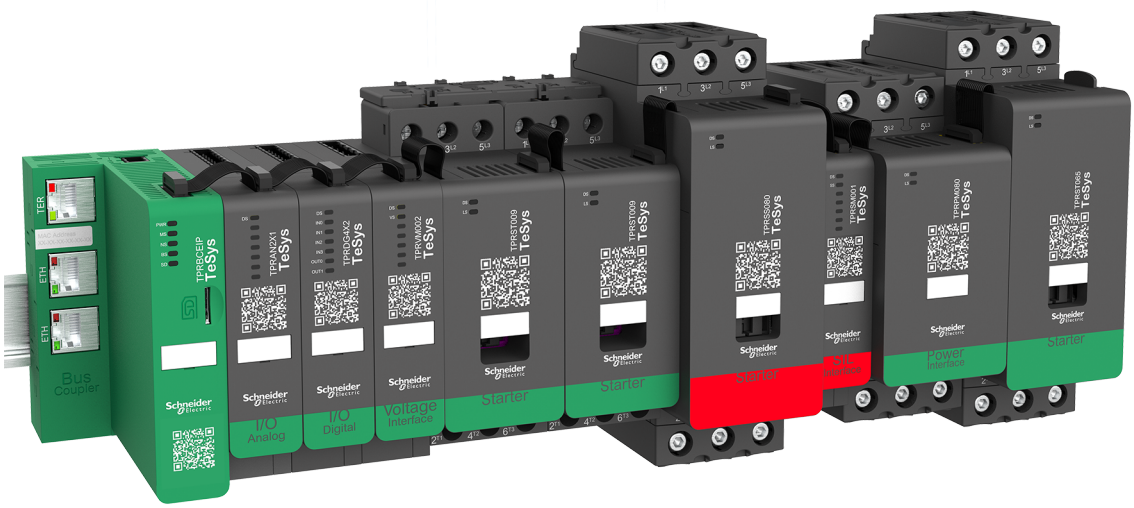
TeSys Active

TeSys™ island: soluzione di gestione dei motori digitali

Guida alla sicurezza funzionale

TeSys offre soluzioni innovative e di collegamento per gli starter.

8536IB1904IT-04
08/2023



Informazioni di carattere legale

Le informazioni contenute nel presente documento contengono descrizioni generali, caratteristiche tecniche e/o raccomandazioni relative ai prodotti/soluzioni.

Il presente documento non è inteso come sostituto di uno studio dettagliato o piano schematico o sviluppo specifico del sito e operativo. Non deve essere utilizzato per determinare idoneità o affidabilità dei prodotti/soluzioni per applicazioni specifiche dell'utente. Spetta a ciascun utente eseguire o nominare un esperto professionista di sua scelta (integratore, specialista o simile) per eseguire un'analisi del rischio completa e appropriata, valutazione e test dei prodotti/soluzioni in relazione all'uso o all'applicazione specifica.

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nel presente documento sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari.

Schneider Electric si riserva il diritto di apportare modifiche o aggiornamenti relativi al presente documento o ai suoi contenuti o al formato in qualsiasi momento senza preavviso.

Nella misura in cui sia consentito dalla legge vigente, Schneider Electric e le sue consociate non si assumono alcuna responsabilità od obbligo per eventuali errori od omissioni nel contenuto informativo del presente materiale, o per qualsiasi utilizzo non previsto o improprio delle informazioni ivi contenute.

Sommario

Informazioni di sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.

L'aggiunta di uno dei due simboli a un'etichetta di sicurezza di "Pericolo" o "Avvertenza" indica che sussiste un pericolo elettrico che potrebbe provocare lesioni personali in caso di mancato rispetto delle istruzioni.

Questo simbolo indica un allarme di sicurezza. Il suo scopo è avvertire l'utente di potenziali rischi di lesioni personali. Rispettare tutti i messaggi di sicurezza abbinati a questo simbolo per evitare eventuali lesioni o la morte.

⚠ PERICOLO

PERICOLO indica una situazione di pericolo che, se non evitata, **provoca** la morte o lesioni gravi.

⚠ AVVERTENZA

AVVERTENZA indica una situazione di pericolo che, se non evitata, **può provocare** la morte o lesioni gravi.

⚠ ATTENZIONE

ATTENZIONE indica una situazione di pericolo che, se non evitata, **può provocare** lesioni lievi o moderate.

AVVISO

AVVISO è utilizzato per indicare procedure non collegate a lesioni fisiche.

Nota

Le operazioni di installazione, utilizzo, riparazione e manutenzione del presente dispositivo elettrico devono essere eseguite esclusivamente da personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Informazioni sul manuale

Ambito del documento

Utilizzare questo documento per conoscere meglio le seguenti funzioni di sicurezza funzionale di TeSys™ island:

- comprensione generale
- aspetti chiave da considerare
- prestazioni
- descrizione dell'hardware
- configurazioni tipiche
- architetture campione
- riferimenti alle norme

Nota di validità

La presente guida è valida per tutte le configurazioni di TeSys island. La disponibilità di alcune funzioni descritte nel manuale dipende dal protocollo di comunicazione utilizzato e dai moduli fisici installati su TeSys island.

Per la conformità dei prodotti alle direttive ambientali, quali RoHS, REACH, PEP e EOLI, consultarewww.se.com/green-premium.

Per le caratteristiche tecniche dei moduli fisici descritti nella presente guida, consultare www.se.com.

Le caratteristiche tecniche presentate nella presente guida dovrebbero essere uguali a quelle visualizzate online. I contenuti potrebbero subire modifiche periodiche per migliorare la chiarezza e l'accuratezza. Se si nota una differenza tra le informazioni contenute nella presente guida e quelle online, fare riferimento alle informazioni online.

Documentazione correlata

Titolo documento	Descrizione	Numero del documento
Guida all'installazione e al funzionamento di TeSys island	Descrive le funzioni principali, l'installazione meccanica, il cablaggio e la messa in servizio di TeSys island e il modo in cui utilizzare e manutenere TeSys island.	DOCA0270IT
Guida rapida e libreria di blocchi di funzione di TeSys island e EtherNet/IP™	Descrive la modalità di integrazione di TeSys island e le informazioni relative alla libreria di TeSys island utilizzata nell'ambiente EtherNet/IP Rockwell Software® Studio 5000®.	DOCA0271IT
TeSys island, guida alla sicurezza funzionale	Descrive le caratteristiche della sicurezza funzionale di TeSys island.	8536IB1904IT
Guida ai blocchi di funzione di terze parti di TeSys island	Contiene informazioni utili per creare blocchi funzione per l'hardware di terze parti.	8536IB1905IT
Guida online del DTM di TeSys island	Descrive la modalità di installazione e uso di diverse funzioni del software di configurazione di TeSys islande la modalità di configurazione dei parametri di TeSys island.	8536IB1907IT
Profilo ambientale del prodotto di TeSys island	Contiene informazioni su materiali costitutivi, potenziale di riciclabilità e impatto ambientale di TeSys island.	ENVPEP1904009
Istruzioni di fine vita del prodotto di TeSys island	Contiene le istruzioni per lo smaltimento di TeSys island.	ENVEOLI1904009
Scheda di istruzioni, bus coupler, TPRBCEIP di TeSys island	Descrive la modalità di installazione del bus coupler Ethernet/IP di TeSys island.	MFR44097
Scheda di istruzioni, bus coupler, TPRBCPFN di TeSys island	Descrive la modalità di installazione del bus coupler PROFINET di TeSys island.	MFR44098
Scheda di istruzioni, bus coupler, TPRBCPFB di TeSys island	Descrive la modalità di installazione del bus coupler PROFIBUS DP di TeSys island.	GDE55148
Foglio di istruzioni, starter e moduli di interfaccia di alimentazione, dimensioni 1 e 2, di TeSys island	Descrive la modalità di installazione degli starter e delle interfacce di alimentazione di dimensioni 1 e 2 di TeSys island.	MFR77070
Foglio di istruzioni, starter e moduli di interfaccia di alimentazione, dimensione 3, di TeSys island	Descrive la modalità di installazione degli starter e delle interfacce di alimentazione di dimensione 3 di TeSys island.	MFR77085
TeSys island, scheda di istruzioni dei moduli di ingresso/uscita	Descrive la modalità di installazione dei moduli I/O analogici e digitali di TeSys island.	MFR44099
TeSys island, scheda di istruzioni dei moduli interfaccia SIL e interfaccia tensione	Descrive la modalità di installazione dei moduli interfaccia di tensione e SIL [1] di TeSys island.	MFR44100

1. Livello di integrità della sicurezza secondo la norma IEC 61508

Terminologia derivata dalle norme

I termini tecnici, la terminologia e le descrizioni corrispondenti in questa guida utilizzano generalmente i termini o le definizioni delle norme pertinenti. Di seguito sono indicate alcune di queste norme.

- **EN ISO 13849-1:** sicurezza del macchinario. Parti dei sistemi di comando legate alla sicurezza, parte 1: principi generali per la progettazione
- **EN ISO 13849-2:** sicurezza del macchinario. Parti dei sistemi di comando legate alla sicurezza, parte 2: convalida
- **IEC 61508:** sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili legati alla sicurezza
- **EN 62061:** sicurezza del macchinario. Sicurezza funzionale dei sistemi di comando elettrici, elettronici ed elettronici programmabili legati alla sicurezza
- **IEC 61511:** sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo
- **EN/IEC 60204-1:** sicurezza del macchinario. Equipaggiamento elettrico delle macchine, parte 1: requisiti generali
- **IEC 61000-6-7:** compatibilità elettromagnetica (EMC). Parte 6-7: norme generiche. Requisiti di immunità per dispositivi destinati a svolgere funzioni in un sistema legato alla sicurezza (sicurezza funzionale) in luoghi industriali
- **IEC 60664-5:** coordinamento dell'isolamento per le apparecchiature nei sistemi a bassa tensione, parte 5: metodo dettagliato per la determinazione delle distanze di isolamento in aria e superficiali inferiori o uguali a 2 mm
- **IEC 60947-4-1:** Interruttori e dispositivi di controllo a bassa tensione, parte 4-1: contattori e starter. Contattori e starter elettromeccanici
- **IEC 60947-5-1:** interruttori e dispositivi di controllo a bassa tensione, parte 5-1: dispositivi di controllo ed elementi di commutazione. Dispositivi elettromeccanici di controllo
- **IEC 60947-7-1:** interruttori e dispositivi di controllo a bassa tensione, parte 7-1: apparecchiature ausiliarie. Morsetti per conduttori di rame
- **IEC 60947-7-2:** interruttori e dispositivi di controllo a bassa tensione, parte 7-2: apparecchiature ausiliarie. Morsetti componibili per conduttori di protezione in rame
- **EN 50205:** relè con contatti a guida forzata (meccanicamente vincolati)
- **IEC TR 62380:** banche dati di affidabilità. Modello generico per la previsione dell'affidabilità di componenti elettronici, schede elettroniche e apparecchiature

Terminologia sulla sicurezza funzionale

ATTENTION

La terminologia sulla sicurezza funzionale utilizzata in questa guida viene definita di seguito.

Termine	Norma	Definizione
Tolleranza ai guasti	IEC 61511-1	Capacità di un elemento funzionale di continuare a eseguire una funzione richiesta in presenza di guasti o errori
Sicurezza funzionale	IEC 61508-4	Parte della sicurezza generale relativa all'apparecchiatura sotto controllo (EUC) e al sistema di controllo EUC che dipende dal funzionamento corretto dei sistemi elettrici, elettronici ed elettronici programmabili legati alla sicurezza (E/E/PE) e altre misure di riduzione dei rischi
Guasto in sicurezza	IEC 61508-4	Guasto di un elemento e/o sottosistema e/o sistema che svolge un ruolo nell'implementazione della funzione di sicurezza la quale: 1. determina il funzionamento non corretto della funzione di sicurezza per mettere l'EUC[2] (o una parte) in uno stato sicuro oppure mantenere uno stato sicuro oppure 2. aumenta la probabilità del funzionamento non corretto della funzione di sicurezza di mettere l'EUC[2] (o una parte) in uno stato sicuro oppure mantenere uno stato sicuro.
Frazione guasti in sicurezza	IEC 61508-4	Il rapporto tra i guasti in sicurezza e i guasti totali del sistema.
Stato sicuro	IEC 61511-1	Stato del processo quando si raggiunge la sicurezza
	IEC 61800-5-2	Stato della PDS(SR)[3] quando si raggiunge la sicurezza
Safe stop	IEC 61800-5-2	Le funzioni di Safe stop vengono definite come segue: • **Safe Torque Off (STO)** ◦ Questa funzione consente di evitare che il motore riceva energia che produce forza. ◦ Questa *sottofunzione di sicurezza* corrisponde a un arresto non controllato conformemente alla categoria stop 0 di IEC 60204-1. • **Safe stop 1 (SS1)** ◦ Decelerazione Safe stop 1 controllata: SS1-d avvia e controlla la velocità di decelerazione del motore entro i limiti selezionati in modo da arrestare il motore ed eseguire la funzione STO (vedere 4.2.3.2) quando la velocità del motore scende al di sotto di un limite specificato oppure ◦ Rampa safe stop 1 monitorata: SS1-r avvia e monitora la velocità di decelerazione del motore entro i limiti selezionati in modo da arrestare il motore ed eseguire la funzione STO quando la velocità del motore scende al di sotto di un limite specificato oppure ◦ SS1-t safe stop 1 temporizzato avvia la decelerazione del motore ed esegue la funzione STO dopo un ritardo dell'applicazione specifico.
Funzione di sicurezza	IEC 61800-5-2	Funzione che deve essere implementata da parte di un sistema legato alla sicurezza o altra misura di riduzione dei rischi, destinata a raggiungere o mantenere uno stato sicuro per l'apparecchiatura o macchina azionata dalla PDS(SR)[3] in relazione a uno specifico evento pericoloso

2. EUC: apparecchiatura sotto controllo
3. Trasmissione di potenza legata alla sicurezza

Termine	Norma	Definizione
Livello di integrità di sicurezza (SIL)	IEC 61508	La norma IEC 61508 definisce i livelli di integrità di sicurezza (SIL) per le funzioni di sicurezza: SIL 1 è il livello di integrità più basso e SIL 4 il più alto. Un'analisi dei pericoli e una valutazione dei rischi costituiscono la base per stabilire il livello di integrità di sicurezza necessario.
Sistema legato alla sicurezza	IEC 61800-5-2	Sistema designato che • implementa le funzioni di sicurezza necessarie per raggiungere e mantenere uno stato sicuro per l'apparecchiatura o macchina azionata dalla PDS (SR)[4] e • destinato a raggiungere, autonomamente o con altre misure di riduzione dei rischi, la necessaria integrità di sicurezza per le funzione di sicurezza necessarie.
Sottosistema	IEC 61800-5-2	Parte del design dell'architettura di primo livello di un sistema legato alla sicurezza, il cui guasto compromette la funzione legata alla sicurezza

Dichiarazione di conformità CE

La dichiarazione di conformità CE per TeSys™ island è disponibile su www.schneider-electric.com.

4. Trasmissione di potenza legata alla sicurezza

Precauzioni

Leggere e comprendere le precauzioni seguenti prima di eseguire qualsiasi procedura indicata in questa guida.

⚠⚠PERICOLO

RISCHIO DI ELETTROCUZIONE, ESPLOSIONE O ARCHI ELETTRICI

- Le operazioni di installazione e di manutenzione di questa apparecchiatura devono essere effettuate solo da personale qualificato.
- Scollegare l'apparecchiatura da tutti i circuiti di alimentazione prima di qualsiasi intervento sull'apparecchiatura o all'interno di essa.
- Utilizzare esclusivamente la tensione specificata quando si utilizza questa apparecchiatura ed eventuali prodotti associati.
- Per verificare che l'alimentazione sia isolata usare sempre un rilevatore di tensione correttamente tarato.
- Utilizzare interblocchi adeguati qualora siano presenti pericoli per il personale e/o l'apparecchiatura.
- I circuiti delle linee elettriche devono essere cablati e protetti conformemente ai requisiti normativi locali e nazionali.
- Utilizzare dispositivi di protezione individuale (DPI) adeguati e conformarsi alle norme relative agli obblighi di sicurezza elettrica sui luoghi di lavoro ai sensi delle norme NFPA 70E, NOM-029-STPS o CSA Z462 o equivalenti locali.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO

- Per le istruzioni complete sulla sicurezza funzionale, consultare la Guida alla sicurezza funzionale di TeSys™ island, 8536IB1904.
- Non smontare, riparare o modificare questa apparecchiatura. Non sono presenti parti riparabili direttamente dall'utente.
- Installare e utilizzare questa apparecchiatura in un alloggiamento opportunamente tarato per l'ambiente applicativo previsto.
- Ogni utilizzo di questa apparecchiatura deve essere testato singolarmente e accuratamente per valutarne il funzionamento corretto prima di essere messo in servizio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ **AVVERTENZA:** questo prodotto può esporre l'utente a prodotti chimici, compreso l'ossido di antimonio (triossido di antimonio), sostanza cancerogena secondo lo Stato della California. Per ulteriori informazioni, consultare il sito www.P65Warnings.ca.gov.

Personale qualificato

Solo personale adeguatamente formato e in grado di comprendere il contenuto della presente guida e di tutta la documentazione relativa al prodotto è autorizzato a lavorare con questo sistema e su di esso.

Il personale qualificato deve essere in grado di rilevare possibili pericoli che potrebbero derivare dalla modifica dei valori dei parametri e in generale dall'apparecchiatura meccanica, elettrica o elettronica. Il personale qualificato deve conoscere perfettamente le norme, le disposizioni e le normative per la prevenzione degli incidenti industriali e deve attenersi a esse in fase di progettazione e implementazione del sistema.

L'uso e l'applicazione delle informazioni contenute nella presente guida richiedono esperienza nella progettazione e programmazione dei sistemi di controllo automatizzati. Solo l'utente, il costruttore delle macchine o l'integratore possono conoscere tutte le condizioni e tutti i fattori presenti durante l'installazione, la configurazione, il funzionamento e la manutenzione della macchina o del processo e possono determinare l'automazione e le apparecchiature associate e i dispositivi di sicurezza e interblocchi correlati che sia possibile utilizzare in modo efficace e corretto.

Durante la scelta delle apparecchiature di automazione e controllo, e di eventuali altre apparecchiature o software correlato per una particolare applicazione, prendere in considerazione anche le norme e/o normative locali, regionali o nazionali applicabili.

È importante attenersi a ogni informazione di sicurezza, requisito elettrico e standard normativo applicabile alla macchina o processo nell'uso di questa apparecchiatura.

Uso previsto

I prodotti descritti nella presente guida, insieme a software, accessori e opzioni, sono starter per carichi elettrici a bassa tensione, destinati all'uso industriale conformemente alle istruzioni, indicazioni, esempi e informazioni di sicurezza contenuti in questo documento e in altra documentazione di supporto.

Il prodotto può essere utilizzato solo conformemente a tutte le normative e direttive di sicurezza applicabili, ai requisiti specifici e ai dati tecnici.

Prima di utilizzare il prodotto, è necessario eseguire un'analisi dei pericoli e una valutazione dei rischi dell'applicazione pianificata. In base ai risultati, adottare adeguate misure collegate alla sicurezza.

Poiché il prodotto viene utilizzato come componente di una macchina o processo, garantire la sicurezza delle persone per mezzo della struttura del sistema complessiva.

Utilizzare il prodotto solo con i cavi e gli accessori specificati. Utilizzare esclusivamente accessori e ricambi originali.

Qualsiasi altro utilizzo diverso da quello espressamente consentito è proibito e può causare pericoli imprevisti.

Panoramica sulla sicurezza funzionale di TeSys™ island

Intervallo master: TeSys

TeSys™ è una soluzione innovativa di controllo e gestione del motore prodotto dal leader di mercato mondiale. TeSys offre efficienti prodotti e soluzioni di connessione per la commutazione e la protezione di motori e carichi elettrici in conformità a tutte le principali norme elettriche globali.

Concetto di TeSys island

TeSys island è un sistema multifunzionale modulare dotato di funzioni integrate all'interno di un'architettura di automazione, principalmente per il controllo e la gestione diretti di carichi a bassa tensione. TeSys island può commutare, proteggere e gestire motori e altri carichi elettrici fino a 80 A (AC1) installati in un quadro elettrico di comando.

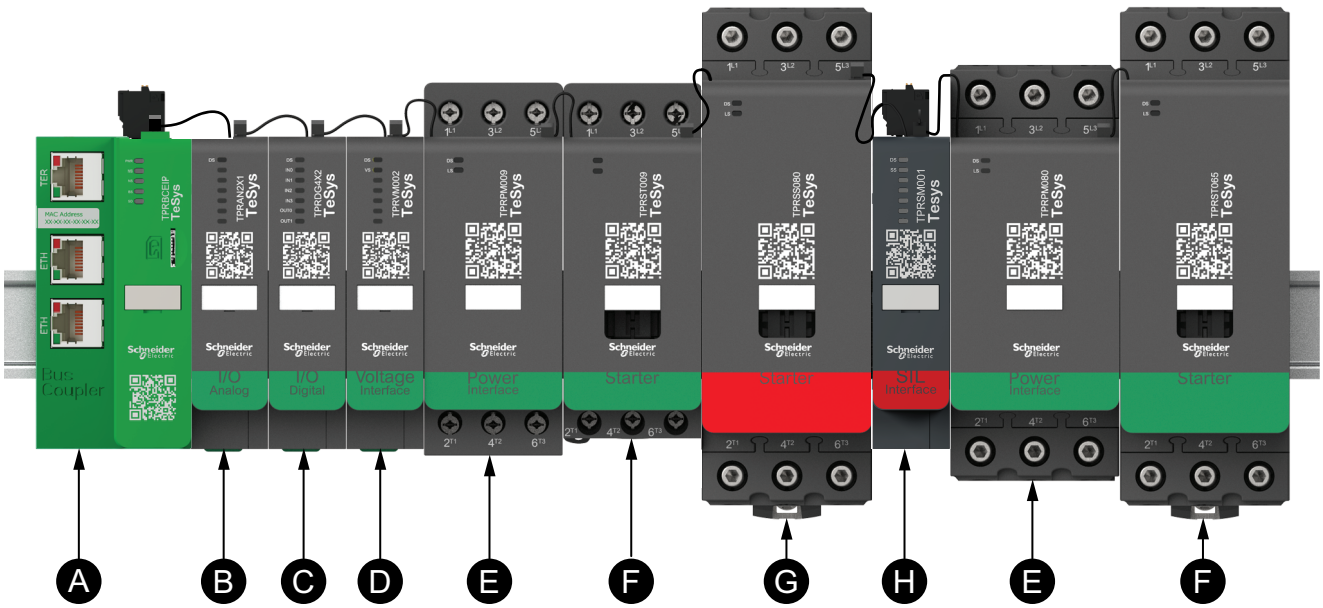
Questo sistema si basa sul concetto di TeSys avatars. Gli avatars:

- Rappresentano sia gli aspetti logici che fisici delle funzioni di automazione
- Determinano la configurazione di TeSys island

Gli aspetti logici diTeSys island sono gestiti tramite degli strumenti software che coprono tutte le fasi di vita del prodotto e dell'applicazione: progettazione, ingegnerizzazione, messa in servizio, funzionamento e manutenzione.

