

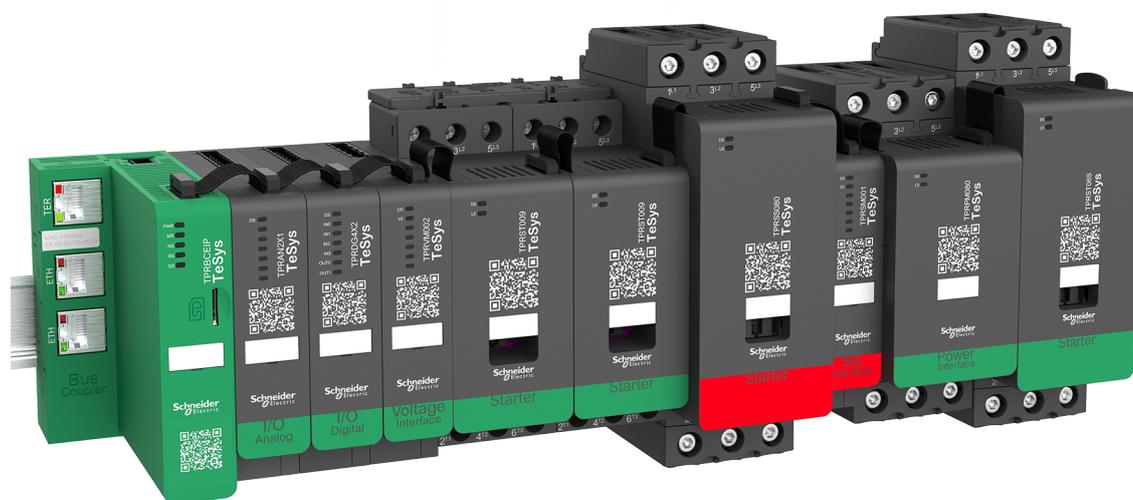
TeSys Active

TeSys™ island – цифровая система управления двигателем

Руководство по функциональной безопасности

TeSys предлагает комплексные инновационные решения для пускателей двигателей.

85361B1904RU-03
09/2021



Правовая информация

Торговая марка Schneider Electric и любые товарные знаки Schneider Electric SE и ее дочерних компаний, упоминаемые в данном руководстве, являются собственностью компании Schneider Electric SE или ее дочерних компаний. Все остальные торговые марки могут быть товарными знаками соответствующих владельцев. Данное руководство и его содержимое защищены действующим законодательством об авторском праве и предоставляются только для информационных целей. Запрещается воспроизводить или передавать любую часть данного руководства в любой форме или любыми средствами (включая электронные, механические, фотокопирование, запись или иные) для любых целей без предварительного письменного разрешения компании Schneider Electric.

Компания Schneider Electric не предоставляет никаких прав или лицензий на коммерческое использование руководства или его содержимого, за исключением неисключительной и персональной лицензии на консультирование по нему на условиях "как есть".

Установка, эксплуатация, сервисное и техническое обслуживание оборудования Schneider Electric должны осуществляться только квалифицированным персоналом.

Поскольку стандарты, спецификации и конструкции периодически изменяются, информация в данном руководстве может быть изменена без предварительного уведомления.

В той степени, в которой это разрешено применимым законодательством, компания Schneider Electric и ее дочерние компании не несут ответственности за любые ошибки или упущения в информационных материалах или последствия, возникшие в результате использования содержащейся в настоящем документе информации.

Schneider Electric, Preventa и TeSys являются товарными знаками и собственностью компании Schneider Electric SE, ее филиалов и аффилированных компаний. Все другие товарные знаки являются собственностью их владельцев.

Содержание

Информация по технике безопасности.....	5
Об издании	6
Область применения документа	6
Примечание по области действия	6
Сопутствующая документация.....	6
Терминология, заимствованная из стандартов.....	8
Терминология, связанная с функциональной безопасностью.....	9
Декларация о соответствии нормам ЕС	10
Меры предосторожности.....	11
Аттестованный персонал	12
Назначение устройства.....	12
Краткое описание средств функциональной безопасности	
TeSys™ island.....	13
Содержание: TeSys	13
Концепция TeSys island	13
Средства функциональной безопасности TeSys island	14
Характеристики функциональной безопасности TeSys island	15
Стандарты и сертифицированные характеристики	15
Условия эксплуатации	16
Одноканальная архитектура (ISO 13849)	16
Двухканальная архитектура (ISO 13849)	16
Категории останова (EN/МЭК 60204–1)	17
Категории электроснабжения ¹	17
Категория электроснабжения 1	17
Категория электроснабжения 2	17
Категория электроснабжения 3	18
Категория электроснабжения 4	19
Проверка соответствия техническим условиям	19
Концепции и компоненты	20
Типовая структура TeSys™ island.....	20
Группа SIL.....	21
Аватары SIL	21
Интерфейсный модуль SIL.....	22
Состояние контактов пускателей SIL	22
Связанный с безопасностью сенсорный элемент	24
Пускатели SIL	25
Внешний связанный с безопасностью элемент	26
Конфигурация: останов SIL, категория останова 0, категория электроснабжения 1	27
Конфигурация: останов SIL, категория останова 0, категория электроснабжения 2	27
Конфигурация: останов SIL, категория останова 1, категория электроснабжения 2	31
Конфигурация: останов SIL, категория останова 0, категория электроснабжения 3/4	34
Конфигурация: останов SIL, категория останова 1, категория электроснабжения 3/4	36

Защитная изоляция кабелей	39
Архитектура для низкой и высокой частоты переключения	40
Низкая частота переключения (< 15 циклов в час)	41
Высокая частота переключения (\geq 15 циклов в час)	42
Примеры архитектуры	44
Останов SIL, категория останова 0, категория электроснабжения 1	45
Останов SIL, категория останова 0, категория электроснабжения 2	46
Останов SIL, категория останова 1, категория электроснабжения 2	48
Останов SIL, категория останова 0, категория электроснабжения 3/ 4	50
Останов SIL, категория останова 1, категория электроснабжения 3/ 4	52
Технические характеристики	54
Интерфейсный модуль SIL	54
Пускатель SIL	54
Данные о надежности	56
Схемы электропроводки аватаров SIL	57
Ввод функции безопасности в эксплуатацию	64
Тестирование монтажа	64
Проверочное испытание функции безопасности	64
Требования к техническому обслуживанию функции безопасности	66
График технического обслуживания	66
Проверки в рамках технического обслуживания	66
Проверки использования устройств	66
Проверочное испытание функции безопасности	66
Приложение. Одноканальная архитектура	67
Архитектурные требования для категории электроснабжения 1	67
Архитектурные требования для категории электроснабжения 2	68
Приложение: Двухканальная архитектура	69
Архитектурные требования для категории электроснабжения 3	69
Архитектурные требования для категории электроснабжения 4	70
Глоссарий	71

Информация по технике безопасности

Важная информация

Внимательно прочтите эти инструкции и изучите оборудование перед его установкой, эксплуатацией и обслуживанием. Следующие специальные сообщения могут появляться в технической документации или на оборудовании, чтобы предупредить о возможной опасности или привлечь ваше внимание к информации, которая разъясняет или упрощает процедуру.



Добавление любого символа к предупреждающей табличке “Опасность” или “Предупреждение” предупреждает о риске поражения электрическим током, что может стать причиной несчастного случая при невыполнении данных инструкций.



Этот символ используется для обозначения опасности. Он используется для предупреждения об опасности травм персонала. Чтобы избежать возможных травм или смертельного исхода, следуйте всем инструкциям, содержащимся в сообщениях о безопасности.

ОПАСНОСТЬ

ОПАСНОСТЬ обозначает опасную ситуацию, которая, если ее не избежать, **приведет к смерти или тяжелому увечью**.

ПРЕДУПРЕЖДЕНИЕ

ПРЕДУПРЕЖДЕНИЕ обозначает опасную ситуацию, которая, если ее не избежать, **может привести к смерти или тяжелому увечью**.

ВНИМАНИЕ

ВНИМАНИЕ обозначает опасную ситуацию, которая, если ее не избежать, **может привести к незначительной травме или травме средней тяжести**.

УВЕДОМЛЕНИЕ

УВЕДОМЛЕНИЕ указывает на ситуации, не связанные с опасностью получения травм.

Обратите внимание

К монтажу, эксплуатации и обслуживанию электрического оборудования должен допускаться только квалифицированный персонал. Компания Schneider Electric не несет ответственности за любые последствия, вытекающие из использования этого материала.

Квалифицированный специалист — это человек, обладающий навыками и знаниями в области проектирования, эксплуатации и установки электрооборудования и прошедший обучение технике безопасности, позволяющей распознавать связанные с изделием опасные ситуации и избегать их.

Об издании

Область применения документа

Настоящий документ служит источником следующей дополнительной информации о средствах функциональной безопасности TeSys™ island:

- общие сведения;
- основные принимаемые во внимание аспекты;
- характеристики;
- описание аппаратных средств;
- типовые варианты конфигурации;
- примеры архитектуры;
- ссылки на стандарты.

Примечание по области действия

Данное руководство касается любых конфигураций TeSys island. Доступность некоторых функций, описанных в данном руководстве, зависит от используемого протокола связи и физических модулей, установленных в системе.

Информация о соответствии изделий экологическим директивам, таким как RoHS, REACH, PEP и EOL, представлена по адресу www.se.com/green-premium.

Технические характеристики физических модулей, описанных в этом руководстве, приведены на сайте www.se.com.

Технические характеристики в данном руководстве должны совпадать с представленными в Интернете. В дальнейшем возможны изменения содержания для повышения ясности и точности. Если информация в данном руководстве и информация в Интернете различаются, используйте информацию из Интернета.

Сопутствующая документация

Название документа	Описание	Номер документа
TeSys island – системное руководство	Представляет и описывает основные функции TeSys island	8536IB1901RU
TeSys island — Руководство по установке	Описывает механический монтаж, подключение и ввод в эксплуатацию системы TeSys island	8536IB1902RU
TeSys island — Руководство по эксплуатации	Описывает работу и техническое обслуживание TeSys island	8536IB1903RU
TeSys island — Руководство по функциональной безопасности	Описывает характеристики функциональной безопасности TeSys island	8536IB1904RU
TeSys island — Руководство по функциональным блокам от сторонних производителей	Содержит информацию, необходимую для создания функциональных блоков оборудования сторонних производителей	8536IB1905RU
TeSys island — Руководство по библиотеке функциональных блоков EtherNet/IP™	Описывает библиотеку TeSys island, используемую в среде Rockwell Software® Studio 5000® EtherNet/IP	8536IB1914RU
TeSys island — Краткое руководство по EtherNet/IP™	Описывает, как быстро интегрировать TeSys island в среду Rockwell Software Studio 5000 EtherNet/IP	8536IB1906RU
TeSys island — Сетевое справочное руководство DTM	Описывает установку и использование различных функций программного обеспечения для	8536IB1907

Название документа	Описание	Номер документа
	конфигурирования TeSys island и настройку параметров TeSys island.	
TeSys island — Руководство по библиотеке функциональных блоков PROFINET и PROFIBUS	Описывает библиотеку TeSys island, используемую в среде Siemens™ TIA Portal	8536IB1917RU
TeSys island — Краткое руководство пользователя для приложений PROFINET и PROFIBUS	Описывает, как быстро интегрировать TeSys island в среду Siemens™ TIA Portal.	8536IB1916RU
TeSys island — Экологический профиль	Описывает материалы изделия и возможности его вторичной переработки, а также содержит информацию о воздействии TeSys island на окружающую среду	ENVPEP1904009
TeSys island — Инструкция по обращению после окончания срока эксплуатации	Содержит указания по действиям после окончания срока службы системы TeSys island	ENVEOL1904009
TeSys island — Инструкция, модуль удаленного подключения, TPRBCEIP	Описывает установку модуля удаленного подключения Ethernet/IP системы TeSys island.	MFR44097
TeSys island — Инструкция, модуль удаленного подключения, TPRBCPFN	Описывает установку модуля удаленного подключения PROFINET системы TeSys island.	MFR44098
TeSys island — Инструкция, модуль удаленного подключения, TPRBCPFB	Описывает установку модуля удаленного подключения PROFIBUS DP системы TeSys island.	GDE55148
TeSys island — Инструкция, пускатели и интерфейсные модули питания, размеры 1 и 2	Описывает установку пускателей и интерфейсных модулей питания TeSys island размеров 1 и 2.	MFR77070
TeSys island — Инструкция, пускатели и интерфейсные модули питания, размер 3	Описывает установку пускателей и интерфейсных модулей питания TeSys island размера 3.	MFR77085
TeSys island — Инструкция: Модули входов/ выходов	Описывает установку аналоговых и цифровых модулей ввода-вывода TeSys island.	MFR44099
TeSys island — Инструкция: Интерфейсные модули SIL (Уровень полноты безопасности) и напряжения	Описывает установку интерфейсных модулей напряжения TeSys island и SIL ¹	MFR44100

1. Уровень полноты безопасности согласно стандарту МЭК 61508.

Терминология, заимствованная из стандартов

В качестве технических и иных терминов и соответствующих описаний в настоящем руководстве, как правило, используются термины и определения, приведенные в соответствующих стандартах. В том числе следующих:

- **EN ISO 13849-1:** «Безопасность машин. Связанные с безопасностью элементы систем контроля. Часть 1. Общие принципы проектирования»
- **EN ISO 13849-2:** «Безопасность машин. Связанные с безопасностью элементы систем контроля. Часть 2. Проверка»
- **МЭК 61508** «Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью»
- **EN 62061:** «Безопасность машин. Функциональная безопасность связанных с безопасностью электрических, электронных и программируемых электронных систем управления и контроля»
- **МЭК 61511** «Функциональная безопасность. Инструментальные системы безопасности для сектора перерабатывающей промышленности»
- **EN/МЭК 60204-1:** «Безопасность машин. Электрическое оборудование машин. Часть 1. Общие требования»
- **МЭК 61000-6-7** «Электромагнитная совместимость (ЭМС). Часть 6-7. Общие стандарты. Требования к помехоустойчивости оборудования, предназначенного для выполнения каких-либо функций в связанных с безопасностью системах (функциональная безопасность) в промышленных средах»
- **МЭК 60664-5** «Изоляционные расстояния для оборудования низковольтных систем. Часть 5. Комплексный метод определения зазоров и путей утечки, равных или менее 2 мм»
- **МЭК 60947-4-1** «Аппаратура распределения и управления низковольтная. Часть 4-1. Контактторы и пускатели. Электромеханические контактторы и пускатели»
- **МЭК 60947-5-1** «Аппаратура распределения и управления низковольтная. Часть 5-1. Аппараты и коммутационные элементы цепей управления. Электромеханические аппараты для цепей управления»
- **МЭК 60947-7-1** «Аппаратура распределения и управления низковольтная. Часть 7-1. Электрооборудование вспомогательное. Клеммные колодки для медных проводников»
- **МЭК 60947-7-2** «Аппаратура распределения и управления низковольтная. Часть 7-2. Электрооборудование вспомогательное. Клеммные колодки защитных проводников для присоединения медных проводников»
- **EN 50205:** Реле с принудительными контактами (механически связанные)
- **IEC TR 62380** «Справочник данных по надежности. Универсальная модель для прогнозирования надежности электронных компонентов, печатных плат и оборудования»

Терминология, связанная с функциональной безопасностью

ATTENTION

Определения терминов, связанных с функциональной безопасностью, которые используются в этом руководстве, приведены ниже.

Термин	Стандарт	Определение
Отказоустойчивость	МЭК 61511-1	Способность функционального элемента продолжать выполнять требуемую функцию при наличии сбоев или ошибок.
Функциональная безопасность	МЭК 61508-4	Часть общей безопасности, обусловленная применением управляемого оборудования (EUC) и системы управления EUC и зависящая от правильности функционирования электрических/электронных/программируемых электронных (E/E/PE) систем, связанных с безопасностью, и других средств по снижению риска.
Безопасный отказ	МЭК 61508-4	Отказ элемента и/или подсистемы и/или системы, играющей роль в реализации функции безопасности, который: <ol style="list-style-type: none"> 1. приводит к ложной работе функции безопасности по переводу управляемого оборудования (EUC)² (или его части) в безопасное состояние; или 2. повышает вероятность ложной работы функции безопасности по переводу управляемого оборудования (EUC)² (или его части) в безопасное состояние.
Доля безопасных отказов	МЭК 61508-4	Отношение частоты безопасных отказов к суммарной частоте отказов системы.
Безопасное состояние	МЭК 61511-1	Состояние процесса, в котором достигается безопасность.
	МЭК 61800-5-2	Состояние PDS(SR) ³ при достижении состояния безопасности
Безопасный останов	МЭК 61800-5-2	Функции безопасного останова Safe Stop определяются следующим образом: <ul style="list-style-type: none"> • Безопасное отключение крутящего момента (STO) <ul style="list-style-type: none"> ◦ Эта функция предотвращает подачу на двигатель энергии, создающей усилие. ◦ Эта <i>подфункция безопасности</i> выполняет неконтролируемый останов и соответствует категории останова 0 по МЭК 60204-1. • Безопасный останов 1 (SS1) <ul style="list-style-type: none"> ◦ Безопасный останов 1 — управляемое торможение: SS1-d — запускает и осуществляет управление интенсивностью торможения двигателя в рамках установленных пределов, чтобы остановить двигатель, и запускает функцию STO (см. 4.2.3.2), когда частота вращения двигателя окажется ниже заданного предела; или ◦ Безопасный останов 1 — мониторинг линейного изменения оборотов: SS1-r — запускает и контролирует интенсивность торможения двигателя в рамках установленных пределов, чтобы остановить двигатель, и запускает функцию STO, когда частота вращения двигателя окажется ниже заданного предела; или ◦ Безопасный останов 1 — управление временем: SS1-t — запускает торможение двигателя и запускает функцию STO после определенной временной задержки.

2. EUC: Equipment under control – управляемое оборудование

3. Связанные с безопасностью системы электрического привода

Термин	Стандарт	Определение
Функция безопасности	МЭК 61800-5-2	Функция, реализованная связанной с безопасностью системой или другими средствами снижения риска, которая предназначена для достижения или поддержания состояния безопасности оборудования или механизмов, управляемых системой PDS(SR) ⁴ , в отношении конкретного опасного события
Уровень полноты безопасности (SIL)	МЭК 61508	Стандарт МЭК 61508 определяет четыре уровня полноты безопасности (SIL) для функций безопасности: SIL 1 — самый низкий уровень полноты безопасности, а SIL 4 — самый высокий. Анализ опасностей и оценка рисков служат основой для определения требуемого уровня полноты безопасности.
Система, связанная с безопасностью	МЭК 61800-5-2	Специализированная система, которая <ul style="list-style-type: none"> • реализует необходимые функции безопасности, требующиеся для достижения или поддержки безопасного состояния оборудования или механизмов, управляемых системой PDS(SR)⁵; и • предназначена для достижения своими средствами или в сочетании с другими средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности.
Подсистема	МЭК 61800-5-2	Часть проекта архитектуры верхнего уровня связанной с безопасностью системы, отказ которой приводит к отказу функции безопасности.

Декларация о соответствии нормам ЕС

Декларации о соответствии TeSys™ island нормам ЕС можно найти на веб-сайте www.schneider-electric.com.

4. Связанные с безопасностью системы электрического привода
5. Связанные с безопасностью системы электрического привода

Меры предосторожности

Необходимо прочитать и усвоить следующие меры предосторожности перед выполнением любых процедур, описанных в данном руководстве.

ОПАСНО

ОПАСНОСТЬ ПОРАЖЕНИЯ ЭЛЕКТРИЧЕСКИМ ТОКОМ, ВЗРЫВОМ ИЛИ ВСПЫШКОЙ ДУГИ

- Электрическое оборудование должно устанавливаться и обслуживаться только квалифицированным персоналом.
- Выключите подачу питания к данному оборудованию перед работой на оборудовании или внутри него.
- При эксплуатации данного оборудования и любых связанных с ним устройств используйте только указанное напряжение.
- Всегда используйте подходящий датчик номинального напряжения, чтобы убедиться, что питание отключено.
- Используйте соответствующие блокировки там, где существует опасность для персонала и/или оборудования.
- Цепи электропитания должны быть подключены и защищены в соответствии с местными и государственными нормативными требованиями.
- Используйте соответствующие средства индивидуальной защиты (СИЗ) и соблюдайте меры безопасности при работе с электрическим оборудованием в соответствии с NFPA 70E, NOM-029-STPS, CSA Z462 или аналогичными местными стандартами.

Несоблюдение данных инструкций приводит к смерти или серьезной травме.

ОСТОРОЖНО

НЕПРЕДНАМЕРЕННОЕ ВКЛЮЧЕНИЕ ОБОРУДОВАНИЯ

- Полный текст инструкций по функциональной безопасности см. в Руководстве по функциональной безопасности TeSys™ island, 8536IB1904.
- Запрещается разбирать, ремонтировать или вносить изменения в конструкцию данного оборудования. Данное оборудование не содержит компонентов, подлежащих обслуживанию со стороны пользователя.
- Установка и эксплуатация данного оборудования производится в шкафу, предназначенном для предусмотренных условий применения данного оборудования.
- Перед вводом в эксплуатацию каждого экземпляра данного оборудования его работоспособность должна быть тщательно индивидуально проверена.

Несоблюдение данных инструкций может привести к смерти, серьезной травме или повреждению оборудования.



ПРЕДУПРЕЖДЕНИЕ: Данное устройство может подвергнуть вас воздействию химических веществ, в том числе окиси сурьмы (трехокиси сурьмы), которая, по информации штата Калифорния, вызывает рак. Для получения дополнительной информации см. www.P65Warnings.ca.gov.

Аттестованный персонал

Только соответствующим образом обученные лица, ознакомившиеся с данным руководством и остальной документацией, связанной с изделием, и понимающие их содержание, имеют право работать с данным изделием.

Квалифицированный специалист должен уметь обнаруживать возможные опасности, которые могут возникнуть в результате изменения значений параметров и, в целом, от механического, электрического или электронного оборудования. Квалифицированный специалист должен быть знаком со стандартами, положениями и правилами предотвращения несчастных случаев на производстве, которые он должен соблюдать при разработке и реализации системы.

