Акционерное Общество
АБС ЗЭиМ Автоматизация

КОНТРОЛЛЕРЫ ИСПОЛНИТЕЛЬНОГО МЕХАНИЗМА КИМ®

Исполнение SIL

Руководство по функциональной безопасности (SIL)

ЯЛБИ.421413.005 Д

Содержание

Лист

Введение 3
1 Сокращения и понятия 3
2 Область применения 5
3 Ввод в эксплуатацию 5
3.1 Принцип работы 5
3.2 Схема подключения 5
3.3 Настройка 7
4 Работа 8
5 Проверка и техническое обслуживание 9
5.1 Общая информация 9
5.2 Проверка неполного хода 9
5.3 Контрольные испытания 11
5.4 Техническое обслуживание 12
6 Параметры безопасности 13

Приложение А. Перечень документов, на которые даны ссылки в настоящем руководстве 15

Настоящее руководство по функциональной безопасности (далее – руководство) распространяется на контроллеры исполнительного механизма КИМ®2, КИМ®3 (далее – контроллеры), применяемые совместно с электрическими приводами и исполнительными механизмами (далее – ЭП) производства ОАО "АБС ЗЭиМ Автоматизация" общепромышленного и взрывозащищенного исполнений, используемыми для перемещения регулирующих и запорно-регулирующих органов арматуры в составе автоматизированных систем управления технологическими процессами.

Настоящее руководство содержит сведения необходимые для эксплуатации ЭП с контроллерами в системах безопасности в соответствии с ГОСТ Р МЭК 61508, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61511.

Перечень документов, на которые даны ссылки в настоящем руководстве, приведен в приложении А.

1 Сокращения и понятия

1.1 Для оценки функций безопасности, в первую очередь, необходимы значения интенсивности отказов, значения PFDavg (средняя вероятность опасного отказа по запросу) и значения SFF (доля безопасных отказов). Краткое описание параметров приведено в таблице 1.

Таблица 1

Параметр	Наименование	Описание
λ_{SD}	Интенсивность обнаруживаемых безопасных отказов (англ. Lambda Safe Detected)	Количество безопасных отказов за единицу времени и выявляются внутренней диагностикой устройства. Отказы считаются безопасными, если в случае их возникновения устройство по-прежнему может выполнять функции безопасности
λ_{SU}	Интенсивность не обнаруживаемых безопасных отказов (англ. Lambda Safe Undetected)	Количество безопасных отказов за единицу времени и не выявляются внутренней диагностикой устройства. Отказы считаются безопасными, если в случае их возникновения, устройство по-прежнему может выполнять функции безопасности
λ_{DD}	Интенсивность обнаруживаемых опасных отказов (англ. Lambda Dangerous Detected)	Количество отказов за единицу времени, приводящие к ошибке выполнения функции безопасности и выявляются внутренней диагностикой устройства
λ_{DU}	Интенсивность не обнаруживаемых опасных отказов (англ. Lambda Dangerous Undetected)	Количество отказов за единицу времени, приводящие ошибке выполнения функции безопасности и не могут быть выявлены внутренней диагностикой устройства
λ_{total}	Общая интенсивность отказов устройства.	Определяется как сумма всех интенсивностей отказов за единицу времени
DC	Охват диагностикой. (англ. Diagnostic Coverage)	Отношение опасных отказов, выявляемых внутренней диагностикой к общей интенсивности отказов
MTBF	Средняя наработка на отказ (англ. Mean time between failures, MTBF)	Средняя продолжительность работы устройства между отказами, то есть показывает, какая наработка в среднем приходится на один отказ. Выражается в часах

Окончание таблицы 1

Параметр	Наименование	Описание
PFD_{avg}	Средняя вероятность опасного отказа по запросу (англ. Average Probability of dangerous Failure on Demand)	Средняя вероятность несрабатывания функции безопасности, когда приходит запрос
SFF	Доля опасных отказов (англ. Safe Failure Fraction)	Свойство устройства определяемое отношением суммы интенсивностей безопасных отказов и опасных обнаруживаемых отказов к сумме интенсивностей безопасных и опасных отказов
T_{proof}	Интервал между контрольными испытаниями	Показатели безопасности действительны для установленного периода работы. По окончании этого периода необходимо проводить контрольные испытания, чтобы убедиться в работоспособности устройства. Обычно T_{proof} = 1 год
MTTR	Среднее время возвращения в исправное состояние после отказа системы. (англ. Mean Time To Restoration)	Среднее время, требуемое для восстановления работоспособности системы безопасности
УПБ (SIL)	Уровень полноты безопасности (англ. Safety Integrity Level)	ГОСТ Р МЭК 61508-1 определяет четыре уровня УПБ
PTC	Охват контрольных испытаний (англ. Proof Test Coverage)	Степень охвата отказов контрольными проверками и эффективность восстановления
HFT	Отказоустойчивость аппаратных средств	Означает, что HFT+1 является минимальным числом отказов, которые могут привести к потере функции безопасности
FIT	Число отказов за время (англ. Failure In Time)	Частота отказов на миллиард часов

2 Область применения

2.1 Настоящее руководство распространяется на ЭП с контроллерами в исполнении SIL, предназначенные для управления промышленной арматурой и сертифицированы для систем безопасности согласно ГОСТ Р МЭК 61508, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61511.