Il TeSys island è costituito da un set di dispositivi installati su un'unica guida DIN e collegati insieme con cavi piatti che assicurano la comunicazione interna tra i moduli. La comunicazione esterna con l'ambiente di automazione avviene su un singolo modulo bus coupler, per cui TeSys island viene visualizzato come un singolo nodo della rete. Gli altri moduli includono starter, interfaccia di potenza, moduli I/O analogici e digitali, moduli interfaccia di tensione e moduli interfaccia SIL (Safety Integrity Level ai sensi della norma IEC 61508), e coprono un'ampia gamma di funzioni operative.

Figura 1 - Panoramica di TeSys island



A	Bus coupler	E	Modulo di interfaccia di alimentazione
B	Modulo I/O analogico	F	Starter standard
C	Modulo I/O digitale	G	Starter SIL
D	Modulo di interfaccia della tensione	H	Modulo di interfaccia SIL

Sicurezza funzionale in TeSys island

TeSys™ island fornisce avatar specifici e dispositivi fisici per creare configurazioni per le funzioni della categoria stop 0 e 1 secondo la norma EN/IEC 60204-1. Gli avatar TeSys sono rappresentazioni digitali dei moduli fisici sull'isola, tuttavia, la funzione di sicurezza di TeSys island si basa solo sui componenti hardware elettromeccanici. I dispositivi specifici sono lo starter SIL[5] e il modulo interfaccia SIL. Un altro concetto importante è il gruppo SIL: una serie di avatar associati a un modulo interfaccia SIL e che seguono la stessa funzione di sicurezza. In un'isola possono essere presenti più gruppi SIL.

TeSys island deve essere integrato con altri elementi legati alla sicurezza in un sistema legato alla sicurezza più ampio per garantire la sicurezza funzionale di una macchina o di un sistema/processo.

5. Livello di integrità della sicurezza secondo la norma IEC 61508.

Caratteristiche di sicurezza funzionale di TeSys island

TeSys™ island fornisce funzioni di sicurezza funzionale conformemente a queste condizioni specifiche:

Norme e caratteristiche certificate

TeSys island rispetta queste direttive e norme:

- Direttiva macchine 2006/42/CE:
  - EN ISO 13849-1: 2015
  - EN 62061: 2016 o IEC 62061: 2015 (edizione 1.2)
- Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili legati alla sicurezza: IEC 61508 edizione 2: 2010
- Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo: IEC 61511 edizione 2: 2016
- Le funzioni categoria stop 0 e categoria stop 1 di TeSys island rispettano la norma EN/IEC 60204-1.

Nel canale singolo, le prestazioni migliori per queste funzioni sono le seguenti:

- Livello prestazioni "d" Categoria 2 ai sensi della norma EN ISO 13849-1
- SIL[6] Capacità 2 conforme alla norma IEC 61508 ed. 2 e IEC 61511 ed. 2
- Capacità SIL CL 2 conforme alla norma EN 62061 ed. 1

Nel canale doppio, le prestazioni migliori per queste funzioni sono le seguenti:

- Livello prestazioni "e" Categoria 4 ai sensi della norma EN ISO 13849-1.
- Capacità SIL 3 conforme alla norma IEC 61508 ed. 2 e IEC 61511 ed. 2
- Capacità SIL CL 3 conforme alla norma EN 62061: 2016 o IEC 62061: 2015 (edizione 1.2)

TeSys island è progettato in modo da supportare diversi livelli di prestazioni di sicurezza funzionale e livelli di integrità della sicurezza a seconda dell'architettura di cablaggio ed è conforme alle caratteristiche di sicurezza funzionale seguenti:

Tabella 1 - Caratteristiche della sicurezza funzionale

Funzione	Funzione di stop legata alla sicurezza	
Posizione di fallback	Contattore aperto	
Tempo di risposta (caso peggiore)	145 ms	
Categoria stop EN/IEC 60204-1	Cat. 0/Cat. 1	
Direttiva macchine	Sì	
Architettura del sistema TeSys island	Canale singolo	Canale doppio
Livello prestazioni EN ISO 13849-1	PL c, d	PL c, d, e

6. Livello di integrità della sicurezza secondo la norma IEC 61508.

Tabella 1 - Caratteristiche della sicurezza funzionale (Continuare)

Categoria cablaggio 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

La certificazione relativa alla sicurezza funzionale è accessibile su www.se.com/tesys/.

NOTA: Per la certificazione relativa agli aspetti funzionali, sarà considerato solo un TeSys island idoneo all'uso in applicazioni legate alla sicurezza, non il sistema completo nel quale è integrato, per garantire la sicurezza funzionale di una macchina o di un sistema/processo.

Condizioni di esercizio

TeSys island è progettato per funzionare alle condizioni seguenti. Altre condizioni possono essere valide per moduli specifici come descritto nella relativa scheda tecnica, disponibile all'indirizzo www.se.com/tesys-island.

- Temperatura ambiente 40 °C
- Motore 400 o 480 V
- Umidità 50%
- Carico 80%
- Installazione orizzontale
- Tutti gli ingressi attivati
- Tutte le uscite attivate
- Tempo di funzionamento 24 ore/giorno, 365 giorni/anno

Architettura a canale singolo (ISO 13849)

TeSys island è applicabile ad architetture a canale singolo nelle quali il rilevamento di un guasto può causare la perdita della funzione di sicurezza.

Architettura a doppio canale (ISO 13849)

TeSys island è applicabile ad architetture a doppio canale nelle quali il rilevamento di un guasto singolo (compresi gli errori in modalità comune) non causa la perdita della funzione di sicurezza.

Categorie stop (EN/IEC 60204-1)

La categoria di stop si riferisce al modo in cui il carico azionato viene disattivato e dipende dal sottosistema esterno legato alla sicurezza che attiva la funzione di stop. Un sottosistema esterno legato alla sicurezza può essere implementato con dispositivi quali i moduli Preventa™ XPS.

Categoria stop 0

La categoria stop 0 è definita come l'arresto del movimento della macchina tramite la disattivazione immediata dell'alimentazione elettrica degli attuatori della macchina. La categoria stop 0 è uno stop non controllato.

Categoria stop 1

La categoria stop 1 è definita come l'arresto del movimento della macchina con l'alimentazione elettrica ancora presente negli attuatori della macchina durante la procedura di stop. L'alimentazione viene rimossa quando lo stop è completo. La categoria stop 1 è uno stop controllato.

Categoria cablaggio[7]

Le categorie del cablaggio riguardano il modo in cui il modulo Preventa™ XPS (o equivalente) esterno viene cablato e il livello di controllo aggiuntivo sulla funzione di sicurezza associato.

Categoria cablaggio 1

Un singolo guasto rilevato può causare la perdita della funzione di sicurezza e non è necessaria alcuna copertura diagnostica.

L'elemento sensore legato alla sicurezza può essere collegato direttamente agli ingressi comuni SIL-IN/SIL.[8] Gli ingressi Mirror In/Mirror Out non vengono utilizzati. Per ulteriori informazioni sul cablaggio degli ingressi comuni SIL-IN/SIL, vedere Elemento sensore legato alla sicurezza, pagina 24.

Categoria cablaggio 2

L'elemento del sensore legato alla sicurezza è collegato via cavo al modulo Preventa XPS (o equivalente). Le uscite del modulo Preventa XPS (o equivalente) sono collegate via cavo agli ingressi comuni SIL-IN/SIL del modulo interfaccia SIL[9].

Per rispettare i requisiti per la categoria 2, il feedback del contatto mirror (Mirror In/Mirror Out) deve essere monitorato da un modulo Preventa XPS (o equivalente) che esegue il monitoraggio diagnostico esterno del contatto mirror. Se il contatto mirror non si chiude allo stop, il riavvio successivo viene impedito per tutti gli starter SIL nel gruppo SIL.

Implementazione del monitoraggio indiretto per la categoria 2

Per soddisfare i requisiti della categoria 2 per la copertura diagnostica (CC>60%), il monitoraggio esterno dello stato del gruppo deve essere implementato per attivare un meccanismo secondario al fine di arrestare la macchina (interruttore con bobina di trip ecc) o evitare l'accesso ad aree pericolose (blocco protezione).

7. Categorie cablaggio in conformità con ISO 13849.
8. Livello di integrità della sicurezza secondo la norma IEC 61508.
9. Livello di integrità della sicurezza secondo la norma IEC 61508

A ciascun gruppo SIL[10] sono associati cinque stati per indicare lo stato operativo. Lo stato 0 indica che non è presente un gruppo SIL in questa posizione. TeSys island supporta fino a 10 gruppi SIL nell'isola.

Stato del gruppo SIL per la funzione di SIL stop:

- 0 = gruppo SIL non presente nella configurazione del sistema
- 1 = gruppo SIL interessato da evento dispositivo avatar
- 2 = comando di stop ricevuto, starter SIL non ancora aperti
- 3 = comando di stop inviato correttamente, tutti gli starter SIL sono aperti
- 4 = comando di stop inviato solo a un canale di ingresso del modulo interfaccia SIL (SIM) (il ponticello o il cablaggio dell'ingresso SIM sta causando un problema), ma gli starter SIL si sono aperti correttamente.
- 5 = funzionamento normale, gli starter SIL possono essere aperti o chiusi

Lo stato 5 è lo stato di funzionamento normale mentre lo stato 3 è lo stato di SIL stop normale. Lo stato 1 indica un problema di firmware o di comunicazione con uno starter SIL. Gli stati 2 e 4 indicano problemi legati a un SIL stop con il cablaggio del SIM, degli starter SIL o del SIL stop. Il monitoraggio indiretto deve cercare gli stati 2 o 4 che persistono più a lungo del tempo di azionamento di un SIL stop e utilizzare le informazioni sullo stato per attivare un meccanismo secondario per arrestare la macchina (interruttore con bobina di trip ecc).

Per leggere lo stato del gruppo SIL, il monitoraggio esterno deve utilizzare il blocco di funzione SystemDiagnostics. Ciascun gruppo SIL nel sistema presenta un'uscita su questo blocco di funzione per il relativo stato del gruppo SIL, contrassegnato sul blocco di funzione come "SILStarterStopMsgGrp *n*", dove *n* è il numero del gruppo SIL nell'isola. Lo stato del gruppo SIL segue la numerazione sopra indicata.

Monitoraggio diagnostico

Poiché il monitoraggio diagnostico si verifica non appena richiesto dalla funzione di sicurezza, il tempo complessivo per rilevare il guasto e portare la macchina in una condizione non pericolosa deve essere inferiore al tempo necessario per raggiungere l'area pericolosa.

Secondo la norma ISO 13849-2, 9.2.3, per la categoria 2: Il $MTTF_d$[11] dell'apparecchiatura di monitoraggio deve essere superiore alla metà del $MTTF_d$ della logica. Il contributo di TeSys island al $MTTF_d$ del monitoraggio diagnostico è $MTTF_d > 100$ anni.

Categoria cablaggio 3

Un guasto singolo non causa la perduta della funzione di sicurezza e se possibile, il guasto singolo deve essere rilevato in corrispondenza o prima del carico medio successivo sulla funzione di sicurezza..

Per rispettare i requisiti per la categoria 3, il feedback del contatto mirror (Mirror In/Mirror Out) deve essere monitorato da un modulo Preventa XPS (o equivalente) che esegue il monitoraggio diagnostico esterno del contatto mirror dello starter SIL[12]. Se il contatto mirror non si apre allo stop, il riavvio successivo viene impedito per tutti gli starter SIL nel gruppo SIL. L'elemento del sensore legato alla sicurezza è collegato via cavo al modulo Preventa XPS (o equivalente). Le uscite del modulo Preventa XPS (o equivalente) sono collegate via cavo agli ingressi comuni SIL-IN/SIL del modulo interfaccia SIL.

In caso di monitoraggio indiretto, il monitoraggio esterno dello stato del gruppo deve cercare gli stati 2 o 4 che persistono più a lungo del tempo di azionamento di un SIL stop. Utilizzare le informazioni sullo stato per impedire il riavvio successivo degli starter SIL del gruppo.

10. Livello di integrità della sicurezza secondo la norma IEC 61508.
11. Tempo medio prima di un guasto pericoloso secondo la definizione di ISO 138491.
12. Livello di integrità della sicurezza secondo la norma IEC 61508

Categoria cablaggio 4

Un guasto singolo non causa la perduta della funzione di sicurezza. Il guasto singolo viene rilevato in corrispondenza o prima del carico medio successivo sulla funzione di sicurezza. Se questo rilevamento non è possibile, un accumulo di guasti non rilevati non causa la perdita della funzione di sicurezza.

Per rispettare i requisiti per la categoria 4, il feedback del contatto mirror (Mirror In/Mirror Out) deve essere monitorato da un modulo Preventa XPS (o equivalente) che esegue il monitoraggio diagnostico esterno del contatto mirror dello starter SIL[13]. Se il contatto mirror non si apre allo stop, il riavvio successivo viene impedito per tutti gli starter SIL nel gruppo SIL. L'elemento del sensore legato alla sicurezza è collegato via cavo al modulo Preventa XPS (o equivalente). Le uscite del modulo Preventa XPS (o equivalente) sono collegate via cavo agli ingressi comuni SIL-IN/SIL del modulo interfaccia SIL.

Test accettazione

L'integratore di sistemi/il produttore della macchina deve eseguire un test di accettazione della funzione di sicurezza per verificare e documentare il corretto funzionamento della funzione di sicurezza. L'integratore di sistemi/il produttore della macchina deve quindi certificare di aver testato l'efficacia delle funzioni di sicurezza utilizzate. Il test di accettazione deve essere eseguito sulla base dell'analisi dei pericoli e della valutazione dei rischi. In caso di modalità richiesta bassa con categoria 4, la funzione di sicurezza deve essere testata almeno una volta al mese. È necessario attenersi a tutte le norme e direttive applicabili.

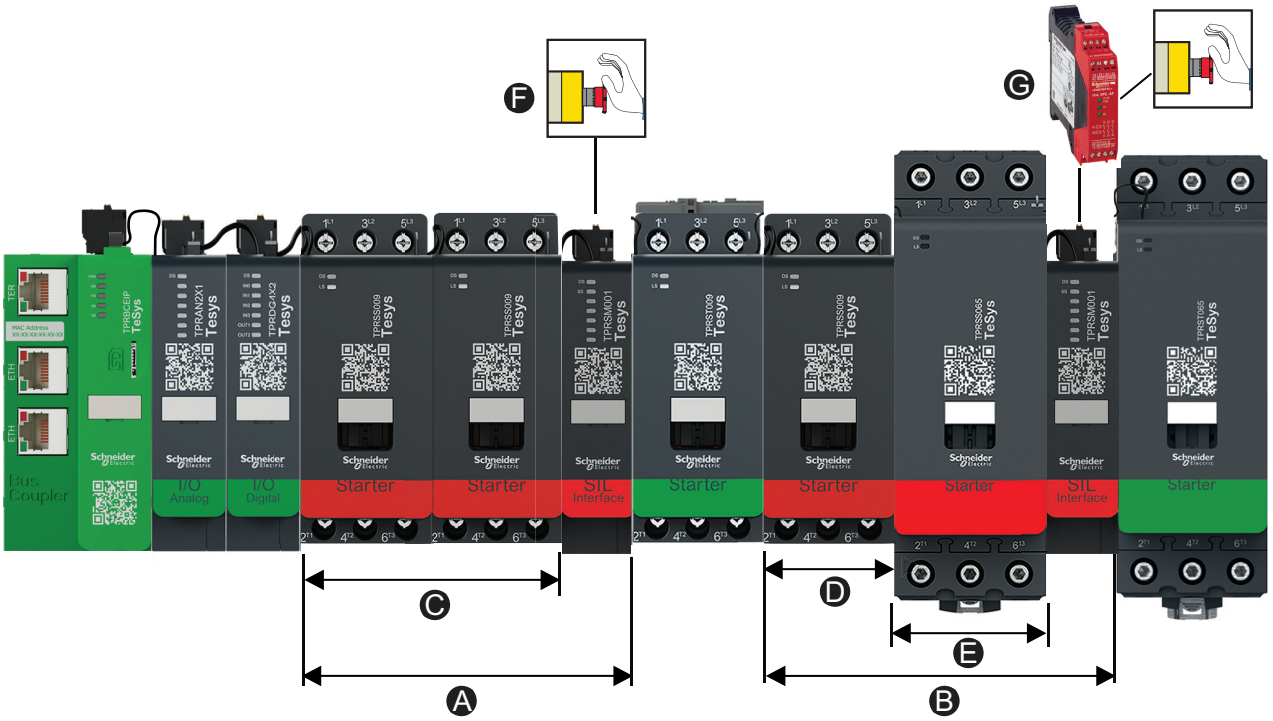
13. Livello di integrità della sicurezza secondo la norma IEC 61508

Concetti e componenti

Struttura tipica di TeSys™ island

La figura seguente mostra un esempio di un TeSys™ island composto da due gruppi SIL[14]. La composizione dell'isola è definita dagli strumenti digitali di TeSys island in base alle esigenze funzionali espresse dall'utente.

Figura 2 - TeSys island con due gruppi SIL



A	Gruppo SIL 1	E	Avatar A4
B	Gruppo SIL 2	F	Categoria cablaggio 1, Categoria stop 0[15]
C	Avatar A1	G	Categoria cablaggio 2, Categoria stop 1[16]
D	Avatar A3		

Gruppo SIL 1: include un avatar che comprende due starter SIL, ad esempio, un avatar (Avatar A1) "Motore a due sensi di marcia: SIL stop, categoria cablaggio 1/2". Il motore reale è collegato a questi starter SIL e segue la logica dell'avatar e i comandi operativi derivanti dal PLC attraverso il bus di campo. Il comando di SIL stop deriva dal pulsante di arresto di emergenza collegato al modulo interfaccia SIL (categoria cablaggio 1) e spinge gli starter SIL a disattivare il carico ed entrare nello stato sicuro (contattore aperto e motore diseccitato).

Gruppo SIL 2: comprende due avatar, ad esempio un "Contattore: SIL stop, categoria cablaggio 1/2" (Avatar A3) e un "Motore a un senso di marcia: SIL stop, categoria cablaggio 1/2" (Avatar A4), ciascuno dei quali composto da un singolo starter SIL. Entrambi gli avatar seguono la logica degli avatar e i comandi operativi

14. Livello di integrità della sicurezza secondo la norma IEC 61508.
15. Categoria cablaggio 1 in conformità con ISO 13849. Categoria stop 0 in conformità con EN/IEC 60204-1.
16. Categoria cablaggio 2 in conformità con ISO 13849. Categoria stop 1 in conformità con EN/IEC 60204-1.

derivanti dal PLC attraverso il bus di campo. Il comando di SIL stop deriva dal modulo Preventa™ XPS (o equivalente) esterno cablato al modulo interfaccia SIL e spinge gli starter SIL a disattivare il carico ed entrare nello stato sicuro (categoria cablaggio 2).

Gruppo SIL

Un gruppo SIL[17] è composto da uno o più avatar SIL, tutti assegnati a un singolo modulo interfaccia SIL. Tutti gli avatar SIL nel gruppo SIL reagiscono a un singolo comando di SIL stop. Il modulo interfaccia SIL è sempre installato a destra dell'ultimo starter SIL incluso nel gruppo SIL (estremità del bus coupler).

Un'isola può includere vari gruppi SIL.

Avatar SIL

Gli avatar SIL[17] disponibili per le funzioni SIL Stop sono:

- Contattore: SIL Stop, categoria cablaggio 1/2
- Contattore: SIL Stop, categoria cablaggio 3/4
- Motore a un senso di marcia: SIL Stop, categoria cablaggio 1/2
- Motore a un senso di marcia: SIL Stop, categoria cablaggio 3/4
- Motore a due sensi di marcia: SIL Stop, categoria cablaggio 1/2
- Motore a due sensi di marcia: SIL Stop, categoria cablaggio 3/4
- Motore a due velocità: SIL Stop, categoria cablaggio 1/2
- Motore a due velocità: SIL Stop, categoria cablaggio 3/4
- Motore due velocità e due sensi di marcia: SIL Stop, categoria cablaggio 1/2
- Motore due velocità e due sensi di marcia: SIL Stop, categoria cablaggio 3/4
- Trasportatore a un senso di marcia: SIL Stop, categoria cablaggio 1/2
- Trasportatore a un senso di marcia: SIL Stop, categoria cablaggio 3/4

Gli avatar SIL sono composti da dispositivi hardware specifici, quali starter standard, starter standard e il necessario modulo interfaccia SIL che gestisce il gruppo SIL al quale sono assegnati gli avatar SIL.

NOTA: Gli avatar SIL sono destinati alle applicazioni con una bassa frequenza di comandi operativi, sotto una media annuale di cicli di 15 di avvii/stop all'ora.

Starter SIL **Starter standard** **Modulo interfaccia SIL**

17. Livello di integrità della sicurezza secondo la norma IEC 61508.

Modulo interfaccia SIL

Il modulo interfaccia SIL[18] (SIM) di TeSys™ island è un modulo accessorio necessario per abilitare la funzione di sicurezza funzionale dell'isola.

La funzione di SIL stop si ottiene tramite mezzi elettromeccanici senza alcuna comunicazione digitale o interazione del bus coupler.

Il SIM:

- si interfaccia con un modulo Preventa™ XPS (o equivalente) esterno
- comanda la funzione di stop del gruppo SIL
- scambia dati operativi con il bus coupler
- segnala le informazioni operative attraverso i LED del pannello anteriore.