Использование и применение информации, содержащейся в данном руководстве, требует опыта в разработке и программировании автоматизированных систем управления. Только вы, пользователь, производитель оборудования или интегратор, можете знать обо всех условиях и факторах, присутствующих во время монтажа, настройки, эксплуатации и технического обслуживания оборудования или процесса, и, следовательно, можете определять средства автоматизации и связанное с изделием оборудование, а также сопутствующие меры безопасности и блокировки, которые можно эффективно и правильно использовать.

При выборе оборудования для автоматизации и управления (и любого другого соответствующего оборудования или программного обеспечения) для конкретного применения необходимо также учитывать применимые местные, региональные или национальные стандарты и/или нормативы.

При использовании данного оборудования обратите особое внимание на соблюдение любых указаний по технике безопасности, электрических требований и нормативных стандартов, касающихся вашего оборудования или процесса.

Назначение устройства

Изделия, описанные в данном руководстве наряду с программным обеспечением, принадлежностями и дополнительным оборудованием, служат пускателями для низковольтных электрических нагрузок и предназначены для промышленного использования в соответствии с инструкциями, указаниями, примерами и информацией по безопасности, содержащимися в этом документе и другой сопроводительной документацией.

Изделие может использоваться только в соответствии со всеми применимыми правилами безопасности и директивами, приведенными требованиями и техническими данными.

Перед использованием изделия необходимо выполнить анализ опасностей и оценку рисков планируемого применения. На основании полученных результатов должны быть приняты соответствующие меры безопасности.

Поскольку изделие используется в качестве компонента оборудования или процесса, необходимо обеспечить безопасность людей за счет построения системы в целом.

Эксплуатируйте изделие только с указанными кабелями и принадлежностями. Используйте только оригинальные принадлежности и запасные части.

Любое использование, кроме явно разрешенного, запрещено и может привести к непредвиденным опасностям.

Краткое описание средств функциональной безопасности TeSys™ island

Содержание: TeSys

TeSys™ – это инновационное решение для контроля и управления двигателем от лидера мирового рынка. TeSys комплексные эффективные продукты и решения для коммутации и защиты двигателей и электрических нагрузок в соответствии со всеми основными мировыми электрическими стандартами.

Концепция TeSys island

TeSys island — это модульная многофункциональная система, обеспечивающая интегрированные функции в рамках архитектуры автоматизации, прежде всего для прямого контроля и управления низковольтными нагрузками. TeSys island может переключать, помогать защищать и управлять двигателями и другими электрическими нагрузками до 80 А (AC1), установленными в электрической панели управления.

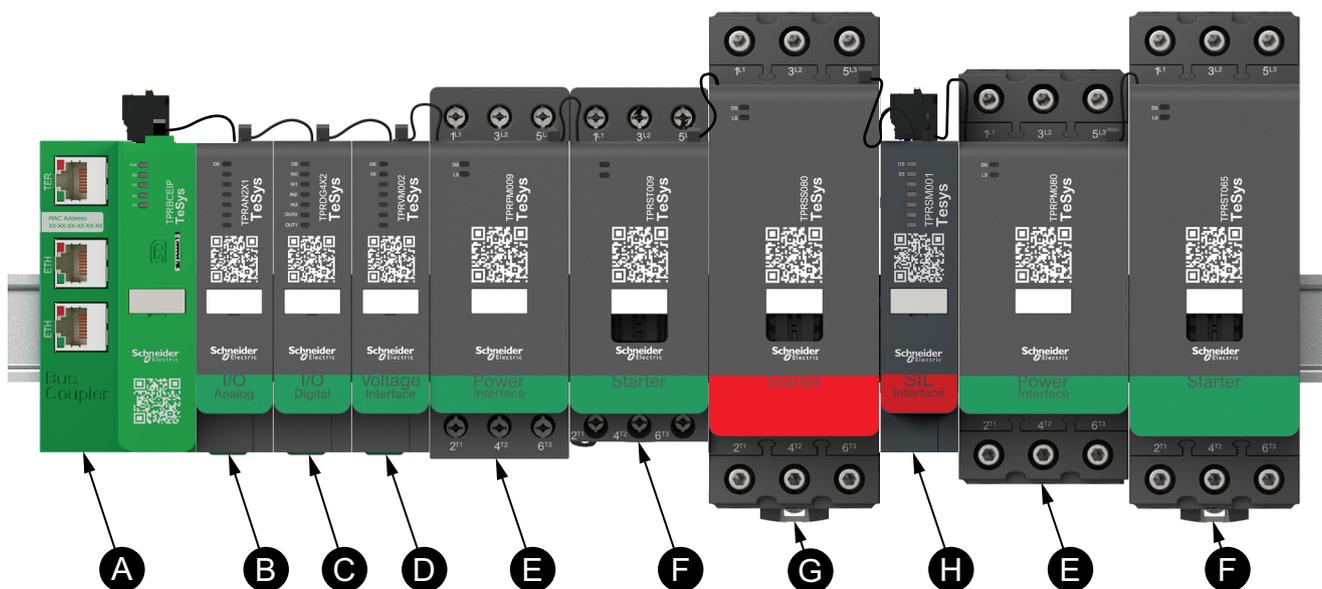
Эта система разработана на основе концепции аватаров TeSys. Эти аватары:

- Представляют логические и физические аспекты функций автоматизации
- Определяют конфигурацию системы

Логические аспекты системы управляются программными средствами, охватывающими все фазы жизненного цикла продукта и приложения: проектирование, проектирование, ввод в эксплуатацию, эксплуатацию и техническое обслуживание.

Физическая система состоит из набора устройств, установленных на одной DIN-рейке и соединенных плоскими кабелями, обеспечивающими внутреннюю связь между модулями. Внешняя связь со средой автоматизации осуществляется через один модуль удаленного подключения, и система рассматривается как единый узел в сети. Также используются другие модули: пускатели, модули силового интерфейса, модули аналоговых и цифровых входов-выходов, интерфейсные модули напряжения и интерфейсные модули SIL («Уровень полноты безопасности» согласно стандарту IEC 61508), охватывающие широкий спектр рабочих функций.

рисунок 1 - Обзор TeSys island



A	Модуль удаленного подключения	E	Интерфейсный модуль питания
B	Аналоговый модуль ввода-вывода	F	Стандартный пускатель
C	Цифровой модуль ввода-вывода	G	Пускатель SIL
D	Интерфейсный модуль напряжения	H	Интерфейсный модуль SIL

Средства функциональной безопасности TeSys island

Система TeSys™ island включает определенные аватары и физические устройства для построения конфигураций, реализующие функции категории останова 0 и категории останова 1 согласно EN/МЭК 60204-1. Аватары системы TeSys — это цифровые представления физических модулей системы, однако функции безопасности TeSys island обеспечиваются исключительно электромеханическими аппаратными компонентами. Определенными устройствами является пускатель и интерфейсный модуль SIL⁶. Еще одной важной концепцией является группа SIL: совокупность аватаров, которые связаны с одним интерфейсным модулем SIL и действуют в соответствии с одной и той же функцией безопасности. В одну систему может входить несколько групп SIL.

Для обеспечения функциональной безопасности машины или системы (процесса) система TeSys island должна быть интегрирована с другими связанными с безопасностью элементами в более масштабную связанную с безопасностью систему.

6. Уровень полноты безопасности согласно стандарту МЭК 61508.

Характеристики функциональной безопасности TeSys island

Система TeSys™ island обеспечивает возможности функциональной безопасности в соответствии со следующими условиями:

- Стандарты и сертифицированные характеристики, стр. 15
- Условия эксплуатации, стр. 16
- Одноканальная архитектура (ISO 13849), стр. 16
- Двухканальная архитектура (ISO 13849), стр. 16
- Категории останова (EN/МЭК 60204–1), стр. 17
- Категории электроснабжения (ISO 13849), стр. 17
- Проверка соответствия техническим условиям, стр. 19

Стандарты и сертифицированные характеристики

TeSys island соответствует следующим директивам и стандартам:

- Директива по машинам, механизмам и машинному оборудованию 2006/42/CE:
 - EN ISO 13849-1: 2015
 - EN 62061: 2016 или МЭК 62061: 2015 (ред. 1.2)
- Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью: МЭК 61508, ред. 2: 2010
- Функциональная безопасность. Инструментальные системы безопасности для сектора перерабатывающей промышленности: МЭК 61511, ред. 2: 2016
- Функции категории останова 0 и категории останова 1 системы TeSys island соответствуют требованиям EN/МЭК 60204-1.

При одном канале наивысшим уровнем эффективности этих функций являются:

- Уровень эффективности «d» категории 2 согласно EN ISO 13849-1
- SIL⁷ Соответствие уровню 2 согласно МЭК 61508, ред. 2, и МЭК 61511, ред. 2
- Соответствие уровню SIL CL 2 согласно EN 62061, ред. 1

При двух каналах наивысшим уровнем эффективности этих функций являются:

- Уровень эффективности «e» категории 4 согласно EN ISO 13849-1
- Соответствие уровню SIL 3 согласно МЭК 61508, ред. 2, и МЭК 61511, ред. 2
- Соответствие уровню SIL CL 3 согласно EN 62061: 2016 или МЭК 62061: 2015 (ред. 1.2)

Система TeSys island, в зависимости от архитектуры электроснабжения, рассчитана на поддержку различных уровней эффективности функциональной безопасности и полноты безопасности и соответствует характеристикам функциональной безопасности, описанным в следующей таблице.

Таблица 1 - Характеристики функциональной безопасности

Функция	Связанная с безопасностью функция останова
Положение при отключении	Разомкнутый контактор
Время срабатывания, в худшем случае	145 мс

7. Уровень полноты безопасности согласно стандарту МЭК 61508.

**Таблица 1 - Характеристики функциональной безопасности
(продолжение)**

Категория останова EN/МЭК 60204–1	Кат. 0/Кат. 1	
Директива по машинам, механизмам и машинному оборудованию	Да	
Архитектура системы TeSys island	Одноканальная	Двухканальная
Уровень эффективности EN ISO 13849-1	PL c, d	PL c, d, e
Категория электроснабжения ISO 13849-1	Кат. 1, 2	Кат. 3, 4
SIL CL EN 62061	SIL CL 2	SIL CL 3
SIL МЭК 61508 / МЭК 61511	SIL 2	SIL 3

Подтверждающий функциональную безопасность сертификат размещен по адресу www.se.com/tesys/.

Примечание: При сертификации, связанной с функциональными аспектами, должна рассматриваться только система TeSys island, пригодная для применения в связанных с безопасностью целях, а не все система, в которую она была интегрирована для обеспечения функциональной безопасности машины или системы (процесса).

Условия эксплуатации

Система TeSys island рассчитана на длительное использование в следующих условиях. Другие условия могут применяться к конкретным модулям, как описано в их технической спецификации, представленной на www.se.com/tesys-island.

- Температура окружающего воздуха 40 °C (104 °F)
- Двигатель 400/480 В
- Влажность 50%
- Нагрузка 80%
- Горизонтальный монтаж
- Все входы активированы
- Все выходы активированы
- Работа 24 часа в сутки, 365 дней в году

Одноканальная архитектура (ISO 13849)

TeSys island можно использовать для создания одноканальных архитектур, в случае которых обнаруженный отказ может приводить к потере соответствующей функции безопасности.

Двухканальная архитектура (ISO 13849)

TeSys island применяется в двухканальных архитектурах, в которых одиночный обнаруженный отказ (включая отказы группового типа) не приводит к потере функции безопасности.

Категории останова (EN/МЭК 60204–1)

Категория останова определяет порядок отключения питаемой нагрузки от напряжения и зависит от внешней связанной с безопасностью подсистемы, которая запускает выполнение функции останова. Внешняя связанная с безопасностью подсистема может быть реализована в виде таких устройств, как модули Preventa™ XPS.

Категория останова 0

Категория останова 0 предполагает останов движения машины путем немедленного отключения электроэнергии от приводных устройств машины. Категория останова 0 соответствует неконтролируемому останову.

Категория останова 1

Категория останова 1 предполагает останов движения машины при сохранении подачи электроэнергии на приводные устройства машины на протяжении всего процесса останова. Подача электроэнергии прекращается после завершения останова. Категория останова 1 соответствует контролируемому останову.

Категории электроснабжения⁸

Категории электроснабжения определяют способ подключения внешнего модуля Preventa™ XPS (или аналогичного) и соответствующий дополнительный уровень контроля функции безопасности.

Категория электроснабжения 1

Одиночный обнаруженный отказ может привести к потере функции безопасности, и диагностическое покрытие не требуется.

Связанный с безопасностью сенсорный элемент может быть непосредственно подключен к общим входам SIL-IN/SIL⁹. Зеркальные контакты входа/выхода не используются. Дополнительную информацию о подключении общих входов SIL-IN/SIL см. в разделе *Связанный с безопасностью сенсорный элемент*, стр. 24.

Категория электроснабжения 2

Связанный с безопасностью сенсорный элемент подключается к модулю Preventa XPS (или аналогичному). Выходы модуля Preventa XPS (или аналогичного) подключаются к общим входам SIL-IN/SIL интерфейсного модуля SIL⁹.

Для выполнения требований категории 2 необходим мониторинг обратной связи зеркального контакта (зеркальный вход / зеркальный выход) модулем Preventa XPS (или аналогичным), который выполняет внешний диагностический мониторинг зеркального контакта. Если зеркальный контакт не замыкается при останове, то следующий перезапуск блокируется для всех пускателей SIL в группе SIL.

Реализация непрямого мониторинга для категории 2

Чтобы выполнить требования категории 2 для диагностического охвата (DC > 60 %), необходимо реализовать внешний мониторинг состояния группы для включения дополнительного механизма останова машины (шунтовой автоматический выключатель и т. п.) или для предотвращения доступа в опасные зоны (блокировка ограждения).

8. Категории электроснабжения согласно ISO 13849.

9. Уровень полноты безопасности согласно стандарту МЭК 61508.

Каждая группа SIL¹⁰ имеет пять связанных состояний, указывающих на ее эксплуатационное состояние. Состояние 0 указывает, что в этом слоте нет группы SIL. TeSys island поддерживает до 10 групп SIL в одном модуле island.

Состояние группы SIL для функции останова SIL:

- 0 = группа SIL отсутствует в конфигурации системы;
- 1 = группа SIL управляется событием устройства аватара;
- 2 = получена команда останова, пускатели SIL еще не разомкнуты;
- 3 = успешно отправлена команда останова, все пускатели SIL разомкнуты;
- 4 = отправлена команда останова только по одному входному каналу интерфейсного модуля SIL (SIM) (проблему вызывает переключатель или проводка ввода SIM), но пускатели SIL успешно разомкнуты;
- 5 = нормальная работа, пускатели SIL могут быть разомкнуты или замкнуты.

Состояние 5 — это нормальное рабочее состояние, а состояние 3 — это нормальное состояние останова SIL. Состояние 1 указывает на проблему микропрограммного обеспечения или связи с пускателем SIL. Состояния 2 и 4 указывают на проблемы, касающиеся останова SIL, связанные с модулями SIM, пускателями SIL или проводкой команды останова SIL. Непрямой мониторинг должен отслеживать существование состояний 2 или 4 в течение периода, превышающего время активации команды останова SIL, и использует информацию о состоянии для включения дополнительного механизма для останова машины (шунтовой автоматический выключатель и т. п.).

Для считывания состояния группы SIL внешняя система мониторинга должна использовать функциональный блок SystemDiagnostics. Каждая группа SIL в системе имеет вывод на этот функциональный блок своего статуса группы SIL, обозначенного в функциональном блоке как "SILStarterStopMsgGrp *n*", где *n* — это номер группы SIL в системе. Состояние группы SIL следует за показанным выше номером.

Диагностический мониторинг

Поскольку диагностический мониторинг происходит моментально при появлении запроса функции безопасности, общее время обнаружения отказа и перевода машины в безопасное состояние должно быть короче, чем время достижения опасной зоны.

Согласно ISO 13849-2, 9.2.3 для категории 2: Значение $MTTF_d^{11}$ оборудования мониторинга должно быть больше половины $MTTF_d$ логики. Вклад модуля TeSys island в значение $MTTF_d$ диагностического мониторинга составляет $MTTF_d > 100$ лет.

Категория электроснабжения 3

Одиночный отказ не приведет к потере функции безопасности. И во всех случаях, когда это практически возможно, одиночный отказ будет обнаружен в момент или до начала следующего запроса функции безопасности.

Для выполнения требований категории 3 необходим мониторинг обратной связи зеркального контакта (зеркальный вход/выход) модулем Preventa XPS (или аналогичным), который выполняет внешний диагностический мониторинг зеркального контакта пускателя SIL¹⁰. Если зеркальный контакт не размыкается при останове, то следующий перезапуск блокируется для всех пускателей SIL в группе SIL. Связанный с безопасностью сенсорный элемент подключается к модулю Preventa XPS (или аналогичному). Выходы модуля Preventa XPS (или аналогичного) подключаются к общим входам SIL-IN/SIL интерфейсного модуля SIL.

10. Уровень полноты безопасности согласно стандарту МЭК 61508.

11. Среднее время до опасного отказа, согласно определению ISO 13849-1.

В случае непрямого мониторинга внешний мониторинг состояния группы должен следить за состояниями 2 или 4, которые сохраняются дольше времени активации останова SIL. Используйте информацию о состоянии для блокирования следующего перезапуска группы пускателей SIL.

Категория электроснабжения 4

Одиночный отказ не приведет к потере функции безопасности. Одиночный отказ будет обнаружен в момент или до начала следующего запроса функции безопасности. Если это обнаружение невозможно, то накопление необнаруженных отказов не приведет к потере функции безопасности.

Для выполнения требований категории 4 необходим мониторинг обратной связи зеркального контакта (зеркальный вход/выход) модулем Preventa XPS (или аналогичным), который выполняет внешний диагностический мониторинг зеркального контакта пускателя SIL¹². Если зеркальный контакт не размыкается при останове, то следующий перезапуск блокируется для всех пускателей SIL в группе SIL. Связанный с безопасностью сенсорный элемент подключается к модулю Preventa XPS (или аналогичному). Выходы модуля Preventa XPS (или аналогичного) подключаются к общим входам SIL-IN/SIL интерфейсного модуля SIL.

Проверка соответствия техническим условиям

Для проверки надлежащего действия функций безопасности и оформления подтверждающего документа системный интегратор и (или) производитель машины обязан выполнить проверку соответствия функций безопасности техническим условиям. Настоящим системный интегратор и (или) производитель машины подтверждает, что проверку эффективности используемых функций безопасности выполнил. Проверка соответствия техническим условиям должна проводиться на основании анализа опасностей и оценки рисков. В случае режима работы с низкой частотой запросов и категории 4 проверка функций безопасности должна проводиться не реже одного раза в месяц. Соблюдение требований всех применимых стандартов, норм и правил обязательно.

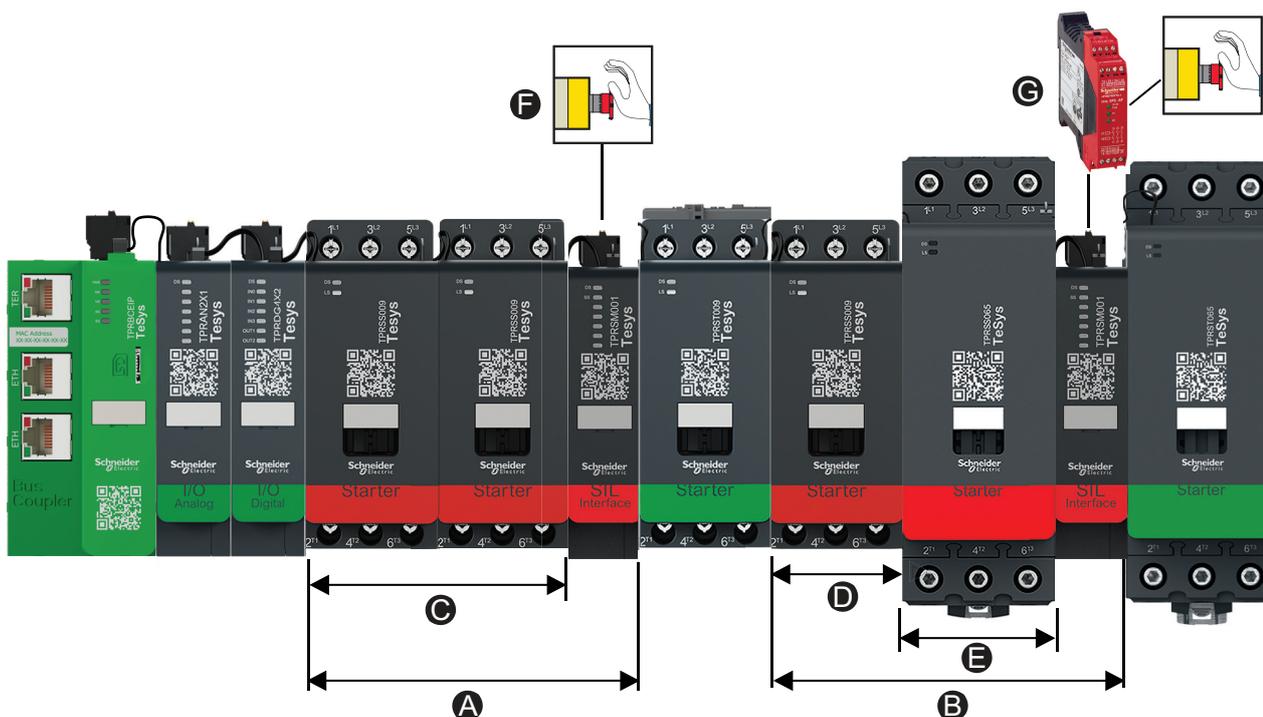
12. Уровень полноты безопасности согласно стандарту МЭК 61508.

Концепции и компоненты

Типовая структура TeSys™ island

На иллюстрации ниже приведен пример TeSys™ island, состоящий из двух групп SIL¹³. Состав системы определяется цифровыми средствами TeSys island в зависимости от функциональных потребностей, указанных пользователем.