3 Ввод в эксплуатацию

3.1 Принцип работы

3.1.1 ЭП с контроллером рассчитан на работу в режиме низкой интенсивности запросов безопасности и должны использоваться только в этом режиме. Если помимо функции безопасности один и тот же ЭП должен выполнять функцию рабочего устройства, не имеющую отношение к безопасности, не допускается превышение максимально допустимого количества рабочих циклов.

3.1.2 Значение отказоустойчивости (HFT) равно 0.

3.1.3 Функции безопасности ЭП могут рассматриваться, как устройство типа B.

ЭП с контроллером может выполнять следующие функции безопасности:

- "Оставаться на месте" (Stayput) – при наличии сигнала "АВАРИЯ" запрещается движение вала ЭП;
- "Аварийное выключение" – при наличии сигнала "Авария" ЭП переходит в безопасное положение "ОТКРЫТО", "ЗАКРЫТО" или заранее заданное положение.

3.1.4 Для повышения надежности линии сигнала "АВАРИЯ", дискретный вход "АВАРИЯ" должен быть инвертирован. То есть активным уровнем для сигнала "АВАРИЯ" будет "0" – (0-8) В, пассивным "1" – (18-30) В. При этом обрыв линии связи будет восприниматься как "Авария".

Команда "АВАРИЯ" выполняется, если переключатель режимов управления находится в положениях "ДИСТ" или "МЕСТ". В рабочем режиме переключатель режимов управления должен быть установлен в положение "ДИСТ".

3.2 Схема подключения

3.2.1 Схема подключения контроллера КИМ3 к системе безопасности приведена на рисунке 1а.

За нормальное состояние принято следующее состояние контроллера КИМ3 и системы безопасности:

- отсутствуют неисправности;
- система готова к выполнению функции безопасности.

Сигнал "АВАРИЯ" – контакты в нормальном режиме работы замкнуты. В случае аварии их нужно разомкнуть.

Сигнал "ГОТОВНОСТЬ" – контакты в нормальном состоянии замкнуты. Они размыкаются в случае неисправности или если переключатель режимов управления находится в положении "0" или "МЕСТ".

Для питания могут использоваться как внешний, так и внутренний источник питания (контакты 28 и 29).

3.2.2 Схема подключения контроллера КИМ2 к системе безопасности приведена на рисунке 1б.

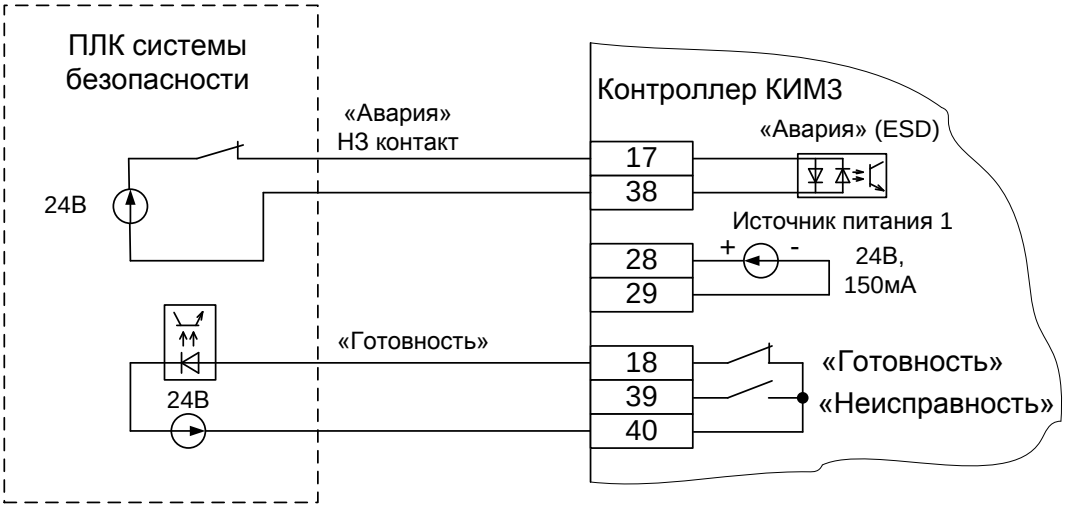
За нормальное состояние принято следующее состояние контроллера КИМ2 и системы безопасности:

- отсутствуют неисправности;
- система готова к выполнению функции безопасности.