Stato contatti starter SIL

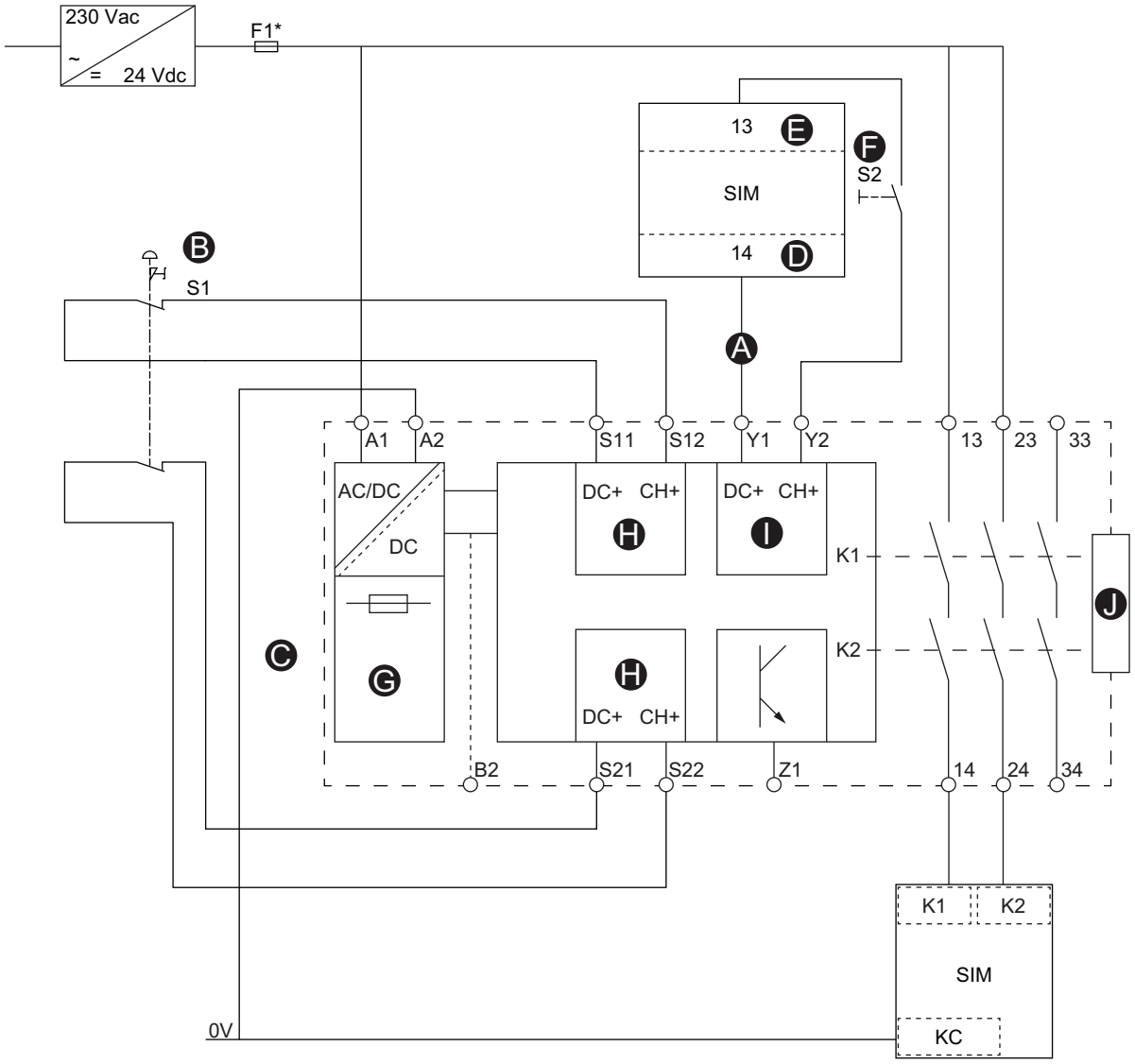
Lo stato degli starter SIL[18] appartenente a un gruppo SIL viene comunicato tramite i collegamenti In/Out SIM Mirror. Ciò consente l'implementazione delle architetture della categoria cablaggio 2[19] in cui i contatti mirror sono collegati al modulo Preventa XPS (o equivalente). Queste configurazioni forniscono funzionalità di monitoraggio dirette dei dispositivi elettromeccanici tramite un elemento di contatto meccanicamente vincolato, che offre una copertura diagnostica fino al 99%. Consultare EN ISO 13849-1, Tabella E.1: stime della copertura diagnostica (DC).

Tabella 2 - Stato contatti starter SIL

Stato gruppo SIL	Stato Mirror In/Out
Tutti gli starter SIL sono aperti	Il contatto Mirror In/Out è chiuso
Almeno uno starter SIL è chiuso	Il contatto Mirror In/Out è aperto
Nessuna alimentazione a TeSys island o guasto rilevato dalla funzione di sicurezza	Il contatto Mirror In/Out è aperto

18. Livello di integrità della sicurezza secondo la norma IEC 61508.
19. Categoria cablaggio 2 in conformità con ISO 13849.

Figura 3 - SIM verso cablaggio modulo Preventa XPS-AF



A	Condizioni di avvio esterne (ESC)	F	Pulsante di avvio (S2)
B	Pulsanti di arresto di emergenza (S1)	G	Alimentazione
C	Modulo Preventa XPS-UAF	H	Ingresso
D	SIM mirror out	I	Avvio
E	SIM mirror in	J	Prolunga

Elemento sensore legato alla sicurezza

Il modulo SIM è collegato a monte:

- alla sorgente 24 V CC
- all'elemento del sensore legato alla sicurezza o a un modulo Preventa XPS (o equivalente).

Il modulo SIM è progettato con due canali di ingresso per gli elementi del sensore legati alla sicurezza a doppio canale. Per un livello di tolleranza ai guasti più elevato, si raccomanda l'uso dell'architettura a due canali di ingresso.

Per gli schemi di cablaggio seguenti, vedere Legenda schemi di cablaggio canale SIM, pagina 24.

Figura 4 - SIM: cablaggio a un canale

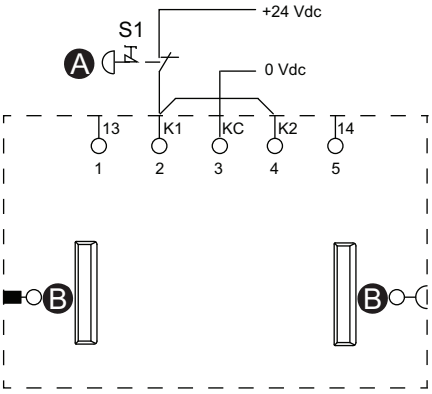


Figura 5 - SIM: cablaggio a due canali

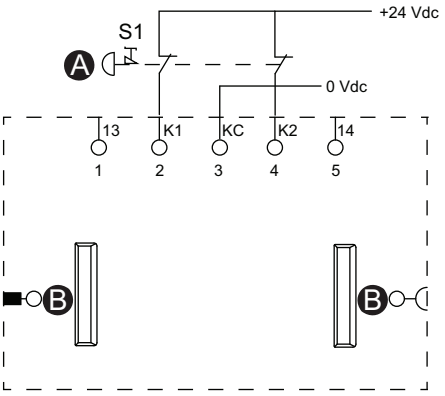


Tabella 3 - Legenda schemi di cablaggio canale SIM

A	Pulsanti di arresto di emergenza (S1)
B	Connettore cavo piatto

Starter SIL

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Per le istruzioni complete sulla sicurezza funzionale, consultare la Guida alla sicurezza funzionale di TeSys™ island, 8536IB1904.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Gli starter SIL[20] offrono funzioni analoghe agli starter standard ma sono associati a un modulo interfaccia SIL.

Le funzioni principali degli starter SIL sono le seguenti:

- Funzione categoria stop 0 e 1[21]
- Controllo operativo per i carichi
- Misurazione dei dati elettrici relativi al carico
- Fornitura di dati di monitoraggio dell'energia se è installato un modulo interfaccia di tensione in TeSys island

Per un singolo starter possono essere necessari più starter SIL per una singola funzione di TeSys avatar. Ad esempio, l'avatarMotore a due sensi di marcia: SIL Stop, categoria cablaggio 1/2[22] include due starter SIL. Inoltre, gli avatars che utilizzando starter SIL includono sempre un modulo interfaccia SIL.

Gli starter SIL sono collegati:

- a monte a un commutatore
- a valle al carico

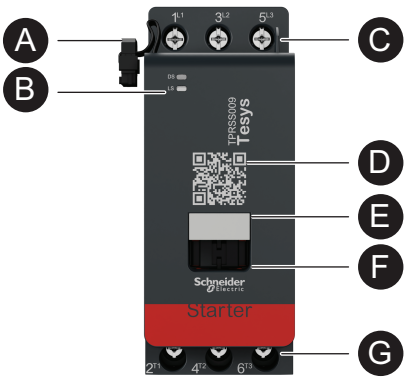
I SIL comunicano con il bus coupler, inviando i dati operativi e ricevendo i comandi.

Tabella 4 - Valori nominali starter SIL

Valori di potenza		Amperaggio	Riferimento
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

20. Livello di integrità della sicurezza secondo la norma IEC 61508
21. Categoria stop 0 e 1 in conformità con la norma EN/IEC 60204-1.
22. Categoria cablaggio 1 e 2 in conformità con ISO 13849.

Figura 6 - Funzioni starter SIL



A	Cavo piatto (per il collegamento al modulo a sinistra)	E	Tag nome
B	Indicatori di stato LED	F	Bridge mobile
C	Collegamenti elettrici a monte	G	Collegamenti elettrici a valle
D	Codice QR		

Elemento esterno legato alla sicurezza

TeSys™ island deve essere integrato con altri elementi legati alla sicurezza in un sistema legato alla sicurezza più ampio per garantire la sicurezza funzionale di una macchina o di un sistema/processo.

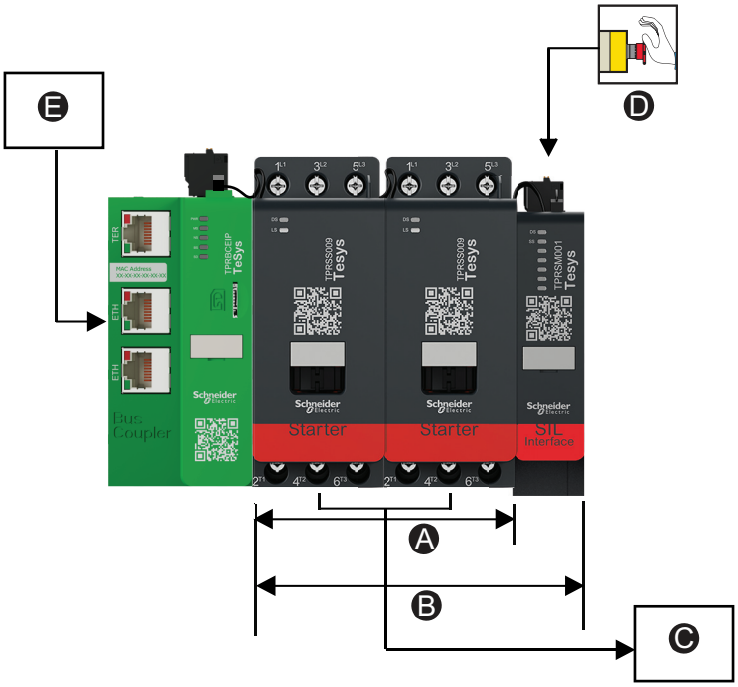
Le configurazioni seguenti illustrano i dispositivi tipici.

Configurazione SIL stop, categoria stop 0, categoria cablaggio 1

NOTA: Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 1 in conformità con ISO 13849. Categoria stop 0 in conformità con EN/IEC 60204-1.

Il SIL stop del motore è controllato direttamente dall'apertura del contatto del pulsante di arresto di emergenza.

Figura 7 - SIL Stop



A	Avatar A1	D	Categoria cablaggio 1, categoria stop 0
B	Gruppo SIL 1	E	PLC
C	Motore		

Configurazione SIL stop, categoria stop 0, categoria cablaggio 2

NOTA: Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 2 in conformità con ISO 13849. Categoria stop 0 in conformità con EN/IEC 60204-1.

Figura 8 - Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 1/2, categoria stop 0, categoria cablaggio 2 (monitoraggio indiretto)

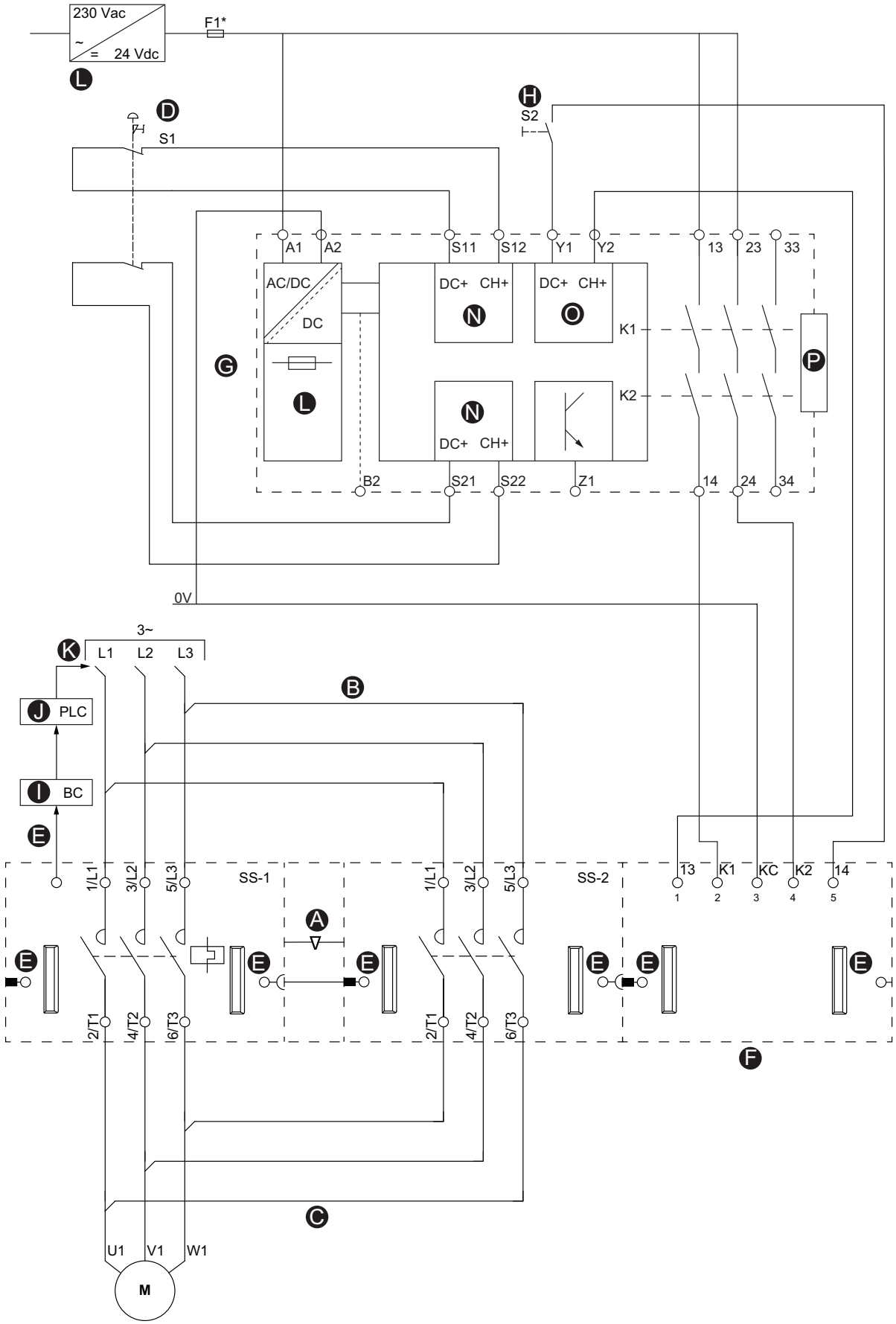
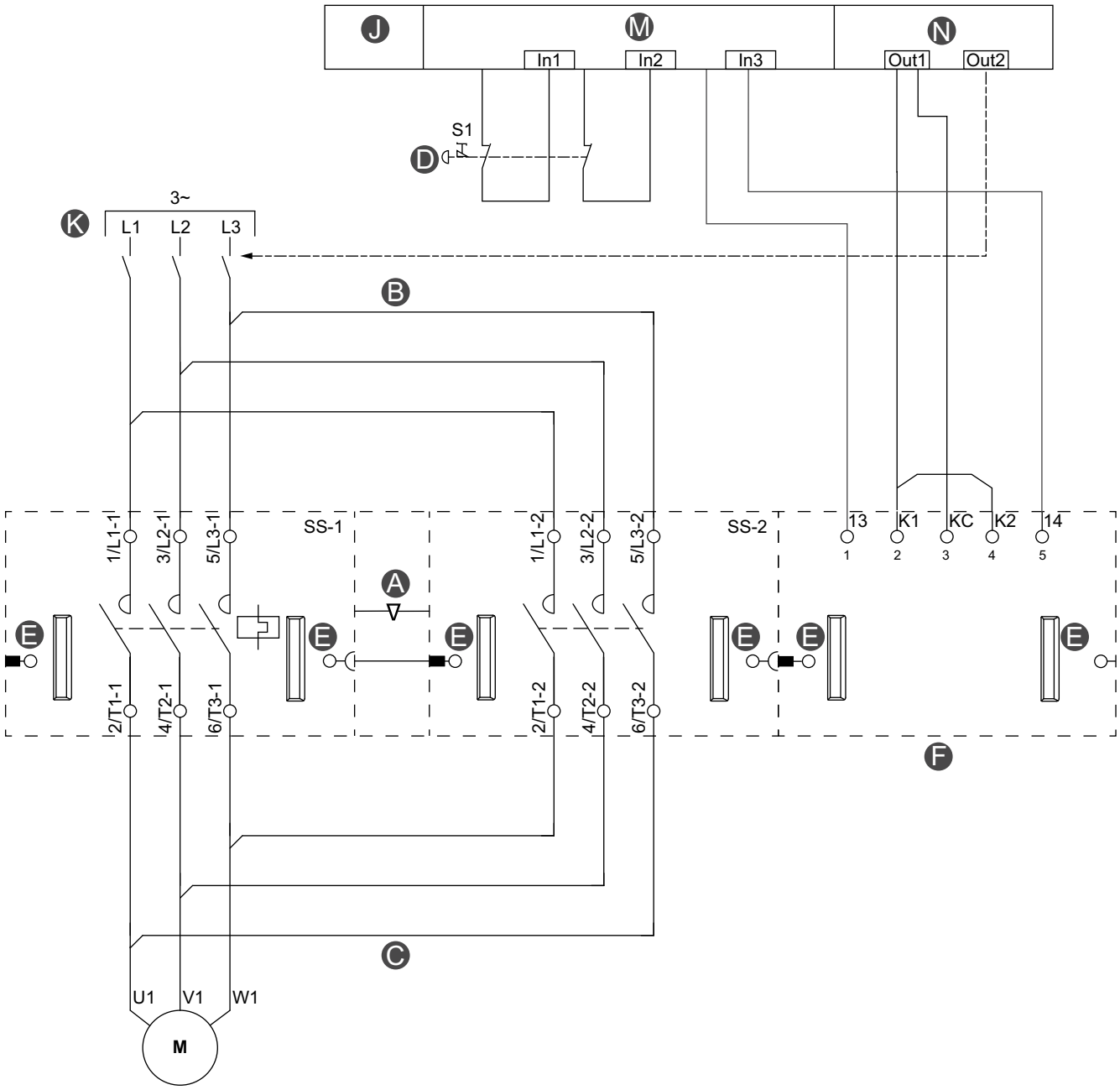


Tabella 5 - Legenda per Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 1/2, categoria stop 0, categoria cablaggio 2 (monitoraggio indiretto), pagina 28

A	Interblocco meccanico	I	Bus coupler
B	Collegamento parallelo	J	PLC
C	Collegamento inverso	K	Interruttore a monte
D	Pulsanti di arresto di emergenza (S1)	L	Alimentazione
E	Connettore cavo piatto	N	Ingresso
F	Modulo interfaccia SIL (SIM)	O	Avvio
G	Modulo Preventa XPS-UAF	P	Prolunga
H	Pulsante di avvio (S2)		

Figura 9 - Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 1/2, categoria stop 0, categoria cablaggio 2 (monitoraggio diretto)



A	Interblocco meccanico	F	Modulo interfaccia SIL (SIM)
B	Collegamento parallelo	J	PLC funzione di sicurezza
C	Collegamento inverso	K	Interruttore a monte
D	Pulsanti di arresto di emergenza (S1)	M	Ingresso digitale
E	Connettore cavo piatto	N	Uscita digitale

Configurazione SIL stop, categoria stop 1, categoria cablaggio 2

NOTA: Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 2 in conformità con ISO 13849. Categoria stop 1 in conformità con EN/IEC 60204-1.

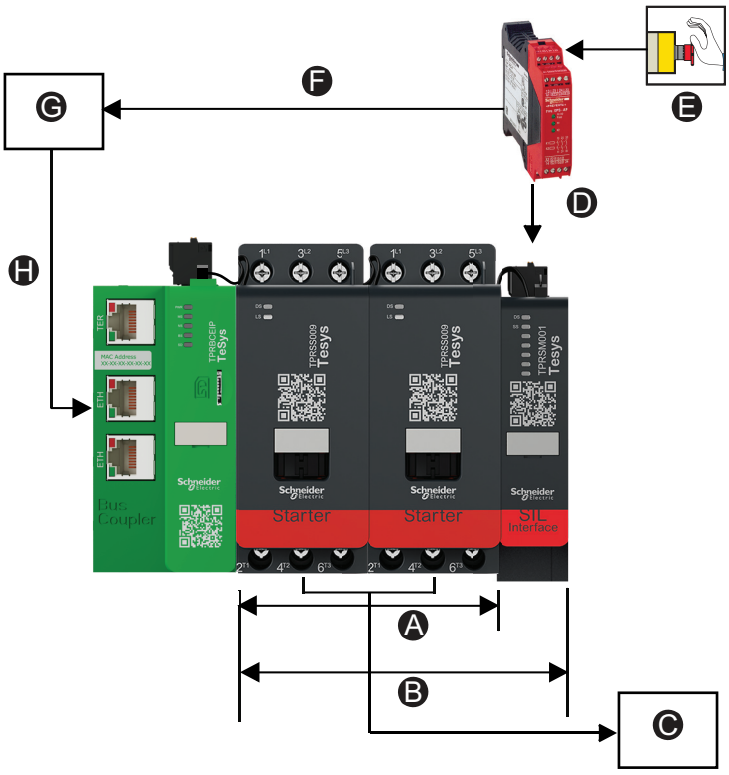
La categoria stop 1 è definita come "uno stop controllato con l'alimentazione disponibile per gli attuatori della macchina per raggiungere lo stop e quindi lo scollegamento dell'alimentazione al raggiungimento dello stop".

