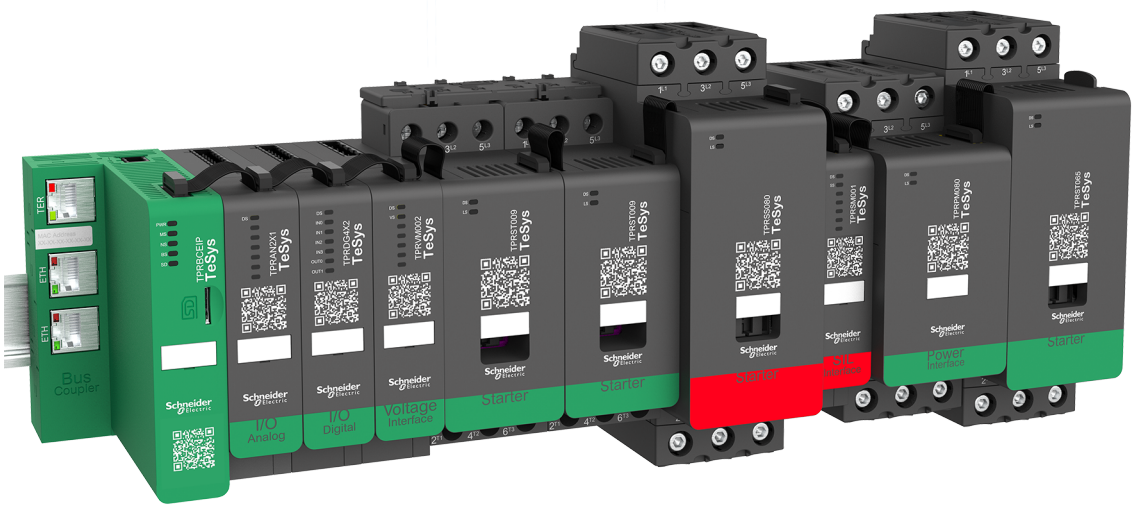
TeSys Active

TeSys™ island – Solution numérique de gestion des moteurs

Guide de sécurité fonctionnelle

TeSys propose des solutions innovantes et connectées pour les démarreurs de moteurs.

8536IB1904FR-04
08/2023



www.schneider-electric.com

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Table des matières

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'équipement ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.

L'ajout d'un de ces symboles à une étiquette de sécurité « Danger » ou « Avertissement » indique qu'il existe un danger électrique qui entraînera des blessures si les instructions ne sont pas respectées.

Ceci est le symbole d'une alerte de sécurité. Il sert à vous avertir d'un danger potentiel de blessures corporelles. Respectez toutes les consignes de sécurité accompagnant ce symbole pour éviter toute situation potentielle de blessure ou de mort.

⚠ DANGER

DANGER indique un danger immédiat qui, s'il n'est pas évité, **entraînera** la mort ou des blessures graves.

⚠ AVERTISSEMENT

AVERTISSEMENT indique un danger potentiel qui, s'il n'est pas évité, **pourrait entraîner** la mort ou des blessures graves.

⚠ ATTENTION

ATTENTION indique un danger potentiel qui, s'il n'est pas évité, **pourrait entraîner** des blessures légères ou de gravité moyenne.

AVIS

AVIS concerne des questions non liées à des blessures corporelles.

Remarque importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

On entend par personnel qualifié des personnes disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

Au sujet de ce guide

Champ d’application

Ce document aborde les points suivants en lien avec la sécurité fonctionnelle TeSys™ island :

- Compréhension générale
- Aspects clés à prendre en considération
- Performances
- Description du matériel
- Configurations types
- Exemples d’architecture
- Références aux normes

Champ d’application

Ce guide est valable pour tous les contrôleurs TeSys island. La disponibilité de certaines fonctions décrites dans ce guide dépend du protocole de communication utilisé et des modules physiques installés sur le TeSys island.

Pour obtenir des informations sur la conformité du produit aux directives environnementales (RoHS, REACH, PEP et EOLI), accédez à la page www.se.com/green-premium.

Pour les caractéristiques techniques des modules physiques décrites dans ce guide, voir sur www.se.com.

Les caractéristiques techniques présentées dans ce guide doivent être identiques à celles fournies en ligne. Nous nous réservons cependant le droit de modifier ce contenu lorsque nécessaire pour améliorer la clarté et la précision. Si vous constatez une différence entre les informations contenues dans ce guide et les informations en ligne, utilisez ces dernières.

Document(s) à consulter

Titre du document	Description	Référence
TeSys island – Guide du système, de l'installation et de l'utilisation	Décrit les principales fonctions, l'installation mécanique, le câblage et la mise en service du TeSys island, ainsi que l'utilisation et la maintenance du TeSys island.	DOCA0270FR
TeSys island – EtherNet/IP™ – Guide de démarrage rapide et de la bibliothèque de blocs de fonction	Explique comment intégrer TeSys island et les informations de la bibliothèque TeSys island dans l'environnement EtherNet/IP de Rockwell Software® Studio 5000®.	DOCA0271FR
TeSys island – Guide de sécurité fonctionnelle	Décrit les fonctions de sécurité fonctionnelle de TeSys island.	8536IB1904FR
TeSys island – Guide de blocs de fonction tiers	Contient les informations nécessaires pour créer des blocs de fonction pour équipements tiers.	8536IB1905FR
Guide d'aide en ligne TeSys island pour DTM	Explique comment installer et utiliser diverses fonctions du logiciel de configuration TeSys island et comment configurer les paramètres TeSys island.	8536IB1907FR
TeSys island – Profil environnemental de produit	Décrit les matériaux constitutifs, la recyclabilité et l'impact environnemental potentiel de TeSys island.	ENVPEP1904009
TeSys island – Instructions de fin de vie	Contient les instructions de fin de vie pour TeSys island.	ENVEOLI1904009
TeSys island – Instruction de service du coupleur de bus, TPRBCEIP	Décrit la procédure d'installation du coupleur de bus Ethernet/IP TeSys island.	MFR44097
TeSys island – Instruction de service du coupleur de bus, TPRBCPFN	Décrit la procédure d'installation du coupleur de bus PROFINET TeSys island.	MFR44098
TeSys island – Instruction de service du coupleur de bus, TPRBCPFB	Décrit la procédure d'installation du coupleur de bus PROFIBUS DP TeSys island.	GDE55148
Fiche d'installation TeSys island – Démarreurs et des modules d'interface d'alimentation, Tailles 1 et 2	Décrit la procédure d'installation des démarreurs et modules d'interface d'alimentation taille 1 et taille 2 pour TeSys island.	MFR77070
Fiche d'installation TeSys island – Démarreurs et des modules d'interface d'alimentation, Taille 3	Décrit la procédure d'installation des démarreurs et modules d'interface d'alimentation taille 3 pour TeSys island.	MFR77085
Fiche d'instructions TeSys island Modules d'entrées/ de sorties	Décrit la procédure d'installation des modules d'E/S analogiques et numériques de TeSys island.	MFR44099
Fiche d'instructions TeSys island Interface SIL et modules d'interface de tension	Décrit la procédure d'installation des modules d'interface de tension TeSys island et des modules d'interface SIL[1].	MFR44100

1. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508)

Terminologie issue des normes

Les termes techniques, la terminologie et les descriptions correspondantes du guide utilisent normalement les termes ou définitions des normes pertinentes. Ces normes comprennent notamment les suivantes :

- **EN ISO 13849-1 :** Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception
- **EN ISO 13849-2 :** Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2 : Validation
- **CEI 61508 :** Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité
- **EN 62061 :** Sécurité des machines – Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité
- **CEI 61511 :** Sécurité fonctionnelle – Systèmes de sécurité instrumentés pour l'industrie de procédé
- **EN/CEI 60204-1 :** Sécurité des machines – Équipement électrique des machines – Partie 1 : Exigences générales
- **CEI 61000-6-7 :** Compatibilité électromagnétique (CEM) – Partie 6-7 : Normes génériques – Exigences d'immunité pour les équipements destinés à remplir des fonctions dans un système relatif à la sécurité (sécurité fonctionnelle) sur les sites industriels
- **CEI 60664-5 :** Coordination de l'isolement des équipements dans les systèmes basse tension – Partie 5 : Méthode complète de détermination des distances d'isolement et des lignes de fuite inférieures ou égales à 2 mm
- **CEI 60947-4-1 :** Ensembles d'appareillage basse tension – Partie 4-1 : Contacteurs et démarreurs de moteurs – Contacteurs et démarreurs électromécaniques
- **CEI 60947-5-1 :** Ensembles d'appareillage basse tension – Partie 5-1 : Appareils pour circuit de commande et éléments de commutation – Appareils électromécaniques pour circuits de commande
- **CEI 60947-7-1 :** Ensembles d'appareillage basse tension – Partie 7-1 : Équipements auxiliaires – Blocs de jonction pour conducteurs en cuivre
- **CEI 60947-7-2 :** Ensembles d'appareillage basse tension – Partie 7-2 : Équipements auxiliaires – Bloc de jonction de conducteur de protection pour conducteurs en cuivre
- **EN 50205 :** Relais à contacts guidés (liés mécaniquement)
- **CEI TR 62380 :** Manuel des données de fiabilité – Modèle universel pour la prédiction de la fiabilité des composants électroniques, des circuits imprimés et des équipements

Terminologie de la sécurité fonctionnelle

ATTENTION

La terminologie de sécurité fonctionnelle utilisée dans ce guide est définie ci-dessous.

Terme	Standard	Définition
Tolérance aux défauts	CEI 61511-1	Capacité d'un élément fonctionnel à continuer d'assurer une fonction requise en présence de défauts ou d'erreurs.
Sécurité fonctionnelle	CEI 61508-4	Partie de la sécurité globale relative à l'équipement commandé (EUC) et au système de commande de l'EUC qui dépend du bon fonctionnement des systèmes électriques, électroniques et électroniques programmables (E/E/PE) relatifs à la sécurité et aux autres mesures de réduction des risques
Défaillance en sécurité	CEI 61508-4	Défaillance d'un élément et/ou d'un sous-système et/ou d'un système qui joue un rôle dans la mise en œuvre de la fonction de sécurité qui : 1. entraîne le fonctionnement erroné de la fonction de sécurité pour mettre l'équipement commandé (EUC[2]), ou une partie de l'équipement commandé, en état sécurisé ou pour conserver l'état sécurisé ; ou 2. augmente la probabilité d'un fonctionnement erroné de la fonction de sécurité pour mettre l'équipement commandé (EUC[2] (ou une partie de l'équipement commandé) en état sécurisé ou pour conserver l'état sécurisé.
Proportion de défaillances en sécurité	CEI 61508-4	Rapport entre le taux de défaillances « en sécurité » et le taux de défaillance total du système.
État sécurisé	CEI 61511-1	État du procédé lorsque la sécurité est atteinte.
	CEI 61800-5-2	État du PDS(SR)[3] lorsque la sécurité est atteinte.
Arrêt de sécurité	CEI 61800-5-2	Les fonctions d'arrêt de sécurité sont définies comme suit : • **Contrôle de couple de sécurité (STO)** ◦ Cette fonction permet d'éviter qu'un puissance génératrice de force ne soit fournie au moteur. ◦ Cette *sous-fonction de sécurité* correspond à un arrêt non contrôlé conformément à la catégorie d'arrêt 0 de la norme CEI 60204-1. • **Arrêt de sécurité 1 (SS1)** ◦ Arrêt de sécurité 1 avec décélération contrôlée : SS1-d lance et contrôle la décélération du moteur dans des limites sélectionnées pour arrêter le moteur et exécute la fonction STO (voir 4.2.3.2) lorsque la vitesse du moteur tombe en dessous d'une limite définie. ◦ Arrêt de sécurité 1 avec rampe surveillée : SS1-r lance et surveille la décélération du moteur dans des limites sélectionnées pour arrêter le moteur et exécute la fonction STO lorsque la vitesse du moteur tombe en dessous d'une limite définie. ◦ Arrêt de sécurité 1 temporisé : SS1-t lance la décélération du moteur et exécute la fonction STO après une temporisation spécifique à l'application.
Fonction de sécurité	CEI 61800-5-2	Fonction implémentée par un système relatif à la sécurité ou autres mesures de réduction des risques visant à assurer ou à maintenir un état sécurisé de

2. EUC : Equipment under control
3. système d'entraînement de puissance relatif à la sécurité

Terme	Standard	Définition
		l'équipement ou de la machine entraînée par le PDS(SR) [4] par rapport à un événement dangereux particulier.
Niveau d'intégrité de sécurité (SIL)	CEI 61508	La norme CEI 61508 définit quatre niveaux d'intégrité de sécurité (SIL) pour les fonctions de sécurité : SIL 1 est le niveau d'intégrité le plus bas et SIL 4 le plus élevé. Le niveau d'intégrité de sécurité requis est déterminé sur la base d'une analyse des dangers et d'une évaluation des risques.
Système relatif à la sécurité	CEI 61800-5-2	Système désigné répondant à cette double définition : • Implémente les fonctions de sécurité nécessaires pour assurer ou maintenir un état sécurisé de l'équipement ou de la machine entraînée par les PDS(SR)[5]. • Vise à assurer, seul ou avec d'autres mesures de réduction des risques, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises.
Sous-système	CEI 61800-5-2	Dans l'architecture de haut niveau d'un système relatif à la sécurité, partie de la conception dont la défaillance entraînerait la défaillance d'une fonction relative à la sécurité

Déclaration de conformité CE

Les déclarations de conformité CE pour TeSys™ island sont disponibles sur www.schneider-electric.com.

4. système d'entraînement de puissance relatif à la sécurité
5. Systèmes d'entraînement de puissance relatif à la sécurité

Précautions

Vous devez avoir lu et compris les précautions suivantes avant d'effectuer les procédures décrites dans ce manuel.

⚠⚠DANGER

RISQUES D'ÉLECTROCUTION, D'EXPLOSION OU D'ARC ÉLECTRIQUE

- Seul un personnel qualifié doit effectuer l'installation et l'entretien de cet appareil.
- Mettez hors service toutes les alimentations avant de travailler sur ou dans cet équipement.
- Lors de l'utilisation de cet équipement et de tout produit associé, respectez toujours la tension indiquée.
- Utilisez toujours un dispositif de détection de tension à valeur nominale appropriée pour vous assurer que l'alimentation est coupée.
- Utilisez les verrouillages appropriés dès lors qu'il existe des risques pour le personnel et/ou pour l'équipement.
- Les circuits de ligne électrique doivent être raccordés et protégés conformément aux exigences réglementaires nationales et européennes.
- Portez un équipement de protection individuelle (EPI) adapté et respectez les normes de sécurité en vigueur pour les travaux électriques (normes NFPA 70E, NOM-029-STPS ou CAN/CSA Z462 ou équivalentes).

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

⚠AVERTISSEMENT

RISQUE DE FONCTIONNEMENT INATTENDU

- Pour des instructions complètes sur la sécurité fonctionnelle, reportez-vous au Guide de sécurité fonctionnelle de TeSys™ island, 8536IB1904.
- Vous ne devez en aucun cas démonter, réparer ni modifier cet équipement. Il ne comprend aucune pièce remplaçable par l'utilisateur.
- Installez et utilisez cet équipement dans une armoire adaptée à l'environnement prévu de l'application.
- Chaque implémentation de cet équipement doit être individuellement et rigoureusement testée quant à son bon fonctionnement avant toute mise en service.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ **AVERTISSEMENT :** Ce produit peut vous exposer à des produits chimiques tels que l'oxyde d'antimoine (trioxyde d'antimoine), classé par l'État de Californie comme cancérigène. Pour plus d'informations, voir www.P65Warnings.ca.gov.

Personnel qualifié

Seules des personnes dûment formées, ayant lu et compris le présent manuel et toute autre documentation relative au produit doivent être autorisées à travailler sur et avec ce produit.

La personne qualifiée doit être en mesure de détecter les dangers possibles afférents à la modification des valeurs de paramètre et, plus généralement, au fonctionnement des équipements mécaniques, électriques et électroniques. La personne qualifiée doit être familiarisée avec les normes, dispositions et règlements concernant la prévention des accidents industriels, et doit les observer lors de la conception et de l'implémentation du système.

L'utilisation et l'application des informations contenues dans ce manuel exigent une connaissance experte de la conception et de la programmation des systèmes de contrôle automatisés. Seul vous, l'utilisateur, le constructeur de machines ou l'intégrateur, pouvez connaître toutes les conditions et tous les facteurs présents lors de l'installation, de la configuration, de l'utilisation et de l'entretien de la machine ou du procédé. Par conséquent, vous seul pouvez déterminer quels automatismes, équipements associés, protections et verrouillages peuvent être utilisés efficacement et sans danger.

Au moment de sélectionner l'équipement d'automatisme et de commande et les équipements et logiciels connexes pour une application particulière, vous devez également tenir compte des normes, lois et règlements en vigueur au niveau national et européen.

Une attention particulière doit être portée aux informations de sécurité, exigences électriques et normes industrielles applicables à la machine ou au procédé dans le cadre de l'utilisation de cet équipement.

Utilisation prévue

Les produits décrits dans ce document, ainsi que les logiciels, accessoires, options et démarreurs pour charges électriques basse tension, sont destinés à une utilisation industrielle conformément aux instructions, directives, exemples et informations de sécurité contenus dans les présentes et dans d'autres documents auxiliaires.

Le produit doit être utilisé uniquement dans le respect de toutes les réglementations et directives de sécurité en vigueur, ainsi que de toutes exigences et données techniques spécifiées.

Avant d'utiliser le produit, vous devez effectuer une analyse des dangers et une évaluation des risques pour l'application envisagée. En fonction des résultats ainsi obtenus, les mesures de sécurité appropriées devront être prises.

Dans la mesure où le produit est utilisé comme composante d'une machine ou d'un processus, la conception globale du système doit garantir la sécurité des personnes.

Utilisez le produit uniquement avec les câbles et accessoires indiqués. Utilisez uniquement des accessoires et pièces de rechange d'origine.

Tout usage autre que l'utilisation explicitement autorisée est interdit et peut créer des dangers imprévus.

Vue d’ensemble de la sécurité fonctionnelle TeSys™ island

Gamme maître : TeSys

TeSys™ est une solution innovante de contrôle et de gestion des moteurs, proposée par le leader mondial du marché. TeSys propose des produits et des solutions connectés et efficaces pour la commutation et la protection des moteurs et des charges électriques, en conformité avec toutes les principales normes électriques mondiales.

Concept TeSys island

TeSys island est un système multifonctionnel modulaire offrant des fonctions intégrées au sein d’une architecture d’automatisme, qui sont principalement destinées au contrôle direct et à la gestion des charges basse tension. TeSys island permet la commutation, la protection et la gestion des moteurs et autres charges électriques jusqu’à 80 A (AC1) installées dans un tableau de commande électrique.

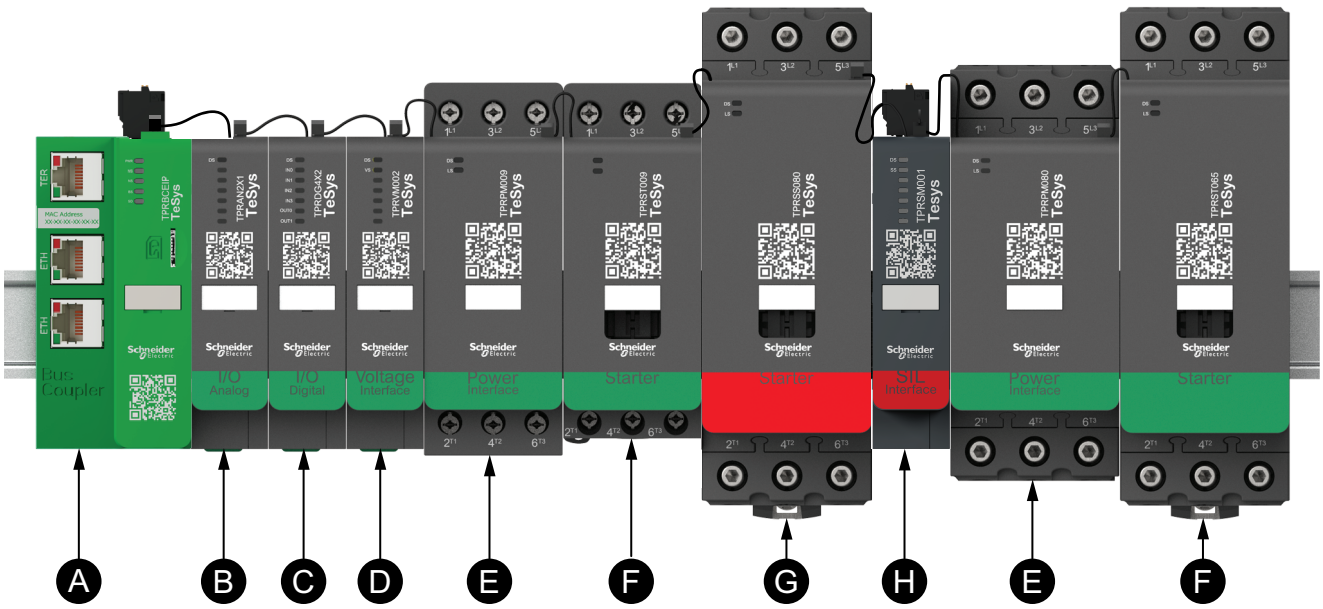
Ce système est conçu autour du concept d’« TeSys avatars ». Ces avatars :

- Représentent les éléments logiques et physiques des fonctions d’automatisme
- Déterminent la configuration de l’îlot TeSys island

Les éléments logiques de l’îlot TeSys island sont gérés à l’aide d’outils logiciels tout au long du cycle de vie du produit et de l’application, de la conception à la maintenance, en passant par l’étude technique, la mise en service et l’exploitation.

L’îlot TeSys island physique se compose d’un ensemble d’équipements installés sur un rail DIN simple et interconnectés par des câbles plats assurant la communication interne entre les modules. Un coupleur de bus permet la communication externe avec l’environnement d’automatisme. L’îlot TeSys island est considéré comme un seul et unique nœud sur le réseau. Les autres modules comprennent les démarreurs, les modules d’interface d’alimentation, les modules d’E/S analogiques et numériques, les modules d’interface de tension et les modules d’interface SIL (Safety Integrity Level, selon la norme CEI 61508), représentant un large éventail de fonctions opérationnelles.