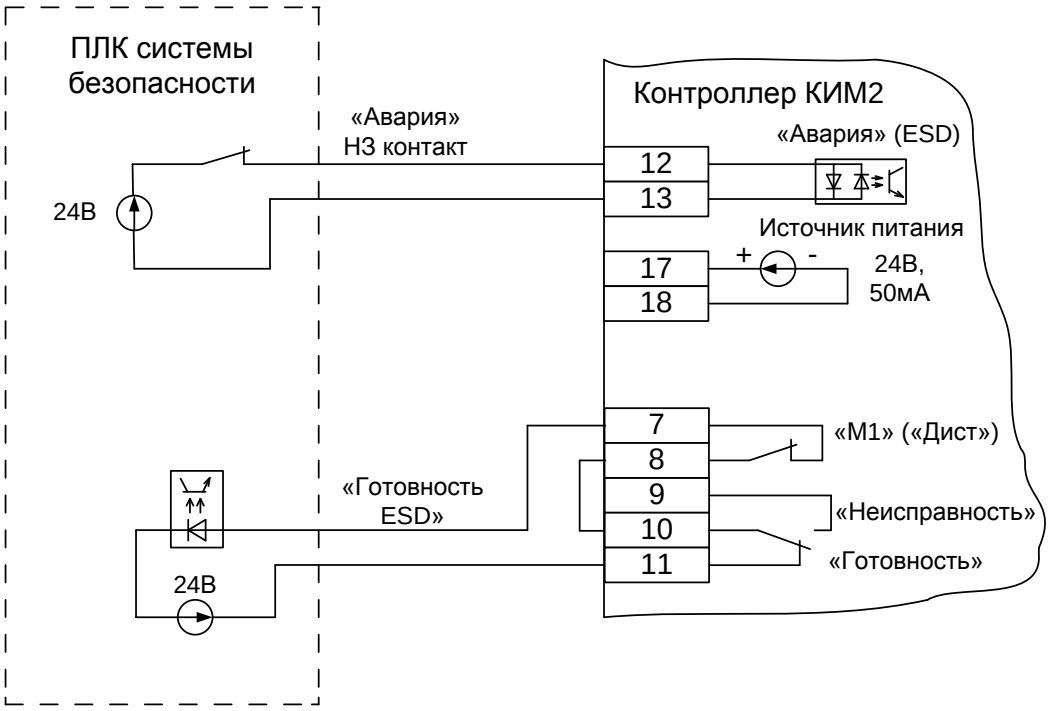
Сигнал "АВАРИЯ" – контакты в нормальном режиме работы замкнуты. В случае аварии их нужно разомкнуть.

Сигнал "ГОТОВНОСТЬ ESD" – формируется последовательным соединением сигнала "ГОТОВНОСТЬ" (нет неисправности) и сигнала "ДИСТ" (переключатель режимов управления в положении "ДИСТ") на многофункциональном выходе "М1" – контакты в нормальном состоянии замкнуты. Цепь размыкается в случае неисправности или если переключатель режимов управления находится в положении "0" или "МЕСТ".

Для питания могут использоваться как внешний, так и внутренний источник питания (контакты 17 и 18).



а) контроллер КИМ3



б) контроллер КИМ2

Рисунок 1 – Схема подключения контроллеров к системе безопасности

Если дискретные входы или выходы стандартной системы управления соединяются с выходами или входами программируемого логического контроллера (далее – ПЛК) системы безопасности, то необходимо обеспечить отсутствие воздействия на функцию безопасности компонентов стандартной системы управления. Отсутствие воздействия также должно обеспечиваться в случае сбоев в стандартных компонентах. Необходимым условием для этого является гальваническая развязка между критичными и не критичными для безопасности компонентами.

3.3 Настройка

3.3.1 Контроллеры должны быть настроены в соответствии с руководством по эксплуатации на ЭП и контроллер.

Настройка функций безопасности контроллеров производится с помощью кнопок панели местного управления (далее – ПМУ), расположенных на лицевой панели. Порядок настройки контроллера КИМ3 приведен в таблице 2.