Quando viene attivato l'arresto di emergenza, il comando di stop viene prima inviato a un dispositivo esterno (es. un PLC o una trasmissione). In questo modo, il processo viene arrestato in modo controllato e non scollegando immediatamente l'alimentazione. Dopo un periodo predefinito, il comando SIL stop viene inviato al SIM per interrompere l'alimentazione dei carichi sugli avatar SIL nel gruppo SIL associato.

L'impostazione consigliata è l'uso di un PLC per fare in modo che il processo venga arrestato correttamente prima che si verifichi il SIL stop.

Il comando di stop può essere indirizzato direttamente a un ingresso digitale del PLC o a un avatar del modulo I/O digitale di TeSys™ island utilizzando uno degli ingressi digitali letti dal PLC. Una volta ricevuto un input di comando di stop, il PLC avvia uno stop controllato emettendo un comando di stop operativo diretto all'avatar di TeSys island di destinazione.

Figura 10 - Comando di stop



A	Avatar A1	E	Categoria cablaggio 2, categoria stop 1
B	Gruppo SIL 1	F	Comando categoria stop 1 controllato
C	Motore	G	PLC
D	Stop non controllato	H	Comando di stop operativo

Figura 11 - Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 1/2, categoria stop 1, categoria cablaggio 2

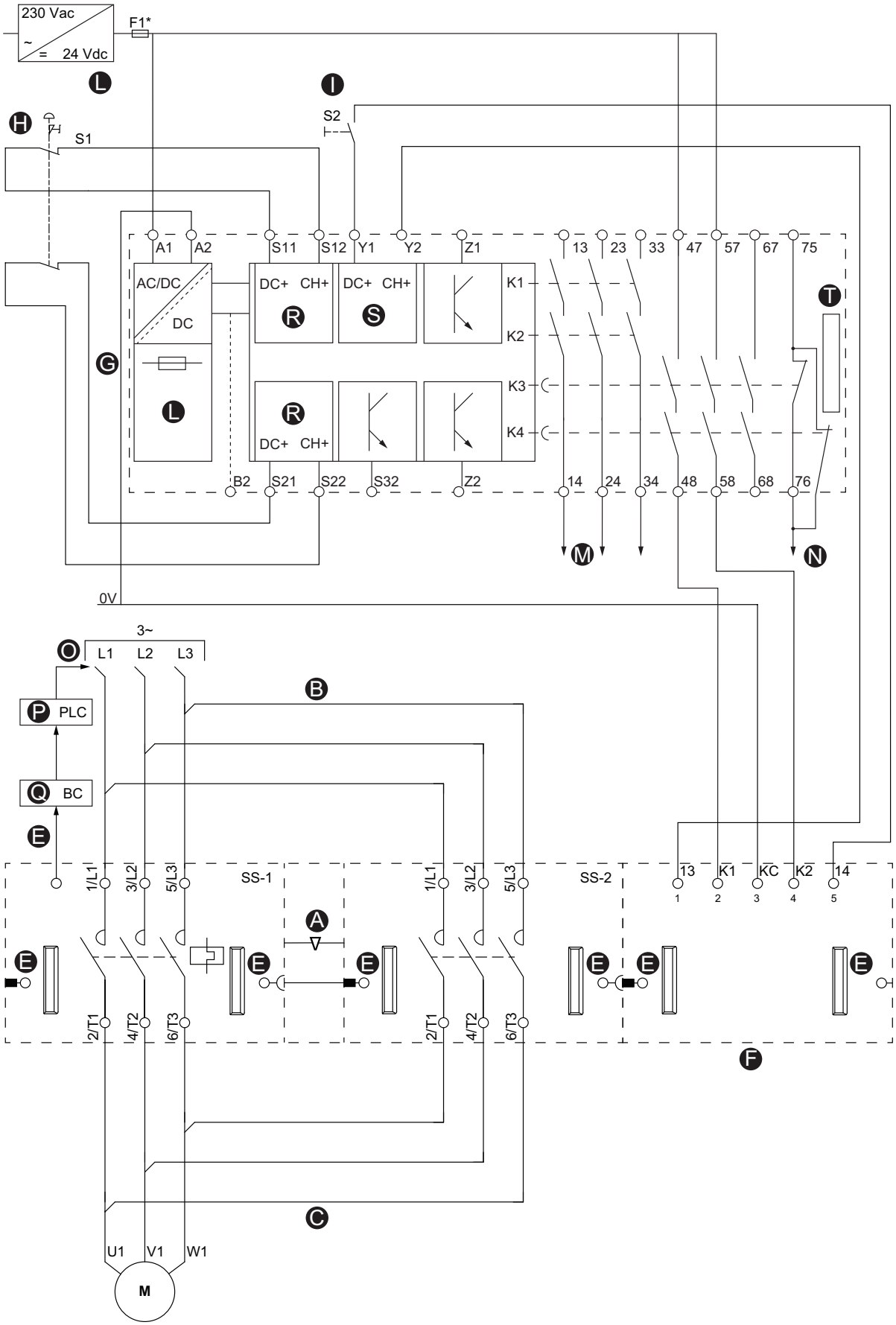


Tabella 6 - Legenda per Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 1/2, categoria stop 1, categoria cablaggio 2, pagina 32

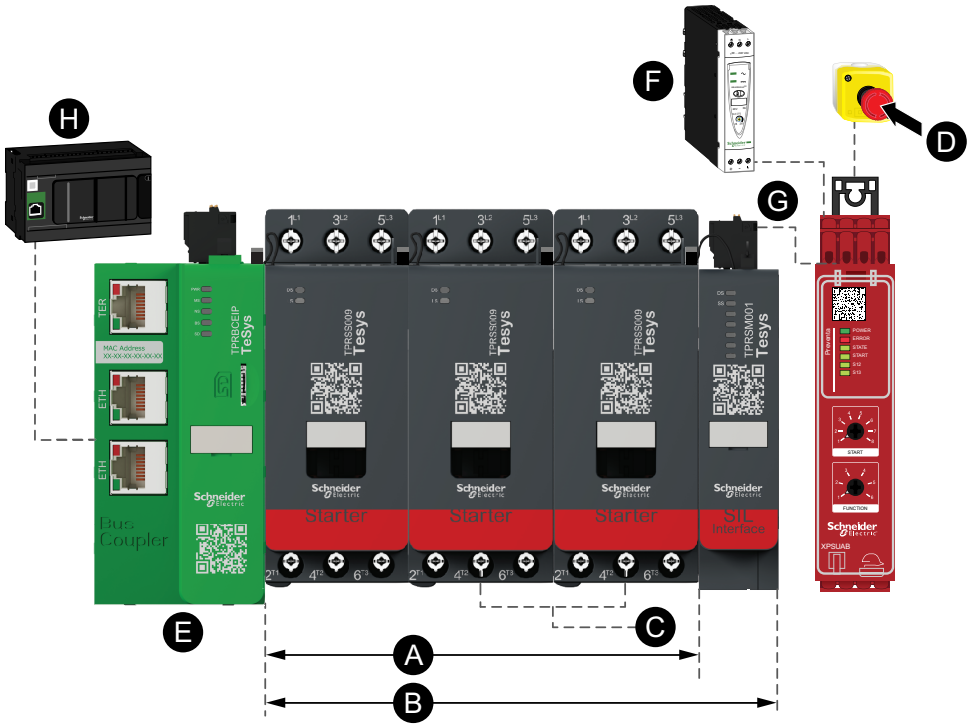
A	Interblocco meccanico	M	Stop controllato
B	Collegamento parallelo	N	Categoria stop 1
C	Collegamento inverso	O	Interruttore a monte
E	Connettore cavo piatto	P	PLC
F	Modulo interfaccia SIL (SIM)	Q	Bus coupler
G	Modulo Preventa XPS-UAF	R	Ingresso
H	Pulsante di arresto di emergenza	S	Avvio
I	Pulsante di avvio S2	T	Prolunga
L	Alimentazione		

Configurazione SIL stop, categoria stop 0, categoria cablaggio 3/4

NOTA: Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 3/4 in conformità con ISO 13849. Categoria stop 0 in conformità con EN/IEC 60204-1.

Il SIL stop del motore è controllato direttamente dall'apertura del contatto del pulsante di arresto di emergenza.

Figura 12 - SIL stop, categoria cablaggio 3/4



A	Avatar A1	E	Bus coupler
B	Gruppo SIL 1	F	24 V CC
C	Motore	G	Modulo Preventa XPS-UAF
D	Categoria cablaggio 3/4, categoria stop 0	H	PLC

Figura 13 - Esempio: motore a un senso di marcia: configurazione SIL stop, categoria cablaggio 3/4, categoria stop 0, categoria cablaggio 3/4

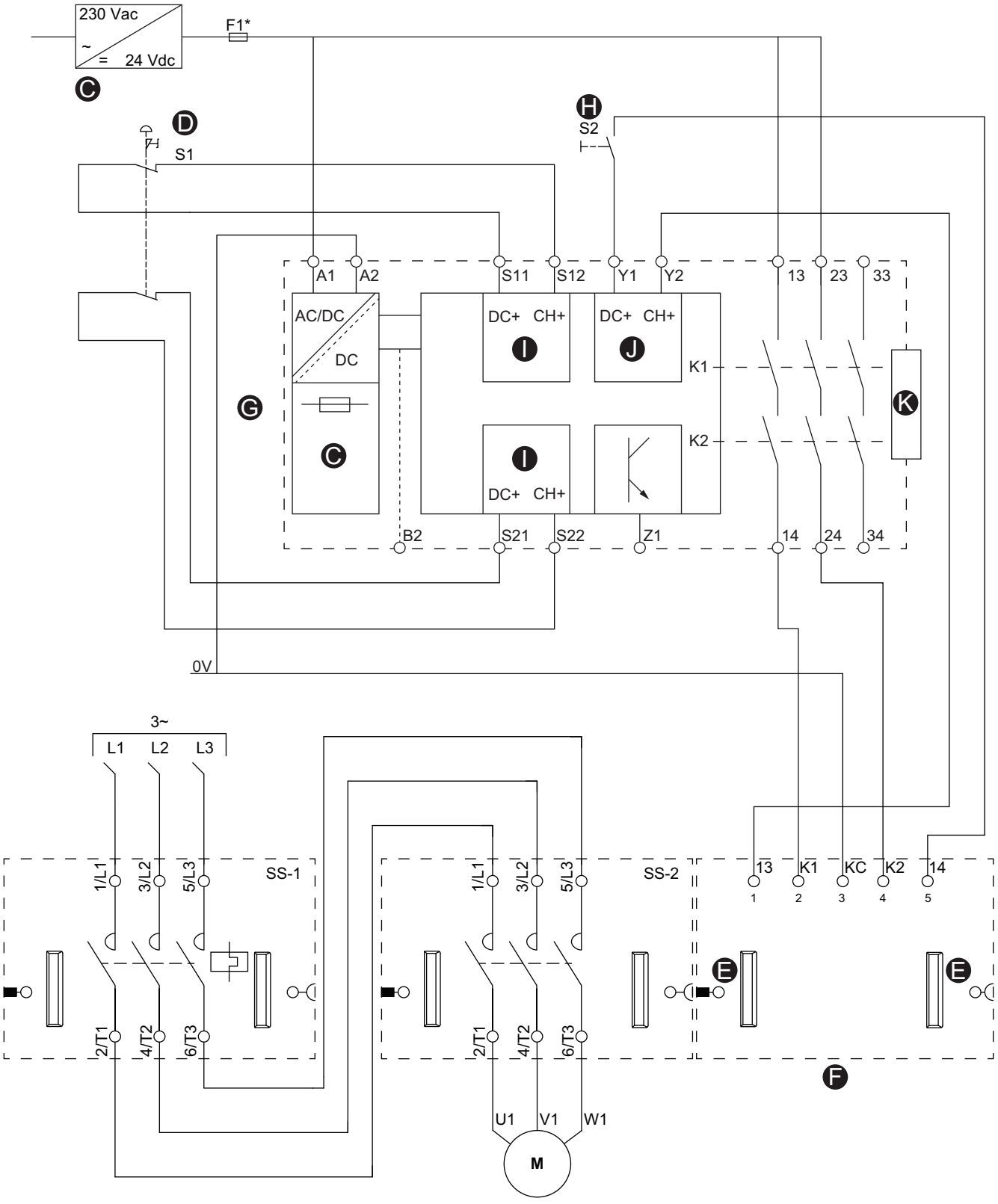


Tabella 7 - Legenda per Esempio: motore a un senso di marcia: configurazione SIL stop, categoria cablaggio 3/4, categoria stop 0, categoria cablaggio 3/4, pagina 35

C	Alimentazione	H	Pulsante di avvio (S2)
D	Pulsanti di arresto di emergenza (S1)	I	Ingresso
E	Connettore cavo piatto	J	Avvio
F	Modulo interfaccia SIL (SIM)	K	Prolunga
G	Modulo Preventa XPS-UAF		

Configurazione SIL stop, categoria stop 1, categoria cablaggio 3/4

NOTA: Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 3/4 in conformità con ISO 13849. Categoria stop 1 in conformità con EN/IEC 60204.

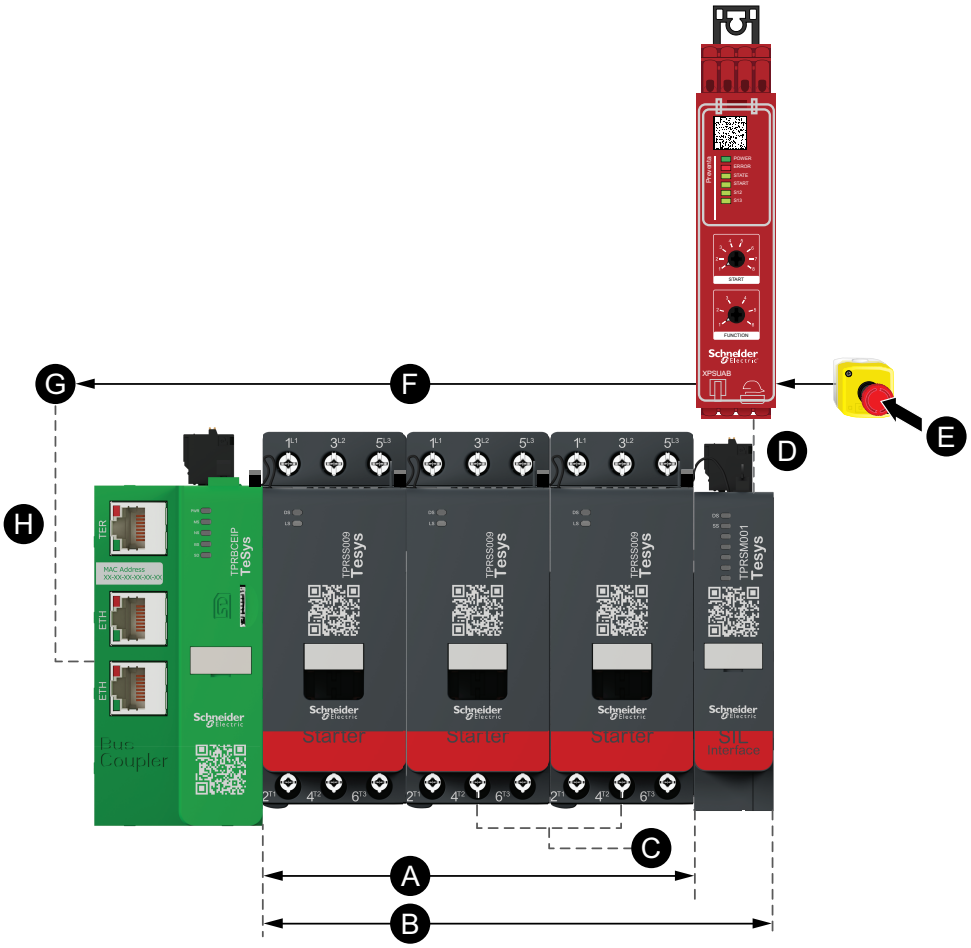
La categoria stop 1 è definita come "uno stop controllato con l'alimentazione disponibile per gli attuatori della macchina per raggiungere lo stop e quindi lo scollegamento dell'alimentazione al raggiungimento dello stop".

Quando viene attivato l'arresto di emergenza, il comando di stop viene prima inviato a un dispositivo esterno (es. un PLC o una trasmissione). In questo modo, il processo viene arrestato in modo controllato e non scollegando immediatamente l'alimentazione. Dopo un periodo predefinito, il comando SIL stop viene inviato al SIM per interrompere l'alimentazione dei carichi sugli avatar SIL nel gruppo SIL associato.

Per la configurazione, la raccomandazione è l'uso di un PLC per fare in modo che il processo venga arrestato correttamente prima che si verifichi il SIL stop.

Il comando di stop può essere indirizzato direttamente a un ingresso digitale del PLC o a un avatar del modulo I/O digitale di TeSys™ island utilizzando uno degli ingressi digitali letti dal PLC. Una volta ricevuto un input di comando di stop, il PLC avvia uno stop controllato emettendo un comando di stop operativo diretto all'avatar di TeSys island di destinazione.

Figura 14 - Comando di stop, categoria 3/4



A	Avatar A1	E	Categoria cablaggio 3/4, categoria stop 1
B	Gruppo SIL 1	F	Comando categoria stop 1 controllato
C	Motore	G	PLC
D	Stop non controllato	H	Comando di stop operativo

Figura 15 - Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 3/4, categoria stop 1, categoria cablaggio 3/4

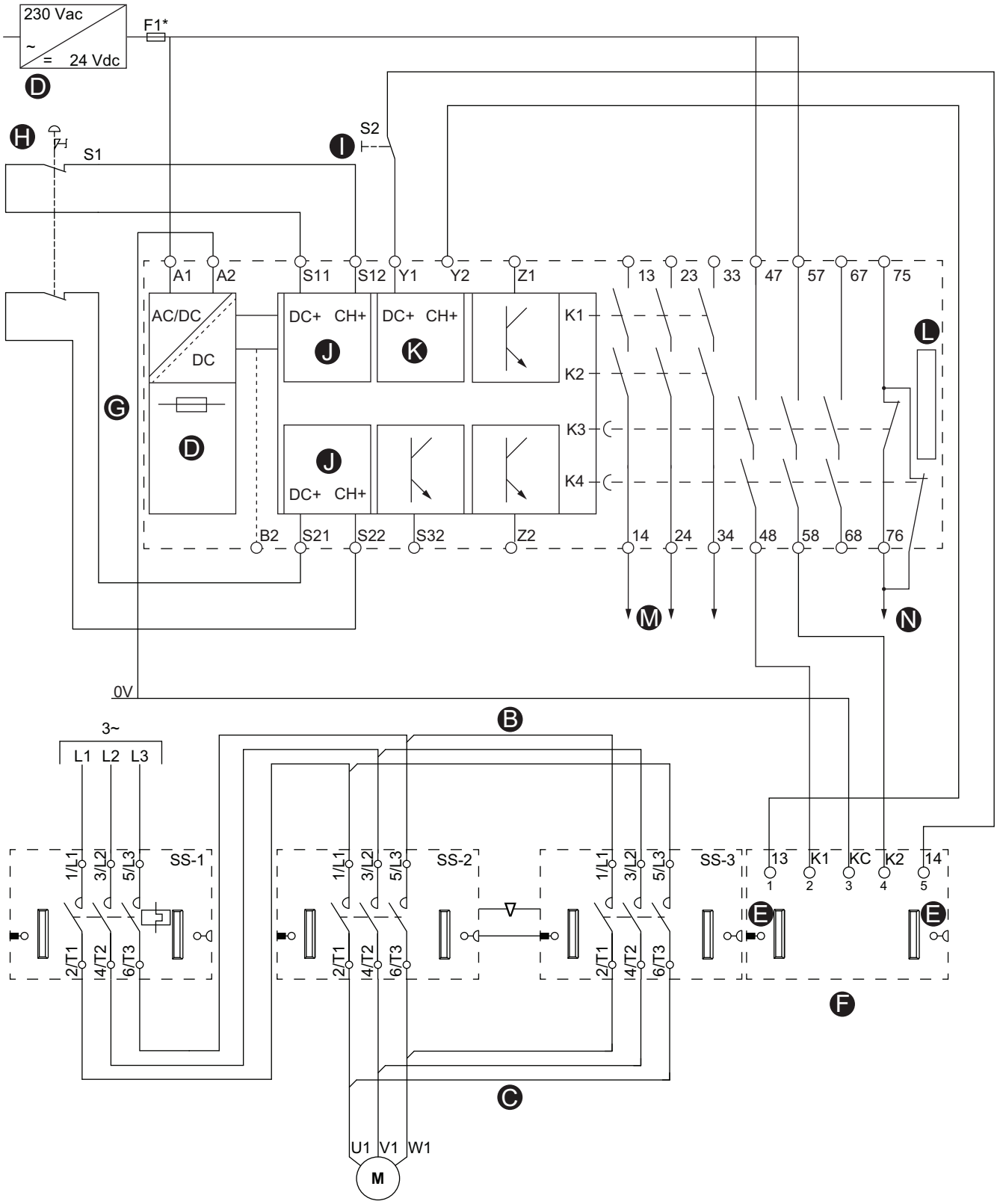


Tabella 8 - Legenda per Esempio: motore a due sensi di marcia: configurazione SIL stop, categoria cablaggio 3/4, categoria stop 1, categoria cablaggio 3/4, pagina 38

B	Collegamento parallelo	I	Pulsante di avvio S2
C	Collegamento inverso	J	Ingresso
D	Alimentazione	K	Avvio
E	Connettore cavo piatto	L	Prolunga
F	Modulo interfaccia SIL (SIM)	M	Stop controllato
G	Modulo Preventa XPS-UAF	N	Categoria stop 1
H	Pulsanti di arresto di emergenza (S1)		

Isolamento del cavo protetto

⚠PERICOLO

FUNZIONAMENTO IMPREVISTO

Verificare di aver installato i cavi del sistema legato alla sicurezza ai sensi della norma ISO 13849-2.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

Se possono verificarsi cortocircuiti e circuiti incrociati con i cavi del sistema legato alla sicurezza che non vengono rilevati dai dispositivi a monte, è necessaria l'installazione di un cavo protetto ai sensi della norma ISO 13849-2.

In caso di installazione di un cavo non protetto, i due segnali (entrambi i canali) di una funzione di sicurezza nello stato cortocircuito possono essere collegati alla tensione esterna se il cavo è danneggiato. In tal caso, la funzione di sicurezza non è più operativa.