рисунок 2 - TeSys island с двумя группами SIL



A	Группа SIL 1	E	Аватар A4
B	Группа SIL 2	F	Категория электроснабжения 1, категория останова 0 ¹⁴
C	Аватар A2	G	Категория электроснабжения 2, категория останова 1 ¹⁵
D	Аватар A3		

Группа SIL 1: состоит из одного автара, в который входят два пускателя SIL: например автара «Двигатель, два направления вращения - останов SIL, кат. 1/2» (Аватар A1). Фактический двигатель подключается к этим пускателям SIL и действует в соответствии с логикой и управляющими командами соответствующего автара, поступающими от ПЛК по шине fieldbus. Команда останова SIL поступает от кнопки аварийного останова, подключенной к интерфейсному модулю SIL (категория электроснабжения 1). Ее обработка приводит к тому, что пускатели SIL прерывают подачу напряжения на нагрузку и переходят в безопасное состояние (контактор разомкнут, напряжение на двигатель не подается).

13. Уровень полноты безопасности согласно стандарту МЭК 61508.

14. Категория электроснабжения 1 согласно требованиям ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

15. Категория электроснабжения 2 согласно требованиям ISO 13849. Категория останова 1 согласно стандарту EN/МЭК 60204-1.

Группа SIL 2: состоит из двух аватаров, например «Выключатель - останов SIL, кат. 1/2» (Аватар А3) и «Двигатель, одно направление вращения - останов SIL, кат. 1/2», в каждый из которых входит один пускатель SIL. Оба аватара действуют согласно логике и управляющим командам аватара, поступающим от ПЛК по шине fieldbus. Команда останова SIL поступает от внешнего модуля Preventa™ XPS (или аналога), который подключен к интерфейсному модулю SIL, и ее отработка приводит к тому, что пускатели SIL прерывают подачу напряжения на нагрузку и переходят в безопасное состояние (категория электроснабжения 2).

Группа SIL

Группа SIL¹⁶ состоит из одного из нескольких аватаров SIL, связанных с одним интерфейсным модулем SIL. Все аватары SIL одной группы SIL реагируют на одну команду останова SIL. Интерфейсный модуль SIL всегда устанавливается справа от последнего пускателя SIL, входящего в группу SIL (с противоположной стороны от модуля удаленного подключения).

В систему может входить несколько групп SIL.

Аватары SIL

Аватары SIL¹⁶, доступны для функций останова SIL:

- Переключатель – останов SIL, кат. 1/2
- Переключатель – останов SIL, кат. 3/4
- Двигатель, одно направление вращения - останов SIL, кат. 1/2
- Двигатель, одно направление вращения - останов SIL, кат. 3/4
- Двигатель, два направления вращения - останов SIL, кат. 1/2
- Двигатель, два направления вращения - останов SIL, кат. 3/4
- Двигатель двухскоростной - останов SIL, кат. 1/2
- Двигатель двухскоростной - останов SIL, кат. 3/4
- Двигатель двухскоростной, два направления вращения - останов SIL, кат. 1/2
- Двигатель двухскоростной, два направления вращения - останов SIL, кат. 3/4
- Конвейер, одно направление вращения - останов SIL, кат. 1/2
- Конвейер, два направления вращения - останов SIL, кат. 3/4

Аватары SIL состоят из определенных аппаратных устройств, в том числе пускателей SIL, стандартных пускателей и необходимого интерфейсного модуля SIL, управляющего группой SIL, в которую включены соответствующие аватары SIL.

Примечание: Аватары SIL предназначены для применения в условиях низкой частоты эксплуатационных команд — среднее значение за год должно быть ниже 15 циклов пуск-останов в час.

16. Уровень полноты безопасности согласно стандарту МЭК 61508.

Пускатель SIL



Стандартный пускатель



Интерфейсный модуль SIL



Интерфейсный модуль SIL

Интерфейсный модуль SIL¹⁷ (SIM) системы TeSys™ island является вспомогательным модулем, необходимым для активирования функциональной безопасности системы.

Функция останова SIL реализуется исключительно электромеханическими средствами без использования цифровой связи или модуля удаленного подключения.

Модуль SIM:

- подключается к внешнему модулю Preventa™ XPS (или аналогичному);
- управляет функцией останова своей группы SIL;
- обменивается эксплуатационными данными с модулем удаленного подключения;
- предоставляет эксплуатационную информацию посредством светодиодных индикаторов, расположенных на передней панели.

Состояние контактов пускателей SIL

Информация о состоянии пускателей SIL¹⁷, входящих в группу SIL, передается через зеркальные контакты входа/выхода модуля SIM. Это позволяет реализовать архитектуру категории электроснабжения 2¹⁸, когда зеркальные контакты подключаются к модулю Preventa XPS (или аналогичному). Эти конфигурации позволяют осуществлять непосредственный мониторинг электромеханических устройств механически связанным контактным элементом, обеспечивающим диагностическое покрытие до 99 %. См. EN ISO 13849-1, табл. E.1 «Оценка диагностического покрытия (DC)».

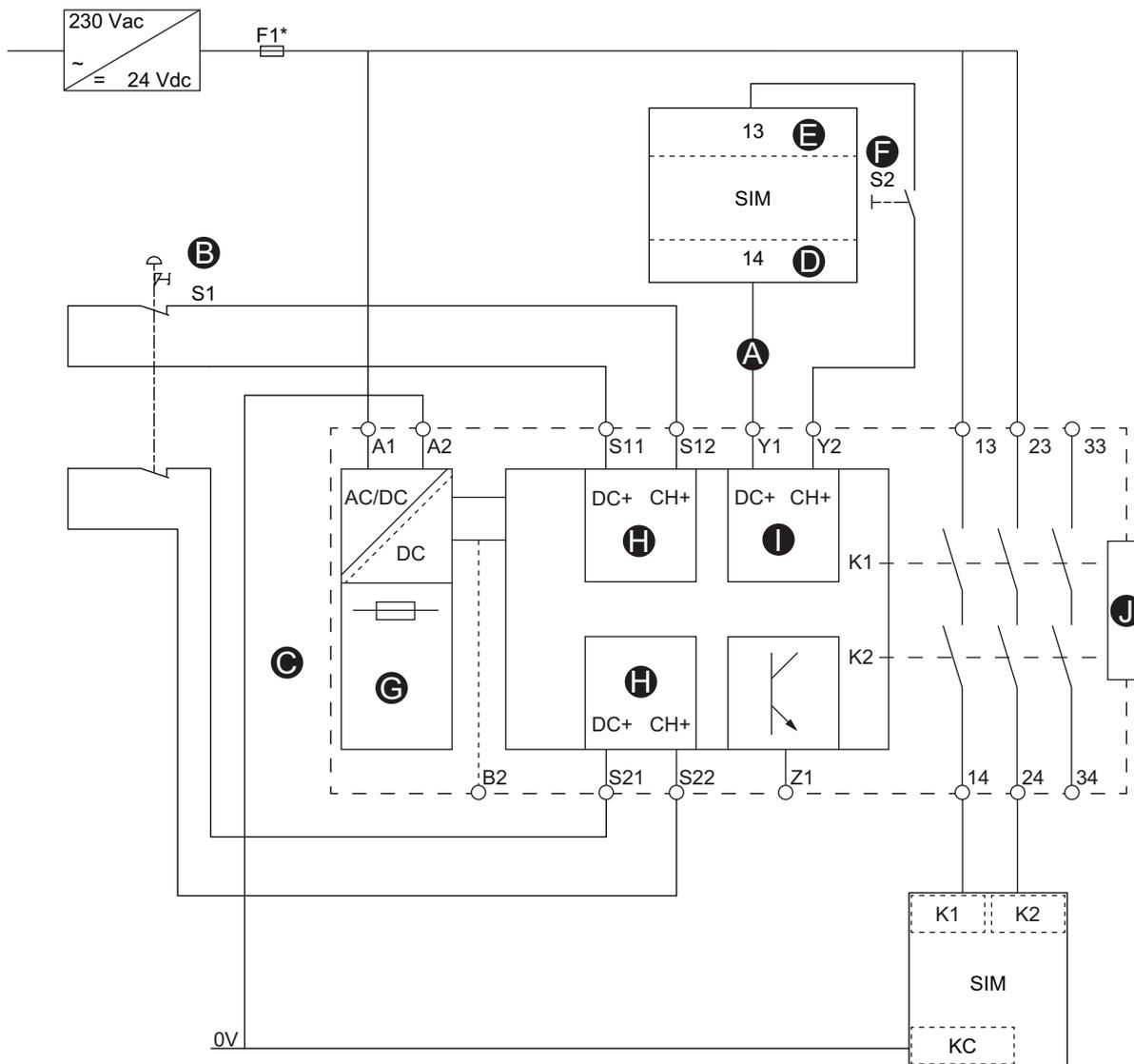
Таблица 2 - Состояние контактов пускателя SIL

Состояние группы SIL	Состояние зеркального контакта входа/выхода
Все пускатели SIL разомкнуты	Зеркальный контакт входа/выхода замкнут
По крайней мере один пускатель SIL замкнут	Зеркальный контакт входа/выхода разомкнут
Питание на TeSys island не подается или обнаружен отказ функции безопасности	Зеркальный контакт входа/выхода разомкнут

17. Уровень полноты безопасности согласно стандарту МЭК 61508.

18. Категория электроснабжения 2 согласно ISO 13849

рисунок 3 - Подключение модуля SIM к модулю Preventa XPS-AF



A	Внешние условия пуска (ESC)	F	Кнопка пуска (S2)
B	Кнопка аварийного останова (S1)	G	Источник питания
C	Модуль Preventa XPS-UAF	H	Вход
D	Зеркальный выход модуля SIM	I	Пуск
E	Зеркальный вход модуля SIM	J	Расширение

Связанный с безопасностью сенсорный элемент

Вход модуля SIM подключается:

- к источнику напряжения 24 В постоянного тока;
- к связанному с безопасностью сенсорному элементу или к модулю Preventa XPS (либо аналогичному).

Для обеспечения возможности использования с двухканальными связанными с безопасностью сенсорными элементами модуль SIM имеет два входных канала. Для обеспечения более высокой отказоустойчивости рекомендуется использовать архитектуру с двумя входными каналами.

Для приведенных ниже схем коммутации используйте Условные обозначения для схем коммутации каналов модулей SIM, стр. 24.

рисунок 4 - Модуль SIM — одноканальная коммутация

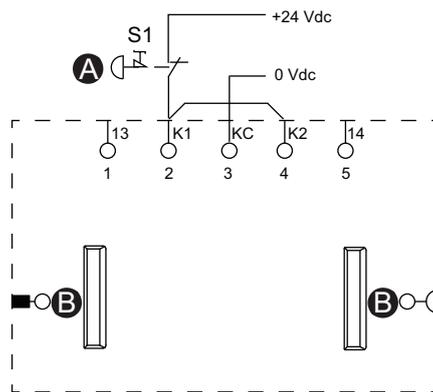


рисунок 5 - Модуль SIM — двухканальная коммутация

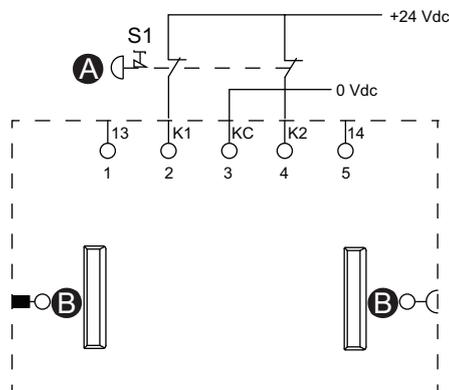


Таблица 3 - Условные обозначения для схем коммутации каналов модулей SIM

A	Кнопка аварийного останова (S1)
B	Разъем плоского кабеля

Пускатели SIL

▲ ОСТОРОЖНО

НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ ОБОРУДОВАНИЯ

Полный текст инструкций по функциональной безопасности см. в Руководстве по функциональной безопасности TeSys™ island, 8536IB1904.

Несоблюдение данных инструкций может привести к смерти, серьезной травме или повреждению оборудования.

Функциональные возможности пускателей SIL¹⁹ аналогичны обеспечиваемым стандартными пускателями, но они связываются с интерфейсными модулями SIL.

Основные функции пускателей SIL следующие:

- обеспечение останова категорий 0 и 1²⁰;
- обеспечение управляющего контроля нагрузок;
- измерение связанных с нагрузкой электрических параметров;
- предоставление данных для мониторинга энергопотребления при наличии в системе интерфейсного модуля напряжения.

Для функционирования одного аватара TeSys может требоваться несколько пускателей SIL. Например, аватар «Двигатель, два направления вращения - останов SIL, кат. 1/2»²¹ включает два пускателя SIL. Кроме того, аватары, в которых используются пускатели SIL, обязательно имеют интерфейсный модуль SIL.

Пускатели SIL подключаются:

- на входе к автоматическому выключателю;
- на выходе к нагрузке.

Пускатели SIL обмениваются данными с модулем удаленного подключения, передавая ему эксплуатационные данные и получая команды.

Таблица 4 - Классификация пускателей SIL

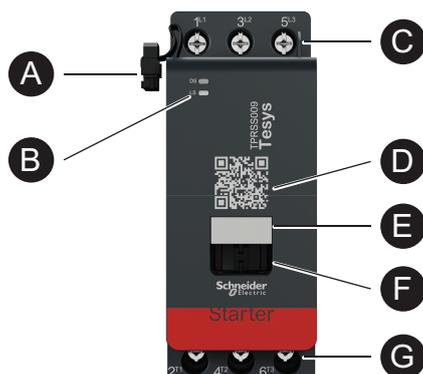
Номинальная мощность		Ток	Артикул
кВт	л. с.		
4	5	0,18-9	TPRSS009
11	15	0,5-25	TPRSS025
18,5	20	0,76-38	TPRSS038
30	40	3,25-65	TPRSS065
37	40	4-80	TPRSS080

19. Уровень полноты безопасности согласно стандарту МЭК 61508.

20. Категории останова 0 и 1 согласно стандарту EN/МЭК 60204-1.

21. Категории электроснабжения 1 и 2 согласно стандарту ISO 13849.

рисунки 6 - Схема пускателей SIL



A	Плоский кабель (для коммутации с расположенным слева модулем)	E	Идентификационная табличка
B	Светодиодные индикаторы состояния	F	Мобильная перемычка
C	Входные силовые контакты	G	Выходные силовые контакты
D	QR-код		

Внешний связанный с безопасностью элемент

Для обеспечения функциональной безопасности машины или системы (процесса) система TeSys™ island должна быть интегрирована с другими связанными с безопасностью элементами в более масштабную связанную с безопасностью систему.

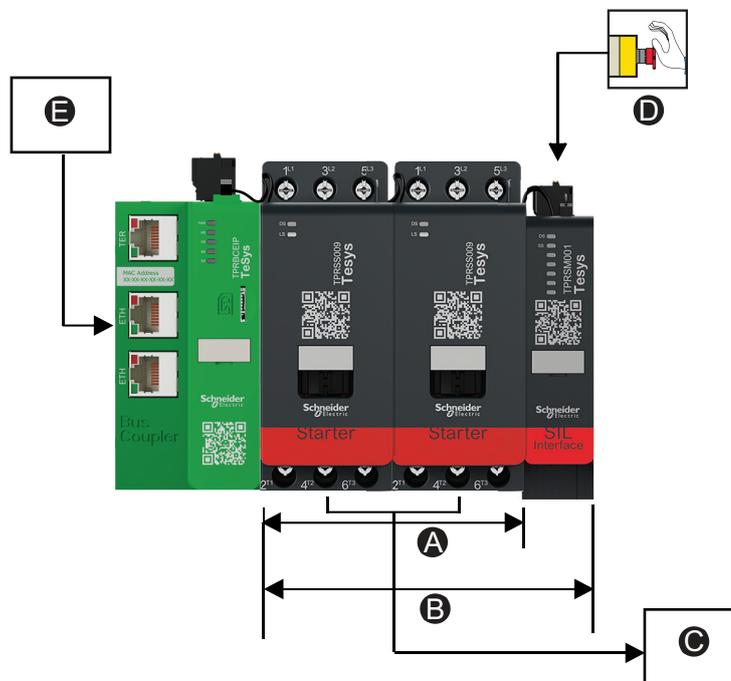
Следующие конфигурации служат иллюстрацией использования типовых устройств.

Конфигурация: останов SIL, категория останова 0, категория электроснабжения 1

Примечание: Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 1 согласно стандарту ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

Управление остановом SIL электродвигателя осуществляется непосредственно размыканием контактов кнопки аварийного останова.

рисунок 7 - Останов SIL



A	Аватар A2	D	Категория электроснабжения 1, категория останова 0
B	Группа SIL 1	E	ПЛК
C	Электродвигатель		

Конфигурация: останов SIL, категория останова 0, категория электроснабжения 2

Примечание: Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 2 согласно стандарту ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

рисунок 8 - Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 1/2 — категория останова 0, категория электроснабжения 2» (непрямой мониторинг)

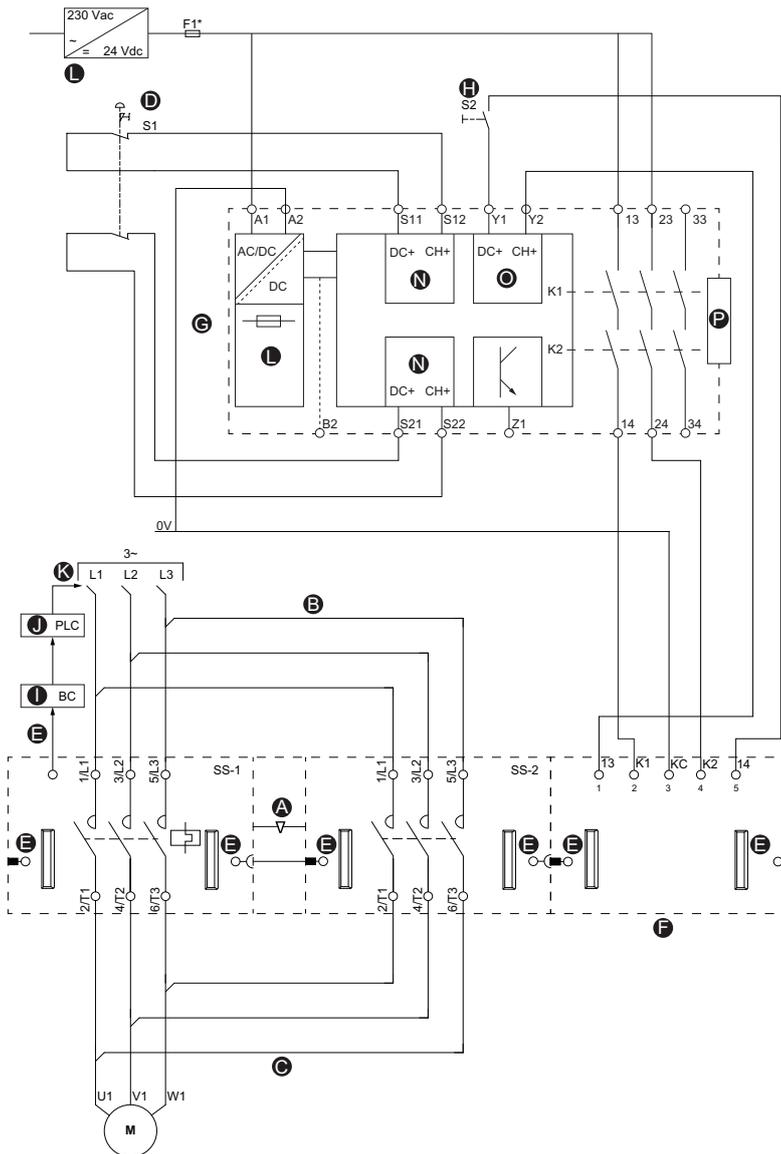


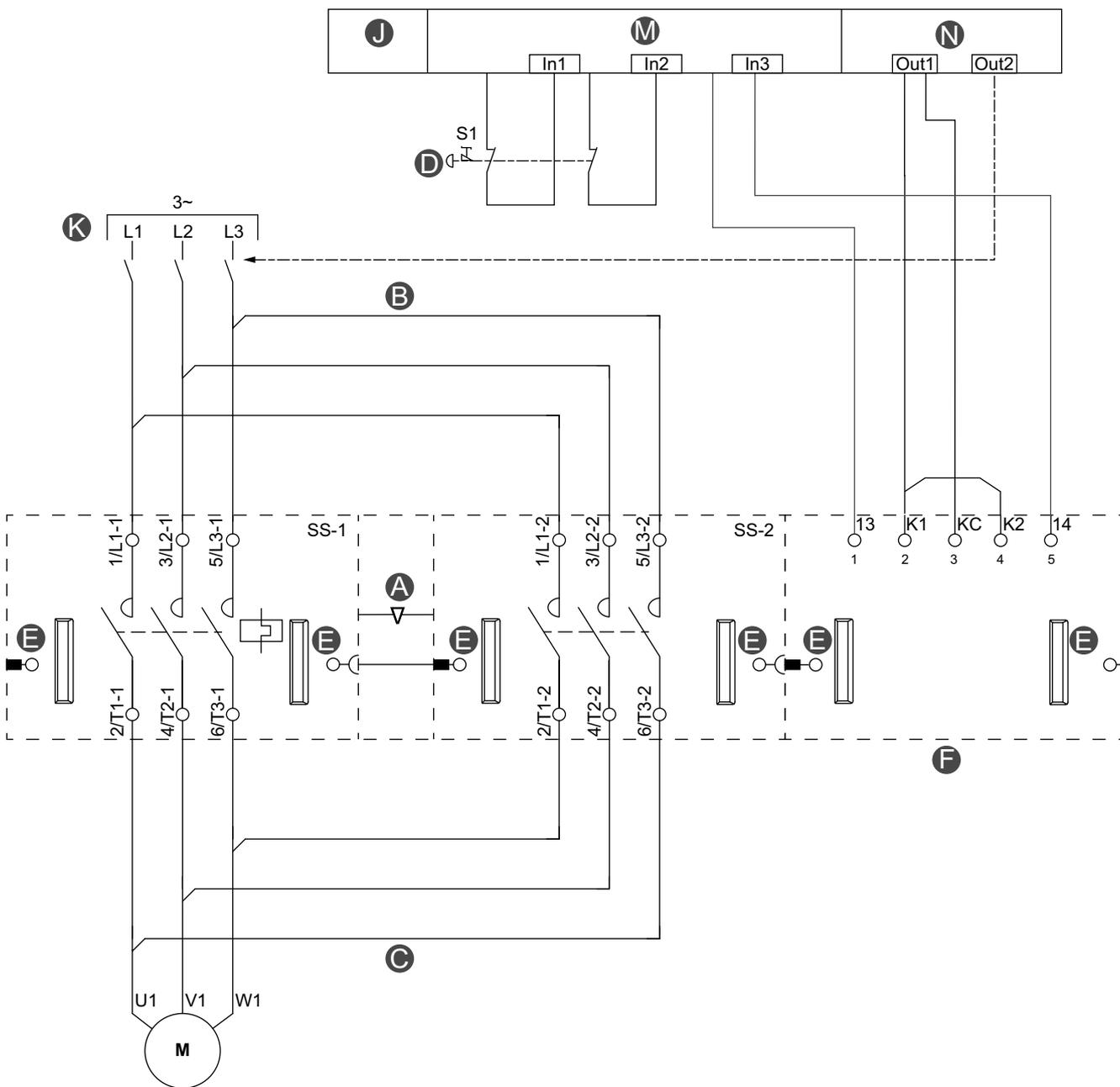
Таблица 5 - Легенда Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 1/2 — категория останова 0, категория электроснабжения 2» (непрямой мониторинг), стр. 28

A	Механическая блокировка	I	Модуль удаленного подключения
B	Параллельная связь	J	ПЛК
C	Реверсная связь	K	Автоматический выключатель на входе
D	Кнопка аварийного останова (S1)	L	Источник питания
E	Разъем плоского кабеля	N	Вход
F	Интерфейсный модуль SIL (SIM)	O	Пуск

Таблица 5 - Легенда Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 1/2 — категория останова 0, категория электроснабжения 2» (непрямой мониторинг) (продолжение)

G	Модуль Preventa XPS-UAF	P	Расширение
H	Кнопка пуска (S2)		

рисунок 9 - Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 1/2 — категория останова 0, категория электроснабжения 2» (прямой мониторинг)



A	Механическая блокировка	F	Интерфейсный модуль SIL (SIM)
B	Параллельная связь	J	ПЛК функции безопасности

C	Реверсная связь	K	Автоматический выключатель на входе
D	Кнопка аварийного останова (S1)	M	Цифровой ввод
E	Разъем плоского кабеля	N	Цифровой выход

Конфигурация: останов SIL, категория останова 1, категория электроснабжения 2

Примечание: Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 2 согласно стандарту ISO 13849. Категория останова 1 согласно стандарту EN/МЭК 60204-1.