Figure 1 - Présentation de TeSys island



A	Coupleur de bus	E	Module d'interface d'alimentation
B	Module d'E/S analogiques	F	Démarreur standard
C	Module d'E/S numériques	G	Démarreur SIL
D	Module d'interface de tension	H	Module d'interface SIL

Sécurité fonctionnelle dans TeSys island

TeSys™ island fournit des avatars et des dispositifs physiques spécifiques pour construire des configurations pour les fonctions de Catégorie d'arrêt 0 et de Catégorie d'arrêt 1 selon la norme EN/CEI 60204-1. Les avatars TeSys sont des représentations numériques des modules physiques de l'îlot. Toutefois, la fonction de sécurité de TeSys island repose exclusivement sur des composants matériels électromécaniques. Les équipements spécifiques sont le démarreur SIL[6]et le module d'interface SIL. Un autre concept important est le groupe SIL : un ensemble d'avatars associés à un module d'interface SIL et qui suivent la même fonction de sécurité. Plusieurs groupes SIL sont possibles à l'intérieur d'un même îlot.

TeSys island doit être intégré à d'autres éléments relatifs à la sécurité dans un système relatif à la sécurité plus large pour contribuer à la sécurité fonctionnelle d'une machine ou d'un système/procédé.

6. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.

Caractéristiques de sécurité fonctionnelle de TeSys™ island

TeSys™ island offre des caractéristiques de sécurité fonctionnelle conformes aux conditions spécifiques suivantes :

Normes et caractéristiques certifiées

TeSys island suit les directives et normes suivantes :

- Directive Machines 2006/42/CE :
  - EN ISO 13849-1 : 2015
  - EN 62061 : 2016 ou CEI 62061 : 2015 (édition 1.2)
- Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité : CEI 61508 édition 2 : 2010
- Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de procédé : CEI 61511 édition 2 : 2016
- Les fonctions de Catégorie d'arrêt 0 et de Catégorie d'arrêt 1 TeSys island suivent la norme EN/CEI 60204-1.

En monocanal, les performances les plus élevées pour ces fonctions sont :

- Niveau de performance « d », Catégorie 2 selon EN ISO 13849-1
- SIL[7] Capacité 2 selon CEI 61508 éd. 2 et CEI 61511 éd. 2
- Capacité SIL CL 2 selon EN 62061 éd. 1

En bicanal, les performances les plus élevées pour ces fonctions sont :

- Niveau de performance « e », Catégorie 4 selon EN ISO 13849-1
- Capacité SIL 3 selon CEI 61508 éd. 2 et CEI 61511 éd. 2
- Capacité SIL CL 3 selon EN 62061 : 2016 ou CEI 62061 : 2015 (édition 1.2)

TeSys island est conçu pour prendre en charge différents niveaux de performance de sécurité fonctionnelle et d'intégrité de la sécurité en fonction de son architecture de câblage. Les caractéristiques de sécurité fonctionnelle mises en œuvre sont décrites dans le tableau suivant.

Tableau 1 - Caractéristiques fonctionnelles de sécurité

Fonction	Fonction d'arrêt de sécurité	
Position de repli	Contacteur ouvert	
Temps de réponse (pire des cas)	145 ms	
Catégorie d'arrêt EN/CEI 60204-1	Cat. 0 / Cat. 1	
Directive Machines	Yes	
Architecture du système TeSys island	Monocanal	Bicanal

7. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508

Tableau 1 - Caractéristiques fonctionnelles de sécurité (Suite)

Niveau de performance EN ISO 13849-1	PL c, d	PL c, d, e
Catégorie de câblage ISO 13849-1	Cat 1, 2	Cat 3, 4
SIL CL EN 62061	SIL CL 2	SIL CL 3
SIL CEI 61508 / CEI 61511	SIL 2	SIL 3

Le certificat de sécurité fonctionnelle est disponible sur www.se.com/tesys/.

NOTE: Pour la certification relative aux aspects fonctionnels, seul un TeSys island adapté à une utilisation dans des applications relatives à la sécurité sera pris en compte, et non le système complet dans lequel il est intégré pour contribuer à la sécurité fonctionnelle d'une machine ou d'un système/procédé.

Conditions de fonctionnement

TeSys island est conçu et construit pour supporter durablement les conditions suivantes. Certains modules pourront faire l'objet d'autres critères ; reportez-vous à la fiche technique correspondante disponible sur www.se.com/tesys-island.

- Température ambiante de 40 °C (104 °F)
- Moteurs de 400/480 V
- 50 % d'humidité
- 80 % de charge
- Montage à l'horizontale
- Toutes les entrées activées
- Toutes les sorties activées
- Fonctionnement 24 heures/jour, 365 jours/an

Architecture monocanal (ISO 13849)

TeSys island s'applique aux architectures monocanal dans lesquelles un défaut détecté peut entraîner la perte de la fonction de sécurité.

Architecture bicanal (ISO 13849)

TeSys island s'applique aux architectures bicanal dans lesquelles un défaut détecté (y compris les défauts de mode commun) n'entraîne pas la perte de la fonction de sécurité.

Catégories d'arrêt (EN/CEI 60204-1)

La catégorie d'arrêt correspond à la manière dont la charge entraînée est mise hors tension ; elle dépend du sous-système relatif à la sécurité externe qui déclenche la fonction d'arrêt. Un sous-système relatif à la sécurité externe peut être implémenté avec des équipements tels que les modules Preventa™ XPS.

Catégorie d'arrêt 0

La catégorie d'arrêt 0 est définie comme arrêt du mouvement de la machine par coupure immédiate de l'alimentation électrique des actionneurs de la machine. La catégorie d'arrêt 0 est un arrêt non contrôlé.

Catégorie d'arrêt 1

La catégorie d'arrêt 1 est définie comme arrêt du mouvement de la machine avec maintien de l'alimentation électrique des actionneurs de la machine pendant le procédé d'arrêt. L'alimentation est coupée une fois l'arrêt terminé. La catégorie d'arrêt 1 est un arrêt contrôlé.

Catégories de câblage[8]

Les catégories de câblage se rapportent à la façon dont le module XPS externe Preventa™ (ou équivalent) est raccordé, et au niveau de contrôle supplémentaire sur la fonction de sécurité.

Catégorie de câblage 1

Un seul défaut détecté peut entraîner la perte de la fonction de sécurité et aucune couverture de diagnostic n'est nécessaire.

L'élément capteur relatif à la sécurité peut être raccordé directement aux entrées SIL-IN / SIL Common.[9] Les entrées Mirror In / Mirror Out ne sont pas utilisées. Pour plus d'informations sur le câblage des entrées SIL-IN / SIL Common, voir Élément capteur relatif à la sécurité, page 24.

Catégorie de câblage 2

L'élément capteur relatif à la sécurité est relié à un module Preventa XPS (ou équivalent). Les sorties du module Preventa XPS (ou équivalent) sont connectées aux entrées SIL-IN / SIL Common du module d'interface SIL[9].

Pour satisfaire aux exigences de la catégorie 2, le retour de contact miroir (Mirror In / Mirror Out) doit être surveillé par un module Preventa XPS (ou équivalent) qui effectue un diagnostic externe du contact miroir. Si le contact miroir ne se ferme pas à l'arrêt, le prochain redémarrage est empêché pour tous les démarreurs SIL du groupe SIL.

Implémentation de la surveillance indirecte pour la catégorie 2

Pour satisfaire aux exigences de la catégorie 2 en matière de couverture de diagnostic (DC > 60 %), une surveillance externe de l'état du groupe doit être implémentée pour déclencher un mécanisme secondaire d'arrêt de la machine (déclenchement shunt de disjoncteur, etc.) ou pour empêcher l'accès aux zones dangereuses (verrouillage de sécurité).

8. Catégories de câblage selon la norme ISO 13849.
9. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.

Chaque groupe SIL[10] dispose de cinq états pour indiquer l'état de fonctionnement. L'état 0 indique qu'il n'y a pas de groupe SIL présent dans cet emplacement. TeSys island permet d'avoir jusqu'à 10 groupes SIL de l'îlot.

État du groupe SIL pour la fonction Arrêt SIL :

- 0 = Groupe SIL absent de la configuration du système.
- 1 = Groupe SIL affecté par l'événement d'avatar matériel.
- 2 = Commande d'arrêt reçue, les démarreurs SIL ne sont pas encore ouverts.
- 3 = Commande d'arrêt émise avec succès, tous les démarreurs SIL sont ouverts.
- 4 = Commande d'arrêt émise sur un seul canal d'entrée de module d'interface SIL (SIM) (cavalier ou câblage d'entrée de module SIM à l'origine d'un problème), mais les démarreurs SIL se sont correctement ouverts.
- 5 = Fonctionnement normal, les démarreurs SIL peuvent être ouverts ou fermés.

L'état 5 est l'état de fonctionnement normal et l'état 3 est l'état d'arrêt SIL normal. L'état 1 indique un problème de micrologiciel ou de communication avec un démarreur SIL. Les états 2 et 4 indiquent des problèmes liés à l'arrêt SIL avec le module SIM, les démarreurs SIL ou le câblage d'arrêt SIL. La surveillance indirecte doit s'intéresser à des états 2 ou 4 persistant plus longtemps que le temps d'activation d'un arrêt SIL, et utiliser les informations d'état pour déclencher un mécanisme secondaire d'arrêt de la machine (déclenchement shunt d'un disjoncteur, etc.).

Pour lire l'état du groupe SIL, la surveillance externe doit utiliser le bloc de fonction SystemDiagnostics. Chaque groupe SIL du système dispose d'une sortie sur ce bloc de fonction pour l'état de son groupe SIL, étiquetée sur le bloc de fonction comme « SILStarterStopMsgGrp *n* », où *n* est le numéro du groupe SIL dans l'îlot. L'état du groupe SIL suit l'énumération ci-dessus.

Surveillance diagnostique

La surveillance diagnostique a lieu immédiatement à la sollicitation de la fonction de sécurité. Le temps nécessaire pour détecter le défaut et amener la machine à un état non dangereux doit par conséquent être plus court que le temps nécessaire pour atteindre la zone dangereuse.

Selon ISO 13849-2, 9.2.3, pour la catégorie 2 : Le $MTTF_d$[11] de l'équipement de surveillance doit être supérieur à la moitié du $MTTF_d$ de la logique. La contribution de TeSys island au $MTTF_d$ de la surveillance diagnostique est $MTTF_d$ > 100 ans.

Catégorie de câblage 3

Un seul défaut n'entraînera pas la perte de la fonction de sécurité et, chaque fois que cela est possible, le défaut unique sera détecté au plus tard lors de la sollicitation suivante de la fonction de sécurité.

Pour satisfaire aux exigences de la catégorie 3, le retour de contact miroir (Mirror In / Mirror Out) doit être surveillé par un module Preventa XPS (ou équivalent) qui effectue un diagnostic externe du contact miroir du démarreur SIL[10]. Si le contact miroir ne s'ouvre pas à l'arrêt, le prochain redémarrage est empêché pour tous les démarreurs SIL du groupe SIL. L'élément capteur relatif à la sécurité est relié à un module Preventa XPS (ou équivalent). Les sorties du module Preventa XPS (ou équivalent) sont connectées aux entrées SIL-IN / SIL Common du module d'interface SIL.

En cas de surveillance indirecte, la surveillance externe de l'état du groupe doit rechercher si les états 2 ou 4 persistent plus longtemps que le temps d'activation

10. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
11. Temps moyen avant défaillance dangereuse au sens de la norme ISO 13849-1.

d’un arrêt SIL. Utilisez les informations d’état pour empêcher le prochain redémarrage des démarreurs SIL du groupe.

Catégorie de câblage 4

Un seul défaut n’entraînera pas la perte de la fonction de sécurité. Le défaut unique est détecté au plus tard à la prochaine demande de la fonction de sécurité. Si cette détection n’est pas possible, une accumulation de défauts non détectés n’entraînera pas la perte de la fonction de sécurité.

Pour satisfaire aux exigences de la catégorie 4, le retour de contact miroir (Mirror In / Mirror Out) doit être surveillé par un module Preventa XPS (ou équivalent) qui effectue un diagnostic externe du contact miroir du démarreur SIL[12]. Si le contact miroir ne s’ouvre pas à l’arrêt, le prochain redémarrage est empêché pour tous les démarreurs SIL du groupe SIL. L’élément capteur relatif à la sécurité est relié à un module Preventa XPS (ou équivalent). Les sorties du module Preventa XPS (ou équivalent) sont connectées aux entrées SIL-IN / SIL Common du module d’interface SIL.

Essai d’acceptation

L’intégrateur de système ou fabricant de machines doit effectuer un essai de réception de la fonction de sécurité pour vérifier et documenter la fonctionnalité correcte de la fonction de sécurité. L’intégrateur de système ou fabricant de machines certifie ainsi avoir testé l’efficacité des fonctions de sécurité utilisées. L’essai d’acceptation doit être effectué sur la base de l’analyse des dangers et de l’évaluation des risques. Dans le cas d'un mode de faible sollicitation de catégorie 4, la fonction de sécurité doit être testée au moins une fois par mois. Toutes les normes et tous les règlements applicables doivent être respectés.

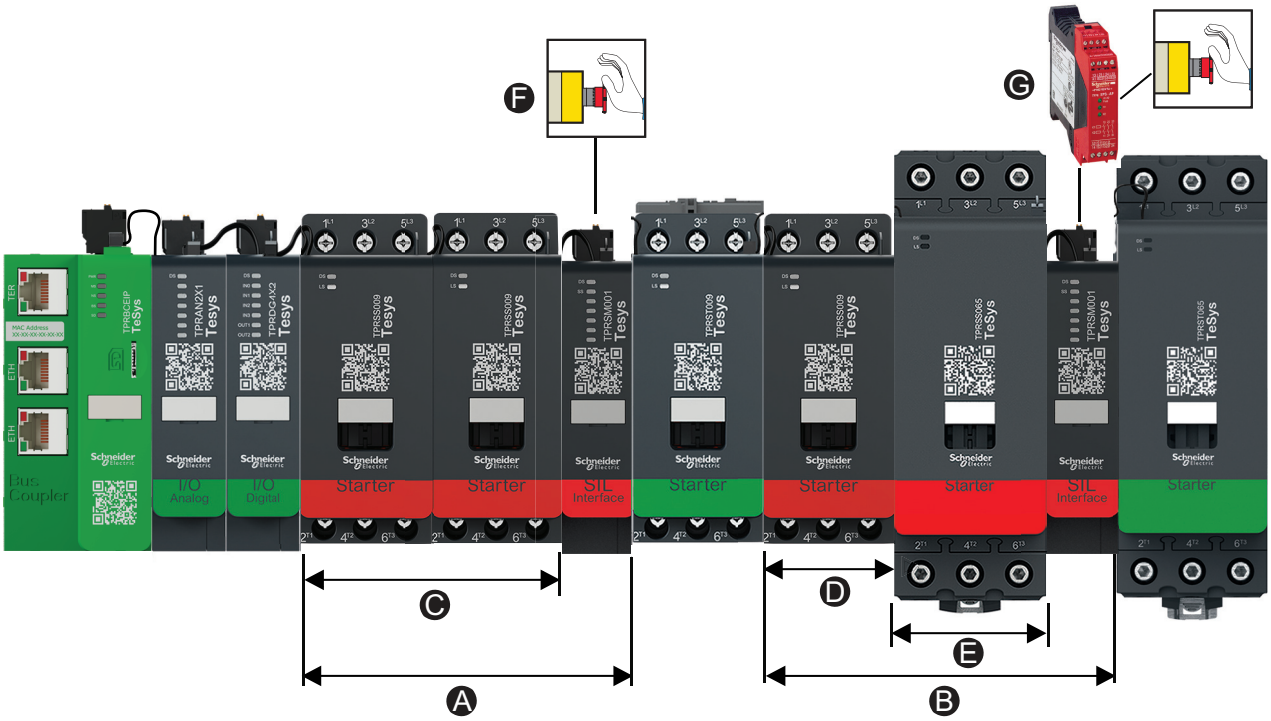
12. Safety Integrity Level (niveau d’intégrité) selon la norme CEI 61508.

Concepts et composants

Structure TeSys™ island type

L'illustration ci-dessous montre un exemple de TeSys™ island composé de deux groupes SIL[13]. La composition de l'îlot est définie par les outils numériques de TeSys island en fonction des besoins fonctionnels exprimés par l'utilisateur.

Figure 2 - TeSys island avec deux groupes SIL



A	Groupe SIL 1	E	Avatar A4
B	Groupe SIL 2	F	Catégorie de câblage 1, Catégorie d'arrêt 0[14]
C	Avatar A1	G	Catégorie de câblage 2, Catégorie d'arrêt 1[15]
D	Avatar A3		

Groupe SIL 1 : comprend un avatar incluant deux démarreurs SIL, par exemple, un avatar « Moteur deux directions – Arrêt SIL, W. Cat 1/2 » (Avatar A1). Le moteur proprement dit est raccordé à ces démarreurs SIL et suit la logique de l'avatar ainsi que les commandes opérationnelles provenant de l'automate via le bus de terrain. La Commande d'arrêt de sécurité, provenant du bouton d'arrêt d'urgence relié au module d'interface SIL (catégorie de câblage 1), commande aux démarreurs SIL de mettre la charge hors tension et de passer en état sécurisé (le contacteur est ouvert et le moteur est hors tension).

Groupe SIL 2 : comprend deux avatars, par exemple un avatar « Commutateur – Arrêt SIL, W. Cat 1/2 » (Avatar A3) et un avatar « Moteur une direction – Arrêt SIL, W. Cat 1/2 » (Avatar A4), chacun composé d'un seul démarreur SIL. Les deux

13. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
14. Catégorie de câblage 1 selon la norme ISO 13849. Catégorie d'arrêt 0 selon EN/CEI 60204-1.
15. Catégorie de câblage 2 selon la norme ISO 13849. Catégorie d'arrêt 1 selon EN/CEI 60204-1.

avatars suivent la logique de l'avatar ainsi que les commandes opérationnelles provenant de l'automate via le bus de terrain. La commande d'arrêt SIL provient du module externe Preventa™ XPS (ou équivalent) raccordé au module d'interface SIL. Elle commande aux démarreurs SIL de mettre la charge hors tension et de passer en état sécurisé (catégorie de câblage 2).

Groupe SIL

Un groupe SIL[16] est composé d'un ou plusieurs avatars SIL, tous affectés à un seul module d'interface SIL. Tous les avatars SIL du groupe SIL réagissent à une même commande d'arrêt SIL. Le module d'interface SIL est toujours installé à droite du dernier démarreur SIL compris dans le groupe SIL (côté opposé au coupleur de bus).

Un îlot peut comprendre plusieurs groupes SIL.

Avatars SIL

Les avatars SIL[16] disponibles pour les fonctions d'arrêt SIL sont les suivants :

- Commutateur – Arrêt SIL, W. Cat 1/2
- Commutateur – Arrêt SIL, W. Cat 3/4
- Moteur une direction – Arrêt SIL, W. Cat 1/2
- Moteur une direction – Arrêt SIL, W. Cat 3/4
- Moteur deux directions – Arrêt SIL, W. Cat 1/2
- Moteur deux directions – Arrêt SIL, W. Cat 3/4
- Moteur deux vitesses – Arrêt SIL, W. Cat 1/2
- Moteur deux vitesses – Arrêt SIL, W. Cat 3/4
- Moteur deux vitesses, deux directions – Arrêt SIL, W. Cat 1/2
- Moteur deux vitesses, deux directions – Arrêt SIL, W. Cat 3/4
- Convoyeur une direction – Arrêt SIL, W. Cat 1/2
- Convoyeur deux directions – Arrêt SIL, W. Cat 3/4

Les avatars SIL se composent d'équipements matériels spécifiques, dont des démarreurs SIL, des démarreurs standard et le module d'interface SIL requis, qui gère le groupe SIL auquel les avatars SIL sont affectés.

NOTE: Les avatars SIL sont conçus pour des applications avec une fréquence de commandes opérationnelles faible, c'est-à-dire en dessous d'une moyenne annuelle de 15 cycles marche/arrêt par heure.

Démarreur SIL

Démarreur standard

Module d'interface SIL

16. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.

Module d'interface SIL

Le module d'interface SIL[17] (SIM) TeSys™ island est un module accessoire nécessaire pour activer la fonction de sécurité fonctionnelle de l'îlot.

La fonction d'arrêt SIL est obtenue par des moyens purement électromécaniques, sans aucune communication numérique ni intervention du coupleur de bus.

Le module SIM :

- s'interface avec un module XPS Preventa™ (ou équivalent) externe ;
- commande la fonction d'arrêt de son groupe SIL ;
- échange des données de fonctionnement avec le coupleur de bus ;
- fournit une indication opérationnelle par l'intermédiaire de voyants en face avant.