Architettura commutazione frequenza bassa/alta

Le informazioni in questa sezione possono essere utilizzate per stabilire se l'architettura operativa è a frequenza bassa o alta.

La parte elettromeccanica dello starter SIL[23] è caratterizzata da un B10d.

Per calcolare il $MTTF_d$ (ai sensi della norma ISO 13849-1) o λd (ai sensi della norma IEC 62061), si applica la formula seguente:

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

dove $\lambda d=1/MTTF_d$

Nop: numero medio di operazioni annuali

Ai sensi della norma ISO 13849, il tempo di funzionamento di un componente elettromeccanico è limitato a T10d (tempo medio fino a quando il 10% dei componenti non si guasta pericolosamente[24]).

Pertanto, il tempo di funzionamento di uno starter SIL è limitato a:

$$T10d=B10d/Nop$$

Il B10d dello starter SIL è B10d = 1.369.863 e supponendo un T10d di 10 anni, il numero di cicli per uno starter SIL di TeSys island è limitato a Nop = B10d/T10 = 131.400/anno (o una media annuale di 15 cicli/h).

Se l'applicazione richiede un Nop inferiore a tale valore, rientra nella categoria di frequenza di commutazione bassa (dove gli avatar SIL possono essere utilizzati così come sono). Altrimenti, rientra nella categoria di frequenza di commutazione alta (dove la funzione di sicurezza deve essere implementata con un avatar SIL dedicato, come descritto di seguito).

23. Livello di integrità della sicurezza secondo la norma IEC 61508.
24. Si guasta pericolosamente ai sensi della norma ISO 13849

Frequenza commutazione bassa (< 15 cicli all'ora)

Nella frequenza commutazione bassa, le funzioni di SIL[25] stop e di controllo operativo acceso/spento possono essere ottenute contemporaneamente con un avatar SIL.

Figura 16 - Esempio di avatar con starter SIL

Tabella 9 - Frequenza commutazione bassa: funzioni operative e di sicurezza

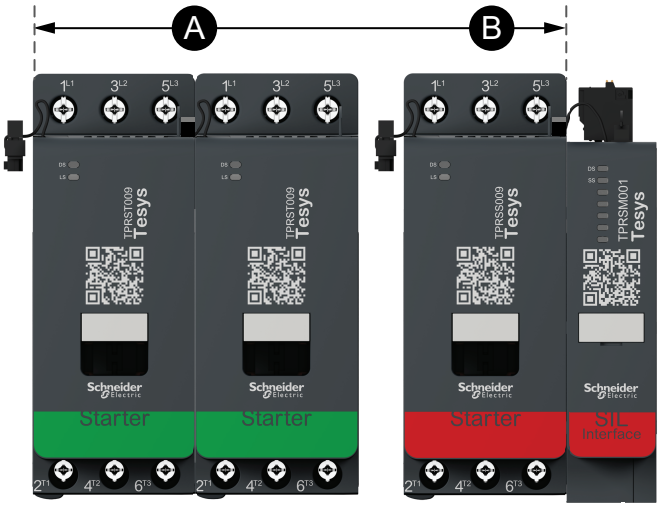
Avatar SIL	Modulo 1	Modulo 2	Modulo 3	Modulo 4	Modulo 5
Contattore: SIL Stop, categoria cablaggio 1/2[26]	Starter SIL	SIM	-	-	-
Contattore: SIL Stop, categoria cablaggio 3/4[27]	Starter SIL	Starter SIL	SIM	-	-
Motore a un senso di marcia: SIL Stop, categoria cablaggio 1/2	Starter SIL	SIM		-	-
Motore a un senso di marcia: SIL Stop, categoria cablaggio 3/4	Starter SIL	Starter SIL	SIM	-	-
Motore a due sensi di marcia: SIL Stop, categoria cablaggio 1/2	Starter SIL	Starter SIL	SIM	-	-
Motore a due sensi di marcia: SIL Stop, categoria cablaggio 3/4	Starter SIL	Starter SIL	Starter SIL	SIM	-
Motore a due velocità: SIL Stop, categoria cablaggio 1/2	Starter SIL	Starter SIL	SIM	-	-
Motore a due velocità: SIL Stop, categoria cablaggio 3/4	Starter SIL	Starter SIL	Starter SIL	SIM	-
Motore due velocità e due sensi di marcia: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter SIL	Starter SIL	SIM
Motore due velocità e due sensi di marcia: SIL Stop, categoria cablaggio 3/4	Starter SIL	Starter SIL	Starter SIL	Starter SIL	SIM
Trasportatore a un senso di marcia: SIL Stop, categoria cablaggio 1/2	Starter SIL	SIM	-	-	-
Trasportatore a un senso di marcia: SIL Stop, categoria cablaggio 1/2	Starter SIL	Starter SIL	SIM	-	-

25. Livello di integrità della sicurezza secondo la norma IEC 61508.
26. Categoria cablaggio 1 e 2 in conformità con ISO 13849.
27. Categoria cablaggio 3 e 4 in conformità con ISO 13849.

Frequenza commutazione alta (≥ 15 cicli all'ora)

Per l'uso ad alta frequenza, isolare la funzione di sicurezza d quella operativa mediante un avatar SIL[28] per la funzione di sicurezza e un avatar standard per la funzione operativa. Gli starter standard vengono quindi cablati in serie a valle dello starter SIL. Frequenza commutazione alta: la tabella delle funzioni operative e di sicurezza contiene alcuni esempi di avatar standard utilizzati a valle dello starter SIL per architetture di SIL Stop, categoria cablaggio 1/2[29] e SIL stop, categoria cablaggio 3/4[30].

Figura 17 - Avatar standard per la funzione operativa + avatar SIL utilizzato per la funzione di sicurezza: SIL stop, categoria cablaggio 1/2



A	Avatar standard
B	Avatar SIL

Tabella 10 - Frequenza commutazione alta, SIL stop, categoria cablaggio 1/2: funzioni operative e di sicurezza

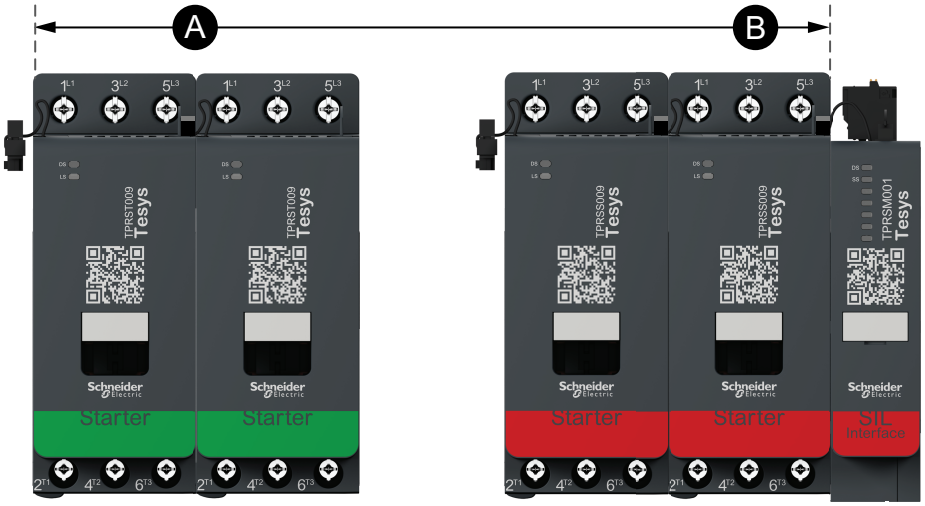
Avatar standard	Avatar SIL	Modulo 1	Modulo 2	Modulo 3	Modulo 4	Modulo 5	Modulo 6
Contattore	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter SIL	SIM	—	—	—
Motore a un senso di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter SIL	SIM	—	—	—
Motore a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter SIL	SIM	—	—
Motore a due velocità	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter SIL	SIM	—	—
Motore a due velocità e a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter standard	Starter standard	Starter SIL	SIM
Trasportatore a un senso di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter SIL	SIM	—	—	—
Trasportatore a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter SIL	SIM	—	—

28. Livello di integrità della sicurezza secondo la norma IEC 61508.
29. Categoria cablaggio 1 e 2 in conformità con la norma ISO 13849.
30. Categoria cablaggio 3 e 4 in conformità con ISO 13849.

Tabella 10 - Frequenza commutazione alta, SIL stop, categoria cablaggio 1/2: funzioni operative e di sicurezza (Continuare)

Avatar standard	Avatar SIL	Modulo 1	Modulo 2	Modulo 3	Modulo 4	Modulo 5	Modulo 6
Motore YD a un senso di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter standard	Starter SIL	SIM	—
Motore YD a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 1/2	Starter standard	Starter standard	Starter standard	Starter standard	Starter SIL	SIM

Figura 18 - Avatar standard per la funzione operativa + avatar SIL utilizzato per la funzione di sicurezza: SIL stop, categoria cablaggio 3/4



A	Avatar standard
B	Avatar SIL

Tabella 11 - Frequenza commutazione alta, SIL stop, categoria cablaggio 3/4: funzioni operative e di sicurezza

Avatar standard	Avatar SIL	Modulo 1	Modulo 2	Modulo 3	Modulo 4	Modulo 5	Modulo 6	Modulo 7
Contattore	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter SIL	Starter SIL	SIM	—	—	—
Motore a un senso di marcia	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter SIL	Starter SIL	SIM	—	—	—
Motore a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter standard	Starter SIL	Starter SIL	SIM	—	—
Motore a due velocità	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter standard	Starter SIL	Starter SIL	SIM	—	—
Motore a due velocità e a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter standard	Starter standard	Starter standard	Starter SIL	Starter SIL	SIM
Motore YD a un senso di marcia	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter standard	Starter standard	Starter standard	Starter SIL	Starter SIL	SIM
Motore YD a due sensi di marcia	Contattore: SIL Stop, categoria cablaggio 3/4	Starter standard	Starter standard	Starter standard	Starter standard	Starter SIL	Starter SIL	SIM

Architetture campione

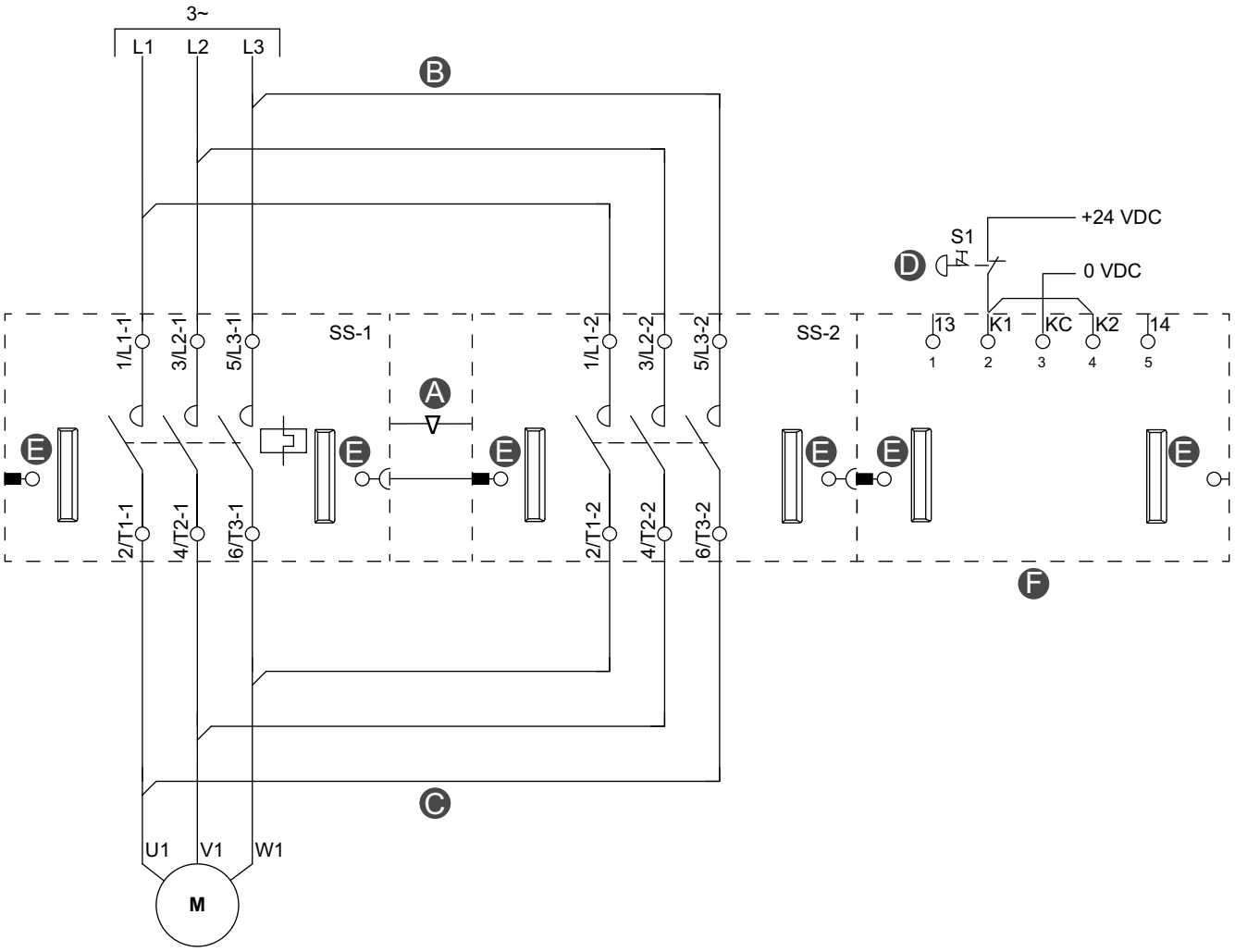
Per la sicurezza funzionale di TeSys™ island sono disponibili le architetture seguenti:

- SIL Stop, categoria stop 0, categoria cablaggio 1[31]
- SIL stop, categoria stop 0, categoria cablaggio 2
- SIL stop, categoria stop 1, categoria cablaggio 2
- SIL stop, categoria stop 0, categoria cablaggio 3/4
- SIL stop, categoria stop 1, categoria cablaggio 3/4

31. Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 1, Categoria 2 e 3/4 in conformità con ISO 13849. Categoria stop 0 e categoria 1 in conformità con EN/IEC 60204-1.

SIL stop, categoria stop 0, categoria cablaggio 1

Figura 19 - Esempio: SIL Stop, categoria stop 0, categoria cablaggio 1[32]

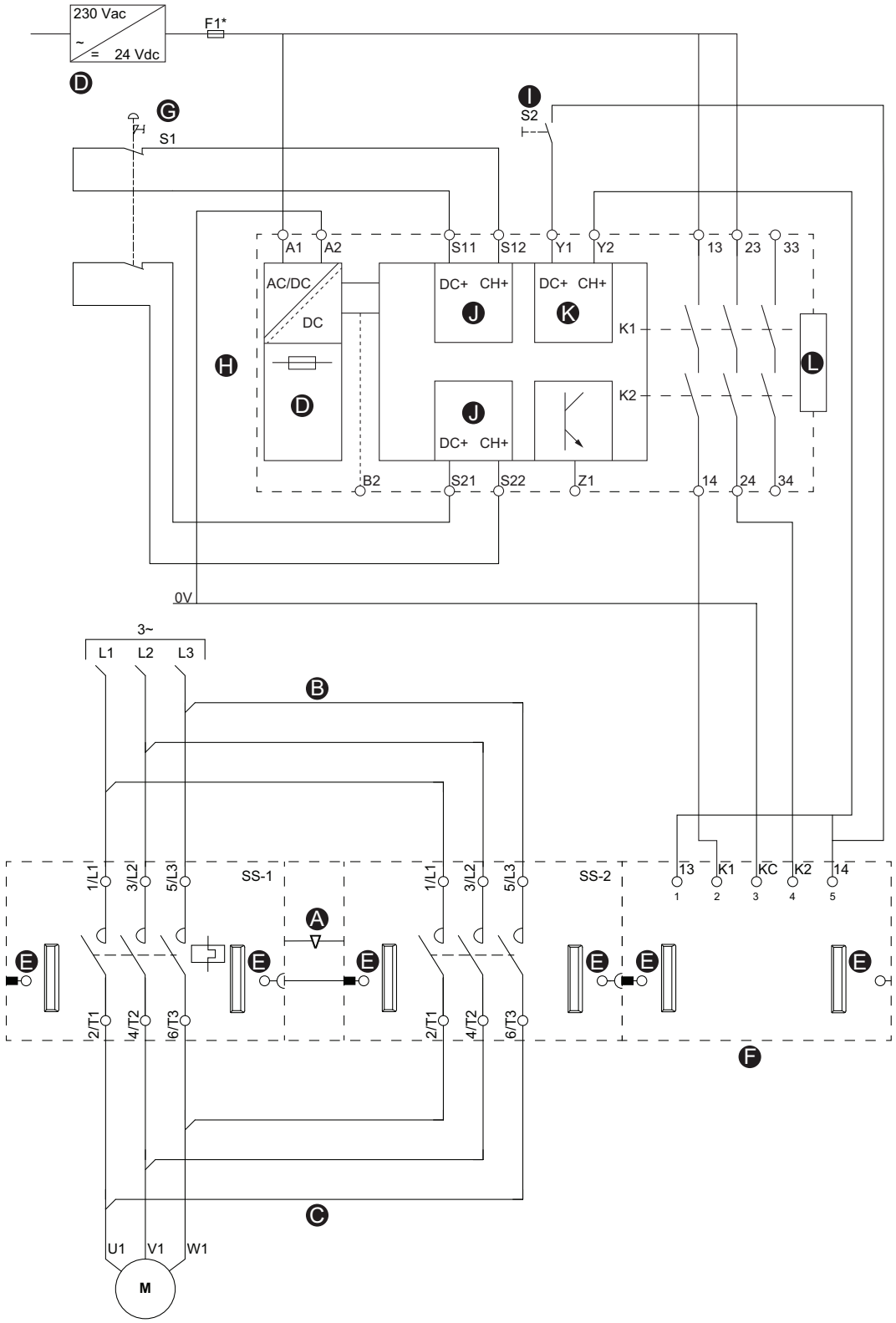


A	Interblocco meccanico	D	Pulsanti di arresto di emergenza (S1)
B	Collegamento parallelo	E	Connettore cavo piatto
C	Collegamento inverso	F	Modulo interfaccia SIL (SIM)

32. Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 1 in conformità con ISO 13849. Categoria stop 0 in conformità con EN/IEC 60204-1.

SIL Stop, categoria stop 0, categoria cablaggio 2

Figura 20 - Esempio SIL Stop, categoria stop 0, categoria cablaggio 2[33]



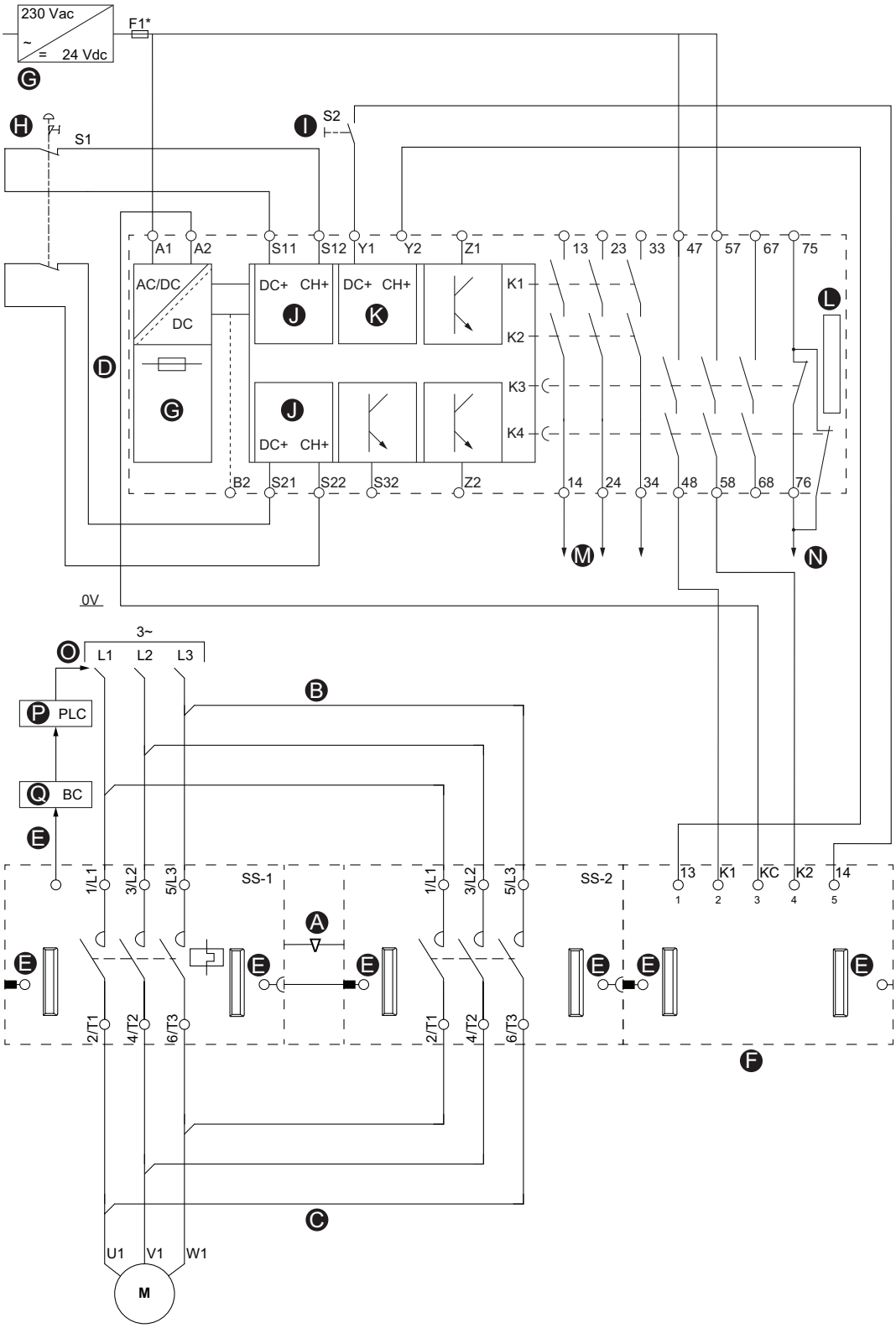
33. Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 2 in conformità con ISO 13849. Categoria stop 0 in conformità con la norma EN/IEC 60204-1.