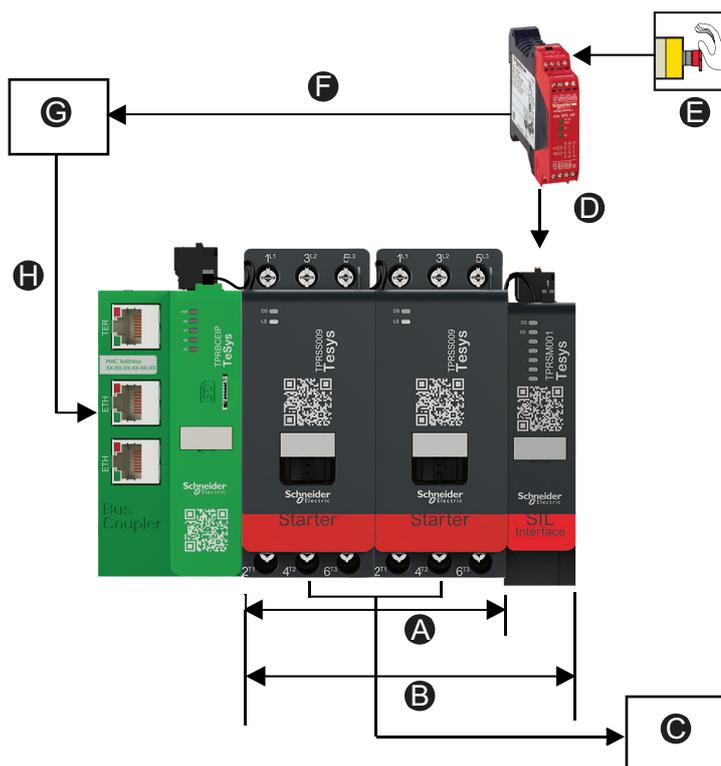
Категория останова 1 определяется как: «управляемый останов при наличии питания на приводах машины до достижения останова и отключении питания после останова».

При активации аварийного останова команда останова сначала отправляется на внешнее устройство (например, ПЛК или привод). Таким образом, процесс останова происходит под контролем, а не посредством моментального отключения питания. После истечения заданного времени команда останова SIL отправляется модулю SIM для прекращения подачи напряжения на нагрузки аватаров SIL соответствующей группы SIL.

Для настройки рекомендуется использовать ПЛК, что помогает обеспечить правильный останов процесса до отработки останова SIL.

Команда останова должна подаваться непосредственно на цифровой вход ПЛК или на аватар модуля цифровых входов/выходов TeSys™ island, для чего должен использоваться один из цифровых входов, считываемых ПЛК. После получения входной команды останова ПЛК инициализирует контролируемый останов путем отправки команды эксплуатационного останова на целевой аватар TeSys island.

рисунок 10 - Команда останова



A	Аватар A2	E	Категория электромонтажа 2, категория останова 1
B	Группа SIL 1	F	Команда контролируемого останова категории 1
C	Электродвигатель	G	ПЛК
D	Неконтролируемый останов	H	Команда эксплуатационного останова

Таблица 6 - Легенда Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 1/2 — категория останова 1, категория электроснабжения 2», стр. 32

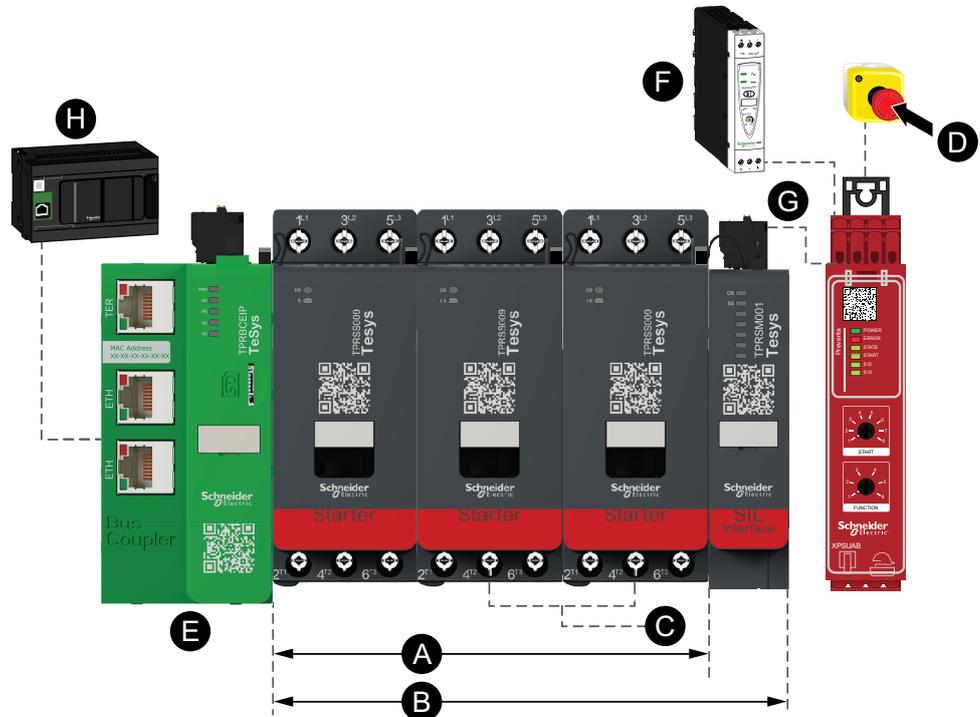
A	Механическая блокировка	M	Контролируемый останов
B	Параллельная связь	N	Категория останова 1
C	Реверсная связь	O	Автоматический выключатель на входе
E	Разъем плоского кабеля	P	ПЛК
F	Интерфейсный модуль SIL (SIM)	Q	Модуль удаленного подключения
G	Модуль Preventa XPS-UAF	R	Вход
H	Кнопка аварийного останова	S	Пуск
I	Кнопка запуска S2	T	Расширение
L	Источник питания		

Конфигурация: останов SIL, категория останова 0, категория электроснабжения 3/4

Примечание: Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 3/4 согласно стандарту ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

Управление остановом SIL электродвигателя осуществляется непосредственно размыканием контактов кнопки аварийного останова.

рисунок 12 - Останов SIL, категория электроснабжения 3/4



A	Аватар A2	E	Модуль удаленного подключения
B	Группа SIL 1	F	24 В постоянного тока
C	Электродвигатель	G	Модуль Preventa XPS-UAF
D	Категория электроснабжения 3/4, категория останова 0	H	ПЛК

рисунок 13 - Пример: Конфигурация: «Двигатель, одно направление вращения - останов SIL, кат. 3/4 — категория останова 0, категория электроснабжения 3/4»

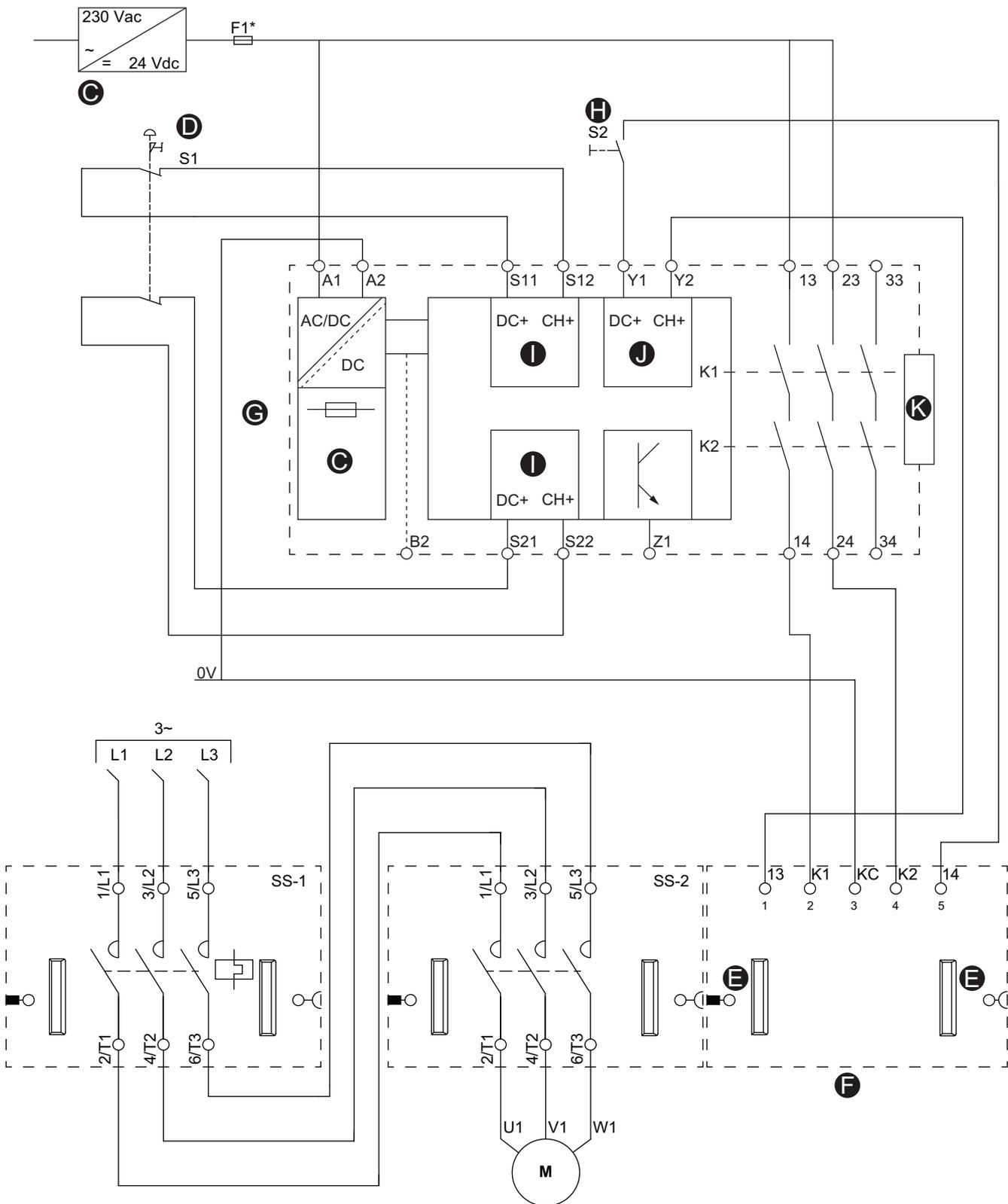


Таблица 7 - Легенда Пример: Конфигурация: «Двигатель, одно направление вращения - останов SIL, кат. 3/4 — категория останова 0, категория электроснабжения 3/4», стр. 35

C	Источник питания	H	Кнопка пуска (S2)
D	Кнопка аварийного останова (S1)	I	Вход
E	Разъем плоского кабеля	J	Пуск
F	Интерфейсный модуль SIL (SIM)	K	Расширение
G	Модуль Preventa XPS-UAF		

Конфигурация: останов SIL, категория останова 1, категория электроснабжения 3/4

Примечание: Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 3/4 согласно стандарту ISO 13849. Категория останова 1 согласно стандарту EN/МЭК 60204.

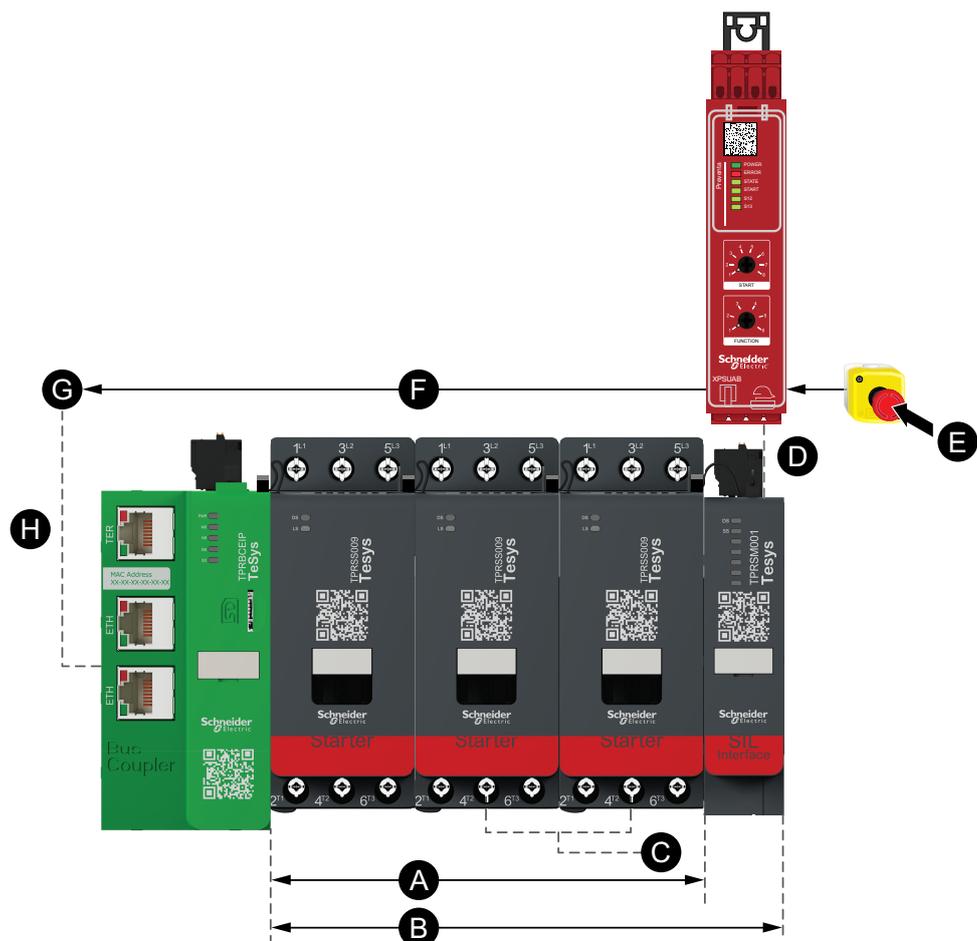
Категория останова 1 определяется как: «управляемый останов при наличии питания на приводах машины до достижения останова и отключении питания после останова».

При активации аварийного останова команда останова сначала отправляется на внешнее устройство (например, ПЛК или привод). Таким образом процесс останова происходит под контролем, а не посредством моментального отключения питания. После истечения заданного времени команда останова SIL отправляется модулю SIM для прекращения подачи напряжения на нагрузки аватаров SIL соответствующей группы SIL.

Для настройки рекомендуется использовать ПЛК, что помогает обеспечить правильный останов процесса до отработки останова SIL.

Команда останова должна подаваться непосредственно на цифровой вход ПЛК или на аватар модуля цифровых входов/выходов TeSys™ island, для чего должен использоваться один из цифровых входов, считываемых ПЛК. После получения входной команды останова ПЛК инициализирует контролируемый останов путем отправки команды эксплуатационного останова на целевой аватар TeSys island.

рисунок 14 - Команда останова, категория электроснабжения 3/4



A	Аватар A2	E	Категория электроснабжения 3/4, категория останова 1
B	Группа SIL 1	F	Команда контролируемого останова категории 1
C	Электродвигатель	G	ПЛК
D	Неконтролируемый останов	H	Команда эксплуатационного останова

рисунок 15 - Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 3/4 — категория останова 1, категория электроснабжения 3/4»

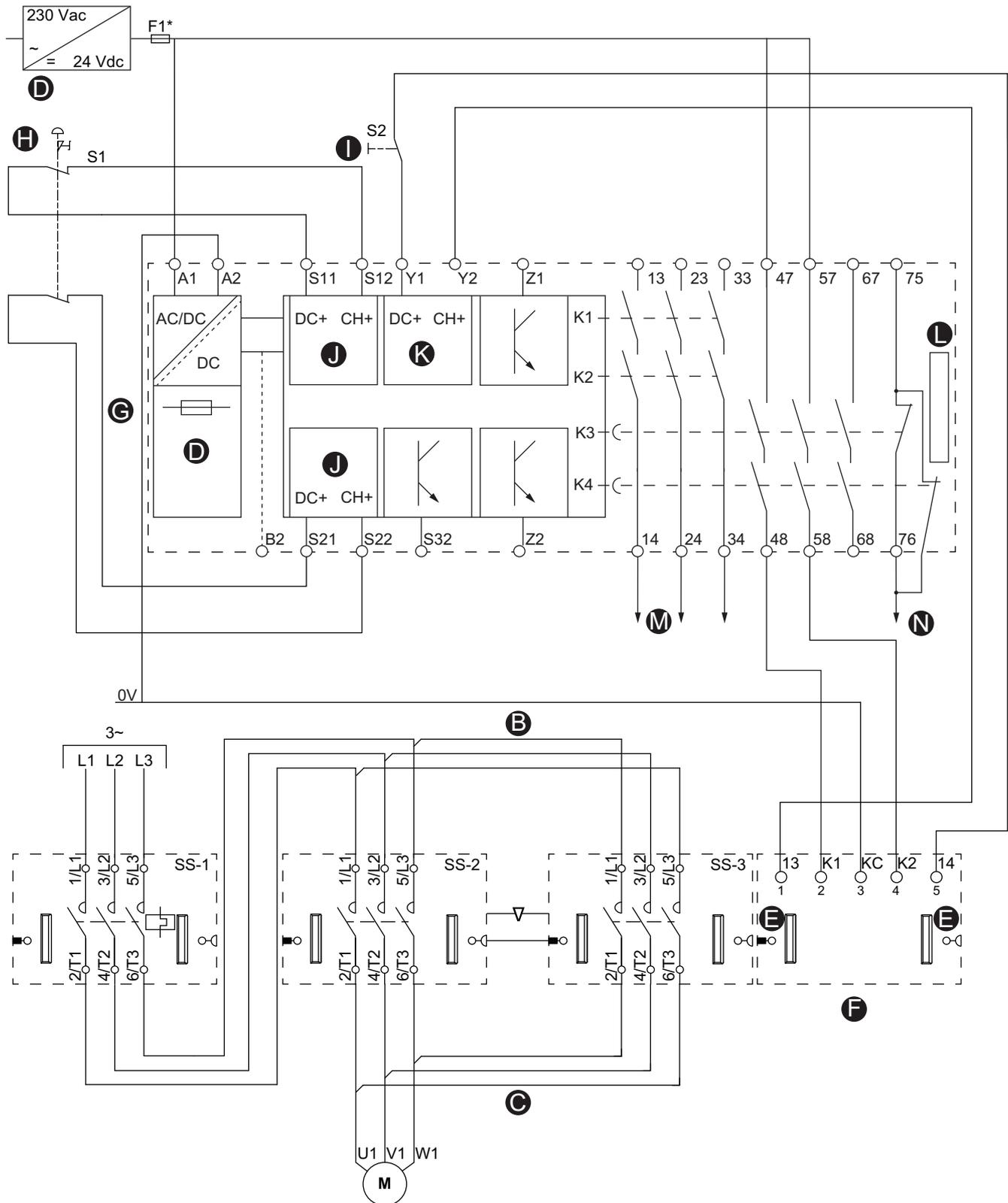


Таблица 8 - Легенда Пример: Конфигурация: «Двигатель, два направления вращения - останов SIL, кат. 3/4 — категория останова 1, категория электроснабжения 3/4», стр. 38

B	Параллельная связь	I	Кнопка запуска S2
C	Реверсная связь	J	Вход
D	Источник питания	K	Пуск
E	Разъем плоского кабеля	L	Расширение
F	Интерфейсный модуль SIL (SIM)	M	Контролируемый останов
G	Модуль Preventa XPS-UAF	N	Категория останова 1
H	Кнопка аварийного останова (S1)		

Защитная изоляция кабелей

⚠ ОПАСНО

НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ ОБОРУДОВАНИЯ

Прокладка кабелей связанной с безопасностью системы должна быть выполнена в соответствии с требованиями ISO 13849-2.