Таблица 2 – Настройка контроллера КИМ3

Действие	Прядок выполнения
Инвертировать дискретный вход "АВАРИЯ"	Войти в меню настройки. Выбрать пункты меню ***"Аппаратура/Дискретный ввод/Инверсия"***. Установить значение ***"0000 0000 0100 0000"*** и сохранить
Установить функцию для входа "АВАРИЯ"	Выбрать пункты меню ***"Параметры/ I Сигнал Авария/I1"***. Для функции безопасности "Оставаться на месте" (Stayput) установить **I1** = 4 (стоп). Для функции безопасности "Аварийное выключение" (Emergency shut down) установить действие при наличии сигнала "АВАРИЯ": - **I1** = 1 – для перевода арматуры в закрытое положение; - **I1** = 2 – для перевода арматуры в открытое положение; - **I1** = 3 – для перевода арматуры в заданное положение. Заданное положение определяется параметром **I2**
Установить приоритет относительно состояния "превышение момента"	Выбрать пункты меню ***"Параметры/ I Сигнал Авария/I3"***. Установить **I3** = 0, если превышение момента нельзя игнорировать. Установить **I3** = 1, если превышение момента можно игнорировать. В таком случае необходимо использовать арматуру с 3-5 кратным запасом по моменту относительно максимального момента ЭП
Установить приоритет относительно состояния "перегрев электродвигателя"	Выбрать пункты меню ***"Параметры/ I Сигнал Авария/I4"***. Установить **I4** = 0, если перегрев ЭД нельзя игнорировать. Установить **I4** = 1, если допустимо игнорировать перегрев электродвигателя (далее – ЭД). **Игнорирование перегрева ЭД недопустимо во взрывоопасных зонах**

Порядок настройки контроллера КИМ2 приведен в таблице 3.

Таблица 3 – Настройка контроллера КИМ2

Действие	Прядок выполнения
Инвертировать дискретный вход "АВАРИЯ"	Войти в меню настройки. Выбрать пункты меню ***"Hard /dInP /InvE"***. Установить значение ***"08"*** и сохранить

Окончание таблицы 3

Действие	Прядок выполнения
Установить функцию для входа "АВАРИЯ"	Выбрать пункты меню ***"SEtP /IGrP /I.001"***. Для функции безопасности "Оставаться на месте" (Stayput) установить **I.001** = 4 (стоп). Для функции безопасности "Аварийное выключение" (Emergency shut down) установить действие при наличии сигнала "АВАРИЯ": - **I.001** = 1 – для перевода арматуры в закрытое положение; - **I.001** = 2 – для перевода арматуры в открытое положение; - **I.001** = 3 – для перевода арматуры в заданное положение. Заданное положение определяется параметром **I.002**
Установить приоритет относительно состояния "превышение момента"	Выбрать пункты меню ***"SEtP /IGrP /I.003"***. Установить **I.003** = 0, если превышение момента нельзя игнорировать. Установить **I.003** = 1, если превышение момента можно игнорировать. В таком случае необходимо использовать арматуру с 3-5 кратным запасом по моменту относительно максимального момента ЭП
Установить приоритет относительно состояния "перегрев электродвигателя"	Выбрать пункты меню ***" SEtP /IGrP /I.004"***. Установить ***I.004*** = 0, если перегрев ЭД нельзя игнорировать. Установить ***I.004*** = 1, если допустимо игнорировать перегрев ЭД. **Игнорирование перегрева ЭД недопустимо во взрывоопасных зонах**
Настроить дискретный выход "М1" на формирования сигнала "ДИСТ"	Войти в меню настройки. Выбрать пункты меню ***"Hard /doUt /dom1"***. Установить значение ***"01"*** и сохранить

Для ограничения несанкционированного изменения настроек необходимо установить пользовательский пароль.

3.3.2 Порядок ввода в эксплуатацию ЭП с контроллером выполнять согласно с руководством по эксплуатации на ЭП.

4 Работа

4.1 В течении всего срока службы ЭП необходимо соблюдать требования руководства по эксплуатации на ЭП и контроллер.

Условием безопасной работы ЭП является регулярное техобслуживание и проверки с определенной периодичностью (параметр T_{proof}).

Во время работы переключатель режимов управления должен находиться в положениях "ДИСТ". В положениях "МЕСТ" и "0" функция безопасности не выполняется. Для исключения несанкционированного переключения режимов управления на селектор должен быть повешен замок.

Порядок открытия и закрытия при наличии сигнала "АВАРИЯ" совпадает с настройками для режима нормальной эксплуатации. Останов при достижении положения "ОТКРЫТО" или "ЗАКРЫТО" может выполняться, как без уплотнения, так и с уплотнением.

В контроллерах КИМ2 и КИМ3 реализована автоматическая корректировка направления включения по определенному порядку чередования фаз в сети основного питания. Для этого в контроллерах КИМ3 с трехфазным питанием параметр **A12** должен быть равен 6, в контроллерах КИМ2 параметр **A12** должен быть равен 2.

5 Проверка и техническое обслуживание

5.1 Общая информация

5.1.1 К проверке и техническому обслуживанию ЭП с контроллером допускается только квалифицированный персонал, обученный для проведения таких работ. Результаты проверок должны регистрироваться в соответствующих журналах. Необходимо оценить степень влияния проверок и технического обслуживания на другие устройства и производственный процесс.