État des contacts des démarreurs SIL

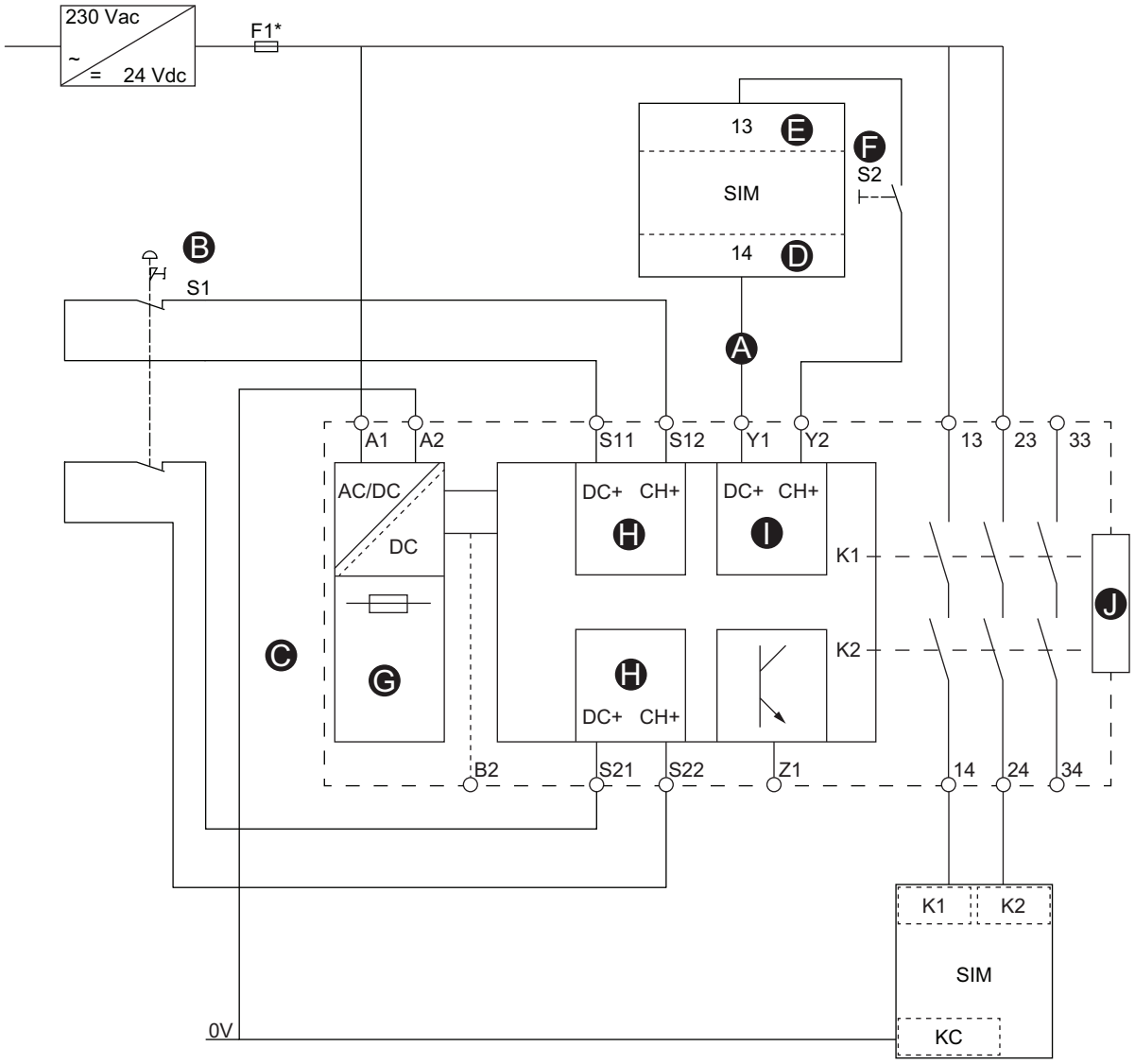
L'état des démarreurs SIL[18] appartenant à un groupe SIL est signalé via les connexions Mirror In/Out du module Modules SIM. Ceci permet l'implémentation d'architectures avec catégorie de câblage 2[19] dans lesquelles les contacts miroir sont connectés au module Preventa XPS (ou équivalent). Ces configurations permettent une surveillance directe des dispositifs électromécaniques par un élément de contact relié mécaniquement, ce qui donne une couverture de diagnostic allant jusqu'à 99 %. Voir EN ISO 13849-1, Tableau E.1 – Estimations pour la couverture de diagnostic (DC).

Tableau 2 - État des contacts des démarreurs SIL

État du groupe SIL	État du contact Mirror In/Out
Tous les démarreurs SIL ouverts	Contact Mirror In/Out fermé
Au moins un démarreur SIL fermé	Contact Mirror In/Out ouvert
TeSys island hors tension ou défaut détecté par la fonction de sécurité	Contact Mirror In/Out ouvert

17. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
18. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508
19. Catégorie de câblage 2 selon la norme ISO 13849

Figure 3 - Raccordement du module SIM au Preventa XPS-AF



A	Conditions de démarrage externe (ESC)	F	Bouton de démarrage (S2)
B	Bouton d'arrêt d'urgence (S1)	G	Alimentation
C	Module Preventa XPS-UAF	H	Entrée
D	Module SIM – Mirror Out	I	Début
E	Module SIM – Mirror In	J	Extension

Élément de capteur relatif à la sécurité

Le module SIM est connecté en amont comme suit :

- À la source 24 VCC
- À l'élément capteur relatif à la sécurité ou à un module Preventa XPS (ou équivalent)

Le module SIM est conçu avec deux canaux d'entrée pour recevoir des éléments capteur relatifs à la sécurité bicanaux. Pour un niveau plus élevé de tolérance aux pannes, l'architecture à deux canaux d'entrée est recommandée.

Pour les schémas de câblage ci-dessous, reportez-vous à la Légende des schémas de câblage des canaux SIM, page 24.

Figure 4 - Modules SIM – Raccordement monocanal

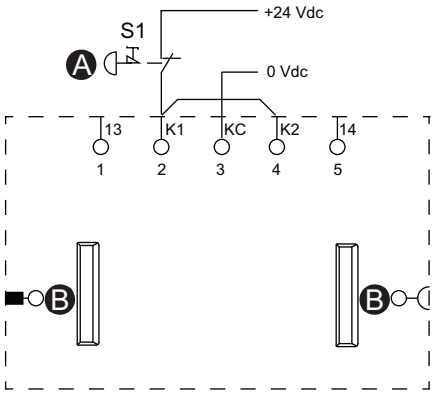


Figure 5 - Modules SIM – Raccordement bicanal

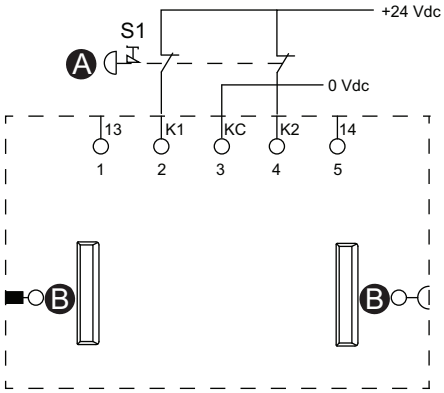


Tableau 3 - Légende des schémas de câblage des canaux SIM

A	Bouton d'arrêt d'urgence (S1)
B	Connecteur pour câble plat

Démarreurs SIL

⚠AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

Pour des instructions complètes sur la sécurité fonctionnelle, reportez-vous au Guide de sécurité fonctionnelle de TeSys™ island, 8536IB1904.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les démarreurs SIL[20] offrent des fonctions similaires aux démarreurs standard mais sont associés à un module d'interface SIL.

Voici les fonctions principales des démarreurs SIL :

- Fournir les fonctionnalités de Catégorie d'arrêt 0 et de Catégorie d'arrêt 1[21]
- Assurer le contrôle opérationnel pour les charges
- Mesurer les données électriques relatives à la charge
- Fournir des données de contrôle énergétique lorsqu'un module d'interface de tension est installé sur l'îlot TeSys island

Plusieurs démarreurs SIL peuvent être nécessaires pour une seule fonction d'TeSys avatar. Par exemple, l'avatar Moteur deux directions – Arrêt SIL, W. Cat 1/2[22] comprend deux démarreurs SIL. De plus, les avatars utilisant des démarreurs SIL comprennent toujours un module d'interface SIL.

Les démarreurs SIL sont raccordés comme suit :

- En amont d'un disjoncteur
- En aval de la charge

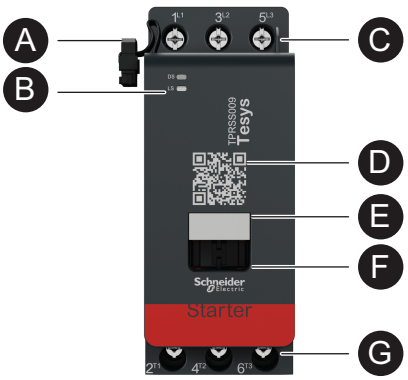
Les démarreurs SIL communiquent avec le coupleur de bus en envoyant des données de fonctionnement et en recevant des commandes.

Tableau 4 - Valeurs nominales des démarreurs SIL

Puissance nominale		Ampérage	Référence
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. Safety Integrity Level (niveau d'intégrité selon la norme CEI 61508)
21. Catégorie d'arrêt 0 et Catégorie d'arrêt 1 selon la norme EN/CEI 60204-1.
22. Catégorie de câblage 1 et Catégorie de câblage 2 selon la norme ISO 13849.

Figure 6 - Caractéristiques des démarreurs SIL



A	Câble plat (pour le raccordement avec le module à gauche)	E	Plaque d'identité
B	Voyants indicateurs d'état	F	Pont mobile
C	Raccordements d'alimentation en amont	G	Raccordements d'alimentation en aval
D	Code QR		

Élément relatif à la sécurité externe

TeSys™ island doit être intégré à d'autres éléments relatifs à la sécurité dans un système relatif à la sécurité plus large pour contribuer à la sécurité fonctionnelle d'une machine ou d'un système/procédé.

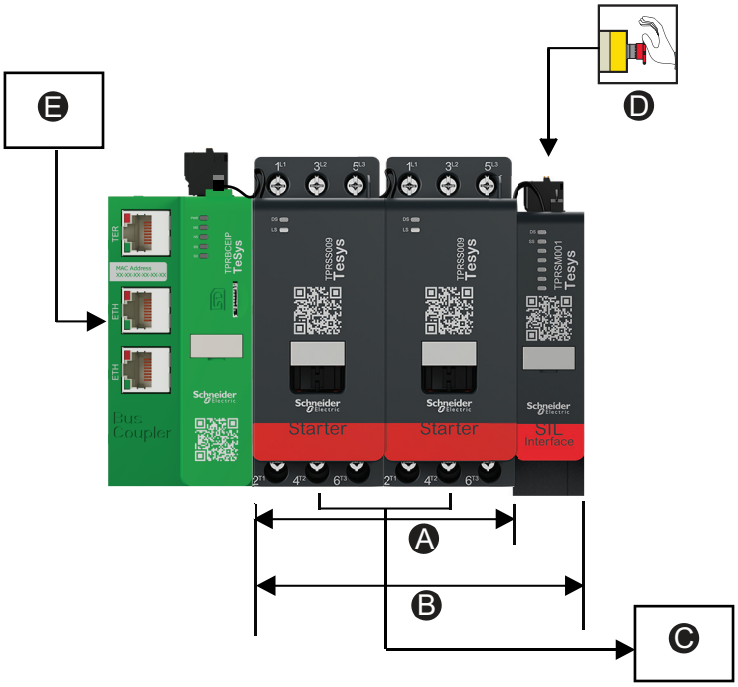
Les configurations suivantes illustrent des équipements types.

Configuration Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 1

NOTE: Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 1 selon la norme ISO 13849. Catégorie d'arrêt 0 selon EN/CEI 60204-1.

L'arrêt SIL du moteur est directement contrôlé par l'ouverture du contact du bouton d'arrêt d'urgence.

Figure 7 - Arrêt SIL



A	Avatar A1	D	Catégorie de câblage 1, Catégorie d'arrêt 0
B	Groupe SIL 1	E	Automate programmable
C	Moteur		

Configuration Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 2

NOTE: Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 2 selon la norme ISO 13849. Catégorie d'arrêt 0 selon EN/CEI 60204-1.

Figure 8 - Exemple : Configuration Moteur deux directions – Arrêt SIL, W. Cat 1/2, Catégorie d'arrêt 0, Catégorie de câblage 2 (surveillance indirecte)

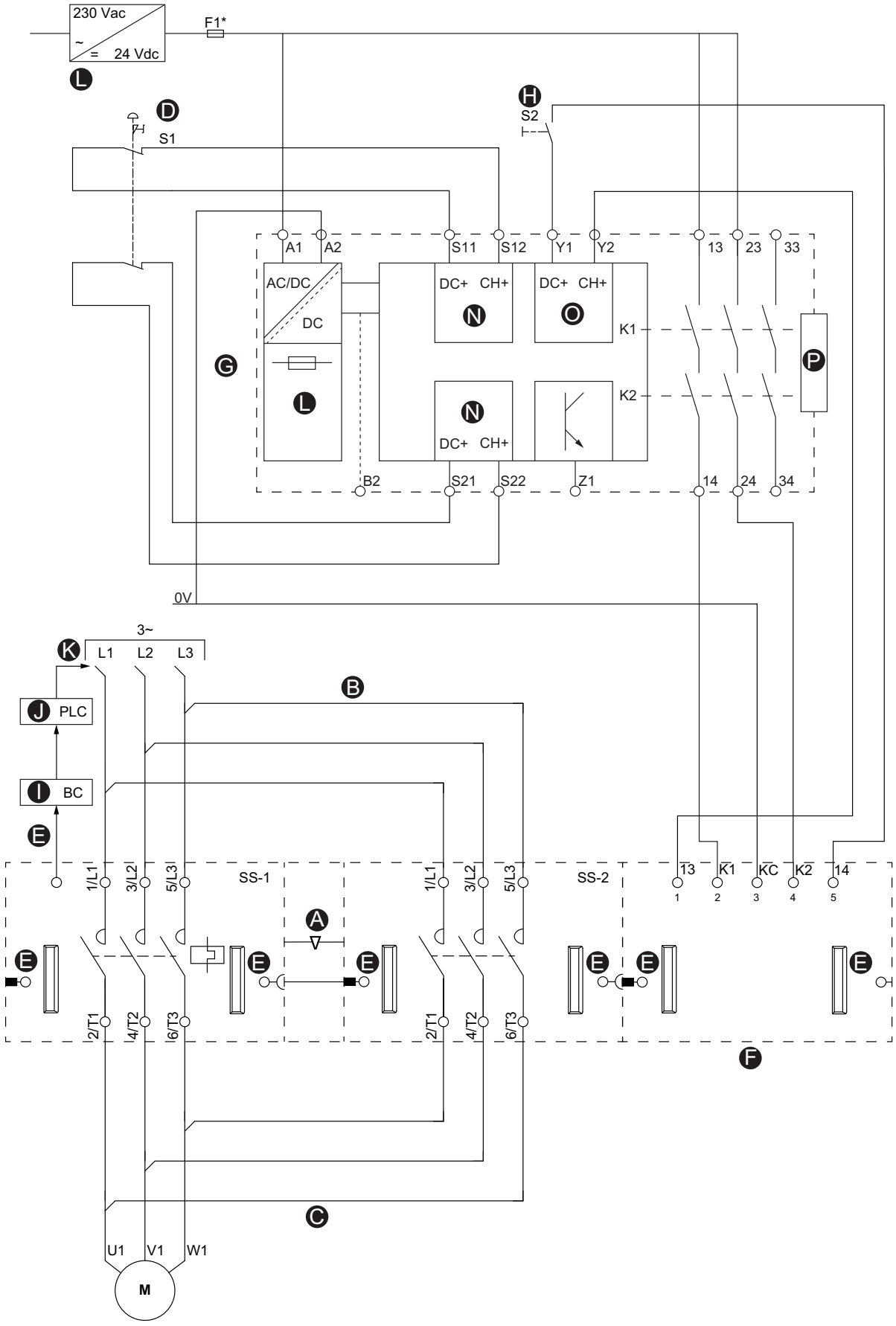
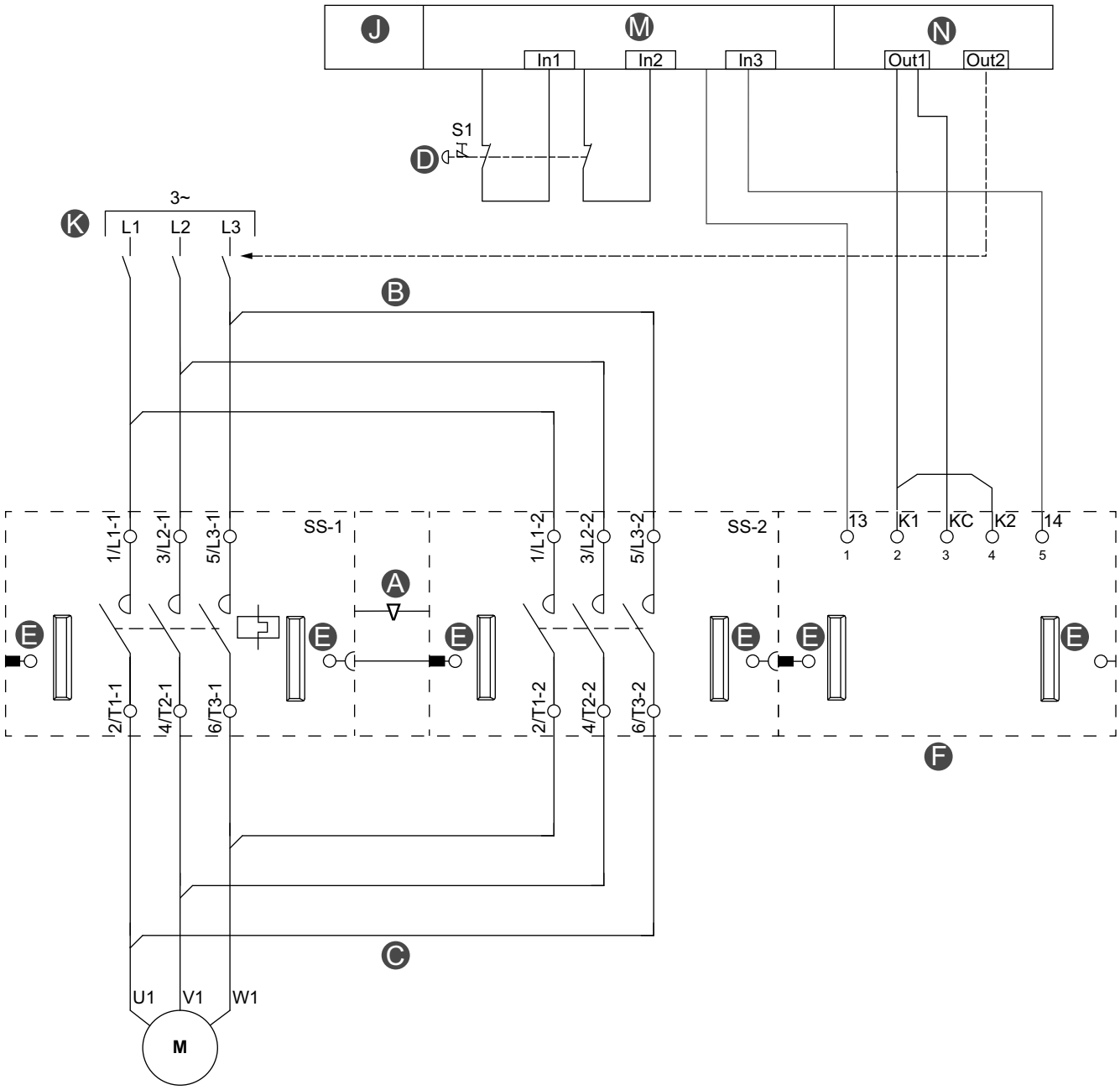


Tableau 5 - Légende pour Exemple : Configuration Moteur deux directions – Arrêt SIL, W. Cat 1/2, Catégorie d'arrêt 0, Catégorie de câblage 2 (surveillance indirecte), page 28

A	Verrouillage mécanique	I	Coupleur de bus
B	Liaison parallèle	J	Automate programmable
C	Liaison inverse	K	Disjoncteur en amont
D	Bouton d'arrêt d'urgence (S1)	L	Alimentation
E	Connecteur pour câble plat	N	Entrée
F	Modules d'interface SIL (SIM)	O	Début
G	Module Preventa XPS-UAF	P	Extension
H	Bouton de démarrage (S2)		

Figure 9 - Exemple : Configuration Moteur deux directions – Arrêt SIL, W. Cat 1/2, Catégorie d'arrêt 0, Catégorie de câblage 2 (surveillance directe)



A	Verrouillage mécanique	F	Modules d'interface SIL (SIM)
B	Liaison parallèle	J	Automate à fonction de sécurité
C	Liaison inverse	K	Disjoncteur en amont
D	Bouton d'arrêt d'urgence (S1)	M	Entrée numérique
E	Connecteur pour câble plat	N	Sortie numérique

Configuration Arrêt SIL, Catégorie d'arrêt 1, Catégorie de câblage 2

NOTE: Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 2 selon la norme ISO 13849. Catégorie d'arrêt 1 selon EN/CEI 60204-1.

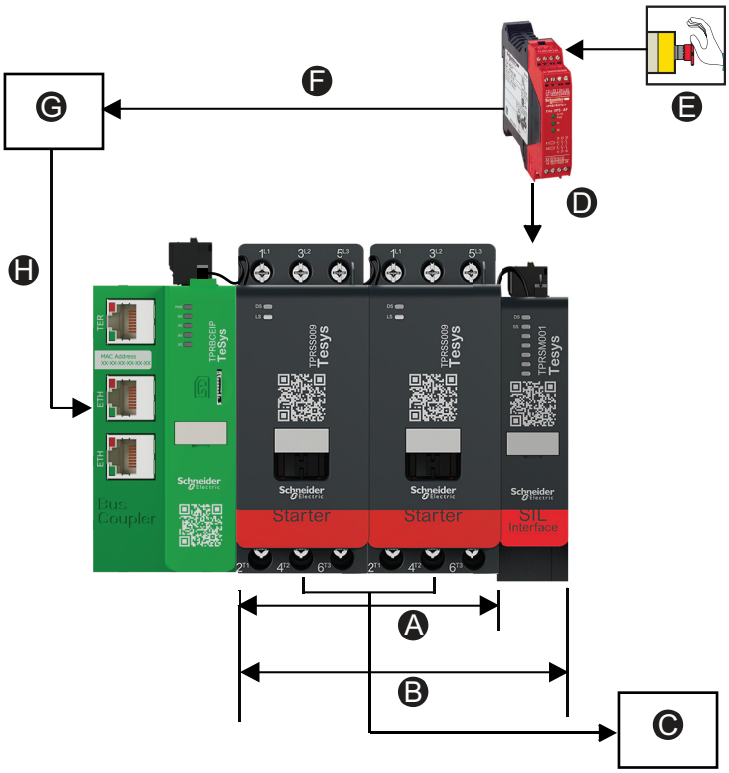
La catégorie d'arrêt 1 est définie comme « arrêt contrôlé avec maintien de l'alimentation des actionneurs de la machine pour atteindre l'arrêt, puis coupure de l'alimentation une fois l'arrêt atteint ».

Lorsque l'arrêt d'urgence est déclenché, la commande d'arrêt est d'abord envoyée à un dispositif externe (par exemple, un automate ou un variateur). Le procédé peut ainsi être arrêté de manière contrôlée plutôt que par une coupure d'alimentation immédiate. Après un temps prédéfini, la commande d'arrêt SIL est ensuite envoyée au module SIM pour mettre hors tension les charges sur les avatars SIL dans le groupe SIL associé.

L'installation recommandée consiste à utiliser un automate programmable pour veiller à ce que le procédé soit correctement arrêté avant l'arrêt SIL.

La commande d'arrêt peut être acheminée directement vers une entrée numérique de l'automate ou vers un avatar de module d'E/S numériques TeSys™ island, l'une de ses entrées numériques étant lues par l'automate. Sur réception d'une commande d'arrêt en entrée, l'automate déclenche un arrêt contrôlé en adressant une commande d'arrêt opérationnel à l'avatar TeSys island cible.