Tabella 12 - Legenda per Esempio: SIL Stop, categoria stop 0, categoria cablaggio 2, pagina 46

A	Interblocco meccanico	G	Pulsanti di arresto di emergenza (S1)
B	Collegamento parallelo	H	Modulo Preventa XPS-UAF
C	Collegamento inverso	I	Pulsante di avvio (S2)
D	Alimentazione	J	Ingresso
E	Connettore cavo piatto	K	Avvio
F	Modulo interfaccia SIL (SIM)	L	Estensione

SIL stop, categoria stop 1, categoria cablaggio 2

Figura 21 - Esempio SIL Stop, categoria stop 1, categoria cablaggio 2[34]



34. Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 2 in conformità con ISO 13849. Categoria stop 1 in conformità con la norma EN/IEC 60204-1.

Tabella 13 - Legenda per Esempio: SIL stop, categoria stop 1, categoria cablaggio 2, pagina 48

A	Interblocco meccanico	J	Ingresso
B	Collegamento parallelo	K	Avvio
C	Collegamento inverso	L	Estensione
E	Connettore cavo piatto	M	Stop controllato
F	Modulo interfaccia SIL (SIM)	N	Categoria stop 1
G	Alimentazione	O	Interruttore a monte
H	Pulsanti di arresto di emergenza (S1)	P	PLC
I	Pulsante di avvio S2	Q	Bus coupler

SIL stop, categoria stop 0, categoria cablaggio 3/4

Figura 22 - Esempio SIL Stop, categoria stop 0, categoria cablaggio 3/4[35]

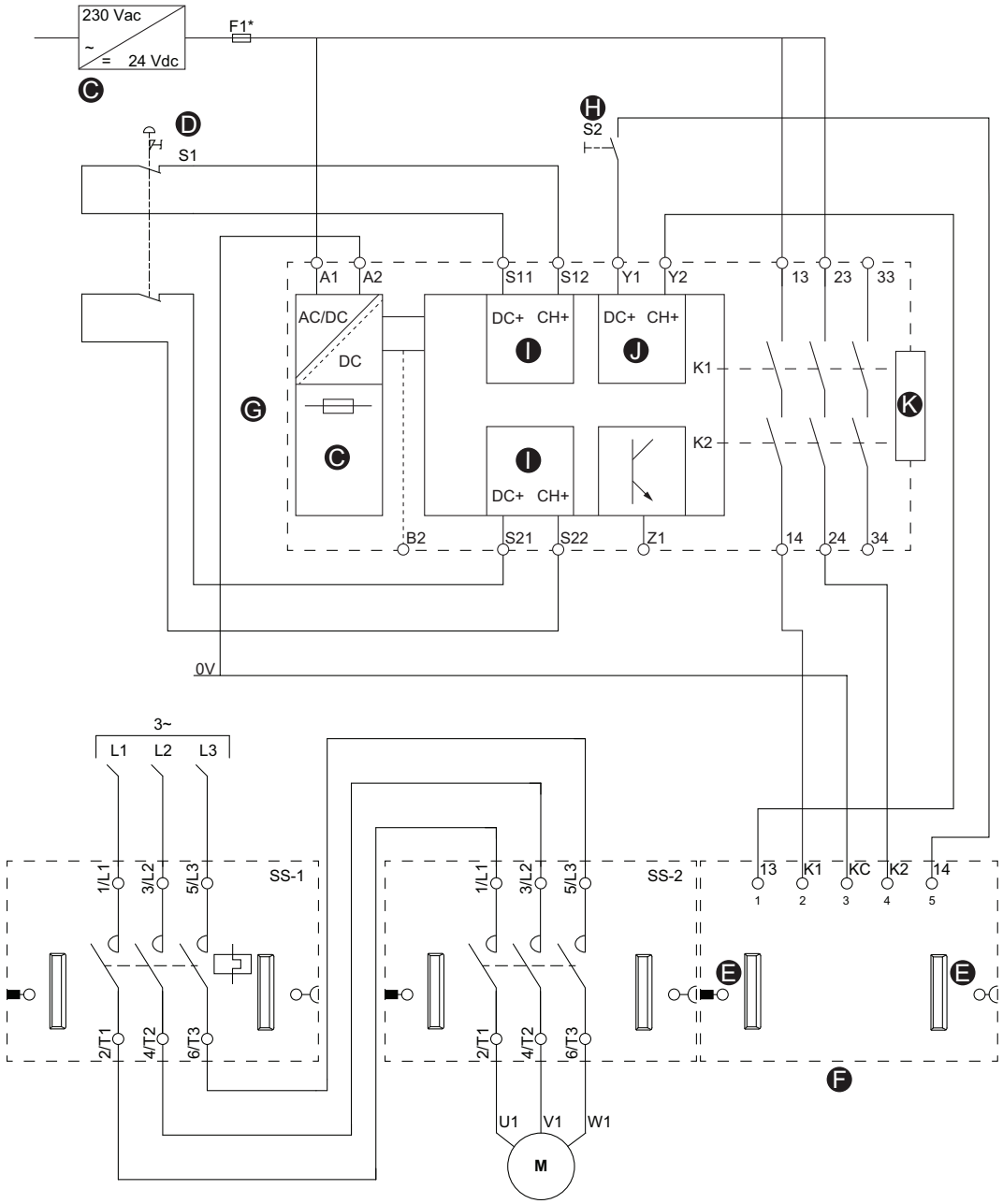


Tabella 14 - Legenda per Esempio: SIL stop, categoria stop 0, categoria cablaggio 3/4, pagina 50

C	Alimentazione	H	Pulsante di avvio (S2)
D	Pulsanti di arresto di emergenza (S1)	I	Ingresso
E	Connettore cavo piatto	J	Avvio

35. Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 3/4 in conformità con ISO 13849. Categoria stop 0 in conformità con la norma EN/IEC 60204-1.

Tabella 14 - Legenda per Esempio: SIL stop, categoria stop 0, categoria cablaggio 3/4 (Continuare)

F	Modulo interfaccia SIL (SIM)	K	Estensione
G	Modulo Preventa XPS-UAF		

SIL stop, categoria stop 1, categoria cablaggio 3/4

Figura 23 - Esempio SIL Stop, categoria stop 1, categoria cablaggio 3/4[36]

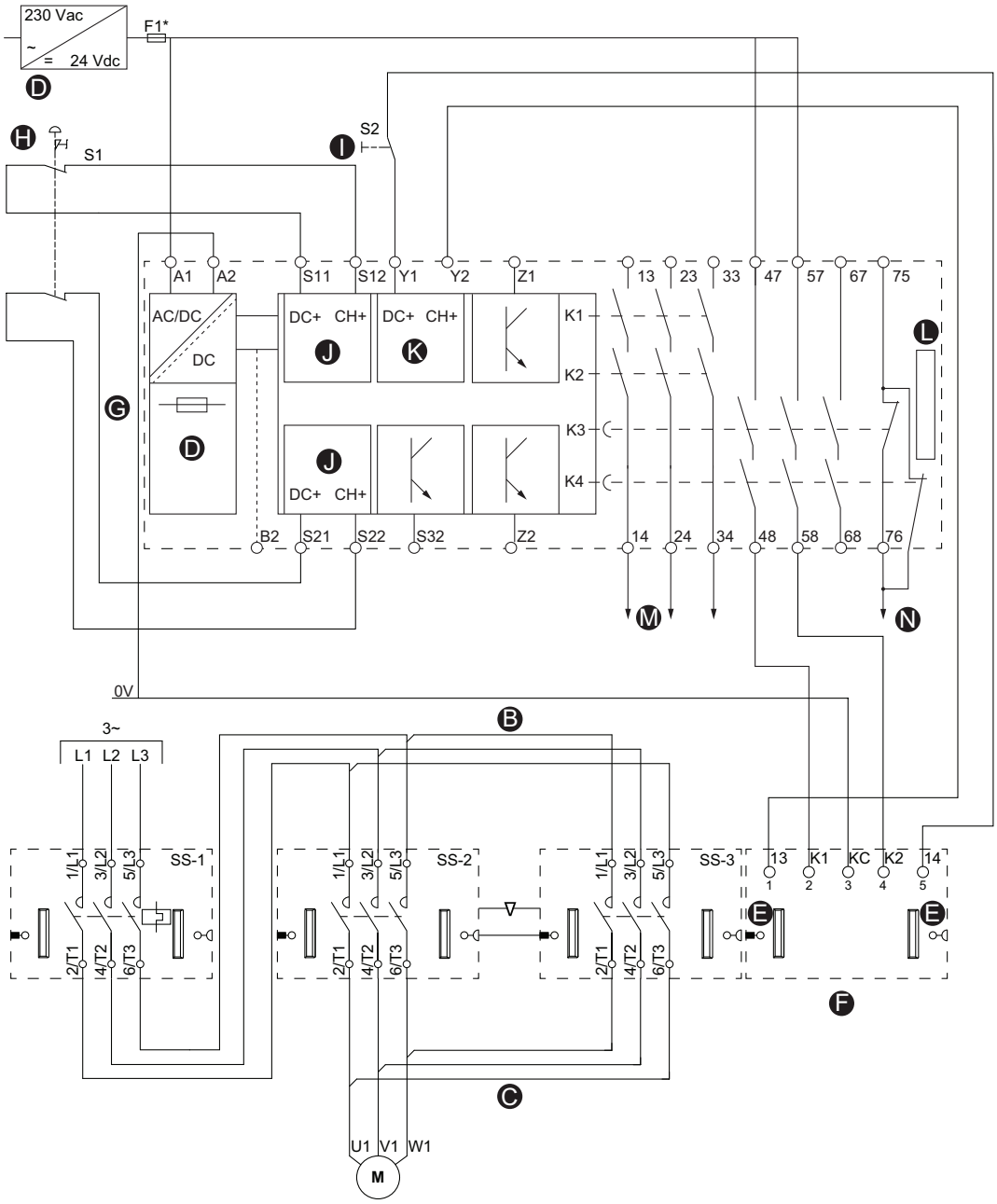


Tabella 15 - Legenda per Esempio: SIL stop, categoria stop 1, categoria cablaggio 3/4, pagina 52

B	Collegamento parallelo	I	Pulsante di avvio S2
C	Collegamento inverso	J	Ingresso
D	Alimentazione	K	Avvio
E	Connettore cavo piatto	L	Estensione

36. Livello di integrità della sicurezza secondo la norma IEC 61508. Categoria cablaggio 3/4 in conformità con ISO 13849. Categoria stop 1 in conformità con la norma EN/IEC 60204-1.

Tabella 15 - Legenda per Esempio: SIL stop, categoria stop 1, categoria cablaggio 3/4 (Continuare)

F	Modulo interfaccia SIL (SIM)	M	Stop controllato
G	Modulo Preventa XPS-UAF	N	Categoria stop 1
H	Pulsanti di arresto di emergenza (S1)		

Dati tecnici

Modulo interfaccia SIL

Tabella 16 - Valori calcolati del modulo interfaccia SIL[37] (SIM)

Architettura	SIM					
	PFH[38]	**PFD[39]**	**SFF[40]**	**HFT[41]**	**$MTTF_d$ (anni)**	**CC[42]**
Categoria cablaggio 1[43]	Da $2,10^{-10}$ a	Da $2,10^{-5}$ a	>90%	1	17.459	Non pertinente
Categoria cablaggio 2			>99%			90%
Categoria cablaggio 3			>99%			90%
Categoria cablaggio 4			99%			99%

NOTA: I valori PFD e PFH vengono calcolati come segue:

- Intervallo di prova = 20 anni
- MTTR[44]=MRT[45]= 24 ore

Requisiti architetturali definiti in IEC 61508-2 tabella 3 e EN 62061 tabella 5 conformi ai livelli fino a SIL 3.

Starter SIL

I dati seguenti consentono di definire il livello di prestazioni per gli starter SIL[37].

B10: **1.000.000**

% di guasti pericolosi[46]: **73%**

$B10_d$: **1.369.863**

Supponendo un numero di operazioni = 131.400 cicli/anno (media di 15 cicli/ora)

La tabella seguente contiene i valori calcolati dello starter SIL:

Tabella 17 - Starter SIL nel canale singolo

Categoria cablaggio[43]	**SFF**	**HFT**	**$MTTF_d$ (anni)**	**CC**
Categoria 1	27%	0	100 anni	Non pertinente
Categoria 2: monitoraggio diretto	90%	0	100 anni	≥ 90%

37. Livello di integrità della sicurezza secondo la norma IEC 61508.
38. Frequenza media del guasto pericoloso [h-1], secondo la definizione di IEC 61508-4
39. Probabilità di un guasto pericoloso a richiesta, secondo la definizione di IEC 61509-4.
40. Frazione guasti in sicurezza, secondo la definizione di IEC 61509-4.
41. Tolleranza ai guasti in sicurezza, secondo la definizione di IEC 61509-4.
42. Copertura diagnostica, secondo la definizione di IEC 61509-4.
43. Categorie cablaggio 1, 2, 3 e 4 in conformità con ISO 13849.
44. Tempo medio alla riparazione, secondo la definizione di IEC 61509-4
45. Tempo medio di riparazione, secondo la definizione di IEC 61509-4
46. Guasto pericoloso secondo la definizione di IEC 61508-4

Tabella 18 - Starter SIL nel canale doppio

Categoria di cablaggio	SFF	HFT	$MTTF_d$ (anni)	CC
Categoria 3	27%	0	100 anni	≥ 90%
Categoria 4	90%	0	100 anni	≥ 99%

Il rapporto tra PFH_d e PFD degli starter SIL, a seconda dell'architettura e dell'intervallo di prova, viene indicato nella tabella seguente:

Tabella 19 - Starter SIL: PFH_d e PFD

Categoria di cablaggio	PFH (IEC 61508)	PFD (IEC 61508) Ti=10 anni[47]	PFD (IEC 61508) Ti=5 anni[47]
Categoria 1	1.10E-06	4.80E-02	4.82E-03
Categoria 2: monitoraggio diretto	1.10E-06	4.82E-03	5.06E-04
Categoria 3	4.5E-09	-	1.30E-04
Categoria 4	2.5E-10	-	2.5E-06

Requisiti architetturali definiti in IEC 61508-2 tabella 3 e EN 62061 tabella 5 conformi ai livelli fino a SIL 2.

Architettura di categoria 2 necessaria per soddisfare i vincoli architetturali SIL 2 (conseguiti tramite il monitoraggio diretto Mirror In/Mirror Out).

NOTA: Il rilevamento dei guasti e la reazione ai guasti specificata devono essere eseguiti prima che possa verificarsi la situazione pericolosa gestita dalla funzione di controllo collegata alla sicurezza.

47. Intervallo di prova

Dati sull'affidabilità

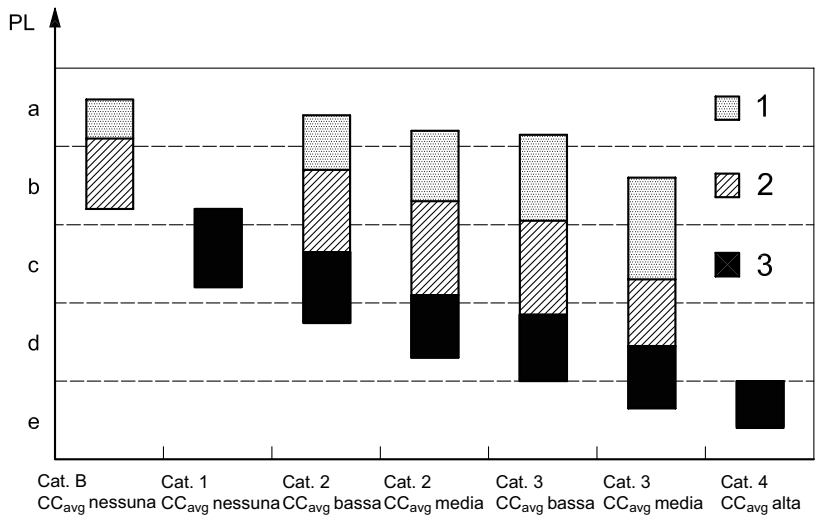
Riferimenti alla norma della funzione di sicurezza

La funzione di stop SIL[48] ha la priorità su uno stop attivato per motivi operativi (EN ISO 13849-1, 5.2.1).

Il livello di prestazioni dipende dalla categoria di cablaggio[49], $MTTF_d$, e DC_{avg}.

Lo schema seguente mostra la posizione di TeSys™ island in base ai requisiti della categoria.

Figura 24 - Posizione di TeSys island in base ai requisiti della categoria



Chiave

PL: livello di prestazione

1 $MTTF_d$ di ciascun canale = bassa

2 $MTTF_d$ di ciascun canale = media

3 $MTTF_d$ di ciascun canale = alta

Tabella 20 - Procedura semplificata per la valutazione del PL ottenuto dalle parti dei sistemi di comando legate alla sicurezza (SRP/CS)

Categoria	**B**	**1**	**2**	**2**	**3**	**3**	**4**
CC_{avg}	**nessuna**	**nessuna**	**bassa**	**media**	**bassa**	**media**	**alta**
$MTTF_d$ di ciascun canale							
basso	a	non coperto	a	b	b	c	non coperto
medio	b	non coperto	b	c	c	d	non coperto
alto	non coperto	c	v	d	d	d	e

In base all'architettura e alla categoria di cablaggio di TeSys island, gli indicatori chiave (CC_{avg}, $MTTF_d$, PL) per TeSys island sono conformi ai valori indicati nella tabella seguente.

48. Livello di integrità della sicurezza secondo la norma IEC 61508.
49. Categorie cablaggio in conformità con ISO 13849.

Tabella 21 - Valori degli indicatori chiave per le architettura a canale singolo e doppio

Architettura del sistema TeSys island	Categoria	Tolleranza ai guasti singoli[50]	CC_{avg}	$MTTF_d$ di ciascun canale	PL mirato
Canale singolo	1	No	Nessuno	Alto (≥ 30 anni)	c
	2	No	Da basso (≥ 60%) a medio (≥ 90%)	Da basso (≥ 3 anni) ad alto (≥ 30 anni)	c, d
Canale doppio	3	Sì			c, d, e
	4	Sì	Alto (≥ 99%)	Alto (≥ 30 anni)	e

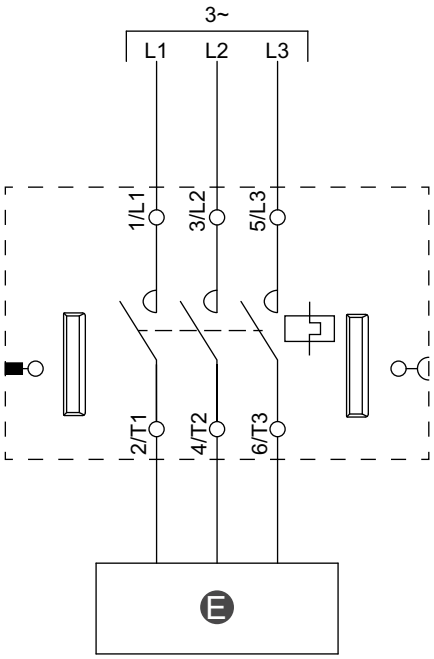
Cablaggio avatar SIL

Gli schemi di cablaggio in questa sezione sono per gli avatar SIL[51] La tabella seguente contiene una legenda per gli schemi di questa sezione.

Tabella 22 - Legenda degli schemi di cablaggio

A	Interblocco meccanico
B	Collegamento parallelo
C	Collegamento inverso
E	Circuito elettrico

Figura 25 - Contattore: SIL Stop, categoria cablaggio 1/2[52]



50. La tolleranza ai guasti singoli significa che un singolo guasto (compresi gli eventi in modalità comune) non devono causare la perdita della funzione di sicurezza.
51. Livello di integrità della sicurezza secondo la norma IEC 61508.
52. Categoria cablaggio 1 e 2 in conformità con ISO 13849.