5.1.2 ЭП с контроллером оснащены системами внутренней диагностики. Диагностика работает непрерывно в режиме простоя и в режиме выполнения команд стандартного управления.

В режиме простоя внутренняя диагностика охватывает:

- исправность датчика положения (связь и исправность микросхемы, наличие магнита);
- исправность датчика момента (связь и исправность микросхемы, наличие магнита);
- исправность датчика перегрева ЭД (связь и наличие);
- исправность системы основного питания (наличие питания, наличие всех фаз и порядок их чередования);
- исправность линии связи сигнала "АВАРИЯ".

В режиме выполнения команд стандартного управления внутренняя диагностика дополнительно охватывает:

- исправность датчика положения по движению выходного органа ЭП;
- исправность датчика момента по изменению момента (контролируется при уплотнении);
- исправность силового коммутатора по току ЭД;
- исправность схемы измерения тока по току ЭД;
- исправность механической части ЭП по перемещению выходного вала.

Так как охват диагностики при выполнении команд стандартного управления значительно больше, чем в простое, для обеспечения необходимых показателей безопасности рекомендуется не реже одного раза в месяц использовать стандартное управление. Для правильного контроля наличия движения ЭП должен быть включен на время не менее 5 с. Если нет возможности проводить такую ежемесячную проверку, то следует заменить ее проверкой неполного хода по 5.2.

5.2 Проверка неполного хода

5.2.1 Проверка неполного хода (далее – ПНХ) может выполняться двумя способами:

- с использованием входа безопасности "АВАРИЯ" – применяется для контроллеров КИМ2, КИМ3;
- с использованием встроенных средств контроллера КИМ3.

5.2.2 Выполнение ПНХ с использованием входа безопасности "АВАРИЯ"

Управление ПНХ должно выполняться безопасной системой ПЛК. Проверка выполняется путем подачи сигнала на вход "АВАРИЯ" (установка на входе "АВАРИЯ" низкого уровня) на время не менее 5 с и контроля наличия сигнала "ГОТОВНОСТЬ". При этом параметр **J8** должен быть не более 5 с. Проверка считается успешной, если во время проверки не снимается сигнал "ГОТОВНОСТЬ" и отсутствуют неисправности.

После проверки, используя стандартную систему управления или местное управление, перевести выходной орган ЭП в исходное положение.

В этом случае для выполнения ПНХ может использоваться схема, приведенная на рисунке 1.

5.2.3 Выполнение ПНХ с использованием встроенных средств контроллера КИМ3

Для выполнения этого способа проверки многофункциональный дискретный вход "Мвх1" настроить на выполнение ПНХ, выбрав с помощью кнопок ПМУ пункт меню ***"Аппаратура/Дискретный ввод/Многофун.вход 1"*** , установить ***"Проверка неполного хода (ПНХ)"***.

После запуска ПНХ (PST) выполняются следующие проверки:

- арматура должна находиться в одном из крайних положений, которое определяется параметром **V1**;

- выполняется движение ЭП из крайнего положения на величину в процентах, определяемую параметром **V2**;

- выполняется движение ЭП обратно в крайнее положение;

- контролируется время движения из крайнего положения и обратно.

Во время проверки не должно происходить защитного отключения и проверка должна успешно завершиться за время заданное параметром **V3**.

Проверка выполняется с наивысшим приоритетом аварийного управления (как сигнал "АВАРИЯ").

Выполнение проверки может быть показано многофункциональным дискретным выходом "М1" или "М2" (при соответствующей настройке).

Схема подключения к системе безопасности для выполнения ПНХ с использованием встроенной системы контроллера КИМ3 приведена на рисунке 2.