Figure 10 - Commande d'arrêt



A	Avatar A1	E	Catégorie de câblage 2, Catégorie d'arrêt 1
B	Groupe SIL 1	F	Commande d'arrêt contrôlé de catégorie 1

C	Moteur	G	Automate programmable
D	Arrêt non contrôlé	H	Commande d'arrêt opérationnel

Figure 11 - Exemple : Configuration Moteur deux directions – Arrêt SIL W. Cat 1/2 – Catégorie d'arrêt 1, Catégorie de câblage 2

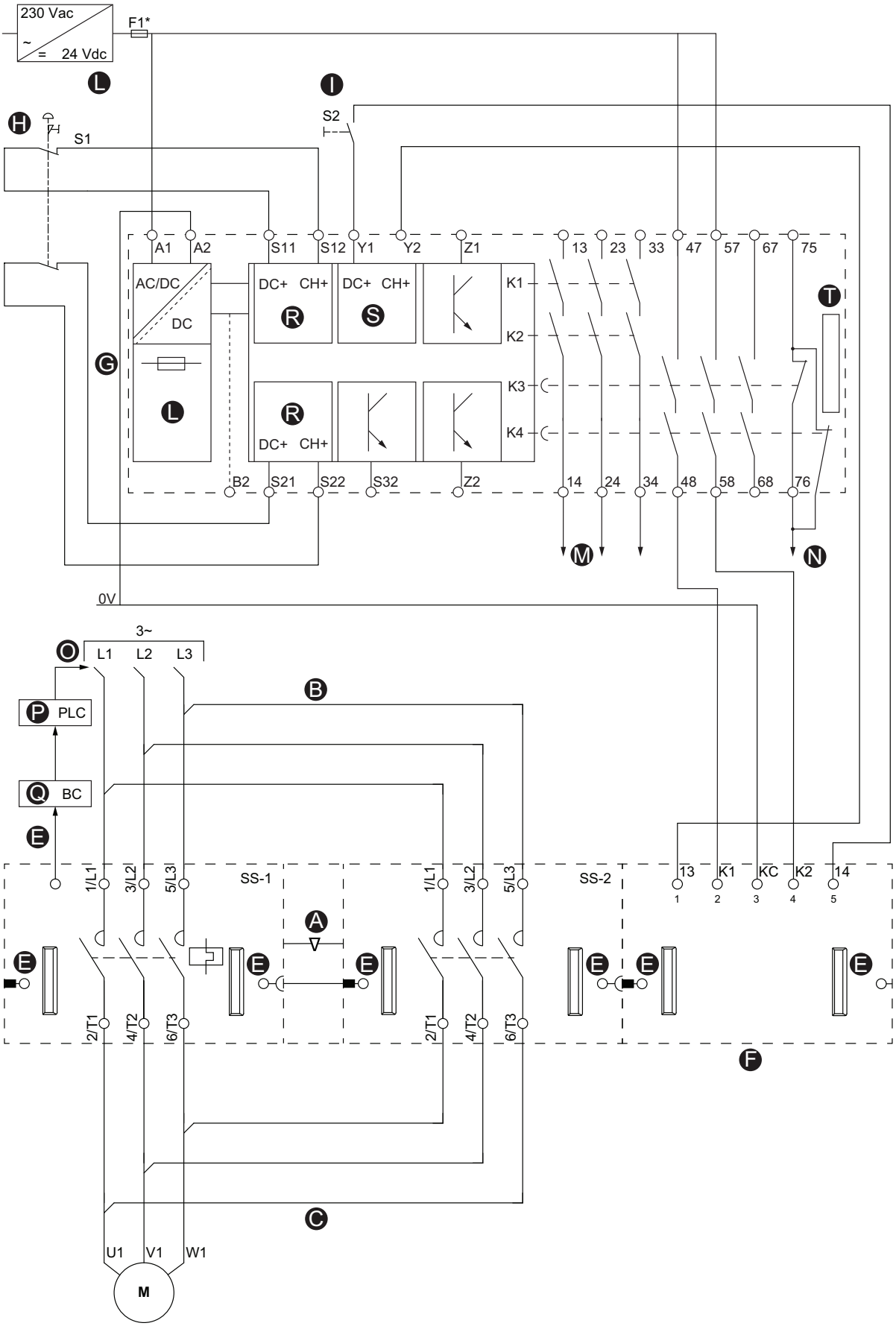


Tableau 6 - Légende pour Exemple : Configuration Moteur deux directions – Arrêt SIL W. Cat 1/2 – Catégorie d'arrêt 1, Catégorie de câblage 2, page 33

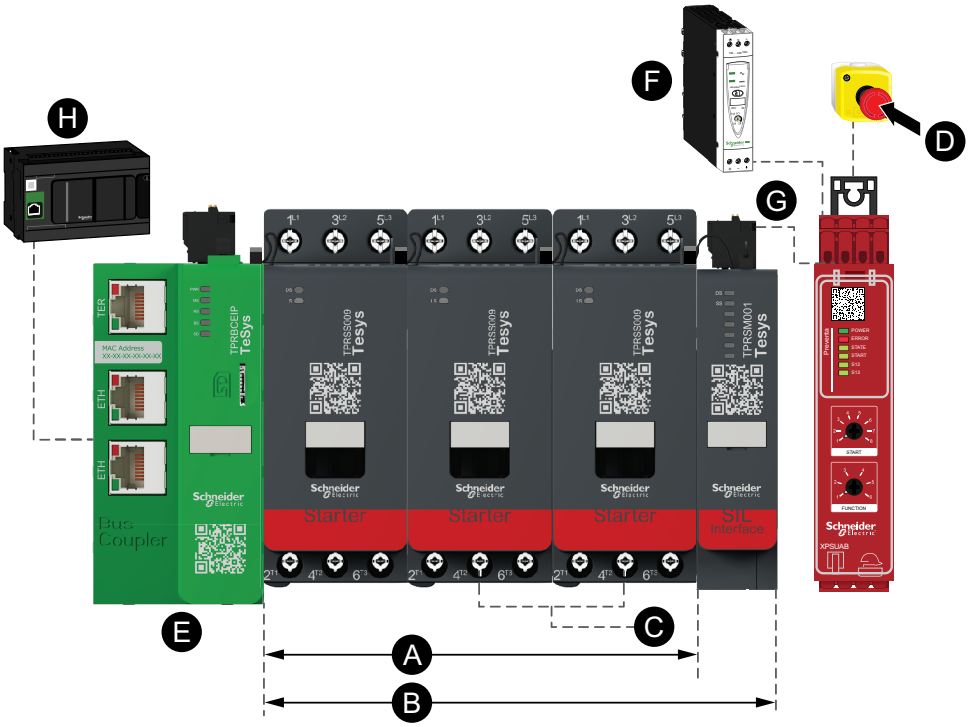
A	Verrouillage mécanique	M	Arrêt contrôlé
B	Liaison parallèle	N	Catégorie d'arrêt 1
C	Liaison inverse	O	Disjoncteur en amont
E	Connecteur pour câble plat	P	Automate programmable
F	Modules d'interface SIL (SIM)	Q	Coupleur de bus
G	Module Preventa XPS-UAF	R	Entrée
H	Bouton d'arrêt d'urgence	S	Début
I	Bouton de démarrage S2	T	Extension
L	Alimentation		

Configuration Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 3/4

NOTE: Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 3/4 selon la norme ISO 13849. Catégorie d'arrêt 0 selon EN/CEI 60204-1.

L'arrêt SIL du moteur est directement contrôlé par l'ouverture du contact du bouton d'arrêt d'urgence.

Figure 12 - Arrêt SIL, Catégorie de câblage 3/4



A	Avatar A1	E	Coupleur de bus
B	Groupe SIL 1	F	24 Vcc
C	Moteur	G	Module Preventa XPS-UAF
D	Catégorie de câblage 3/4, Catégorie d'arrêt 0	H	Automate programmable

Figure 13 - Exemple : Configuration Moteur une direction – Arrêt SIL, W. Cat 3/4, Catégorie d'arrêt 0, Catégorie de câblage 3/4

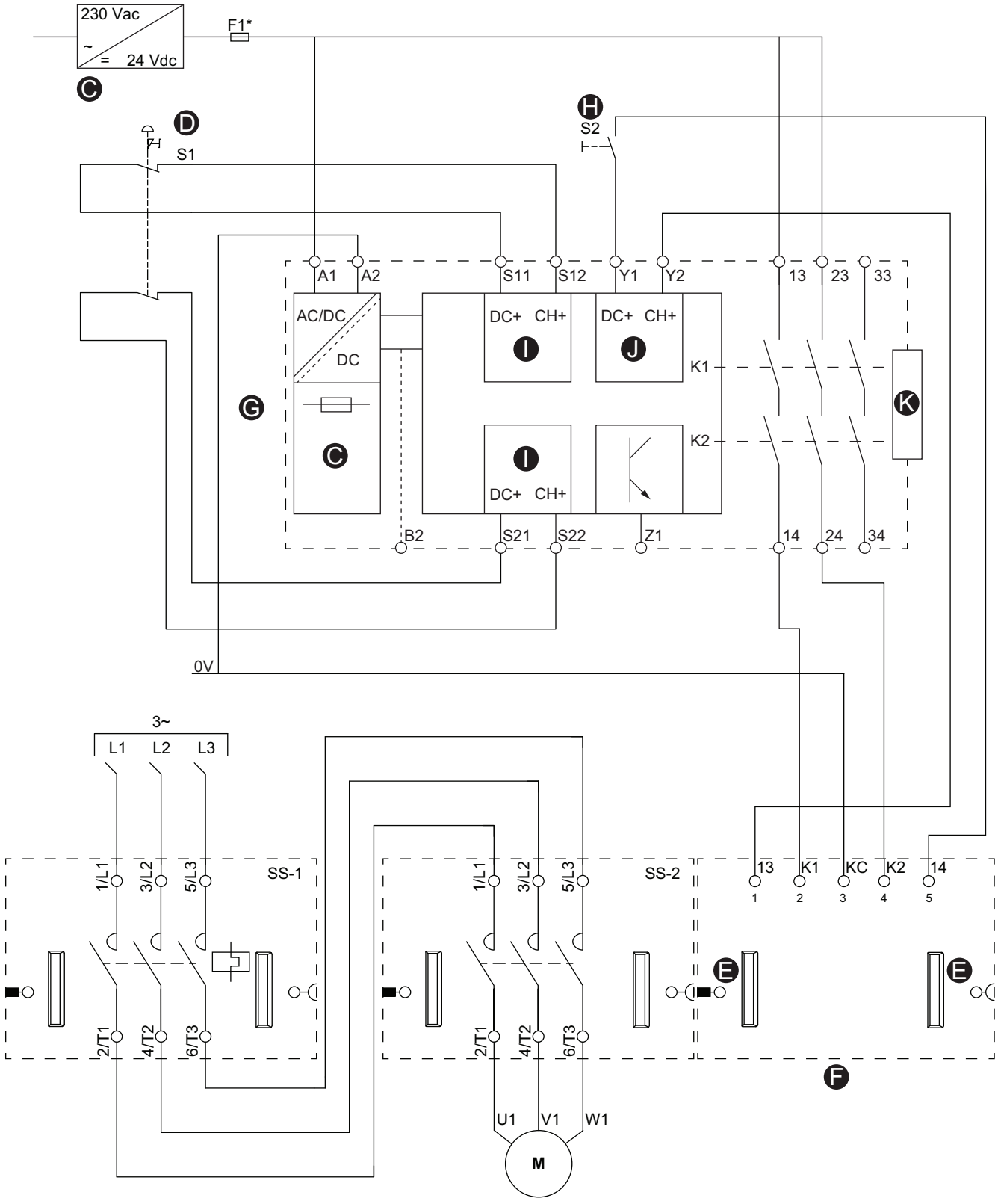


Tableau 7 - Légende pour Exemple : Configuration Moteur une direction – Arrêt SIL, W. Cat 3/4, Catégorie d'arrêt 0, Catégorie de câblage 3/4, page 36

C	Alimentation	H	Bouton de démarrage (S2)
D	Bouton d'arrêt d'urgence (S1)	I	Entrée
E	Connecteur pour câble plat	J	Début
F	Modules d'interface SIL (SIM)	K	Extension
G	Module Preventa XPS-UAF		

Configuration Arrêt SIL, Catégorie d'arrêt 1, Catégorie de câblage 3/4

NOTE: Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 3/4 selon la norme ISO 13849. Catégorie d'arrêt 1 selon EN/CEI 60204.

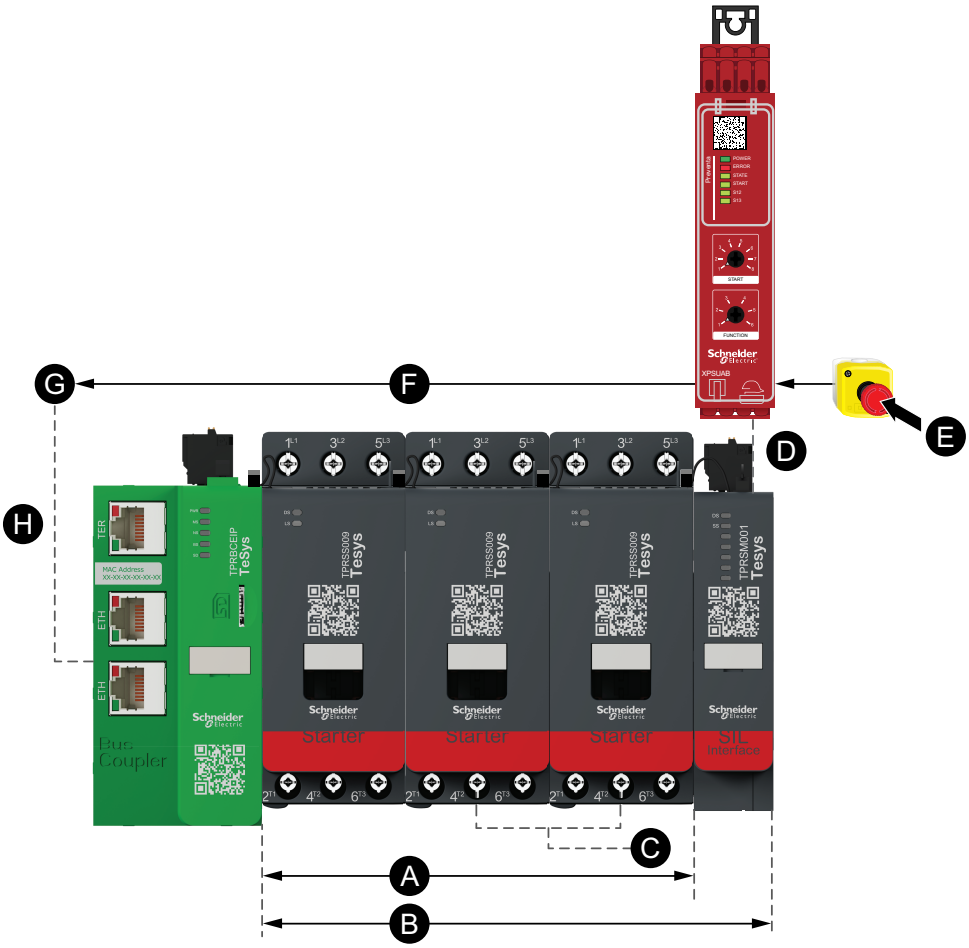
La catégorie d'arrêt 1 est définie comme « arrêt contrôlé avec maintien de l'alimentation des actionneurs de la machine pour atteindre l'arrêt, puis coupure de l'alimentation une fois l'arrêt atteint ».

Lorsque l'arrêt d'urgence est déclenché, la commande d'arrêt est d'abord envoyée à un dispositif externe (par exemple, un automate ou un variateur). Le procédé peut ainsi être arrêté de manière contrôlée plutôt que par une coupure d'alimentation immédiate. Après un temps prédéfini, la commande d'arrêt SIL est ensuite envoyée au module SIM pour mettre hors tension les charges sur les avatars SIL dans le groupe SIL associé.

Pour l'installation, il est recommandé d'utiliser un automate programmable pour veiller à ce que le procédé soit correctement arrêté avant l'arrêt SIL.

La commande d'arrêt peut être acheminée directement vers une entrée numérique de l'automate ou vers un avatar de module d'E/S numériques TeSys™ island, l'une de ses entrées numériques étant lues par l'automate. Sur réception d'une commande d'arrêt en entrée, l'automate déclenche un arrêt contrôlé en adressant une commande d'arrêt opérationnel à l'avatar TeSys island cible.

Figure 14 - Commande d'arrêt, Catégorie de câblage 3/4



A	Avatar A1	E	Catégorie de câblage 3/4, Catégorie d'arrêt 1
B	Groupe SIL 1	F	Commande d'arrêt contrôlé de catégorie 1
C	Moteur	G	Automate programmable
D	Arrêt non contrôlé	H	Commande d'arrêt opérationnel

Figure 15 - Exemple : Configuration Moteur deux directions – Arrêt SIL, W. Cat 3/4, Catégorie d'arrêt 1, Catégorie de câblage 3/4

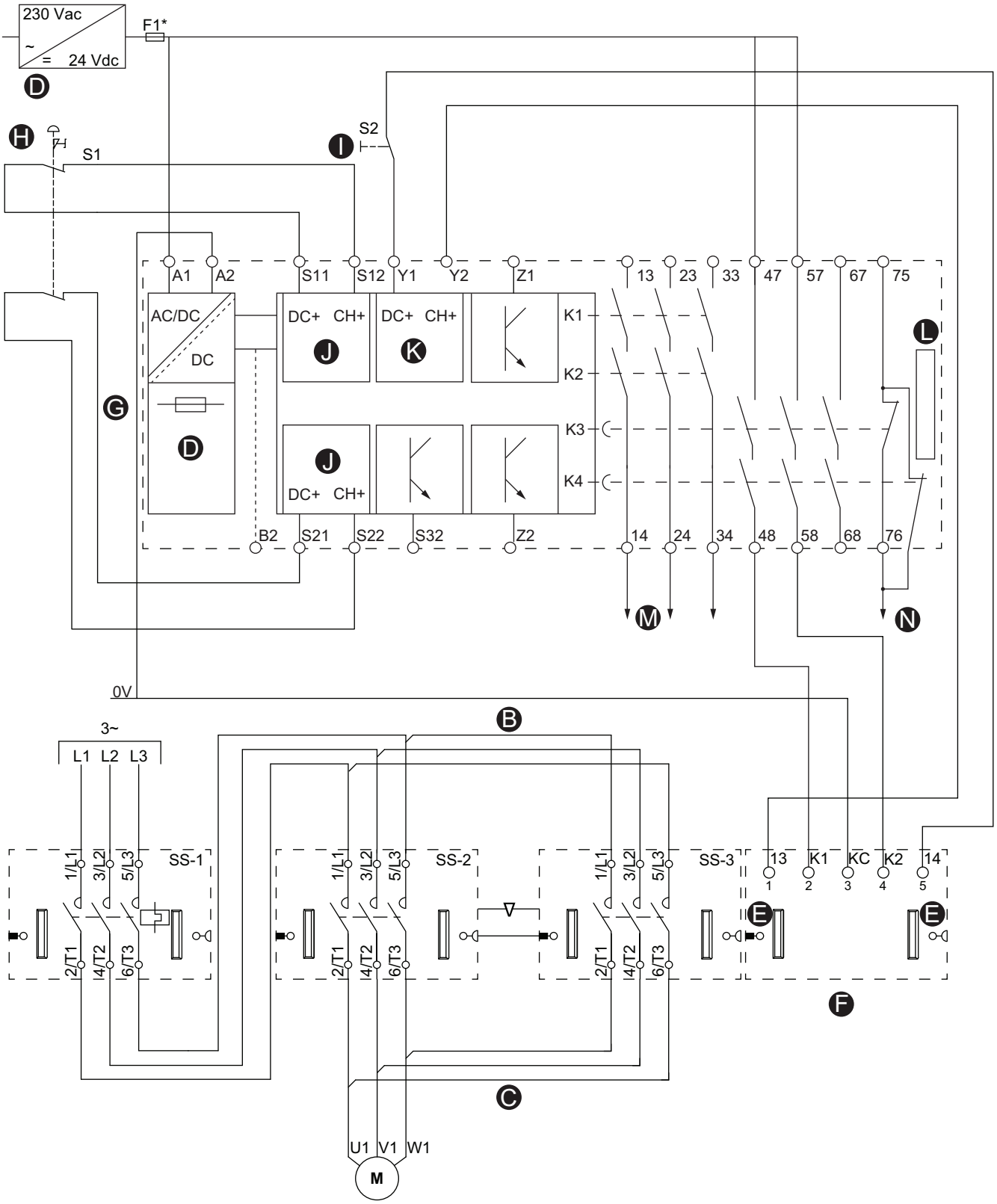


Tableau 8 - Légende pour Exemple : Configuration Moteur deux directions – Arrêt SIL, W. Cat 3/4, Catégorie d'arrêt 1, Catégorie de câblage 3/4, page 39

B	Liaison parallèle	I	Bouton de démarrage S2
C	Liaison inverse	J	Entrée
D	Alimentation	K	Début
E	Connecteur pour câble plat	L	Extension
F	Module d'interface SIL (SIM)	M	Arrêt contrôlé
G	Module Preventa XPS-UAF	N	Catégorie d'arrêt 1
H	Bouton d'arrêt d'urgence (S1)		

Isolation des câbles protégés

⚠DANGER

RISQUE DE FONCTIONNEMENT INATTENDU

Veillez à installer les câbles du système relatif à la sécurité conformément à la norme ISO 13849-2.

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

S'il existe un risque de courts-circuits et de courts-circuits transversaux avec les câbles du système relatif à la sécurité, et qu'ils ne puissent pas être détectés par les équipements en amont, une installation avec câbles protégés conformément à ISO 13849-2 est nécessaire.

Dans une installation avec câbles non protégés, les deux signaux (les deux canaux) d'une fonction de sécurité en court-circuit peuvent être connectés à une tension externe si un câble est endommagé. Dans un tel cas, la fonction de sécurité n'est plus opérationnelle.

Architecture de commutation basse/haute fréquence

Les informations de cette section peuvent être utilisées pour déterminer si vous utilisez une architecture basse ou haute fréquence.

La partie électromécanique du démarreur SIL[23] est caractérisée par un B10d.

Pour calculer le $MTTF_d$ (selon ISO 13849-1) ou λd (selon CEI 62061), on utilise la formule suivante :

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

avec $\lambda d = 1 / MTTF_d$

Nop : Nombre d'opérations annuel moyen

Selon la norme ISO 13849, la durée de fonctionnement d'un composant électromécanique est limitée à T10d (le temps moyen jusqu'à ce que 10 % des composants connaissent une défaillance dangereuse[24]).