Figura 26 - Motore a un senso di marcia: SIL Stop, categoria cablaggio 1/2

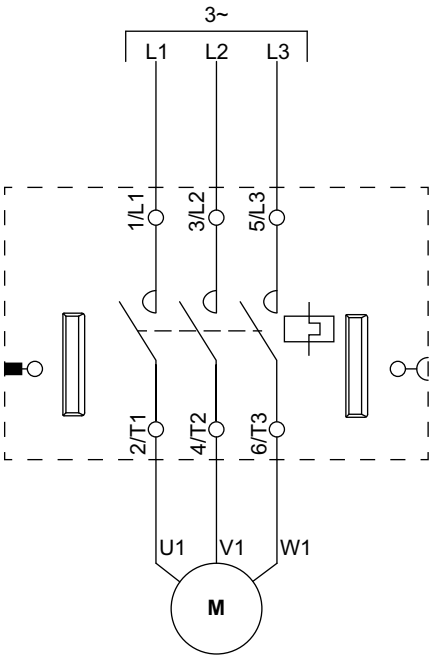


Figura 27 - Motore a due sensi di marcia: SIL Stop, categoria cablaggio 1/2

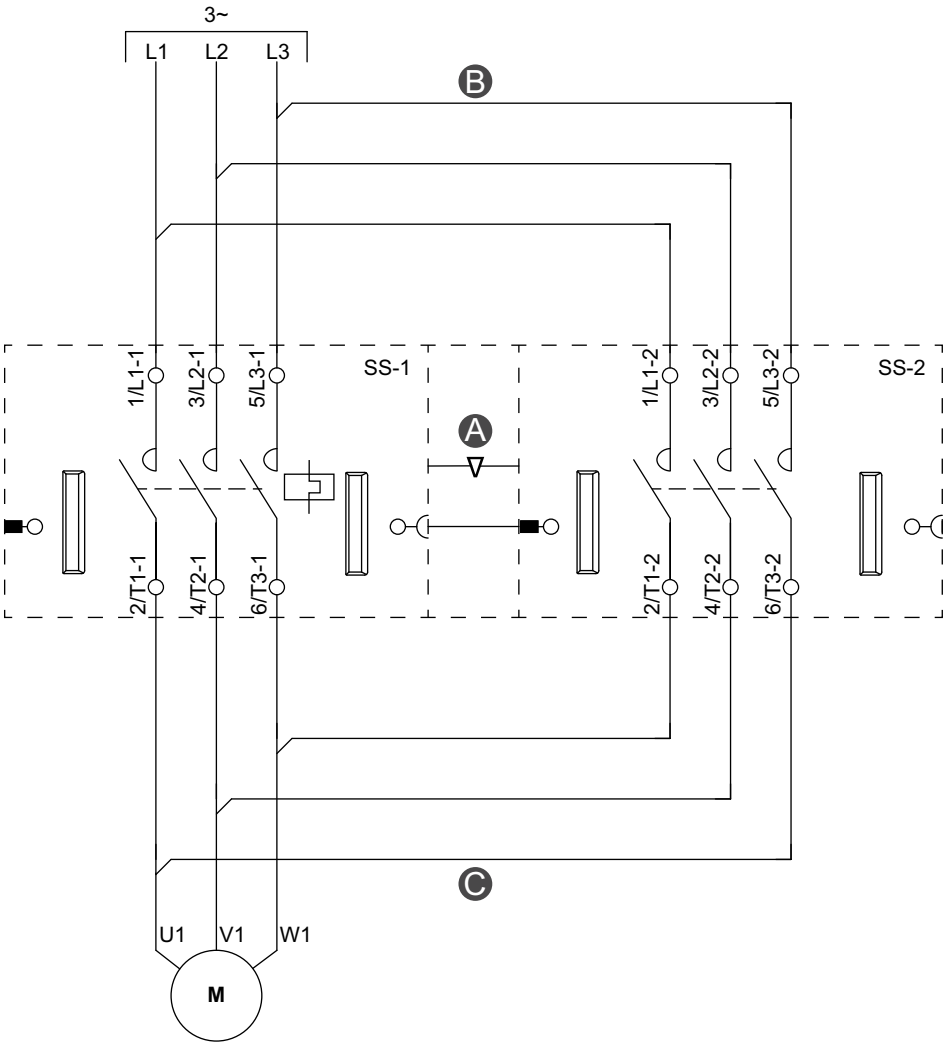


Figura 28 - Motore a due velocità: SIL Stop, categoria cablaggio 1/2

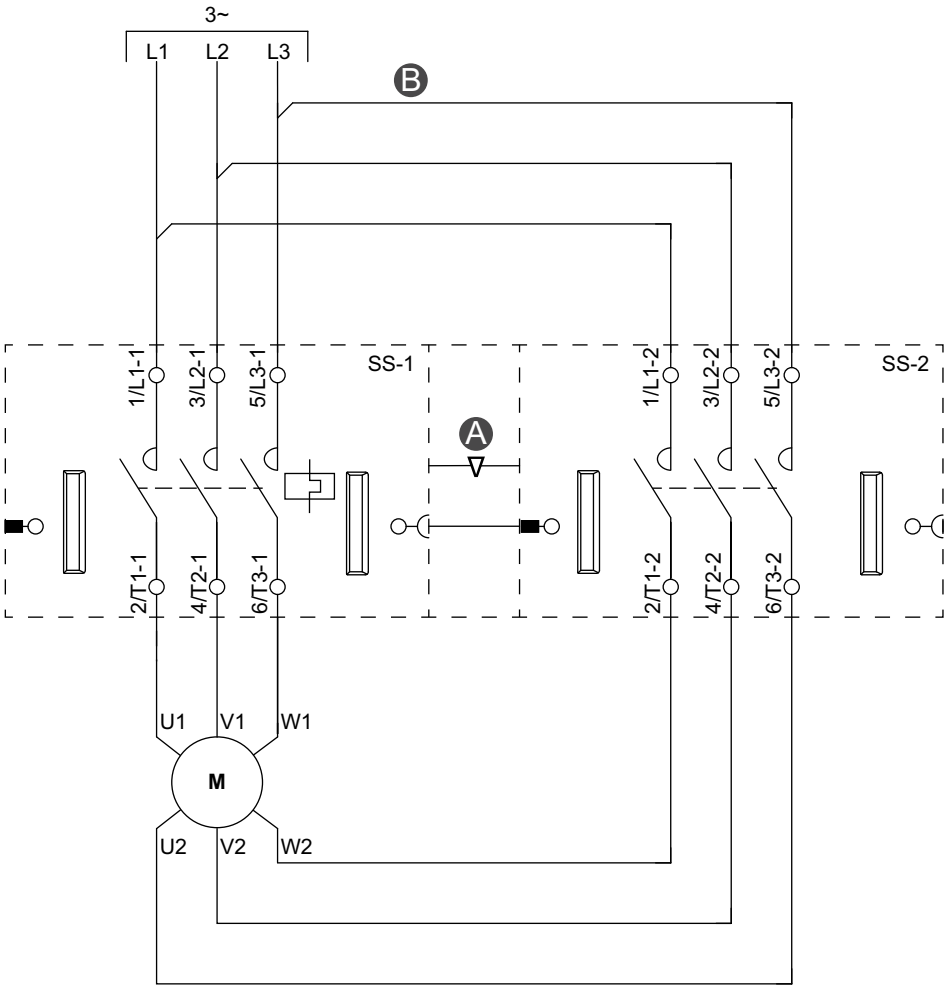


Figura 29 - Motore due velocità e due sensi di marcia: SIL Stop, categoria cablaggio 1/2

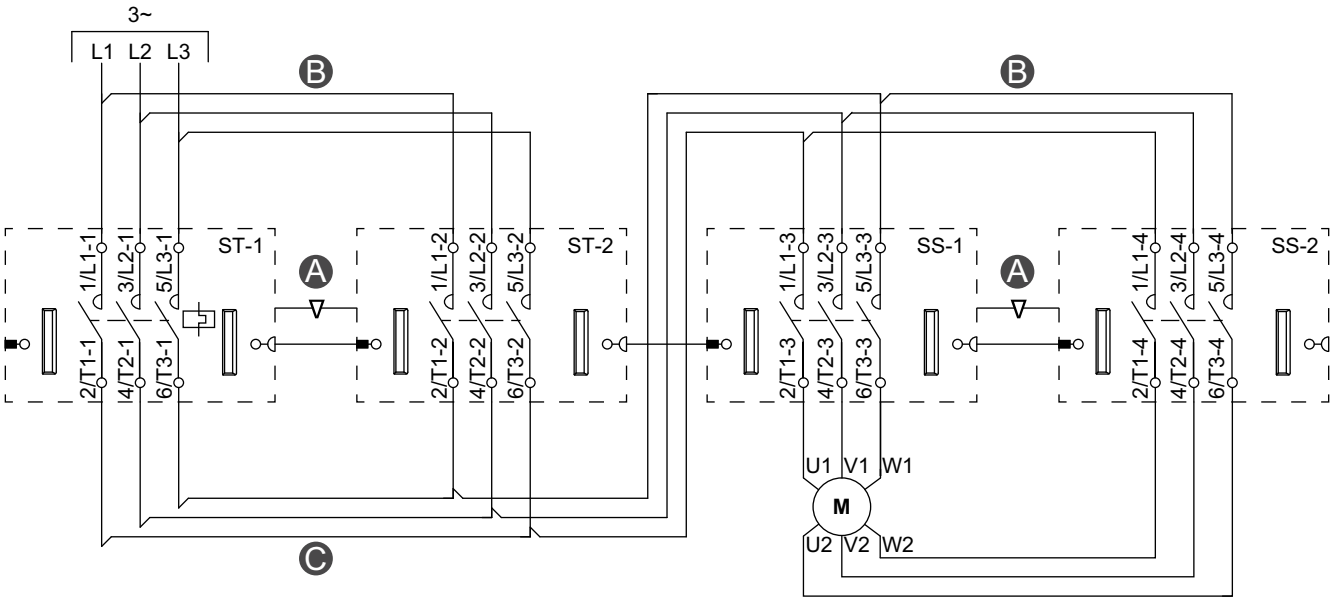


Figura 30 - Contattore: SIL Stop, categoria cablaggio 3/4[53]

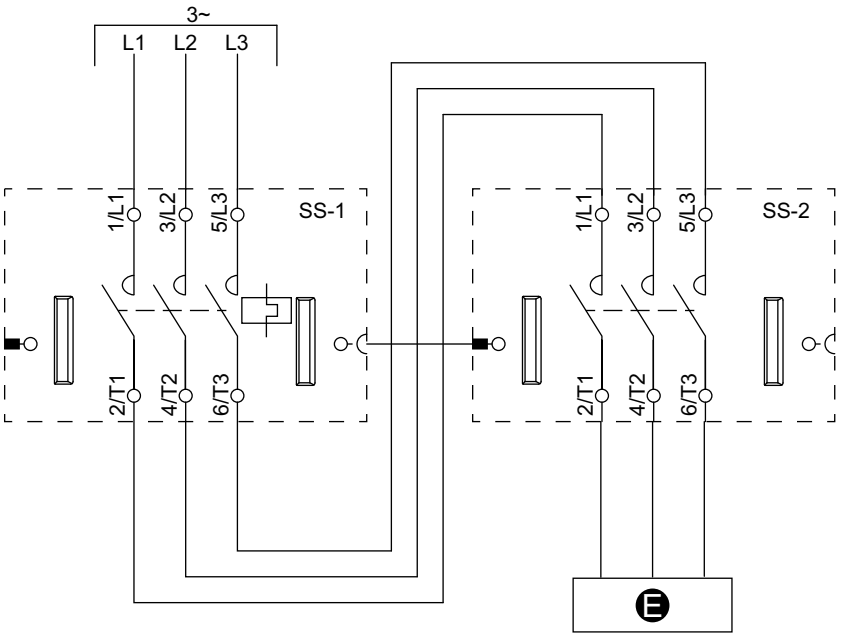
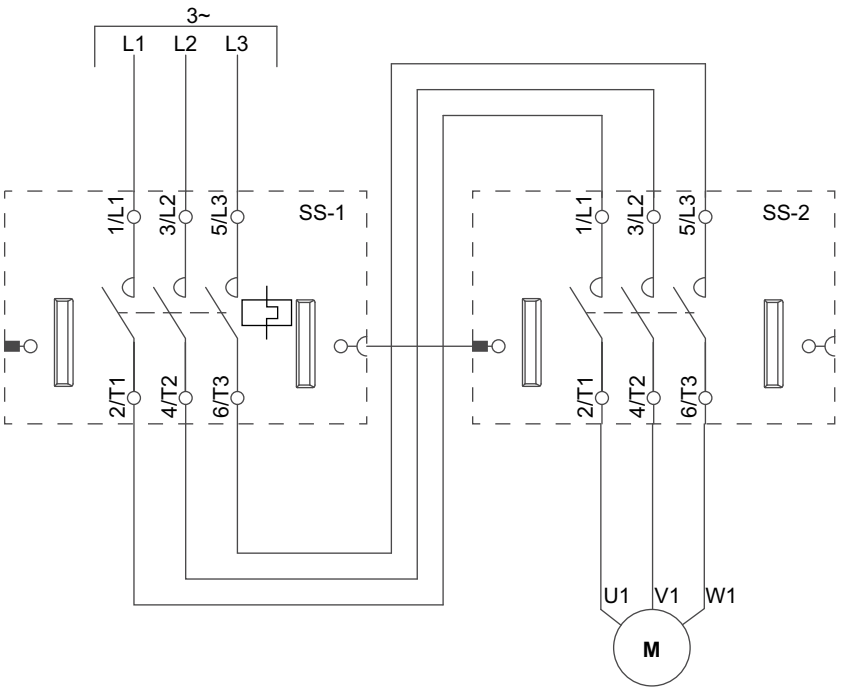


Figura 31 - Motore a un senso di marcia: SIL Stop, categoria cablaggio 3/4



53. Categoria cablaggio 3 e 4 in conformità con ISO 13849.

Figura 32 - Motore a due sensi di marcia: SIL Stop, categoria cablaggio 3/4

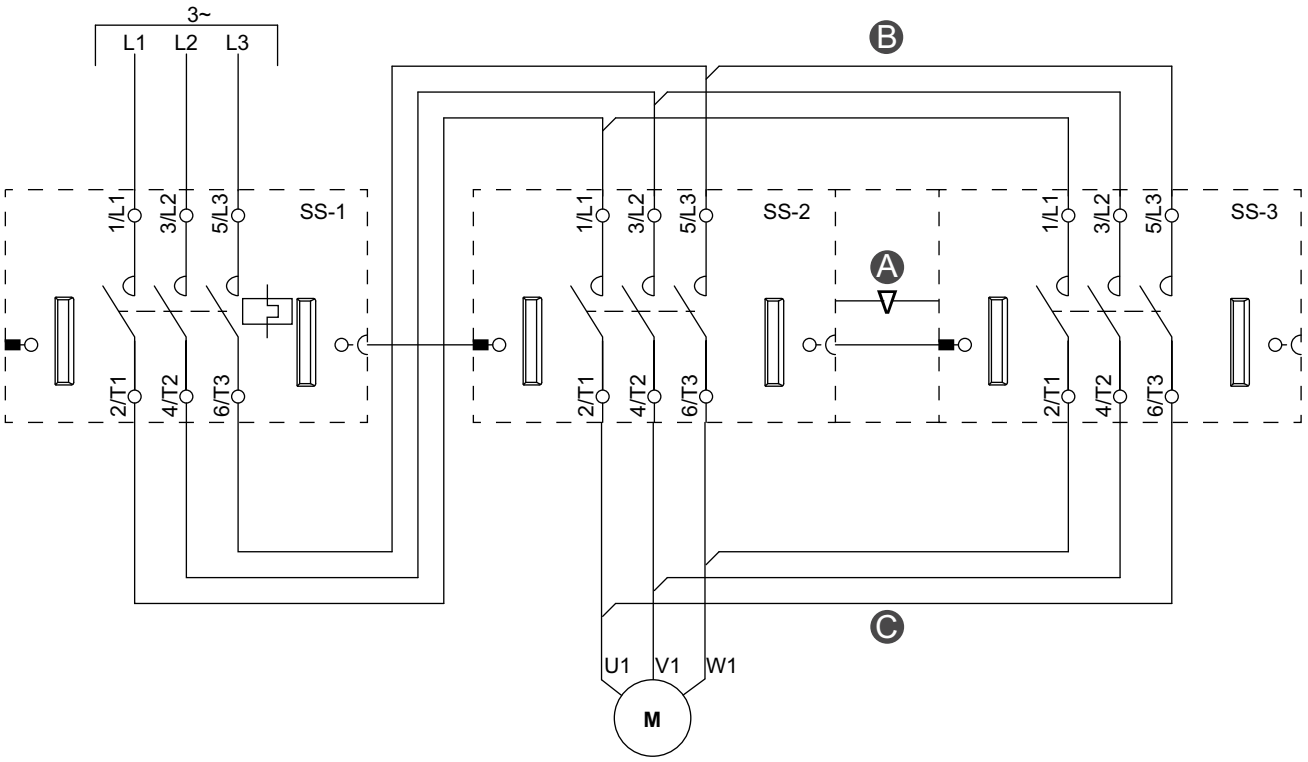


Figura 33 - Motore a due velocità: SIL Stop, categoria cablaggio 3/4

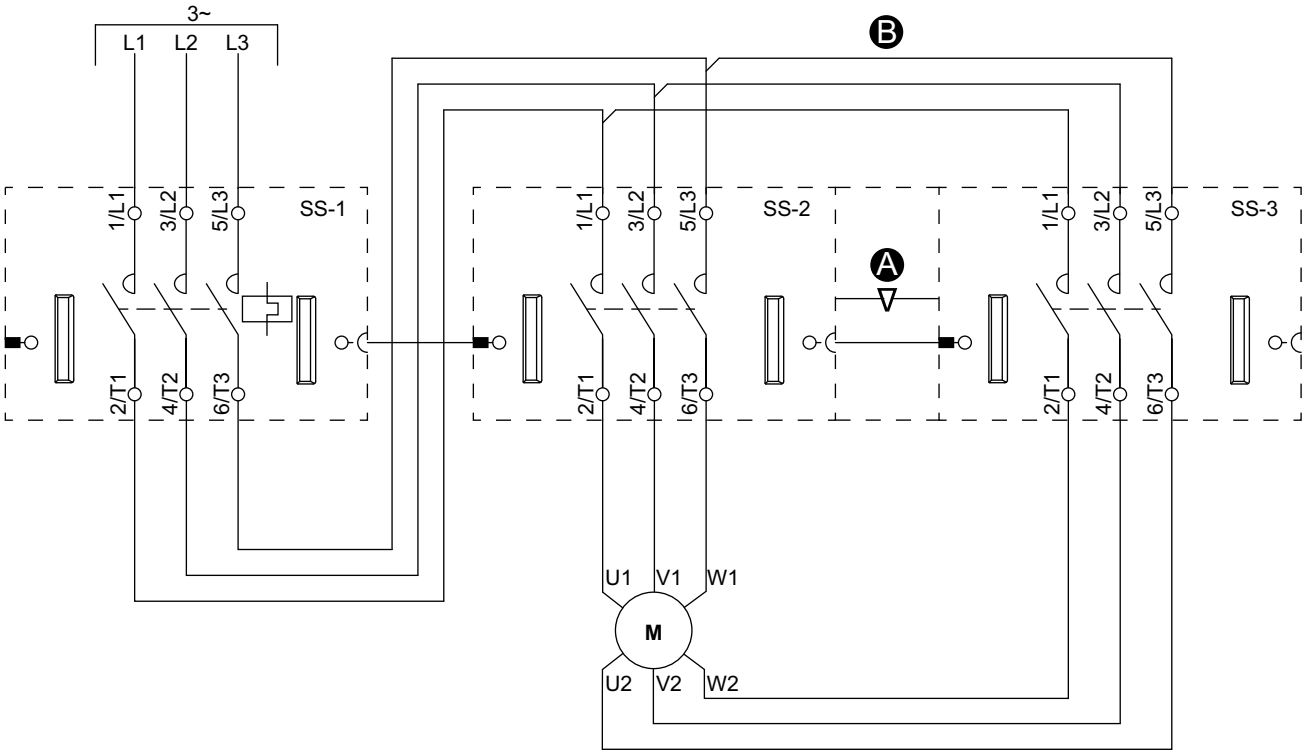


Figura 34 - Motore due velocità e due sensi di marcia: SIL Stop, categoria cablaggio 3/4

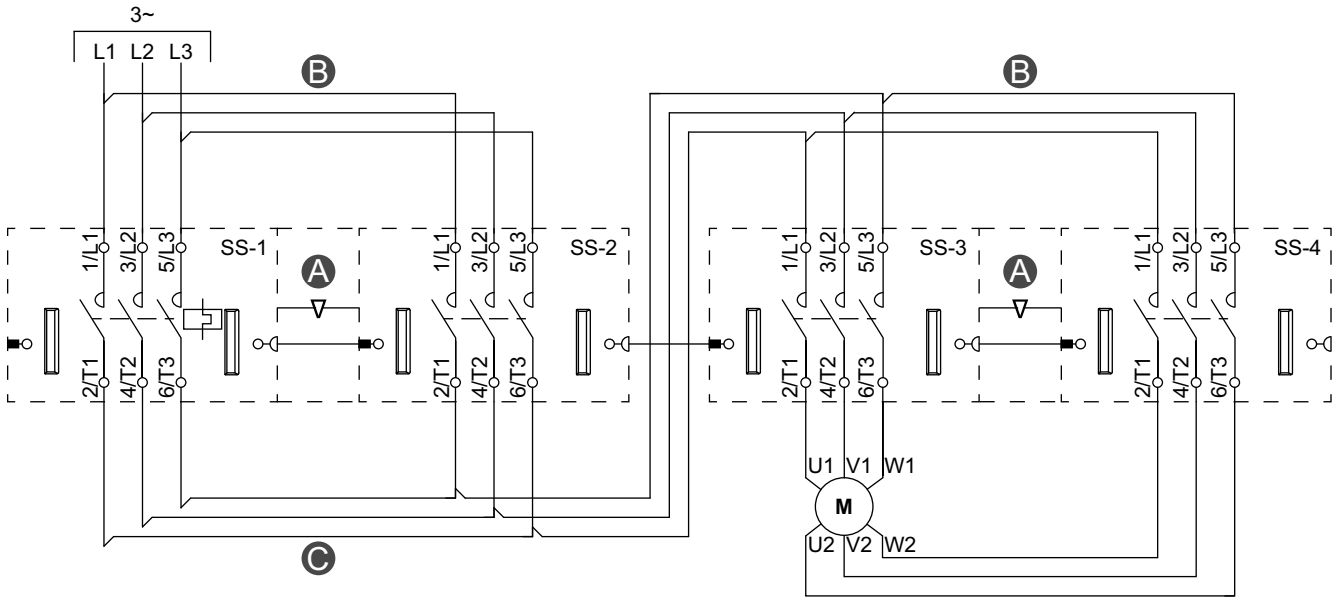


Figura 35 - Trasportatore a un senso di marcia: SIL Stop, categoria cablaggio 1/2