Несоблюдение данных инструкций приводит к смерти или серьёзной травме.

Если существует возможность короткого или перекрестного замыкания кабелей связанной с безопасностью системы, и эти ситуации не могут быть обнаружены предшествующими по цепи устройствами, то необходима защищенная прокладка кабелей в соответствии с требованиями ISO 13849-2.

В случае незащищенной прокладки кабелей в случае повреждения кабеля внешнее напряжение может быть подано на два сигнальных провода (оба канала) функции безопасности. В этом случае функция безопасности действовать не будет.

Архитектура для низкой и высокой частоты переключения

Приведенная в этом разделе информация может быть использована для определения того, какая архитектура используется — для низкой или высокой частоты.

Электромеханическая часть пускателя SIL²² характеризуется B10d.

Для расчета значения $MTTF_d$ (согласно ISO 13849-1) или λ_d (согласно МЭК 62061) применяется следующая формула:

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

$$\text{При этом } \lambda_d = 1 / MTTF_d$$

Nop: среднее количество операций в год

Согласно ISO 13849 срок эксплуатации электромеханического компонента ограничивается значением T10d (среднее время до опасного отказа 10 % компонентов²³).

Следовательно, срок эксплуатации пускателя SIL определяется следующим образом:

$$T10d = B10d / Nop$$

Значение B10d для пускателя SIL равно $B10d = 1\,369\,863$. Если предположить что T10d составляет 10 лет, количество циклов пускателя SIL системы TeSys ограничено следующим значением $Nop = B10d / T10 = 131\,400$ / год (или среднее значение за год составляет 15 цикл/час).

Если для определенной задачи требуется значение Nop ниже указанного, то система относится к категории низкой частоты переключения (при этом аватары SIL можно использовать как есть). Иначе, если система относится к категории высокой частоты переключения (и функция безопасности должна быть реализована с использованием отдельного аватара SIL, как описывается ниже).

22. Уровень полноты безопасности согласно стандарту МЭК 61508.

23. Опасный отказ согласно ISO 13849

Низкая частота переключения (< 15 циклов в час)

При низкой частоте переключения остановов SIL²⁴ и эксплуатационная функция управления включением и выключением могут быть реализованы вместе с помощью аватара SIL.

рисунок 16 - Пример аватара с пускателем SIL



Таблица 9 - Низкая частота переключения — эксплуатационная функция и функция безопасности

Аватар SIL	Модуль 1	Модуль 2	Модуль 3	Модуль 4	Модуль 5
Переключатель - останов SIL, кат. 1/2 ²⁵	Пускатель SIL	SIM	—	—	—
Переключатель - останов SIL, кат. 3/4 ²⁶	Пускатель SIL	Пускатель SIL	SIM	—	—
Двигатель, одно направление вращения - останов SIL, кат. 1/2	Пускатель SIL	SIM		—	—
Двигатель, одно направление вращения - останов SIL, кат. 3/4	Пускатель SIL	Пускатель SIL	SIM	—	—
Двигатель, два направления вращения - останов SIL, кат. 1/2	Пускатель SIL	Пускатель SIL	SIM	—	—
Двигатель, два направления вращения - останов SIL, кат. 3/4	Пускатель SIL	Пускатель SIL	Пускатель SIL	SIM	—
Двигатель двухскоростной - останов SIL, кат. 1/2	Пускатель SIL	Пускатель SIL	SIM	—	—
Двигатель двухскоростной - останов SIL, кат. 3/4	Пускатель SIL	Пускатель SIL	Пускатель SIL	SIM	—
Двигатель двухскоростной, два направления вращения - останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	Пускатель SIL	SIM
Двигатель двухскоростной, два направления вращения - останов SIL, кат. 3/4	Пускатель SIL	Пускатель SIL	Пускатель SIL	Пускатель SIL	SIM
Конвейер, одно направление вращения - останов SIL, кат. 1/2	Пускатель SIL	SIM	—	—	—
Конвейер, два направления вращения - останов SIL, кат. 1/2	Пускатель SIL	Пускатель SIL	SIM	—	—

24. Уровень полноты безопасности согласно стандарту МЭК 61508.
 25. Категория электроснабжения 1 и 2 согласно стандарту ISO 13849.
 26. Категория электроснабжения 3 и 4 согласно стандарту ISO 13849.

Высокая частота переключения (≥ 15 циклов в час)

При использовании с высокой частотой функция безопасности должна быть изолирована от эксплуатационной функции путем использования аватара SIL²⁷ для функции безопасности и стандартного аватара для эксплуатационной функции. Стандартные пускатели подключаются последовательно после пускателей SIL. В разделе Высокая частота переключения – эксплуатационная функция и функция безопасности, стр. 42 показаны примеры стандартных аватаров, используемых после пускателей SIL для архитектуры с остановом SIL, кат. электроснабжения 1/2²⁸ и остановом SIL, кат. электроснабжения 3/4²⁹.

рисунок 17 - Стандартный аватар для эксплуатационной функции + аватар SIL для функции безопасности — останов SIL, кат. 1/2

A	Стандартный аватар
B	Аватар SIL

Таблица 10 - Высокая частота переключения — останов SIL, кат. 1/2 — эксплуатационная функция и функция безопасности

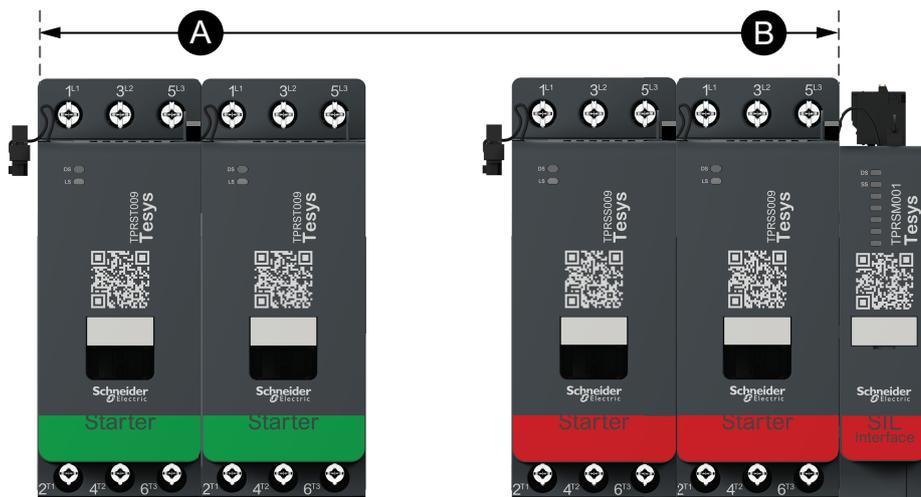
Стандартный аватар	Аватар SIL	Модуль 1	Модуль 2	Модуль 3	Модуль 4	Модуль 5	Модуль 6
Переключатель	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Пускатель SIL	SIM	—	—	—
Нереверсивный двигатель	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Пускатель SIL	SIM	—	—	—
Двигатель, два направления вращения	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	SIM	—	—
Двигатель, две скорости	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	SIM	—	—
Двигатель, две скорости, два направления	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	SIM
Конвейер, одно направление движения	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Пускатель SIL	SIM	—	—	—
Конвейер, два направления движения	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	SIM	—	—
Двигатель «звезда/треугольник», одно направление вращения	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	SIM	—
Двигатель «звезда/треугольник», два направления вращения	Переключатель – останов SIL, кат. 1/2	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	SIM

27. Уровень полноты безопасности согласно стандарту МЭК 61508.

28. Категории электроснабжения 1 и 2 согласно ISO 13849.

29. Категории электроснабжения 3 и 4 согласно стандарту ISO 13849.

рисунок 18 - Стандартный аватар для эксплуатационной функции + аватар SIL для функции безопасности — останов SIL, кат. 3/4



A	Стандартный аватар
B	Аватар SIL

Таблица 11 - Высокая частота переключения — останов SIL, кат. 3/4 — эксплуатационная функция и функция безопасности

Стандартный аватар	Аватар SIL	Модуль 1	Модуль 2	Модуль 3	Модуль 4	Модуль 5	Модуль 6	Модуль 7
Переключатель	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Пускатель SIL	Пускатель SIL	Пускатель SIL	—	—	—
Нереверсивный двигатель	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Пускатель SIL	Пускатель SIL	Пускатель SIL	—	—	—
Двигатель, два направления вращения	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	Пускатель SIL	SIM	—	—
Двигатель, две скорости	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	Пускатель SIL	SIM	—	—
Двигатель, две скорости, два направления	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	Пускатель SIL	SIM
Двигатель «звезда/треугольник», одно направление вращения	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	Пускатель SIL	Пускатель SIL
Двигатель «звезда/треугольник», два направления вращения	Переключатель – останов SIL, кат. 3/4	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Стандартный пускатель	Пускатель SIL	Пускатель SIL	Пускатель SIL

Примеры архитектуры

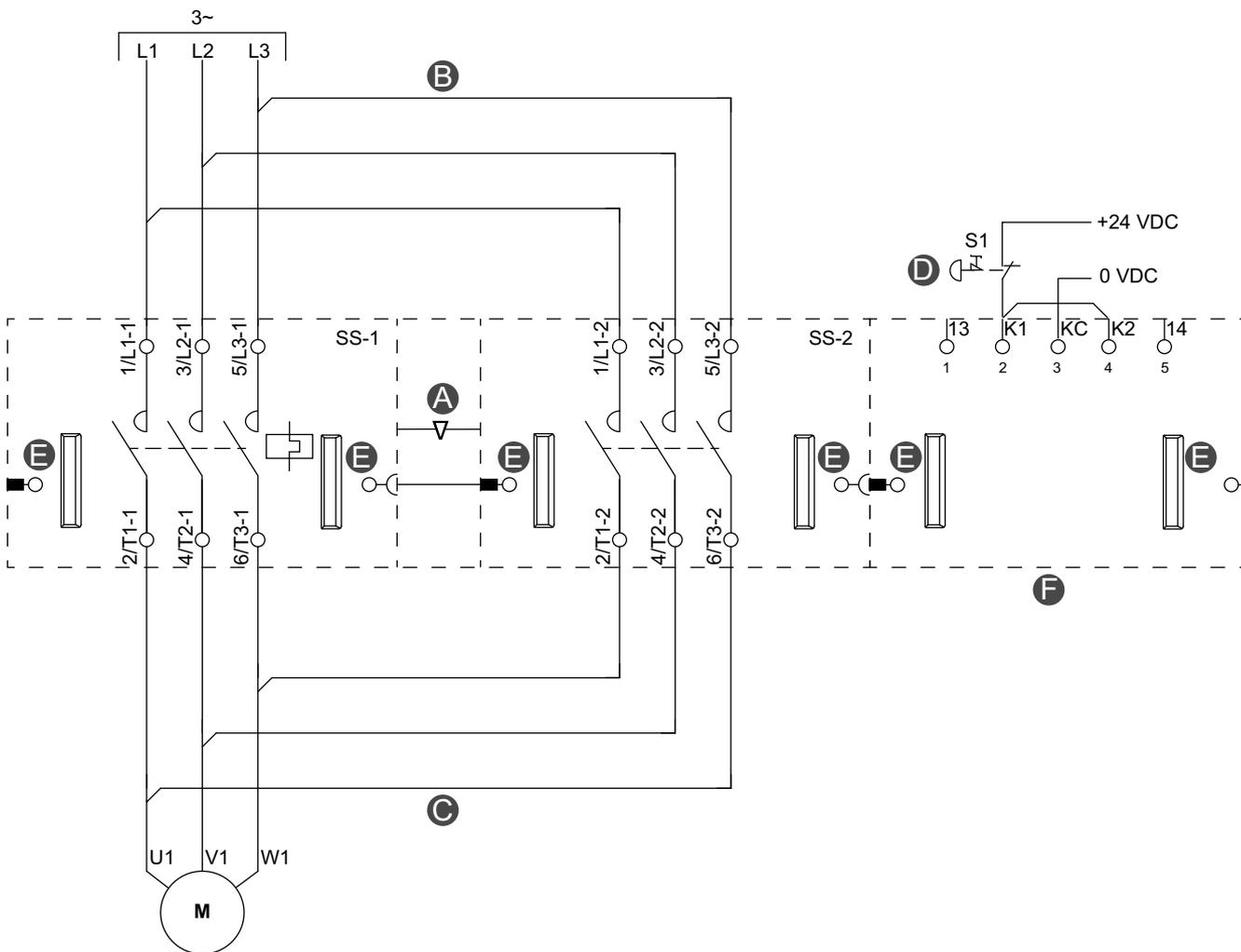
TeSys™ island позволяет реализовать следующие архитектуры функциональной безопасности:

- Останов SIL, категория останова 0, категория электроснабжения 1³⁰
- Останов SIL, категория останова 0, категория электроснабжения 2
- Останов SIL, категория останова 1, категория электроснабжения 2
- Останов SIL, категория останова 0, категория электроснабжения 3/4
- Останов SIL, категория останова 1, категория электроснабжения 3/4

30. Уровень полноты безопасности согласно стандарту МЭК 61508. Категории электроснабжения 1, 2 и 3/4 согласно стандарту ISO 13849. Категории останова 0 и 1 согласно стандарту EN/МЭК 60204-1.

Останов SIL, категория останова 0, категория электроснабжения 1

рисунок 19 - Пример: Останов SIL, категория останова 0, категория электроснабжения 1³¹

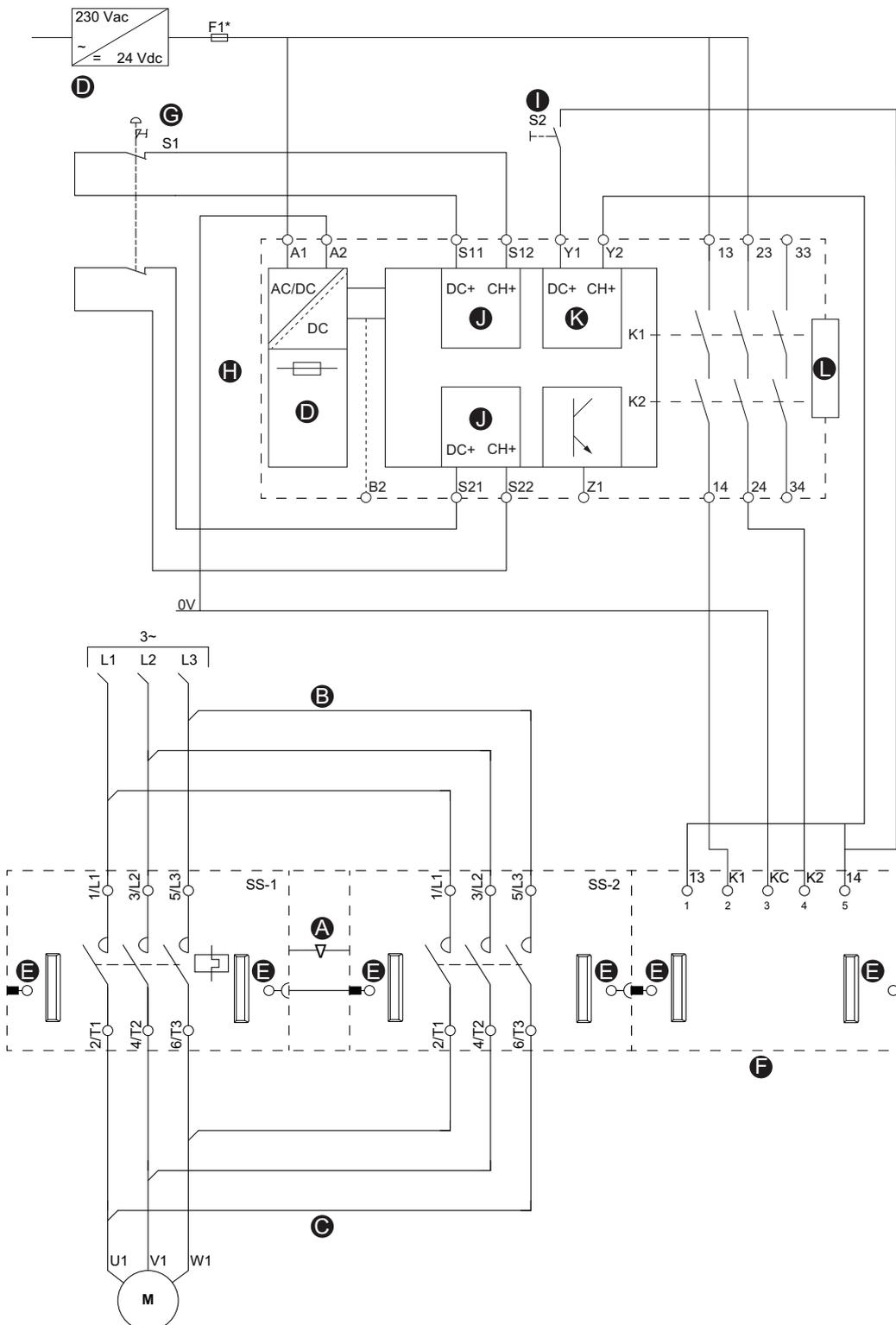


A	Механическая блокировка	D	Кнопка аварийного останова (S1)
B	Параллельная связь	E	Разъем плоского кабеля
C	Реверсная связь	F	Интерфейсный модуль SIL (SIM)

31. Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 1 согласно стандарту ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

Останов SIL, категория останова 0, категория электроснабжения 2

рисунок 20 - Пример: Останов SIL, категория останова 0, категория электроснабжения 2³²



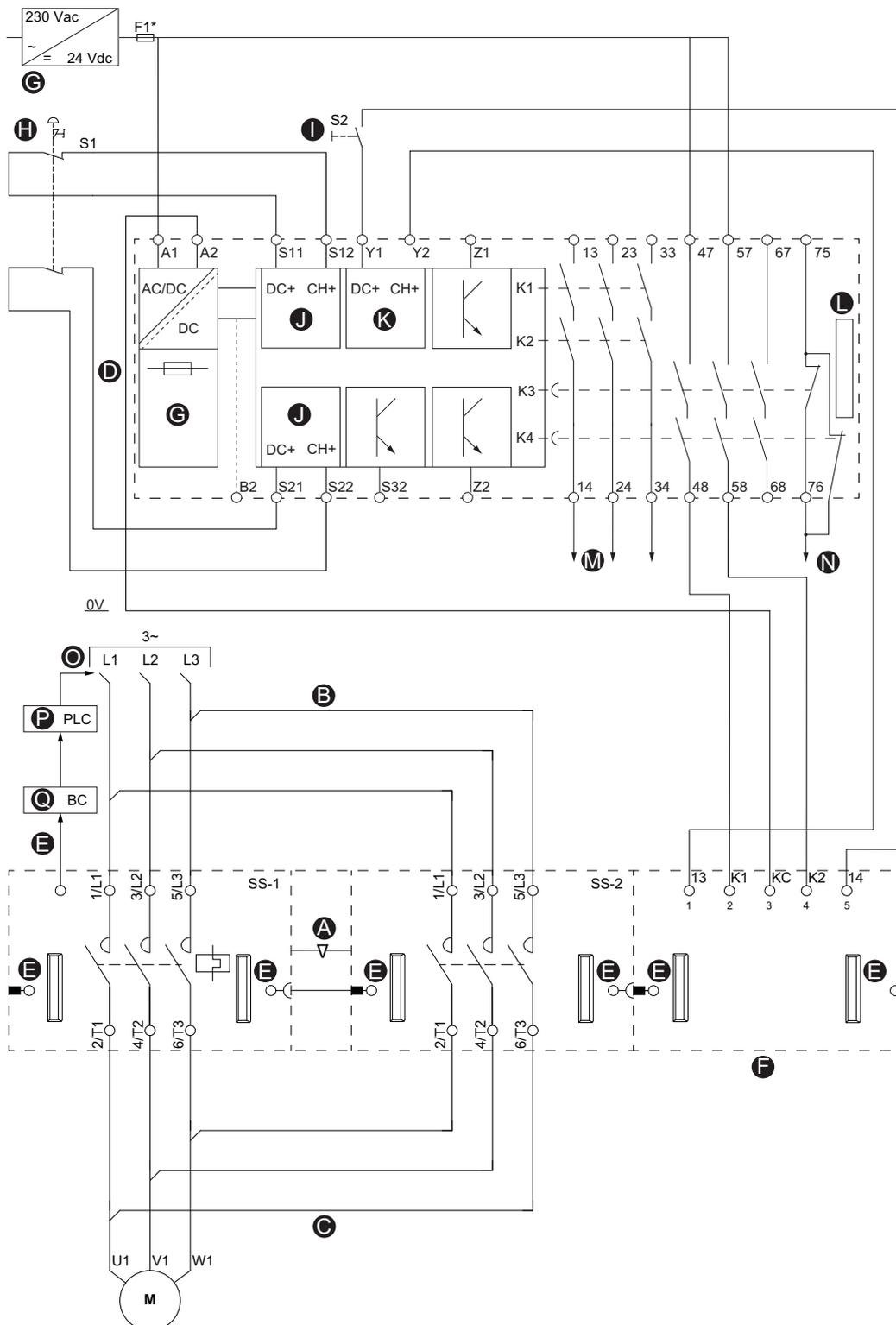
32. Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 2 согласно стандарту ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

Таблица 12 - Легенда для Пример: Останов SIL, категория останова 0, категория электроснабжения 2, стр. 46

A	Механическая блокировка	G	Кнопка аварийного останова (S1)
B	Параллельная связь	H	Модуль Preventa XPS-UAF
C	Реверсная связь	I	Кнопка пуска (S2)
D	Источник питания	J	Вход
E	Разъем плоского кабеля	K	Пуск
F	Интерфейсный модуль SIL (SIM)	L	Расширение