La durée de fonctionnement d'un démarreur SIL est donc limitée à :

$$T10d = B10d / Nop$$

Le B10d du démarreur SIL est B10d = 1 369 863 ; en supposant un T10d de 10 ans, le nombre de cycles pour un démarreur SIL TeSys island est limité à Nop = B10d / T10 = 131 400/an (soit une moyenne annuelle de 15 cycles/h).

Si l'application nécessite un Nop inférieur à cette valeur, elle entre dans la catégorie des fréquences de commutation basses (dans laquelle les avatars SIL peuvent être utilisés tels quels). Sinon, elle tombe dans la catégorie des fréquences de commutation élevées (dans laquelle la fonction de sécurité doit être implémentée avec un avatar SIL dédié comme décrit ci-dessous).

23. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
24. Défaillance dangereuse selon ISO 13849

Fréquence de commutation basse (< 15 cycles par heure)

Pour une fréquence de commutation basse, l'arrêt SIL[25] et les fonctions de commande marche/arrêt opérationnelles peuvent être réalisés avec un avatar SIL.

Figure 16 - Exemple d'avatar avec démarreur SIL

Tableau 9 - Fréquence de commutation basse – Fonctions opérationnelles et de sécurité

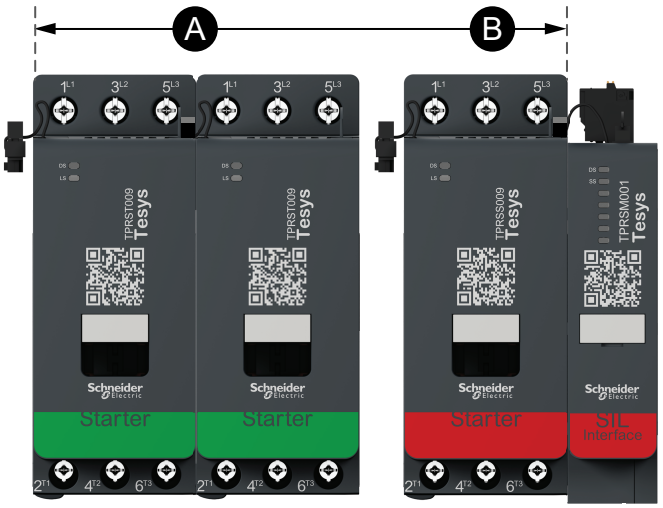
Avatar SIL	Module 1	Module 2	Module 3	Module 4	Module 5
Commutateur – Arrêt SIL, W. Cat 1/2 [26].	Démarreur SIL	SIM	—	—	—
Commutateur – Arrêt SIL, W. Cat 3/4 [27].	Démarreur SIL	Démarreur SIL	SIM	—	—
Moteur une direction – Arrêt SIL, W. Cat 1/2	Démarreur SIL	SIM		—	—
Moteur une direction – Arrêt SIL, W. Cat 3/4	Démarreur SIL	Démarreur SIL	SIM	—	—
Moteur deux directions – Arrêt SIL, W. Cat 1/2	Démarreur SIL	Démarreur SIL	SIM	—	—
Moteur deux directions – Arrêt SIL, W. Cat 3/4	Démarreur SIL	Démarreur SIL	Démarreur SIL	SIM	—
Moteur deux vitesses – Arrêt SIL, W. Cat 1/2	Démarreur SIL	Démarreur SIL	SIM	—	—
Moteur deux vitesses – Arrêt SIL, W. Cat 3/4	Démarreur SIL	Démarreur SIL	Démarreur SIL	SIM	—
Moteur deux vitesses, deux directions – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM
Moteur deux vitesses, deux directions – Arrêt SIL, W. Cat 3/4	Démarreur SIL	Démarreur SIL	Démarreur SIL	Démarreur SIL	SIM
Convoyeur une direction – Arrêt SIL, W. Cat 1/2	Démarreur SIL	SIM	—	—	—
Convoyeur deux directions – Arrêt SIL, W. Cat 1/2	Démarreur SIL	Démarreur SIL	SIM	—	—

25. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
26. Catégorie de câblage 1 et Catégorie de câblage 2 selon la norme ISO 13849
27. Catégorie de câblage 3 et Catégorie de câblage 4 selon la norme ISO 13849

Fréquence de commutation élevée (< 15 cycles par heure)

Pour une utilisation à fréquence élevée, la fonction de sécurité doit être isolée de la fonction opérationnelle par utilisation d'un SIL[28] pour la fonction de sécurité et d'un avatar standard pour la fonction opérationnelle. Les démarreurs standard sont ensuite raccordés en série en aval du ou des démarreurs SIL. Le tableau Fréquence de commutation élevée – Fonctions opérationnelles et de sécurité fournit des exemples d'avatars standard utilisés en aval du ou des démarreurs SIL pour les architectures Arrêt SIL, W. Cat 1/2[29] et Arrêt SIL, W. Cat 3/4[30].

Figure 17 - Avatar standard pour la fonction opérationnelle + avatar SIL pour la fonction de sécurité – Arrêt SIL, W. Cat 1/2



A	Avatar standard
B	Avatar SIL

Tableau 10 - Fréquence de commutation élevée – Arrêt SIL, W. Cat 1/2 – Fonctions opérationnelles et de sécurité

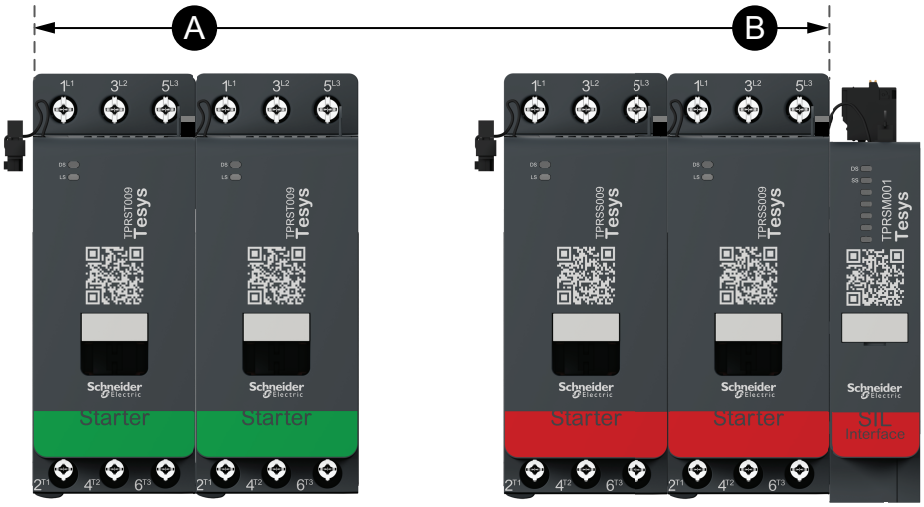
Avatar standard	Avatar SIL	Module 1	Module 2	Module 3	Module 4	Module 5	Module 6
Commutateur	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur SIL	SIM	—	—	—
Moteur une direction	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur SIL	SIM	—	—	—
Moteur deux directions	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur standard	Démarreur SIL	SIM	—	—
Moteur deux vitesses	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur standard	Démarreur SIL	SIM	—	—
Moteur deux vitesses deux directions	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur standard	Démarreur standard	Démar-reur standard	Démar-reur SIL	SIM
Transporteur une direction	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur SIL	SIM	—	—	—
Transporteur deux directions	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur standard	Démarreur SIL	SIM	—	—

28. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
29. Catégorie de câblage 1 et Catégorie de câblage 2 selon la norme ISO 13849.
30. Catégorie de câblage 3 et Catégorie de câblage 4 selon la norme ISO 13849.

Tableau 10 - Fréquence de commutation élevée – Arrêt SIL, W. Cat 1/2 – Fonctions opérationnelles et de sécurité (Suite)

Avatar standard	Avatar SIL	Module 1	Module 2	Module 3	Module 4	Module 5	Module 6
Moteur Y/D une direction	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur standard	Démarreur standard	Démar-reur SIL	SIM	—
Moteur Y/D deux directions	Commutateur – Arrêt SIL, W. Cat 1/2	Démarreur standard	Démar-reur standard	Démarreur standard	Démar-reur standard	Démar-reur SIL	SIM

Figure 18 - Avatar standard pour la fonction opérationnelle + avatar SIL pour la fonction de sécurité – Arrêt SIL, W. Cat 3/4



A	Avatar standard
B	Avatar SIL

Tableau 11 - Fréquence de commutation élevée – Arrêt SIL, W. Cat 3/4 – Fonctions opérationnelles et de sécurité

Avatar standard	Avatar SIL	Module 1	Module 2	Module 3	Module 4	Module 5	Module 6	Module 7
Commuter	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM	—	—	—
Moteur une direction	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM	—	—	—
Moteur deux directions	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM	—	—
Moteur deux vitesses	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM	—	—
Moteur deux vitesses deux directions	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur standard	Démarreur standard	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM
Moteur Y/D une direction	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur standard	Démarreur standard	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM
Moteur Y/D deux directions	Commutateur – Arrêt SIL, W. Cat 3/4	Démarreur standard	Démarreur standard	Démarreur standard	Démarreur standard	Démarreur SIL	Démarreur SIL	SIM

Exemples d’architecture

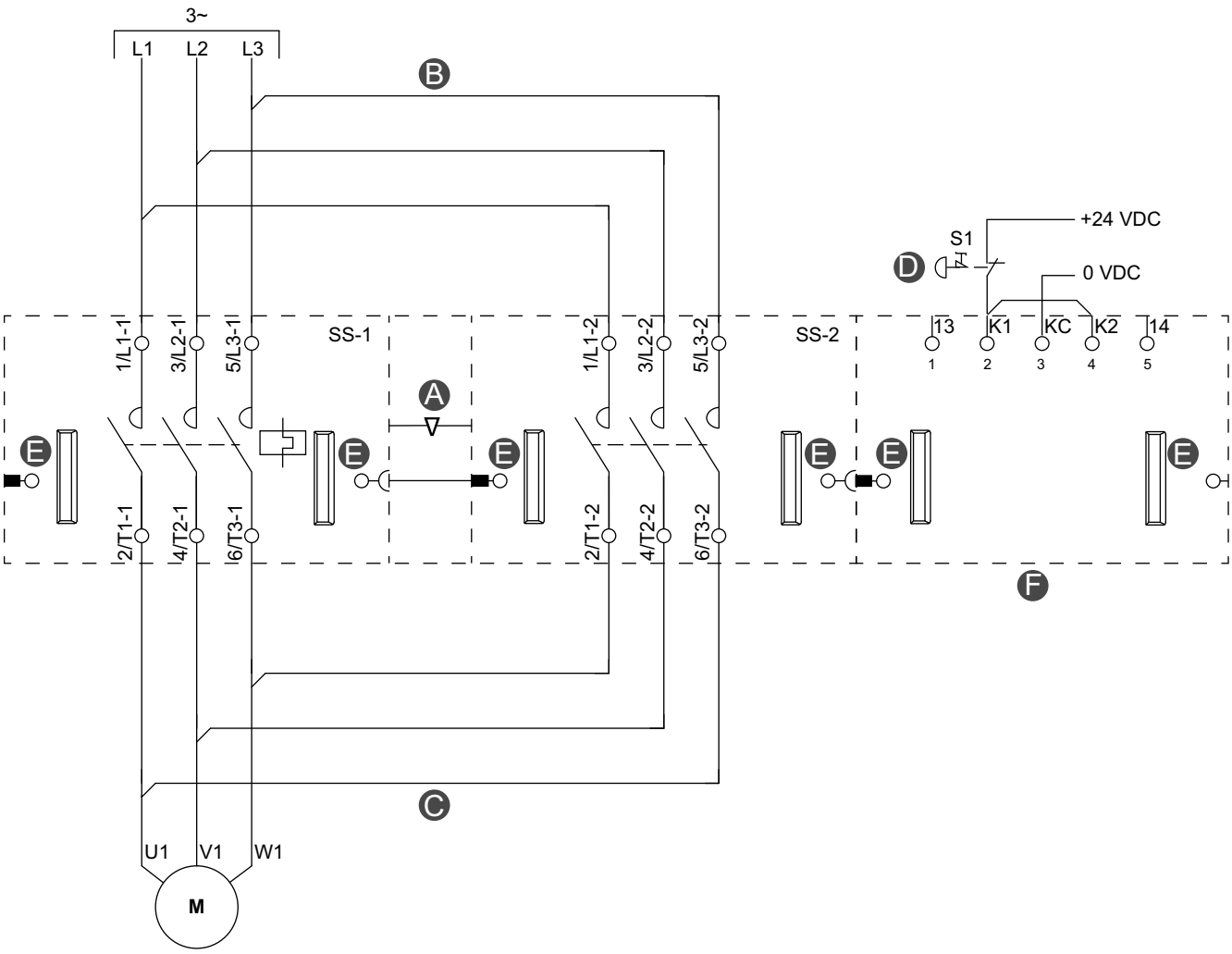
Les architectures suivantes sont disponibles pour la sécurité fonctionnelle de TeSys™ island :

- Arrêt SIL, Catégorie d’arrêt 0, Catégorie de câblage 1[31]
- Arrêt SIL, Catégorie d’arrêt 0, Catégorie de câblage 2
- Arrêt SIL, Catégorie d’arrêt 1, Catégorie de câblage 2
- Arrêt SIL, Catégorie d’arrêt 0, Catégorie de câblage 3/4
- Arrêt SIL, Catégorie d’arrêt 1, Catégorie de câblage 3/4

31. Safety Integrity Level (niveau d’intégrité) selon la norme CEI 61508. Catégorie de câblage 1, Catégorie de câblage 2 et Catégorie de câblage 3/4 selon la norme ISO 13849. Catégorie d’arrêt 0 et Catégorie d’arrêt 1 selon la norme EN/CEI 60204-1.

Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 1

Figure 19 - Exemple : Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 1[32]

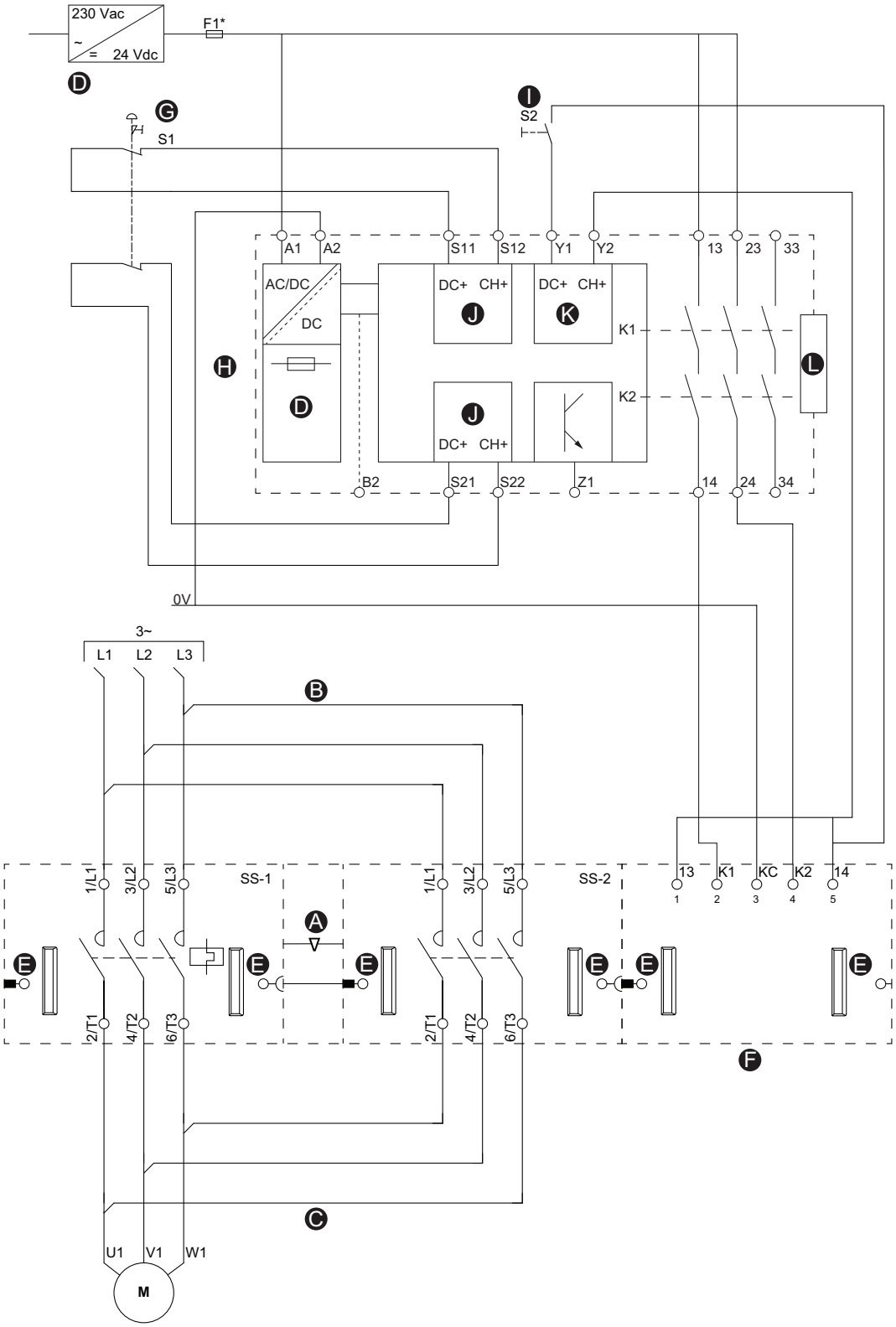


A	Verrouillage mécanique	D	Bouton d'arrêt d'urgence (S1)
B	Liaison parallèle	E	Connecteur pour câble plat
C	Liaison inverse	F	Modules d'interface SIL (SIM)

32. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 1 selon la norme ISO 13849. Catégorie d'arrêt 0 selon EN/CEI 60204-1.

Arrêt SIL, Catégorie d’arrêt 0, Catégorie de câblage 2

Figure 20 - Exemple : Arrêt SIL, Catégorie d’arrêt 0, Catégorie de câblage 2[33]



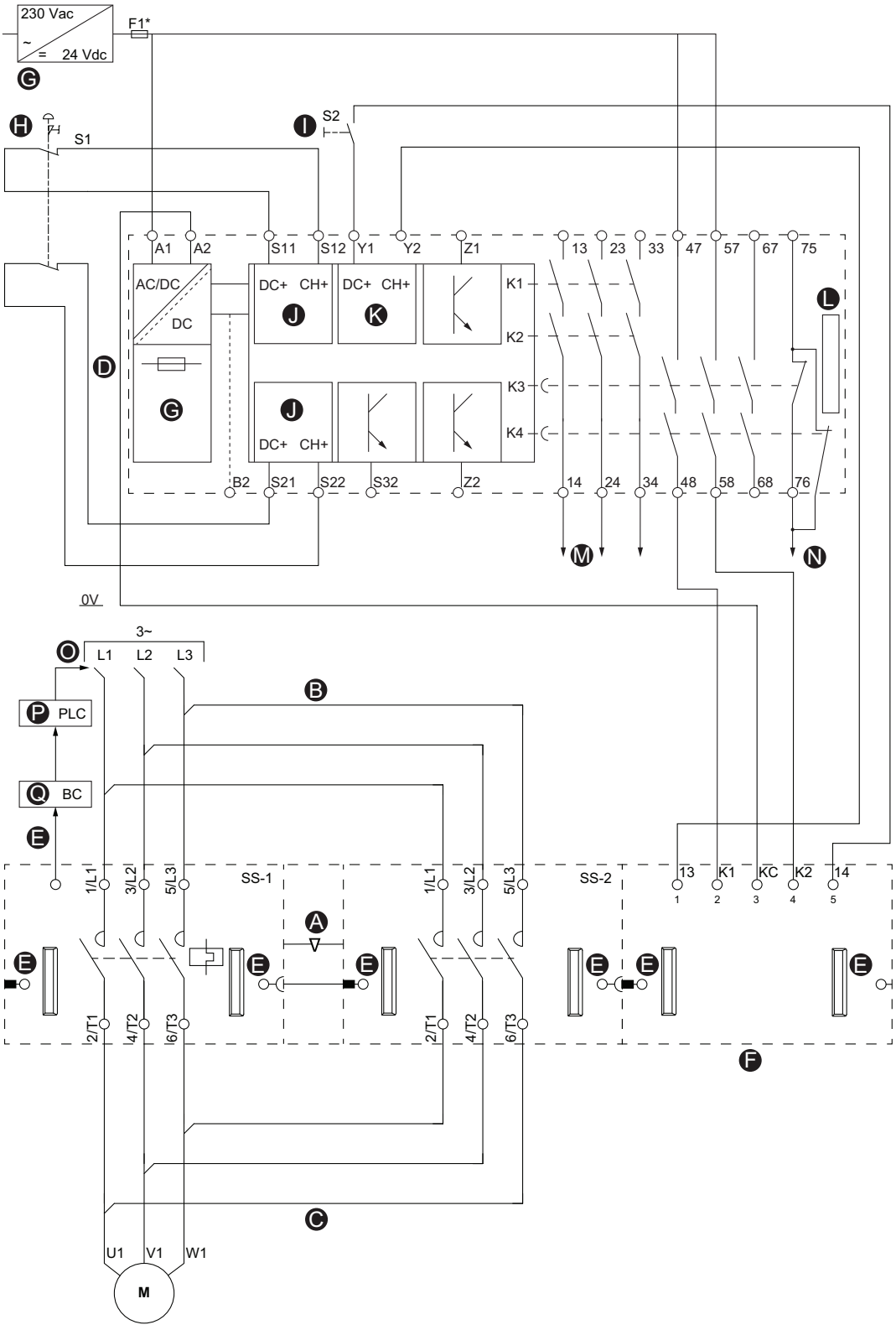
33. Safety Integrity Level (niveau d’intégrité) selon la norme CEI 61508. Catégorie de câblage 2 selon la norme ISO 13849. Catégorie d’arrêt 0 selon EN/CEI 60204-1.

Tableau 12 - Légende de l’exemple : Arrêt SIL, Catégorie d’arrêt 0, Catégorie de câblage 2, page 47

A	Interverrouillage mécanique	G	Bouton d’arrêt d’urgence (S1)
B	Liaison parallèle	H	Module Preventa XPS-UAF
C	Liaison inverse	I	Bouton de démarrage (S2)
D	Alimentation électrique	J	Entrée
E	Connecteur pour câble plat	K	Démarrage
F	Modules d’interface SIL (SIM)	L	Extension

Arrêt SIL, Catégorie d’arrêt 1, Catégorie de câblage 2

Figure 21 - Exemple : Arrêt SIL, Catégorie d’arrêt 1, Catégorie de câblage 2[34]



34. Safety Integrity Level (niveau d’intégrité) selon la norme CEI 61508. Catégorie de câblage 2 selon la norme ISO 13849. Catégorie d’arrêt 1 selon EN/CEI 60204-1.