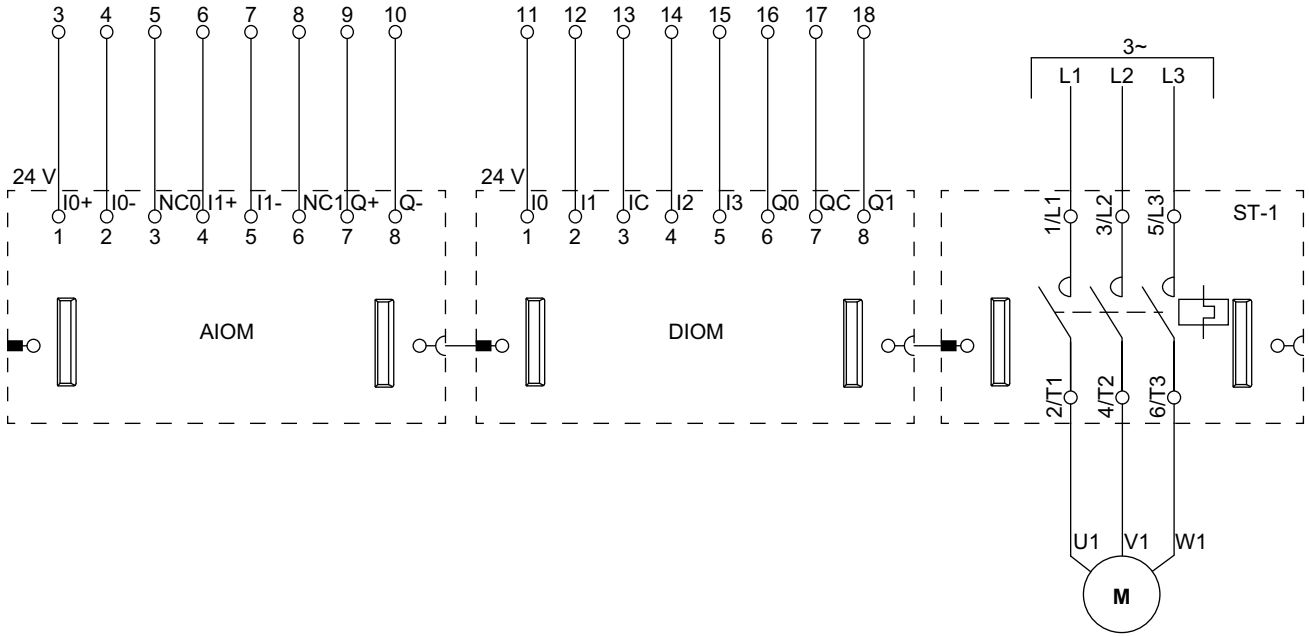
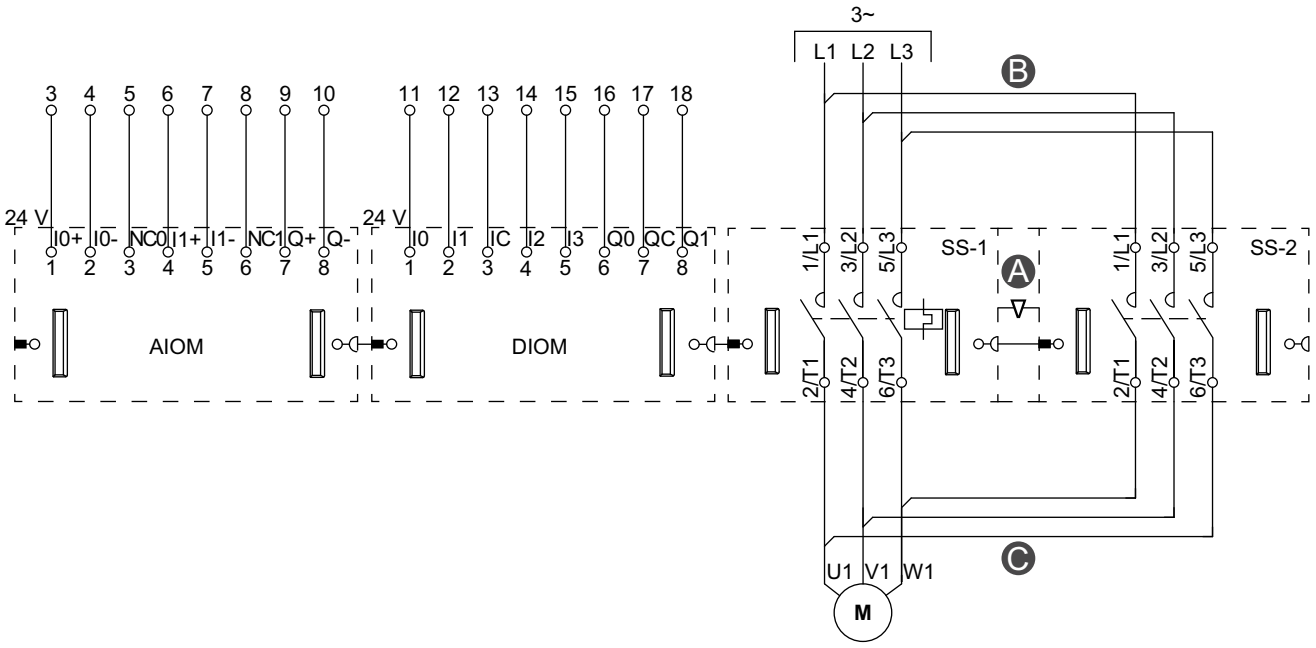


Figura 36 - Trasportatore a un senso di marcia: SIL Stop, categoria cablaggio 1/2



Messa in funzione della funzione di sicurezza

Seguire questa procedura per mettere in funzione la funzione di sicurezza. La procedura comprende due fasi:

- test installazione
- collaudo funzione di sicurezza[54]

Test installazione

Eseguire le operazioni indicate nella tabella seguente per testare l'installazione della funzione di sicurezza.

Tabella 23 - Test installazione

1	Mediante il pannello **DIAGNOSTICA** nel DTM di TeSys™ island, verificare che la topologia fisica corrisponda alla topologia logica.
2	Mediante il pannello **IL MIO AVATAR** nel DTM di TeSys island, verificare nei **PARAMETRI AVATAR** che gli avatar SIL[55] siano associati al gruppo SIL corretto.

Collaudo funzione di sicurezza

Eseguire il collaudo funzione di sicurezza su ciascun gruppo SIL[55] dell'isola. Un gruppo SIL può comprendere vari avatar SIL gestiti da un modulo interfaccia SIL (SIM).

Il collaudo della funzione di sicurezza viene completato se, dopo aver attivato il dispositivo di arresto di emergenza associato a un gruppo SIL, tutti gli starter SIL appartenenti a quel gruppo SIL entrano nello stato sicuro (il carico viene diseccitato).

> **NOTA:** Per la categoria stop 0 (stop non controllato), lo stop deve essere immediato. Per la categoria stop 1 (stop controllato) lo stop entra in funzione dopo un ritardo.[56]

Eseguire le fasi riportate nella tabella seguente per ciascun gruppo SIL sull'isola per eseguire il collaudo della funzione di sicurezza.

54. Collaudo della funzione in base alla definizione presente nella norma IEC 62061
55. Livello di integrità della sicurezza secondo la norma IEC 61508.
56. Categoria Stop 0 e 1 in conformità con EN/IEC 60204-1.

Tabella 24 - Collaudo funzione di sicurezza

1	Attivare il dispositivo di arresto di emergenza associato al gruppo SIL, quindi verificare che tutti gli starter SIL appartenenti al gruppo entrino nello stato sicuro (il carico viene diseccitato). **NOTA:** il LED di stato del dispositivo (DS) emette una luce rossa lampeggiante sugli starter SIL, che indica uno stato di evento lieve del dispositivo. Se il test non viene superato: • Il dispositivo di arresto di emergenza potrebbe essere collegato al SIM sbagliato. Controllare questi collegamenti. • Il dispositivo di arresto di emergenza potrebbe essere collegato in modo errato al SIM. Controllare questi collegamenti. • Alcuni avatar SIL potrebbero non essere collegati al gruppo SIL previsto. Controllare la configurazione.
2	Nel pannello **AVATAR** del DTM o OMT di TeSys™ island, sezione **DIAGNOSTICA**, controllare **STATO** e **REGISTRI EVENTI** per verificare che **Stato gruppo SIL** sia uguale a "**Comando di stop**". Nel Registro eventi viene visualizzato il messaggio "Comando Stop Gruppo SIL, Stato sicuro raggiunto." Se il test non viene superato: • Alcuni avatar SIL potrebbero non essere collegati al gruppo SIL previsto. Controllare la configurazione.
3	Nella sezione **DISPOSITIVI** del pannello **DIAGNOSTICA**, verificare che lo **Stato del Modulo interfaccia SIL** (SIM) sia uguale a "**Comando di stop**". Nel Registro eventi viene visualizzato il messaggio "Comando Stop Gruppo SIL, Stato sicuro raggiunto." Se il test non viene superato: • Il dispositivo di arresto di emergenza potrebbe essere collegato al SIM sbagliato. Controllare questi collegamenti. • Il dispositivo di arresto di emergenza potrebbe essere collegato in modo errato al SIM. Controllare questi collegamenti.
4	Eseguire un comando di avvio a un avatar SIL appartenente al gruppo SIL e verificare che l'avvio non venga completato: gli starter devono restare aperti e il comando di avvio deve essere ignorato fino a quando il dispositivo di arresto di emergenza viene resettato. Se il test non viene superato: • Alcuni avatar SIL potrebbero non essere collegati al gruppo SIL previsto. Controllare la configurazione. Se alcuni di questi collaudi continuano ad avere esito negativo nonostante le azioni correttive, non continuare a utilizzare l'isola. Sostituire i dispositivi che non hanno superato il collaudo.
5	Dopo aver completato il collaudo della funzione di sicurezza, reimpostare il dispositivo di arresto di emergenza e verificare che tutti gli starter SIL e i moduli interfaccia SIL si trovino nello stato Pronto (il LED DS emette una luce verde fissa).

Requisiti di manutenzione della funzione di sicurezza

Questa sezione descrive gli interventi ordinari necessari per la manutenzione della sicurezza funzionale di TeSys™ island.

Piano di manutenzione

Gli intervalli di manutenzione dipendono dalla modalità di frequenza.

- Per la modalità di frequenza bassa (numero medio annuale dei cicli del contattore inferiore a 15 cicli/ora), eseguire la manutenzione ogni 12 mesi.
- Per la modalità frequenza alta (numero medio annuale dei cicli del contattore superiore a 15 cicli/ora o 136.986 cicli/anno), eseguire la manutenzione a intervalli di 1/10° della durata stimata del dispositivo.

La durata stimata del dispositivo (anni) = B10d (=1.369.863)/numero medio annuale di cicli del contattore

Controlli di manutenzione

Controlli di utilizzo del dispositivo

Eseguire i controlli descritti nella tabella seguente per verificare che i cicli del contattore dello starter SIL[57] rientrino nei valori del ciclo di vita accettabili.

1	Utilizzando la funzione **DIAGNOSTICA** del DTM o OMT di TeSys™ island, accedere alle informazioni degli asset del dispositivo per ciascuno starter SIL.
2	Se il **numero di cicli del contattore** è maggiore di B10d (=1.369.863), sostituire lo starter SIL.
3	In caso contrario, utilizzare il **numero di cicli del contattore** per programmare la manutenzione successiva. Vedere Piano di manutenzione, pagina 66.

Collaudo funzione di sicurezza

Eseguire il collaudo funzione di sicurezza su ciascun gruppo SIL[57] . Vedere Collaudo funzione di sicurezza, pagina 64.

57. Livello di integrità della sicurezza secondo la norma IEC 61508.

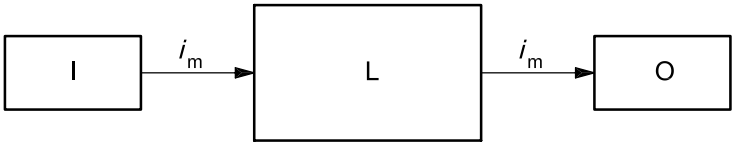
Appendice: Architettura a canale singolo

Questa architettura a canale singolo comprende le categorie di cablaggio 1 e 2.

Requisiti architettonici per la categoria cablaggio 1

L'architettura designata per la **categoria 1** è definita nella norma EN ISO 13849-1, 6.2.4.

Figura 37 - Architettura designata per la categoria 1 (EN ISO 13849-1).



I: dispositivo di ingresso

L: logica

O: dispositivo di uscita

^{i}**m**: mezzi di interconnessione

La parte del sistema di comando legata alla sicurezza (SRP/CS), della categoria di cablaggio 1, deve essere designata e realizzata utilizzando **componenti ben collaudati**.

Un "componente ben collaudato" per un'applicazione legata alla sicurezza è un componente:

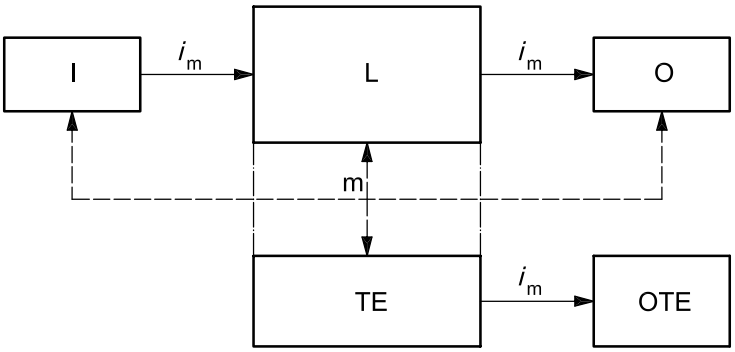
- ampiamente utilizzato in passato con risultati positivi in applicazioni simili oppure
- realizzato e verificato mediante principi che ne dimostrano l'idoneità e l'affidabilità per applicazioni legate alla sicurezza.

Non esiste **alcuna copertura diagnostica** (CC_{avg} = nessuna) nei sistemi di categoria 1.

Requisiti architettonici per la categoria cablaggio 2

L'architettura designata per la **categoria 2** viene definita nella norma EN ISO 13849-1, 6.2.5.

Figura 38 - Architettura designata per la categoria 2 (EN ISO 13849-1).



I: dispositivo di ingresso

L: logica

O: dispositivo di uscita

i**m**: mezzi di interconnessione

m: monitoraggio

TE: apparecchiatura di prova

OTE: uscita dell'apparecchiatura di prova

Le parti dei sistemi di comando legate alla sicurezza (SRP/CS) della categoria di cablaggio 2 devono essere progettate in modo che le relative funzioni vengano controllate a intervalli appropriati dal sistema di comando della macchina.

Nell'architettura a canale singolo, un SIM è associato a uno starter SIL[58].

Nello specifico, per la categoria di cablaggio 2, il contatto mirror viene collegato al modulo Preventa™ XPS (o equivalente). Se lo stato della linea di feedback del contatto mirror non è uguale allo stato di uscita del modulo Preventa XPS (o equivalente), il modulo Preventa XPS (o equivalente) blocca un secondo avvio.

NOTA: Il feedback del contatto mirror trasmette solo le informazioni della diagnosi.

58. Livello di integrità della sicurezza secondo la norma IEC 61508.

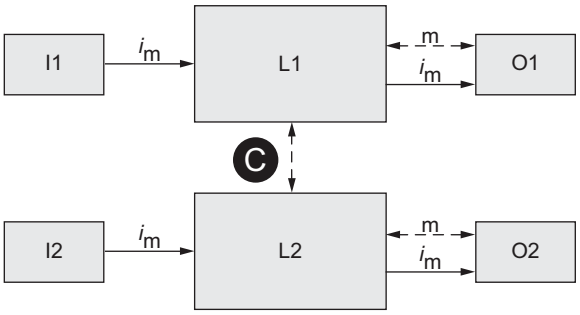
Appendice: Architettura a doppio canale

Questa architettura a doppio canale comprende le categorie di cablaggio 3 e 4.

Requisiti architettonici per la categoria cablaggio 3

L'architettura designata per la categoria 3 è definita nella norma EN ISO 13849-1, 6.2.6.

Figura 39 - Architettura designata per la categoria 3 (EN ISO 13849-1).



im: mezzi di interconnessione

L1, L2: logica

c: monitoraggio incrociato

m: monitoraggio

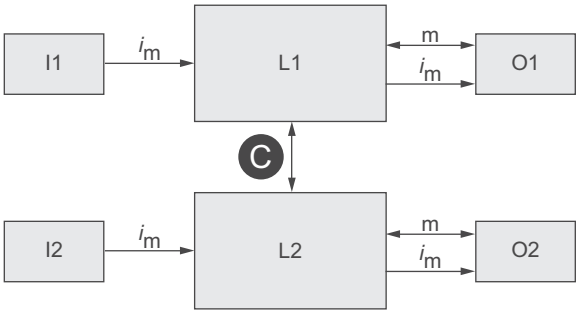
I1, I2: dispositivo di ingresso, (es. sensore)

O1, O2: dispositivo di uscita, (es. contattore principale)

Requisiti architettonici per la categoria cablaggio 4

L'architettura designata per la categoria 4 è definita nella norma EN ISO 13849-1, 6.2.7.

Figura 40 - Architettura designata per la categoria 4 (EN ISO 13849-1).



im: mezzi di interconnessione

L1, L2: logica

c: monitoraggio incrociato

m: monitoraggio

I1, I2: dispositivo di ingresso, (es. sensore)

O1, O2: dispositivo di uscita, (es. contattore principale)

Le linee continue per il monitoraggio rappresentano la copertura diagnostica che è maggiore di quella nell'architettura designata per la categoria 3.

Glossario

A

Frequenza media del guasto pericoloso [h^{-1}] (PFH). (Guasto pericoloso secondo la definizione di IEC 61508-4)

Per mantenere la funzione di sicurezza, la norma IEC 61508 richiede vari livelli di misurazioni per evitare e controllare gli errori rilevati, a seconda del SIL[59] richiesto.

Tutti i componenti di una funzione di sicurezza devono essere soggetti a una valutazione delle probabilità per valutare l'efficacia delle misure implementate per il controllo dei guasti rilevati.

Questa valutazione ha determinato il PFH (Frequenza media del guasto pericoloso[60] [h^{-1}]) per un sistema legato alla sicurezza. Si tratta della probabilità oraria che un sistema legato alla sicurezza subisca un guasto pericoloso e che non sia possibile eseguire correttamente la funzione di sicurezza.

A seconda del SIL, il PFH non deve superare determinati valori per l'intero sistema legato alla sicurezza.

Vengono aggiunti i singoli valori PFH di una catena di funzioni. Il risultato non deve superare il valore massimo specificato nella norma.

Livello di integrità di sicurezza	**Frequenza media del guasto pericoloso[60] [h^{-1}] (PFH) a richiesta elevata o richiesta continua**
4	Da $10^{-9} \le a < 10^{-8}$
3	Da $10^{-8} \le a < 10^{-7}$
2	Da $10^{-7} \le a < 10^{-6}$
1	Da $10^{-6} \le a < 10^{-5}$

E

Norma EN ISO 13849

Questa norma europea specifica la procedura di convalida, compresa l'analisi dei pericoli, la valutazione dei rischi e la prova, per le funzioni e categorie di sicurezza per le parti dei sistemi di comando legate alla sicurezza. Le descrizioni delle funzioni e dei requisiti di sicurezza per le categorie vengono riportate nella norma ISO 13849-1 riguardante i principi generali per la progettazione. Alcuni requisiti per la validazione sono generici e alcuni specifici della tecnologia utilizzata. La norma EN ISO 13849-2 specifica anche le condizioni in base alle quali deve essere eseguita la validazione tramite la prova delle parti dei sistemi di comando legate alla sicurezza.

Norma EN/IEC 60204-1

La categoria stop 0 viene definita come "l'arresto tramite lo scollegamento immediato dell'alimentazione degli attuatori della macchina (ovvero stop non controllato)."

59. Livello di integrità della sicurezza secondo la norma IEC 61508.
60. Guasto pericoloso secondo la definizione di IEC 61508-4

La categoria stop 1 è definita come "uno stop controllato con l'alimentazione disponibile per gli attuatori della macchina per raggiungere lo stop e quindi lo scollegamento dell'alimentazione al raggiungimento dello stop".

F

Misure per evitare i guasti

Gli errori sistematici nelle specifiche, nell'hardware e nel software, di utilizzo e manutenzione nel sistema legato alla sicurezza devono essere evitati, per quanto possibile. Per rispettare questi requisiti, la norma IEC 61508 specifica varie misure atte a evitare i guasti da adottare in base al SIL[61] richiesto. Queste misure atte a evitare i guasti devono coprire l'intero ciclo di vita del sistema legato alla sicurezza, ovvero dalla progettazione allo smantellamento del sistema.

Sicurezza funzionale

La progettazione della sicurezza funzionale e dell'automazione erano due aree completamente separate in passato, ma di recente sono diventate più integrate.

La progettazione e l'installazione delle soluzioni di automazione complesse vengono semplificate dalle funzioni di sicurezza integrate.

Generalmente, i requisiti di progettazione di sicurezza funzionale dipendono dall'applicazione.

Il livello dei requisiti deriva dal rischio e dal potenziale di pericolo legati all'applicazione specifica.

H

Tolleranza ai guasti hardware (HFT) e frazione guasti in sicurezza (SFF)

A seconda del SIL[62] per il sistema legato alla sicurezza, la norma IEC 61508 richiede una tolleranza ai guasti hardware specifica (HFT) in relazione a una parte specifica di guasti in sicurezza, indicati come frazione guasti in sicurezza (SFF).

La HFT è la capacità di un sistema di eseguire la funzione di sicurezza necessaria nonostante la presenza di uno o più guasti hardware.

La SFF di un sistema viene definita come il rapporto tra i guasti in sicurezza e i guasti totali del sistema.

Secondo la norma IEC 61508, il SIL massimo raggiungibile di un sistema è in parte determinato dalla HFT e dalla SFF del sistema.

Questi tipi dono specificati in base ai criteri definiti dalla norma per gli elementi legati alla sicurezza.

SFF	**Sottosistema HFT tipo A**			**Sottosistema HFT tipo B**		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	-	SIL 1	SIL 2
Da 60% a < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
Da 90% a < 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

61. Livello di integrità della sicurezza secondo la norma IEC 61508.
62. Livello di integrità della sicurezza secondo la norma IEC 61508.

I

Norma IEC 61508

La norma IEC 61508 riguarda la sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili legati alla sicurezza.

Invece di un singolo componente, viene considerata come un'unità un'intera catena di funzioni (es. da un sensore attraverso le unità di elaborazione logiche verso l'attuatore).

Questa catena di funzioni deve rispettare i requisiti del livello di integrità di sicurezza nel suo complesso.

L

Modalità richiesta bassa/elevata

La norma IEC 61508 definisce la modalità di funzionamento della richiesta della funzione di sicurezza:

- modalità richiesta elevata o continua (PFH)
- modalità richiesta bassa (PFDavg, PTI)

M

Tempo medio prima di un guasto pericoloso (MTTF $_d$)

La norma ISO 13849-1 definisce il $MTTF_d$ come previsione del tempo medio prima di un guasto pericoloso.

P

Livello prestazioni (PL)

La norma IEC 13849-1 definisce i cinque livelli di prestazioni (PL) per le funzioni di sicurezza.

Il livello a è il più basso mentre il livello e è il più alto.

Cinque livelli (a, b, c, d ed e) corrispondono a diversi valori di probabilità media di guasto pericoloso all'ora[63] all'ora

Livello delle prestazioni	**Probabilità di guasto pericoloso[63] all'ora**
e	Da ≥ 10^{-8} a < 10^{-7}
d	Da ≥ 10^{-7} a < 10^{-6}
c	Da ≥ 10^{-6} a < 3^{-6}
b	Da ≥ 3x 10^{-6} a < 10^{-5}
a	Da ≥ 10^{-5} a < 10^{-4}

S

63. Guasto pericoloso secondo la definizione di IEC 61508-4

Livello di integrità di sicurezza (SIL)

La norma IEC 61508 definisce i livelli di integrità di sicurezza (SIL) per le funzioni di sicurezza.

SIL 1 è il livello di integrità più basso e SIL 4 il più alto.

Un'analisi dei pericoli e una valutazione dei rischi costituiscono la base per stabilire il livello di integrità di sicurezza necessario.

Questo livello viene utilizzato per stabilire se la catena di funzioni pertinente deve essere considerata come funzione di sicurezza e per definire il relativo potenziale di pericolo.

Schneider Electric
800 Federal Street
01810 Andover, MA
USA

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

www.schneider-electric.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

8536IB1904IT-04