Останов SIL, категория останова 1, категория электроснабжения 2

рисунок 21 - Пример: Останов SIL, категория останова 1, категория электроснабжения 2³³



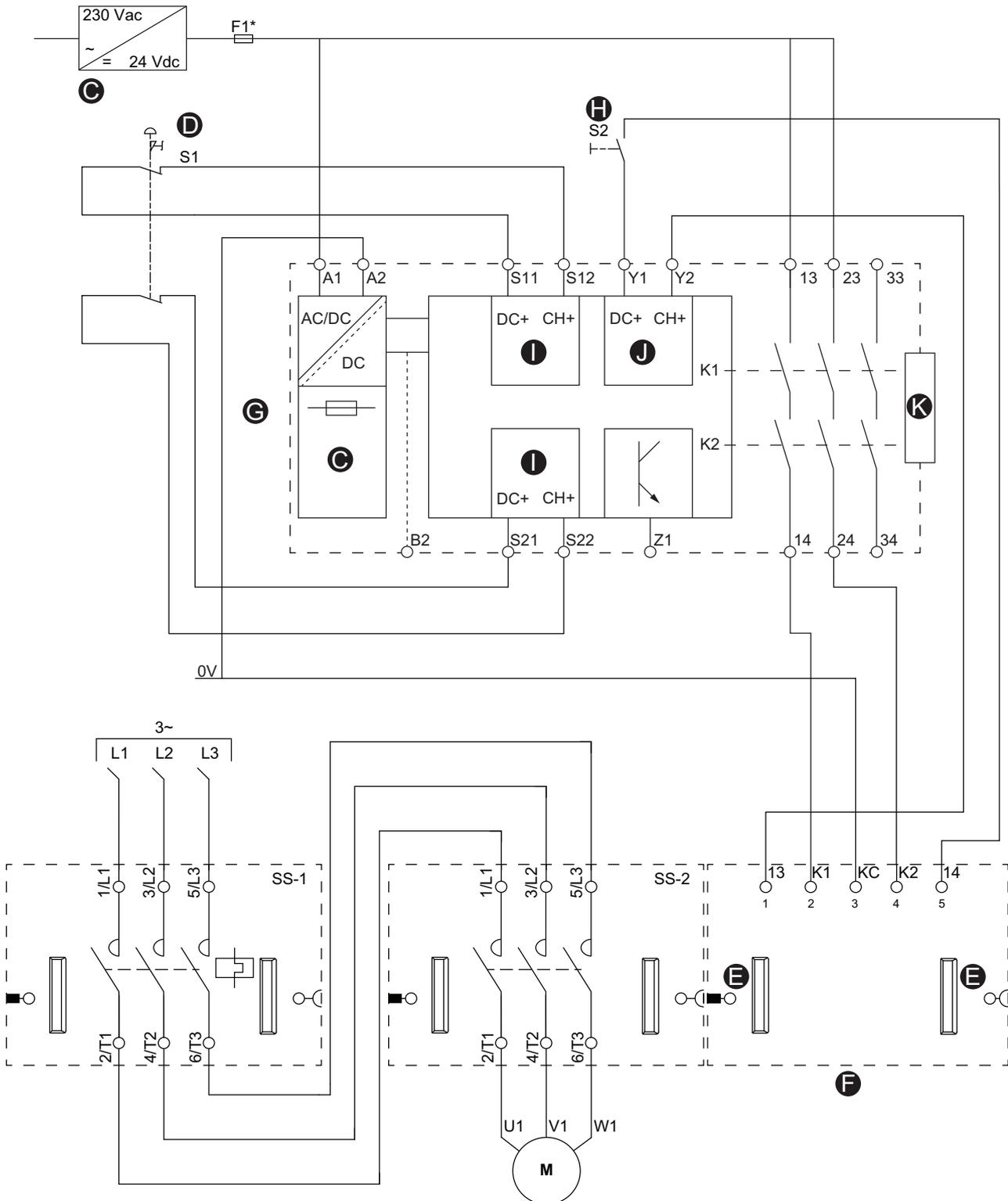
33. Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 2 согласно стандарту ISO 13849. Категория останова 1 согласно стандарту EN/МЭК 60204-1.

Таблица 13 - Легенда для Пример: Останов SIL, категория останова 1, категория электроснабжения 2, стр. 48

A	Механическая блокировка	J	Вход
B	Параллельная связь	K	Пуск
C	Реверсная связь	L	Расширение
E	Разъем плоского кабеля	M	Контролируемый останов
F	Интерфейсный модуль SIL (SIM)	N	Категория останова 1
G	Источник питания	O	Автоматический выключатель на входе
H	Кнопка аварийного останова (S1)	P	ПЛК
I	Кнопка запуска S2	Q	Модуль удаленного подключения

Останов SIL, категория останова 0, категория электроснабжения 3/4

рисунок 22 - Пример: Останов SIL, категория останова 0, категория электроснабжения 3/4³⁴



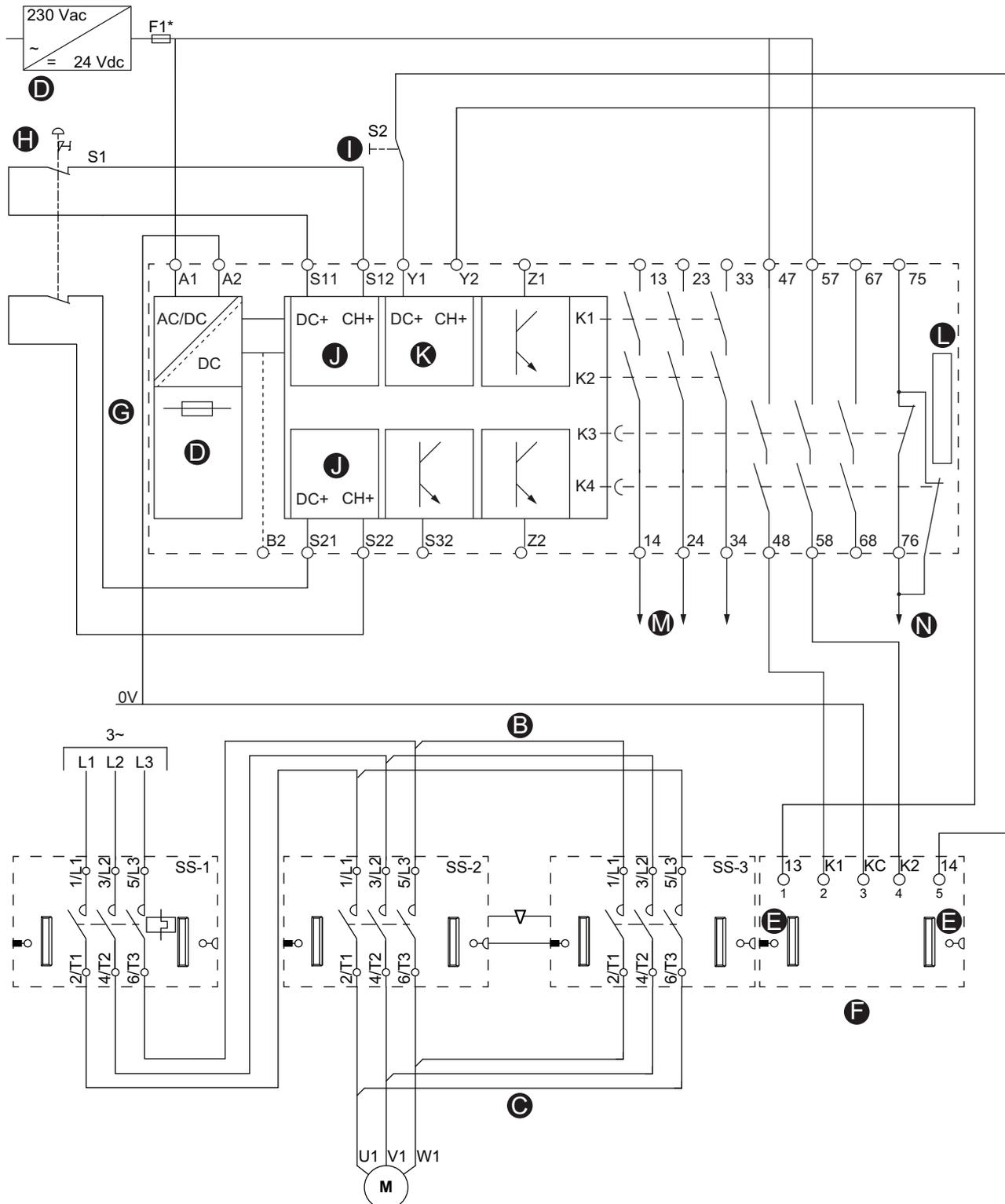
34. Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 3/4 согласно стандарту ISO 13849. Категория останова 0 согласно стандарту EN/МЭК 60204-1.

Таблица 14 - Легенда для Пример: Останов SIL, категория останова 0, категория электроснабжения 3/4, стр. 50

C	Источник питания	H	Кнопка пуска (S2)
D	Кнопка аварийного останова (S1)	I	Вход
E	Разъем плоского кабеля	J	Пуск
F	Интерфейсный модуль SIL (SIM)	K	Расширение
G	Модуль Preventa XPS-UAF		

Останов SIL, категория останова 1, категория электроснабжения 3/4

рисунок 23 - Пример: Останов SIL, категория останова 1, категория электроснабжения 3/4³⁵



35. Уровень полноты безопасности согласно стандарту МЭК 61508. Категория электроснабжения 3/4 согласно стандарту ISO 13849. Категория останова 1 согласно стандарту EN/МЭК 60204-1.

Таблица 15 - Легенда для Пример: Останов SIL, категория останова 1, категория электроснабжения 3/4, стр. 52

B	Параллельная связь	I	Кнопка запуска S2
C	Реверсная связь	J	Вход
D	Источник питания	K	Пуск
E	Разъем плоского кабеля	L	Расширение
F	Интерфейсный модуль SIL (SIM)	M	Контролируемый останов
G	Модуль Preventa XPS-UAF	N	Категория останова 1
H	Кнопка аварийного останова (S1)		

Технические характеристики

Интерфейсный модуль SIL

Таблица 16 - Расчетные значения SIL³⁶ Интерфейсный модуль (SIM)

Архитектура	SIM					
	PFH ³⁷	PFD ³⁸	SFF ³⁹	HFT ⁴⁰	MTTF _d (лет)	DC ⁴¹
Категория электроснабжения 1 ⁴²	2,10 ⁻¹⁰	2,10 ⁻⁵	90 %	1	17 459	Не касается
Категория электроснабжения 2			> 99 %			90%
Категория электроснабжения 3			> 99 %			90%
Категория электроснабжения 4			99%			99%

Примечание: Значения PFD и PFH рассчитываются для следующих условий:

- Интервал испытаний = 20 лет
- MTTR⁴³ = MRT⁴⁴ = 24 часа

Архитектурные требования, приведенные в табл. 3 МЭК 61508-2 и в табл. 5 EN 62061, выполнены для уровней до SIL 3.

Пускатель SIL

Для определения уровня производительности пускателей SIL³⁶ используются следующие данные.

B10: 1 000 000

% опасных отказов⁴⁵: 73 %

B10: 1 369 863

Предполагая, что количество операций = 131 400 цикл/год (в среднем 15 цикл/час)

Рассчитанные значения для пускателя SIL приведены в следующих таблицах:

36. Уровень полноты безопасности согласно стандарту МЭК 61508.
 37. Средняя частота опасных отказов [ч⁻¹] в соответствии с МЭК 61508-4
 38. Вероятность опасного отказа при запросе в соответствии с МЭК 61509-4.
 39. Доля безопасных отказов в соответствии с МЭК 61509-4.
 40. Отказоустойчивость аппаратных средств в соответствии с МЭК 61509-4.
 41. Диагностическое покрытие согласно МЭК 61509-4.
 42. Категории электроснабжения 1, 2, 3 и 4 согласно требованиям ISO 13849.
 43. Среднее время ремонта согласно МЭК 61509-4
 44. Средняя продолжительность ремонта согласно МЭК 61509-4
 45. Определение опасных отказов приведено в МЭК 61508-4

Таблица 17 - Пускатель SIL в одноканальной схеме

Категория электроснабжения ⁴⁶	SFF	HFT	MTTF _d (лет)	DC
Категория 1	27%	0	100 лет	Не касается
Категория 2 — непосредственный мониторинг	90%	0	100 лет	≥ 90%

Таблица 18 - Пускатель SIL в двухканальной схеме

Категория электроснабжения	SFF	HFT	MTTF _d (лет)	DC
Категория 3	27%	0	100 лет	≥ 90%
Категория 4	90%	0	100 лет	≥ 99 %

Соответствие показателей PFH_d и PFD пускателей SIL, зависящее от архитектуры и интервала испытаний, приведено в следующей таблице:

Таблица 19 - Пускатели SIL — PFH_d и PFD

Категория электроснабжения	PFH (МЭК 61508)	PFD (МЭК 61508) T _i = 10 лет ⁴⁷	PFD (МЭК 61508) T _i = 5 лет ⁴⁷
Категория 1	1,10E-06	4,80E-02	4,82E-03
Категория 2 — непосредственный мониторинг	1,10E-06	4,82E-03	5,06E-04
Категория 3	4,5E-09	—	1,30E-04
Категория 4	2,5E-10	—	2,5E-06

Архитектурные требования, приведенные в табл. 3 МЭК 61508-2 и в табл. 5 EN 62061, выполнены для уровней до SIL 2.

Для удовлетворения архитектурных ограничений уровня SIL 2 необходима архитектура категории 2 (реализуется посредством прямого мониторинга «зеркальный вход/выход»).

Примечание: Обнаружение отказа и осуществление соответствующих мер реагирования на отказ должно осуществляться до отработки опасной ситуации связанной с безопасностью функцией управления.

46. Категории электроснабжения 1, 2, 3 и 4 согласно требованиям ISO 13849.

47. Интервал тестирования

Данные о надежности

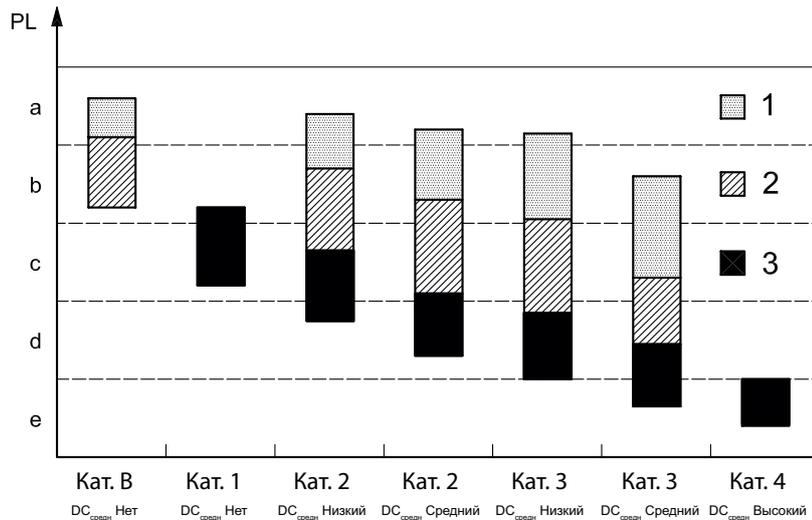
Справочные сведения о стандартах функции безопасности

SIL⁴⁸ Функция останова имеет приоритет относительно останова, запускаемого по эксплуатационным соображениям (EN ISO 13849-1, 5.2.1).

Уровень производительности зависит от категории электроснабжения⁴⁹, MTTF_d и DC_{сред.}

На следующей диаграмме показано положение системы TeSys™ island в зависимости от требований к категории.

рисунок 24 - Положение TeSys island в зависимости от требований к категории



Условные обозначения

PL — уровень эффективности

1 – время MTTF_d каждого канала = низкое

2 – время MTTF_d каждого канала = среднее

3 – время MTTF_d каждого канала = высокое

Таблица 20 - Упрощенная процедура оценки уровня эффективности (PL), обеспечиваемого связанными с безопасностью элементами систем управления (SRP/CS)

Категория	В	1	2	2	3	3	4
DC _{avg}	нет	нет	низкое	среднее	низкое	среднее	высокое
MTTF_d каждого канала							
Низк.	a	Не покрывает	a	b	b	c	Не покрывает
Средн.	b	Не покрывает	b	c	c	d	Не покрывает
Высок.	Не покрывает	c	v	d	d	d	e

Согласно архитектуре TeSys island и категории электроснабжения основные показатели (DC_{avg}, MTTF_d, PL) системы TeSys island соответствуют значениям, показанным в таблице ниже.

48. Уровень полноты безопасности согласно стандарту МЭК 61508.

49. Категории электроснабжения согласно ISO 13849.

Таблица 21 - Значения основных показателей для одно- и двухканальной архитектуры

Архитектура системы TeSys island	Категория	Сохранение работоспособности при единичном отказе ⁵⁰	DC _{avg}	MTTF _d каждого канала	Целевой уровень PL
Одноканальная	1	Нет	Нет	Высок. (≥ 30 лет)	c
	2	Нет	От низк. (≥ 60 %) до средн. (≥ 90 %)	От низк. (≥ 3 лет) до высок. (≥ 30 лет)	c, d
Двухканальная	3	Да			c, d, e
	4	Да	Высок (≥ 99 %)	Высок. (≥ 30 лет)	e

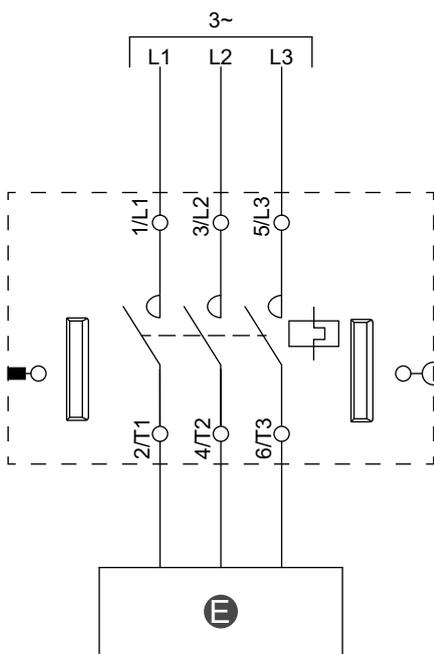
Схемы электропроводки аватаров SIL

В данном разделе приведены схемы электропроводки для аватаров SIL⁵¹. В следующей таблице показаны условные обозначения, используемые на схемах этого раздела.

Таблица 22 - Условные обозначения на схемах электропроводки

A	Механическая блокировка
B	Параллельная связь
C	Реверсная связь
E	Электрическая цепь

рисунок 25 - Выключатель - останов SIL, кат. 1/2⁵²

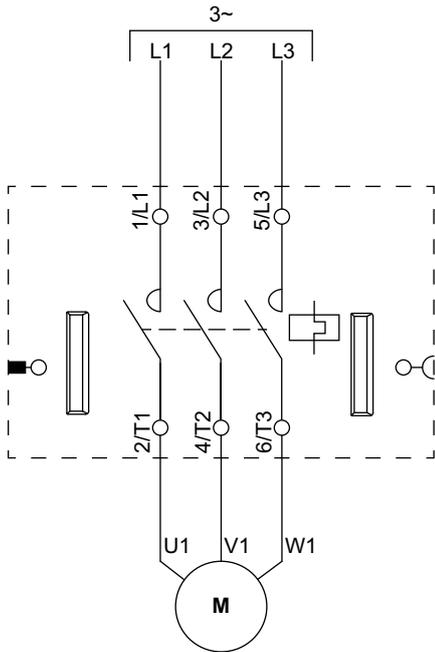


50. Сохранение работоспособности при единичном отказе означает, что единичный отказ (в том числе события по общим причинам) не должен приводить к потере функции безопасности.

51. Уровень полноты безопасности согласно стандарту МЭК 61508.

52. Категория электроснабжения 1 и 2 согласно стандарту ISO 13849.

