de la isla para llevar a cabo la comprobación de la función de seguridad.

52. Comprobación de acuerdo con la norma IEC 62061

53. Nivel de integridad de la seguridad según la norma IEC 61508.

54. Categoría de parada 0 y Categoría de parada 1 según la norma EN/IEC 60204-1.

Tabla 24 - Comprobación de la función de seguridad

1	<p>Active el dispositivo de parada de emergencia asociado al grupo SIL y compruebe que todos los arrancadores SIL pertenecientes al grupo accedan al estado seguro (la carga se desconecta).</p> <p>NOTA: El LED de estado del dispositivo (DS) se iluminará en rojo en los arrancadores SIL, lo que indica un estado de Evento menor de dispositivo.</p> <p>Si no se supera la comprobación:</p> <ul style="list-style-type: none"> • Es posible que el dispositivo de parada de emergencia se haya conectado a un SIM incorrecto. Compruebe estas conexiones. • Es posible que el dispositivo de parada de emergencia no esté correctamente cableado al SIM. Compruebe estas conexiones. • Es posible que algunos avatares SIL no estén conectados al grupo SIL esperado. Compruebe la configuración.
2	<p>En el panel AVATARES del DTM u OMT de TeSys™ island, en la sección DIAGNÓSTICO, consulte el ESTADO y los REGISTROS DE EVENTOS para verificar que el Estado de grupo SIL sea igual a "Comando de parada". En el registro de eventos aparecerá "Comando de parada de Grupo SIL, Estado seguro alcanzado".</p> <p>Si no se supera la comprobación:</p> <ul style="list-style-type: none"> • Es posible que algunos avatares SIL no estén conectados al grupo SIL esperado. Compruebe la configuración.
3	<p>En la sección DISPOSITIVOS del panel DIAGNÓSTICO, verifique que el Estado del módulo de interfaz SIL (SIM) sea igual a "Comando de parada". En el registro de eventos aparecerá "Comando de parada de Grupo SIL, Estado seguro alcanzado".</p> <p>Si no se supera la comprobación:</p> <ul style="list-style-type: none"> • Es posible que el dispositivo de parada de emergencia se haya conectado a un SIM incorrecto. Compruebe estas conexiones. • Es posible que el dispositivo de parada de emergencia no esté correctamente cableado al SIM. Compruebe estas conexiones.
4	<p>Aplique un comando de inicio a un avatar SIL perteneciente al grupo SIL y verifique que el inicio no se haya producido con éxito: los arrancadores deben permanecer abiertos y el comando de inicio debe omitirse hasta que no se haya restablecido el dispositivo de parada de emergencia.</p> <p>Si no se supera la comprobación:</p> <ul style="list-style-type: none"> • Es posible que algunos avatares SIL no estén conectados al grupo SIL esperado. Compruebe la configuración. <p>Si no se supera cualquiera de estas comprobaciones pese a las medidas correctivas, deje de utilizar la isla. Sustituya los dispositivos que no superen las comprobaciones.</p>
5	<p>Una vez completada la comprobación de la función de seguridad, restablezca el dispositivo de parada de emergencia y verifique que todos los arrancadores SIL y los módulos de interfaz SIL estén en el estado Preparado (con el LED DS en verde fijo).</p>

Requisitos de mantenimiento de la función de seguridad

En esta sección se describe la rutina de mantenimiento requerida para preservar la seguridad funcional en su TeSys™ island.

Programa de mantenimiento

Los intervalos de mantenimiento dependen del modo de frecuencia.

- Para el modo de baja frecuencia (el número medio anual de ciclos del contactor es inferior a 15 ciclos/hora), realice el mantenimiento cada 12 meses.
- Para el modo de alta frecuencia (el número medio anual de ciclos del contactor es superior a 15 ciclos/hora o 136.986 ciclos/año), realice el mantenimiento en intervalos que se correspondan con una décima parte de la vida útil estimada del dispositivo.

La vida útil estimada del dispositivo (años) = $B10d (=1.369.863) / \text{número medio anual de ciclos del contactor}$

Comprobaciones de mantenimiento

Comprobaciones de uso de un dispositivo

Lleve a cabo las comprobaciones descritas en la siguiente tabla para verificar que los ciclos del contactor del arrancador SIL⁵⁵ están dentro de los límites de vida útil aceptables.

1	Utilizando la función DIAGNÓSTICO de dispositivos de TeSys™ island DTM u OMT, acceda a la información de activos de dispositivo de cada arrancador SIL.
2	Si el Número de ciclos del contactor es superior al $B10d (=1.369.863)$, sustituya el arrancador SIL.
3	Si no, utilice el valor del Número de ciclos del contactor para programar el siguiente mantenimiento. Consulte la sección Programa de mantenimiento, página 68.