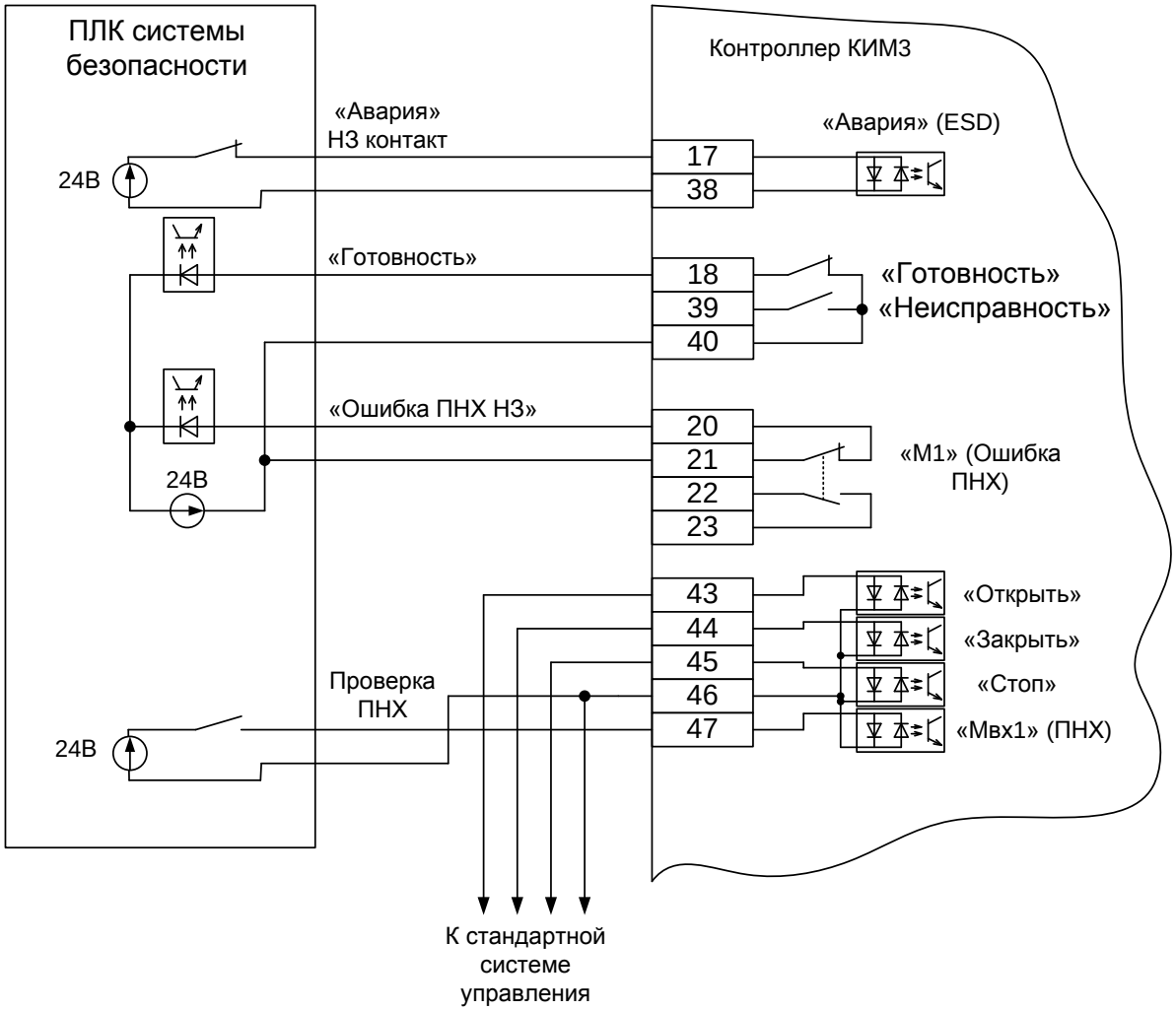


Рисунок 2 – Схема подключения к системе безопасности для выполнения ПНХ с использованием встроенной системы контроллера КИМ3

Если в процессе выполнения проверки поступил сигнал "АВАРИЯ", то будет выполняться действие по этому сигналу. Если в результате действия сигнала "АВАРИЯ" проверка не будет завершена, то будет зафиксирована ошибка проверки.

В результате проверки могут быть выявлены следующие ошибки:

- 1 – ЭП не в исходной позиции;

- 2 – ошибка при движении из исходной позиции (возникла неисправность в ходе движения из исходной позиции);

- 3 – ошибка при движении обратно в исходную позицию (возникла неисправность в ходе движения в исходную позицию);
- 4 – превышено допустимое время выполнения проверки (параметр **V3**);
- 5 – тайм-аут выполнения проверки (проверка не завершена за время **V3**+25 %);
- 6 – проверка прервана (перезапуск процессора).

Номер ошибки (x) показан в надписи на дисплее ***"Ошибка ПНХ (x)"***.

Если в результате проверки обнаружена ошибка, появляется сигнал "НЕИСПРАВНОСТЬ". Также наличие ошибки проверки может быть показано многофункциональным дискретным выходом "М1" или "М2" (при соответствующей настройке). Сигнал "ГОТОВНОСТЬ" не пропадает, если при проверке не возникло неисправностей (ошибки 1, 4, 5, 6) и пропадает, если возникнет неисправность (ошибки 2 и 3).

Для снятия ошибки ПНХ необходимо устранить причину возникновения ошибки и успешно выполнить повторную проверку.

5.3 Контрольные испытания

5.3.1 Контрольные испытания должны проводиться с достаточной регулярностью. Расписание проверок устанавливает эксплуатирующая организация. Показатели безопасности зависят от периодичности контрольных испытаний (T_{proof}). Обычно периодичность составляет T_{proof} = 1 год.