рисунки 26 - Двигатель, одно направление вращения - останов SIL, кат. 1/2



рисунки 27 - Двигатель, два направления вращения - останов SIL, кат. 1/2

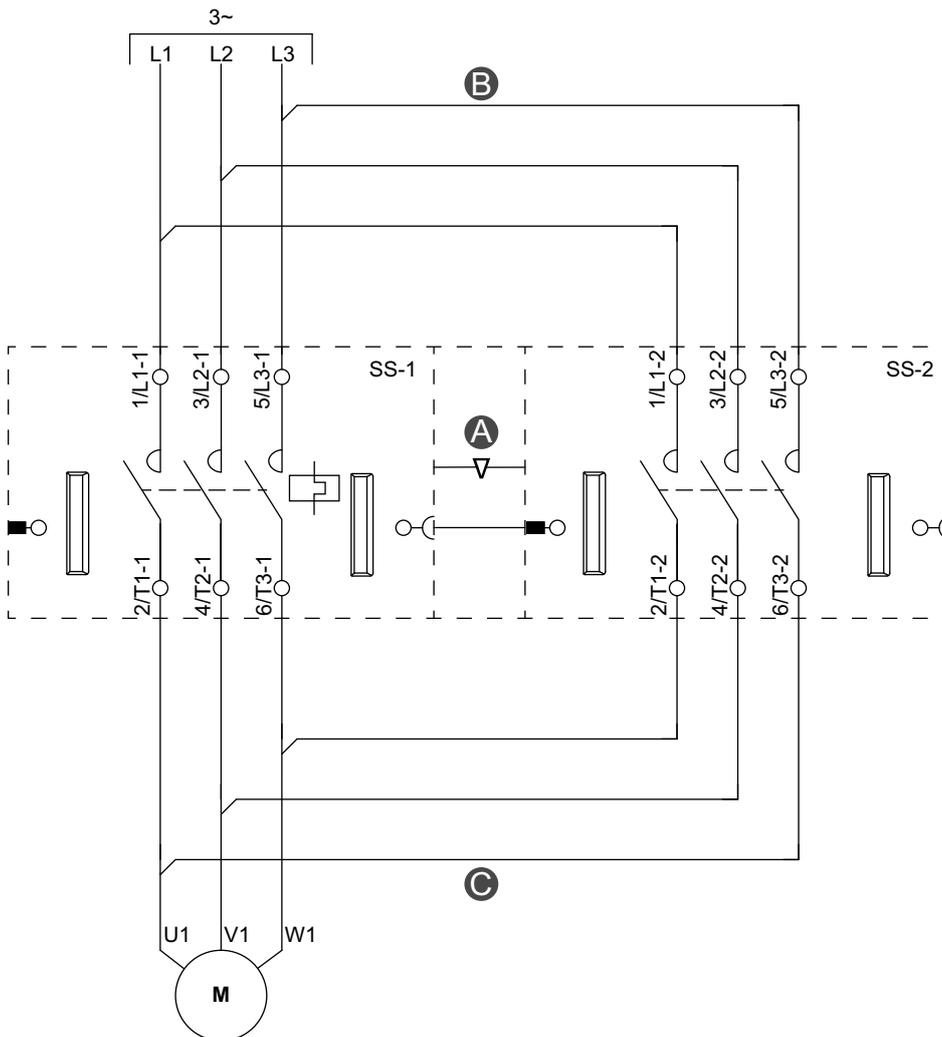


рисунок 28 - Двигатель двухскоростной - останов SIL, кат. 1/2

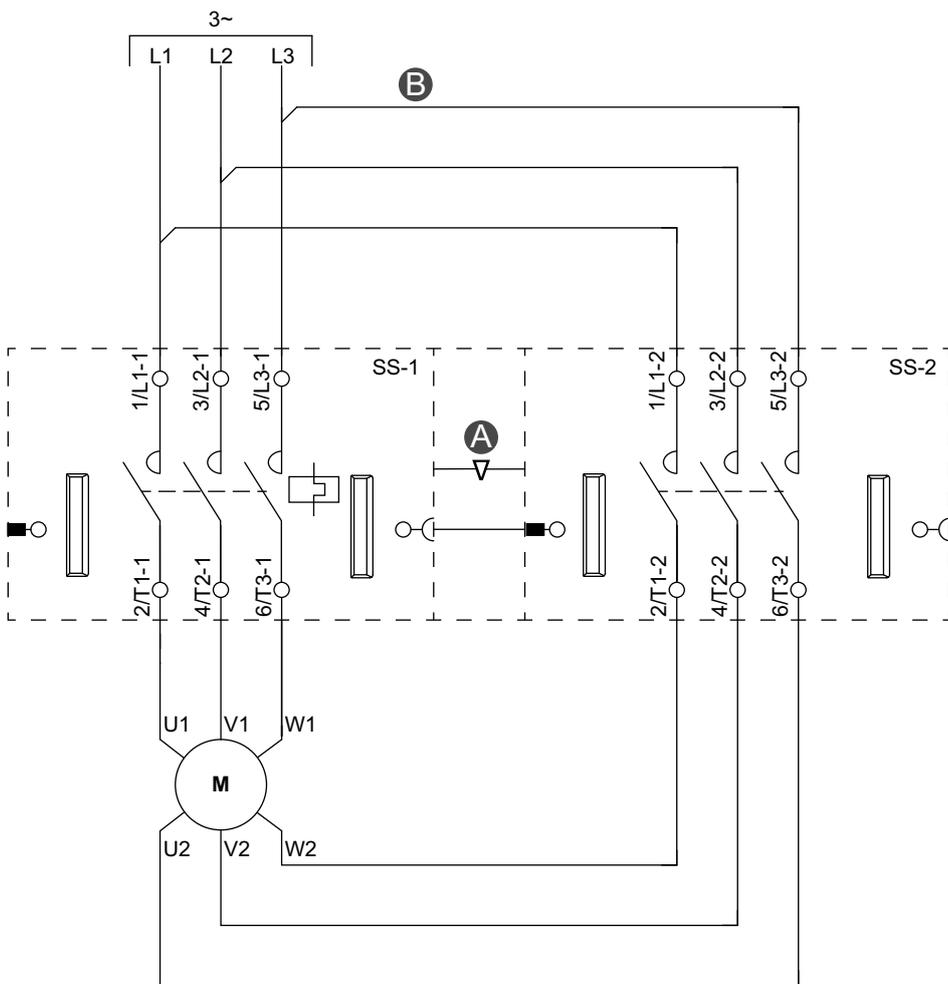
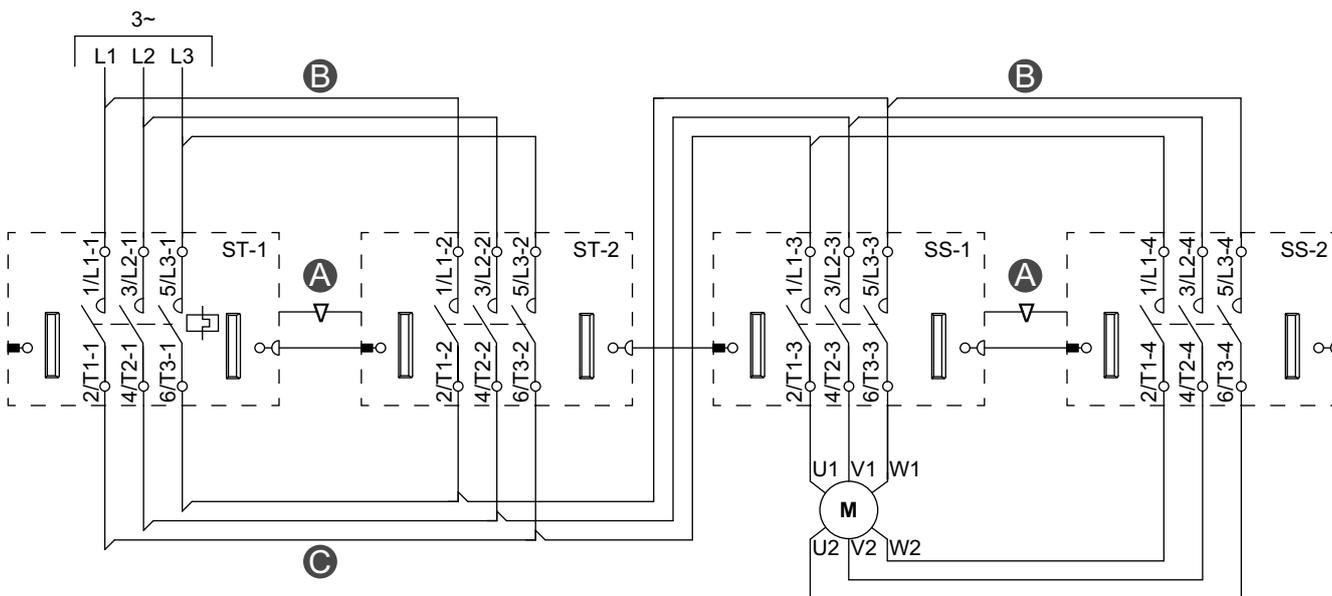
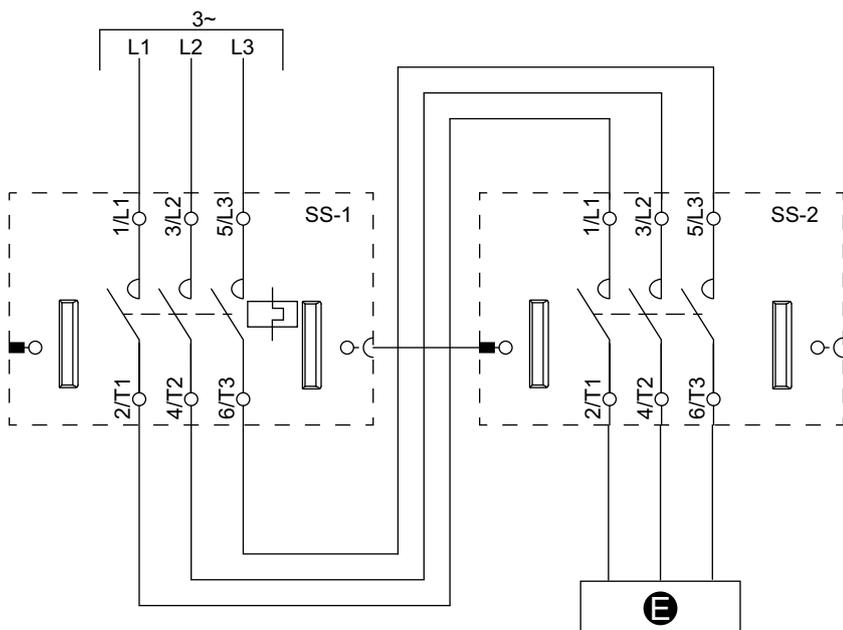
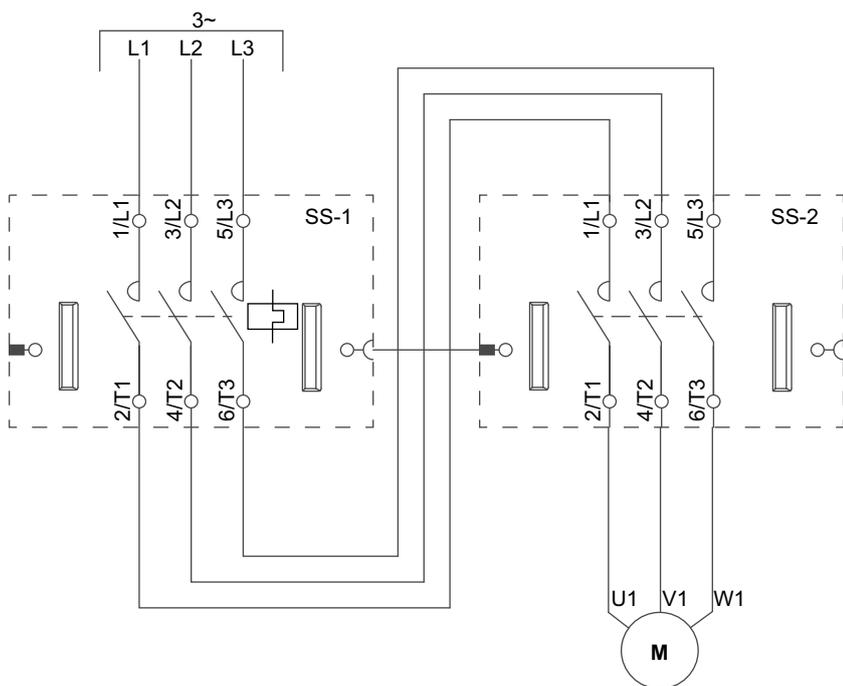


рисунок 29 - Двигатель двухскоростной, два направления вращения - останов SIL, кат. 1/2



рисунки 30 - Выключатель - останов SIL, кат. 3/4⁵³

рисунки 31 - Двигатель, одно направление вращения - останов SIL, кат. 3/4



53. Категории электроснабжения 3 и 4 согласно стандарту ISO 13849.

рисунок 32 - Двигатель, два направления вращения - останов SIL, кат. 3/4

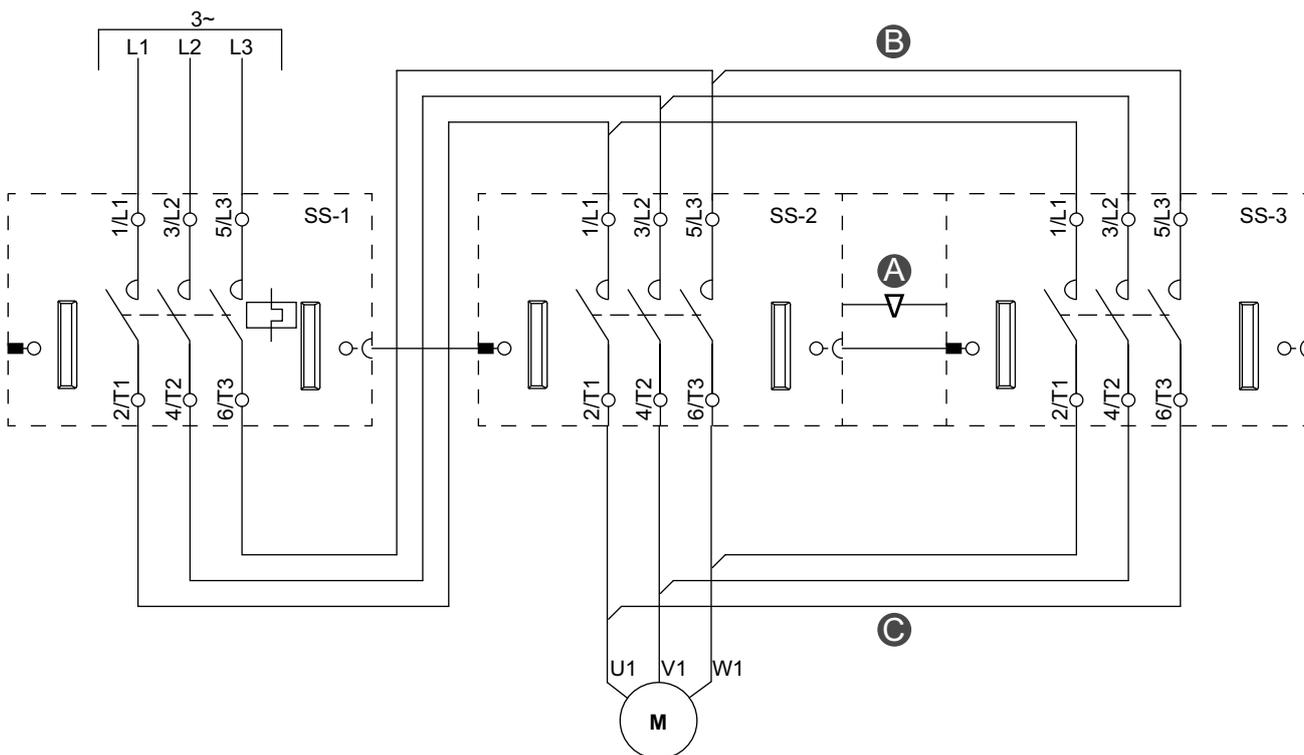


рисунок 33 - Двигатель двухскоростной - останов SIL, кат. 3/4

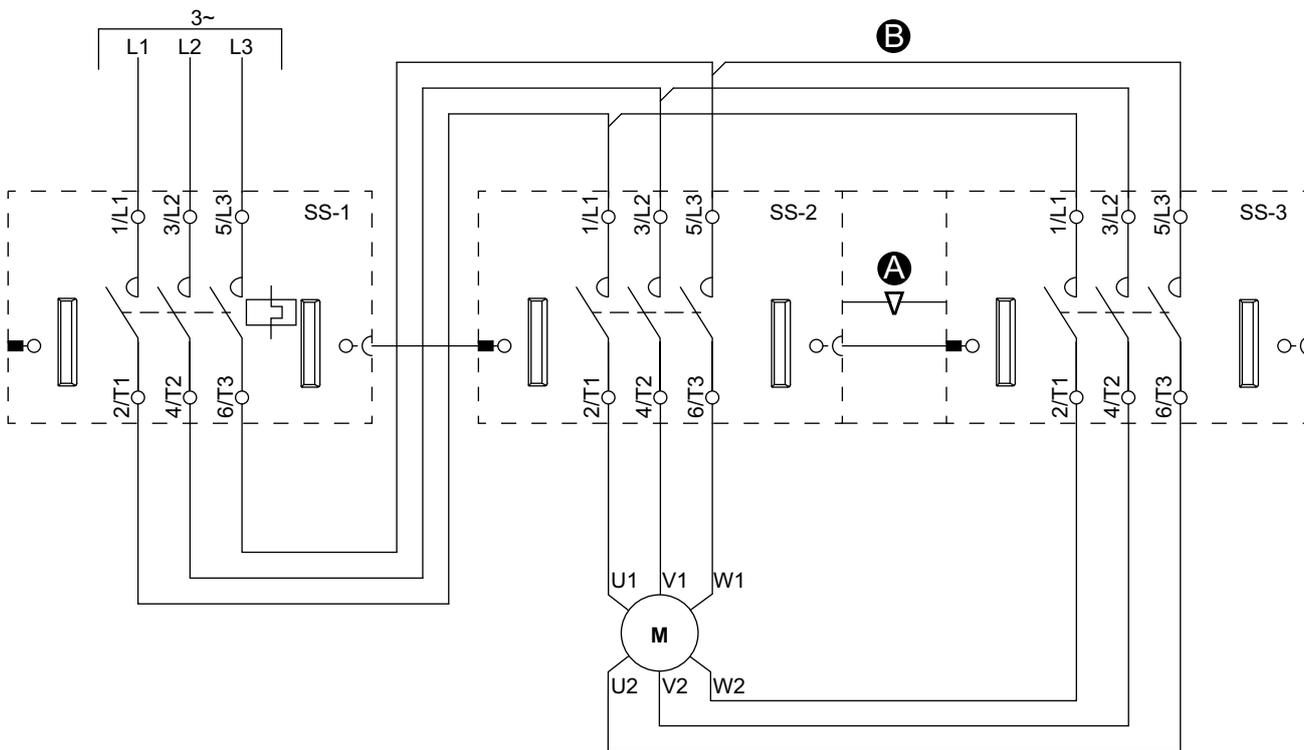


рисунок 34 - Двигатель двухскоростной, два направления вращения - останов SIL, кат. 3/4

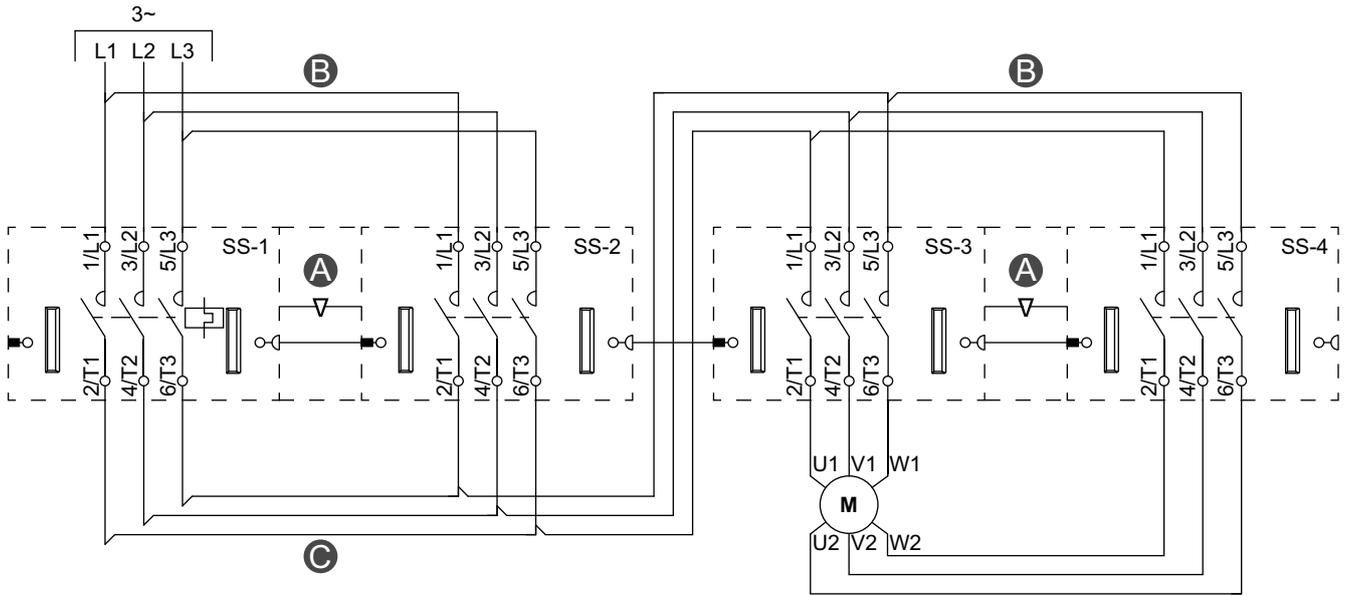


рисунок 35 - Конвейер, одно направление вращения - останов SIL, кат. 1/2

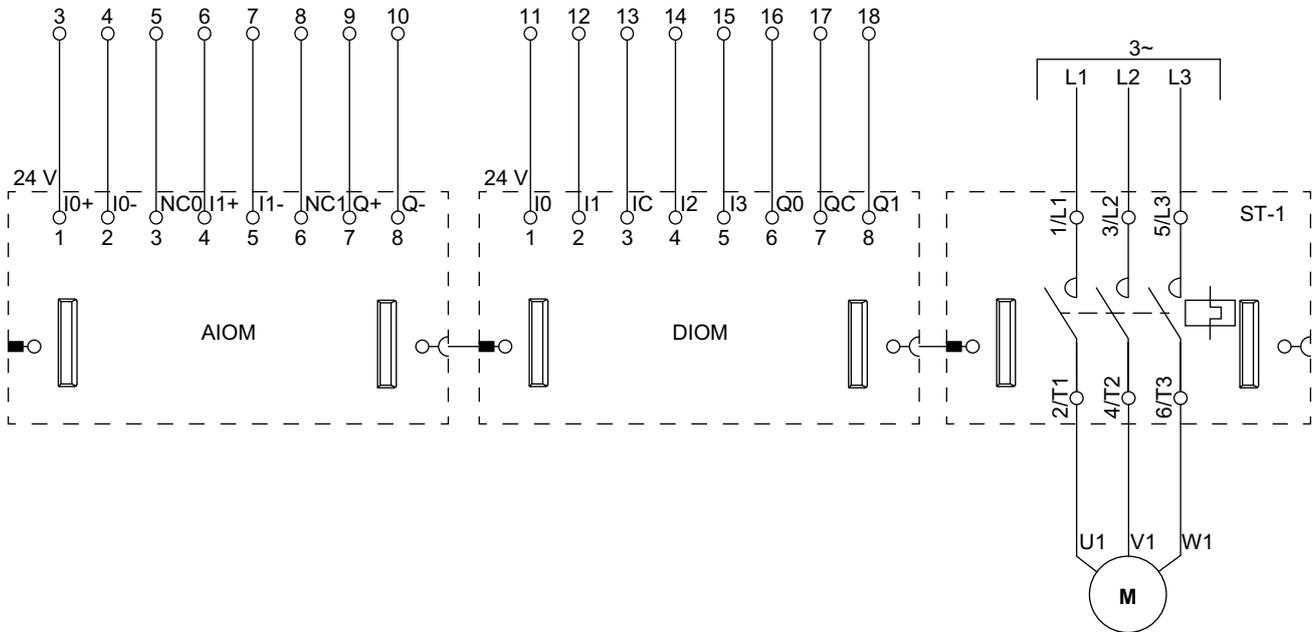
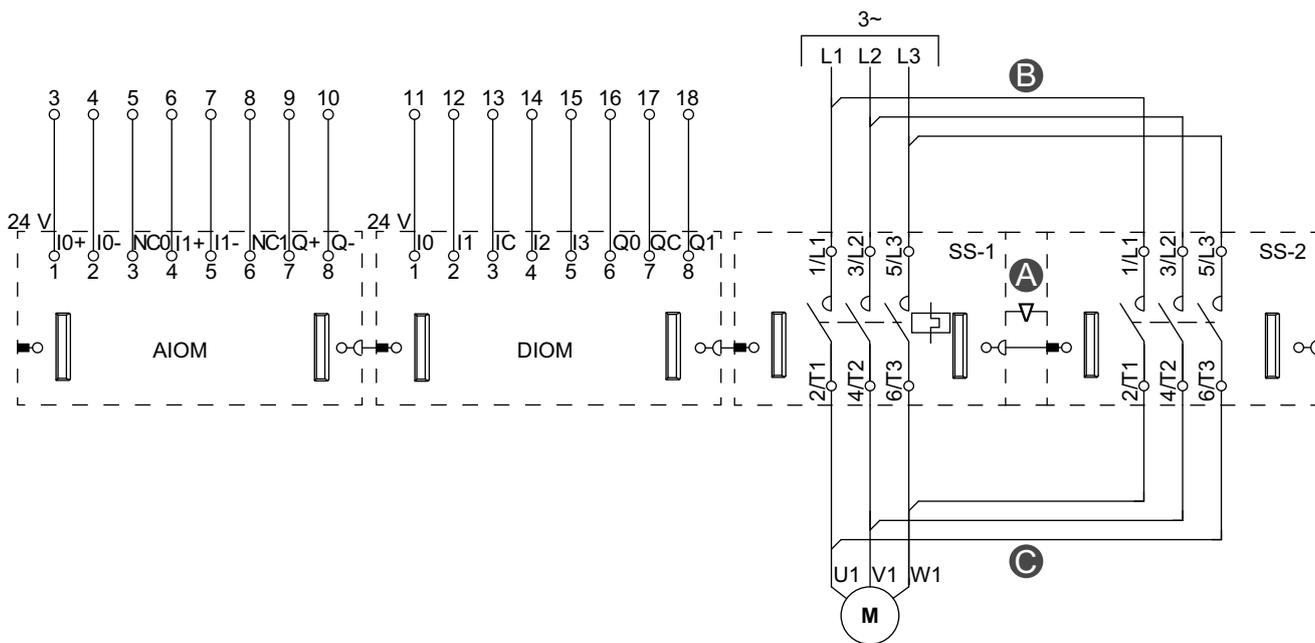