Comprobación de la función de seguridad

Lleve a cabo la comprobación de la función de seguridad en cada grupo SIL⁵⁵. Consulte la sección Comprobación de la función de seguridad, página 66.

55. Nivel de integridad de la seguridad según la norma IEC 61508.

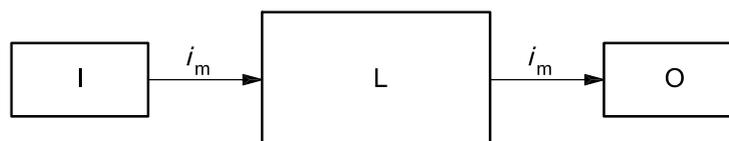
Apéndice: Arquitectura de canal único

Esta arquitectura de canal único engloba las Categorías de cableado 1 y 2.

Requisitos de la arquitectura para la Categoría de cableado 1

La arquitectura designada para la **Categoría 1** se define en la norma EN ISO 13849-1, 6.2.4.

Figura 37 - Arquitectura designada para la Categoría 1 (EN ISO 13849-1)



I: dispositivo de entrada

L: lógica

O: dispositivo de salida

im: medios de interconexión

SRP/CS, la pieza del sistema de control relacionada con la seguridad, con Categoría de cableado 1, debe designarse y crearse utilizando **componentes bien probados**.

Un “componente bien probado” para una aplicación relacionada con la seguridad es un componente que:

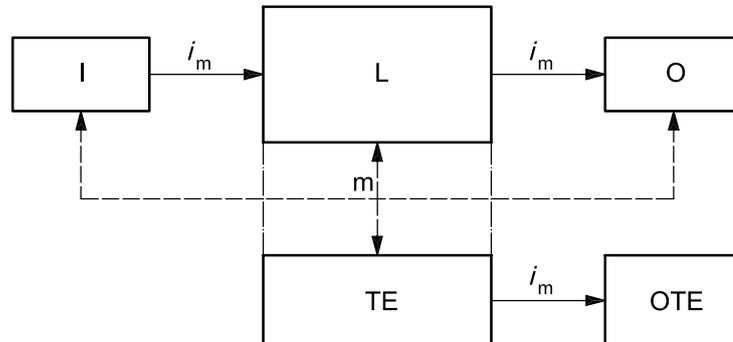
- se ha utilizado extensamente en el pasado con resultados positivos en aplicaciones similares, o bien
- se ha fabricado y verificado utilizando principios que demuestran su idoneidad y fiabilidad para aplicaciones relacionadas con la seguridad.

No hay cobertura de diagnóstico ($DC_{avg} = \text{ninguna}$) dentro de los sistemas de Categoría 1.

Requisitos de la arquitectura para la Categoría de cableado 2

La arquitectura designada para la **Categoría 2** se define en la norma EN ISO 13849-1, 6.2.5.

Figura 38 - Arquitectura designada para la Categoría 2 (EN ISO 13849-1)



I: dispositivo de entrada

L: lógica

O: dispositivo de salida

im: medios de interconexión

m: supervisión

TE: equipo de prueba

OTE: salida del TE

SRP/CS, la pieza del sistema de control relacionada con la seguridad, con Categoría de cableado 2, debe designarse de forma que su función o funciones se comprueben a intervalos adecuados a través del sistema de control de la máquina.

En las arquitectura de canal único, un SIM se asocia con un arrancador SIL⁵⁶.

Más concretamente, para la Categoría de cableado 2, el contacto de espejo está conectado al módulo Preventa™ XPS (o equivalente). Si el estado de la línea de retroalimentación del contacto de espejo no es igual al estado de la salida del módulo Preventa XPS (o equivalente), el módulo Preventa XPS (o equivalente) bloquea un segundo inicio.

NOTA: La retroalimentación del contacto de espejo solo proporciona información de diagnóstico.

56. Nivel de integridad de la seguridad según la norma IEC 61508.

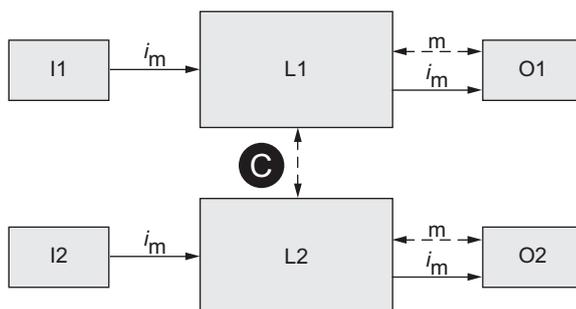
Apéndice: Arquitectura de doble canal

Esta arquitectura de doble canal engloba las Categorías de cableado 3 y 4.