Проверка функций безопасности обязательно должна проводиться после ввода в эксплуатацию, технического обслуживания, ремонта, а также через установленные интервалы T_{proof}.

5.3.2 В контрольные испытания в зависимости от исполнения и конфигурации контроллера входят:

- проверка исправности дискретного выхода "ГОТОВНОСТЬ" для контроллера КИМ3 или дискретных выходов "ГОТОВНОСТЬ" и "М1"("ДИСТ") для контроллера КИМ2;
- проверка функции встроенной ПНХ и исправности дискретного выхода "М1" (***"Ошибка ПНХ (x)"***) – выполняется для контроллера КИМ3;
- проверка правильности настроек;
- проверка выполнения функции "Аварийное выключение";
- проверка выполнения функции "Оставаться на месте".

5.3.3 <u>Проверка исправности дискретного выхода "ГОТОВНОСТЬ" для контроллера КИМ3 или дискретных выходов "ГОТОВНОСТЬ" и "М1"("ДИСТ") для контроллера КИМ2</u>

Установить переключатель режимов управления контроллера в положение "0". При этом контролировать отключение готовности ЭП в системе безопасности.

Установить параметр **C1** = 0 (требуется настройка), выбрав пункты меню:

- для контроллера КИМ3: ***"Параметры/С Парам.управлен /С1"***;
- для контроллера КИМ2: ***"SEtP / CGrP / C.001"***.

Проконтролировать отключение готовности ЭП в системе безопасности и появление индикации неисправности на передней панели контроллера.

Установить параметр **C1** = 1.

5.3.4 <u>Проверка функции встроенной ПНХ и исправности дискретного выхода "М1" (***"Ошибка ПНХ (x)"***) для контроллера КИМ3</u>

Проверку проводить, если ЭП с контроллером КИМ3 настроен на проведение ПНХ встроенными средствами контроллера КИМ3.

Установить ЭП в промежуточное положение или на достаточное расстояние от конечных положений.

Подать команду ***"Проверка ПНХ"*** на дискретный вход "Мвх1" ("ПНХ").

На контроллере КИМ3 должна появиться неисправность ***"Ошибка ПНХ (1)"*** (ЭП не в исходном положении). В систему безопасности должен поступить сигнал "Ошибка ПНХ".

Вернуть ЭП в исходное положение ("ОТКРЫТО" или "ЗАКРЫТО").

Повторно подать команду ***"Проверка ПНХ"*** на дискретный вход "Мвх1" ("ПНХ").

ЭП должен выполнить ПНХ. После успешного выполнения ПНХ неисправность ЭП и сигнал "Ошибка ПНХ" должны отключиться.

5.3.5 Проверка правильности настроек

Войти в меню контроллера. Проверить соответствие параметров, настроек дискретных входов и выходов с сохраненными в журнале при вводе в эксплуатацию.

5.3.6 Проверка функции "Аварийное выключение"

Данная проверка должна проводиться, если ЭП настроен на выполнение закрытия, открытия или перевод в заданное положение по сигналу "АВАРИЯ".

Установить ЭП в промежуточное положение или на достаточное расстояние от конечных положений.

Подать команду стандартного управления в направлении противоположном направлению, установленном функцией "Аварийное выключение".

Подать команду "Аварийное выключение". Для этого установить на дискретном входе "АВАРИЯ" напряжение 0 В.

Функция безопасности работает правильно, если ЭП остановится и выполнит аварийное выключение, т.е. перейдет в безопасное положение.

Не должно быть неисправностей ЭП и не должен пропадать сигнал готовности ЭП в системе безопасности.

5.3.7 Проверка функции "Оставаться на месте"

Данная проверка должна проводиться, если ЭП настроен на выполнение команды "СТОП" по сигналу "АВАРИЯ".

Установить ЭП в промежуточное положение или на достаточное расстояние от конечных положений.

Подать команду "ОТКРЫТЬ" стандартного управления.

Подать команду " Оставаться на месте ". Для этого установить на дискретном входе "АВАРИЯ" напряжение 0 В.

Функция безопасности работает правильно, если ЭП остановился.

Повторить проверку в направлении закрытия.

5.4 Техническое обслуживание

5.4.1 Техническое обслуживание контроллера должен проводить только квалифицированный персонал, специально назначенный для проведения таких работ.

Техническое обслуживание должно проводиться согласно руководству по эксплуатации на ЭП и на контроллер.

По окончании технического обслуживания необходимо выполнить проверку в объеме контрольных испытаний по 5.3.

6 Параметры безопасности

6.1 Расчет параметров безопасности основывается на указанных функциях безопасности. Оценка ЭП с контроллером КИМ3 производится на основе анализа видов, последствий и диагностики отказов (FMEDA – Failure Modes, Effects and Diagnostic Analysis). Анализ FMEDA является этапом оценки функциональной безопасности согласно ГОСТ Р МЭК 61508-2. Методом анализа FMEDA определяются интенсивности опасных и безопасных отказов.