Tableau 13 - Légende de l’exemple : Arrêt SIL, Catégorie d’arrêt 1, Catégorie de câblage 2, page 49

A	Interverrouillage mécanique	J	Entrée
B	Liaison parallèle	K	Démarrage
C	Liaison inverse	L	Extension
E	Connecteur pour câble plat	M	Arrêt contrôlé
F	Modules d’interface SIL (SIM)	N	Catégorie d’arrêt 1
G	Alimentation électrique	O	Disjoncteur amont
H	Bouton d’arrêt d’urgence (S1)	P	Automate programmable
I	Bouton de démarrage S2	Q	Coupleur de bus

Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 3/4

Figure 22 - Exemple : Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 3/4[35]

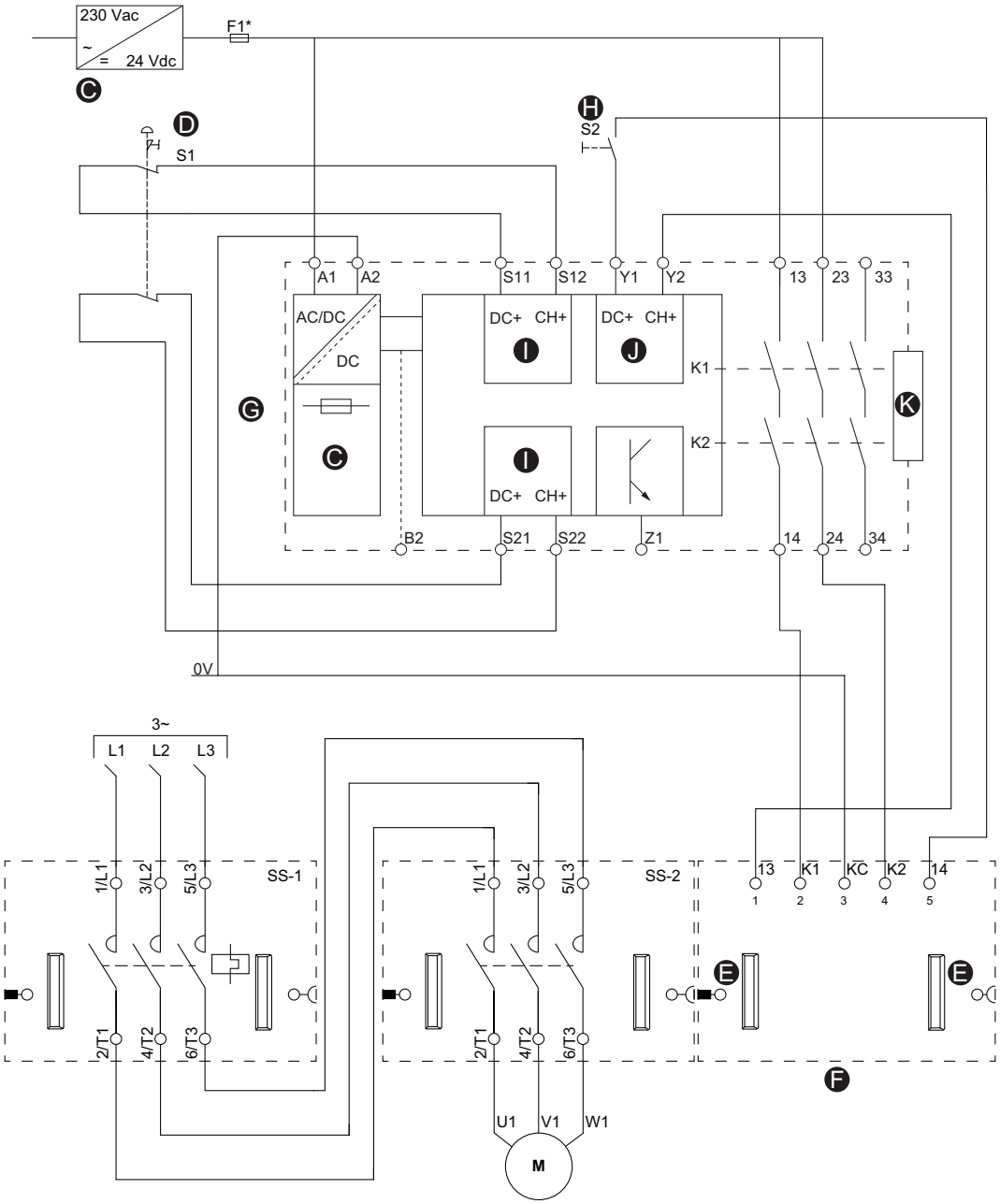


Tableau 14 - Légende de l'exemple : Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 3/4, page 51

C	Alimentation électrique	H	Bouton de démarrage (S2)
D	Bouton d'arrêt d'urgence (S1)	I	Entrée
E	Connecteur pour câble plat	J	Démarrage

35. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 3/4 selon la norme ISO 13849. Catégorie d'arrêt 0 selon EN/CEI 60204-1.

Tableau 14 - Légende de l'exemple : Arrêt SIL, Catégorie d'arrêt 0, Catégorie de câblage 3/4 (Suite)

F	Modules d'interface SIL (SIM)	K	Extension
G	Module Preventa XPS-UAF		

Arrêt SIL, Catégorie d'arrêt 1, Catégorie de câblage 3/4

Figure 23 - Exemple : Arrêt SIL, Catégorie d'arrêt 1, Catégorie de câblage 3/4[36]

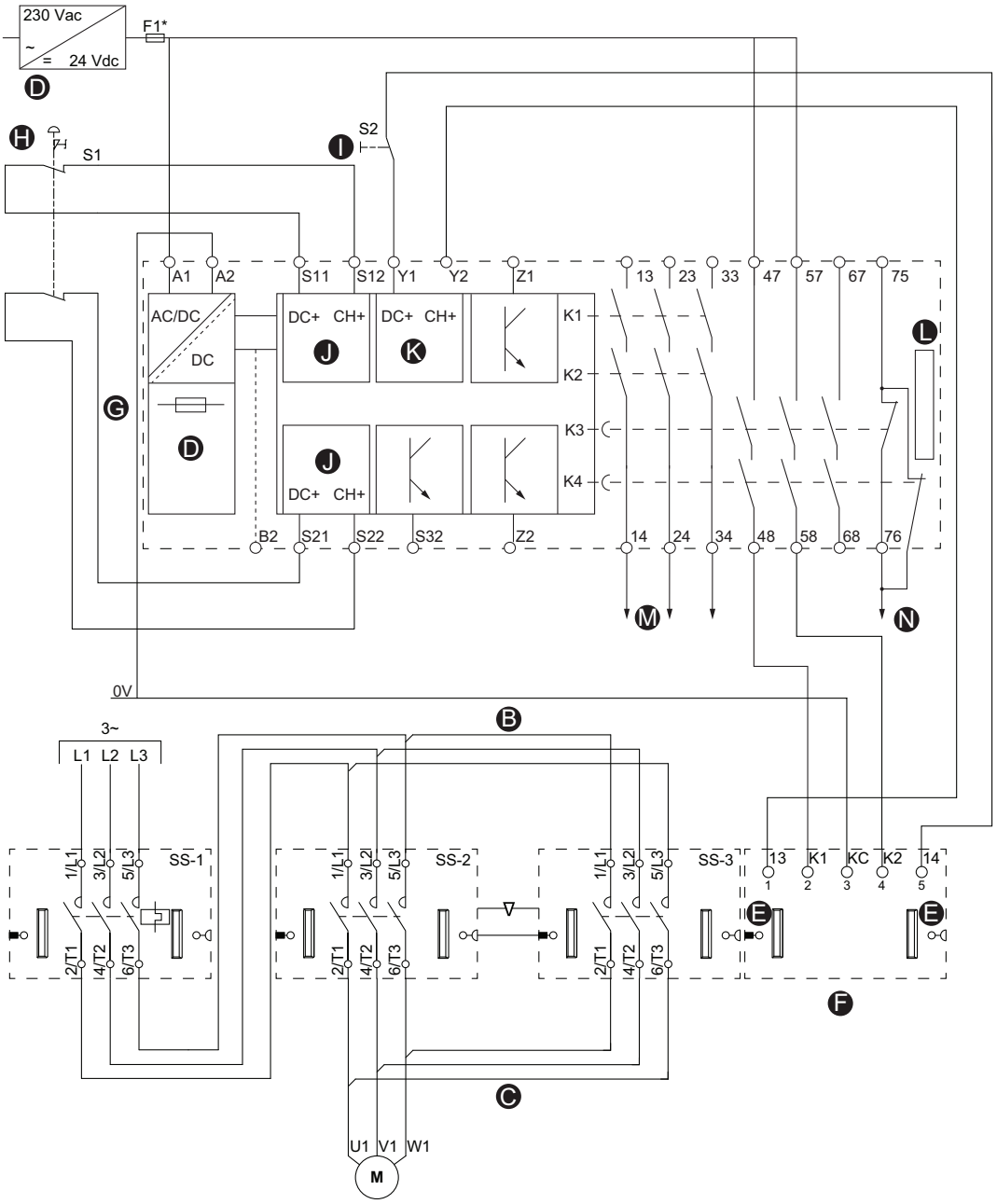


Tableau 15 - Légende de l'exemple : Arrêt SIL, Catégorie d'arrêt 1, Catégorie de câblage 3/4, page 53

B	Liaison parallèle	I	Bouton de démarrage S2
C	Liaison inverse	J	Entrée
D	Alimentation électrique	K	Démarrage
E	Connecteur pour câble plat	L	Extension

36. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508. Catégorie de câblage 3/4 selon la norme ISO 13849. Catégorie d'arrêt 1 selon EN/CEI 60204-1.

Tableau 15 - Légende de l’exemple : Arrêt SIL, Catégorie d’arrêt 1, Catégorie de câblage 3/4 (Suite)

F	Module d’interface SIL (SIM)	M	Arrêt contrôlé
G	Module Preventa XPS-UAF	N	Catégorie d’arrêt 1
H	Bouton d’arrêt d’urgence (S1)		

Données techniques

Module d'interface SIL

Tableau 16 - Valeurs calculées du module d'interface SIL[37] (SIM)

Architecture	SIM					
	PFH[38]	PFD[39]	SFF[40]	HFT[41]	$MTTF_d$ (années)	DC[42]
Catégorie de câblage 1[43]	$2{,}10^{-10}$	$2{,}10^{-5}$	>90 %	1	17 459	Sans objet
Catégorie de câblage 2			>99 %			90 %
Catégorie de câblage 3			>99 %			90 %
Catégorie de câblage 4			99 %			99 %

NOTE: Les valeurs PFD et PFH sont calculées comme suit :

- Intervalle de test = 20 ans
- MTTR[44]=MRT[45]= 24 heures

Les exigences architecturales définies dans le tableau 3 de la norme CEI 61508-2 et le tableau 5 de la norme EN 62061 sont satisfaites jusqu'au niveau SIL 3.

Démarreur SIL

Les données suivantes permettent de définir le niveau de performance des démarreurs SIL[37].

B10 : **1 000 000**

% de défaillances dangereuses[46] : **73%**

$B10_d$: **1 369 863**

En supposant un nombre d'opérations = 131 400 périodes/an (moyenne de 15 périodes/heure)

Le tableau suivant donne les valeurs calculées du démarreur SIL :

Tableau 17 - Démarreur SIL en monocanal

Catégorie de câblage[47]	SFF	HFT	$MTTF_d$ (années)	DC
Catégorie 1	27 %	0	100 années	Sans objet
Catégorie 2 – Surveillance directe	90 %	0	100 années	≥ 90 %

37. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
38. Fréquence moyenne de défaillances dangereuses [h-1], au sens de la norme CEI 61508-4
39. Probabilité de défaillance dangereuse en cas de sollicitation, au sens de la norme CEI 61509-4.
40. Proportion de défaillances en sécurité, au sens de la norme CEI 61509-4.
41. Tolérance aux défaillances du matériel, au sens de la norme CEI 61509-4.
42. Couverture du diagnostic, au sens de la norme CEI 61509-4.
43. Catégories de câblage 1, 2, 3 et 4 selon la norme ISO 13849.
44. Temps moyen avant dépannage, au sens de la norme CEI 61509-4
45. Temps moyen de dépannage, au sens de la norme CEI 61509-4
46. Défaillance dangereuse au sens de la norme CEI 61508-4
47. Catégories de câblage 1, 2, 3 et 4 selon la norme ISO 13849.

Tableau 18 - Démarreur SIL en bicanal

Catégorie de câblage	SFF	HFT	$MTTF_d$ (années)	DC
Catégorie 3	27 %	0	100 années	≥ 90 %
Catégorie 4	90 %	0	100 années	≥ 99 %

Le tableau suivant donne la relation entre les valeurs PFH_d et PFD des démarreurs SIL, en fonction de l'architecture et de l'intervalle de test :

Tableau 19 - Démarreurs SIL – PFH_d et PFD

Catégorie de câblage	PFH (CEI 61508)	PFD (CEI 61508) Ti = 10 ans[48]	PFD (CEI 61508) Ti = 5 ans[48]
Catégorie 1	1,10E-06	4,80E-02	4,82E-03
Catégorie 2 – Surveillance directe	1,10E-06	4,82E-03	5,06E-04
Catégorie 3	4,5E-09	—	1.30E-04
Catégorie 4	2.5E-10	—	2.5E-06

Les exigences architecturales définies dans le tableau 3 de la norme CEI 61508-2 et le tableau 5 de la norme EN 62061 sont satisfaites jusqu'au niveau SIL 2.

Une architecture de catégorie 2 sera nécessaire pour répondre aux contraintes architecturales de SIL 2 (par surveillance directe Mirror In/Mirror Out).

NOTE: La détection de défaut et la réaction aux défaut spécifiées doivent être réalisées avant que la situation dangereuse traitée par la fonction de commande de sécurité ne puisse se produire.

48. Intervalle de test

Données de fiabilité

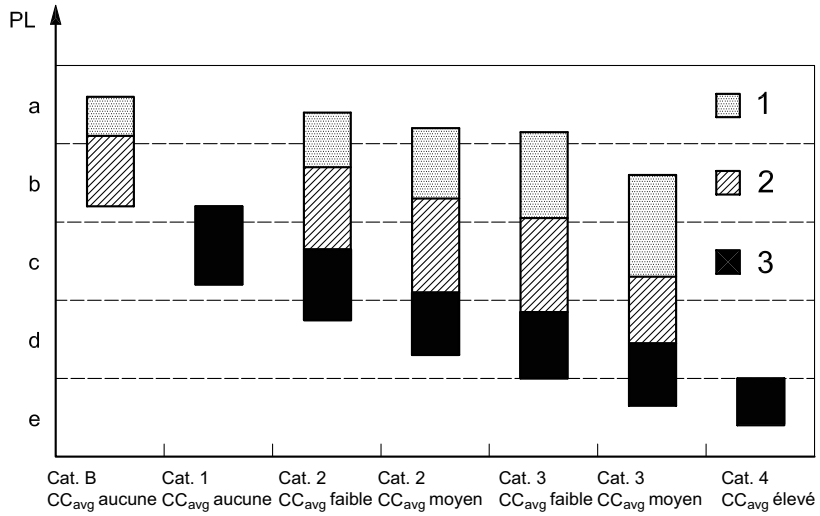
Référence de la norme de la fonction de sécurité

La fonction Arrêt SIL[49] est prioritaire sur un arrêt déclenché pour des raisons opérationnelles (EN ISO 13849-1, 5.2.1).

Le niveau de performance dépend de la catégorie de câblage[50], du $MTTF_d$ et du DC_{avg}.

Le diagramme suivant indique le positionnement de TeSys™ island par rapport aux exigences de la catégorie.

Figure 24 - Positionnement de TeSys island par exigence de catégorie



Légende

PL – Niveau de performance

1 $MTTF_d$ de chaque canal = faible

2 $MTTF_d$ de chaque canal = moyen

3 $MTTF_d$ de chaque canal = élevé

Tableau 20 - Procédure simplifiée pour l'évaluation de la performance des parties des systèmes de contrôle liées à la sécurité (SRP/CS)

Catégorie	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**Aucun**	**Aucun**	**faible**	**moyen**	**faible**	**moyen**	**élevé**
$MTTF_d$ de chaque canal							
Faible	a	Non couvert	a	b	b	c	Non couvert
Moyen	b	Non couvert	b	c	c	d	Non couvert
Élevé	Non couvert	c	v	d	d	d	e

Selon l'architecture de TeSys island et la catégorie de câblage, les indicateurs clés (DC_{avg}, $MTTF_d$, PL) pour TeSys island respectent les valeurs indiquées dans le tableau ci-dessous.

49. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
50. Catégories de câblage selon la norme ISO 13849.

Tableau 21 - Valeurs des indicateurs clés pour les architectures monocanal et bicanal

Architecture du système TeSys island	Catégorie	Tolérance à défaut unique [51]	DC_{avg}	$MTTF_d$ de chaque canal	PL cible
Monocanal	1	Non	Aucune	Élevé (≥ 30 ans)	c
	2	Non	Faible (≥ 60 %) à moyen (≥ 90 %)	Faible (≥ 3 ans) à élevé (≥ 30 ans)	c, d
Bicanal	3	Yes			c, d, e
	4	Yes	Élevé (≥ 99 %)	Élevé (≥ 30 ans)	e

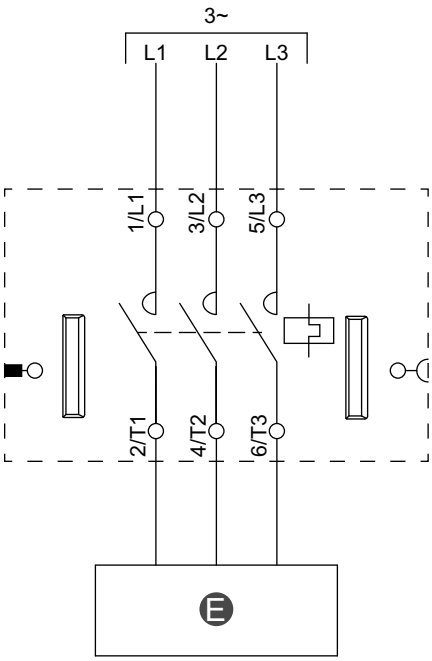
Raccordement des avatars SIL

Les schémas de câblage de cette section concernent les avatars SIL[52]. Le tableau suivant donne la légende des diagrammes de cette section.

Tableau 22 - Légende des schémas de câblage

A	Verrouillage mécanique
B	Liaison parallèle
C	Liaison inverse
E	Circuit électrique

Figure 25 - Commutateur – Arrêt SIL, W. Cat 1/2[53]



51. Tolérance à défaut unique signifie qu'un défaut unique (y compris les événements de mode commun) ne doit pas entraîner la perte de la fonction de sécurité.
52. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
53. Catégorie de câblage 1 et Catégorie de câblage 2 selon la norme ISO 13849.