Requisitos de la arquitectura para la Categoría de cableado 3

La arquitectura designada para la Categoría 3 se define en la norma EN ISO 13849-1, 6.2.6.

Figura 39 - Arquitectura designada para la Categoría 3 (EN ISO 13849-1)



im: medios de interconexión

c: supervisión cruzada

I1, I2: dispositivo de entrada; p. ej.: sensor

L1, L2: lógica

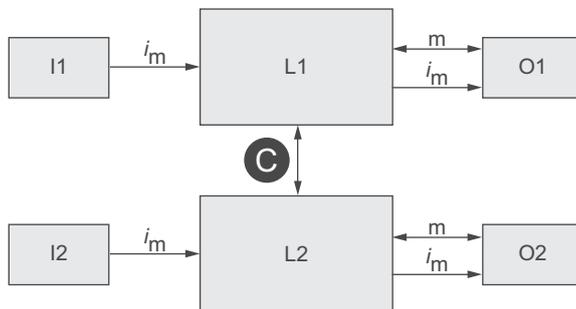
m: supervisión

O1, O2: dispositivo de salida; p. ej.: contactor principal

Requisitos de la arquitectura para la Categoría de cableado 4

La arquitectura designada para la Categoría 4 se define en la norma EN ISO 13849-1, 6.2.7.

Figura 40 - Arquitectura designada para la Categoría 4 (EN ISO 13849-1)



im: medios de interconexión

c: supervisión cruzada

I1, I2: dispositivo de entrada; p. ej.: sensor

L1, L2: lógica

m: supervisión

O1, O2: dispositivo de salida; p. ej.: contactor principal

Las líneas continuas para la supervisión representan una cobertura de diagnóstico que es más alta que en la arquitectura designada para la categoría 3.

Glosario

A

Frecuencia media de fallo peligroso [h⁻¹] (PFH). (Fallo peligroso conforme a la definición de IEC 61508-4)

Para mantener la función de seguridad, la norma IEC 61508 exige diversos niveles de medidas para evitar y controlar los errores detectados, dependiendo del SIL requerido⁵⁷.

Todos los componentes de una función de seguridad deben someterse a una evaluación de probabilidad con el fin de determinar la eficacia de las medidas implementadas para el control de los fallos detectados.

Esta evaluación determina la PFH (Frecuencia media de fallo peligroso⁵⁸ [h⁻¹]) para un sistema relacionado con la seguridad. Esta es la probabilidad por hora con la que un sistema relacionado con la seguridad falla de una forma peligrosa y la función de seguridad no puede ejecutarse correctamente.

Dependiendo del SIL, la PFH no debe superar determinados valores en todo el sistema relacionado con la seguridad.

Se añaden los valores individuales de PFH de una cadena de funciones. El resultado no debe superar el valor máximo establecido por la norma.

Nivel de integridad de seguridad	Frecuencia media de fallo peligroso ⁵⁸ [h ⁻¹] (PFH) con alta demanda o demanda continua
4	$10^{-9} \leq \text{---} < 10^{-8}$
3	$10^{-8} \leq \text{---} < 10^{-7}$
2	$10^{-7} \leq \text{---} < 10^{-6}$
1	$10^{-6} \leq \text{---} < 10^{-5}$

E

Norma EN ISO 13849

Esta Norma europea especifica el proceso de validación, incluyendo el análisis de peligros, la evaluación de riesgos y el ensayo para las funciones de seguridad y las categorías para las piezas de sistemas de control relacionadas con la seguridad. La norma ISO 13849-1 incluye descripciones de las funciones de seguridad y los requisitos de las categorías, además de cubrir los principios generales para el diseño. Algunos requisitos para la validación son generales y otros son específicos para la tecnología utilizada. La norma EN ISO 13849-2 también establece las condiciones bajo las que debe llevarse a cabo la validación mediante el ensayo de las piezas de sistemas de control relacionadas con la seguridad.

Norma EN/IEC 60204-1

La Categoría de parada 0 se define como la “detención de una función mediante la eliminación inmediata de la potencia en los actuadores de la máquina (es decir, una parada no controlada)”.