6.2 Интенсивность отказов механических узлов определяется расчетными методами.

Интенсивность отказов электроники определяется расчетными методами на основе РМ 25 446 и на основе данных производителей электронных компонентов.

ЭП с контроллерами КИМ2, КИМ3 относятся к устройствам типа "B", у которых устойчивость к отказам равна 0. Согласно ГОСТ Р МЭК 61508-2 для устройств типа "B" параметр SFF для уровня полноты безопасности УПБ2 (SIL2) должен составлять не менее 90 %.

Показатели безопасности, приведенные ниже действительны только при соблюдении всех требований указанных в этом документе.

Значение PFD_{avg} может рассчитываться по следующей формуле:

$$PFD_{avg} = \lambda_{DU} PTC(\frac{T_{proof}}{2}) + \lambda_{DU}(1 - PTC)(\frac{T_2}{2}) + \lambda_{DD} MTTR \qquad (1)$$

При расчете значений PFD_{avg} необходимо учесть, что контрольные испытания не обеспечивают полное восстановление системы. В расчетах применяются следующие значения:

- PTC = 90 % (охват контрольных испытаний);
- T_{proof} = 1 год (8760 ч) (период контрольных испытаний);
- T_2 = 10 лет (87600 ч) (срок службы);
- MTTR= 72 ч (среднее время возвращения в исправное состояние).

Примеры результатов расчета показателей безопасности приведены в таблицах 4, 5. Данные в таблицах 4, 5 являются примером расчета, и не должны использоваться для расчета показателей системы безопасности. Для расчета показателей безопасности системы должные использоваться данные приведенные в паспорте на ЭП.

Расчет PFD_{avg} для ЭП с контроллерами КИМ2 и КИМ3 приведены соответственно в таблицах 4 и 5.

Таблица 4 – Пример результатов расчета показателей безопасности для ЭП с контроллером КИМ3

Функция безопасности	Аварийное отключение (Save ESD)	Оставаться на месте (Save STOP)
λ_S	6557 FIT	8973 FIT
λ_{DD}	2562 FIT	188 FIT
λ_{DU}	180 FIT	139 FIT
SFF	98,1 %	98.5 %
DC	27,6 %	2 %
PFD_{avg} T_{proof} = 1 год	$1{,}683 \cdot 10^{-3}$	$1.168 \cdot 10^{-3}$
Уровень полноты безопасности	УПБ 2 (SIL2) (HFT = 0)	УПБ 2 (SIL2) (HFT = 0)

Таблица 5 – Пример результатов расчета показателей безопасности для ЭП с контроллером КИМ2

Функция безопасности	Аварийное отключение (Save ESD)	Оставаться на месте (Save STOP)
λ_S	1736 FIT	2439 FIT
λ_{DD}	962 FIT	332 FIT
λ_{DU}	155 FIT	85 FIT
SFF	94,6 %	97,0 %
DC	33,7 %	11,6 %
PFD_{avg} T_{proof} = 1 год	$1{,}36 \cdot 10^{-3}$	$0{,}728 \cdot 10^{-3}$
Уровень полноты безопасности	УПБ 2 (SIL2) (HFT = 0)	УПБ 2 (SIL2) (HFT = 0)

Приложение А
(обязательное)
Перечень документов, на которые даны ссылки в настоящем руководстве

Таблица А.1

Обозначение	Наименование документа	Номер пункта руководства
ГОСТ Р МЭК 61508-1-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования	Введение, таблица 1, 2.1
ГОСТ Р МЭК 61508-2-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам	Введение, 2.1, 6.1, 6.2
ГОСТ IEC 61508-3-2018	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению	Введение, 2.1
ГОСТ Р МЭК 61508-4-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения	Введение, 2.1
ГОСТ Р МЭК 61508-5-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности	Введение, 2.1
ГОСТ Р МЭК 61508-6-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3	Введение, 2.1
ГОСТ Р МЭК 61508-7-2012	Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства	Введение, 2.1
ГОСТ Р МЭК 61511-1-2018	Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования	Введение, 2.1
ГОСТ Р МЭК 61511-2-2018	Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1	Введение, 2.1
ГОСТ Р МЭК 61511-3-2018	Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности	Введение, 2.1
РМ 25 446-90	Рекомендуемый материал. Изделия приборостроения. Методика расчета показателей безотказности	6.2

АО "АБС ЗЭиМ Автоматизация"
428020, Россия,
Чувашская Республика,
г. Чебоксары, пр. И. Яковлева, 1
тел.: (8352) 30-51-48, 30-52-21
www.abs-zeim.ru