рисунок 36 - Конвейер, два направления вращения - останов SIL, кат. 1/2



Ввод функции безопасности в эксплуатацию

Для ввода функции безопасности в эксплуатацию выполните следующую процедуру. Данная процедура состоит из двух этапов:

- тестирование монтажа;
- проверочные испытания функции безопасности⁵⁴.

Тестирование монтажа

Для испытания монтажа функции безопасности выполните действия, приведенные в следующей таблице.

Таблица 23 - Тестирование монтажа

1	С помощью панели ДИАГНОСТИКА инструмента DTM системы TeSys™ island проверьте соответствие физической топологии логической.
2	В разделе ПАРАМЕТРЫ АВАТАРА панели МОЙ АВАТАР инструмента DTM системы TeSys island убедитесь, что аватары SIL ⁵⁵ связаны с соответствующей группой SIL.

Проверочное испытание функции безопасности

Проверочное испытание функции безопасности производится для каждой группы SIL⁵⁵ в системе. Группа SIL может состоять из нескольких аватаров SIL, управляемых одним интерфейсным модулем SIL (SIM).

Проверочное испытание функции безопасности считается успешно пройденным, если при активации устройства аварийного останова, связанного с группой SIL, все пускатели SIL, относящиеся к этой группе SIL, переходят в безопасное состояние (подача энергии на нагрузку прекращается).

Примечание: Для категории останова 0 (неконтролируемый останов) останов должен быть немедленным. Для категории останова 1 (контролируемый останов) останов эффективен после задержки.⁵⁶

Для проведения проверочного испытания функции безопасности выполните приведенные в следующей таблице действия для каждой группы SIL системы.

54. Определение проверочных испытаний приведено в МЭК IEC 62061

55. Уровень полноты безопасности согласно стандарту МЭК 61508.

56. Категория останова 0 и 1 согласно EN/МЭК 60204-1.

Таблица 24 - Проверочное испытание функции безопасности

1	<p>Приведите в действие связанное с группой SIL устройство аварийного останова и убедитесь, что все относящиеся к этой группе пускатели SIL переходят в безопасное состояние (подача энергии на нагрузку прекращается).</p> <p>Примечание: На пускателях SIL должны мигать красным светодиодные индикаторы «Состояние устройства» (DS), что означает состояние незначительного события устройства.</p> <p>Если испытание не пройдено:</p> <ul style="list-style-type: none"> • возможно, устройство аварийного останова подключено не к тому модулю SIM. Проверьте коммутацию. • возможно, устройство аварийного останова подключено к модулю SIM неправильно. Проверьте коммутацию. • возможно, какие-то аватары SIL не связаны с соответствующей группой SIL. Проверьте конфигурацию.
2	<p>На панели АВАТАРЫ инструмента DTM или OMT системы TeSys™ в разделе ДИАГНОСТИКА проверьте СТАТУС и ЖУРНАЛЫ СОБЫТИЙ, чтобы убедиться, что параметр Состояние группы SIL имеет значение «Команда останова». В журнале событий должна быть запись «SIL Group Stop cmd» (команда останова группы SIL).</p> <p>Если испытание не пройдено:</p> <ul style="list-style-type: none"> • возможно, какие-то аватары SIL не связаны с соответствующей группой SIL. Проверьте конфигурацию.
3	<p>В разделе УСТРОЙСТВА панели ДИАГНОСТИКА убедитесь что параметр Состояние интерфейсного модуля SIL (SIM) имеет значение «Команда останова». В журнале событий должна быть запись «SIL Group Stop cmd» (команда останова группы SIL).</p> <p>Если испытание не пройдено:</p> <ul style="list-style-type: none"> • возможно, устройство аварийного останова подключено не к тому модулю SIM. Проверьте коммутацию. • возможно, устройство аварийного останова подключено к модулю SIM неправильно. Проверьте коммутацию.
4	<p>Примените команду пуска к аватару SIL соответствующей группы SIL и убедитесь, что запуск не будет выполнен: пускатели должны оставаться разомкнутыми и команда пуска должна игнорироваться до тех пор, пока не будет выполнен сброс устройства аварийного останова.</p> <p>Если испытание не пройдено:</p> <ul style="list-style-type: none"> • возможно, какие-то аватары SIL не связаны с соответствующей группой SIL. Проверьте конфигурацию. <p>Если любые из этих испытаний, несмотря на устранение ошибок, не будут успешно пройдены, эксплуатация системы недопустима. Замените устройства, не прошедшие испытания.</p>
5	<p>После того как проверочное испытание функции безопасности будет успешно пройдено, выполните сброс устройства аварийного останова и убедитесь, что все пускатели SIL и интерфейсные модули SIL перешли в состояние готовности (светодиодный индикатор DS непрерывно светится зеленым).</p>

Требования к техническому обслуживанию функции безопасности

В этом разделе описывается процедура технического обслуживания, которая должна регулярно выполняться для поддержания функциональной безопасности TeSys™ island.

График технического обслуживания

Периодичность технического обслуживания зависит от частоты переключения.

- В случае режима низкой частоты переключения (среднее количество циклов переключения контактора за год менее 15 цикл/час) техническое обслуживание требуется проводить раз в 12 месяцев.
- В случае режима высокой частоты переключения (среднее количество циклов переключения контактора за год больше 15 цикл/час или 136 986 цикл/год), техническое обслуживание следует проводить с периодичностью в 1/10 от расчетного срока службы устройства.

Расчетный срок службы устройств (лет) = $V10d$ (= 1 369 863) / среднее количество циклов переключения контактора в год

Проверки в рамках технического обслуживания

Проверки использования устройств

Чтобы убедиться, что количество выполненных контактором пускателя SIL⁵⁷ циклов находится в пределах допустимых для срока службы значений, произведите проверки, описанные в следующей таблице.

1	С помощью функции ДИАГНОСТИКА устройств инструмента DTM или OMT системы TeSys™ island получите сведения о ресурсах устройств для каждого пускателя SIL.
2	Если значение Количество циклов контактора больше $V10d$ (= 1 369 863), пускатель SIL необходимо заменить.
3	Если нет, запланируйте следующее техническое обслуживание согласно значению Количество циклов контактора . См. График технического обслуживания, стр. 66.

Проверочное испытание функции безопасности

Выполните проверочное испытание функции безопасности для каждой группы SIL⁵⁷. См. Проверочное испытание функции безопасности, стр. 64.

57. Уровень полноты безопасности согласно стандарту МЭК 61508.

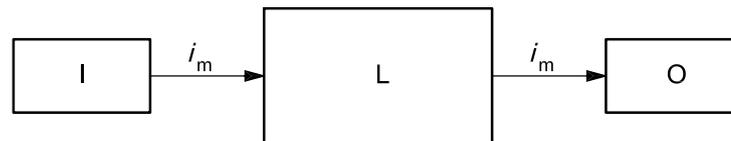
Приложение. Одноканальная архитектура

Эта одноканальная архитектура охватывает категории электроснабжения 1 и 2.

Архитектурные требования для категории электроснабжения 1

Предусмотренная для **категории 1** архитектура определена в стандарте EN ISO 13849–1, 4.2.6.

рисунок 37 - Предусмотренная для категории 1 архитектура (EN ISO 13849–1)



I: устройство на входе

L: логика

O: устройство на выходе

i_m : средства соединения

Проектирование и реализация SRP/CS, связанной с безопасностью части системы управления, для категории электроснабжения 1 должно осуществляться с использованием **достоверно испытанных компонентов**.

Достоверно испытанным компонентом для связанных с безопасностью задач является компонент, который:

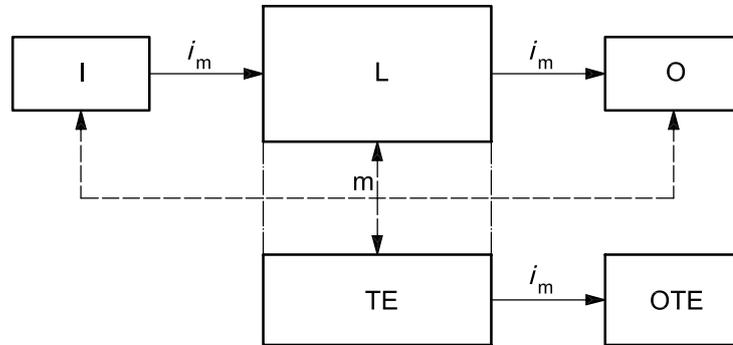
- либо является широко используемым в прошлом для аналогичных задач и показал положительные результаты; либо
- изготовлен и проверен с использованием принципов, которые показывают его пригодность и надежность для задач, связанных с безопасностью.

Для систем категории 1 **диагностического покрытия не требуется** ($DC_{avg} = \text{нет}$).

Архитектурные требования для категории электроснабжения 2

Предусмотренная для категории 2 архитектура определена в стандарте EN ISO 13849–1, 5.2.6.

рисунок 38 - Предусмотренная для категории 2 архитектура (EN ISO 13849–1)



I: устройство на входе

m: мониторинг

L: логика

TE: тестовое оборудование

O: устройство на выходе

OTE: выход TE

i_m: средства соединения

SRP/CS, связанная с безопасностью часть системы управления, категории электроснабжения 2 должна быть спроектирована таким образом, чтобы проверка ее функции осуществлялась системой управления машины с соответствующей периодичностью.

В одноканальной архитектуре интерфейсный модуль SIM связан с пускателем SIL⁵⁸

В частности, для категории электроснабжения 2 зеркальный контакт подключается к модулю Preventa™ XPS (или аналогичному). Если состояние канала обратной связи зеркального контакта не соответствует состоянию на выходе модуля Preventa XPS (или аналогичного), то модуль Preventa XPS (или аналогичный) блокирует второй пуск.

Примечание: Состояние зеркального контакта служит только для диагностики.

58. Уровень полноты безопасности согласно стандарту МЭК 61508.

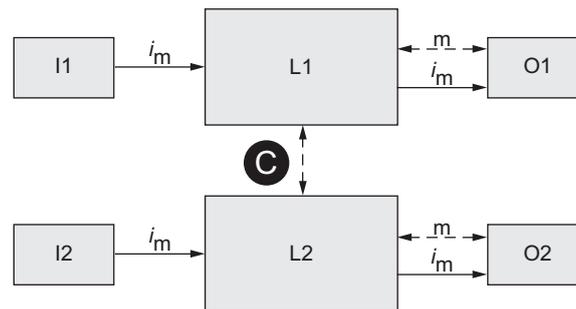
Приложение: Двухканальная архитектура

Эта двухканальная архитектура охватывает категории электроснабжения 3 и 4.

Архитектурные требования для категории электроснабжения 3

Предусмотренная для категории 3 архитектура определена в стандарте EN ISO 13849–1, 6.2.6.

рисунок 39 - Предусмотренная для категории 3 архитектура (EN ISO 13849-1)



i_m : средства соединения

c : перекрестный мониторинг

$I1, I2$: устройство ввода, например датчик

$L1, L2$: логика

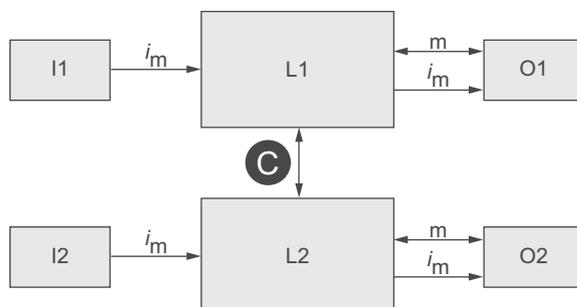
m : мониторинг

$O1, O2$: выходное устройство, например главный контактор

Архитектурные требования для категории электроснабжения 4

Предусмотренная для категории 4 архитектура определена в стандарте EN ISO 13849–1, 7.2.6.

рисунок 40 - Предусмотренная для категории 4 архитектура (EN ISO 13849-1)



i_m : средства соединения

c: перекрестный мониторинг

I1, I2: устройство ввода, например датчик

L1, L2: логика

m: мониторинг

O1, O2: выходное устройство, например главный контактор

Сплошные линии мониторинга представляют диагностическое покрытие, которое превосходит предусмотренную для категории 3 архитектуру.

Глоссарий

А

Средняя частота опасных отказов [ч⁻¹] (PFH). (Определение опасных отказов приведено в МЭК 61508-4)

Для поддержания функции безопасности стандарт МЭК 61508 устанавливает различные уровни мер, необходимых для предотвращения и контроля выявленных ошибок, в зависимости от необходимого уровня SIL⁵⁹.

Все компоненты функции безопасности должны проходить оценку вероятности для определения эффективности мер, реализованных для управления выявленными отказами.

В ходе такой оценки определяется показатель PFH (средняя частота опасных отказов⁶⁰ [ч⁻¹]) для связанной с безопасностью системы. Он отражает вероятность того, что в течение часа связанная с безопасностью система выйдет из строя опасным образом и функция безопасности не сможет быть правильно отработана.

В зависимости от уровня SIL значение PFH не должно превышать определенных значений для связанной с безопасностью системы в целом.

Отдельные значения PFH для элементов цепочки функций суммируются. Результат не должен превышать максимальное значение, предусмотренное стандартом.

Уровень полноты безопасности	Средняя частота опасных отказов ⁶⁰ [ч ⁻¹] (PFH) при высокой частоте запросов или непрерывных запросах
4	$10^{-9} \leq \text{---} < 10^{-8}$
3	$10^{-8} \leq \text{---} < 10^{-7}$
2	$10^{-7} \leq \text{---} < 10^{-6}$
1	$10^{-6} \leq \text{---} < 10^{-5}$

Е

Стандарт EN ISO 13849

Данный европейский стандарт определяет процесс проверки, в том числе анализ опасности, оценку рисков и процедуру испытаний функций безопасности, а также категории связанных с безопасностью элементов систем управления. Описания функций безопасности и предъявляемые в зависимости от категории требования приведены в стандарте ISO 13849-1, охватывающем общие принципы проектирования. Часть требований к проверке носят общий характер, а часть касаются только конкретных используемых технологий. В стандарте EN ISO 13849-2 также определены условия, при которых проверка должна выполняться путем испытания связанных с безопасностью элементов систем управления.

Стандарт EN/МЭК 60204-1

Категория останова 0 определяется как функция «останова путем немедленного прекращения подачи напряжения на приводные устройства машины (т. е. неконтролируемый останов)».

Категория останова 1 определяется как: «управляемый останов при наличии питания на приводах машины до достижения останова и отключении питания после останова».

59. Уровень полноты безопасности согласно стандарту МЭК 61508.

60. Определение опасных отказов приведено в МЭК 61508-4

F

Меры по предупреждению отказов

Систематических ошибок в спецификациях, аппаратных средствах и программном обеспечении, а также связанных с эксплуатацией и техническим обслуживанием отказов в связанной с безопасностью системе необходимо максимально избегать. Для выполнения этих требований стандартом МЭК 61508 предусмотрен ряд мер по предупреждению отказов, необходимость реализации которых зависит от требуемого уровня SIL⁶¹. Эти меры по предупреждению отказов охватывают весь жизненный цикл связанной с безопасностью системы — от проектирования до вывода из эксплуатации.

Функциональная безопасность

Проектирование автоматизации и функциональной безопасности ранее были совершенно разными областями, но в последнее время становятся все более взаимосвязанными.

Проектирование и монтаж сложных решений автоматизации за счет интегрированных функций безопасности упрощается.

Обычно инженерные требования к функциональной безопасности зависят от назначения.

Уровень требований зависит от потенциальных рисков и опасностей, связанных с конкретной задачей.

H

Отказоустойчивость аппаратных средств (HFT) и доля безопасных отказов (SFF)

В зависимости от уровня SIL⁶¹ связанной с безопасностью системы, стандартом МЭК 61508 устанавливаются конкретные требования к отказоустойчивости аппаратных средств (HFT) в сочетании с определенными требованиями к доле безопасных отказов, обозначаемой как SFF (доля безопасных отказов).

Показатель HFT отражает способность системы выполнять необходимую функцию безопасности независимо от возникновения одного или нескольких отказов аппаратных средств.

Показатель SFF системы определяется как отношение частоты безопасных отказов к частоте отказов системы в целом.

Согласно МЭК 61508 наиболее высокий достижимый уровень SIL системы частично определяется значением HFT и частично значением SFF системы.

Эти типы определяются на основе ряда критериев, определяемых стандартом для связанных с безопасностью элементов.

SFF	HFT подсистемы типа А			HFT подсистемы типа В		
	0	1	2	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3	—	SIL 1	SIL 2
От 60 до < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
От 90 до < 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

61. Уровень полноты безопасности согласно стандарту МЭК 61508.

Стандарт МЭК 61508

Стандарт МЭК 61508 регламентирует функциональную безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью.

Компоненты не рассматриваются по отдельности, а вся цепочка функций (например, от датчика до логических обрабатывающих модулей и привода) оценивается как единое целое.

Эта цепочка функций в целом должна отвечать требованиям определенного уровня полноты безопасности.

L

Режим низкой/высокой частоты запросов

Стандарт МЭК 61508 определяет режим высокой частоты запросов функции безопасности:

- режим высокой частоты запросов или непрерывный режим (PFH);
- режим низкой частоты запросов (PFDavg, PTI).

M

Среднее время до опасного отказа (MTTF_d)

Стандартом ISO 13849-1 MTTF_d определяется как ожидаемое среднее время до опасного отказа.

P

Уровень эффективности (Performance Level, PL)

Стандарт МЭК 13849 определяет пять уровней эффективности (PL) функций безопасности:

Уровень «а» является самым низким, а уровень «е» — самым высоким.

Пять уровней (а, b, c, d и e) соответствуют различным значениям средней вероятности опасного отказа⁶² в час.

Уровень эффективности	Вероятность опасного отказа ⁶² в час
e	От $\geq 10^{-8}$ до $< 10^{-7}$
d	От $\geq 10^{-7}$ до $< 10^{-6}$
c	От $\geq 10^{-6}$ до $< 3 \times 10^{-6}$
b	От $\geq 3 \times 10^{-6}$ до $< 10^{-5}$
a	От $\geq 10^{-5}$ до $< 10^{-4}$

S

Уровень полноты безопасности (SIL)

Стандарт МЭК 61508 определяет четыре уровня полноты безопасности (SIL) функций безопасности:

SIL 1 — самый низкий уровень полноты безопасности, а SIL 4 — самый высокий.

62. Определение опасного отказа приведено в МЭК 61508-4

Анализ опасностей и оценка рисков служат основой для определения требуемого уровня полноты безопасности.

Данный показатель используется для определения, может ли соответствующая цепочка функций считаться функцией безопасности и какую потенциальную опасность она должна покрывать.

Schneider Electric
800 Federal Street
01810 Andover, MA
USA (США)

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

www.schneider-electric.com

Стандарты, спецификации и схемы могут изменяться; обратитесь в компанию за подтверждением актуальности информации, опубликованной в данном руководстве.

© 2021 – Schneider Electric. Все права сохраняются.

85361B1904RU-03