57. Nivel de integridad de la seguridad según la norma IEC 61508.

58. Fallo peligroso conforme a la definición de IEC 61508-4

La Categoría de parada 1 se define como “una parada controlada con potencia disponible para que los actuadores de la máquina alcancen la parada y a continuación eliminen la potencia una vez alcanzada la parada”.

F

Medidas para evitar fallos

Deben evitarse todo lo posible los errores en las especificaciones, en el hardware y en el software, así como los fallos en el uso y en el mantenimiento del sistema relacionado con la seguridad. Para cumplir estos requisitos, la norma IEC 61508 establece una serie de medidas para evitar fallos que deben implementarse dependiendo del SIL requerido⁵⁹. Estas medidas para evitar fallos deben abarcar todo el ciclo de vida del sistema relacionado con la seguridad, es decir, desde el diseño hasta el desmantelamiento del sistema.

Seguridad funcional

La automatización y la ingeniería de seguridad funcional son dos áreas que en el pasado eran totalmente independientes, pero que recientemente se han integrado bastante.

La ingeniería y la instalación de soluciones de automatización complejas se simplifican a través de soluciones de seguridad integradas.

Normalmente, los requisitos de ingeniería de seguridad funcional dependen de la aplicación.

El nivel de los requisitos deriva del riesgo y del potencial de peligro que surge de cada aplicación específica.

H

Tolerancia de fallo de hardware (HFT) y Fracción de fallo seguro (SFF)

Dependiendo del SIL⁵⁹ para el sistema relacionado con la seguridad, la norma IEC 61508 exige una tolerancia a fallos de hardware (HFT) específica en relación con una proporción concreta de fallos seguros, mostrada como Fracción de fallo seguro (SFF).

La HFT es la capacidad de un sistema de ejecutar la función de seguridad requerida pese a la presencia de uno o más fallos de hardware.

La SFF de un sistema se define como la relación del índice de fallos seguros con el índice total de fallos del sistema.

De acuerdo con la norma IEC 61508, el SIL máximo alcanzable de un sistema parcialmente está determinado por la HFT y la SFF del sistema.

Estos tipos se especifican basándose en criterios que determina la norma para los elementos relacionados con la seguridad.

SFF	HFT Subsistema Tipo A			HFT Subsistema Tipo B		
	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

59. Nivel de integridad de la seguridad según la norma IEC 61508.

I

Norma IEC 61508

La norma IEC 61508 cubre la seguridad funcional de los sistemas relacionados con la seguridad eléctricos / electrónicos / electrónicos programables.

En lugar de un componente único, se considera como una unidad una cadena de funciones completa (por ejemplo, desde un sensor, pasando por las unidades de procesamiento lógico y hasta el actuador).

Esta cadena de funciones debe cumplir los requisitos del nivel de integridad de seguridad específico en conjunto.

L

Modo de demanda baja/alta

La norma IEC 61508 define el modo de funcionamiento de demanda de la función de seguridad:

- alta demanda o modo continuo (PFH)
- modo de baja demanda (PFDavg, PTI)

M

Tiempo medio hasta fallo peligroso (MTTF_d)

La norma ISO 13849-1 define el MTTF_d como el tiempo medio previsto hasta un fallo peligroso.

P

Nivel de rendimiento (PL)

La norma IEC 13849-1 define cinco niveles de rendimiento (PL) para las funciones de seguridad.

El nivel a es el nivel más bajo y el e es el más alto.

Los cinco niveles (a, b, c, d y e) se corresponden con cinco valores distintos de probabilidad media de fallo peligroso⁶⁰ por hora.

Nivel de rendimiento	Probabilidad de fallo peligroso ⁶⁰ por hora
e	$\geq 10^{-8}$ a $< 10^{-7}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$
a	$\geq 10^{-5}$ a $< 10^{-4}$

S

60. Fallo peligroso conforme a la definición de IEC 61508-4

Nivel de integridad de seguridad (SIL)

La norma IEC 61508 define cuatro niveles de integridad de seguridad (SIL) para las funciones de seguridad.

SIL 1 es el nivel de integridad más bajo y SIL 4 el más alto.

Un análisis de peligros y una evaluación de riesgos sirven como base para determinar el nivel de integridad de seguridad requerido.

Esto sirve para decidir si la cadena de funciones correspondiente debe considerarse como una función de seguridad, y también qué potencial de peligro debe cubrir.

Schneider Electric
800 Federal Street
01810 Andover, MA
EE. UU.

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

www.schneider-electric.com

Debido a que las normas, especificaciones y diseños cambian periódicamente, solicite la confirmación de la información dada en esta publicación.

© 2021 – Schneider Electric. Reservados todos los derechos

85361B1904ES-04