Figure 26 - Moteur une direction – Arrêt SIL, W. Cat 1/2

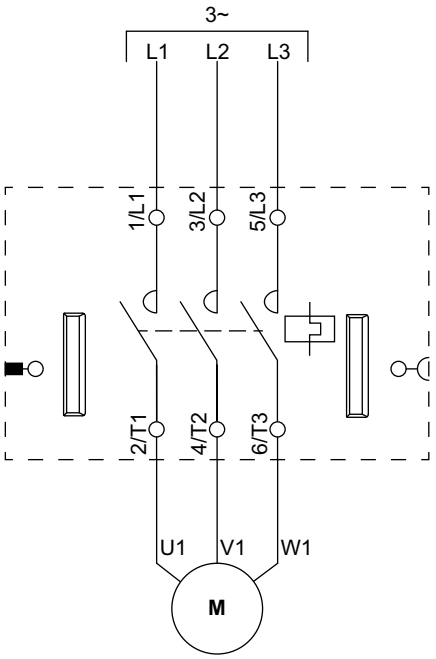


Figure 27 - Moteur deux directions – Arrêt SIL, W. Cat 1/2

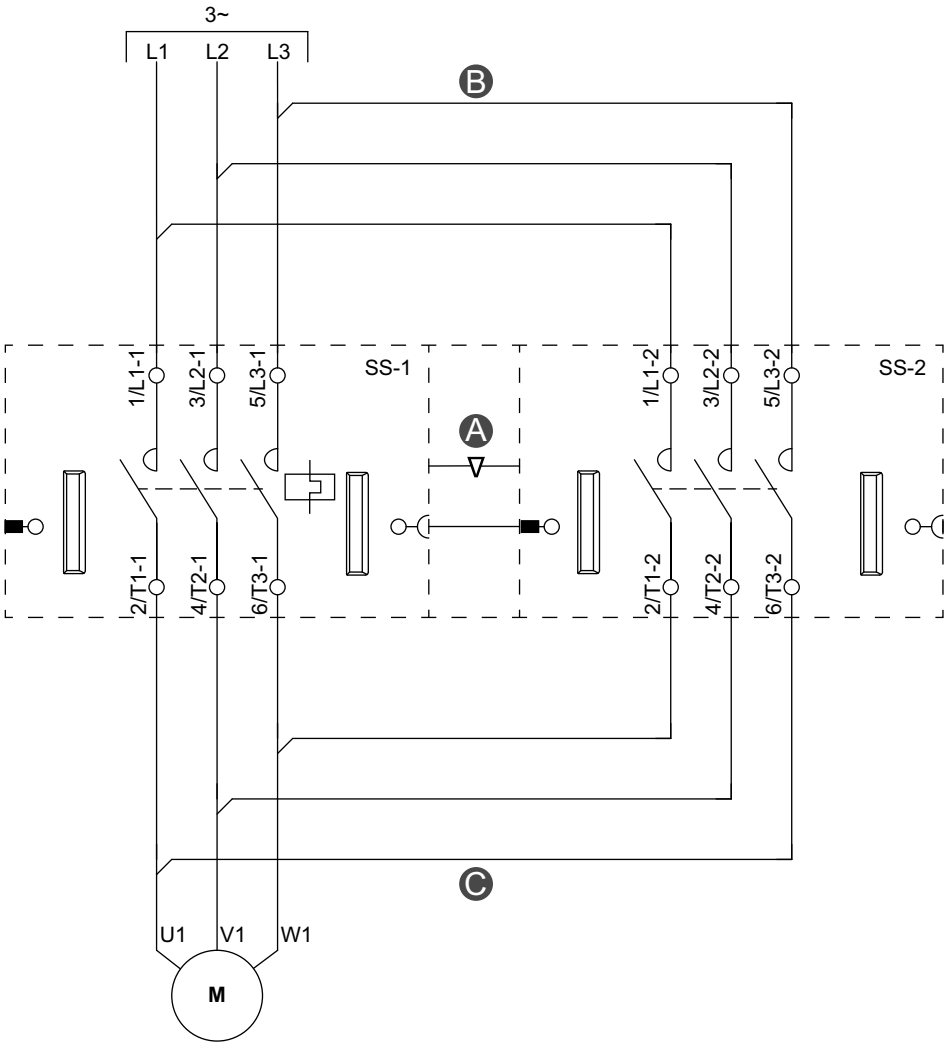


Figure 28 - Moteur deux vitesses – Arrêt SIL, W. Cat 1/2

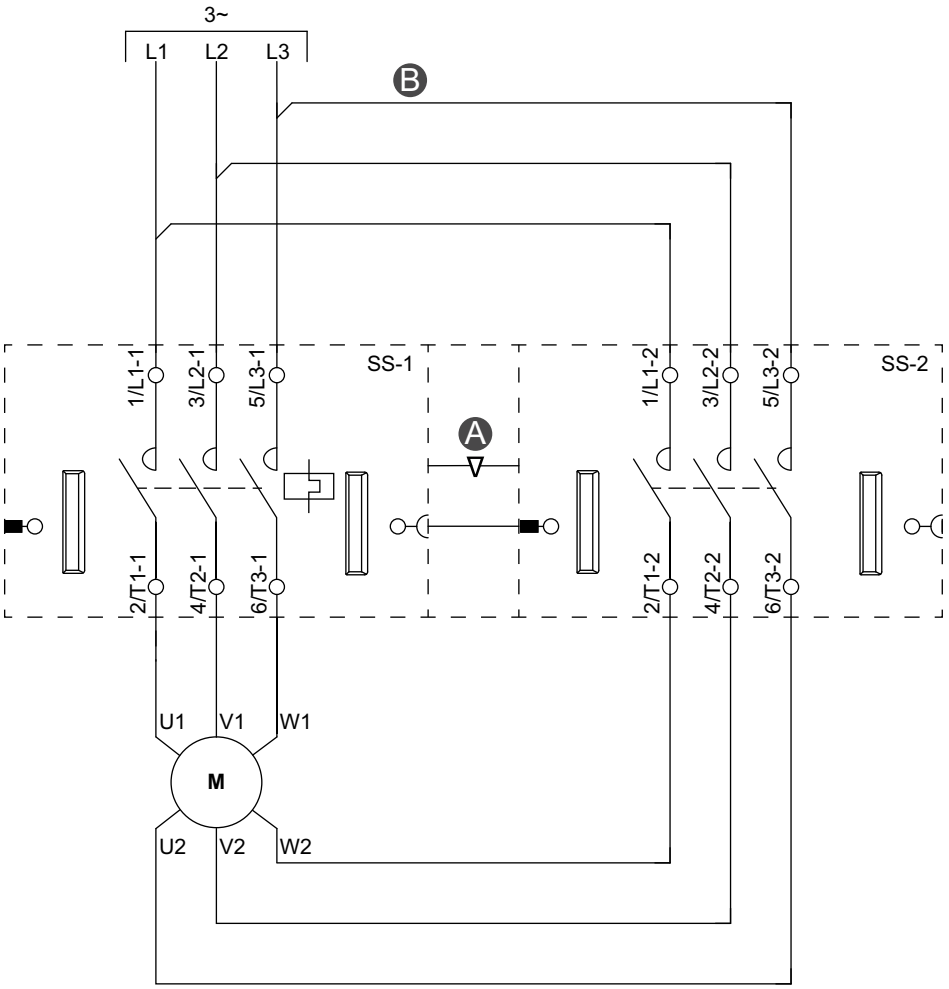


Figure 29 - Moteur deux vitesses, deux directions – Arrêt SIL, W. Cat 1/2

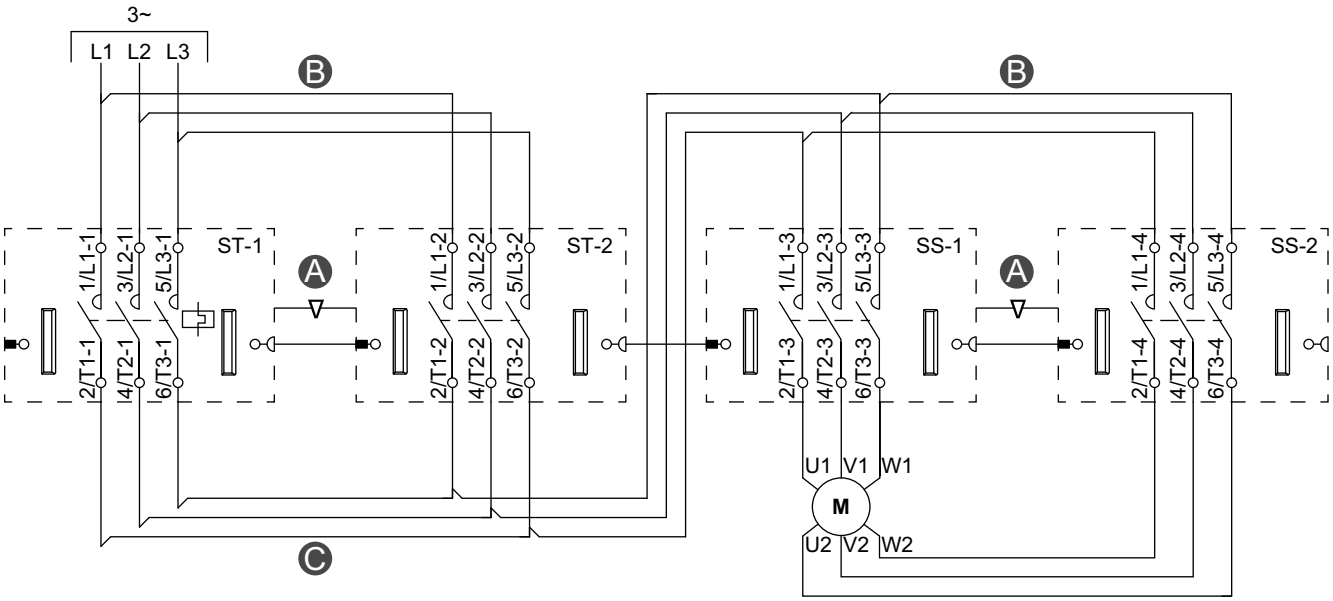


Figure 30 - Commutateur – Arrêt SIL, W. Cat 3/4[54]

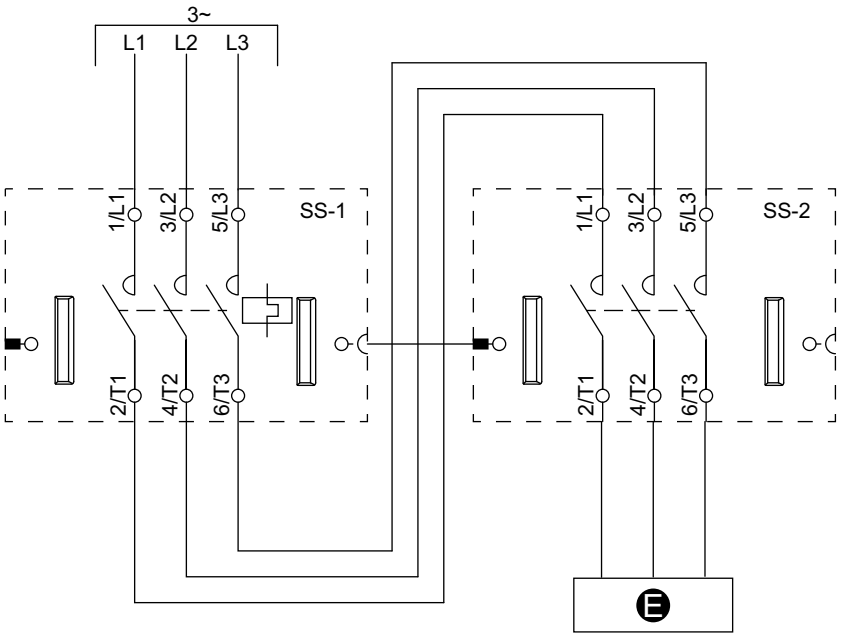
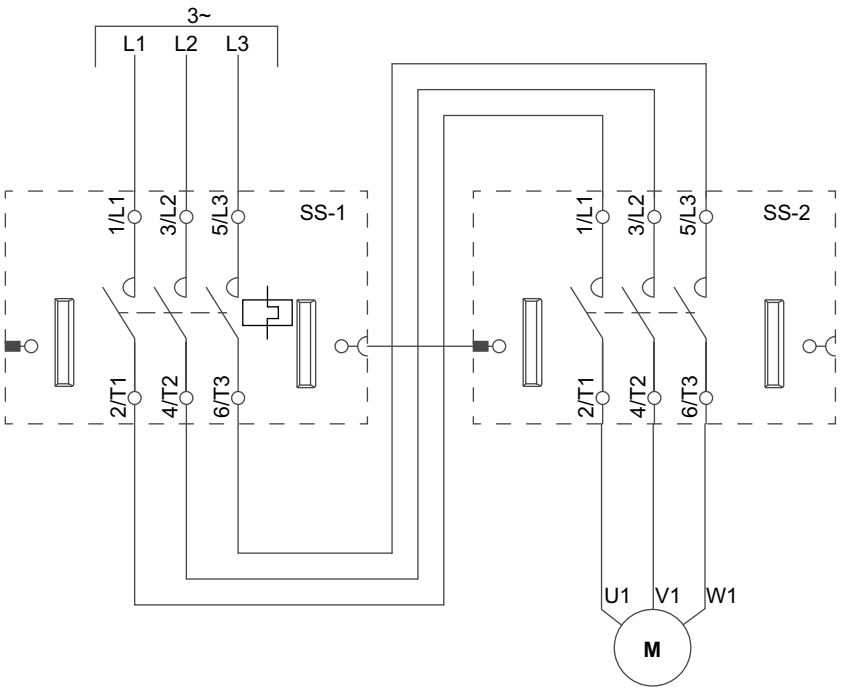


Figure 31 - Moteur une direction – Arrêt SIL, W. Cat 3/4



54. Catégorie de câblage 3 et Catégorie de câblage 4 selon la norme ISO 13849.

Figure 32 - Moteur deux directions – Arrêt SIL, W. Cat 3/4

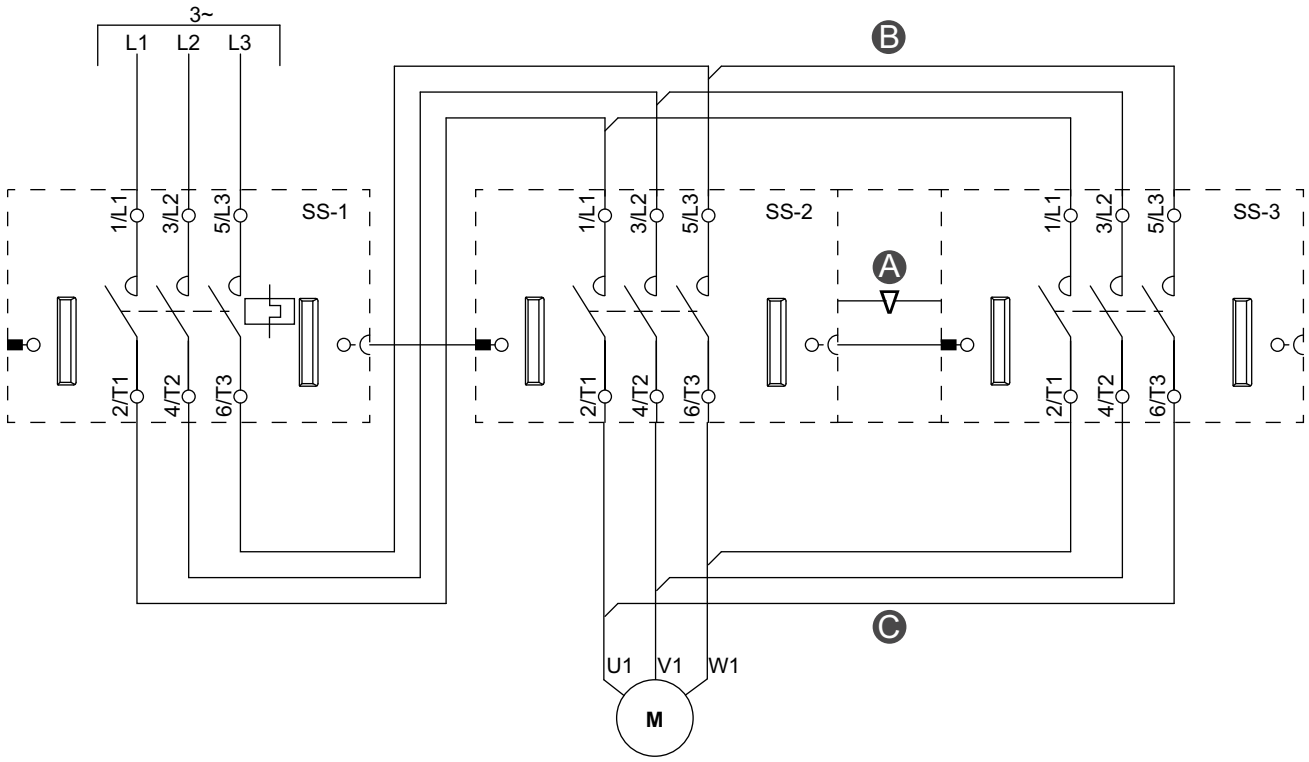


Figure 33 - Moteur deux vitesses – Arrêt SIL, W. Cat 3/4

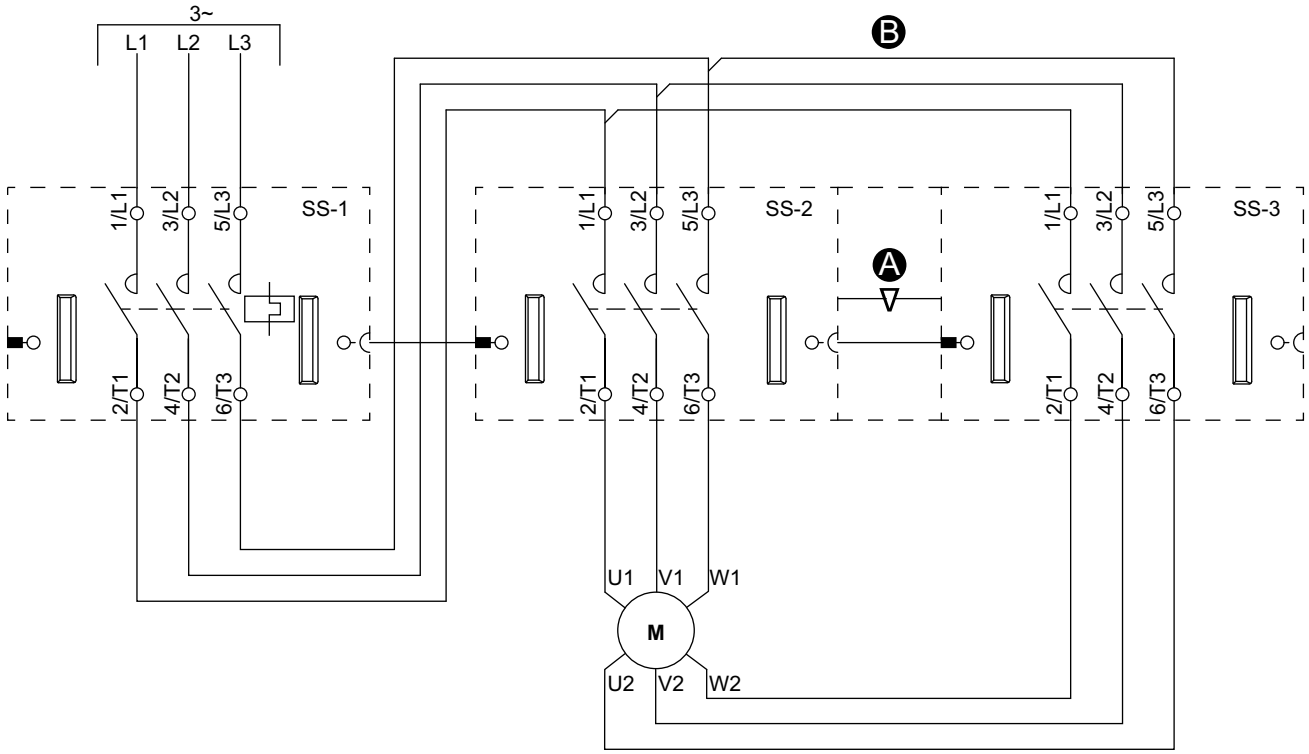


Figure 34 - Moteur deux vitesses, deux directions – Arrêt SIL, W. Cat 3/4

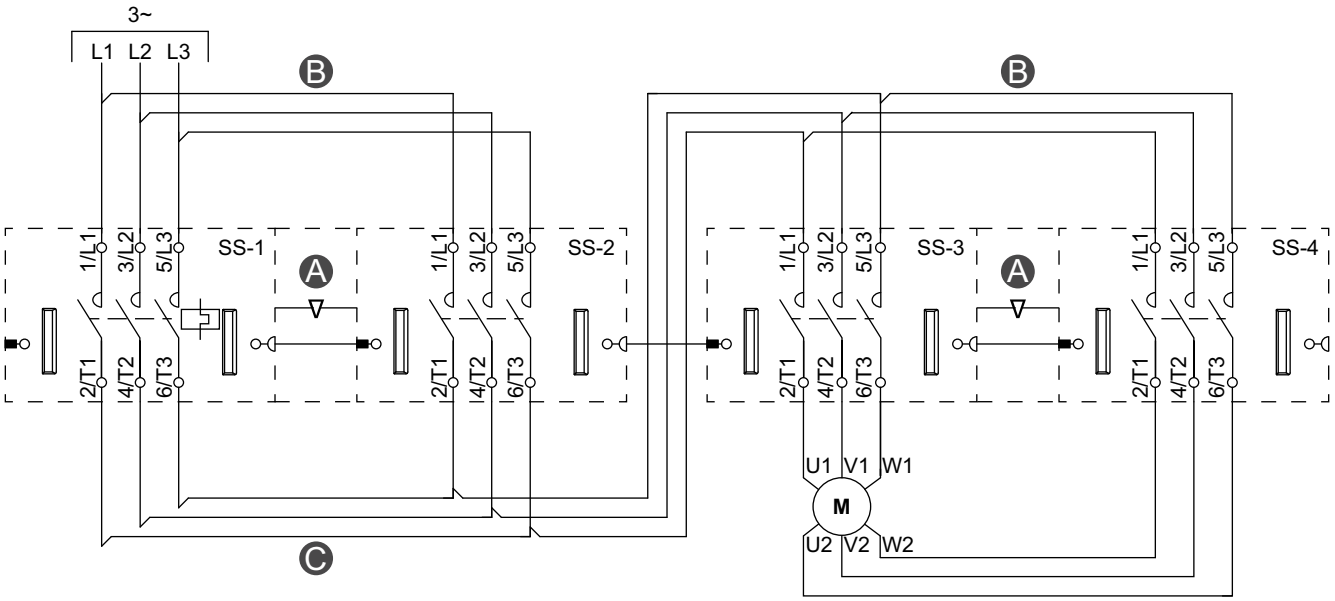


Figure 35 - Convoyeur une direction – Arrêt SIL, W. Cat 1/2

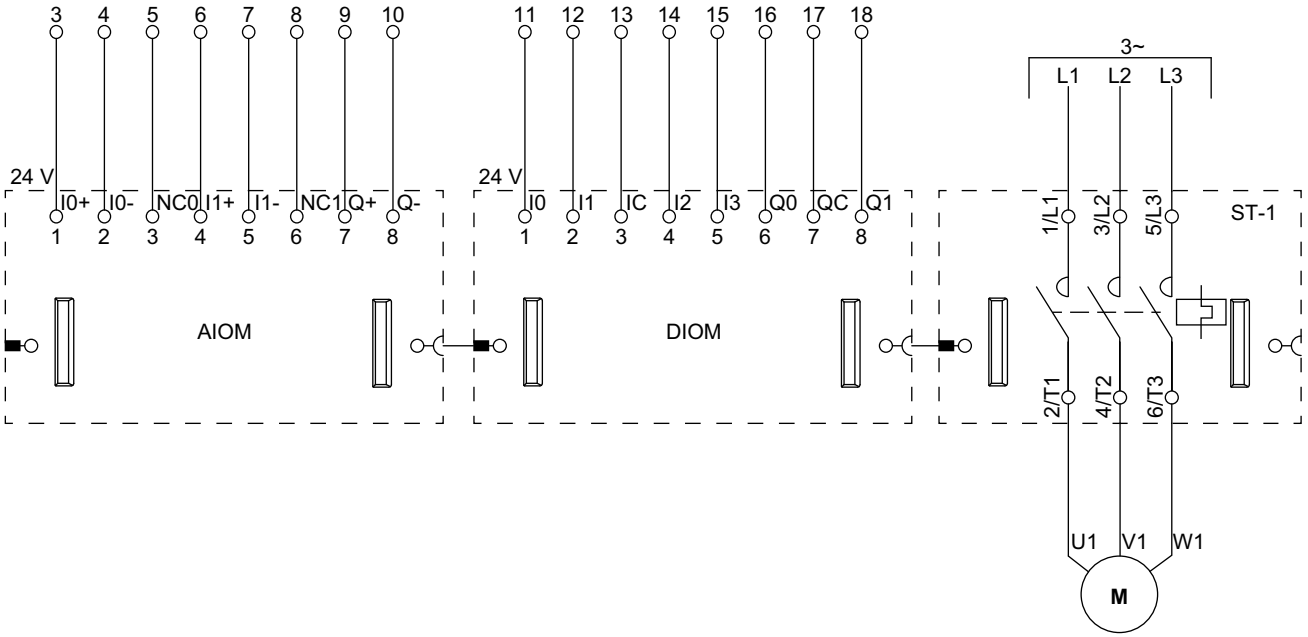
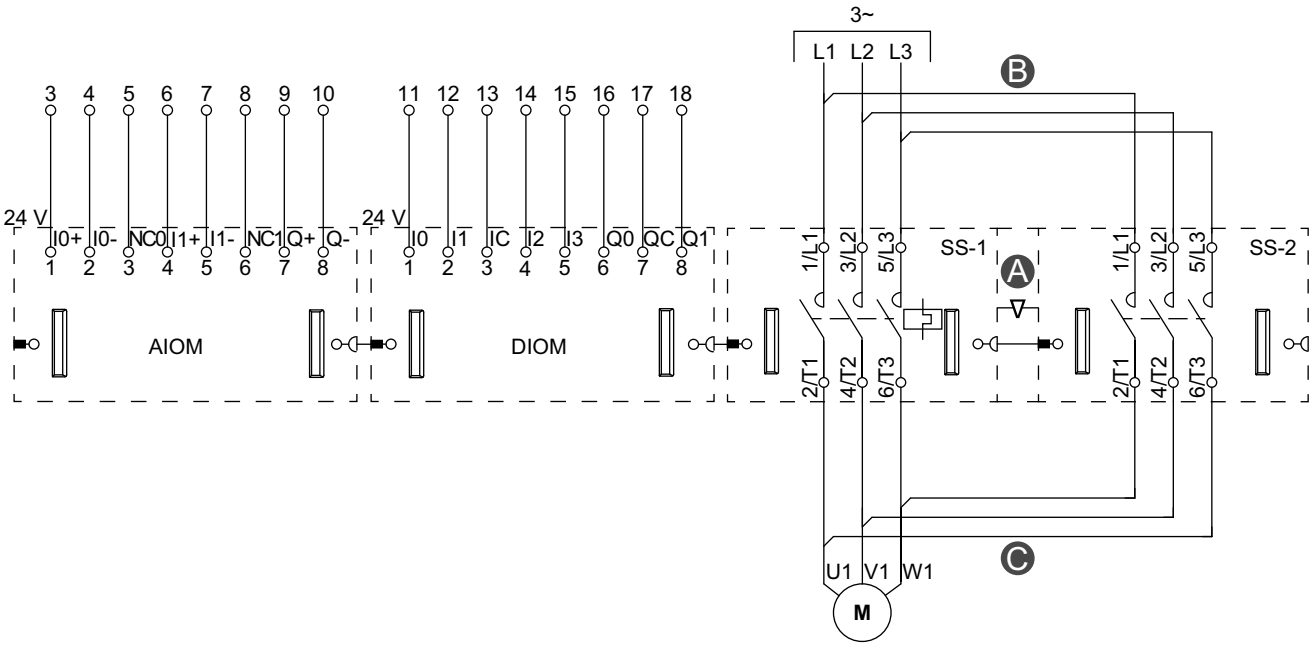


Figure 36 - Convoyeur deux directions – Arrêt SIL, W. Cat 1/2



Mise en service de la fonction de sécurité

Suivez cette procédure pour mettre en service la fonction de sécurité. La procédure comprend deux étapes :

- Essais d'installation
- Essais de la fonction de sécurité[55]

Essais d'installation

Suivez la procédure détaillée dans le tableau suivant pour tester l'installation de la fonction de sécurité.

Tableau 23 - Essai de l'installation

1	Dans le panneau **DIAGNOSTICS** du DTM TeSys™ island, vérifiez que la topologie physique correspond à la topologie logique.
2	Dans le panneau **MON AVATAR** du DTM TeSys island, vérifiez dans **PARAMÈTRES AVATAR** que les avatars SIL sont associés au groupe SIL[56] approprié.

Essai de la fonction de sécurité

L'essai de la fonction de sécurité doit être réalisé pour chaque groupe SIL[56] de l'îlot. Un groupe SIL peut comprendre plusieurs avatars SIL gérés par un module d'interface SIL (SIM).

L'essai de la fonction de sécurité est considéré comme réussi si, lors de l'activation du dispositif d'arrêt d'urgence associé à un groupe SIL, tous les démarreurs SIL appartenant à ce groupe SIL passent à l'état sécurisé (charge mise hors tension).

> **NOTE:** Pour la catégorie d'arrêt 0 (arrêt non contrôlé), l'arrêt doit être immédiat. Pour la Catégorie d'arrêt 1 (arrêt contrôlé), l'arrêt est effectif après un délai.[57]

Pour effectuer l'essai de la fonction de sécurité, suivez la procédure détaillée dans le tableau suivant pour chaque groupe SIL de l'îlot.

55. Essai de fonction au sens de la norme CEI 62061
56. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
57. Catégorie d'arrêt 0 et Catégorie d'arrêt 1 selon la norme EN/CEI 60204-1.

Tableau 24 - Essai de la fonction de sécurité

1	Activez le dispositif d'arrêt d'urgence associé au groupe SIL et vérifiez que tous les démarreurs SIL appartenant au groupe entrent dans l'état sécurisé (charge mise hors tension). **NOTE:** Le voyant d'état du dispositif DS (pour Device Status) des démarreurs SIL clignote en rouge pour indiquer un état d'événement mineur du dispositif. Si l'essai échoue : • Le dispositif d'arrêt d'urgence est peut-être raccordé au mauvais module SIM. Vérifiez ces raccordements. • Le dispositif d'arrêt d'urgence n'est peut-être pas correctement raccordé au module SIM. Vérifiez ces raccordements. • Certains avatars SIL ne sont peut-être pas reliés au groupe SIL en question. Vérifiez la configuration.
2	Dans le panneau **AVATARS** du DTM ou de l'OMT TeSys™ island, section **DIAGNOSTICS**, vérifiez les rubriques **ÉTAT** et **JOURNAUX D'ÉVÉNEMENTS** pour vérifier que l'**état du groupe SIL** est bien « **Commande d'arrêt** ». La mention indiquée dans le journal des événements sera « SIL Group Stop cmd, Safe State achieved ». Si l'essai échoue : • Certains avatars SIL ne sont peut-être pas reliés au groupe SIL en question. Vérifiez la configuration.
3	Dans la section **ÉQUIPEMENTS** du panneau **DIAGNOSTICS**, vérifiez que l'**état du module Interface SIL (SIM)** est bien « **Commande d'arrêt** ». La mention indiquée dans le journal des événements sera « SIL Group Stop cmd, Safe State achieved ». Si l'essai échoue : • Le dispositif d'arrêt d'urgence est peut-être raccordé au mauvais module SIM. Vérifiez ces raccordements. • Le dispositif d'arrêt d'urgence n'est peut-être pas correctement raccordé au module SIM. Vérifiez ces raccordements.
4	Envoyez une commande de démarrage à un avatar SIL appartenant au groupe SIL et vérifiez qu'il n'y a pas de démarrage : les démarreurs doivent rester ouverts et la commande de démarrage doit être ignorée jusqu'à ce que le dispositif d'arrêt d'urgence soit réinitialisé. Si l'essai échoue : • Certains avatars SIL ne sont peut-être pas reliés au groupe SIL en question. Vérifiez la configuration. Si l'un de ces essais continue d'échouer malgré les mesures correctives, cessez d'utiliser l'îlot. Remplacez les appareils pour lesquels l'essai a échoué.
5	Une fois le test de sécurité terminé, réinitialisez le dispositif d'arrêt d'urgence et vérifiez que tous les démarreurs SIL et les modules d'interface SIL sont à l'état Prêt (voyant DS vert fixe).

Exigences relatives à la maintenance de la fonction de sécurité

Cette section décrit les procédures courantes nécessaires au maintien de la sécurité fonctionnelle de votre TeSys island™.

Programme de maintenance

Les intervalles de maintenance dépendent du mode de fréquence.

- En mode basse fréquence (nombre de cycles de contacteurs annuel moyen inférieur à 15 cycles/heure), la maintenance doit être effectuée tous les 12 mois.
- En mode haute fréquence (nombre de cycles de contacteurs annuel moyen supérieur à 15 cycles/heure ou 136 986 cycles/an), effectuez la maintenance à des intervalles correspondant à 1/10e de la durée de vie estimée de l'équipement.

Durée de vie estimée de l'équipement (années) = B10d (= 1 369 863) / nombre de cycles de contacteurs annuel moyen

Contrôles de maintenance

Contrôles de l'état des équipements

Effectuez les contrôles décrits dans le tableau suivant pour vérifier que les cycle des contacteurs des SIL[58] restent dans les limites d'une durée de vie acceptable.

1	En utilisant la fonction **DIAGNOSTICS** des outils DTM ou OMT TeSys™ island, accédez aux informations matérielles de chaque démarreur SIL.
2	Si le **Nombre de cycles de contacteurs** est supérieur à B10d (= 1 369 863), remplacez le démarreur SIL.
3	Si ce n'est pas le cas, utilisez la valeur **Nombre de cycles de contacteurs** pour programmer la prochaine maintenance. Voir Programme de maintenance, page 67.

Essai de la fonction de sécurité

Effectuez l'essai de fonction de sécurité pour chaque groupe SIL[58]. Groupe. Voir Essai de la fonction de sécurité, page 65.

58. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.

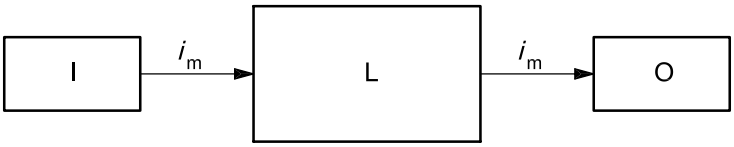
Annexe : Architecture monocanal

Cette architecture monocanal englobe les catégories de câblage 1 et 2.

Exigences architecturales pour la catégorie de câblage 1

L'architecture désignée pour la **catégorie 1** est définie dans la norme EN ISO 13849-1, 6.2.4.

Figure 37 - Architecture désignée pour la catégorie 1 (EN ISO 13849-1)



I : équipement d'entrée (input)

L : logique

O : équipement de sortie (output)

^{i}m : moyens d'interconnexion

Pour la catégorie de câblage 1, le SRP/CS, partie du système de commande relative à la sécurité, doit être conçu et construit à l'aide de **composants éprouvés**.

Un « composant éprouvé » pour une application relative à la sécurité est un composant qui a été :

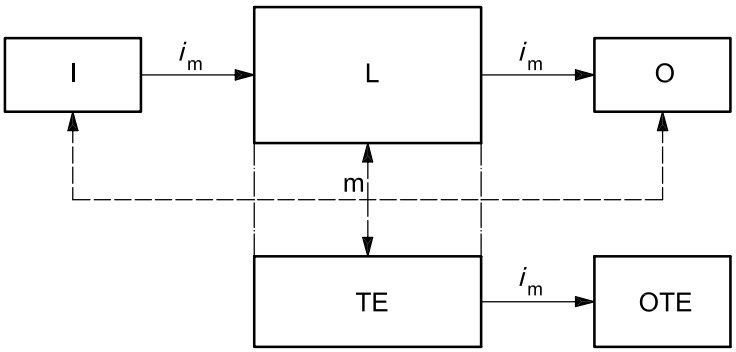
- soit largement utilisé dans le passé avec des résultats positifs dans des applications similaires ;
- soit fabriqué et vérifié selon des principes qui démontrent leur adéquation et leur fiabilité pour des applications relatives à la sécurité.

Il n'y a **pas de couverture de diagnostic** (DC_{avg} = aucune) dans les systèmes de catégorie 1.

Exigences architecturales pour la catégorie de câblage 2

L'architecture désignée pour la **catégorie 2** est définie dans la norme EN ISO 13849-1, 6.2.5.

Figure 38 - Architecture désignée pour la catégorie 2 (EN ISO 13849-1)



I : équipement d'entrée (input)

m : surveillance (monitoring)

L : logique

TE : équipement d'essai

O : équipement de sortie (output)

OTE : sortie de TE

^{i}**m** : moyens d'interconnexion

Pour la catégorie de câblage 2, le SRP/CS, partie du système de commande relative à la sécurité, doit être conçu de sorte que sa ou ses fonctions soient contrôlées à intervalles appropriés par le système de commande de la machine.

Dans une architecture monocanal, un module SIM est associé à un démarreur SIL[59].

En particulier, pour la catégorie de câblage 2, le contact miroir est connecté au module Preventa™ XPS (ou équivalent). Si l'état de la ligne de retour contacteur miroir ne correspond pas à l'état de sortie du module Preventa XPS (ou équivalent), le module Preventa XPS (ou équivalent) bloque tout second démarrage.

NOTE: Le retour contacteur miroir ne transmet que des informations de diagnostic.

59. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.

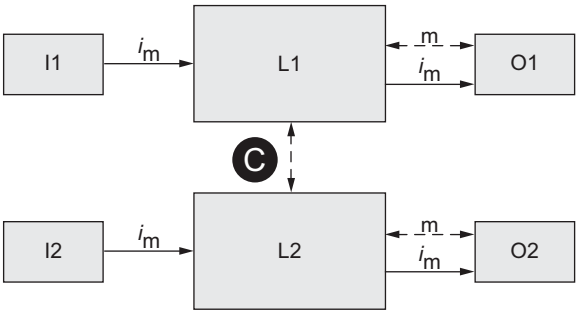
Annexe : Architecture bicanal

Cette architecture bicanal englobe les catégories de câblage 3 et 4.

Exigences architecturales pour la catégorie de câblage 3

L'architecture désignée pour la catégorie 3 est définie dans la norme EN ISO 13849-1, 6.2.6.

Figure 39 - Architecture désignée pour la catégorie 3 (EN ISO 13849-1)



im : moyens d'interconnexion

L1, L2 : logique

c : surveillance croisée

m : surveillance (monitoring)

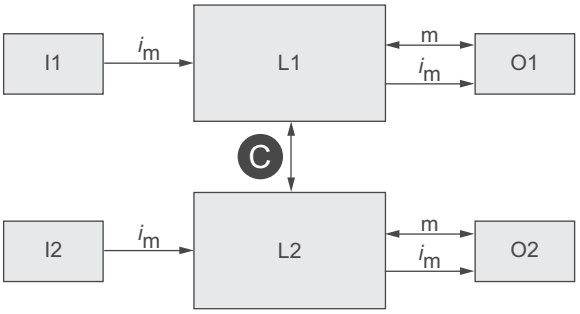
I1, I2 : dispositif d'entrée, par exemple un capteur

O1, O2 : dispositif de sortie, par exemple le contacteur principal

Exigences architecturales pour la catégorie de câblage 4

L'architecture désignée pour la catégorie 4 est définie dans la norme EN ISO 13849-1, 6.2.7.

Figure 40 - Architecture désignée pour la catégorie 4 (EN ISO 13849-1)



im : moyens d'interconnexion

L1, L2 : logique

c : surveillance croisée

m : surveillance (monitoring)

I1, I2 : dispositif d'entrée, par exemple un capteur

O1, O2 : dispositif de sortie, par exemple le contacteur principal

Les lignes pleines pour la surveillance représentent une couverture de diagnostic plus élevée que dans l'architecture désignée pour la catégorie 3.

Glossaire

A

Fréquence moyenne de défaillance dangereuse [h⁻¹] (PFH). (Défaillance dangereuse au sens de la norme CEI 61508-4)

Afin de maintenir la fonction de sécurité, la norme CEI 61508 exige différents niveaux de mesures pour éviter et contrôler les erreurs détectées, en fonction du niveau SIL[60] requis.

Tous les composants d'une fonction de sécurité doivent faire l'objet d'une évaluation de probabilité visant à évaluer l'efficacité des mesures mises en œuvre pour contrôler les défauts détectés.

Cette évaluation a déterminé la valeur PFH (fréquence moyenne de défaillance dangereuse[61] [h^{-1}]) pour un système relatif à la sécurité. Il s'agit de la probabilité par heure qu'un système relatif à la sécurité tombe en panne de manière dangereuse et que la fonction de sécurité ne puisse être exécutée correctement.

Selon le niveau SIL, la PFH ne doit pas dépasser certaines valeurs pour l'ensemble du système relatif à la sécurité.

Les valeurs PFH individuelles d'une chaîne fonctionnelle sont additionnées. Le résultat ne doit pas dépasser la valeur maximale spécifiée dans la norme.

Niveau d'intégrité de sécurité	Fréquence moyenne de défaillance dangereuse[61] [h^{-1}] (PFH) en cas de sollicitation élevée ou de sollicitation continue.
4	$10^{-9} \leq \ldots < 10^{-8}$
3	$10^{-8} \leq \ldots < 10^{-7}$
2	$10^{-7} \leq \ldots < 10^{-6}$
1	$10^{-6} \leq \ldots < 10^{-5}$

E

Norme EN ISO 13849

Cette norme européenne spécifie la procédure de validation, y compris l'analyse des dangers, l'évaluation des risques et les essais, pour les fonctions de sécurité et les catégories des parties des systèmes de commande relatifs à la sécurité. La description des fonctions de sécurité et des exigences pour les catégories est donnée dans la norme ISO 13849-1, qui couvre les principes généraux de conception. Certaines exigences en matière de validation sont générales, d'autres sont propres à la technologie utilisée. La norme EN ISO 13849-2 spécifie également les conditions dans lesquelles la validation par essais des parties des systèmes de commande relatifs à la sécurité doit être effectuée.

Norme EN/CEI 60204-1

La catégorie d'arrêt 0 est définie comme une fonction d'« arrêt par coupure immédiate de l'alimentation des actionneurs de la machine (c'est-à-dire arrêt non contrôlé) ».

60. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.
61. Défaillance dangereuse au sens de la norme CEI 61508-4

La catégorie d'arrêt 1 est définie comme « arrêt contrôlé avec maintien de l'alimentation des actionneurs de la machine pour atteindre l'arrêt, puis coupure de l'alimentation une fois l'arrêt atteint ».

F

Mesures d'évitement des défauts

Les erreurs systématiques dans les spécifications, dans le matériel et le logiciel, ainsi que les défauts d'utilisation et de maintenance du système relatif à la sécurité doivent être évités dans toute la mesure du possible. Pour répondre à ces exigences, la norme CEI 61508 spécifie un certain nombre de mesures d'évitement des défauts qui doivent être implémentées en fonction du niveau SIL[62] requis. Ces mesures d'évitement des défauts doivent couvrir l'ensemble du cycle de vie du système relatif à la sécurité, c'est-à-dire de la conception du système à sa mise hors service.

Sécurité fonctionnelle

L'automatisme et l'ingénierie de la sécurité fonctionnelle sont deux domaines qui demeuraient complètement séparés auparavant, mais qui tendent à s'intégrer de plus en plus.

Les fonctions de sécurité intégrées simplifient l'ingénierie et l'installation des solutions d'automatisme complexes.

En règle générale, les exigences en matière de sécurité fonctionnelle dépendent de l'application.

Le niveau d'exigence résulte du risque et du potentiel de danger découlant de l'application spécifique.

H

Tolérance aux défaillances de matériel (HFT) et proportion de défaillances en sécurité (SFF)

En fonction du SIL[62] du système relatif à la sécurité, la norme CEI 61508 exige une tolérance aux défauts de matériel (HFT, pour Hardware Fault Tolerance) spécifique en relation avec une certaine proportion de défaillances en sécurité (SFF, pour Safe Failure Fraction).

La HFT est la capacité d'un système à exécuter la fonction de sécurité requise malgré la présence d'un ou de plusieurs défauts matériels.

La SFF d'un système est définie comme le rapport entre le taux de défaillances « en sécurité » et le taux de défaillance total du système.

Selon la norme CEI 61508, le SIL maximal qu'un système est susceptible d'obtenir est en partie déterminé par la HFT et la SFF de ce système.

Ces types sont spécifiés sur la base des critères définis dans la norme pour les éléments relatifs à la sécurité.

SFF	**Sous-système HFT Type A**			**Sous-système HFT Type B**		
	0	1	2	0	1	2
≤ 60 %	SIL 1	SIL 2	SIL 3	—	SIL 1	SIL 2
60 % – < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3

62. Safety Integrity Level (niveau d'intégrité) selon la norme CEI 61508.

SFF	Sous-système HFT Type A			Sous-système HFT Type B		
90 %…< 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

I

Norme CEI 61508

La norme CEI 61508 couvre la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité.

Au lieu d'un seul composant, une chaîne fonctionnelle complète (par exemple, d'un capteur à l'actionneur en passant par les unités de traitement logique) est considérée comme une unité.

Cette chaîne fonctionnelle doit satisfaire aux exigences du niveau d'intégrité de sécurité spécifique dans son ensemble.

L

Mode à faible/forte sollicitation

La norme CEI 61508 définit le mode de fonctionnement de la fonction de sécurité selon la sollicitation :

- Mode à forte sollicitation ou sollicitation continue (PFH)
- Mode à faible sollicitation (PFDavg, PTI)

M

Temps moyen avant défaillance dangereuse ($MTTF_d$)

La norme ISO 13849-1 définit le $MTTF_d$ comme le temps moyen prévu avant défaillance dangereuse.

P

Niveau de performance (PL)

La norme CEI 13849-1 définit cinq niveaux de performance (PL) pour les fonctions de sécurité.

Le niveau a est le niveau le plus bas, le niveau e le plus haut.

Cinq niveaux (a, b, c, d et e) correspondent à différentes valeurs de probabilité moyenne de défaillance dangereuse[63] par heure.

Niveau de performance	Probabilité de défaillance dangereuse[63] par heure
e	≥ 10^{-8} à < 10^{-7}
d	≥ 10^{-7} à < 10^{-6}
c	≥ 10^{-6} à < 3×10^{-6}

63. Défaillance dangereuse au sens de la norme CEI 61508-4

Niveau de performance	Probabilité de défaillance dangereuse[64] par heure
b	≥ 3 × 10^{-6} à < 10^{-5}
a	≥ 10^{-5} à < 10^{-4}

S

Niveau d’intégrité de sécurité (SIL)

La norme CEI 61508 définit quatre niveaux d’intégrité de sécurité (SIL) pour les fonctions de sécurité.

SIL 1 est le niveau d’intégrité le plus bas et SIL 4 le plus élevé.

Le niveau d’intégrité de sécurité requis est déterminé sur la base d’une analyse des dangers et d’une évaluation des risques.

Le résultat permet de décider si la chaîne fonctionnelle en question doit être considérée comme une fonction de sécurité et quel potentiel de danger elle doit couvrir.

64. Défaillance dangereuse au sens de la norme CEI 61508-4

Schneider Electric
5985 McLaughlin Road
01810 Andover, MA
États-Unis

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

www.schneider-electric.com

Les normes, spécifications et conceptions pouvant changer de temps à autre, veuillez demander la confirmation des informations figurant dans cette publication.

8536IB1904FR-04